National Technical University
"Kharkiv Polytechnic Institute"

MODERN PROBLEMS OF COMPUTER SCIENCE AND IT-EDUCATION

collective monograph

PREMIER Publishing
VIENNA, AUSTRIA
2020

Editorial Board:

Karina MELNYK — PhD in Technical Science, Associate Professor, Department of Software Engineering and Management Information Technologies of National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine

Olexander SHMATKO — PhD in Technical Science, Associate Professor, Department of Software Engineering and Management Information Technologies of National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine

Scientific Board:

Michail GODLEVSKIY — Doctor of Technical Science, Full Professor, Department of Software Engineering and Management Information Technologies of National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine

Serhii YEVSEIEV — Doctor of Technical Science, Senior Research, Department of Cyber Security and Information Technology, Simon Kuznets Kharkiv National University of EconomicsEvseev, Kharkiv, Ukraine

Olga CHEREDNICHENKO — PhD in Technical Science, Associate Professor, Department of Software Engineering and Management Information Technologies of National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine

Reviewers:

Igor GAMAYUN — Doctor of Technical Science, Full Professor, Department of Software Engineering and Management Information Technologies of National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine

Authors:

ALEKSIYEV Volodymyr, BILOVA Mariia, BORYSOVA Natalia, CHEREDNICHENKO Olga, FEDORCHENKO Volodymyr, GOLOSKOKOV Alexander, GOLOSKOKOVA Anna, HARASYMCHUK Oleh, HAVRYLOVA Alla, HOLUBNYCHYI Dmytro, IVASHCHENKO Oksana, KALACHOVA Vironika, KOZULIA Mariia, KOZULIA Tatiana, LIUTENKO Irina, MELNYK Karina, MELNYK Marharyta, MILOV Oleksandr, OPIRSKYY Ivan, ROMASCHENKO Natalya, RYABUKHA Yurii, SALO Nataliia, SHMATKO Olexander, SOROKA Mykhailo, TRETIAK Viacheslav, TRYSTAN Andrii, VLASOV Andrii, VOVK Maryna, YANHOLENKO Olha, YEVSEIEV Serhii.

Modern Problems Of Computer Science And IT-Education : collective monograph / [editorial board K. Melnyk, O. Shmatko].– Vienna : Premier Publishing s.r.o., 2020.– 236 p.

ISBN 978-3-903197-19-0

The collective monograph highlights modern problems of development and using information technologies for resolving some issues in different domain areas. The proposed theoretical methodologies, models and practical approaches are considered and investigated in the context of IT-education, software engineering, artificial intelligence and cybersecurity. Every chapter describes methods, efficient algorithms and resolutions specific for the particular domain area and field of knowledge.

Authors are responsible for the content and accuracy.

© Collective authors, 2020

© Premier Publishing s.r.o. 2020

Contents

CHAPTER I. DECISION SUPPORT SYSTEMS AND INTELLIGENT SYSTEMS 4

The decision-making support in case of transboundary emergency 4

Mathematical models of decision-making in environmental management information systems 17

The problem of decision-making in conditions of fuzzy initial information 28

Methodical bases of information support for complex analysis of system objects difficult / weakly structured 43

CHAPTER II. CYBERSECURITY 65

Self-organizing organizational structures of cybersecurity systems 65

Improved umac algorithm with crypto-code mceliece's scheme 79

New method for assessing the risk of automated information systems information security based on fuzzy-multiple approach 93

Security analysis of LTE technology 105

Technology of protection video informational resource in the critical information infrastructure 120

Cyber safety prevention methods for children 132

CHAPTER III. DATABASE AND KNOWLEDGE SYSTEMS 142

Database replication method based on the task of (0,1)-knapsack 142

CHAPTER IV. PROJECT MANAGEMENT AND SOFTWARE ENGINEERING 157

Static and dynamic models for planning the quality improvement of the software development process 157

Information support for distributed teamwork knowledge management 169

CHAPTER V. IT-EDUCATION 193

Automated system for students' knowledge testing 193

Models and methods of preparing effective schedule in adaptive educational system 208

Automation of the educational process in Ukraine higher military education institutions 224

CHAPTER I. DECISION SUPPORT SYSTEMS AND INTELLIGENT SYSTEMS

The decision-making support in case of transboundary emergency

Olga Cherednichenko
Doctor of Philosophy, Associate Professor
Department of Software Engineering and Management Information Technologies
National Technical University "Kharkiv Polytechnic Institute"
ORCID https://orcid.org/0000–0002–9391–5220

Maryna Vovk
Doctor of Philosophy, Associate Professor
Department of Software Engineering and Management Information Technologies
National Technical University "Kharkiv Polytechnic Institute"
ORCID https://orcid.org/0000–0003–4119–5441

Abstract. *This paper is devoted to the support of decision-making processes in the case of transboundary emergency. Subsystems for collecting data on the state of the environment are distinguished. The use of electronic remote sensing measuring devices is carried out using a connection to a base station or via a telemetry network. The meta-model of the device provides a standard for the representation of devices in the decision-making system in emergency situations of a transboundary nature. The model for constructing an adaptive infrastructure for a flexible decision support system in case of transboundary emergency has been developed.*

Keywords: *Decision-making, Decision support systems, Transboundary emergency, Environmental monitoring, Device meta-model*

Introduction

The society development at the present stage is increasingly faced with problems of ensuring the safety and protection of mankind and the environment. A man-made impact on the natural environment is growing and the intensification of the use of natural resources, but not always rational and without proper technological measures. In many countries of the world, there is a steady tendency to increase the number of industrial accidents and destructive natural phenomena. Preparation of complex decisions for reconciling the contradictory conditions of economic development and the safe functioning of industrial facilities is a prerequisite for the

national security of each country. A significant place in the problem of providing industrial and environmental safety is safety assessment.

Modern management of the consequences of man-made accidents, natural disasters and various types of emergencies is based on the active use of information technology. The activity related to information technology in this process is to determine the management system and its associated resources, establish communication with these resources and deploy them where necessary. The problem of organizing the collection, processing, and analysis of information, is currently one of the most urgent and unresolved issues. The use of information computer systems makes this process more effective.

Support of decision-making

Nowadays the support of decision-making is understood as the process of understanding the situation in order to make the optimal decision and determine the purpose, planning and generating ways of its implementation, the formation of a variant using expert knowledge and methods of mathematical programming, modeling the consequences of the decisions made to evaluate them. How the decision is considered a variant of one or another action and solving the situation for an optimal solution – finding a solution using the decision support system (DSS), configured for the domain [1–3]. Information technology is used to implement the DSS, which ensures the decision-making process at all its stages (Fig. 1).

It provides the mechanisms of communication between devices and interfaces to connect multiple devices into a single network. This approach allows providing the interface with compatible and incompatible devices, thereby making them interact efficiently. The benefit of the suggested architecture is that it allows deploying the emergency infrastructure in a quick manner and gathering the environmental information in a single data storage integrated with the decision support system. This in turn, increases the chances to eliminate the damage caused by an accident due to the well-judged and effective decisions. The challenge associated with the usage of the developed architecture is the volume of data that has to be processed and the processing itself. Since the collected data may be characterized as incomplete, inconsistent and inaccurate, the modern techniques of its filtering, cleaning, processing and estimating should be used.

The following generalized stages of the decision-making process [3, 4] can be distinguished in the development of DSS:

1) assessment of information support for identifying the state of the object;
2) diagnostics of the situation of decision-making and the definition of goals;
3) planning of actions;
4) the formation of solutions options.

In real life, the complex task of monitoring the state of the environment often arises to correctly determine the situation and make the right decisions [2]. In this case, it is necessary to monitor all the indicators of the state of the environment at the same time. A system that could perform such a task should have the ap-

propriate software, hardware, and information support. There is a global problem of environmental monitoring in transboundary areas, since providing complete information and a clear coordination plan in the event of an emergency is impossible [1]. Various measuring and recording devices are used to estimate emissions and identify the most harmful substances. Emergency services are used by various personal devices that collect current information about the current state of the environment. The information collected should be communicated quickly and uninterruptedly at the command center to coordinate activities and ensure communication between different geographically separate locations.

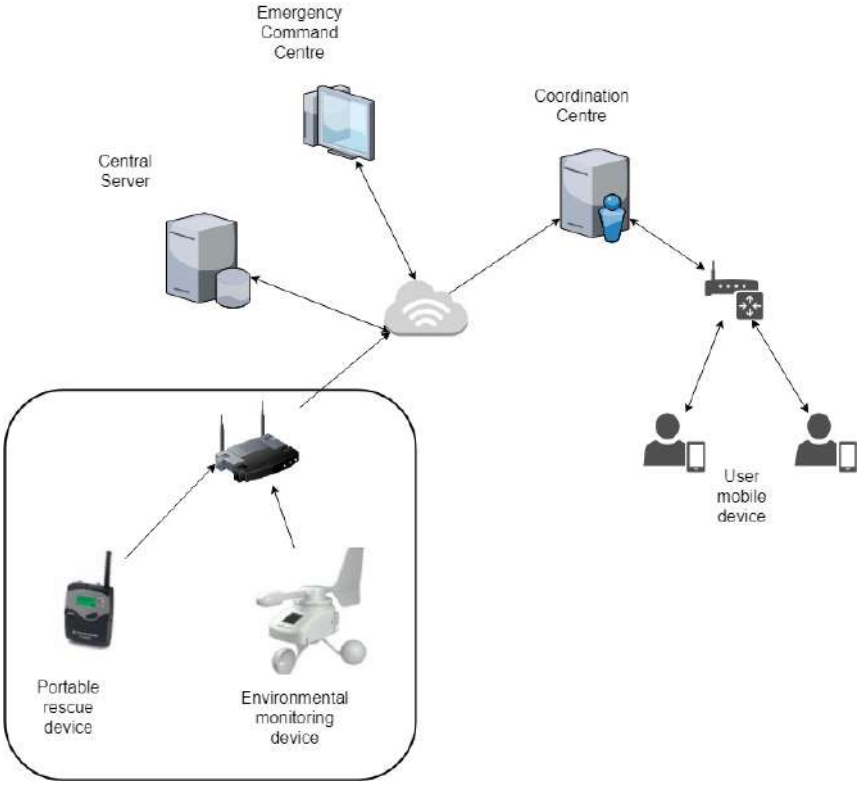


Figure 1. – DSS architecture

Usually, in any territory, there are already a number of observation networks belonging to different services, but they are separated, not coordinated in chronological, parametric, and other aspects. Therefore, the task of preparing estimates, forecasts, criteria of alternatives to the choice of managerial decisions based on regional departmental data is, in general, uncertain.

The following subsystems for collecting data on the state of the environment are distinguished [5]:

– geophysical monitoring (analysis of atmospheric pollution data, exploring meteorological and hydrological data of the environment, as well as studying elements of the inanimate component of the biosphere, including objects created by man);

– Climatic monitoring (control and forecasting of fluctuations of the climatic system: covers the part of the biosphere that influences the formation of the climate: the atmosphere, the ocean, ice cover, etc. Climatic monitoring is closely connected with hydrometeorological observations.);

– biological monitoring (based on monitoring of the reaction of living organisms to environmental pollution); monitoring of the population's health (a system of measures for monitoring, analyzing, estimating and forecasting the state of physical health of the population), etc.

Currently, in monitoring programs, in addition to the traditional "manual" selection, the emphasis has been put on the collection of data using real-time electronic remote sensing measuring devices.

The use of electronic remote sensing measuring devices is carried out using a connection to a base station or via a telemetry network, or through terrestrial lines, cellular telephone networks or other telemetry systems. The advantage of remote monitoring is that many databases can be used in a single database for storage and analysis. This dramatically increases the response rate when reaching the threshold levels of monitored indicators, for example, in individual control areas. This approach allows monitoring activities to take immediate action if the threshold is exceeded.

The necessary part of any environmental monitoring or measurement project is the use of equipment. Some devices, such as counters and flight kits, are designed for sampling. Others, such as analyzers, data loggers and data buoys, are intended for long-term monitoring programs. Although buoys, probes and automated samplers, as a rule, are specific to water quality control projects, sensors and data loggers can be used to monitor virtually any environmental parameter. Data centers, when used together with telemetry and data logger, provide real-time data and access to the project from anywhere at any time. Measurement equipment is selected based on the accuracy, budget, and whether remote monitoring is required. When responding to emergencies where there is a potential danger to the environment, it is very important that the rescue service and its employees first determine what dangerous factors need to be measured. Rescues in transboundary emergency situations require intensive training so that the saviors know what potential risks exist and how to properly measure, prevent and control the danger. Rescuers can measure the risk by using monitoring equipment directly on the spot. Examples of such equipment are:

– pocket testers of various ground, water, and other fences;
– portable sets of chemical tests;
– portable monitors and sensors;
– portable weather stations, etc.

The practical implementation of the universal environmental monitoring complex is based on the principles of service-oriented processing of digital data. Support for management decisions is based on the creation and use of structured information on the state of the environment, as well as on the mechanisms for processing these data in order to identify recommendations.

Provision of an interface between the medical devices used for monitoring and the software system of information processing is provided by the service-oriented architecture of the device (SOAP). The purpose of the SOAP software component is to provide an interface with compatible and incompatible devices that allow them to interact. Conceptually SOAP acts as an intermediate level between devices and software applications. The feature of SOAP is that programs and devices generate service objects that are perceived by the system. The application service defines the requirements for some functionality or function of the device, while the device service object defines the capabilities of the device.

Traditionally, Service Oriented Architecture (SOA) services provide an interface between applications and enterprise systems. SOAP leads this abstraction to the level of communication of devices. The services provide an interface between devices (supporting data processing and management) and applications (which consume data and user management). By providing two levels of service objects between applications and devices, applications can refer to aggregated data and management, not to the parameters of a specific device. Similarly, device object objects can use device services as managed interfaces with device parameters that govern their interaction with devices. Additional benefits of this architecture are described below.

Differentiating device features from application software makes it possible to test applications and their associated services, regardless of devices. Application services can set the minimum functional requirements for potential device parameters. By verifying applications and application services for compliance with minimum requirements, it can be assumed that any group of devices that meet the aggregate of requirements can safely and effectively perform the operations specified in the application.

Application services determine atomic procedures for device parameters that can be verified along with the corresponding applications. The device services define access to parameters (device data, settings, actions) that prevent multiple applications from controlling one setting and allow similar settings to be combined within a single service.

This architecture has a drawback, which is to create additional layers between applications and devices. Nevertheless, it has the advantage of simplifying the structure of the service. Application services should be occupied only by defining the type of data and management required for the application, while the device services handle only the access and organization of the device data. This leads to more simple requirements for each set of services. Consequently, the complexity and responsibility of applications and devices are greatly reduced.

SOAP is an intermediate layer that allows applications to communicate with devices without relying on technology or platforms that depend on device drivers. Instead, SOAP generates intermediate software code for each device based on the device model. SOAP has two interfaces: the interface of the application and the interface of the device. The application interface allows applications to request certain device services, such as instrument metrics, settings, and signal information. The device interface supports SOAP communication hardware. The purpose of SOAP is to compare the requirements of the application data with the device model and to compare these requirements with the capabilities of compatible devices. This reconciliation process serves to confirm that applications are compatible with connected devices, as well as create semantically valid connections between applications and devices. To establish a connection between the application and the device, SOAP performs the following actions:

1. The application is introduced into the system: SOAP provides an API that allows the application to describe its requirements.

2. The device connects to the system.

3. The device model is loaded into the SOAP: The device model is introduced and associated with the corresponding devices.

4. Generation of services: requirements of the model of the device and the application are transferred to the services of the device and application services.

5. Services are combined: application services are combined with the services of the devices. Checking if all application services are satisfied is checked.

6. Generation of message processing module: The module is generated from the grammar contained in the model of the device.

7. Generate Dynamic Protocol: The protocol manager is generated from the grammar contained in the device model.

8. Application Launch: Communication between the application and the associated device starts.

Because SOAP acts as an intermediate layer, it must provide interfaces for all components. The application interface consists of an API that allows applications to register with SOAP and describe their requirements. Applications are presented as application objects that contain methods for returning object descriptions. SOAP makes a request for a list of requirements from the side of the application, generates application services from the requirements and allows the application to send and receive messages. The requirements described in the applications are presented as an application service object, each of which contains one or more service object objects. The requirement should be related to the compatible service of the device. The application service also serves as a communication interface for applications.

SOAP allows any device to be connected to an information system, provided that the corresponding description of the device is provided to the system. If the device is “fully compatible”, it will automatically download its model when connected. Otherwise, the model should be downloaded with the help of the

administrator. This approach uses a model that supports various communication interfaces, including a serial port (RS-232), an Ethernet port (TCP or UDP), a USB port, or a wireless connection. The device model is translated from an XML representation into an object model so that it can be used in SOAP. Objects inside the model of the device are realized as objects of abstract elements of the model, while the parameters of the model are implemented as objects of the parameter.

Service-oriented architecture is shown in the Figure 2.

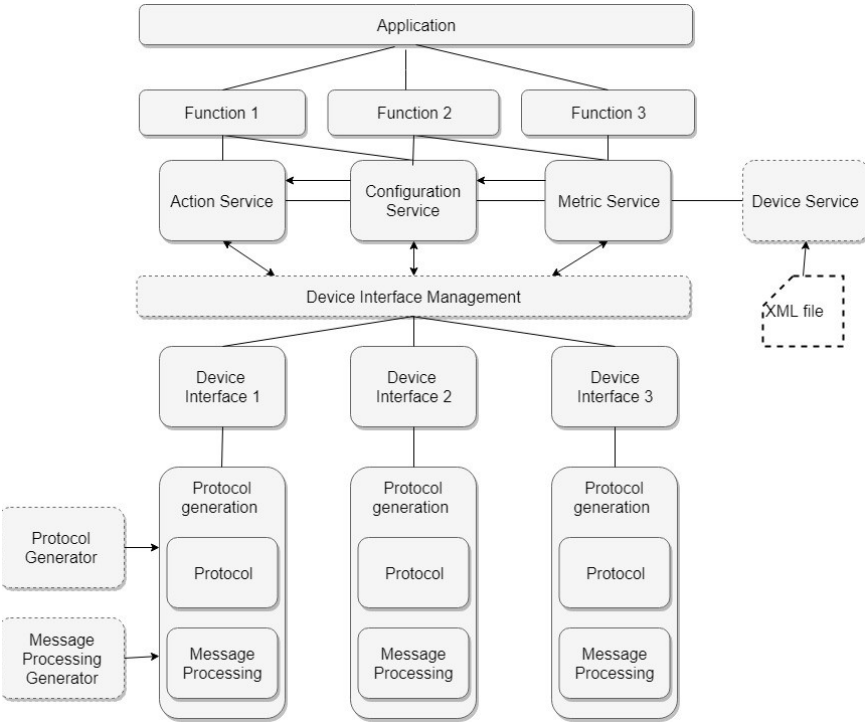


Figure 2. – Service-oriented architecture

The meta-model of the device (MIM) provides a standard for the representation of devices in the decision-making system in emergency situations of a transboundary nature. It reflects the communicative capabilities and properties of the device, such as gauge indicators, warning types, drives functions, status messages. The model is based on an abstract representation of a generalized device for collecting environmental parameters (Fig. 3). One of the requirements of the system is the availability of a standard way for communication between the device and the system. In particular, the following information should be distributed among interacting subsystems:

1. Functionality: systems should understand the types of messages allowed and the effect caused by each type of message.

2. Semantic data: values transmitted from the device should be interpreted by the receiver.

3. Message format: The receiver should be able to parse message values according to their semantics and type of message.

4. Communication protocol: Devices should know how and when messages are sent.

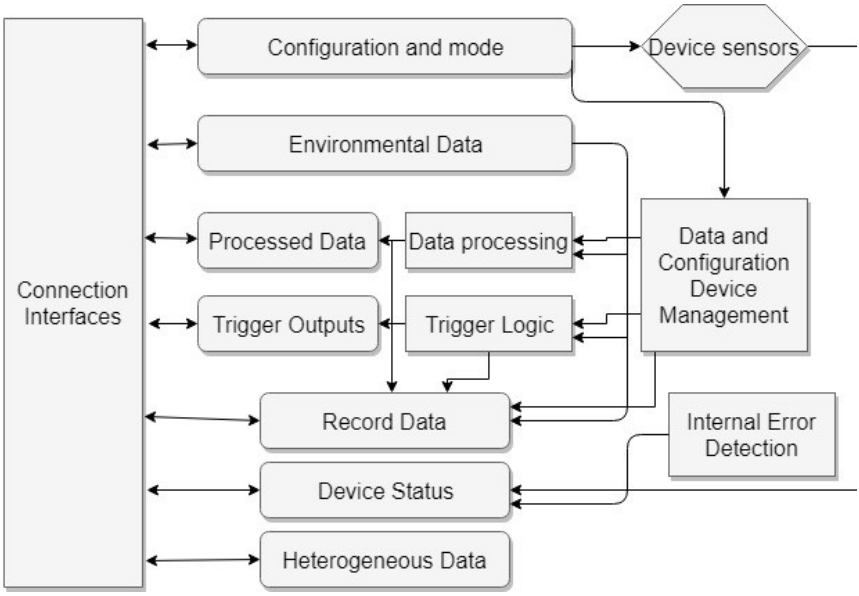


Figure 3. – General structure of the device

The first two requirements relate to the content and use of device messages. The control system should be able to understand the contents of the parameters it receives, as well as the consequence of the commands that it sends to the device. The third and fourth requirements deal with the structure of alerts and the communication interface. In terms of the OSI model, the message format is processed at level 5–7, while the communication protocol is processed at levels 1–4. Given these requirements, there are two issues that the decision-making system in emergencies of a transboundary nature should address. First, how to organize and present a description of the device for collecting environmental parameters, that is, the problem of representation (simulation) of the device. Second, how to get a description of this device for a control system, provided that the control system does not have a priori knowledge of the structure of the device and protocols; this problem can be considered as a translation problem. These problems can be easily solved if each device has a fixed, relatively small set of parameters, and if each device uses the same communication protocol and message structure.

Devices for collecting environmental parameters cover a much wider area than the area of the peripheral devices of the personal computer. The list of possible parameters is enormous and constantly growing, as well as the list of patented communication protocols. In order to solve this problem, you must first determine the scope of the equipment in terms of data semantics, message formats, and communication protocols. This leads to the creation of a large list of properties of the device, functions and protocols. After this list is created, it is possible to classify similar properties together, which gives generalized structures common to all medical devices. These structures can be used to create descriptions for specific devices.

The meta-model of the device is the result of analysis and classification. By discovering common elements on all environmental parameter collectors, you can create a language to describe specific devices, which is a prerequisite for maintaining device functionality and communicating with the decision-making system in emergencies of a transboundary nature.

The subject domain model is a field of knowledge that should cover MSM. After examining a plurality of examples of devices that can be applied to the collection of environmental parameters, it has been found that the devices contain all or some of the following:

– sensors for measuring environmental parameters;

– internal logic that allows you to determine the behavior of the device (including monitoring of sensors, actuators and data processing inside the device);

– internal memory for storing commands, sensor data, device status data, sensor data processed;

– an interface through which a rescue team member can control the device, observe its state, read its internal data;

– an interface by which the control system can communicate with the device to control its operation or read data;

– the interface to which the device can be connected.

The meta-model of the device is the adaptation of the information object-oriented domain model. Objects inside the model contain attributes and methods that describe the properties and functionality of a component of a simulated device. When a set of objects is selected and organized to describe a particular device, these objects formate an information database for this device.

Objects within the model are organized in eight packages, which include (Fig. 4):

– system package: contains a general description of the device, that is, the combination of all functions of the device;

– environmental package: data channels and metrics that determine the measurement methods of environmental indicators;

– physical package: provides signals for the environment package;

– control package: provides remote control of the device;

– an additional service package: contains objects that control the properties of the device and allow you to collect data from the device;

– communication package: manages the communication protocol of the lower level;
– archiving package: supports data logging from devices;
– the data packet: contains different data on the environment.

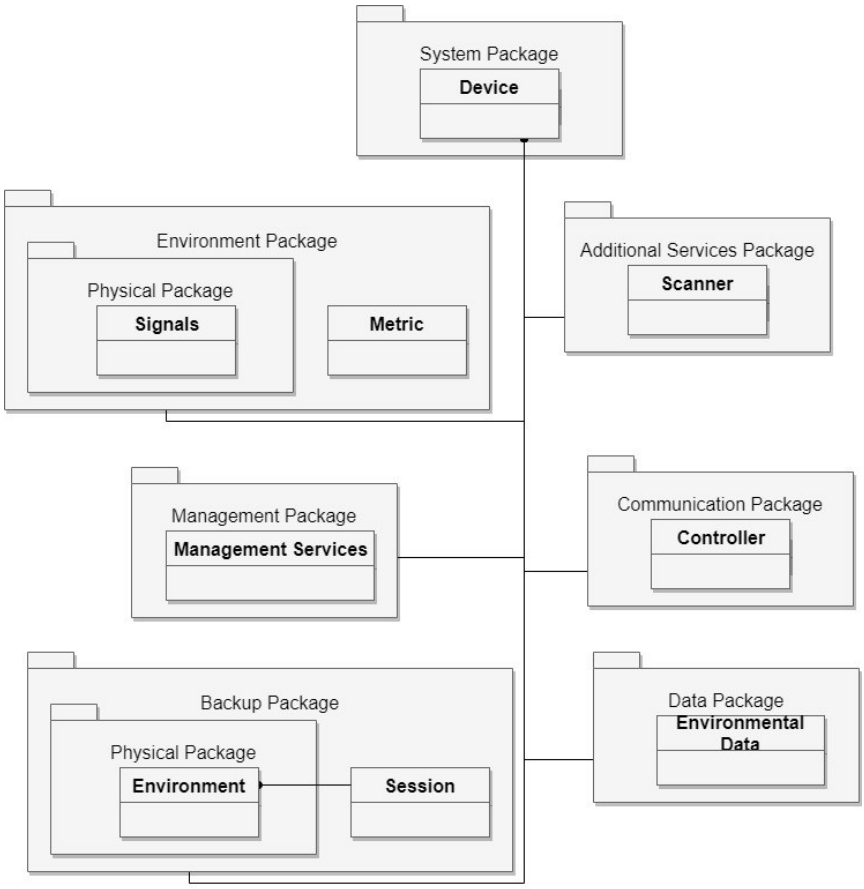


Figure 4. – Structure of the information model of the domain

Like an information model, the device's meta-model is organized in the form of a functional hierarchy of the device. Figure 5 shows the meta-model of the device at the high level of the object model, which can be implemented in practice as an XML schema that allows you to write model models in the form of XML documents.

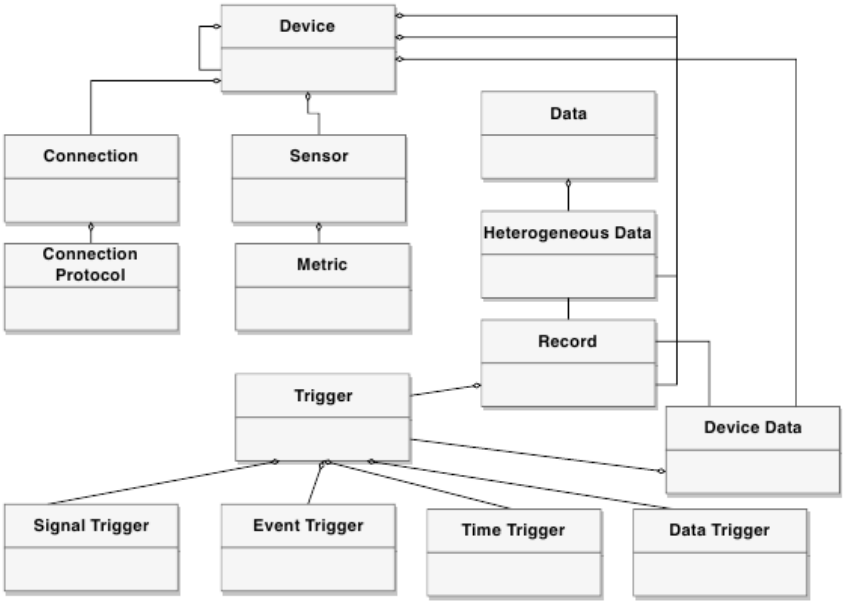


Figure 5. – The structure of the device's meta-model

As in the information models, objects within MMP are grouped in packages, the structure of which is given below:

– device: contains the model of the device of the upper level (object Device), is an analog of the system package;

– sensor: describes the sensors of the device, using Metric and Setting objects.

Data: contains device data, such as device performance information, log data, etc.;

– trigger: contains objects for processing data, as well as facilities for providing messages;

– Communication: describes the communication interfaces and protocols of the device similar to the package.

MSM is designed to be easily encoded as an XML schema. It is built from objects that are grouped in packages. Objects are assigned an object type and three attributes and at least one parameter. Objects can also contain other objects, forming a hierarchy of object types. Most of the information associated with the object is within its parameters. Each parameter contains data values, along with a set of attributes. While the set of object types and attributes is finite, the device model can determine its own types of parameters and attributes of parameters.

Simple devices for registering environmental parameters will have only one "Device" object in their model. More complex devices, such as a monitored lethal device, can be connected to other devices in a hierarchical order. It allows using a model to describe different device topologies.

Conclusion

In the case of transboundary emergencies, the process of decision-making requires monitoring of the environment state; organizing of subsystems interaction, collection, and processing of data. The ecological system is considered as a complex object, the state of which cannot be estimated explicitly.

Devices for collecting environmental parameters cover a much wider area than the area of the peripheral devices of the personal computer. The list of possible parameters is enormous and constantly growing, as well as the list of patented communication protocols. In order to solve this problem, firstly it is reasonable to determine the scope of the equipment in terms of the semantics of data, message formats, and communication protocols. This leads to the creation of a large list of properties of the device, functions, and protocols. If the list is created, it is possible to classify similar properties together, which gives generalized structures common to all devices. These structures can be used to create descriptions for specific devices.

The model of environmental assessment allows determining the level of environmental safety on the basis of the obtained values of indicators by monitoring results. The ecological system is considered as a complex object, the state of which cannot be evaluated explicitly, therefore, it is proposed to form an estimate of its state on the basis of observed parameters. In this work, it is proposed to measure the values of environmental safety indicators on the basis of a one-parameter logistic model.

Thus, a model for constructing an adaptive infrastructure for a flexible decision support system in case of transboundary emergency has been developed. The issues of ensuring the interoperability of components through the conceptual models of devices and external subsystems are considered. The advantages of the developed method of processing of ecological information on the basis of creating a system of attributes and maximizing their information content in terms of the amount and time of data processing of monitoring are considered.

References:

1. Tkachenko V. The Concept of Device Meta-Model for Real-Time Communication in the Transboundary Environment Monitoring System / V. Tkachenko, O. Cherednichenko, M. Godlevskyi // Problems of Infocommunications. Science and Technology: PIC S&T, 2018. Conference Proceedings. October 9–12. – Kharkiv. Ukraine.– 2018. by IEEE, Inc. 2018.
2. Power D. J., Sharda R., Burstein F. Decision support systems.– John Wiley & Sons, Ltd. 2015.
3. Henrique dos Santos P., Neves S. M., Sant'Anna D. O., Henrique de Oliveira C., & Carvalho H. D. The Analytic Hierarchy Process Supporting Decision Making For Sustainable Development: An Overview Of Applications. Journal of Cleaner Production (2018). Doi:10.1016/j.jclepro.2018.11.270.

4. Furems E. Knowledge-based multi-attribute classification problems structuring / D. Ruan, J. Montero, J. Lu, L. Martinez, P. D'hondt, E. Kerre // Computational Intelligence in Decision and Control.– Singapore: World Scientific Publisher, 2008. – P. 465–470.
5. Chettri N. et al. Long term environmental and socio-ecological monitoring in transboundary landscapes // International Centre for Integrated Mountain Development (ICIMOD) – Kathmandu, Nepal. 2015.

Mathematical models of decision-making in environmental management information systems

Olha Yanholenko
Doctor of Philosophy, Associate Professor
Department of Software Engineering and Management Information Technologies
National Technical University "Kharkiv Polytechnic Institute"
ORCID https://orcid.org/0000–0001–7755–1255

Oksana Ivashchenko
Phd student, assistant
Department of Software Engineering and Management Information Technologies
National Technical University "Kharkiv Polytechnic Institute"
ORCID https://orcid.org/0000–0003–3636–3914

Abstract. *The given work represents the mathematical models that can be used in order to provide an effective functioning of environment management information systems. The decision support component of such type of systems may rely on a set of fuzzy models or models of artificial intelligence, in particular Intelligence Theory. The classification of fuzzy models based on fuzziness representation is suggested. The tools of algebra of predicates and the comparator identification models are described.*

Keywords: *Decision-making, Decision support systems, Environment management information systems, Fuzzy models, Artificial intelligence models*

Introduction

One of the priority directions of the national security of Ukraine is to provide ecologically and technologically safe conditions for citizens' life, preservation of the environment and rational use of natural resources. The development of the information and methodological basis of the ecological safety systems should be based on three components of sustainable ecological, social and economic development in the context of improving the quality of the environment and the safety of people's lives. One of the promising areas of such research is the search for new methodological approaches to solving environmental problems and the creation of intelligent decision support systems in managing the environmental quality of the environment.

The given work considers mathematical tools that are used to process data in order to implement management functions in ecological security systems. The basis of most information systems is the recording of statistical data. Preliminary data analysis involves an assessment of the center of distribution, variation, distribution form. The statistical methods of processing information include the following types of analysis, such as: dispersion, factor, cluster, regression, correlation. Data mining is used to identify hidden knowledge stored in collected information [1]. Data Mining methods include: basic methods based on overview; fuzzy logic;

genetic algorithms; neural networks. Thus, decision support systems (DSS) rely on a wide range of mathematical tools represented by a sufficiently developed set of methods and approaches for collecting, processing and storing data.

Mathematical Fuzzy Models of Decision-Making

It is necessary to include the statement of problems which are connected with the use of the theory of fuzzy sets to the special class of tasks of management of ecological safety. This is substantiated by the fact that the parameters and variables are not certain values and cannot be described by distribution laws based on sufficient statistical data. Therefore, there is a need for analysis of models and algorithms in decision support systems with fuzzy outcomes that can be used in environmental safety management tasks, in particular risk assessments. The type of models and algorithms in decision support systems, methods of their research will essentially depend on ways of describing the source data on the basis of the theory of fuzzy sets. Decision-making problems can be classified in the following way [2].

By means of fuzziness representation:

a) using the membership function $\mu_A(x)$, where A is a fuzzy set in X, $x \in X$. Y – a set of possible values of the membership function (MF);

b) using a set of hierarchically ordered precise sets of levels;

c) with combined fuzzy-statistical approaches that take into account both the vagueness of the parameters and the stochasticity of their membership functions.

By area $\%$:

a) the whole base set $\%$;

b) subsets of the base set $\%$ (for example, fuzzy sets of the level);

c) a numerical axis that generates a special class of fuzzy sets – fuzzy numbers.

By area Y:

a) interval [0, 1] – most often used;

b) the entire numerical axis or its individual intervals;

c) a natural number of numbers;

d) a finite or infinite distributive grid L;

e) some linearly ordered set;

f) fuzzy set.

As a result, we get a fuzzy MF

$$\mu_A(x) = \left(y,\ \mu_B(y)\right). \tag{1}$$

By the nature of belonging $\mu_A(x)$ to the value of the set Y:

a) $\mu_A(x) \in Y$;

b) $\mu_A(x) \subset Y$.

Such fuzzy sets have been called interval-valued.

As an example, let's consider the vector set:

a) the membership function is defined for the entire vector (homogeneous fuzzy sets) $x = \left(x_1, x_2, ..x_n\right) \in X,\ \mu_A(x) = \alpha$;

b) several MF are defined for the whole vector (vector-valued fuzzy sets) $x=(x_1,x_2...x_n)\in X,\ \mu_A(x)=(\mu_{A_1}(x),....\mu_{A_m}(x))$;

c) MF are defined for each element of the vector separately (heterogeneous fuzzy sets) $x=(x_1,x_2...x_n)\in X,\ \mu_A(x)=(\mu_1(x_1)...\mu_n(x_n))$.

One of the main elements on the basis of which the theory of fuzzy sets is constructed is a method of representing fuzzy-based MF, which in turn, is used in models and algorithms of decision support systems (DSS). Therefore, let's briefly consider the basic approaches to the construction of MF.

Currently, it is possible to distinguish two groups of methods of constructing MF: direct and indirect. They in turn fall into two subgroups of methods that differ in the way of an expert survey: a group (used by a group of experts) and an individual (one expert is involved). In direct methods, the expert directly sets the rules for determining the values of the MF, which characterizes the concept *A*. In indirect methods, the value of MF is chosen to satisfy pre-formulated conditions. Expert information is only the source code used for further processing. In this case, additional conditions may be imposed both on the form of information received and on the processing procedure. An example of such a condition for pairwise comparison of objects is the following statement. If one of the objects is rated α times more appropriate than the other one, then the second one is $1/\alpha$ more prioritized than the first.

The result of the decision of the decision maker is a matrix $B=\|b_{ij}\|$ of size $n\times n$, where n is the number of points u_i in which the values of the MF are compared. The element b_{ij} of matrix *B* is a subjective estimate of the relation $\mu_A(u_i)/\mu_A(u_j)$. The value b_{ij} is assigned according to the scale. The values of MF $\mu_A(u_1),...\mu_A(u_n)$ at points $u_1,...u_n$ are determined on the basis of solving the problem of finding the proper vector of matrix *B*

$$BW^T=\nu_{\max}W,$$

where $\nu_{\max}$ – the maximal real number of matrix *B*,

$W=(w_1,...w_n)$ – the corresponding own vector with

$\mu_A(u_i)=w_i/\sum_{i=1}^{n}w_i,\ i=\overline{1,n}$.

Different methods of constructing MF can be considered. According to one of the classifications, we distinguish the following groups of models that are used in the DSS.

1. By the number of stages (one-stage and multi-stage). In fact, the first ones are used to solve static tasks, and the second ones are dynamic ones.

2. By the number of experts (individual and collective).

3. By the number of criteria used (one-criterion and multi-criteria).

4. By the nature of the description of advantages, one can identify models of fuzzy mathematical programming and fuzzy binary relations of alternatives.

Mathematical programming (MP) is the most interesting group of decision-making models. The following sets of tasks for fuzzy mathematical programming (FMP) are proposed.

Task 1. Optimization of a given ordinary function $f: X \to R^1$, where X – given a universal set of alternatives, on the given fuzzy set of admissible alternatives $\mu_C: X \to [0,1]$.

To solve such a class of tasks, the FMP proposes to consider the function

$$\overline{f}(x) = f(x) / \sup_{x \in \sup p\mu_c} f(x) \tag{2}$$

as a MF fuzzy set. As a result, this allows applying the Bellman-Zadeh approach to solving this problem, according to which rational choice of alternative, which has the maximum degree of belonging to the fuzzy solution, is considered. Such an alternative is determined on the basis of the solution of the problem

$$\max_{x \in X} \min\left\{\mu_C(x),\ \overline{f}(x)\right\}. \tag{3}$$

Task 2. Fuzzy version of the standard MP problem. Let the following problem of MP be set

$$f(x) \to \max,\ \phi(x) \le 0,\ x \in X. \tag{4}$$

The fuzzy variant of this task will come out if "soften" restrictions, allowing the possibility of their violation with one degree or another. Instead of maximizing the function $f(x)$, it seeks to achieve some given value of this function, assigning different degrees of permissibility of deviations of $f(x)$ values from the desired value. In this case, the problem of FMP is written as follows:

$$f(x) \tilde{\ge} z_0,\ \ \phi(x) \tilde{\le} 0,\ x \in X. \tag{5}$$

The sign "~" means the fuzziness of the corresponding inequalities. In this case, the value z_0 determines some sufficient value of the target function. One of the approaches to formalizing such a task is to formulate fuzzy set goals and constraints:

$$\mu_C(x) = \begin{cases} 0, & f(x) \le z_0 - a, \\ \mu(x,a), & z_0 - a < f(x) < z_0, \\ 1, & f(x) \ge z_0; \end{cases}$$

$$\mu_C(x) = \begin{cases} 0, & \phi(x) \ge b, \\ v(x,b), & 0 < \phi(x) < b, \\ 1, & \phi(x) \le 0. \end{cases}$$

Values a and b set some threshold values that determine the strong violation of inequalities

$$f(x) \ge z_0,\ \phi(x) \le 0,$$

where μ and m are some functions that describe the degree of performance of the corresponding inequalities from the point of view of an expert. The Bellman-Zadeh approach can be applied to the formulated problem.

Task 3. The maximized function is fuzzy given by the mapping task $\mu_f: X \times R^1 \to [0,1]$. In this case, the fuzzy description of the estimation of the choice of the alternative x_0 corresponds to each fixed value $x_0 \in X$.

Problem 4. The usual MP problem is formulated, in which the constraint parameters are fuzzy numbers.

Task 5. Uncertainties are described as parameters of the optimized function and restrictions imposed on the target function.

In the general case, when there are n and m fuzzy restrictions, a fuzzy solution is defined as a fuzzy subset D of a set %, resulting from the following methods of fusion of fuzzy goals and fuzzy constraints.

1. Intersection 1 (taking the minimum) of fuzzy sets of goals and constraints $\mu_{D_1} = \mu_{G_1} \Lambda ... \Lambda \mu_{G_n} \Lambda ... \Lambda \mu_{C_m}$.

2. Intersection 2 (limited product) of fuzzy set of goals and constraints $\mu_{D_2} = \mu_{G_1} \circ .... \mu_{G_n} \circ \mu_{C_1} \circ ... \circ \mu_{C_m}$.

3. A linear combination of fuzzy sets of goals and constraints

$$\mu_{D_3} = \sum_{i=1}^{n} \alpha_i \mu_{G_i} + \sum_{j=1}^{m} \beta_j \mu_{C_j};$$

$$\alpha_i,\ \beta_j \geq 0,\ \sum_{i=1}^{n} \alpha_i + \sum_{j=1}^{m} \beta_j = 1.$$

It should be noted that $\mu_{D_2}(x) \leq \mu_{D_1}(x) \leq \mu_{D_3}(x)\ \ \forall x \in X$.

The following two variants of the solution of the problem of FMP with the fuzzy set of admissible alternatives are presented.

Option 1. Based on the decomposition of a fuzzy set of constraints on the set of levels and the representation of the problem of the FMP in the form of a set of ordinary tasks of optimizing the target function $\phi(x)$ on subsets of the level C_λ, where λ is the level of belonging. At the same time, a subset $N(\lambda) \subseteq C_\lambda$ is introduced on which the function $\phi(x)$ reaches its maximum value

$$N(\lambda) = \left\{ x \setminus x \in X,\ \phi(x) = \sup_{x' \in C_\lambda} \phi(x') \right\}.$$

We can say that the objective function $\phi(x)$ is maximized on the set of alternatives, which, with a degree not less than λ, are permissible in the original problem of the FMP.

Thus, the solution of the problem is written in the following form

$$\mu_D^1(x) = \sup_{\lambda : x \in N(\lambda)} \lambda$$

or

$$\mu_D^1(x) = \begin{cases} \mu_C(x), & \text{if } x \in \bigcup_{\lambda > 0} N(\lambda) \\ 0, & \text{otherwise.} \end{cases}$$

Option 2. Decision-making person when making a decision should be based not only on the size of the MF, but also on the corresponding meaning of the target function. The second solution is based on the concept of Pareto-optimal elements for a minimized function and a fuzzy set of constraints. As a result, the decision has the form

$$\mu_D^2(x)=\begin{cases}\mu_C(x), & \text{if } x\in P^0,\\ 0, & \text{otherwise;}\end{cases}$$

where P^0 is the Pareto set.

As a result, the need for a compromise between the desire to get as much value as possible $\phi(x)$ and the desire to take as much as possible an alternative is taken into account.

Models and algorithms of FMP for task 2 are considered. In the case where there are no grounds to set the coefficients of the target function and constraints in the form of precisely defined numbers, tolerance fields (tolerance intervals) are introduced The problem with fuzzy parameters in the description of the objective function and constraints can be represented as follows. It is necessary to find

$$\min f(x,\tilde{a})=\left[f_1(x,\tilde{a}_1),\ldots f_k(x,\tilde{a}_k)\right]$$

provided

$$x\in X=\left\{x\in E^n \setminus g_j(x,\tilde{b})\le 0,\ j=\overline{1,m}\right\},$$

where $\tilde{a}_i=(\tilde{a}_{i,1}\ldots\tilde{a}_{ip})$, $\tilde{b}_j=(\tilde{b}_{j1},\ldots\tilde{b}_{js})$ – respectively vectors of fuzzy parameters included in the target function and restrictions.

Fuzzy parameters are supposed to be fuzzy numbers. The concept of α-Pareto-optimal solution of the problem, where α is the level of belonging or α, is the intersection of fuzzy numbers $\tilde{a}_{ir},\tilde{b}_{jq}$. In this case, the expert should choose a satisfactory solution among α-Pareto-optimal solutions based on its subjective judgments. The minimal task is formulated, which is used as a means of generation of α-Pareto-optimal solutions. If decision-maker is not satisfied with the current α-Pareto-optimal solution, then it is possible to improve it by adjusting its reference levels.

In addition to the FMP in the DSS, other mathematical instruments are used as well: fuzzy games, fuzzy relations and graphs, fuzzy models of expected utility, fuzzy models of collective decision-making, dynamic decision making models, linguistic models. Let's dwell briefly on the apparatus of fuzzy games.

Consider the fuzzy game statement of the problem. Let X_1 and X_2 be universal sets of strategies that players can choose 1 and 2, respectively $D_{X_i}\subset X_i$, $i=1,2$. Acceptable player strategies are described by sets. A pair $(x_1\in X_1,\ x_2\in X_2)\in X_1\times X_2$ is called a situation. For each player, functions are given $f_i(x_1,x_2): X_1\times X_2\to R^1$ – subjective assessments of situations where R^1 – a numerical axis interpreted as a universal set of estimates. Each player seeks to achieve his goal

$$f_1(x_1,x_2)\to\max,\ x_1\in D_{X_1},$$

$$f_2(x_1,x_2)\to\max,\ x_2\in D_{X_2}.$$

In doing so, different principles of rational behavior are used. The main ones are: the principle of the best guaranteed result and the principle of equilibrium. A fuzzy game model can be represented as follows. Let $D_{X_i}\subset X_i$ – fuzzy sets, which are described by the functions of belonging $\mu_C: X_C\to[0,1]$. The goals of the

players are described by fuzzy sets G_i in the universal set of ratings R^1 with the membership function $\bar{\mu}_{G_i} : R^1 \to [0,1]$. Let's denote $\mu_{G_i}(x_1,x_2) = \tilde{\mu}_{G_i}\left(f_i(x_1,x_2)\right)$, $i = 1,2$.

The concept of fuzzy set of realized optimal situations is introduced $\mu^*_{D_i}(x_1,x_2) = \min\left\{\mu_i(x_i), \mu_{G_i}(x_1,x_2)\right\}$.

The goals of the players are defined as

$$\mu^*_{D_1}(x_1,x_2) \to \max,\ x_1 \in X_1,$$

$$\mu^*_{D_1}(x_1,x_2) \to \max,\ x_2 \in X_2.$$

Another type of fuzzy problems solved by environment management IS are multi-criteria problems [3]. Closely related to the problem of collective decision making is the task of multi-purpose (multi-criteria) decision making. Multi-criteria optimization in a fuzzy setting can be represented as a system $\langle X, C_1, ..., C_n, L\rangle$, where X is a universal set of alternatives, L is a lattice, and the criterion C_i $(i = 1,...,n)$ is an L-fuzzy set $\mu_{C_i} \in F_L(X)$, $F_L(X) = \{\mu_{C_i} \mid \mu_{C_i} : X \to L\}$.

If all criteria are regarded as equivalent and comparable, then in accordance with the principle of merging we have a set $\langle X, D, L\rangle$, where $D = C_1 \cap ... \cap C_n$, i.e. $\mu_D = \mu_{C_1} * ... * \mu_{C_n}$ where $*$ is one of the variants of the operation of intersection of fuzzy sets in $F_L(X)$. However, in real conditions, decision making occurs when there are criteria of unequal significance. Then, if there are many fuzzy criteria $M = \left\{\mu_{C_1}, ..., \mu_{C_n}\right\}, \mu_{C_i} \in F_L(x)$ and many criteria weights $\Pi = \{P_1, ..., P_n\}$, then a fuzzy subset Q $M : Q \subset M$

$$\mu_Q(\mu_{C_i}(x)) = \begin{cases} P_i, & if\ C_i \in M, \\ 0, & if\ C_i \notin M \end{cases}$$

determines the weighing criteria.

The criteria weighting procedure is considered as a mapping $\nu : P(N_n) \to L$, where $P(N_n)$ is the set of all subsets of criteria indices $N_n = \{1,...,n\}$, L is a lattice. The function $D : X \to L$ that represents the solutions is determined using a fuzzy integral.

$$D = \int_{N_n} \nu \circ g(\cdot) = \sup_{M \in P(N_n)} \inf_{i \in M} (\nu_x(i) \wedge g(M)).$$

In the multi-criteria case, the objective function is a vector function $\phi(x) = (\phi_1(x), ..., \phi_m(x))$, i.e. $\phi : X \subset R^n \to R^m$ and a strict order on R^m is impossible. Any two alternatives x and y are comparable to each other if and only if either $\phi_i(x) \geq \phi_i(y)$ or $\phi_i(x) \leq \phi_i(y)$ $\forall i$. Thus, the concept of optimality is replaced in vector optimization with the concept of non-dominance. While in a single-criterion problem, the solution is an optimum point, in a multi-criteria problem it gives a lot of effective (Pareto optimal) alternatives.

$$P^0 = \left\{x^0 \in X \mid \forall y \in X, \phi_i(y) \geq \phi_i(x^0) \Rightarrow \phi_i(y) = \phi_i(x^0); i = 1,...,n\right\}.$$

To further narrow this set P^0, additional information from the decision maker is needed. The various procedures used in this case mainly boil down to explicit or implicit folding of particular criteria into a single criterion. Examples of

such generic criteria can be a weighted sum of fuzzy criteria $C = \sum_{i=1}^{n} w_i C_i$; the multiplication of type $C = \prod_{i=1}^{n} w_i C_i$; minimum of the relation $C = \min_{i=1,...,n}(C_i / w_i)$, where C_i are the normalized criteria (fuzzy goals according to Bellman and Zadeh), and w_i are their weights ($i = 1,...,n$).

The fuzzy formulation of the problem of multi-criteria choice implies that there are a lot of compared alternatives $A = \{A_i,...,A_m\}$ and a set of comparison criteria (aspects) $C = \{C_1,...,C_n\}$, and a fuzzy evaluation of an alternative A_j by a criterion C_i is characterized by a membership function $\mu_{R_{ji}}(r_{ji}), r_{ji} \in R$, and the relative importance w_i of a criterion C_i is a membership function $\mu_{w_i}(w_i), w_i \in R^+$. There is a fuzzy set of optimal alternatives.

When constructing a solution, a fuzzy weighted average estimate $\overline{r}_j = \sum_{i=1}^{n} w_i r_{ji} / \sum_{i=1}^{n} w_i$ of the alternative A_j with the membership function can be used:

$$\mu_{R_j}(\overline{r}_j) = \sup_{\overline{r}_1,...,\overline{r}_n} \bigwedge_{i=1}^{n} \mu_{w_i}(w_i) \bigwedge_{k=1}^{n} \mu_{R_{jk}}(r_{jk}).$$

The membership levels in the optimal set are defined as the intersection of fuzzy estimates R_j with the so-called maximizing set M^*, which membership function $\mu_{M^*}(\overline{r}) = \left[\overline{r} / \overline{r}_{\max}\right]^p$ (p is an integer) reflects the degree to which the current value of the estimate is close to the maximum possible $\overline{r}_{\max} = \sup_{\overline{r}} \left(\bigcup_{j=1}^{m} \sup p\mu_{R_j}(r_j) \right)$. As a fuzzy optimal alternative A_*, the supremum of this intersection is taken over all weighted average estimates.

It is convenient to carry out the description of multi-criteria tasks by building preference relations between alternatives with the subsequent allocation of a fuzzy set of non-dominated alternatives. For example, in the generalized FMP model, in contrast to the described approaches, which are based on comparing fuzzy sets in the same estimate space by criteria, the tasks are analyzed in which fuzziness of all components of the decision-making system is possible. The following problems can be considered:

1) the set of permissible alternatives X (it may be fuzzy $\mu_A : X \to [0,1]$);

2) a universal set of estimates of *R* alternatives from *X*.

A fuzzy preference relation $\mu_p : R \times R \to [0,1]$ is set on the set of ratings. The choice is evaluated on the basis of this relationship, as well as a fuzzy mapping of the goal $\mu_\phi : X \times R \to [0,1]$, according to which any alternative $x_0 \in X$ is assigned a fuzzy rating $\mu_\phi(x_0, y)$, which is a fuzzy subset of the set of estimates *R*. It is required to establish a rule of rational choice of alternatives from the set *X*.

The solution to this problem is determined by constructing on the set of alternatives X a fuzzy preference relation, which is induced by the original fuzzy relation R extended to the class of all fuzzy subsets $F(R \times R)$ of the Cartesian product $R \times R$ with the subsequent extraction from it of a fuzzy set of non-dominant alternatives.

The concept of domination and non-dominance structures of solutions in multicriteria problems allows us to consider general cases in which there is information about the preferences of decision makers. The concepts of fuzzy convex cones and fuzzy polar cones are introduced. These structures embrace the concept of optimality in the sense of Pareto and some other constructions.

A particular case of a multi-criteria approach is the linear vector optimization problem; for its solution, a concretization of the Bellman and Zadeh scheme is proposed. Examples of selecting one specific solution from the set of effective solutions of vector maximization by fuzzy linear programming methods: the previously found best and worst solutions serve as the boundaries of fuzzy ranges in the corresponding fuzzy linear programming problem.

The choice of a specific solution from the Pareto set can also be carried out using the method of target programming, the idea of which is to find solutions that are located as close as possible to the vector of simultaneously unattainable goals (the ideal point). Otherwise, the problem of multi-criteria choice can be viewed as the task of grouping (clustering) alternatives based on introducing some difference relation (for example, ultrametrics) on set *X*, describing the distances between fuzzy subsets of the set of alternatives; in particular, various blur factors may be used, including De Luc's fuzzy entropy and Termini.

In the early stages of the design of real systems (the stages of analysis of the technical specifications and the development of technical proposals) there is a set of signs, according to which the expert evaluation of options takes place and the best design variant is chosen in a certain sense. Therefore, in the course of the analysis, the technical assignment should be presented as a composite linguistic variable, the meaning of which is expressed using a set of reference membership functions. The source data is conveniently grouped into a matrix of possible design solutions: its rows contain a description of alternatives $a_k, k = 1,...,q$, and the columns correspond to features $C_l, l = 1,...,r$. The cells of the matrix are filled with membership functions, built on the basis of verbal-graphic assessments of experts. The rule for choosing the best option can be written as

$$D(w,a) = \sum_{l=1}^{r} w_l(C_l) \cdot \rho_l(a_k, a_{\text{NB}}), \quad D_{\text{MD}} = \min D(w,a_k)$$

where $w_l(C_l)$ are the weight coefficients of attributes;

$\rho_l(a_k, a_{эт})$ is the generalized indicator of the difference between the current and reference scores according to the l-th attribute, having the form $\rho = a\rho_{F(x)} + b\rho_x$ ($\rho_{F(x)}$ – metric in $F(x)$, ρ_x – metric in *X*, a and b are the corresponding importance coefficients).

Artificial Intelligence Models of Decision-Making

The most promising today is the use of models and methods, information technologies, based on the results obtained in solving the problems of artificial intelligence (AI). Science that studies the mechanisms of natural intelligence in

order to use the acquired knowledge to create systems of artificial intelligence, is developed in work [4] and is called the theory of intelligence.

The presence of algebra of finite predicates opens the possibility of a transition from algorithmic description of information processes to describing them in the form of equations, and equations specify the relationship between variables. All variables in the equation are equal, any of them can act both in the role of independent and in the role of dependent. At the same time, the equations give that advantage over algorithms, which can calculate the system's response even with incomplete certainty of input signals, while the incompletely developed algorithm is not operational. It is established that in the conditions of changing the knowledge about the object, the system of equations placed on the structure of the system is always ready for use, and the algorithm often requires a radical change in its structure.

Predicates of any type can be written as formulas. The type of finite predicates is given by specifying the plural $V = \{E_1, E_2, ..., E_B\}$ and, $i = \overline{1,m}$ and – the number of elements in the set. On the support *M* we introduce the disjunctive conjunctive predicate algebra. In the role of basic elements of this algebra we use the predicates 0 and 1, as well as the predicates of recognition x_i^a of the subject a for the variable, $i = \overline{1,m}$,

$$x_i^a = \begin{cases} 1, & if\ x_i = a, \\ 0, & if\ x_i \neq a. \end{cases}$$

The classic identification task is to determine the function of the signal transformation by this object on the input x and the output signal in the object. This identification is called direct, because it is carried out with direct access to the source signal of the object. However, in some cases, it is necessary to indirectly identify the object when the investigator has no direct access to the output signal. Many tasks of this type can be solved by the method of comparative identification of an object. This method allows us to elaborate the basic provisions of the theory of intelligence in a deductive way, based solely on facts that can be physically observed, it has proven itself well in the processing of information objects of various levels [4].

In the general case, the system receives k tasks that perform alternately for different sets of input signals. Patterns of signal processing are written in the form of a system of logical conditions:

$$\begin{cases} K_1(L_1, L_2, ..., L_k) = 1; \\ K_2(L_1, L_2, ..., L_k) = 1; \\ ... \\ K_j(L_1, L_2, ..., L_k) = 1. \end{cases}$$

These conditions associate predicate variables $L_1, L_2, ..., L_k$ with each other. Here $K_1, K_2, ..., K_j$ are predicates from the predicates $L_1, L_2, ..., L_k$.

The knowledge on which the expert makes decisions can be formalized using methods of the theory of intelligence, in particular the method of comparative identification [4]. The comparator implements a predicate $K(y_1, y_2, ..., y_m) = t$ that

corresponds to the relation K, which contains input signals $y_1, y_2, ..., y_m$. At the same time t – this is the binary response of the comparator, $t \in \Sigma, \Sigma = \{1,0\}$. The inputs of the comparator are connected by their outputs with the identified information processes r_1, r_2, …, r_m. Information processes represent the mechanisms of reception of incoming physical signals $x_1, x_2, ..., x_m$. The comparator together with the information processes connected to it is called the identified object. The predicate $P(x_1, x_2, ..., x_m) = t$ of an object is expressed in the form $P(x_1, x_2, ..., x_m) = K(r_1(x_1), r_2(x_2), ..., r_m(x_m))$. Signals $y_1 = r_1(x_1)$, $y_2 = r_2(x_2)$, … $y_m = r_m(x_m)$, are internal states of the object, inaccessible for observation.

Conclusion

New opportunities provided by fuzzy set models and artificial intelligence models allow to improve decision-making processes in environment monitoring systems. The theory of fuzzy sets in recent years has become a powerful and fairly common mathematical tool allowing to solve problems in which there are elements of fuzziness or in which the decision is made on the basis of subjective assessments. Depending on the object and purpose of the simulation, different types of fuzzy models are distinguished. These include models of fuzzy mathematical programming, models of fuzzy expected utility, fuzzy models of collective decisions, fuzzy models of multi-criteria problems, dynamic and linguistic models of decision making. Algorithms for finding solutions using fuzzy models are most often reduced to converting the original fuzzy problem into a determinant one, to which known algorithms can be applied.

Artificial intelligence models, including models of the Theory of Intelligence, allow modeling of decision-making process as close to the real functioning of human's brain as possible. These models are based on the instruments of algebra of predicates. Thus, to describe the tasks of environmental safety management, we can use the methods of the formulation description in the language of predicate algebras. In the theory of intelligence precisely predicates are a universal means of formal description of the structure of any object. All described models can be used as a basis for analysis of environmental information and alternatives selection during decision-making.

References:

1. Barseghyan A. A. Data analysis technologies: Data Mining, Visual Mining, Text Mining, OLAP / A. A. Barseghyan, M. S. Kupriyanov, V. V. Stepanenko, I. I. Kholod.– St. Peregburg: BHV-Petersburg, 2007. – 384 p.
2. Bede B. Mathematics of Fuzzy Sets and Fuzzy Logic / B. Bede.– Springer, 2013 – 400 p.
3. Bector C. R., Chandra S. Fuzzy Mathematical Programming and Fuzzy Matrix Games. C. R. Bector, S. Chandra.– Springer, 2006.
4. Bondarenko M. F. Brain-like structures: a reference guide. Volume One / M. F. Bondarenko, Yu. P. Shabanov-Kushnarenko.– Kyiv: Naukova Dumka, 2011.– 460 p.

The problem of decision-making in conditions of fuzzy initial information

Alexander Goloskokov
Doctor of Philosophy in Technical Science, Professor
Department of Software Engineering and Management Information Technologies
National Technical University "Kharkiv Polytechnic Institute"
ORCID https://orcid.org/0000–0003–1824–6255

Irina Liutenko
Doctor of Philosophy in Technical Science, Associate Professor
Department of Software Engineering and Management Information Technologies
National Technical University "Kharkiv Polytechnic Institute"
ORCID https://orcid.org/0000–0003–4357–1826

Abstract. *The problem of decision making is investigated. The task is immersed in a fuzzy environment. A method for its solution is proposed. The ways of the initial information formalization are considered. A procedure has been developed for checking the external consistency of the formalization of fuzzy source information, which makes it possible to identify the need for correcting the formalization of the source data and thereby increase their consistency in the decision-making task. We consider the consistency check of the initial data formalization on the probabilities of the outcomes of alternatives. At the same time, two subtasks are investigated – checking the external consistency and the internal consistency of the initial information. The verification procedures are stated and the example illustrating their use is described.*

Keywords: *decision-making task, fuzzy environment, source data, formalization*

Introduction

The problem of decision making or the problem of choosing alternatives is one of the most common classes of tasks that not only the researcher faces. Mathematics, armed with modern computer technology, plays a prominent role in the analysis of this problem, but as long as the use of mathematical tools according to their capabilities, without overestimating or diminishing the role of mathematics and mathematics in the decision-making process.

The decision-making task can be formulated as follows. There are many solutions (alternatives), the implementation of each of which leads to the onset of some consequences (outcomes). Analysis and evaluation of outcomes by a set of performance indicators (criteria) uniquely characterizes alternatives.

It is necessary, having studied the preferences of the decision maker (DM), to build a model for choosing an alternative that is the best in some specific sense.

The system of preferences of decision makers will be understood as the totality of its ideas (about the criteria for achieving the goal, advantages and disadvantages

of the compared alternatives), allowing to make a targeted choice of elements from a variety of alternatives. Decision makers' preferences are identified, structured and formalized in the course of a special study aimed at building a model.

The decision-making body is often forced to act in the face of uncertainty, that is, the decision maker has less information than is necessary for the expedient organization of his actions in the decision-making process. Uncertainty in decision-making due to lack of reliability and the amount of information on the basis of which the decision maker makes a decision.

It is clear that it is impossible to reduce problems with uncertainties to exactly posed mathematical problems. For this, it is necessary to remove uncertainties in one way or another, and the artificial introduction of unambiguity means coarsening of the initial data, which contributes to obtaining a clear, but incorrect result.

Thus, the analysis of decision-making tasks under uncertainty cannot be performed by the forces of some mathematicians, and always the competence of an expert, i.e. a professional in this particular subject area is necessary and sometimes decisive. Consequently, the problem of decision making under uncertainty conditions is not mathematical, but only a mathematician can study all the many facets of a problem and create a system of procedures that will lead to the necessary solution.

Recent studies in the field of decision theory and its applications have led to the realization that the decision-making task is formulated and discussed by the decision-maker in a professional language (a subset of the natural language) reflecting the specifics of the tasks. The consequence of this is the use in the search for the best solution of qualitative elements: concepts and relationships with fuzzy boundaries, statements with a multi-valued scale of truth. The construction of decision-making models for problems that have a fuzzy verbal description has become possible by introducing the concepts of a fuzzy set and a linguistic variable.

The emergence of a fuzzy description of the decision problem is possible, in particular, in the following cases.

1. Restrictions on modeling resources (temporary, cost) do not allow, in principle, the existing clear information and force system analysts to use the knowledge of experts, who are expressed by the latter in a fuzzy verbal form. As a result, the usual decision-making task is "immersed" in a fuzzy environment.

2. The available numerical information does not allow one to find a solution by formal methods under the existing restrictions on resources, but the decision maker nonetheless finds it using his experience, which he can convey as a set of fuzzy rules.

3. Resources for the elaboration of all variants of the project of a complex object are absent, and the experience of designers is expressed in the form of a verbal description. The task of eliminating some of the options is set based on a vector quality indicator with fuzzy estimates of the values of its components. In this case, the design problem already in its original form is "immersed" in a fuzzy environment.

In all the cases listed above, it is necessary to refer to the approximate knowledge of experts, which they confidently use in the decision-making process. The

use of fuzzy verbal concepts with which the decision maker operates allows introducing qualitative descriptions into consideration and taking into account the uncertainty of the decision-making task, achieving a complete description of all factors relevant to this task and not giving in to an exact quantitative description.

The processing of fuzzy information in decision-making tasks is provided by using a linguistic approach, in which not only numbers are allowed as values of variables, but also words and sentences of a natural language, and the theory of fuzzy sets serves as their formalization apparatus.

Applying the expected utility as a criterion for the selection of alternatives in the conditions of stochastic uncertainty, the analysis of the solution boils down to obtaining initial data of two types:

1) information about the preferences of the decision maker, which is then formalized as a utility function;

2) information on stochastic uncertainty, which is then formalized as a probability distribution.

In the general case, both the utility function and the probability distribution are subjective dependencies, i.e. the method of their construction is the collection of basic data during the dialogue with the decision maker. Of the possible ways to set functions (analytical, graphical, tabular), the most reliable from a practical point of view is a tabular, since in this case the dialogue is conducted in terms of a specific task without using a language of formulas or graphs that is far from the decision maker.

As a usefulness of the authors understand the degree of suitability of the alternative to the goal facing the decision maker.

If the utility value is considered on the interval $[0;1]$, then the information on the preferences of the decision maker, formalized as a utility function, is given in the form of statements:

$$< \text{The criterion-based outcome } G \text{ has utility } \upsilon > \qquad (1)$$

At the same time G, both the estimate and its usefulness υ may be fuzzy (LARGE, LOW, etc.), formalized membership functions $\mu G(x)$, $\mu\upsilon(u)$, $x \in X$, $u \in [0,1]$.

Obtaining information on stochastic uncertainty to specify a probability distribution when objective data (the probabilities themselves or their statistical estimates are absent) occurs as follows.

It is assumed that the source of this information is the decision maker with his experience and knowledge of the decision-making environment. For example, when choosing a site for exploration of ore, water cut of the ore body can be used as a criterion for assessing outcomes. Sufficient statistical material is not available, and the decision maker has grounds for setting the distribution of only subjective probability.

Another example is the task of choosing a resource distribution plan, where it is necessary to provide the resource for the chief of a geological exploration expedition, and its exact location is unknown. In this task, there is also neither method for calculating the probability of the expedition leader staying at one or another point of the terrain, nor sufficient statistical material, but there are still certain reasons for estimating the subjective probability: aerial photographs of the

area, area of the last communication session, information from residents of the geological exploration area, etc.

In the first of the given examples, the outcome of each alternative can be identified with the corresponding criterion assessment from a continuous set X. Therefore, in problems of this type, the probability distribution is defined as continuous directly on X.

In the second example, it is natural for the decision maker to conduct a dialogue on the basis of a discrete and finite set of possible outcomes.

The continuous probability distribution is specified as a distribution function or corresponding density. The dialogue is usually conducted in terms of the distribution function F on a set of possible criterion assessment X. By definition $F(x') = P(x \le x'); x \in X$. In case of fuzzy answers of the decision maker, the distribution function is specified in the form $(G) = \lambda$, where both the criterion assessment G and the probability λ can be fuzzy.

Decision maker responses can be presented in the form:

$$< \text{The criterion assessment} \, G \, \text{of the specified outcome is probability} \, \lambda > \quad (2)$$

where G is a subset X;

λ – corresponding to him a clear or fuzzy number from [0, 1].

So, the initial data can be presented in the form of statements like (1) – (2), and each separate statement contains a certain amount of data.

Each alternative is given by a fuzzy description Φ, consisting of a finite number of fuzzy statements $g_i : \{g_1, ... g_i, ... g_n\}$.

A separate statement g_i is called an informational granule and looks like

$$g_i =< \text{Argument value} \, \psi_i \, \text{corresponds to the value of the function} \, \omega_i >, \quad (3)$$

where ψ_i is the fuzzy value of the argument with the membership function $\mu_{\psi_i}(y), y \in Y$;

ω_i – fuzzy value with membership function $\mu_{\omega_i}(z), z \in Z$.

The statement (1) is used to describe the utility function. As ψ_i, there is a certain fuzzy criterion assessment of G_i from the set X, and as ω_i, the corresponding fuzzy utility υ_i from the interval [0;1]. The corresponding informational granule has the form:

$$g_i =< \text{The criterion assessment} \, G_i \, \text{has utility} \, \upsilon_i > \quad (4)$$

Strictly speaking, in (4) the usefulness is determined not of the criterial evaluation of G_i, but of some outcome with such an assessment. The informational granule of type (4) actually consists of two elementary statements:

- $\psi_i =< \text{The criterion assessment is} \, G_i >$,
- $\Omega_i =< \text{The utility is} \, \upsilon_i >$.

The statement (2) is used to build the probability distribution, and the ω_i is the fuzzy probability λ_i with the membership function $\mu_{\lambda_i}(p), p \in [0,1]$. The corresponding informational granule has the form:

$$g_i =< \text{The criterion assessment} \, G_i \, \text{has utility} \, \lambda_i > . \quad (5)$$

This also refers to the outcome with the assessment G_i. And the granule of type (5) also consists of two elementary statements:

– $\psi_i =<$ the criterion assessment is $G_i >$,

– $\Omega_i =<$ The probability is $\upsilon_i >$.

Thus, we considered the presentation of the initial data in the decision making problem.

Next, you need to build a model of alternative choice, the best in a particular sense. This can be done using a method suitable for solving the problem posed of choosing the optimal alternative in the context of fuzzy initial information.

Note that the decision is made in conditions of uncertainty. This means that we can only talk about the class of "suitable" solutions. This fact was quite clearly formulated by the Italian economist Pareto as far back as 1904 in the form of the so-called Pareto principle. According to Pareto, possible solutions should be sought only among non-improved alternatives, i.e. alternatives, the improvement of which by one criteria leads to their deterioration by other criteria. This principle makes it possible, firstly, to compress many alternatives, and secondly, it demonstrates the losses that decision makers have for certain indicators, trying to improve a certain indicator.

Effective solution of the problem of choosing the optimal alternative in the conditions of fuzzy initial information implies the solution of the following tasks:

– checking the external consistency of the formalization of fuzzy source information;

– checking the consistency of the formalization of fuzzy source information about the probabilities of the outcomes of alternatives.

Main part

Consider the task of checking the external consistency of the formalization of fuzzy source information.

At the present stage of development of science and technology, the decision-making task (DMT) has not lost its relevance. Of the many possible productions of the DMT, we consider the most frequently encountered problem.

Suppose there are many feasible alternatives and criteria for evaluating their effectiveness. The implementation of the i-th alternative may lead to the appearance of the j-th outcome. Evaluation of outcomes is carried out on a set of performance criteria. The decision maker, by means of preferences on a set of these criteria, needs to choose the most effective alternative.

When solving practical tasks, the decision maker most often has to act under conditions of uncertainty, due to the lack of reliability and amount of information on the basis of which the decision is made. In this case, the DMT cannot be formulated in strict mathematical terms. This leads to the need to use the knowledge of an expert, which can be presented in the form of individual statements – informational granules.

A continuous set of possible outcomes according to the criterion of effectiveness X we will represent in the form of a union of a set of subsets, each of which

represents a certain generalized outcome, characterized by a corresponding criterion assessment.

The implementation of the i-th alternative leads to the appearance of one of these outcomes, which can be interpreted as the realization of a random variable. This manifests the stochastic uncertainty of the problem.

Baseline information received from experts should contain information about the preferences of the decision maker and the stochastic uncertainty of the problem.

Thus, to specify an alternative, we will use two types of informational granules.

1. The preferences of the decision maker can be formalized using the utility function. In this case, the informational granule has the form:

g_{kj} = < The criterion assessment of the j-th outcome by the k-th criterion (G_{kj}) has the utility u_{kj} >,

where G_{kj}, u_{kj} is the fuzzy values of the criteria evaluation, formalized by the membership functions $\mu_{G_{kj}}(x)$, $\mu_{u_{kj}}(u)$, $u \in [0;1]$, $x \in X$,

X_k is the set of possible criterion assessments by the k-th criterion.

As an example:

g_{11} =< Low profit has low utility >,

g_{12} =< High profit has a rather high utility >.

2. The stochastic uncertainty of the source data can be formalized using a probability distribution. In this case, the information granule has the form

g_{kj} = < Criterion assessment of the j-th outcome by the k-th criterion (G_{kj}) can be obtained with the probability p_{kij} >,

where p_{kij} is a fuzzy probability, formalized by the membership function $\mu_{p_{kij}}(p)$, $p \in [0,1]$.

An example of an informational granule is:

- g_{11} =< Small profits can be obtained with an average probability >,
- g_{12} =< High profits can be obtained with a probability below average >.

On the basis of informational granules in this paper it is proposed to form an informational granule, which makes it possible to formalize the initial data as a whole.

For the k-th criterion, the i alternative is given by the information granule of the form:

$$\Phi_{ik} = \{g_{k1},...,g_{kj},...,g_{km_k}\}.$$

The properties of vagueness and stochasticity of the initial information necessitate the verification of its consistency. That is, it is necessary to check the conformity of the formal data of the task with the representations of the decision maker.

In assessing the degree of consistency of fuzzy source data, several subtasks are distinguished: consistency, completeness, and redundancy checks.

Consider the procedure for checking the external consistency of the initial data formalization on the utility function based on the use of information granules of the first type.

The set of possible outcomes X is continuous and is a set of realizations of a random variable. An example would be the volume of sales. In this case, a random variable on the set of possible outcomes can be characterized by a parametric family of probability densities

$$D_k = \{f_{kz}(x)\},$$

where $z = \overline{1; z_k}$, z_k is the power of the set $D_k, x \in X$.

The degree of confidence (probability) in the appearance of the j-th outcome according to the k-th criterion at a fixed probability density $f_{kz}(x)$ according to the k-th criterion is determined by the formula:

$$p_{kj} = \int_X \mu_{G_{kj}}(x) f_{kz}(x) dx,$$

where $z = \overline{1; z_k}$, z_k is the power of the set $D_k \left(D_k = \left\{f_{kz}(x)\right\}\right)$.

The set X is continuous, and the probability density is given on it $f_{kz}(x)$, $x \in X$, therefore, the resulting degree of confidence p_{kj} is a clear number from the segment [0;1].

On the basis of information about the usefulness of the appearance of the j-th outcome according to the k-th criterion, formalized by the membership functions $\mu_{u_{kj}}(u), u \in [0;1]$, and the values of the degree of confidence in the appearance of this outcome, one can determine its expected utility

$$\mu_{eu_{kj}}(u) = \mu_{u_{kj}}\left(\frac{u}{p_{kj}}\right),$$

where $u \in [0;1]$.

The assessment of the external consistency of fuzzy initial information formalization about the utility function is reduced to a comparison of the obtained membership functions of fuzzy values of the expected utility $\mu_{eu_{kj}}(u)$. In this case, it is necessary to conduct a series of pairwise comparisons of the values of the membership functions from the fuzzy values of the expected outcome utility values by the k-th criterion.

Given the fact that a one-to-one comparison of the membership functions of fuzzy values is impossible, the result of checking the external consistency of the formalization of informational granules containing information about the utility function does not give an unambiguous answer to the question of whether they think the decision maker or not. To compare the values of the membership functions, it is proposed to use fuzzy numbers ranking indexes.

The result of the comparison is the number C, reflecting the degree of confidence that the expected utility of one outcome is greater than the expected utility of another. The value of this criterion can be obtained in accordance with one of the indexes of ranking fuzzy numbers:

$$C = \sup_{u \in [0;1]} \inf_{\substack{\upsilon \in u \\ u, \upsilon \in [0;1]}} \min\{1 - \mu_{eu_{kj}}(\upsilon), \mu_{eu_{kj+1}}(\upsilon)\}.$$

The number C is the degree of external consistency of formalization of the initial data on the utility function. If the decision maker satisfies the obtained result, then the source data can be considered externally consistent. Otherwise, it is necessary to correct the source data in order to eliminate the found contradictions.

Let us consider an example illustrating the application of the above procedure for checking the external consistency of the fuzzy initial information formalization on the utility function of the decision maker's representations.

Suppose there is an enterprise in which to invest investment funds. The company, depending on the investment and the external environment, can produce and sell products of various sizes. Suppose you can implement two investment projects. The first project is the first alternative. The second project is the second alternative. Possible values of the volume of sales – outcomes – form a set of X. Each outcome will be evaluated using the linguistic variable (criterion) "Profit".

For each alternative, two generalized outcomes may appear, which are evaluated by the "Profit" criterion:

– "Low profit", which has little utility. Low utility is a linguistic variable with the membership function of the form $\mu_{u_{11}}(u) = 1 - |u - 0.6|$;

– "Average profit", characterized by average utility. Average utility is a linguistic variable with the membership function of the form $\mu_{u_{12}}(u) = 1 - |u - 0.3|$.

At the same time, the fuzzy criterial evaluation "low profit" is formalized by the membership function $\mu_{G_{11}}(x) = 1 - |x - 5| / 5$, and the fuzzy criterial evaluation "average profit" – by the membership function $\mu_{G_{12}}(x) = 1 - |x - 6| / 2.5$.

The membership functions of fuzzy utilities, the appearance of outcomes will be set parametrically.

So, the degree of confidence that the profit will be low is calculated as follows:

$$p_{11} = \int_X \mu_{G_{11}}(x) f_{10}(x) dx = C_0 \int_0^{10} (1 - \frac{|x-5|}{5}) \cdot e^{0,2x} dx = 0,958 .$$

Next, on the basis of available information about the utility of obtaining low profits and on the basis of the calculated degree of confidence that the profits will be low, we determine the membership function of the expected utility of low profits using the formula:

$$\mu_{eu_{11}}(u) = \mu_{u_{11}}\left(\frac{u}{p_{11}}\right).$$

Similarly, the degree of confidence that the resulting profit will have an average value is calculated as follows:

$$p_{12} = \int_X \mu_{G_{12}}(x) f_{10}(x) dx = C_0 \int_0^{10} (1 - \frac{|x-6|}{2,5}) \cdot e^{0,2x} dx = 0,89 .$$

And the membership function of the expected utility of profit with an average value is as follows:

$$\mu_{eu_{12}}(u) = \mu_{u_{12}}\left(\frac{u}{p_{12}}\right).$$

Next, we find the degree of external consistency of the original data. Making a profit with an average value is preferable for decision makers in terms of utility than making low profits, and it is necessary to check whether the conclusion drawn from a fuzzy description is consistent with this. In essence, we find the degree of confidence that the membership function of the expected utility of profit with an average value is greater than that of obtaining low profit:

$$C = \sup_{u\in[0;1]} \inf_{\substack{\upsilon\in u \\ u,\upsilon\in[0;1]}} \min\{1-\mu_{eu_{11}}(\upsilon), \mu_{eu_{12}}(\upsilon)\}.$$

Based on the above calculations, it was found that the degree of external consistency of the source data on the utility function $C = 0.23$, which means that it is possible to conclude from the fuzzy initial description that making a profit with an average value is preferable to obtaining a low profit with a degree of consistency 0.23 The result obtained cannot be considered satisfactory, since $C < 0.5$, which indicates the inconsistency of the initial data formalization to the representations of the decision maker. In this case, the decision maker needs to return to the initial presentation of the source data and pay attention to the correctness of the informational granules, in particular, the formalization of fuzzy utility values by the corresponding membership functions. Indeed, there is a contradiction in the initial data: the small utility is formalized $\mu_{u_{11}}(u) = 1 - |u - 0.6|$, and the average utility is $\mu_{u_{12}}(u) = 1 - |u - 0.3|$.

It is necessary to make changes to the formalization of the source data, for example, a small utility is more correct to formalize $\mu_{u_{11}}(u) = 1 - |u - 0.3|$, and the average utility is $\mu_{u_{12}}(u) = 1 - |u - 0.6|$.

In this case, by carrying out similar calculations, we find that the initial information about the utility function of the outcomes is outwardly consistent with the degree $C = 0.58876$. This value of the degree of external consistency of formalization of the initial data on the utility function is acceptable for the decision maker. But the question comes on whether it is possible to increase the degree of consistency?

Change the membership function of the small utility to $\mu_{u_{11}}(u) = 1 - |u - 0.3| / 0.3,$ and the membership function of the average utility – to $\mu_{u_{12}}(u) = 1 - |u - 0.6| / 0.4$. At the same time, we obtain the degree of external consistency of fuzzy source data $C = 0.81461$, which indicates the decision maker to a high degree of consistency in the formalization of the source data.

In the considered example, the results of the first carried out procedure for checking the degree of external consistency of formalizing the initial data on the utility function indicated the decision maker to make changes to the formalization of a fuzzy description, and subsequent executions of this procedure made it possible to achieve a high degree of external consistency of formalizing the source data in the decision task.

Consider the task of checking the consistency of the formalization of fuzzy source information about the probabilities of the outcomes of alternatives.

There are many acceptable alternatives and criteria for evaluating their effectiveness. There are several possible outcomes for each alternative. The implementation of the i-th alternative leads to the j-th outcome. Evaluation of outcomes is carried out on a set of performance criteria. The decision maker, by means of preferences on a set of these criteria, needs to choose the most effective alternative.

The DMT arising in practice is far from always strictly defined. The available source information may be unclear or insufficient to formalize the DMT in strict mathematical terms. In such situations, decision makers need to act in the face of uncertainty, and the use of expert knowledge, which can be presented as individual statements – informational granules, becomes decisive

The continuous set of possible by the criterion of the effectiveness of the outcomes of X is represented as a union of a set of subsets, each of which is some generalized outcome, characterized by a corresponding criterion assessment. The implementation of the i-th alternative leads to the appearance of one of these outcomes, which can be interpreted as the realization of a random variable. This manifests the stochastic uncertainty of the problem.

The initial information received from experts should contain information about the preferences of the decision maker and the stochastic uncertainty of the problem. Thus, to specify an alternative, we will use two types of informational granules:

1. Decision maker preferences can be formalized using the utility function. In this case, the informational granule has the form

g_{kj} =< The criterion assessment of the j-th outcome by the k-th criterion $\left(G_{kj}\right)$ has utility u_{kj} >,

where G_{kj}, u_{kj} are the indistinct values of the criteria evaluation, formalized by the membership functions $\mu_{G_{kj}}(x)$, $\mu_{u_{kj}}(u)$, $u \in [0;1]$,

$x \in X_k$, X_k, are the set of possible criterion assessments by the k-th criterion.

As an example:

- g_{11} =< Low profit has low utility >,
- g_{12} =< High profit has a rather high utility >.

2. The stochastic uncertainty of the source data can be formalized using a probability distribution. In this case, the informational granule looks like

g_{kj} = < The criterion assessment of the j-th outcome by the k-th criterion $\left(G_{kj}\right)$ can be obtained with the probability p_{kij} >,

where p_{kij} is the fuzzy probability, formalized by the membership function $\propto_{p_{kij}}(p)$, $p \in [0,1]$.

An example of such an informational granule is:

- g_{11} =< Low profits can be obtained with an average probability >,
- g_{12} =< High profits can be obtained with a probability below the average >.

The criterion assessment of the outcome is a random variable. A continuous set of possible outcomes X_k is a set of realizations of a random variable (for example, the amount of profit obtained), which can be characterized by a parametric family of probability densities

$$D_k = \{f_{kz}(x)\},$$

where $z = \overline{1; z_k}$, z_k is the cardinality of the set $D_k, x \in X_k$.

Thus, for the k-th criterion, the i - th alternative is displayed as an informational granule of the form:

$$\Phi_{ik} = \{g_{k1}, ..., g_{kj}, ..., g_{km_k}\}.$$

The properties of vagueness and stochasticity of the initial information make it necessary to check its consistency. Namely, the verification of the conformity of the formal data of the task with the representations of the decision maker. In this case, it is possible to distinguish the check of consistency, completeness and redundancy.

Consider the process of checking the consistency of formalizing fuzzy source information about the probabilities of the outcomes of alternatives in a decision-making task. At the same time, the authors distinguish two subtasks: checking internal consistency and checking external consistency.

Consider the procedure for checking internal consistency.

Internal consistency means the correspondence of a formalized fuzzy information about the probabilities of the outcomes of alternatives to the given parametric family of probability densities $D_k = \{f_{kz}(x)\}$, ($z = \overline{1; z_k}$, z_k is the cardinality of the set D_k).

On the basis of the formed information granules, the degree of confidence (probability) of the appearance of the j-th outcome of the i-th alternative by the k-th criterion at a fixed probability density is determined $f_{kz}(x)$

$$p^o_{kij} = \int_{X_k} \mu_{G_{kj}}(x) f_{kz}(x) dx,\ k = \overline{1,d},\ i = \overline{1,n},\ j = \overline{1,m_k},\ z = \overline{1,z_k}.$$

Given the fact that probability density $f_{kz}(x)$ is given on a continuous set X_k, the resulting degree of confidence p^o_{kij} is a clear number from the interval $[0;1]$.

Next, you need to calculate the compatibility of the obtained degree of confidence p^o_{kij} with a fuzzy probability p_{kij}, contained in the original fuzzy description:

$$c_{kij}(f_{kz}) = \mu_{p_{kij}}(p^o_{kij}),\ k = \overline{1,d},\ i = \overline{1,n},\ j = \overline{1,m_k}.$$

The next step in checking the internal consistency is to find the degree of compliance with a given probability density $f_{kz}(x)$ generated by the information capsule for the i-th alternative according to the k-th performance criterion:

$$c_{ki}(f_{kz}) = \min_j c_{kij}(f_{kz}),\ k = \overline{1,d},\ i = \overline{1,n},\ j = \overline{1,m_k},\ z = \overline{1,z_k}.$$

As a result, the degree of internal consistency of the formalization of fuzzy initial information about the probabilities of the occurrence of various outcomes of the i-th alternative is found by the formula:

$$H_i = \sup_{f_{kz} \in D_k} c_{ki}(f_{kz}).$$

If the obtained value of the degree of internal consistency exceeds a certain predetermined value that satisfies the decision maker (for example, 0.5), then the initial data are considered internally consistent in probability. Otherwise, it is necessary to correct the formalization of the source data.

Let us turn to the consideration of the external consistency of the formalization of fuzzy source data on the probabilities of the emergence of outcomes – alternatives.

External consistency means the compliance of the conclusions obtained on the basis of informational granules with the representations of the decision maker. The verification of the external consistency of the initial data formalizationin probability is a comparison of the corresponding membership functions of fuzzy probabilities.

Considering that a one-to-one comparison of the membership functions of fuzzy values is impossible, the result of checking the external consistency of informational granules, containing information about the probabilities of different outcomes of alternatives, does not give an unambiguous answer to the question of whether they are contradictory to the decision maker or not. To compare the values of the membership functions, it is proposed to use the fuzzy numbers ranking index.

The result of the comparison is the number T, reflecting the degree of confidence that the probability of the $(j+1)$-th outcome is greater than the probability of the j-th outcome. This number, in accordance with one of the indexes of ranking fuzzy numbers, is determined as follows:

$$T = \inf_{p \in [0;1]} \sup_{q \le p} \max\{\mu_{p_{kij}}(p), 1 - \mu_{p_{kij+1}}(q)\}.$$

The obtained value of the criterion T is the degree of external consistency of the formalization of the initial data on the probabilities of the outcomes of alternatives. If the result satisfies the decision maker, then the source data is considered to be externally consistent in probability, otherwise correction of the source data is necessary.

Consider an example that illustrates the application of the consistency check procedure for formalizing fuzzy source information about the probabilities of the outcomes of alternatives appearing in a decision task.

Suppose there is an enterprise that is considered by potential investors. The company, depending on the investment and the environment, can produce and sell products of various volumes. Two investment projects can be implemented.

The first project is the first alternative. The second project is the second alternative.

Possible values of the volume of sales (outcomes) form a set of X. We will evaluate each outcome using the "Profit" criterion. This criterion is formalized using a linguistic variable.

For each alternative, two generalized outcomes may appear, which are assessed according to the "Profit" criterion as follows.

– "low profit", formalized by the function of belonging of the species $\mu_{G_{11}}(x) = 1 - |x - 5|/5$;

– "average profit", formalized by the membership function of the form $\mu_{G_{12}}(x) = 1 - |x - 6|/2.5$.

Information granules containing information about the stochastic uncertainty of the problem, for the first alternative, look like:

– g_{11} = <"low profit" can be obtained with a "very small probability">, where the fuzzy probability "very small probability" is formalized by the membership function $\mu_{p_{111}}(p) = 1 - |p - 0.1|,\ p \in [0,1]$;

– g_{12} = <"average profit" can be obtained with a "average probability">, where the fuzzy probability "average probability" is formalized by the membership function $\mu_{p_{112}}(p) = 1 - |p - 0.4|,\ p \in [0,1]$.

Information granules, containing information about the stochastic uncertainty of the problem, for the second alternative look like:

– g_{11} = <"low profit" can be obtained with a "small probability">, where the fuzzy probability "small probability" is formalized by the membership function $\mu_{p_{121}}(p) = 1 - |p - 0.2|,\ p \in [0,1]$;

– g_{12} = <"average profit" can be obtained with a "rather smallprobability">, where the fuzzy probability "rather small probability" is formalized by the membership function $\mu_{p_{122}}(p) = 1 - |p - 0.3|,\ p \in [0,1]$.

The resulting profit value is a random variable. This random variable is characterized by the class of probability densities on the corresponding set of criterion assessments:

$$D = \{f_z(x)\},\ f(x) = c \cdot e^{t \cdot x},\ c = t/(e^{10 \cdot t} - 1), t = \{0.2, 0.4, 0.8\},\ D = \{f_0, f_1, f_2\}.$$

Consider checking the external consistency of the original data in probability.

According to the first decision in this example, according to the decision maker, the probability of the outcome "high profit" (the second outcome) is greater than the probability of the outcome "small profit" (the first outcome). Does this view correspond to the formalization of the source data? This is a check of the external consistency of the fuzzy initial information formalization on probability.

According to the formula defined above, we find the degree of confidence that the probability of a second outcome is greater than the probability of the first:

$$T = \inf_{p \in [0;1]} \sup_{q \le p} \max\{\mu_{p_{111}}(p), 1 - \mu_{p_{112}}(p)\}.$$

We get $T = 0.4$ degree of confidence that the probability of a second outcome ("average probability") is greater than the probability of the first one ("very small probability").

This value of the degree of external consistency of the initial data formalization on the probability of occurrence of the decision makers may be considered satisfactory. But the question arises, is it possible to increase the degree of external consistency?

We make some changes in the source data formalization in the formalization of the source data. If the fuzzy probability "average probability" is formalized by the membership function $\mu_{p_{112}}(p) = 1 - |p - 0.6|$, $p \in [0,1]$, then, by carrying out appropriate calculations, we obtain that the desired degree of external consistency is $T = 0.6$. This value suits the decision maker more than 0.4, because indicates a higher level of compliance with the formed fuzzy description of the decision makers.

In the second alternative, the value of the degree of external consistency $T = 0.5$, which is acceptable for the decision maker and, therefore, means the external consistency of formalizing the initial data on the probabilities of the outcome of the second alternative.

Consider checking the internal consistency of a formalized source information.

According to the procedure defined above, we find that the degree of internal consistency of the fuzzy initial information formalization about the probabilities of the occurrence of different outcomes of the first alternative is equal to $H_1 = 0.767$. In the second alternative, the corresponding degree is $H_2 = 0.867$.

The values of degrees obtained in this example H_1 and H_2 exceed the value of 0.5 satisfying the decision maker, which gives grounds to consider the formalized initial data on probabilities internally consistent, i.e. corresponding to a given parametric family of probability densities.

Conclusion

The considered procedure for checking the external consistency of the fuzzy initial information formalization on the utility function reveals the need to correct the formalization of the initial data. This correction improves the consistency of the source data in the decision-making task. The procedure for checking the consistency of the fuzzy source information formalization about the probabilities of the outcomes of alternatives reveals the need to correct the formalization of the source data, which also increases their consistency in the decision-making task.

The mathematical apparatus defined above allows to increase the efficiency of the decision-making problem being solved.

References:

1. Borisov A. N. Processing fuzzy source information in decision-making systems / A. N. Borisov, A. V. Alekseev, G. V. Merkuryeva et al.– Moscow: Radio and Communications, 1989.– 304 p.
2. Goloskokov A. E. The problem of choosing the optimal alternative in the conditions of fuzzy initial information / A. E. Goloskokov, E. A. Stepanova // Bulletin of Kharkov State Polytechnic University. – Kharkov: KSPU.2000.– No. 121.– P. 99–103.
3. Goloskokov A. E. Verification of external consistency of formalization of fuzzy initial information in the decision-making problem / A. E. Goloskokov, E. A. Stepanova // Open information and computer integrated technologies. Issue 12.– Kharkov: KhAI.2002. – No. 12.– P. 80–84.

Methodical bases of information support for complex analysis of system objects difficult / weakly structured

Tatiana Kozulia
Doctor of technical science, Professor
Department of Software Engineering and Management Information Technologies
National Technical University "Kharkiv Polytechnic Institute"
ORCID https://orcid.org/0000–0001–5107–9140

Mariia Kozulia
Doctor of Philosophy, Associate Professor
Department of Software Engineering and Management Information Technologies
National Technical University "Kharkiv Polytechnic Institute"
ORCID https://orcid.org/0000–0002–4090–8481

Abstract. *The complex methodological approaches for solving problem tasks objects quality assessment are determined on the basis of system analysis means combination and of the information and software complex development of research data processing with use of modern mean knowledge providing. Methodological support is based on theoretical knowledge in field of information entropy theory, synergetic, knowledge-oriented databases development; information space of integrating entities unity principles. The scientific and practical foundations of methodological and informational support for the determination of complex systems state assessment and their functional capabilities, safety level of the investigated objects, using of knowledge-oriented information systems for obtaining knowledge on the research objects results at level "state (system –environment) – change – process – system state". The generalized algorithmic approach from complex system object analysis as integrity having its microstructure to which it is proposed to attribute not only component components and elements, but also processes of its functioning is developed. Practical implementation of the proposed informational and methodological approaches for complex systems study analysis on the entropy-information basis is shown on the results of quality and safety functioning assessment of natural-technological, ecological-economic systems, providing operational control and safety management of technological processes.*

Keywords: *environmental safety, methods of system analysis, mathematic modeling methods, information monitoring systems, safety state identification, environmental knowledge-oriented systems, information program of systems quality assessment*

Introduction

In general nature situations uniqueness or nuances of economic, social and ecological manifestation; in relation to uncertainty due to reasons of irregularity or randomness, stochasticity of controlled processes and goals ambiguity, criteria,

alternatives of actions and consequences during hard time constraints, it is proposed to form a methodological complex of analysis and complex objects state assessment on theory of synergetics, entropy and information for the study of systems of weak organizational hierarchical structure base for – COHS.

Information uncertainty about the assessment of the state and changes of such systems is determined by the presence of ignorance about the interconnection of the components in the system itself, the stochastic nature of the external environment, the probabilistic nature of internal processes in systems and their relationship with the environment (E).

Review of recent publications

System object state analysis within the decision-making task requires a procedure for determining the goal, indicators of the preconditions for its achievement (criteria) and the ways of rational bringing the systems to the goal. Thus, two critical cases are considered in relation to object functioning and the control processes:

1) uncertainty is reduced to a priori ignorance of the consequences quantitative characteristics on the base of constructing a statistically grounded action plan and solving vector optimization problems with solving the problems of displaying a real system in a compact mathematical form;

2) practically complete conditions uncertainty and functioning laws, ambiguity of goals and criteria is solved on the basis of intuitive-logical analysis of ODM, the application of mathematical support for the quantitative expression of intuitive evaluations and experience.

These DM approaches have significant disadvantages in uncertainty elements presence: for the first direction – different types of uncertainty are not solved and ignorant non-formalized factors related to the achievement of the goal (decision-making); in the second case, the subjective component significantly increases when establishing a final decision that overlooks the objective factors of multicriteria assessment of the state, processes and situation, provided the goal is achieved.

The main disadvantage of the proposed methodology of organizing system objects regarding their quality and safety management is the application of concepts, definitions, formalized representations, etc. the traditional synergetic G. Haken concerning the self-organizing ordering in order to obtain purposeful systems in the plane of the concepts of chaos and the order by random nature trajectory of systems motion in the phase space [1, 2], the introduction of a synergetic information theory for statistical representation of the chaotic system state in form of its uniformly distributed elements by any sign value [3]. In defining the system state from the thermodynamic approach standpoint, according to I. R. Prigogine [4], is used concepts of stability and destabilization with disorder maximization, that is, the entropy growth and bifurcation point attainment.

Self-organization concept as a transition from a chaotic to a more orderly state is the base of dissipative structures formation. Such systemic transitions are the result of irreversible non-equilibrium processes considered [5–7].

To describe the relations with available input and output information in the form of knowledge about the state and process, data on the intermediate variables that determine the transformation in the system using logical networks [8].

Imitation models are widely used in the study of the environment and individual objects, usually to determine their state and forecast changes in order to avoid environmental hazards, planning threats elimination measures [9]. At present, an appeal to the information component of the external person world is relevant. In this sense, the use of models based on the theory of information entropy, namely the Shannon entropy, which is used to solve problems from many different knowledge fields, first of all, the study of ecological and economic systems, became widespread. Thus, based on the results of remote ecosystems sensing, the prospect of applying this approach in natural objects monitoring data assessment [10] has been established. The prospect of the entropy approach introduction is also defined for the social issues analyze, for example, the assessment of business processes development and economic decisions adoption [11, 12].

In general, in a large number of decision-making tasks, the analysis of the man-made object state of socio-ecological and economic content and its quality management is based only on experimental data (training sample) [13]. Decision-making in the conditions of local information and implicit knowledge leads to errors in the decision-making on the homeostasis maintenance in natural-technogenic formations. The sequence of factors, events, conditions of real processes is characterized by a certain causal connection of explicit and implicit dependencies. The formalization of implicit dependencies is associated with indirect causative relationships based on the construction of formal algebra-logical models of implicit selection constructs [14].

It is precisely in order to eliminate the aforementioned disadvantages within the boundaries of denoted DMtasks, a consistent solution of uncertainty is considered on the base of a complex methodology that contains the provisions of the theory of information entropy, synergetics, logical and mathematical structures theories, using the experience of scientists in solving individual problems in this research area.

The methodology for assessment the quality (conformity) of a complex organizational system involves establishing mechanisms to eliminate the direct link between economic growth and deterioration of environment state, providing an analytical state conformity assessment and systems functioning in the plane of probabilistic-entropy risk-level of safety requirements implementation. It is the consideration of the generalized single thermodynamic nature of any system, the above analysis of entropy method use of successive reduction and the solution of uncertainties allows us to propose a comprehensive methodical introduction comparative estimation system of any nature system objects quality of under the entropy state function and changes based on meaningful improvement of the proposed methods and their combination to achieve the goal of the study. Such an analytical system allows us to use the proposed methods not only individually, in

complex tasks and objects that are contradictory in nature, they use consecutive-entropy correspondences in the form ΔS is an input information for a comparator; comparator identification of monitoring information allows to obtain initial data for factor situation analysis (cognitive modeling) with the further establishment of an entropy function for assessing the state and estimating the processes probability and obtaining the final result in the decision making in conditions of uncertainty.

Proposed methods

Mathematical assurance system objects quality in situation of uncertainty according to strengthening the stabilizing mechanisms processes of natural order self-organization in object, the processes establishment of transformational content that lead to targeted effects, ordering weighty factors, which enhance or create conditions for the full stable it functionality implementation.

For consider dynamic changes characteristics in systems offered to contact to Lyapunov function. State and processes is characterized entropy $S(K)$ and its production $S'(K)$ under conditions when argument is an invariant K and is variable. For such K in changing entropy role information measure is information entropy of the form [15–17]

$$S(K) = \chi \cdot \ln K . \tag{1}$$

Then stable processes are conditional $dS(K)|_j = 0$, where j defines extreme conditions. According to Lyapunov's stability criteria, the state of the system becomes stable dynamically, if entropy production has maximum that inherent for processes and objects realized in nature:

$$d^2S(K)|_j > 0;\ d^2S'(K)|_j < 0 . \tag{2}$$

Statistically entropy minimum state is unstable, since there is a probability of self-satisfactory processes fluctuating appearance, which allows further entropy growth. Entropy growth in dynamical processes as a function of K by Lyapunov's criteria virtue the state of minimum entropy considered dynamically stable. Indeed, organization of a stable thermodynamic flow (matter transmission, energy, information) between systems in nature and at the level of technical, natural and technical objects defines stationary states sequence that locally minimum production principle of Prigogine entropy under self-organization condition and guarantees the stability of the systems by Lyapunov (Fig. 1) [16, 17].

For system research object "object 0-state (systems as components) – process (system of processes, operator state change or support) – object i-state (system)" in existing systems of economic, social and environmental monitoring as an input information stream (x_1, x_2) and output variable (y) problem formulation for fuzzy rules base forming of typical algorithm has form: $x_1 = A_{i1} \wedge x_2 = A_{i2}$ for $y = B_i$, $i = \overline{1, N}$ [15, 16].

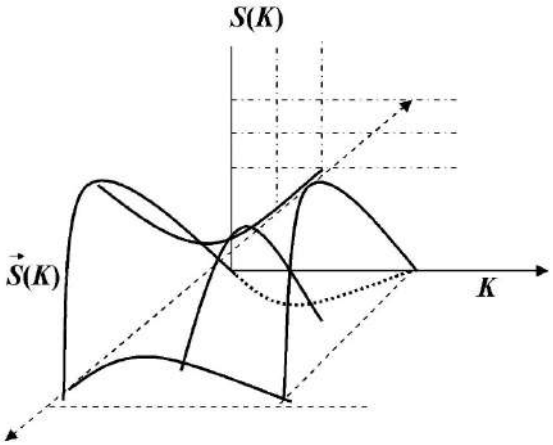


Figure 1. – System stability based on max entropy production

According to monitoring information initial data samples are formed, taking into account presence of well-known and sufficient values amount $\eta = y_j$ to set the exact value ξ, which are educational sample base in such form:

$$\left(x_1^{(\eta,\xi)}, x_2^{(\eta,\xi)}, y^{(\eta,\xi)}\right)\ \left(\eta, \xi = \overline{1,K}\right), \tag{3}$$

where $x_1^{(\eta,\xi)}$, $x_2^{(\eta,\xi)}$, $y^{(\eta,\xi)}$ – respectively, input and output variables value from experiment objects characteristics $\eta = y_j$ and ξ;

K – total number of experimental data in training sample.

Among the monitoring objects characteristics set their minimum and maximum values, which under these conditions reflect the ability to achieve necessary target points. Similarly source data is analyzed – systems state at unsatisfactory ($y^{\min}$) and conforming to requirements at an acceptable natural / permissible level ($y^{\max}$):

$$x_1 \in \left[x_1^{\min}, x_1^{\max}\right],\ x_2 \in \left[x_2^{\min}, x_2^{\max}\right],\ \mathrm{y} \in \left[y^{\min}, \mathrm{y}^{\max}\right].$$

Appropriately set fuzzy sets with linguistic values: L – external factors (properties, parameters, characteristics, etc.), M – internal factors, H – state, characteristic. The membership functions intersect at the level of 0,5, with point estimate form, taking into account entropy function form (Fig. 2).

Variable space distribution is divided according to the specified sets into such a number of segments (Fig. 2):

$$\left[x_1^{\min}, x_1^{\max}\right] = 3,\ \left[x_2^{\min}, x_2^{\max}\right] = 5, \left[y^{\min}, \mathrm{y}^{\max}\right] = 4\ .$$

For x_1 specified fuzzy sets $\{L_1, M_1, H_1\}$, for x_2 as a dynamic estimate of the greater volume information, generalizing content the set takes into account the "process": LM – factors interaction at their "meeting" in the system, HM – internal factors influence on system properties, taking into account changes in compo-

sition and structure, implementing destructive phenomena of recured and non-recured nature – $\{L_2, LM_2, M_2, HM_2, H_2\}$, accordingly the output variable is formed y – $\{L_y, LM_y, HM_y, H_y\}$.

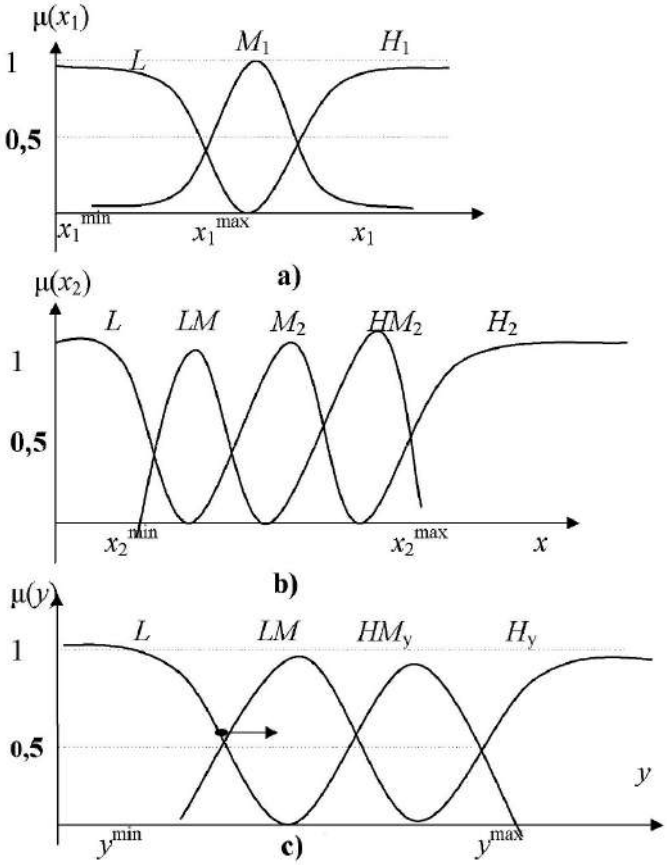


Figure 2. – Variables distribution space in object quality assessment

The discrepancy conditional entropy is defined:

$$S\left(\xi(x)/\eta(x)\right) = -\int_{-\infty}^{\infty} f(x)\,\ln f(x)\,dx =$$

$$= \ln\sqrt{2\pi\sigma}\int_{-\infty}^{\infty} f(x)\,dx + \frac{1}{2\sigma^2}\int_{-\infty}^{\infty} f(x)x^2\,dx = \ln\sigma\sqrt{2\pi} + \ln\sqrt{e} = \ln\sigma\sqrt{2\pi e},$$

where $\int_{-\infty}^{\infty} f(x)\,dx = 1$, $\int_{-\infty}^{\infty} f(x)x^2\,dx = D = \sigma^2$.

For the information-entropy system state assessment according to analytical expressions, functional is used:

$$I(x) = \log_2 n + \sum_{i=1}^{n} p(x_i) \cdot \log_2 p(x_i) \quad (4)$$

Object interaction with external systems is characterized by unstable dynamic equilibrium with an objective reduction of ordering due to exchange variations of information, substance and energy. The irreversible processes in time and the future uncertainty are identified as entropy dynamics, the quantitative characteristics of which according to the content of a certain level allows the membership function to be accepted as changes in entropy $\varnothing S$.

The consideration of systems interaction with synergistic effect of self-organizing action leads to the stationary state stabilization "system (H_0) – environment (W)" in form "state 0 – process (external factor – internal factor, internal factor – internal factor) – state0" (Fig. 3) taking into account the existing situation uncertainty (Fig. 2 b). The system stabilization in interaction with environment, characterized by chaotic influence, depends on arbitrary processes probability, are reduced by negative entropy values of factors interaction (LM, HM_2), which is determined on a phenomenological base. Thus, in the field of uncertainty at the interval $[a, b]$ between values $[x_2^{\min}, x_2^{\max}]$ by entropy assessment an unidentified event and managerial action factor are established [15–18].

The most complex situation in case of researching "system (H_0) – environment (W)" within the "system (H_0) – environment (W)" in form "state 0 – process (external factor – internal factor, internal factor – internal factor) – state1" is solved analytical description of situation uncertainty base with implementation of intermediate states unstable in negentropy centers presence and active destabilization factors (Fig. 4).

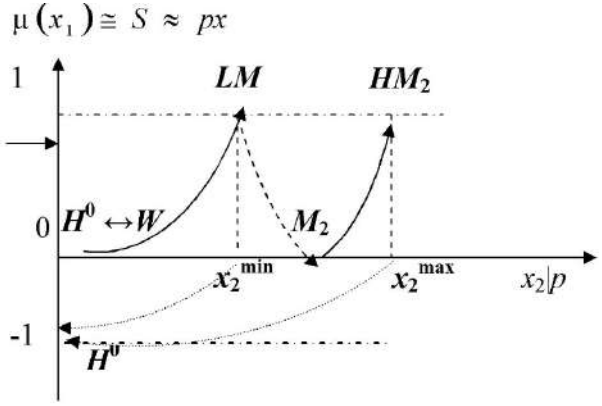


Figure 3. – Solving the uncertainty system state by the entropy trajectory of self-healing processes

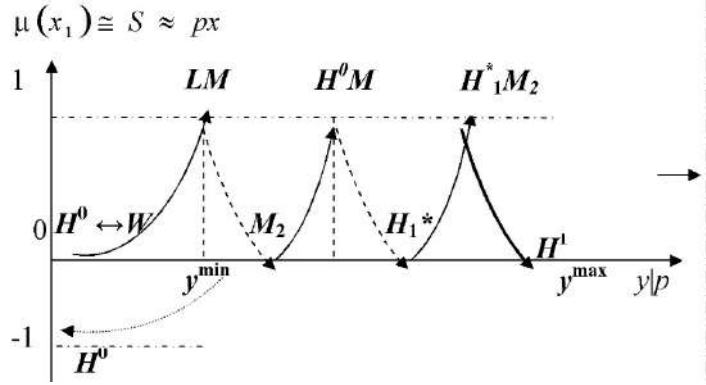


Figure 4. – Uncertainty determination in "object – environment" state assessment task on homeostasis recovery synergetic

Avoiding expert procedures objectively address the initial natural homeostasis "object – environment" H_0, around which there are external and internal nature factors interactions, which, according to the entropy function is defined as a return to natural relationships resumption between systems $H_0 \leftrightarrow W \rightarrow LM \rightarrow H_0$ or self-organizing synergistic effects of disorder desire to stable equilibrium condition provided $S'(K), S(\xi|\eta), \varnothing S \rightarrow 0$ (Fig. 4) [15–18].

Features of logic-mathematical methods introduction and uncertainty consistent solution means. For relationships describing with available input and output information in knowledge form about state and process, data about the intermediate variables that determine the transformation in the system, use logical networks.

The implicit situation with regard to the processes in the system is characterized by the existence of several alternatives and the need to synchronize selected events within the fixed changes made. The implicit choice is thus determined by combining the synchronization and selection structures. So, processes P_1 and P_2 can lead to changes by presence of activity in processes P_4 and P_5, which ultimately stabilizes the system (Fig. 5), taking into account intermediate events t, which contribute to the satisfactory flow of processes by entropy assessment $-S \rightarrow \max, \Delta S_{proz} \rightarrow -\max, \Delta S_{syst} \rightarrow \min$.

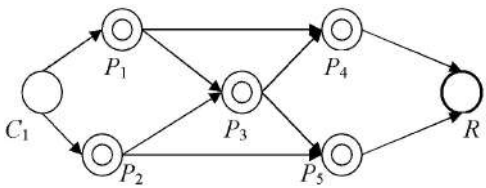


Figure 5. – The situation of implicit changes processes choice in the system between P_4 and P_5 at realization of initial situation C_1 into result of R

Thus, it is proposed to avoid uncertainty at decision way to manage system objects of socio-ecological and economic content using constructive mathematical logic models, combining the state and processes analysis in the systems and beyond with environment.

Entropy-graph models usage for natural-technogenic objects within the "state (system – environment) – process – state of the system" study.

There are no infinite straight lines in nature, so there is invariance at infinite scales number in nature. Each system can be highly organized, that is, have a developed and complex structure, less organized with a simple structure, completely chaotic, when its elements are distributed randomly and, on average, in a homogeneous manner. According to the fundamental provisions structures formation theory in irreversible processes, there is necessity appeal to fractal geometry with getting connection between the basic concepts of chaos and structure, the entropy of different nature systems state quantitative assessment (Fig. 6).

Systems structural organization measure entropy function is adopted in relation to the implementation of equilibrium or imbalance, the direction determination of structures development or degradation in the system object.

In process of development and evolution (new structures sequence) of a complex system by important factors in maintaining stability and integrity are the self-organization within the systems internal environment and their interaction with the environment, the links maintenance that homogenize the system space, not allowing voltage points creation – an entropy explosion, the chaos realization. The main task for complex systems synergetic analysis is to identify the main factors at each stage of successive and irreversible transition from one systems state to another with the implementation of a certain internal organization level and the structural elements connection degree with the predominance of a certain communication type between them. To identify pre-crisis states, an integrated signaling approach is implemented based on modern synergetic, multifractal and wavelet analysis methods, entropy methods, graphological models, etc [15–18].

Significant long-term deviation from equilibrium state leads to consolidation in space-time system existence environment dissipative formations accumulation, the dissipation intensification with a sharp system change in attractor direction (Fig. 7).

In order to satisfy the homeostatic state in relation to the object implementation of natural (defined from the beginning) macro functions, it is necessary to fully realize the extremely minimal number of important functions for system stability informational support. This requires compliance with high activity conditions of components, system elements, structural integrity and significant functional flexibility. It is the synergetics of system object homeostasis is determined by the information entropy balance of internal and external environment and the reserve of flexibility constituent elements and stability, which ensures structural integrity and further maintains the primacy of its macro properties.

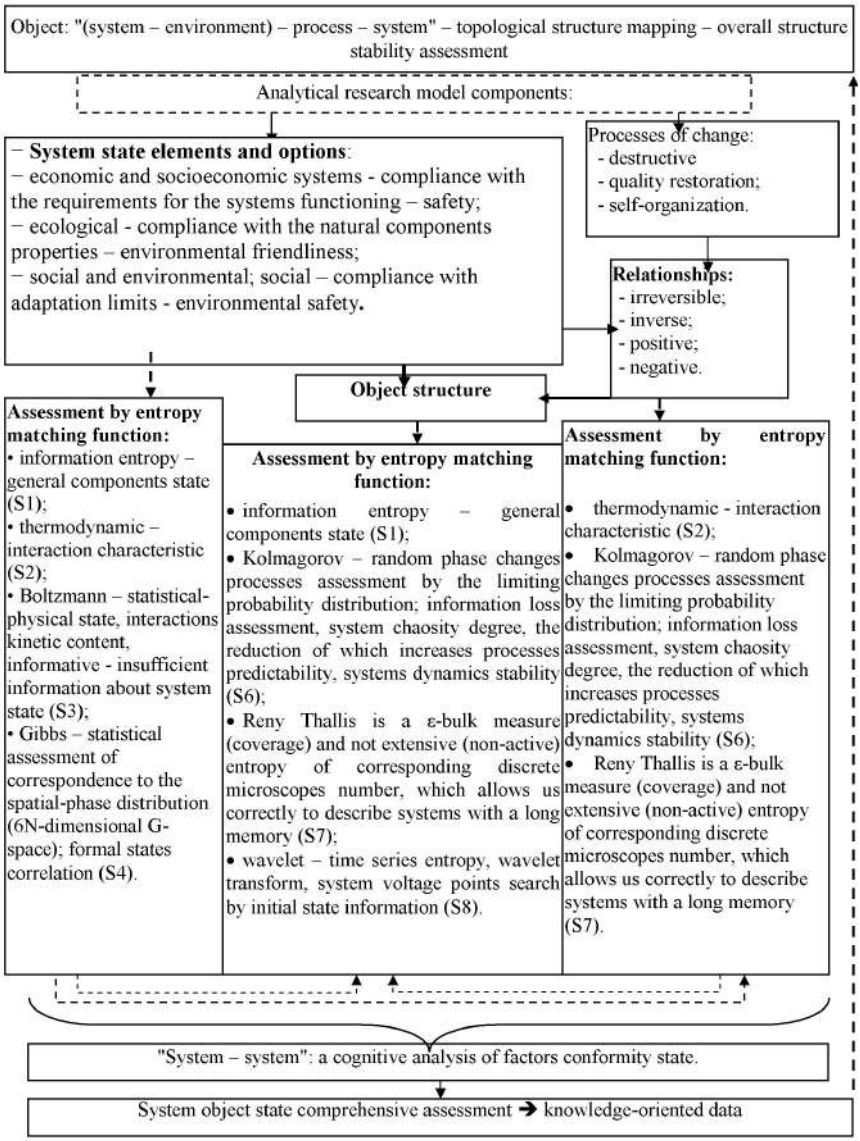


Figure 6. – Schema of system object "state – processes" research

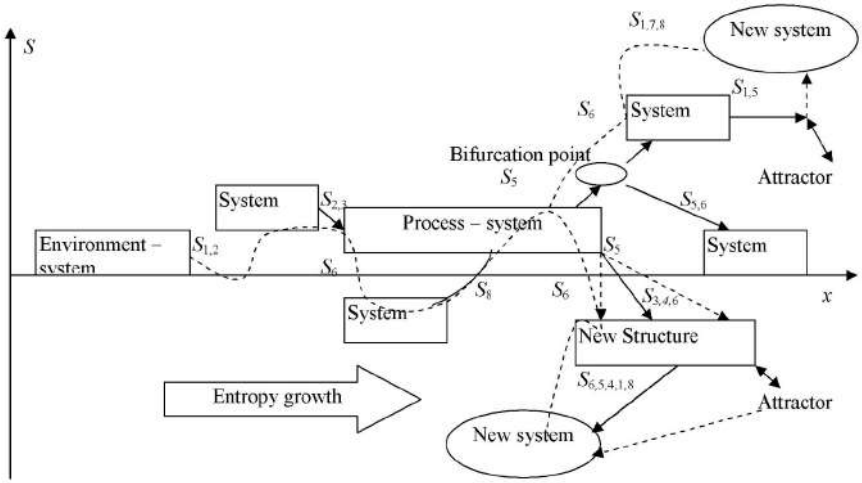


Figure 7. – Schema of system state changes by entropy-information assessment equilibration search: $S_{1,2,3,4,5,6,7,8}$ – information, thermodinamical, Bolzman, Gibbs, Shennon, Kolmagorov, Renny-Thallis entropies, wavelet entropy

Providing the structure of investigated system object in two complexes form determines the necessity of an integrated approach to finding optimum for goals and conditions reconciliation, ensuring complexity and systemicity in sustainable development problems solution (definition of goals, conditions for the development process and organizational structure creation of execution and conditions). Thus, integrated approach to study complex structured systems is determined by its components connection and the compromise achievement of its "interests". Point interests coincidence as an external attractor of interaction "object – environment" is achieved by processes implementation, state changes, determined by the entropy trajectory of economic development and entropy growth of external environment (surrounding systems) $S_{1,7,8}$; influences realization on environment systems and their functionality preservation at the expense of entropy voltage decrease trajectories at adaptation and self-organization $S_{5,6}$ (see Fig. 7). According to the decoupling concept, this state for socio ecology and economical systems is reflected as the economic development polarity with respect to the ecological subsystem.

It is proposed to modify the analysis scheme of a complex system research object. On the basis of the observation data received by the structural matrix, it is expedient to construct a model in graph form which have the cognitive map content, that is factor analysis base in relation to the systems dynamics and the determination of the further self-organization direction regarding stable systemic education structurization by influence factors – x_1, x_2, x_3, x_4 (the first factors group) responsible $\overline{x}_{\text{input}} = \overline{x}_6, \overline{x}_7, \overline{x}_8, \overline{x}_9$ provided internal system structure functionality

(x_1, x_2 – promoting system development, x_3, x_4 – negative impact) and system elements state, namely x_5, x_6, x_7, x_8, x_9 (second group) are relevant $\overline{x}_{\text{syst}} = \overline{x}_1, \overline{x}_2, \overline{x}_3, \overline{x}_4, \overline{x}_5$, and action factors on external environment on system side $\overline{x}_{\text{output}}$ (third group of factors) positive x_{10} (system performance) and negative impact in the form of waste x_{11} [16]. There is schema of system object graph model – oriented graph $G = G(X, A)$ (Fig. 8), where X – analized systems set: X_1, X_2, X_3, X_4 – environment recourses; climate; socio-economic environment; transport; X_5, X_6, X_7, X_8, X_9 – state of atmosphere; hydrosphere; soil; flora, fauna; X_{10} – man state; X_{11} – external ecological environment; A – connections between systems a_{ji} where V – information entrance system, j – information exit system.

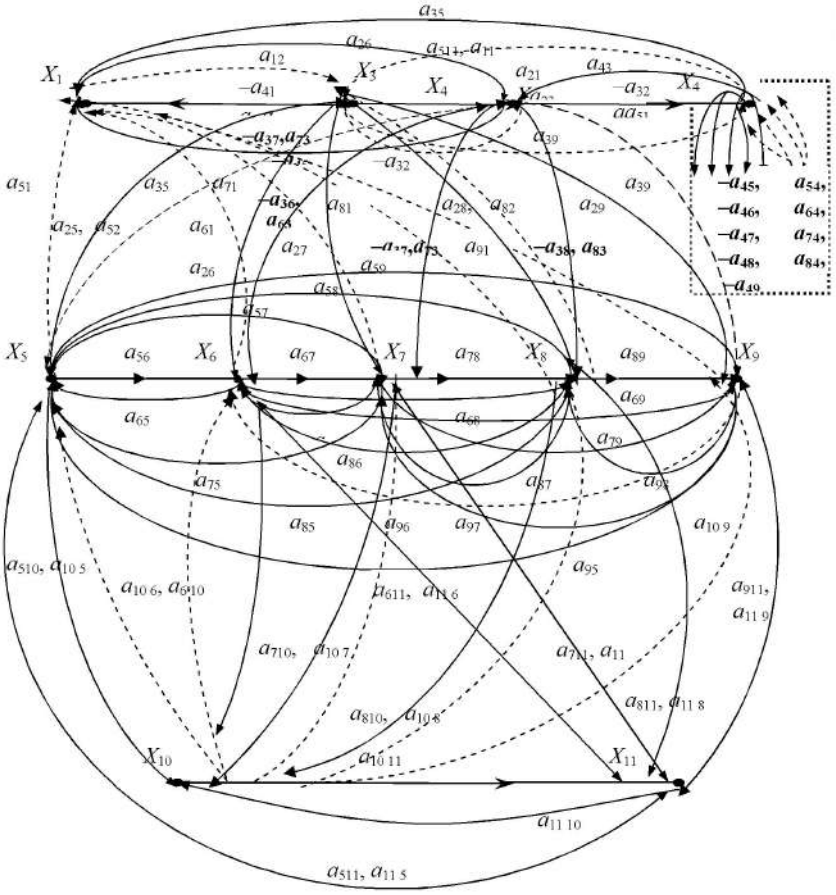


Figure 8. – Schema of system object graph model – oriented graph $G = G(X, A)$

The complex system mathematical model formulation with a reflection of its structural features as an ecological, socio-economic object of research is carried out in this order. The structural system matrix is arranged: the inputs to the system are reflected on the matrix left side, the system outputs on the matrix right side (Fig. 9 a).

x_i	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	x_9	x_{10}	x_{11}
1	×	←	→	←	↵	↵	↵	↵	↵		
2	→	×	→	→	→	→	→	→	→		
3	→	→	×	→	→	→	→	→	→		
4	→	→	→	×	→	→	→	→	→		
5	→	→		→	×	→	→	→	→	→	→
6	→	←	→	→	→	×	→	→	→	→	→
7	→	←	→	→	→	→	×	→	→	→	→
8	→	→	→	→	→	→	→	×	→	→	→
9	→	←	←	←	→	→	→	→	×		→
10					→	→	→	→	→	×	→
11					→	→	→	→	→	→	×

a

x_i	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	x_9	x_{10}	x_{11}
1	×	a_{12}	a_{13}	$-a_{41}$	a_{51}	a_{61}	a_{71}	a_{81}	a_{91}		
2	a_{21}	×	a_{23}	a_{24}	a_{25}	a_{26}	a_{27}	a_{28}	a_{29}		
3	$-a_{31}$	a_{32}	×	a_{34}	a_{35}	$-a_{36}$	$-a_{37}$	$-a_{38}$	a_{39}		
4	$-a_{41}$	a_{42}	a_{43}	×	$-a_{45}$	$-a_{46}$	$-a_{47}$	$-a_{48}$	$-a_{49}$		
5	a_{51}	a_{52}	a_{35}	a_{54}	×	a_{56}	a_{57}	a_{58}	a_{59}	$a_{5\,10}$	$a_{5\,11}$
6	a_{61}	a_{26}	a_{63}	a_{64}	a_{65}	×	a_{67}	a_{68}	a_{69}	$a_{6\,10}$	$a_{6\,11}$
7	a_{71}	a_{27}	a_{73}	a_{74}	a_{75}	a_{76}	×	a_{78}	a_{79}	$a_{7\,10}$	$a_{7\,11}$
8	a_{81}	a_{82}	a_{83}	a_{84}	a_{85}	a_{86}	a_{87}	×	a_{89}	$a_{8\,10}$	$a_{8\,11}$
9	a_{91}	a_{29}	a_{39}		a_{95}	a_{96}	a_{97}	a_{98}	×	$a_{10\,9}$	$a_{9\,11}$
10					$a_{10\,5}$	$a_{10\,6}$	$a_{10\,7}$	$a_{10\,8}$	$a_{10\,9}$	×	$a_{10\,11}$
11					$a_{11\,5}$	$a_{11\,6}$	$a_{11\,7}$	$a_{11\,8}$	$a_{11\,9}$	$a_{11\,10}$	×

b

Figure 9. – Structural matrix of system object "(system – environment) – processes-external environment–state of the system"

The links between the elements of a complex system structure are interactions constant (direct and inverse relationships) and probable (possible, random: direct and inverse relationships), which are weak in influence, informative [16]. The (Fig. 9) has the following designations: x_1, x_2, x_3, x_4 – provision of E systems resources; climatic conditions; the state of the socio-economic environment; transport / communication; x_5, x_6, x_7, x_8, x_9 – atmospheric air condition; hydro resources; soil / surface of the earth's cover; vegetation; the animal world; x_{10} – human condition / livelihood; x_{11} – impact on ecological emergency; connections (see Fig. 8) are constant (–) |→ – strait, ←| – inverse and random (– – -) |→ – strait, ↵– inverse probabilistic relationships.

All matrix columns are indicated x_j according to the coordinates $(x_1,...,x_k,x_{k+1},...,x_n,x_{n+1},...,x_l)$, where k – last number of input coordinates (tasks, targeted studies); n – number of system core coordinates; l – last coordinate number of external obstacles, environmental impacts. All elements of the matrix are indicated a_{ji}, where j – matrix column number; V– line number. For diagonal elements takes place $j = i$, non-diagonal $j \uparrow i$ (Fig. 9 b). Established expressions for operators, the resulting numerical values of their coefficients are used to analyze the system state of the research object.

Scientific results. According to research tasks defines the main ways models and methodological approaches improving complex systems safety level evaluation by analyses "state (system – environment) – changes – process – system state". Defined methods characteristics state investigation "system – environment" according to the methodological approaches analysis in the environmental, ecological and economic analysis fields to environmental safety assess. The methods system information data disparate objects monitoring comprehensive assessment, entropy and knowledge base processing methods, analysis and environmental and socio-economic information evaluation is offered.

To assess ecological safety level "system – environment" proposes an algorithm (Fig. 10) for probabilistic-entropy approach implementation to determine the state by information amount ξ, which is contained in obtained previous stage results of the problem solution or is established relatively to the system characteristics η.

The research object general condition is determined by such dependencies of the information function

$$I(\xi|\eta) = S(\xi) - MS(\xi|\eta);$$

$$I(\eta|\xi) = -\sum_i p_{ij} \log_2 \frac{p_{ij}}{P\{\xi = x_i\} P\{\eta = y_j\}}, \quad (5)$$

where $I(\xi|\eta)$ – amount of information in ξ relatively η;

$I(\eta|\xi)$ – amount of information in η relatively ξ;

$S(\xi)$ – state entropy ξ;

$MS(\xi|\eta)$ – conditional entropy expected value at variable ξ;
p_{ij} – compatible probability distribution.

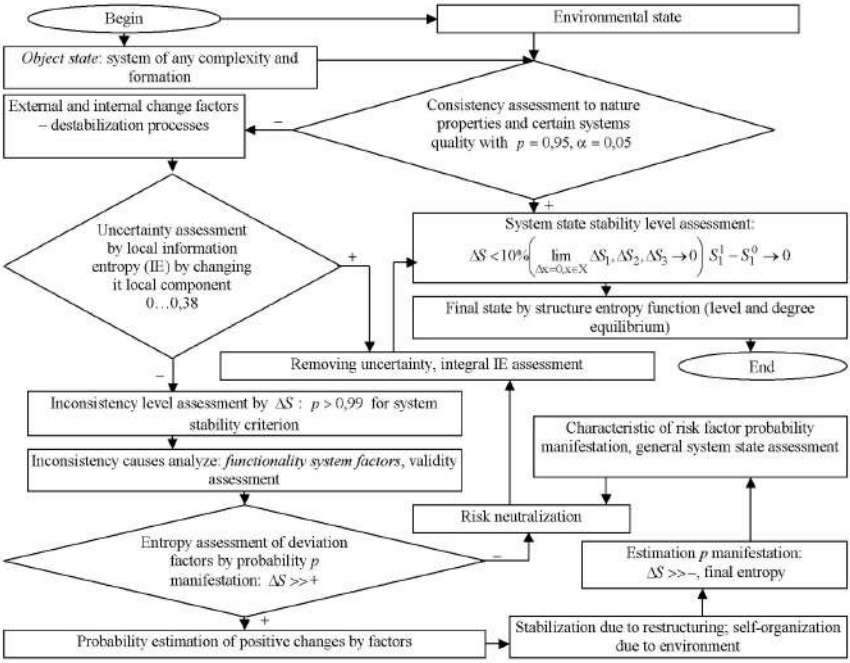


Figure 10. – Probabilistic-entropy assessment of system state and risk factors: ρ – probability of matching the natural properties; α – estimation error; $\varnothing S$, $\varnothing S_1$, $\varnothing S_2$, $\varnothing S_3$ – estimation of general changes, probabilistic, stochastic, random processes respectively

As ξ and η determine the same ratio: the amount of information in η relatively ξ and amount of information in ξ relatively η, then $I(\eta|\xi) = S(\xi)$ [18].

Found that organizational and technical systems related to fuzzy conditions system of their operation, requiring appropriate phenomenological framework usage of experience, knowledge, based on knowledge-based information systems. Applied only thermodynamic nature as a basis for object systems modeling, which permitted entropy method consistent reduction and uncertainties solution designed for comprehensive methodological support of the entropy-comparator conformity quality system objects assessment of any nature safety requirements (Fig. 11).

Logical transformation core is given by relations graph of the component state criteria for ξ and η (fig. 11) [15, 18].

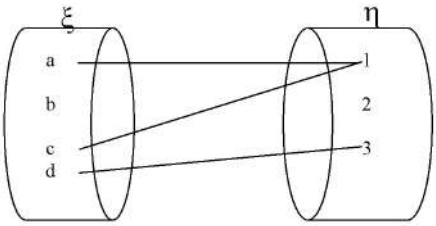


Figure 11. – Graphic scheme core linear logical transformation $K(x,y)$

Providing environmental and economic analysis of the system object ξ due to its complexity and multiple ties with environment gets into the uncertainty situation by the evaluation criteria: economic development level (a – economical system), socio-economic index society well-being (b – socio-economic system), environmental level (c – ecological system), population health assessment (d – social system). Available informational inaccuracies, absence proposed to supplement by the relationship function, for example, existing general information on economic (1), social (2) and environmental (3) quality indicators (see Fig. 11). For getting data about ξ introduced linear-logical transformation core by providing a general quality assessment for ξ, which takes into account all evaluation criteria, that is, have a connection and the final result taking into account the information by η:

$$K(x,y)=\left(x^a \vee x^c\right)y^1 \vee x^d y^3 \qquad ;$$

$$Q(y)=\exists x\in\{a,b,c,d\}\left(\left(\left(x^a \vee x^c\right)y^1 \vee x^d y^3\right)\wedge P(x)\right)=$$

$$=\exists x\in\{a,b,c,d\}\left(\left(\left(x^a \vee x^c\right)y^1 \vee x^d y^3\right)\wedge\left(x^a \vee x^b \vee x^c \vee x^d\right)\right)=y^1 \vee y^3.$$

As $K_1(x,y)$, $K_2(y,z)$, $K(x,z)$ are rectangular matrices, then the conjunction of predicates is considered as a product of matrices:

$$K(x,z)=K_1(x,y)\cdot K_2(y,z)=\underset{y\in N}{\vee}\left(K_1(x,y)\wedge K_2(y,z)\right).$$

Proposed a number of information technology for integrated complex systems safety analysis, designated improvement areas in case of information and methodological support formation for natural and man-made objects comprehensive quality assessment.

Established scientific and practical principles methodological, informational support complex systems state measurement and their functionality, investigated objects safety level based on usage of knowledge-based information systems obtaining knowledge by the study object results at "state (system – environment) – changes – process – system state".

Developed algorithmic approach for object comprehensive analysis in whole, with its microstructure, which proposed to refer not only components and object system and operation processes. In systematic analysis introduced unique

continuous real objects variables display for which the entropy is infinite, via information function (see Fig. 10).

According to provided methodological support information entropy function is introduced to establish the information uncertainty degree, ie the lack about system and its dynamics state information.

Proposed to avoid uncertainty in solving system socio-ecological-economic content objects environmental safety level assessment due to using mathematical logic structural models, combining state analysis and processes in systems, interacting with the environment: entropy state assessment and processes, quality level comparator identification (safety, environmental).

In a detailed system objects study based on their hierarchical structure resulting entropy function is perceived as uncertain behavior not well-ordered system of any dimension. To assess natural territorial complexes state applied thermodynamics, physical, informational entropy to determine environmental quality level for complex objects by only inconsistency measure environmental safety boundaries disparate systems and processes in them: maximum entropy production for one conditions group group (ξ) compatible with its minimum for other (η):

$$S\left(\xi \mid \eta = y_j\right) = -\sum_i p_{ilj} \log_2 \; p_{ilj}, \tag{6}$$

$$MS\left(\xi \mid \eta\right) = -\sum_j P\left(\eta = y_j\right) \sum_i p_{ilj} \log_2 \; p_{ilj}, \tag{7}$$

where $S\left(\xi \mid \eta\right)$ – conditional entropy η at $\xi = x$;

$MS\left(\xi \mid \eta\right)$ – mathematical expectation of conditional entropy with variable ξ.

Adopted entropy adherence function for investigated system objects and determines deviation state level object component and its overall from equilibrium, homeostasis "system – environment", which presented information about danger on any grounds.

The information space concept, system analysis related with conceptual study object model definition under scenario and target approach in order to create knowledge-based systems to it safety situation assess and sustainable development. The information and software develop approaches for solving complex tasks in complex heterogeneous objects assessment for their operation compliance with the environmental safety requirements was analyzed.

Developed the informational-software for practical application ecological safety level integrated assessment methods which based on entropy and information approaches by awareness monitoring data.

Information part formed for system formation state assessment in knowledge-based systems form. Within information and methodological support developed knowledge base on existing data basis about the system, additional information obtained as a result of uncertainty removal provided complex system low level investigation. New data obtained as a final result consistent uncertainties decrease at

detailed scheme study "state1 – process – state 2" applying state system formation "object – environment", with phased complex methodological and information support implementation in complex systems quality assessment (Fig. 12) [15, 18].

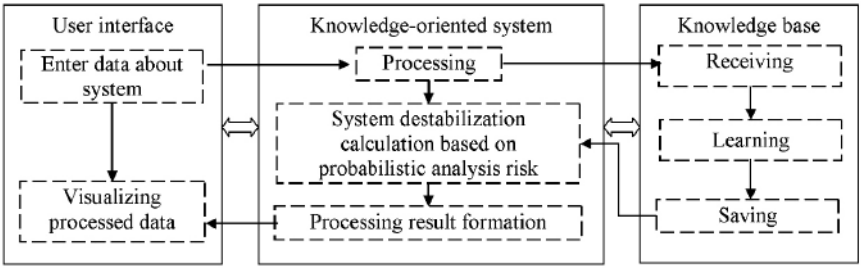


Figure 12. – General scheme of knowledge-oriented information system

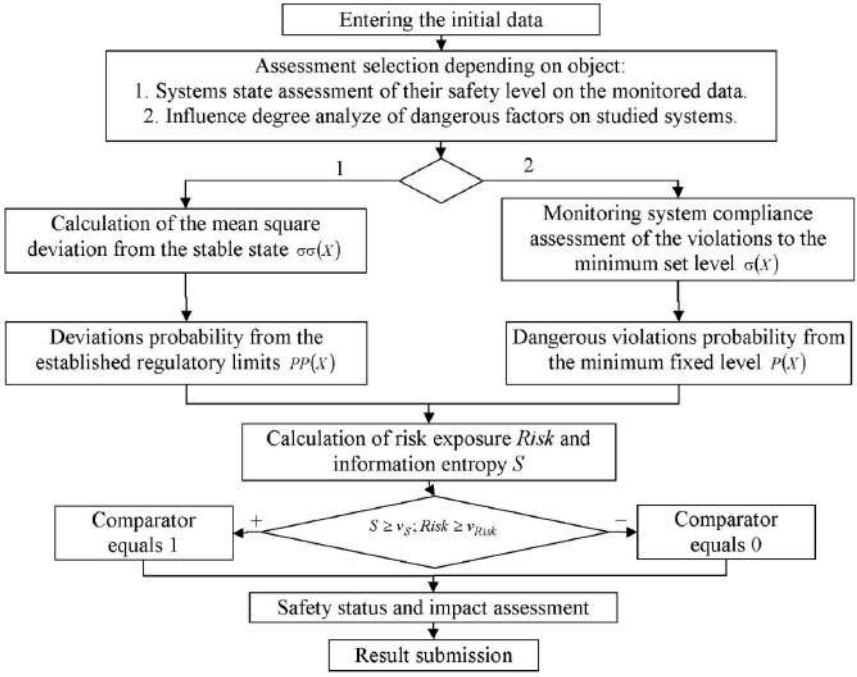


Figure 13. – Assessment of environmental safety level

In practice, the proposed information and software implemented for the comprehensive analysis results on the entropy-information based complex objects study, given the practical environmental safety evaluation results for natural and industrial objects (Zmiev district, heat station), environmental and economic

systems (Zmiev district – population health system) and operative safety control man-made objects based on Android (Fig. 13).

Introduced comprehensive complex objects safety evaluation system is realized in practice in natural and man-made complex safety analyzing in Zmiev district landfill monitoring studies, whose territory is affected by industrial and energy differs significant accumulation of heavy metals (HM) in soils and appropriate level health (Fig. 14).

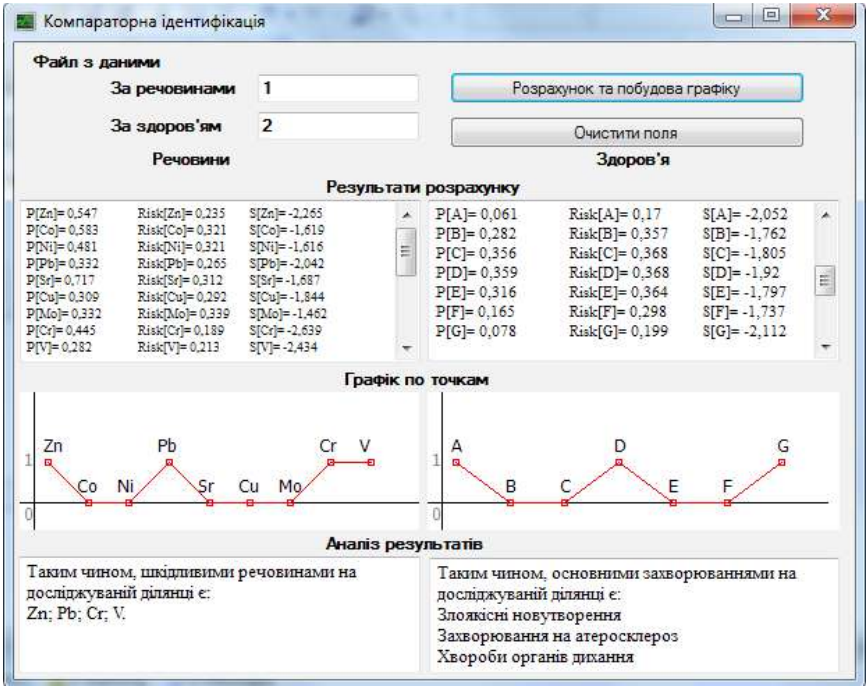


Figure 14. – Ecological safety level assessment of the soil and population health state

At the micro level of complex system analysis to ensure proposed methodological approaches implementation to assess object level safety which is considered at example of factors restoration estimation attainable children with cerebral palsy state capacity (Fig. 15).

On this figure we have the following designations:

– PVI – periventricular ischemia;
– VGK1, VGK2, VGK3, VGK4 – intragastric hemorrhages (I, II, III, IV stages);
– PVL1, PVL2, PVL3 – periventricular leukomalacia (I, II, III stages).

The mobile devices oriented software that functioning on operating system Android, for continuous security processes monitoring on the example selecting effective treating sludge water means at coal-concentrated industries (Fig. 16).

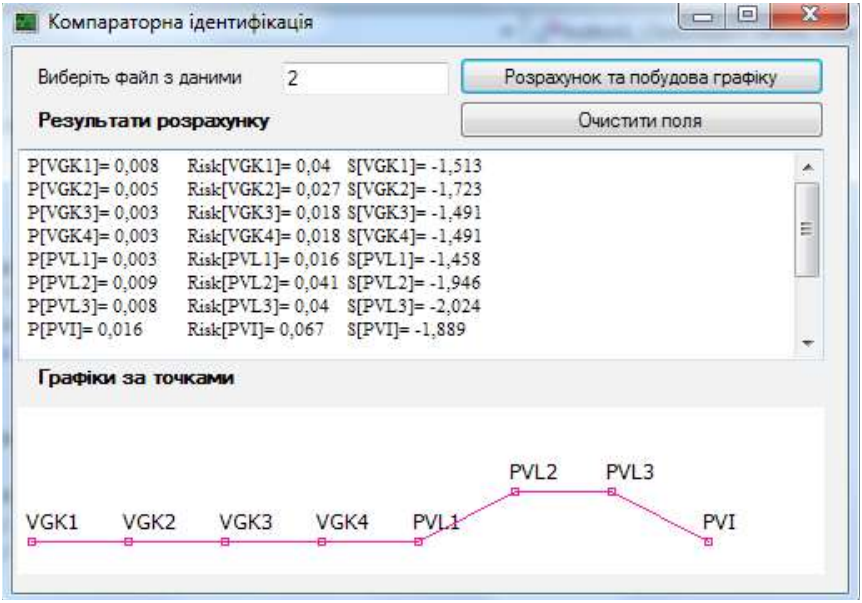


Figure 15. – Program evaluation of stabilization state factor of children cerebral palsy patients

Figure 16. – Deposition process state determination according to the experimental data

Thus, the proposed entropy approach to substantiating a comprehensive system for evaluating the overall object and processes state of an external and internal nature, based on a knowledge-oriented base and system entropy theory, allows to solve problems of various directions and purposes from the standpoint of identifying conditions for achieving the goal and realizing natural coherence "object – environment".

Conclusion

1. The information and methodological support comprehensive analysis of the environmental safety of objects based on entropy and information awareness approaches of monitoring data. Algorithmic implementation of methodological support software for quality evaluation of complex systems-level research "state (system – environment) – process – system state" is proposed [15–18].

2. Analyzed approaches in developing information and software support for solving complex tasks of heterogeneous complex objects accordance assessment to their environmental sustainable development operation and environmental safety requirements.

3. The software was developed for continuous environmental safety monitoring in terms of anthropogenic impact areas, the unstable system state, management and selection of effective production processes according to the provided comprehensive analysis and assessment of diverse complex systems and dangerous situations [15–18].

References:

1. Николис Г. Самоорганизация в неравновесных системах: От диссипативных структур к упорядоченности через флуктуации. [Текст] / Г. Николис, И. Пригожин.– М.: Мир, 1979.– 512 с.
2. Бриллюэн Л. Научная неопределенность и информация [Текст] /Бриллюэн Л.– М.: Мир, 1966.– 272 с.
3. Вяткин В. Б. Синергетическая теория информации: пояснения и терминологические замечания [Электронный ресурс] / В. Б. Вяткин // Научный журнал КубГАУ.2012. – № 80(06).– С. 1–36.– Режим доступу до журн.: URL: http://ej.kubagro.ru/2012/06/pdf/46.pdf
4. Пригожин И. Р. Конец неопределенности [Текст] / И. Р. Пригожин.– Ижевск. НИЦ, 2000.– 208 с.
5. Пригожин И. Р. Порядок из хаоса [Текст] / И. Р. Пригожин, И. Стенгерс.– М.: Наука, 1986.– 432 с.
6. Коваль А. В. Модель сценарно-целевого похода при построении информационно-аналитической системы [Текст] / А. В. Коваль, Ю. Д. Бойко, Е. А. Зайцева // Системный анализ и информационные технологи: материалы 16-й Между народ. н-т конф. SAIT-14. – К.: УНК "ИПСА» НУТУ «КПИ», 2014.– С. 105–106.

7. Горбань И.И. Энтропия неопределенности [Текст] / И.И. Горбань // Математичні машини і системи.2013.– № 2.– С. 105–117.
8. Вечірська І.Д. Про дослідження властивостей лінійних логічних перетворень [Текст] / І.Д. Вечірська, Ю.П. Шабанов-Кушнаренко // Системи обробки інформації.2007.– Вип. 8 (66).– С. 130–133.
9. Xinghao Wang. Editorial: environmental informatics for environmental planning and management / Wang Xinghao // Journal of Environmental Informatics 2007.– № 9(1) – P. 1–3.
10. Kumari J. Entropy change as influenced by anthropogenic impact on a boreal land cover – a case study [Text] / J. Kumari, A. Govind, A. Govind. // Journal of Environmental Informatics.2006.– № 7(2) – P. 75–83.
11. Jae-Yoon, Jung. An entropy-based uncertainty measure of process models [Text] / Jae-Yoon Jung, Chang-Ho Chin, Jorge Cardoso.– Information Processing Letters.2011.– № 111.– P. 135–141.
12. Parvathi Chundi, Rui Zhang, Entropy Based Measure Functions for Analyzing Time Stamped Documents, Proceedings of the Fourth Workshop on Text Mining [Text] / Parvathi Chundi Rui Zhang.– Sixth SIAM International Conference on Data Mining, Hyatt Regency Bethesda, Bethesda, Maryland.– 2006.
13. Барабаш, О.В. Побудова нечіткої бази знань системи управління складною організаційно-технічною системою [Текст] / О.В. Барабаш, В.А. Савченко, А.С. Слюняєв // Авиационно-космическая техника и технология.2010.– № 2 (69).– С. 79–82.
14. Голян Н.В. Алгебро-логические модели конструкций неявного выбора в бизнес процессах [Текст] / Н.В. Голян, Ю.П. Шабанов-Кушнаренко // Системи обробки інформації.2011.– Вип. 8(98).– С. 275–278.
15. Козуля М.М. «Комплексна інформаційно-системна оцінка рівня екологічної безпеки складних об'єктів», дис. канд. наук., Сум. держ. ун-т, Суми, 2017.
16. Козуля Т.В. Основы методологии комплексной оценки экологичности системных объектов (Теоретико-практические основы методологии комплексной оценки экологичности территориальных и объектовых систем.) Монография.– Saarbrücken: Palmarium Academic Publishing, 2014.– 298 с.
17. Kozulia T., Kozulia M. Determining the object structure of ecological and economic research and knowledge base for decision support Problems of atomic science and technology, 2017. – № 3(109). Series: Nuclear Physics Investigations (68), – P. 85–89.
18. Kozulia T.V., Kozulia M.M. Integrated information system assessment of complex objects safety level. Bulletin of the National Technical University "KhPI". Series: System analysis, control and information technology.– Kharkiv.– № 55(1276).2017.– P. 39–45.

CHAPTER II. CYBERSECURITY

Self-organizing organizational structures of cybersecurity systems

Oleksandr Milov
Doctor of Philosophy, Associate Professor
Department of Cyber Security and Information Technology
Simon Kuznets Kharkiv National University of Economics
ORCID: https://orcid.org/0000–0001–6135–2120

Volodymyr Aleksiyev
Doctor of Technical Sciences, Professor
Department of Cyber Security and Information Technology
Simon Kuznets Kharkiv National University of Economics
ORCID: http://orcid.org/0000–0001–6767–7524

Abstract. *The issues of self-organization of the team of agents in cybersecurity systems are discussed in this section. The approaches to the definition of self-organization, functions and structures of self-organizing systems are presented. Formed a set of mathematical models included in the model of self-organization. For the structures under consideration, such system characteristics as stability, sensitivity and flexibility are defined, and a list of tasks that ensure the assessment of the stability of the organizational structures of cybersecurity systems is defined.*

Keywords: *self-organization, stability, mathematical model, adaptability, structural and functional models*

Introduction

Cybersecurity systems (CS) undoubtedly belong to the class of complex organizational systems, the main features of which are the number of their constituent elements, the variety of links between the elements, and the limiting uncertainty (a priori or arising during operation).

The approach to solving the problem of managing such complex systems may consist in creating systems capable of self-organization, and possibly making logical decisions, i.e., making decisions in alternatives that are equally likely. When constructing the structure of such systems, the principles of self-organization are used.

Usually self-organizing systems are considered based on biological principles [1]. A characteristic feature of such systems is continuous adaptability to changing

external and internal conditions and continuous improvement of functioning under constant conditions, taking into account past experience. The above properties are typical for self-organizing systems.

By self-organization we mean the development of an optimal algorithm for the functioning of a system and the choice of a learning strategy in accordance with a pledged function, or self-organization is the creation, reproduction or improvement of an organization of a complex dynamic system.

Perhaps the following definition of a self-organizing system is a set of interconnected elements (subsystems) that, independently on the basis of accumulated experience under the influence of the external environment and internal microstates, increase the degree of their organization with the aim of improving the functioning of the system and implementing the inherent functionality.

New approaches to the definition of "self-organization" offer synergetics. One of the properties of self-organizing systems is its purposeful (expedient) behavior. Under expediency is understood as a general characteristic of the behavior of complex dynamic systems, aimed at achieving a specific end result. The concept of expediency means that an act or behavior can be considered directed towards achieving a "goal", that is, a final condition in which the system establishes a certain temporal or spatial relationship with another system. Then the term "expediency" is used as a synonym for a goal controlled by feedback.

Analysis and synthesis of cybersecurity systems with the properties of self-organizing systems should be performed using a systematic approach, i.e. from different sides and at different levels. Within the framework of a unified system approach, an extensive network of mathematical models of systems can be built, taking into account different generalities, different types (classes) of organization and a different subject area.

A cyber security system as a self-organizing system is characterized by a set of functions performed by it. The functional description consists in defining the functions of the system, given in accordance with the spatial or structural feature. System functions are defined through interconnections with other systems.

Analysis of self-organizing structures of cybersecurity systems

Structural description is reduced to the description of the structure based on functional characteristics. The structural approach is otherwise called morphological. It focuses on the analysis of the elements of the structure and their organization. Each element is considered as a system, the functions of which are realized with the help of connections of this element with others. There are informational, structural and financial ties. The informational description of a system determines the dependence of its structural and functional properties on external and internal information.

The mathematical model of a self-organizing system is constructed in accordance with its definition and properties [2–4]. The basis for building the model is a structural-functional approach. From the point of view of this approach, the self-organizing SS system can be viewed as a set:

$$SS = \langle \Sigma, \Phi, R_w, G, A, P, \Theta \rangle,$$

where Σ is the structure of the system;

Φ – system function;

R_w –is the emergence ratio;

G – many goals;

A – the relation of adaptability;

P – a set of memory elements;

Θ – set of time moments.

System structure. One of the most important characteristics of a self-organizing system is its structure. The concept of structure reflects the orderliness, organization of the system. The definition of the concept "structure" is reduced to the statement that this is a way of organizing – interconnection – of separate parts or elements. The structure of the system will be understood as a set of elements and relations between them, which are determined on the basis of the distribution of functions and goals set for the system. Moreover, the structure Σ is considered as a multigraph with certain nodes:

$$\Sigma = \langle S, C, R, R_i \rangle$$

where S is the set of elements of the system (the nodes of the multigraph);

C – the set of parameters of elements (the set of statements regarding the properties of the nodes of a multigraph);

R – the set of connections between the elements (arcs of a multigraph);

R_i – the incidence relation that assigns a pair of nodes to each arc.

The structure of self-organizing systems is characterized by integrity, adaptability and development.

The integrity of the structure of the system is determined by the set of elements and the branched connections between them. Depending on the purpose of the study, there are several criteria for distinguishing a system, forming a system of parameters. The integrity of the system is manifested in two laws:

– the whole is not reduced to the simple sum of the parts;
– a change in one part causes a change in the other parts and in the system as a whole.

The adaptability of the structure of the system, its response to changes in the environment emphasize its dynamic properties – its variability in functioning. The property of adaptability determines the internal transformations of the structure, which are implemented by the elements, do not go beyond its borders and are aimed at maintaining and improving functioning.

The extreme form of system variability is the development of its structure, which is understood as the complication of the system, its accumulation of information, the transition to a more ordered state.

System function It is, in contrast to the structure, an external manifestation of its properties when interacting with the encompassing environment (the market).

The function of the system is a way to act when the goal is achieved and for a self-organizing system is determined by its goal.

Set the system function as

$$\Phi = \langle \Pi, F \rangle,$$

where Π – the set of variables that determine the function of the system;

$X \subseteq \Pi = W \times M$;

X – is the set of input actions that interact with the information inputs W;

F – the set of functions on variables that, for each element, determine the dependence of the output variables on the input variables.

A state is a set of essential properties that the system possesses at a given time. The state of the system is determined by the set of states of its elements.

The functions implemented by the self-organizing system can be conditionally divided into three groups: target, basic (basic), auxiliary (additional).

The objective function corresponds to the main functional purpose of the system and is set solely by the purpose of its operation.

The main functions reflect the orientation of the system and are a combination of the macrofunctions implemented by it, necessary for the most optimal achievement of the goal, and are determined by the objective function and the system quality criteria.

By additional functions, we will mean functions aimed at maintaining or improving the quality of the system's functioning within certain limits.

The set of functions of the self-organizing system, as well as the structure, is determined by unity, adaptability and development. Since it has integrity, the first condition for its existence should be the unity of its functioning. The function is the defining side of the system and represents the unity of its composite properties, internal processes, relationships. The unity of the functioning of the system is the subordination of the behavior of the system of a single goal. The adaptability of the functions of the system is manifested in their change depending on changes in the external and internal environment. The development of the system in functional terms is expressed in the expansion of its functional capabilities.

Emergence. The emergence relationship R_w reflects the unity of the structure and function of the system, the relationship between them. It is a parameter forming a system: from the two previous objects – structures and functions – it forms a system. Neither structure nor function form a system. The emergence in some way connects the elements of the structure with functions, maps Φ into Σ: $R_w = |\Phi| \times |\Sigma|$, where $|\ldots|$ means a set of elements of Φ or Σ; $\times$ – the sign of the Cartesian product of two sets.

Set of goals. The set G corresponds to the set of goals facing the system; G is a multi-grid, i.e., a distributive grid endowed with join, intersection, and composition operations. If $\alpha_1 \le \alpha_2$, then $\alpha_1 \circ \alpha \le \alpha_2 \circ \alpha$ and $\alpha \circ \alpha_1 \le \alpha \circ \alpha_2$ $\forall \alpha, \alpha_1, \alpha_2 \in G$. The order relation on G is interpreted as follows: if $\alpha_1, \ldots, \alpha_n \in G$ and $\alpha_1 \le \alpha_2$, then the solution of the α_2 problem provides for the solution of the α_1 problem; $\alpha_1 \cup \alpha_2$

interpreted as a task consisting in solving problems α_1 and α_2; $\alpha_1 \cap \alpha_2$ – as the largest of those problems whose solution is obtained simultaneously with the solution of problems α_1 and α_2. The operation of composition on G is interpreted as a strictly sequential solution of problems, and the closure of G with respect to composition means that an arbitrary development of a set of targets in time is provided in the system. The sets Σ and G are connected as follows. Let $H(\Sigma)$ be the set of mappings that preserve the order of a partially ordered set Σ into itself. Then $H(\Sigma)$ is a multigrid with operations $\cup$, $\cap$, and $\circ$, and there is a homomorphism $\gamma : G \to H(\Sigma)$.

The assignment of a mapping $\gamma : G \to H(\Sigma)$ reflecting the restructuring of the system under the influence of the goal α can be taken as a comparison of the goal $\alpha \in G$ and the structure $\sigma \in \Sigma$ of some new structure $\sigma' = \gamma(\alpha)\sigma$.

Adaptability. The relationship of adaptability links the behavior and structure of the system with changes in the effects of the external environment and with internal states. Adaptability in some way reflects the effects of the external environment X and the state M on the structure Σ and the function Φ. This ratio falls into two: A_1 and A_2. $A_1 < A_2$ and. Here

$$A_1 = |\Xi| \times |\Sigma|; \quad A_2 = |\Xi| \times |\Phi|$$

where $\Xi = W \times M$, $X \subseteq \Xi$.

Time. Θ is a directed set of moments of time, that is, a set with an operation ≤. In a self-organizing system, a specific situation ς is put in correspondence with each moment of time, that is, there is a map $\beta : \Theta \to \Omega$, where Ω is a set of situations.

Memory. In order to use previous experience, the cyber security system must be able to accumulate and store information, that is, have a memory. Memory is a set $P = \{z_\beta\}_{\beta \in I}$ of various elements representing a distribution grid with join $\cup$ and intersection $\cap$ operations. The operation of intersection of the elements z1 and z2 is interpreted as the allocation of a common memory area for situations ς1 and ς2, which have similar parts, and the join operation – as the allocation of a part of memory for dissimilar situations ς1 and ς2. The closedness of the set P with respect to the operations of union and intersection extends the number of possible states of memory.

Let $K(Q,U)$ be the set of maps of a Cartesian product $\Omega \times \Omega = \Omega^2$ into the set of solutions U: $K(\Omega,U) = \{\varphi \mid \varphi : \Omega^2 \to U\}$. The set $K(Q,U)$ will also be a distributive grid. For the memory operation, it is necessary that the grid $K(Q,U)$ be mapped homomorphically to the grid P, that is, that a homomorphism $\xi : K(\Omega,U) \to P$ exists.

The structural-functional approach includes two stages.

Structural analysis. One of the most important characteristics of the system is its structure. The structures of self-organizing systems are distinguished by a large number and variety of elements and connections between them, which are derived from the distribution of system functions and the goals set for it.

The goal of structural analysis is to build a visual model that displays the existing system of relations of elements both with the external environment and with each other.

When building models of self-organizing systems, their structure should be considered at the level of organization, functioning and implementation. When analyzing the system at the organization level, the following is done:

– a description of its composition and construction of the structural scheme;
– definition of subsystem functions and drawing up their functional diagram;
– description of connections between subsystems and between elements.

When analyzing at a functional level:

– functions of the system, subsystems and elements are studied;
– their relationships are determined;
– a generalized functional structure of the tasks of the self-organizing system is compiled.

When analyzing at the implementation level:

– identifies the main elements necessary for the implementation of a self-organizing system;
– a structural model of the system is compiled, taking into account the topology of the location of the elements and their interaction with each other and with the external environment.

Functional analysis. Functional analysis is based on the study of the functioning of the system in time, its interaction with the external environment, expressed in its perception of input signals and disturbing influences and in its response in the form of output signals. The functioning of the system in time is determined by its transition from state to state and the change in output signals. We define the concept of functional analysis.

Model of operation – predicts a change in state over time.

The set of moments of time Θ is a directed set of real non-negative numbers. The set Θ can be continuous, discrete, or discrete-continuous. The functioning of the system in time is considered as the transition of the system from state to state.

The state of a self-organizing system is defined as a set of states of its elements:

$$\vec{m} = \left(m_1, m_2, ..., m_i, ...m_n\right), \vec{m} \in M,$$

where $\vec{m}$ is the state of the system; m_i is the state of the i-th element;

M is the state space, which is defined as the Cartesian product:

$$M = M_1 \times M_2 \times ... \times M_i \times ... \times M_n,$$

where M_i – set of states of the i-th element.

Input signals $\vec{w} \in W$ of the self-organizing system. Here W is the input signal space, which is a vector $\vec{w}(\tau) = \left(w_1(\tau), w_2(\tau), ..., w_i(\tau), ..., w_n(\tau)\right)$, where $w_i(\tau)$ is the input signal at the i-th input of the system at the time τ.

The input signal space W is called the direct product $W = W_1 \times W_2 \times ... \times W_i \times ... \times W_n$, where W_i is the set of signals of the i-th input.

The output signals of the system $v \in V$ are defined in the same way as the input signals: $\vec{v}(\tau) = (v_1(\tau), v_2(\tau), ..., v_i(\tau), ..., v_m(\tau))$, where vi($\tau$) is the signal of the i-th output at the time τ.

The output signal space $V = V_1 \times V_2 \times ... \times V_i \times ... \times V_m$, where V_i is the set of signals of the i-th output.

The study of the dynamics of self-organizing systems is complicated by the fact that they are systems with aftereffect. The future of its behavior depends on the prehistory of its states, i.e. the state $\vec{m}(\tau)$ of the system at a time $\tau > \tau_0$ is determined by how it came to a state $\vec{m}(\tau_0)$. The difficulty also lies in the fact that these systems belong to the class of indeterministic. To trace the causal relationships in them is impossible. The dependence of the output signals on the input and on their states is ambiguous.

Structural and functional model. Although biological self-organizing systems may be distributed, it seems appropriate to select in them the blocks corresponding to the functions performed. Taking into account the above presentation of the self-organizing system, the structural-functional model shown in (Fig. 1) is proposed. Here are the following designations:

- S is a self-organizing network;
- BSP – block the source program;
- the BSS is a block of structural self-organization;
- BFS – block of functional self-organization;
- BPS – block parametric self-organization;
- BG – block of the goals;
- BCC – block of criteria calculation;
- BM – block of memory block;
- BC – control block.

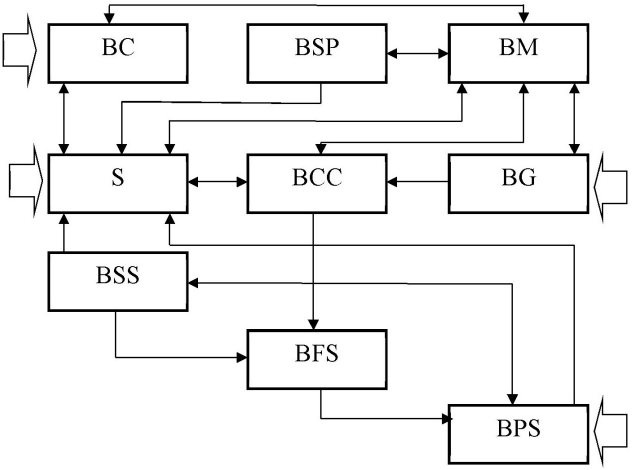


Figure 1. – Structural and functional model of self-organizing system

External environment. The external environment will be understood as a set of elements that are not included in the system, but a change in their state causes a change in its state. Since the system is connected to the environment with its informational and control inputs and outputs, we will assume that the environment affects the system through its inputs. The medium may include any source of information. Sometimes, for the purpose of simplification, the environment is considered as a source of successive signals, selected from a finite alphabet. In the case of a cybersecurity system, the external environment is a multitude of sources of threats.

Self-organizing network. It is the network S of the self-organizing system that represents the indeterministic part of the system. With the help of other blocks, an object model is built on the network, a sequence of heuristics and self-organization algorithms are implemented.

We define a sequence of heuristics as a sequential construction of a statement in discrete time, when at the initial moment a certain system of statements is specified, and at each next moment a system of statements is obtained according to certain rules (programs) from those available at the previous time. These rules may change during the evolution of a sequence of heuristics.

The sequence of heuristics is characterized by the ambiguity of intermediate results. The ambiguity is determined, on the one hand, by its nature as a search procedure, on the other, by the position of each of the rules applied in their general list, as well as accumulated constraints and heuristics. By fixing the sequences of states of the self-organizing system, as well as the laws and heuristics that led to the achievement of the goal, one can obtain various implementations of the heuristics sequence.

The sequence of operations given in a certain self-organizing system when it reaches its goal, obtained when implementing a certain specific set of conditions, is called the implementation of a sequence of heuristics.

A network consists of a set of elements determined by the complexity of the task, with a changing function of the element and a multitude of adjustable connections. The parameters of links and elements, their functions change depending on the class of the tasks being solved, their specific conditions and environmental conditions when solving the problem. Network rebuilding is carried out depending on the state of other units of the system.

Source program BIL makes a selection of the types of elements used in solving a particular class of problems. Specifies a preliminary structure of the system, a preliminary set of functions of the elements that will be used during self-organization, a preliminary set of parameters. In addition, it sets restrictions on the structure of the system, types of functions of elements, parameters. The source program may include an extension of the class of tasks solved by the system.

Structural self-organization. The BSS changes the network structure by increasing or decreasing the number of elements in the network, changing the pattern, number and nature of connections. This unit controls the highest level of system adaptability.

Functional self-organization. The BFS adapts the type of functions of network elements according to and controls the start of structural self-organization when the resources of functional self-organization are exhausted and the target is not achieved.

Parametric self-organization. BPS adjusts the system parameters by one of the methods described above. If the target is not reached within a certain time, it starts the block of functional self-organization.

The goals of the self-organizing system. BC manages the development of criteria for self-organizing system. The goals of the system in this case are set from the outside and are predefined for the system.

Calculation of the criteria. The selection and calculation of criteria is carried out by BVK. The selection of criteria is determined by the goal and is made from the set of permissible criteria that are heuristic and is laid in IOO during the design of the system.

The accumulation and storage of information is made in the BP, which is associated with almost all the blocks of the self-organizing system. It stores information about the past behavior of the system, about the situations that led to the achievement of the goal.

Control block. Recording and retrieval of information from the memory, depending on the signals at the control output of the network, is controlled by the BC.

Sustainability, sensitivity and flexibility of organizational structures of Cyber Security

In the theory of automatic control of systems, the stability of a system is understood as its ability to return to its original state when external influences are eliminated. This definition, when applied to cybersecurity structures, would mean that the technological and organizational structures are capable of self-healing (or self-organization) when restoring the previous state of the functioning environment. However, firstly, this situation does not take place in cyber threats, since they are in continuous development under the influence of various factors, such as changes in the general nature of threats, the emergence of hybrid threats, general economic trends, scientific and technological progress and other factors. Therefore, it cannot be considered possible to return to the initial state, i.e. complete removal of external influences. Secondly, the technological and organizational structures can undergo changes only as a result of the decision made on its reconstruction, modernization, replacement, etc. Although at some stage in the development of the security system it may be advisable to return to the structure that has already been used, the decision to do so is made in a specific situation and is a consequence of responding to external threats.

Thus, the concept of sustainability, as it exists in the literature, does not apply to the structures of cybersecurity systems.

Another concept of sustainability is formulated by J. Casti [5]. Considering the structures described by oriented graphs, we introduce the concept of stability, connecting the effect of changes in the value of the function $v_i(t)$, describing the state

of a vertex of the graph u_j to the initial changes of $p_j(t)$ to another u_j depending on the intensity of the influence $f(u_i, u_j)$ (propagation of disturbances in the graph). A node u_i is called stable if an infinite sequence of values of the function $v_i(t)$ is bounded. And the whole graph is stable if all its vertices are stable.

The structure of cybersecurity systems that ensure the sustainable implementation of various business processes operating in virtual environments created by Internet technologies is, as a rule, a hierarchical structure that can be described as a tree type graph, where each of the vertices is in turn described by a graph primarily of information flows. Within the framework of the strategic management structure, the cybersecurity system structure is a subgraph, some of its vertices are adjacent to the vertices of another graph, representing the structure of both cyber attacks and means of countering them. The complexity of using the concept of sustainability lies, firstly, in determining a single function that characterizes all the vertices of the structure, and secondly, in determining the intensity of influence of some structures on others, and finally, this concept of sustainability does not take into account the possibility of changing the composition of the vertices of the structure graph, which is precisely the most important in the study of the structures of cybersecurity systems.

Thus, it is necessary to develop such a concept of sustainability, which would [6]:

- took into account the continuity of changes in the structure of multiple cyber attacks of the security system;
- did not contradict the specifics of changes in the technological and organizational structure of the cyber security system associated with decision making;
- took into account the possibility of changes in the composition of the elements of the structure;
- had an interpretation in both information technology and economic categories and would allow to construct quantitative assessments of all components of the structure of strategic, tactical and operational management.

From the point of view of assessing the quality of the structure in relation to the environment of the formation of cyber attacks, the tasks of assessing sustainability are the most important. They are designed to clarify the conditions for maintaining the structure. If the concept of structure flexibility can be viewed from the standpoint of the flexibility of hardware and software, then the concepts of stability and sensitivity are not considered at all. To introduce these concepts, it is necessary to consider the structure as a dynamic object with the property of adaptability. The following construction is not limited to the framework of a certain structure that constitutes a structure, first of all, of strategic management, but is in a sense universal and proceeds from the general principles of sustainability.

In the future, if the structure that is part of the overall cybersecurity strategic management structure is considered in its relationship with others, it will be called a substructure. If the structure is considered independently, then it will be called simply a structure.

Consider the external environment of any substructure. It includes both the external environment of the entire security system and other substructures. Over time, the external environment of functioning undergoes certain changes. Let the external environment be described at each moment of time t by the vector of parameters ξ_t from the space of possible states of the external environment Ξ. Fixing some time point t_0, we follow the change of the vector t_0 during the time interval $[t_0, t_1]$. During the time $D_t = t_1 - t_0$ in the space of possible states of the external environment Ξ, the trajectory of the environment will be formed, consisting of the sets ξ_t, $t \in [t_0, t_1]$. Denote the time interval $[t_0, t_1] = T$. If the laws of environmental change are known, and it is possible to unambiguously determine its behavior on the interval T, then in all subsequent constructions the concept of a trajectory can be used. For the purposes of determining sustainability, it is not so much the change in the state of the environment of the formation of cyber threats in the past observed periods as the prediction of its state and the predicted trajectory. The laws of changing the state of the environment of a security system cannot be considered absolutely known due to its great variability and insufficient knowledge. Therefore, we can only talk about the predictive set of environmental conditions. This set is determined by the factors taken into account, forecast accuracy, initial conditions, etc.

We call the set of predicted states of the external environment on the interval T the variety of the external environment Ξ_T. The volume of this variety, $-V_\Xi-$, will be determined by the variability of the external environment, the parameters describing it, and the accuracy of the forecast. The specific form of this quantity depends on the structure under consideration and needs special construction.

Let S be the space of various structures of one purpose (for example, structures of information security systems). The concept of quality includes, as an integral part, the degree of compliance of the security system structure with a multitude of potential cyber threats in such a way that the structure should as far as possible meet the requirements of the external conditions at each point in time. Consequently, each point ξ_t of the trajectory of the environment in the space Ξ will correspond to some structure S_t from the space S. The combination of these structures constitutes the trajectory of the structure during the time interval T.

Considering the predictive set of states of the environment, we obtain the set of all structures corresponding to the elements of the variety of the environment. We call this set the variety of structures S_T. Thus, if $a()$ is a mapping that allows the structure S to be constructed from the current state of the external environment (multiple attacks) ξ, then we have:

$$0 : \Xi \to S, \tag{1}$$

$$a(\Xi_T) = S_T. \tag{2}$$

The main characteristic of the diversity of S_T structures is its volume $-V_S$. The essence of the V_S volume is a reflection of the degree of diversity of structures that

need to be built to ensure that the structure corresponds to the set of potential cyber threats from the environment of operation at each time point from interval T.

The concepts introduced allow us to come to the following definition of stability.

Definition 1. The stability of the structure – the ability of the structure to ensure the invariability of the results of the functioning of the cybersecurity system with a constant strategy of its behavior under the conditions of hybrid threats (the ability of the structure to correspond to the greatest possible diversity of the external environment).

The structure S_0 corresponding to the initial state of the external environment ξ_0 is called stable in correspondent to the variety Ξ_T, if the condition

$$V_S(S_T) << \delta V_{\Xi}(\Xi_T), \tag{3}$$

where the variety Ξ_T is obtained by the prediction on the initial state ξ_0; the variety S_T is obtained according to (2).

The concept of sustainability thus defined is closest to the sustainability of adaptive systems.

The concept of sensitivity of a structure is closely related to the concept of stability. They can be considered as reciprocal. Depending on the situation in which the structure is studied, and the objectives of the study, either both concepts can be used, or each of them separately.

Definition 2. Let us call the sensitivity of a structure the ability of a system to change its state and the result of functioning when changing a multitude of cyber threats from the external environment. The measure of sensitivity is the ratio of the volume of necessary changes that must be made in the structure to the volume of changes in the state of the environment from the point of view of multiple cyber threats during the period of time T:

$$d(S_0, T) = \frac{V_S(S_T)}{V_{\Xi}(\Xi_T)}. \tag{4}$$

The measure of sensitivity and stability are among the many criteria for the quality of a structure. The importance of the criteria is determined by the current situation and the purpose of the functioning of the security system as a whole. As was noted, in different situations of functioning of cybersecurity systems, the criteria may have different interpretations and, moreover, the very concept of quality includes a different set of criteria, the role of a particular criterion as positive or negative also depends on the situation of solving problems. In particular, under the conditions of a constructed and functioning structure, the addition of the concept of stability is stability with correspondence to transformation.

Let some resources be allocated to ensure compliance of the structure with the current state of the environment, for example, the amount of funds that can be spent on the transformation of the cybersecurity system (or the allowable amount of losses from non-compliance with many cyber threats) – C^* and the maximum time T^*. Then, if the original structure S_0 is to be transformed into S_t, then the transformation process must satisfy the following conditions:

$$C(S_0, S_t) \leq C^* \quad (5)$$

$$t(S_0, S_t) \leq T^* \quad (6)$$

where $C(,)$ – transformation cost;

$t(,)$ – time to transform.

The restriction (5) reflects the availability of funds for the transformation, and the restriction (6) means that the transformation must not only be carried out, but also within a certain period. A longer time deprives of its expediency, since the forecast of the state of the environment cannot be reliable for a longer period due to its large variability.

Definition 3. We call a structure flexible with correspondent to resources if the changes that need to be carried out in it during time T satisfy the constraints (5) – (6).

If, along with the variety of structures of S_T, the variety of S_R can be obtained – all sorts of transformations of the original structure within the constraints, then the concept of sustainability receives the following extension.

Definition 4. We call a structure stable in resources with correspondent to the variety Ξ_ν if $S_R \supseteq S_T = a(\Xi_T)$.

Those, the structure has the ability to comply with the state of the external environment (the set of potential cyber threats) for a given period of time with given restrictions on resources.

From consideration of the concepts introduced, it follows that the process of assessing the stability of a structure breaks down into a number of subtasks:

Determine the set of parameters describing the set of cyber threats from the external environment – ξ.

Determine the current state of multiple cyber threats from the external environment – ξ_0.

Predict the state of the multitude of threats for a given period of time T and build a diversity of the external environment Ξ_ν.

Design a mapping $0()$, allowing to construct the structure under study.

Construct the structure S_0, corresponding to the initial state ξ_0 and the variety S_T, corresponding to the variety Ξ_ν.

Determine the stability and sensitivity of the structure S_0 with respect to the variety Ξ_ν.

To determine the flexibility of the structure, it is necessary to solve additional problems.

Determine the amount of resources allocated for the transformation of the cybersecurity system (C^*, T^*).

Identify the many possible transformations – S_R.

Determine the flexibility of the structure with respect to resources.

Conclusion

In the modern environment of the Internet virtual space, there is an invariable threat of cyber-attacks. It should also be considered the different nature of these cyber threats and the appropriate environment or distribution space, for example, data transmission channels, data processing systems or computing systems, as well as data warehouses. In most cases, cyber threat is not only one type of attack, intrusion or data compromise, but a series of certain way planned or relatively random incidents that can provoke a synergistic effect of their influence and lead to extremely undesirable consequences. Consequently, a special approach is needed to ensure the reliability of cyber defense, considering the hybrid nature of the threats and the actual open space of the Internet, including other (heterogeneous) conditions for transmission and communication in the digital environment.

It is proposed to consider the cyber defense system as a self-organizing organizational structure, which is constructed like the functioning, development and adaptation of biological organisms. This should contribute to the creation of systems that provide an adequate level of protection when the conditions for self-organization and adaptation to external threats are realized, as well as the desire to obtain a synergistic effect on the cyber defense systems. For the construction of such systems described mathematical tools. In turn, the direction of development of self-organizing organizational structures of cybersecurity systems should satisfy the conditions of stability, sensitivity and flexibility of organizational structures.

References:

1. Camazine Scott. Self-organization in Biological Systems / Scott Camazine, Jean-Louis Deneubourg, Nigel R. Franks, James Sneyd, Eric Bonabeau, Guy Theraula. Princeton University Press, 2003.– 538 p.
2. Gershenson Carlos. Design and Control of Self-organizing Systems. Mexico City Boston Vicosa Madrid Cuernavaca Beijing CopIt ArXives, 2007.– 188 p.
3. Gershenson C. A General Methodology for Designing Self-Organizing Systems. ECCO working paper 2006. 2005–05.
4. Fernando Rosas, Pedro A. M. Mediano, Martín Ugarte, and Henrik J. Jensen. An Information-Theoretic Approach to Self-Organization: Emergence of Complex Interdependencies in Coupled Dynamical Systems. Entropy 2018. 20, 793.
5. Castie John. Large systems. Connectivity, complexity and disaster.– M.: Mir, 1982.– 216 p.
6. Milov A. V., Polyakova O. Yu. Modeling the system characteristics of the economy. Lecture notes.– Kharkov: Publishing House INZHEEK, 2004.(Russian).

Improved umac algorithm with crypto-code mceliece's scheme

Serhii Yevseiev
Doctor of Technical Science, Senior Research
Department of Cyber Security and Information Technology
Simon Kuznets Kharkiv National University of Economics
ORCID: http://orcid.org/0000–0003–1647–6444

Alla Havrylova
Senior Lecturer
Department of Cyber Security and Information Technology
Simon Kuznets Kharkiv National University of Economics
ORCID: https://orcid.org/0000–0002–2015–8927

Abstract. *The article discusses the mathematical model of the mini-version of the UMAC hashing algorithm, using various cryptoalgorithms as a pseudo-random substrate when generating key data, presents the results of studies of the considered mini-versions. A new approach is proposed to ensure the cryptographic stability of this hashing algorithm based on Mac-Elis crypto-code constructions on modified elliptic codes. This approach will provide the required level of cryptographic security in post-quantum cryptography.*

Keywords: *Mac-Elis crypto-code, UMAC hashing algorithm, El-Gamal cryptosystems*

Introduction

The development of decentralized systems is closely related to the use of cryptographic data processing tools. As a rule, such systems use asymmetric algorithms on elliptic curves (El-Gamal cryptosystems, digital signature ECDSA), the SHA-2 algorithm (version SHA-256) is used as the hash functions. The main advantages of such systems in the digital economy are: anonymity of transfers, the minimum cost of making a profit, the minimum commission from transactions, security and reliability. However, in 2018, it was decentralized circulation and cryptocurrency storage systems that took the first place in the number of cyber-attacks. In addition, the increase in demand for this type of banking activity causes certain difficulties in the operation (computational capabilities) of such systems (increase in electronic clients of systems, improvement of verification protocols, appearance of smart contracts). All this requires a revision of the cryptoalgorithms used in decentralized systems, and first of all, hashing algorithms.

Material and method

To ensure the required levels of speed and security in the protocols of decentralized systems it is proposed to use the winning algorithm of the NESSIE

competition, based on universal hash algorithms. The features of such hashing algorithms are their theoretical predictability of the collision probability and the uniform distribution of the entire power of the algorithm profiles on the collision set [1]. Consider the main characteristics of this algorithm on the example of its mini-version, which allows conducting research on the entire set of hash codes. This approach is used by the scientists of the school Gorbenko I. D. to assess the strength of block-symmetric ciphers

Reduced model UMAC (mini-UMAC). UMAC message authentication code generation scheme uses several transformation layers in its structure, including a block symmetric cipher (AES cipher recommended for use) [1].

It was shown above that the scheme of forming UMAC codes consists of the following layers:

– three-level universal hashing for generating hash-codes $Y = Hash(K, M, Taglen)$;
– cryptographic transformations using a block symmetric cipher to form a pseudo-random substrate $Pad = PDF(K, Nonce, Taglen)$;
– $Tag = UMAC(K, M, Nonce, Taglen) = Y \oplus Pad$.

Consider each layer of the UMAC message authentication code generation scheme for scaling.

We construct a mini-version of the three-level universal hashing without changing the structure of algebraic transformations by simply reducing the dimension of the blocks and the processed data eight times.

The corresponding length of the hash code $Y_{\min i}$ of the reduced model of the first layer will be a multiple of 4 bits; we will form its value by combining (concatenating) four sequences $Y_{\min iL3_i}$

$$Y_{\min i} = Y_{\min iL3_1} \| Y_{\min iL3_2} \| Y_{\min iL3_3} \| Y_{\min iL3_4},$$

where $Y_{\min iL3_i}$ – is the result of multi-level hashing of the message of the reduced model of the first layer mini-UMAC.

Consider the process of forming a single block $Y_{\min iL3_i}$ (we will not perform the second level of hashing in the reduced model):

$$Y_{\min iL3_i} = Y_{\min iL3} = Hash_{\min iL3}\left(K_{\min iL3_1}, K_{\min iL3_2}, Hash_{\min iL1}\left(K_{\min iL1}, M_{\min i}\right)\right),$$

where $K_{\min iL1}$, $K_{\min iL3_1}$, $K_{\min iL3_2}$ – are the mini-UMAC key sequences;

$Hash_{\min iL1}$ и $Hash_{\min iL3}$ – are reduced versions of the first and third levels hashing, respectively.

At the first level, a 32-bit string array $M_{\min i}$ is transformed by a function $NH(K_{L1}, M_i)$. This string is the result of first-level hashing $Y_{\min iL1} = NH_{\min i}(K_{\min iL1}, M_{\min i})$.

The value of the function $NH_{\min i}(K_{\min iL1}, M_{\min i})$ is calculated according to the following rule. The information block $M_{\min i}$ is divided into eight four-bit sub-blocks.

$$M_{\min i} = M_{\min i_1} \| M_{\min i_2} \| \ldots \| M_{\min i_8}.$$

Similarly, a key sequence K_{L1} is represented as a sequence of eight four-bit sub-blocks:

$$K_{\min iL1} = K_{\min iL1_1} \| K_{\min iL1_2} \| ... \| K_{\min iL1_8} .$$

After that (taking the initial state $Hash_{L1} = 0$) the following operations are performed:

$$Hash_{\min iL1} = Hash_{\min iL1} +_8 ((M_{\min i_0} +_4 K_{\min iL1_0}) \times_8 (M_{\min i_4} +_4 K_{\min iL1_4})),$$
$$Hash_{\min iL1} = Hash_{\min iL1} +_8 ((M_{\min i_1} +_4 K_{\min iL1_1}) \times_8 (M_{\min i_5} +_4 K_{\min iL1_5})),$$
$$Hash_{\min iL1} = Hash_{\min iL1} +_8 ((M_{\min i_2} +_4 K_{\min iL1_2}) \times_8 (M_{\min i_6} +_4 K_{\min iL1_6})),$$
$$Hash_{\min iL1} = Hash_{\min iL1} +_8 ((M_{\min i_3} +_4 K_{\min iL1_3}) \times_8 (M_{\min i_7} +_4 K_{\min iL1_7})),$$

where $+_8$, $+_4$ – addition operations modulo 28 and 24, respectively;

$\times_8$ – multiplication operation modulo 28.

As a result of calculations, an eight-bit value is formed $Y_{\min iL1} = Hash_{\min iL1}$.

The third level of hashing converts the eight-bit data $Y_{\min iL1}$ sent to its input into a hash code $Y_{\min iL3}$ of length 4 bits. The key sequences $K_{\min iL3_1}$ and $K_{\min iL3_2}$ are the lengths of 16 and 4 bits, respectively.

Hashable data $Hash_{\min iL1}$ and key sequence $K_{\min iL3_1}$ are evenly divided into four blocks, each of which is represented as an integer $Y_{\min iL2_i}$ and $K_{\min iL3_{1i}}$, $i = 1,2,...,4$.

The hash value $Y_{\min iL3}$ is calculated as follows:

$$Y_{\min iL3} = \left(\left(\left(\sum_{i=1}^{4} Y_{\min iL2_i} K_{\min iL3_{1i}} \right) \bmod(17) \right) \bmod(2^4) \right) xor(K_{\min iL3_2}),$$

where $(x)xor(y)$ – is the "exclusive OR" operation on the values x and y.

The mini-version of the final transform for generating the mini-UMAC message authentication codes consists of modulo 2 values $Y_{\min i}$ and $Pad_{\min i}$: $Tag_{\min i} = Y_{\min i} \oplus Pad_{\min i}$.

Thus, the scaling of the applied transformations on the respective layers of the formation of the message authentication codes makes it possible to construct a reduced model of UMAC, experimentally investigate the collision properties of the generated images (codes). The scaling factor in the development of the UMAC mini-model is chosen so that the length of the generated hash-codes Y, pseudo-random substrates Pad and message authentication codes $Tag = Y \oplus Pad$ is equal to the length of the mini-block block of the AES symmetric block cipher [2], i.e. 16 bits. The choice of such a scaling factor allows, on the one hand, preserving the algebraic structure of the basic transformations of the UMAC algorithm, including the AES algorithm included in its scheme, on the other hand, it makes it possible to conduct experimental studies using the methods of statistical testing of hypotheses and mathematical statistics, considering a limited set of elements Y, Pad and $Tag = Y \oplus Pad$ and the corresponding results for estimating the number of collisions as a sample from the general population.

Let us consider the method of statistical estimation of the collision properties of the formed elements (we denote them for simplicity $h(x)$), consider the basic conditions and limitations when conducting experiments.

Methods of statistical studies of collision properties

Experimental studies of the collision properties of UMAC message authentication codes will be carried out along the appropriate transformation layers:

1. At the first stage, collisional properties of the mini-version of universal hashing are investigated. To do this, it is necessary to confirm in the course of the experiment theoretical estimates of the number of collisions generated by the hash-codes $Y_{\min i}$;

2. At the second stage, collisional properties of pseudorandom substrates are investigated based $Pad_{\min i}$ on the analysis of the properties of the reduced Baby-Rijndael cipher model;

3. At the third stage, collisional properties of message authentication codes generated using mini-UMAC $Tag_{\min i} = Y_{\min i} \oplus Pad_{\min i}$ are investigated. This is the most important part of the research, since it will allow us to answer the question about preserving the properties of universal hashing after applying the layer of cryptographic information transformation.

Estimation of the number of collisions of the generated elements is carried out taking into account the collision properties of universal hashing, which allows to confirm the hypothesis about the preservation of collision properties of universal hashing at all stages of the formation of message authentication codes mini-UMAC.

The idea of universal hashing is to define such a set of elements of a finite set H of hash-functions $h: A \to B$, $|A| = a$, $|B| = b$, so that the random selection of a function $h \in H$ would provide a low collision probability, i.e. for any different inputs x_1 and x_2 the probability that $h(x_1) = h(x_2)$ (the probability of collision, collision) cannot exceed some predetermined value ε:

$$P_{кол} = P(h(x_1) = h(x_2)) \le \varepsilon,$$

moreover, the probability of a collision can be calculated as

$$P_{кол} = \frac{\delta_H(x_1, x_2)}{|H|},$$

where $\delta_H(x_1, x_2)$ – the number of such hash-functions in H for which the values $x_1, x_2 \in A$, $x_1 \uparrow x_2$ cause a collision, i.e. $h(x_1) = h(x_2)$.

We give two definitions of universal hashing [1].

1. Let $0 < \varepsilon < 1$. H is ε – a universal hash-class (abbreviated $\varepsilon - U(H, A, B)$,) if for two different elements $x_1, x_2 \in A$ there are no more than $|H| \cdot \varepsilon$ functions $f \in H$ such that $h(x_1) = h(x_2)$, if $\delta_H(x_1, x_2) \le \varepsilon |H|$ for all, $x_1, x_2 \in A$, $x_1 \uparrow x_2$.

2. Let $0 < \varepsilon < 1$. H is ε – a strictly universal hash-class (abbreviated $\varepsilon - SU(H, A, B)$), if the following conditions are true:

– for everyone $x_1 \in A$ and for everyone $y_1 \in B$, $\left|\{h \in H : h(x_1) = y_1\}\right| = |H| / |B|$;

– for everyone $x_1, x_2 \in A$, $x_1 \uparrow x_2$, and for everyone, $y_1, y_2 \in B$, $\left|\{h \in H : h(x_1) = y_1, h(x_2) = y_2\}\right| \le \varepsilon |H|$.

The definition of a universal class of hash-functions is equivalent to the definition of an authentication code generation algorithm, in which the number of different authentication code generation rules (number of keys) for which there is a collision (matching authentication codes) for two arbitrary input sequences is limited. The number of such keys cannot exceed the value $P_{кол} \cdot |H|$, where $P_{кол}$ – is the probability of a collision, $|H|$ – is the number of all rules (keys).

The definition of a strictly universal class of hash functions is equivalent to the definition of such an algorithm for the formation of authentication codes, in which the following rules will be executed:

1. The number of rules for the formation of the authentication code (the number of keys) for which the value of the authentication code does not change for an arbitrary input sequence is limited. The number of such keys cannot exceed the value $|H|/|B|$, where $|H|$ – is the number of all keys, $|B|$ – is the number of possible states of the authentication code;

2. The number of rules for the formation of an authentication code (the number of keys) for which the corresponding values of the authentication code for two arbitrary input sequences do not change is limited. The number of such keys cannot exceed the value $P_{кол}|H|$, where $P_{кол}$ – is the probability of a collision, $|H|$ – is the number of all keys.

The probability of collision of authentication codes in a scheme with strictly universal hashing is defined as $P_{кол} \le \varepsilon$.

The basis of the proposed method of statistical research of collision properties of the formed elements $h(x)$ is an empirical estimate of the maxima of the number of keys (hashing rules) for which:

1. For arbitrary $x_1, x_2 \in A$, $x_1 \uparrow x_2$ equality holds

$$h(x_1) = h(x_2). \tag{1}$$

2. For arbitrary $x_1 \in A$ and $y_1 \in B$ equality

$$h(x_1) = y_1. \tag{2}$$

3. For arbitrary $x_1, x_2 \in A$, $x_1 \uparrow x_2$ and $y_1, y_2 \in B$ equalities hold.

$$h(x_1) = y_1, h(x_2) = y_2. \tag{3}$$

The evaluation by the first criterion corresponds to the verification of the fulfillment of the condition for the universal class of hash functions, the evaluation by the second and third criterion – the conditions for the strictly universal class of hash-functions.

We introduce the following notation:

$$n_1(x_1, x_2) = \left|\{h \in H : h(x_1) = h(x_2)\}\right|,\ x_1, x_2 \in A,\ x_1 \uparrow x_2;$$

$$n_2(x_1, y_1) = \left|\{h \in H : h(x_1) = y_1\}\right|,\ x_1 \in A,\ y_1 \in B;$$

$$n_3(x_1, x_2, y_1, y_2) = \left|\{h \in H : h(x_1) = y_1, h(x_2) = y_2\}\right|,\ x_1, x_2 \in A,\ x_1 \uparrow x_2,\ y_1, y_2 \in B.$$

The first indicator $n_1(x_1, x_2)$ characterizes the number of hashing rules for which for given ones $x_1, x_2 \in A$, $x_1 \uparrow x_2$ equality (1) holds, i.e. the number of keys for which there is a collision (hash codes match) for two input sequences x_1 and x_2.

The second indicator $n_2(x_1, y_1)$ characterizes the number of hashing rules for which $x_1 \in A$, $y_1 \in B$ equality (2) is fulfilled for given ones, i.e. the number of keys for which the hash code value does not change for the input sequence.

The third indicator $n_3(x_1, x_2, y_1, y_2)$ characterizes the number of hashing rules for which $x_1, x_2 \in A$, $x_1 \uparrow x_2$, $y_1, y_2 \in B$ equality (3) is fulfilled for given, i.e. the number of keys for which the two input sequences x_1 and x_2 the corresponding hash code values y_1 and y_2 do not change.

Since the number of keys for which equalities (1), (2) and (3) can hold, should not exceed the corresponding values $P_{кол} \cdot |H|$, $|H|/|B|$ and $P_{кол}|H|/|B|$ we will estimate the maximum number of such keys for each of the considered set of elements.

Thus, the technique allows to evaluate the statistical characteristics of the maxima of these quantities, and then compare the results with the number $P_{кол} \cdot H$ (for the first criterion), with the number $|H|/|B|$ (for the second criterion) and the number $P_{кол} \cdot H$ (for the third criterion).

As statistical indicators for assessing the collision properties, which are carried out experimental studies are used:

- mathematical expectations $m(n_1)$, $m(n_2)$ and $m(n_3)$ the maximum number of hashing rules, under which equalities (1), (2) and (3) are satisfied, respectively;
- variances $D(n_1)$, $D(n_2)$ and $D(n_3)$, characterizing the dispersion of the values of the number of hashing rules for which equalities (1), (2) and (3) are satisfied, relative to their mathematical expectations $m(n_1)$, $m(n_2)$ and $m(n_3)$, respectively.

Evaluation of collision properties by the above criteria is carried out in the average sense. In other words, when setting up an experiment, a limited set of elements $x_1, x_2 \in A$, $x_1 \uparrow x_2$ and the corresponding hash-images $y_1, y_2 \in B$ are used, considering the corresponding results as a sample from the general population.

The natural estimate for the expectation m of a random variable X is the arithmetic average of its observed values X_i (or statistical average) [1]:

$$\tilde{m} = \frac{1}{N}\sum_{i=1}^{N} X_i ,$$

where N – the number of realizations of the random variable X.

The variance estimate of the random variable X is determined by the expression

$$\tilde{D} = \frac{1}{N-1}\sum_{i=1}^{N} (X_i - \tilde{m})^2 .$$

By virtue of the central limit theorem of probability theory, for large values of the number of realizations N, the arithmetic average will have a distribution close

to the normal law with the expectation $m[\tilde{m}] \approx \tilde{m}$ and standard deviation $\sigma[\tilde{m}] \approx \frac{\sigma}{\sqrt{N}}$, where σ – standard deviation of the estimated parameter.

In this case, the probability that the estimate deviates from its expected value by less than ε (by confidence probability) is equal to [1]:

$$P(|\tilde{m} - m| < \varepsilon) \approx 2\Phi\left(\frac{\varepsilon}{\sigma[\tilde{m}]}\right),$$

where $\Phi(x)$ – Laplace function, determined by the expression:

$$\Phi(x) = \frac{1}{\sqrt{2\pi}} \int_0^x e^{-\frac{t^2}{2}} dt \,. \tag{4}$$

Thus, when conducting experimental studies of collisional properties, methods of statistical testing of hypotheses and mathematical statistics are used.

1. From the general population of the random variable X, a sample is formed as follows:

– for the average statistical estimate of the expectation $m(n_1)$ and variance $D(n_1)$, the maximum at which the equality holds is used as a random variable $n_1(x_1, x_2)$ therefore, a sample of the volume $N: x_1,\ldots,x_n$ is formed by selecting N sets, each of which contains M pairs of elements $x_1, x_2 \in A$, $x_1 \uparrow x_2$ and evaluates $n_1(x_1, x_2)$ those, the total volume of the formed pairs of elements $x_1, x_2 \in A$, $x_1 \uparrow x_2$ will be $N \times M$;

– for the average estimate $m(n_2)$ and $D(n_2)$ the random variable is the maximum $n_2(x_1, y_1)$ at which equality holds $y_1 = h(x_1)$, therefore, the sample of the volume $N: x_1,\ldots,x_n$ is formed by selecting N sets, each of which contains M pairs of elements $x_1 \in A$, $y_1 \in B$ and is estimated $n_2(x_1, y_1)$. The total volume of the formed pairs of elements $x_1 \in A$, $y_1 \in B$ will be $N \times M$;

– for the average estimate $m(n_3)$ and $D(n_3)$ the random variable is the maximum $n_3(x_1, x_2, y_1, y_2)$ at which the equalities are fulfilled $y_1 = h(x_1)$ and $y_2 = h(x_2)$, therefore, the sample of the volume $N: x_1,\ldots,x_n$ is formed by selecting N sets, each of which contains M quadruple elements $x_1, x_2 \in A$, $x_1 \uparrow x_2$, $y_1, y_2 \in B$ and $n_3(x_1, x_2, y_1, y_2)$ is estimated, the total the volume of fours formed will be $N \times M$.

2. In experimental studies of collision hashing properties, the arithmetic average of the observed maximum values n_i and variance is estimated $\tilde{D}(n_i)$, $i = 1,2,3$.

3. The reliability of the average estimates obtained is justified as follows. The accuracy is fixed ε and the value of the Laplace function is calculated, which, in accordance with expression (4), gives the corresponding confidence probabilities:

$$P(|\tilde{m}(n_i) - m(n_i)| < \varepsilon) \approx 2\Phi\left(\frac{\varepsilon}{\sigma[\tilde{m}(n_i)]}\right), \; \sigma[\tilde{m}(n_i)] \approx \frac{\sqrt{\tilde{D}(n_i)}}{\sqrt{N}}.$$

In the reverse formulation of the problem, i.e. for a fixed confidence probability P_4 with a sample size of N, the confidence interval is defined as follows:

$$\tilde{m}(n_i) - t_\rho \cdot \sigma[\tilde{m}(n_i)] < m(n_i) < \tilde{m}(n_i) + t_\rho \cdot \sigma[\tilde{m}(n_i)], \tag{5}$$

where t_ρ – root of the equation $2\Phi(t_\rho) = P_\partial$.

Thus, the technique, using reduced models of individual transformation layers, on the basis of an estimate of the collision distribution of the images being formed, makes it possible to experimentally investigate the collision properties of message authentication codes.

Experimental results

Using the developed miniature UMAC model (mini-UMAC) and the method of statistical study of the collision properties of message authentication codes, we will experimentally estimate the distribution of the number of collisions (collisions) of the images being formed.

Since in the UMAC scheme discussed above, the first layer (during the formation of the hash-code $Y_{\min i}$) uses the family of universal hashing functions that were studied in detail in [1–7], we will conduct statistical studies only on the second layer (during the formation of a pseudo-random substrate $Pad_{\min i}$) and at the final stage of formation authentication codes (after performing the summation $Tag_{\min i} = Y_{\min i} \oplus Pad_{\min i}$). It is at these stages, according to our assumption, that the universality properties of the generated authentication codes are violated.

To form a miniature UMAC model (mini-UMAC), we use:

1-st layer:

Let us denote the procedure of encrypting a data block T of the length of a Blocklen-byte using the secret key K of the length of the Keylen-byte as a function $Enchiper(K,T)$. Then the procedure for the formation of a pseudo-random key sequence $K' = KDF(K, Index, Numbyte)$ can be represented as the following iterative (for all $n = 1,2,...,n$) transformations:

$$T_i = Index \| i,$$

$$K'_i = Enchiper(K,T),$$

$$K' = K'_1 \| K'_2 \| ... \| K'_n,$$

where $n = \left\lceil \frac{Numbyte}{Blocklen} \right\rceil$.

The generated sequence of pseudo-random key data bits K' has a length of Numbyte-bytes, a multiple of the length of the block Blocklen-bytes.

$$n = \left\lceil \frac{Numbyte}{Blocklen} \right\rceil = \frac{1024 + 16 \times 3}{32} = \frac{1072}{32} = 33{,}5 \approx 33 \Rightarrow i = 1,2,...,33, T_i = Index \| i$$

For the first layer $Index = 1, => T_i$:

T1 = 1 ||1 = 00000001

T2 = 1 ||2 = 0000000100000010

T3 = 1 ||3 = 0000000100000011

T18 = 1 ||18 = 0000000100010010

T19 = 1 ||19 = 0000000100010011

T20 = 1 ||20 = 0000000100010100

T4 = 1 ||4 = 0000000100000100
T5 = 1 ||5 = 0000000100000101
T6 = 1 ||6 = 0000000100000110
T7 = 1 ||7 = 0000000100000111
T8 = 1 ||8 = 0000000100001000
T9 = 1 ||9 = 0000000100001001
T10 = 1 ||10 = 0000000100001010
T11 = 1 ||11 = 0000000100001011
T12 = 1 ||12 = 0000000100001100
T13 = 1 ||13 = 0000000100001101
T14 = 1 ||14 = 0000000100001110
T15 = 1 ||15 = 0000000100001111
T16 = 1 ||16 = 0000000100010000
T17 = 1 ||17 = 0000000100010001
T21 = 1 ||21 = 0000000100010101
T22 = 1 ||22 = 000000010010110
T23 = 1 ||23 = 000000010010111
T24 = 1 ||24 = 000000010011000
T25 = 1 ||25 = 000000010011001
T26 = 1 ||26 = 000000010011010
T27 = 1 ||27 = 000000010011011
T28 = 1 ||28 = 000000010011100
T29 = 1 ||29 = 000000010011101
T30 = 1 ||30 = 000000010011110
T31 = 1 ||31 = 000000010011111
T32 = 1 ||32 = 0000000100100000
T33 = 1 ||33 = 0000000100100001

$$K' = K'_1 \| K'_2 \| ... \| K'_n$$

2-nd layer:

$$n = \left[\frac{Numbyte}{Blocklen} \right] = \frac{24 \times 4}{32} = \frac{96}{32} = 3 \Rightarrow i = 1,2,3,$$

$$T_i = Index \| i$$

For the second layer $Index$ =2, => T_i :

T1 = 2 ||1 = 0000001000000001 =>K1
T2 = 2 ||2 = 0000001000000010 =>K2
T3 = 2 ||3 = 0000001000000011 =>K3
KL2 = K1 || K2 || K3

3-rd layer:

$$n = \left[\frac{Numbyte}{Blocklen} \right] = \frac{64 \times 4}{32 \times 4} = 2 \Rightarrow i = 1,2$$

$$T_i = Index \| i$$

For the third layer $Index$ =3, => T_i :
T1 = 3 ||1 = 0000001000000001 =>K1
T2 = 3 ||2 = 0000001000000010 =>K2
KL3 = K1 || K2

When conducting statistical studies of the collision properties of the values formed $Pad_{\min i}$ and $Tag_{\min i}$ for each experiment, mathematical expectations $m(n_1)$, $m(n_2)$ and $m(n_3)$, variances $D(n_1)$, $D(n_2)$ and $D(n_3)$, as well as for fixed accuracy ε =0,1, the corresponding confidence probabilities were calculated $P(|\tilde{m}(n_i) - m(n_i)| < \varepsilon)$. Studies were conducted on the sample, the volume N = 100, for the formation of

each element of the sample was calculated by a maximum of a set of M = 1000 tuples of elements. Thus, the total volume of the formed sets was N × M = 105.

The results of experimental studies are summarized in Table 1.

When examining the collision properties of authentication codes generated using the mini version of the AES cipher, the number of keys for which equality $h(x_1) = h(x_2)$ is performed was zero for all tests, i.e. $n_1(x_1, x_2) = 0$ in all N = 100 experiments. This result is explained by the following property. The AES cipher (like its mini version) implements a bijective mapping of a set of plaintext into a set of cipher programs, i.e. for a fixed key, the generated cipher texts corresponding to different plaintext will be different. The experimental research conducted by the first criterion entered was precisely to count the number of keys in which there is a collision (collision) of two cipher texts corresponding to two different plaintext, which is impossible by definition of a bijective cipher. In this regard, the statistical data on the first criterion for the mini version of the AES cipher in the table 1 are not listed as non-informative.

Table 1. – The results of experimental studies of the collision properties of authentication codes generated using mini-AES and mini-UMAC, mini MASH-1, MASH-2 and mini-UMAC

	mini-AES, $Pad_{\min i}$	mini-UMAC, $Tag_{\min i}$	MASH-1	MASH-2
$\tilde{m}(n_1)$	–	4.23	41.42	0
$\tilde{D}(n_1)$	–	0.18	42.74	0
$P_4 = P(\lvert\tilde{m}(n_1) - m(n_1)\rvert < \varepsilon)$	–	0.98	0.98	≈ 1
$\tilde{m}(n_2)$	6.68	4.78	3.99	1
$\tilde{D}(n_2)$	0.42	0.42	0.01	0
$P_4 = P(\lvert\tilde{m}(n_2) - m(n_2)\rvert < \varepsilon)$	0.88	0.88	0.99	≈ 1
$\tilde{m}(n_3)$	0.19	5.31	0.26	0.31
$\tilde{D}(n_3)$	0.15	0.24	0.21	0.22
$P_4 = P(\lvert\tilde{m}(n_3) - m(n_3)\rvert < \varepsilon)$	0.99	0.96	0.97	0.97

The analysis of the data in Table 1 suggests that the results obtained are adequate and that they correspond to the statistical properties of the entire population of data. For fixed accuracy = 0,1, high confidence values were obtained, which indicates the validity and reliability of the experimental results obtained.

Let us analyze the results of statistical studies of the collision properties of message authentication codes, compare the obtained results of average estimates of mathematical expectations $m(n_1)$, $m(n_2)$ and $m(n_3)$ the number of hashing rules

for which equalities (1), (2) and (3) are satisfied, respectively, with theoretical estimates: number $P_{кол} \cdot |H|$ (for the first criteria), with a number $|H|/|B|$ (for the second criterion) and a number $P_{кол} \cdot H$ (for the third criterion).

Consider the first criterion by which we estimate the number of hashing rules for which there is a collision (coincidence of authentication codes) for two arbitrary input sequences. In accordance with theoretical estimates, this value is bounded above by a number $P_{кол} \cdot |H|$. Let us specify this (theoretical) estimate for authentication codes generated using mini-AES and mini-UMAC.

The power of the key set for mini-AES and mini-UMAC is $|H| = 2^{16}$, the power of the set of generated authentication codes is also $|B| = 2^{16}$. If we use the upper estimate of the probability of collisions as the inverse of the power of the generated authentication codes $P_{кол} = 2^{-16}$, we get $n_1(x_1, x_2) \le P_{кол} \cdot |H| = 1$. For the mini version of the AES cipher, this condition is met (justified by the bijectivity of the encryption transform), but the collisional properties of mini-UMAC are significantly inferior to this upper theoretical estimate. In fact, the number of collisions is more than four times higher than the theoretical limit and this position is confirmed with a high confidence level $P_4 = P(|\tilde{m}(n_1) - m(n_1)| < 0{,}1) > 0{,}98$.

Consider the second criterion by which the hashing rules are evaluated, for which for an arbitrary input sequence the value of the authentication code does not change. According to theoretical estimates, this value for authentication codes generated using mini-AES and mini-UMAC is bounded above by a number $|H|/|B| = 1$. The experimental results obtained indicate that the collisional properties of authentication codes generated using mini-AES and mini-UMAC do not satisfy the second criterion, the number of keys for which the value of the authentication code does not change several times the arbitrary input sequence exceeds the theoretical estimate for universal hashing.

In accordance with the third criterion, the number of hashing rules is estimated, for which, for two arbitrary input sequences, the corresponding values of the authentication code do not change. The theoretical estimate of this value for universal hashing is bounded above by a number $P_{кол} \cdot |H|$, which, using the upper estimate of the probability of collisions $P_{кол} = 2^{-16}$, gives $n_3(x_1, x_2, y_1, y_2) \le P_{кол} \cdot |H| = 1$. The values given in table 2 indicate that the collisional properties of authentication codes generated using mini-AES satisfy the third criterion. At the same time, the number of mini-UMAC keys, for which the corresponding authentication code values do not change for two arbitrary input sequences, is more than five times higher than the upper theoretical estimate.

Thus, to ensure the universality of the UMAC hash code, it is necessary to "replace" the substrate based on the block symmetric AES cipher with a crypto-resistant sequence, which ensures the crypto-resistance of the entire hashing system. In [3, 4], as a "replacement", it is proposed to use the MASH-1 and MASH-2 hashing algorithms, which provide the required level of cryptographic strength. Evaluation of cryptographic strength is given in (Table 2).

However, the results presented in table 1 show that the implementation of the key hashing scheme based on the MASH-1 algorithm, while changing the values of the initialization vector by the secret key, does not allow for high collision properties. The number of collisions that occur significantly higher than the upper theoretical boundaries, both in the first and second criteria, therefore, this design is not a universal and, especially, strictly universal hashing scheme.

Table 2. – Results of experimental studies of the statistical security of hashing algorithms using the NIST STS package

Generator	The number of tests where the test passed > 99%	The number of tests where the test passed > 96%
MASH-1	101 (53%)	188 (99%)
MASH-2	126 (67%)	189 (100%)
MASH(EC)	141 (74%)	189 (100%)
HMAC-SHA-256	134 (71%)	187 (98%)
EMAC	138 (73%)	189 (100%)
RIPEMD-160	129 (68%)	189 (100%)
UMAC+MASH-2	173 (91%)	189 (100%)

This result was obtained with a high confidence level for high accuracy. Thus, for the first criterion, the confidence interval was (confidence 0,98), for the second criterion (confidence 0,99), for the third (confidence 0,97). The considered key hashing scheme based on the MASH-1 algorithm, when the initialization vector values change with a secret key, satisfies only the third criterion.

Using key hashing based on the MASH-2 algorithm when changing the values of the initialization vector with a secret key, on the contrary, provides high collision characteristics of universal hashing. So, their use as a "substrate" significantly reduces the rate of conversion and the formation of a hash code. A promising direction is the use of crypto-code structures proposed in [5]. (Fig. 1) shows a block diagram of the hashing algorithm, taking into account the use, *Pad* as a substrate, of the Mac-Alice crypto-code construct on elliptic (EC) modified elliptical (shortened / extended) codes.

This approach ensures the preservation of the properties of the universal hashing algorithm, as well as the required level of security, efficiency and reliability in the formation of the hash code.

Conclusion

Thus, the results of statistical studies of the collision properties of hash codes based on mini-AES and mini-UMAC, as well as MASH-1 and MASH-2, allow us to state:

– the cryptographic layer of the formation of message authentication codes (mini-AES) satisfies the properties of universal hashing, the probability of a

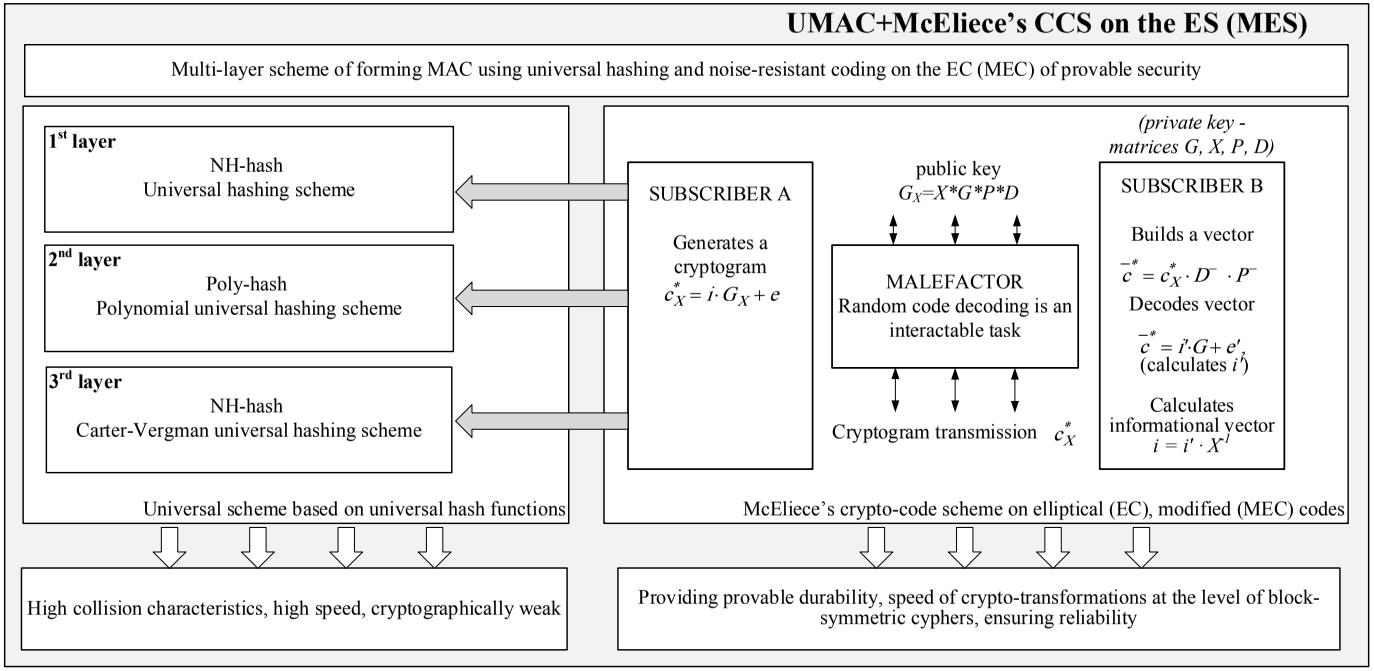


Figure 1 – The block diagram of the UMAC algorithm with Mc-Alice's KKK on the EC

collision of generated hash images does not exceed a predetermined value. However, this transformation layer does not satisfy the properties of strictly universal hashing;

– the result of the formation of message authentication codes using the mini-UMAC scheme does not satisfy the properties of both universal hashing and, especially, the properties of strictly universal hashing. This is explained by the fact that the scheme with simple sum modulo two (XOR) of two universal hash results does not always preserve the properties of universal hashing;
– the use of the MASH-1 algorithm as a hash-code does not satisfy the requirements for security and speed, the MASH-2 algorithm does not satisfy the speed of transformations, which does not allow their practical use in decentralized cryptocurrency systems.

The proposed application of the Mac-Alice crypto-code construct on elliptic (EC), modified elliptical (shortened / elongated) codes (MEC) retains the universality property on the first two layers of the UMAC algorithm, provides the required level of security, efficiency and reliability when generating the message hash. Thus, this algorithm allows increasing the levels of basic hashing functions in the blockchain technology in Bitcoin protocols under the conditions of using a full-scale quantum computer.

References:

1. Yevseiev S. P., Iohov O. Y. ta Korol O. H. Heshuvannia daniih v informaciyniih systemah. Monografia. – Kharkiv, Ukraiina: Vyd. KhNEU, 2013.
2. Yevseiev S., Ostapov S. ta Koroliov R. Vykorystannia mini-versiy dlia ocinky stiykosti blokovo-symetrychnyh shyfriv, Naukovo-tehnichnyi zurnal "Bezpeka informacii", – Tom 23. – № 2. – P. 100–108. 2017.
3. Parhuc L., Korol O., i Yevseiev S. Razrabotka modeli i metodaa kaskadnogo formirovaniya MAC s ispolzovaniiem modulyarniih preobraxovaniiy, Zahyst informacii: naukovo-tehnichnyi zurnal, – Tom 15. – № 3. – P. 186–196. 2013.
4. Yevseiev S., i Korol O. Metod kaskadnogo formirovaniia MAC-kodov na osnove modulyarnyh preobrazovaniy, Izvestiia Vysshiih tehnicheskih uchebniih zavedeniy Azerbaydzana, – № 1(89). – P. 71–78. 2014.
5. Yevseiev S., Korol O., and Kots H. Construction of hybrid security systems based on the crypto-code structures and flawed codes, Vostochno-yevropeyskiy zurnal peredovyh tehnologiy, 4/9(88). 2017. – P. 4–20.

New method for assessing the risk of automated information systems information security based on fuzzy-multiple approach

Olexander Shmatko
Doctor of Philosophy in Technical Science, Associate Professor
Department of Software Engineering and Management Information Technologies
National Technical University "Kharkiv Polytechnic Institute"
ORCID https://orcid.org/0000–0002–2426–900X

Natalya Romaschenko
Master Student
Department of Software Engineering and Management Information Technologies
National Technical University "Kharkiv Polytechnic Institute"
ORCID https://orcid.org/0000–0002–4500–4481

Abstract. *The subject of the study is the process of assessing the level of information security risk that is being implemented with the help of the fuzzy logic apparatus. The purpose of this work is to develop a methodology for assessing the degree of information security risk, which would avoid the uncertainty factor, that occurs when some parts of information about the analyzed automated information system are absent. The methodology is based on the use of fuzzy logic and fuzzy sets. Which implies the introduction of the term sets for each of the system characteristics and the linguistic assessment of the indicators. The tasks to be solved are to analyze existing information security risk assessment methodologies for identifying their strengths and weaknesses. On the basis of the conducted analysis, a new method for assessing the risk of automated information systems information security is proposed. The following results were obtained: the advantages and disadvantages of qualitative and quantitative methodologies for assessing the risk degree of automated systems information security were identified; the main stages of the proposed methodology were described; the degree of information security risk is calculated in comparison to the FAIR methodology. Conclusion: The methodology provides an opportunity to translate the obtained results of risk assessment from a mathematical language into a linguistic form that is more comprehensible to the decision-maker. This increases the effectiveness of the management of automated information systems protection mechanisms.*

Keywords: *information security, risk assessment, information security risk assessment methodology, fuzzy sets, linguistic form*

Introduction

The accession of humanity to the era of high-end technology has accelerated the development of Internet technologies and computing, which has encouraged the booming development of automated information systems (AIS), which are

gaining popularity. AIS is the information base of various services that deal with technical, economic and other tasks. Accordingly, existing threats have also been modified and acquired hybridity signs. Currently they combine the influence of all components of security: information security (InfoSec), cyber security (CyberSec), and security of information (SI). Threats have gained signs of hybridization. The main object of which is the economic sector of the country. There is a need for crosscutting (hybrid) technology to counteract the dangers that play a significant role in business processes. That is why, during the design and development of reliable AIS, it is necessary to provide a set of measures aimed at ensuring their protection against deliberate or accidental influences that may lead to a system failure. Among the security threats to the AIS, which directly affect the system, the personnel and its clients are internal and external threats, show synergy in crosscutting application with social engineering. Both the first and the second, depending on the target and nature of the influence on the activity of certain subjects and objects, can be divided into economic, physical and intellectual [1–3].

Providing information security is part of the information system management as a whole. In this case, one of the most important components of the InfoSec management system is the risk assessment, which is intended to determine the effectiveness of the applicable protection mechanisms based on the corresponding metrics. The remaining problem is to improve the existing methods for assessing InfoSec risk in connection with the emergence of new types of hazards. The task of improving the existing methods for assessing the security risk in the AIS remains currently topical due to the emergence of new types of hybrid cyber threats.

Analysis of Recent Studies and Publications

In the modern scientific community there is a significant number of researchers whose subject matter is to assess the risk of systems InfoSec. For example, [4] classifies existing risk analysis of IS, describes the sequence of risk analysis processes, compares software tools for SI risk management. Another example of research in this subject area is the work [5; 6], which describes the methods of assessment and risk management.

The article [7] proposes a mathematical formulation of risk using the SI main concepts of such risk management methodologies as MEHARI, EBIOS, CRAMM and SP 800–30 (NIST).

Basics for risk assessment, in particular in the context of assessing the risks of access control systems that decide on authorization, are presented in [8].

In the article [9] approaches and program solutions for assessing and controlling information risks as a fundamental organizational stage in the development of information security systems of computerized systems are considered.

In the article [10] an advanced methodology of information risk assessment in an automated system was proposed and analyzed. The necessary normative-legal documents of information security are mentioned. The performance of the prototype

expert system is considered, which allows to assess the level of information risk for a certain automated system and to determine the need for additional information security measures [11].

The article [12] analyzes the process of the most common models of information security risk assessment in information and telecommunication systems. The main approaches to information security risk assessment are revealed.

The analysis of threats to information security and a detailed description of the intended sources, classification and the reasons for their occurrence is given in [13].

Main materials of the study

After analyzing the existing scientific literature from the specified subject area, two main groups of methodology for assessing information security risks are possible to determine: quantitative and qualitative.

Table 1. – Advantages and disadvantages of qualitative and quantitative methodologies of InfoSec risk degree assessment

+/–	Quantitative	Qualitative
Advantages	– Risks are the financial consequences priority; – assets are the financial values priority; – obtaining simplified risk management results and investment returns into providing security; – results can be expressed in specific management terminology (for example, monetary value and probability is expressed as a certain percentage); – accuracy tends to increase over time as the business constantly records data.	– Provides clarity and understanding of risk classification; – the opportunity to reach consensus; – there is no need to determine the financial value of assets; – it is easier to involve people who are not experts in the field of computer security.
Disadvantages	– Importance influence attributed to risks on the basis of judgmental opinions of participants; – the process for achieving reliable results and consensus takes a lot of time; – calculation might be complex and time-consuming; – the results are presented only in monetary terms and they are difficult to interpret for “non-techies”; – the process requires special knowledge, so it is difficult to train staff.	– Insufficient distinction between among significant risks; – it is difficult to justify investments in control of implementation, because there are no grounds for the analysis of costs and benefits; – the results depend on the quality of the created risk management team

Quantitative methods use measurable, objective data to determine the value of assets, likelihood of loss and associated risks. The goal is to calculate the numerical values for each of the components collected during the risk assessment and analysis of costs and benefits [14].

Qualitative methods use a relative risk or asset value based on rating or categorization, such as low, medium, high, not important, important, very important, on a scale from 1 to 10. A qualitative model evaluates the actions and probabilities of identified risks at a rapid rate and in a cost-effective way. Risk sets are written and analyzed in a qualitative risk assessment, and can serve as a basis for a targeted quantitative assessment. Quantitative and qualitative information security risk assessment methods have both advantages and disadvantages (Table 1).

Accordingly, the combination of quantitative and qualitative methods represents a mixed set of advantages and disadvantages of the above mentioned methods. At present, hybrid types of risk assessment have the most practical interest.

The relation between methods of detecting attacks and risk assessment methods is presented in Figure 1.

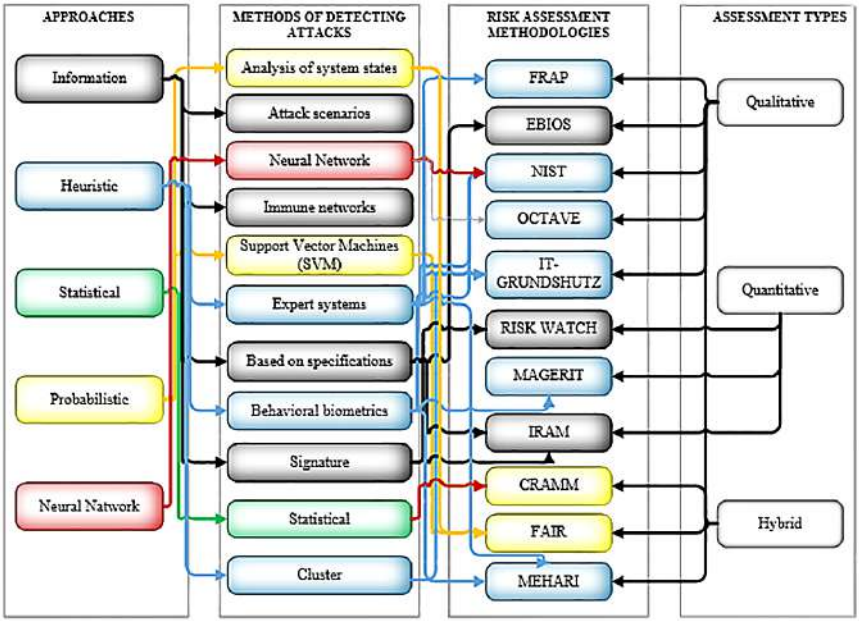


Figure 1. – The relation between methods of detecting attacks and risk assessment

Given the different nature of the threats to the profiles of the computer system, consider some of the methods of risk assessment [3]. The heuristic approach is implemented in the evaluation methods of NIST, IT-Grundshutz, OCTAVE, MEHARI and MAGERIT. Their common advantages include the flexibility – it allows

to conduct an analysis for organizations of different sizes; a detailed description and analysis of the information assets of the research object. In most cases, the above methods give the investigator a qualitative assessment. The disadvantages are the lack of automation of some functions and the human factor's impact on the end result.

CRAMM and FAIR methodologies refer to the probabilistic assessment approach. Their advantage is to provide a comprehensive risk assessment for InfoSec, a detailed description of existing risks and high efficiency of use. Also, the methodologies allow to evaluate the effectiveness of countermeasures. Disadvantages include the ability to work only with existing information assets.

The information approach is represented by the IRAM, EBIOS, and RISK WATCH methodologies.

The conducted analysis showed that the considered methodologies do not allow to conduct an assessment of functional efficiency, based on both technical and economic indicators. To obtain estimates of the risk level of equivalent cash capital and the immediate display of its security, it is proposed to use methodologies based on an integrated approach to risk assessment that combines quantitative and qualitative methods of analysis, including CRAMM and FAIR methodologies, structural schemes are presented in the Figure 2, 3 respectively[14].

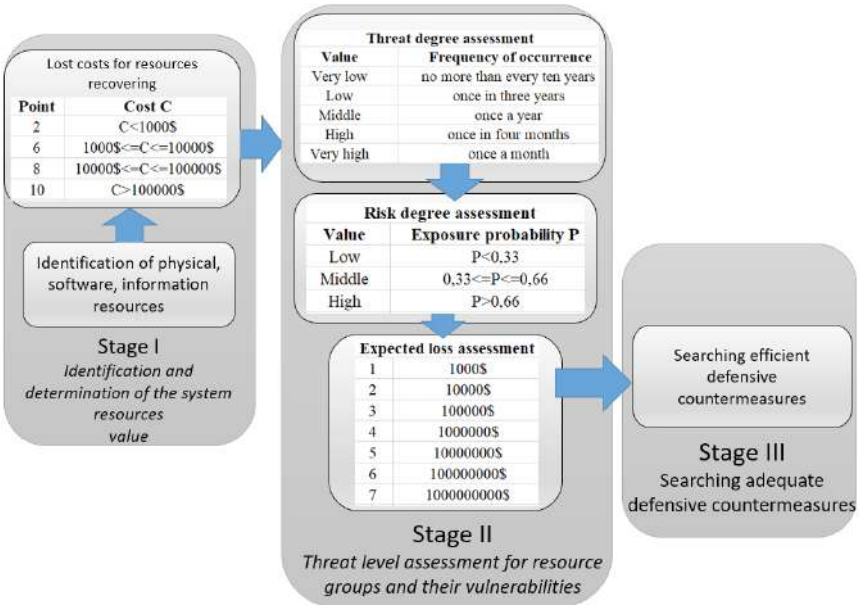


Figure 2. – CRAMM Methodology – crosscutting approach to risk assessment

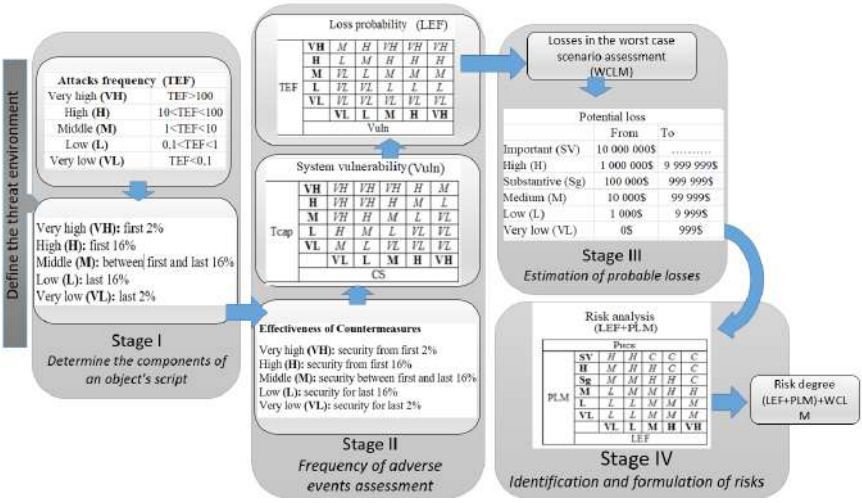


Figure 3. – FAIR risk assessment methodology

The methodologies of the crosscutting approach to risk assessment, as a rule, use the following stages (steps) [15; 16]:

At the first stage, everything is analyzed regarding the identification and determination of the value of system resources: the definition of the boundaries of the system under investigation: information about the configuration of the system, information about responsible individuals for physical and software resources, determining the number of users of the system, their privileges. Identification of physical, software and informational resources within the boundaries of the system is carried out. A model of the information system is being built from the standpoint of the InfoSec.

The second stage identifies threats and assesses the level of threats to resource groups and their vulnerabilities, assesses the dependence of user-defined services on specific resource groups and the existing level of threats and vulnerabilities, calculates risk levels and analyzes the results. At the end of the stage, the customer receives identified and assessed levels of risk to his system.

The third stage of the study is to find adequate countermeasures – the search for a security solution that best suits the requirements of the customer. At this stage, it generates several variants of countermeasures that are adequate to the identified risks and their levels.

The combination of two qualitative and quantitative approaches will combine the benefits of each of them, provided by them separately, and will open the possibility of obtaining the necessary characteristics for the effective organization of security systems.

Despite the high efficiency of the above-mentioned methodologies, they still have a significant common flaw – they require a significant amount of resources to assess

the risk of InfoSec, that is, it is necessary to process a large volume of information that takes a lot of time and effort. There is a need to improve the existing methods for assessing the risk of InfoSec, which would simplify the estimation process and would allow to gain the end results in a linguistic form that is comprehensible to the decision maker. Accordingly, the purpose of the article is to develop a risk assessment methodology for InfoSec based on a fuzzy-multiple approach.

Proposed method

Security risks of information systems are very closely related to uncertainty. Two cases of uncertainty can be determined: identification of the current and future state of the systems.

When solving tasks related to security risk assessment, the question about the qualitative interpretation of certain levels of parameters often arises. The linguistic assessment of the security level is clearer and best describes the state of IT infrastructure security, which in turn encourages the manager to take one or another decision.

In order to fulfill the linguistic assessment, two things are required:

First, you need to define a linguistic scale for evaluation. Most often pentascale is used (five-level classifier) "Very low (VL) – Low (L) – Average (A) – High (H) – Very high (VH)".

Secondly, it is necessary to collect all available information to define linguistic assessment: quantitative data collected in a group of similar objects of observation.

For example, for a qualitative assessment of the level of information security, it is necessary to collect statistical information on similar information systems for a relatively short period of monitoring. This is necessary to maintain the condition of statistical homogeneity. At the same time, it is necessary to take into account the laws that are inherent to the objects of information security.

It should be noted that there are no general universal rules for accurate and rapid assessment of AIS information security. A set of problems may also arise with the collection of initial data for linguistic analysis.

There is a question connected to the additional data analysis, which is related to different time segments of observations. There may be a question about replacing the missing data in one-time period with the data from another similar one, and the parameters of this law will be given according to special rules in order to satisfy the necessary authenticity of the identification of the monitoring law.

The presence of quasistatistics makes it possible to make qualitative conclusions about the behavior of a particular parameter of the investigated IS, makes it possible to conduct a linguistic analysis of input data.

Basic steps of the linguistic classification:

1. The studies of the source data set and its verification as a quasi-statistic are conducted. There is evidence that some data distribution law is hidden in these data, for example, the "gray" Pospelov scale.

2. Next, define the main nodes. In the absence of expert evaluation, nodal points can be determined by the simple rule: node point – left end of media interval, nodal

point – right end of media interval, middle point – corresponds to the maximum histogram or median histogram.

3. The interval between the two nodal points standing next is divided into three zones, the middle one is the zone of expert uncertainty in the classification. Thus, the primary linguistic interpretation of the histogram is complete.

After the classificatory definition it is possible to make a correction of pestascale. To do this, you can modify nodal classification points, bringing them closer together and narrowing the uncertainty zone. You can also replace the nodal point with an absolute confidence interval and try to expand it on both sides of the nodal point. All clarifications must be made on the basis of an agreed expert evaluation.

Apply the proposed methodology to compare its effectiveness with the FAIR method. The initial data for the calculation are taken from [14].

Stage 1. In the first stage, term sets are introduced to describe the basic sets of the IS state and the subset of states, described in the natural language:

The complete set of information security status assessment E of IS is broken down into five subsets of the form:

E_1 – subset of states "extremely unsuccessful state of IS InfoSec";

E_2 – subset of states "unsuccessful state of IS InfoSec";

E_3 – subset of states of "average quality of the IS InfoSec state";

E_4 – subset of states "relatively safe state of IS InfoSec";

E_5 – subset of states "the maximum safe state of the IS InfoSec".

The corresponding set E of a full risk set of IS InfoSec threats G is divided into 5 subsets:

G_1 – subset of "marginal threat risk of InfoSec";

G_2 – subset of "high threat risk to InfoSec";

G_3 – subset of "average threat risk to InfoSec";

G_4 – subset of "low threat risk to InfoSec";

G_5 – subset of " insignificant risk threat to InfoSec".

Assume that G takes the value from zero to one by definition.

For an arbitrary separate indicator of the InfoSec assessment X_i, the complete set of its values of B_i is divided into five subsets:

B_{i1} – subset "very low level of indicator X_i ";

B_{i2} – subset of "low level of indicator X_i ";

B_{i3} – subset of "average level of indicator X_i ";

B_{i4} – subset of "high level of indicator X_i ";

B_{i5} – subset of "very high level of indicator X_i ".

An additional condition for matching the sets B, E and G of the following form is performed: if all the indicators in the analysis have, according to the classification, the level of the subset B_{ij}, then the state of the InfoSec is qualified as E_j, and the degree of InfoSec threat risk is qualified as G_j. Fulfilment of this condition affects the correct quantitative classification of the levels of indicators and the correct determination of the level of significance of the indicator in the evaluation system.

Stage 2. Construct a set of indicators $X = \{X_i\}$ in the number $N = 4$, which, according to expert-analyst, on the one hand, affect the assessment InfoSec threat risk, and, on the other hand, evaluate the different sides of IS InfoSec (Table 2).

Table 2. – A set of indicators X

Characteristic	Current value
X_1	1.2
X_2	0.7
X_3	0.025
X_4	0.004

Stage 3. Summarize to each indicator the level of its significance for the analysis of r_i. To estimate this level, you need to position all the values in descending order of magnitude so that the rule is complied with:

$$r_1 \geq r_2 \geq ... \geq r_n \quad (1)$$

If the system of indicators is put in descending order of their significance, then the significance of the i-th index should be determined by the Fishburn's rule [17]:

$$r_i = \frac{1}{N} = \frac{1}{4} = 0.25 \quad (2)$$

The Fishburn's Rule reflects the fact that nothing is known about the level of significance of the indicators (1). Then the estimate (2) corresponds to the maximum entropy of the existing information uncertainty about the object of the study.

Stage 4. Construct a classification of the current value g of the risk factor G as a criterion for dividing this set into a subset (Table 3):

Table 3. – Value of indicator g

Interval G	Set names
$0.8 < g < 1$	G_1 – subset of "marginal threat risk to InfoSec";
$0.6 < g < 0.8$	G_2 – subset of "high threat risk to InfoSec";
$0.4 < g < 0.6$	G_3 – subset of "average threat risk to InfoSec";
$0.2 < g < 0.4$	G_4 – subset of "low threat risk to InfoSec";
$0 < g < 0.2$	G_5 – subset of " insignificant risk threat to InfoSec".

Stage 5. Construct a classification of the current values x of the X indicators as a criterion for breaking up the complete set of their values into a subset of type B (Table 4):

Table 4. – Value Subset Partition

Indicator name	Criteria of subset partition				
	B_{i1}	B_{i2}	B_{i3}	B_{i4}	B_{i5}
X_1	x_1 <0.02	0.02< x_1 <0.16	0.16< x_1 <0.84	0.84< x_1 <1	1< x_1
X_2	x_2 <0.02	0.02< x_2 <0.16	0.16< x_2 <0.84	0.84< x_2 <1	1< x_2
X_3	x_3 <0.02	0.02< x_3 <0.16	0.16< x_3 <0.84	0.84< x_3 <1	1< x_3
X_4	x_4 <0.02	0.02< x_4 <0.16	0.16< x_4 <0.84	0.84< x_4 <1	1< x_4

Stage 6. Evaluate the current level of indicators and reduce the results (Table 5):

Table 5. – Indicator's Level Evaluation

Indicator name	Current value
Very high (VH)	X_1 >1
High (H)	0.1< X_2 <1
Medium (M)	0.01< X_3 <0.1
Low (L)	0.001< X_4 <0.01
Very low (VL)	<0.001

Stage 7. Classify the current values of x according to the criterion of Table 4. The result of the classification is (Table 6).

$\lambda_{ij} = 1$, if, and $\lambda_{ij} = 0$, when the value does not fall into the selected range of classification.

Table 6. – Classification Result

Indicator name	Significance	The result of classification by subsets				
		B_{i1}	B_{i2}	B_{i3}	B_{i4}	B_{i5}
X_1	0.25	0	0	0	0	1
X_2	0.25	0	0	1	0	0
X_3	0.25	0	1	0	0	0
X_4	0.25	1	0	0	0	0

Stage 8. Carry out arithmetical steps to assess the degree of bankruptcy risk of g:

$$G = \sum_{j=1}^{5} g_i \sum_{i=1}^{N} r_i \lambda_{ij}$$

where: $g_i = 0.9 - 0.2(j-1)$

The value of G corresponds to subset of "average threat risk to InfoSec".

$G = 0.25 \cdot 0.1 + 0.25 \cdot 0.3 + 0.25 \cdot 0.5 + 0.25 \cdot 0.9 = 0.45$

The obtained result of the InfoSec risk degree corresponds to the research result in [14].

Conclusions

Information is one of the most important resources in modern ISs, therefore, it is necessary to estimate the risk degree of asset exposure to anomalies and attacks. Existing methods for InfoSec risk assessment such as FAIR, MAGERIT, NIST, CRAMM are often used for this purpose. In this case, the above methodologies do not take into account the fact that IS security risks are closely related to the uncertainty that needs to be addressed. The proposed methodology of risk assessment of the InfoSec can solve this problem – it overcomes the uncertainty and allows the researcher to assess the risk degree in a linguistic form. The calculations of the system information security level in comparison to the calculations using the FAIR methodology are given in the work. It is possible to state that the proposed methodology does not yield to its efficiency. Indeed, under the same input conditions, identical values of the indicators in the linguistic form of evaluation were obtained. In the case of using the methodology, the researcher gets the opportunity to formulate conclusions about the level of the system security, and to develop recommendations for the implementation of the necessary security mechanisms.

References:

1. Judin O. K. Information security. Regulatory support. – Kyiv : NAU. 2011.
2. Lenkov S. V., Peregudov D. A. & Horoshko V. A. Methods and means of information protection. – Kyiv: Arij. 2008.
3. Jevsejev S. P. Methodology for building security systems for banking information resources. UDC004.056:336.71. 2018.
4. Baranova E. K. Information security risk analysis and assessment techniques. Educational resources and technologies, 1(9), 2015.– P. 73–79.
5. Anikina I. V., Emaletdinova L. Ju. & Kirpichnikova A. P. Methods for assessing and managing information security risks in corporate information networks. Bulletin of the University of Technology, 18(6), 2015. – P. 195–197.
6. Puzyrenko O. G., Ivko S. O. & Lavrut O. O. Analysis of the process of information security risk management in providing information and telecommunication systems. Systems of information processing, 8(124), 2014. – P. 128–134.
7. Ghazouani M., Faris S., Medromi H. & Sayouti A. Information security risk assessment – a practical approach with a mathematical formulation of risk. International Journal of Computer Application, 103(8), 2014.– P. 36–42.
8. Khambhammettu H., Logrippo L., Boulares S & Adi K. A Framework for Risk Assessment in Access Control Systems. Computers & Security, 2013. – 38 p.
9. Chunarova A. V., Parhomenko I. I. & Sashhuk I. I. Analysis of approaches and software solutions for the assessment and control of information risks in the computerized. Bulletin of the Engineering Academy of Ukraine, 2. 2014.– P. 138–142.

10. Buchyk S. S. Methodology for assessing information risks in an automated system. Knowledge-based technologies, 3 (35), 2017. – 224 p.
11. Buchyk S. S. & Shalaev V. A. Analysis of instrumental methods for determining information security risk information and telecommunication systems. Knowledge-based technologies, 3(35), 2017. – P. 215–225.
12. Puzyrenko O. G., Ivko S. O., Lavrut O. O. & Klymovych O. K. Application of information security risk assessment models in information and telecommunication systems. Systems of information processing, 3(128), 2015. – P. 75–79.
13. Gonchar S. Analysis of probability of realization of threats of information protection in automated control systems of technological process. Information protection, 16(1), 2014. – P. 40–46.
14. Korol' O. G. Estimation of the quality of global network services based on Ethernet technologies using a complex indicator. Systems of information processing, 2(148), 2017. – P. 100–110.
15. Kuznecov O. O., Evseev S. P. & Kavun S. V. Information protection and economic security of the enterprise. – Kharkiv: HNEU. 2008. – 360 p.
16. Smirnov O. A., Evseev S. P., Zhukarev, V. Ju., Korol' O. G., Sorokin V. Je. & Meleshko Je. V. D. Technologies and standards of computer networks. – Donetsk: DonIZT, 2012. – 453 p.
17. Cirlov V. L. Basics of Information Security. – Rostov n/D: Feniks 2008.

Security analysis of LTE technology

Oleh Harasymchuk
Doctor of Technical Science, Associate Professor
Department of Information Security
Lviv Polytechnic National University
ORCID: https://orcid.org/0000–0002–8742–8872

Ivan Opirskyy
Doctor of Technical Science, Associate Professor
Department of Information Security
Lviv Polytechnic National University
ORCID: https://orcid.org/0000–0002–8461–8996

Abstract. *In the course of carrying out this work, the research of the fourth generation network (LTE) security issues was conducted. The research was carried out in the context of both the network itself and the user equipment. Besides, the security was considered as the both low-level (physical channels) and the high-level (security standards, defined by the 3GPP consortium). In case of the high-level security, the responsibility for the infringement of the standards lies on the network operator. In the case of low-level – both on the network operator and on the manufacturers of mobile terminals and USIM modules.*

Keywords: *LTE, Mobile network, base station, network node, network vulnerability, authentication, security, threats*

Introduction

The condition of communication development mainly determines economic level of any country. The development of mobile communication need huge investment in country economic, increasing integration level of international collaboration, development of small, medium-sized businesses and infrastructure of general use communication. The trend, when the transition of data plays the main role, demonstrates itself more and more clearly in global communication industry development. Nowadays people get used to fast speed Internet and it's becoming the same necessity in common life, as fixed was before.To provide the proper level of service, subscriber must be sure that the communication will be available anytime and everywhere. To achieve this goal, efforts are aimed to construct 4G network with usage of LTE (Long Term Evolution) that mostly meets the requirements of the fourth generation mobile technologies. Modern mobile communication devices combine functions of cellphones and PC that allows to use it not only for communication but also for working with different multimedia information, data transmission via the network etc. During the period of intensive technology development and expansion, when the mobile communication became the part of daily life, the issue of digital information security is extremely relevant. The security of

data transmission by exposed channel, that is radio broadcast, is one of the modern mobile networks current issues.

System of the the fourth generation mobile technologies (LTE)

One of the technologies that's designed for solving vital problems of modern telecommunications is the Long Term Evolution (long-term evolution) technology, or, briefly, LTE technology. According to this, the mobile communications networks, based on such technology, that's called LTE-networks. High speed means a completely different level of convenience for the subscriber. Therefore, the first significant advantage of LTE is the improved user experience while using apps that require high data transmission speed. For example, during watching online video, mobile gaming or using virtual reality online apps.The LTE network consists of the two most important components: the radio-access network E-UTRAN (Evolved Universal Terrestrial Radio Access Network) and the base network SAE (System Architecture Evolution) or EPC (Evolved Packet Core Network) core network. Simplified [1] network architecture is depicted in Fig. 1. SAE – System Architecture Evolution – network core architecture, developed by the 3GPP consortium for the LTE wireless standard. SAE is an evolutionary follow-up of the GPRS network core.

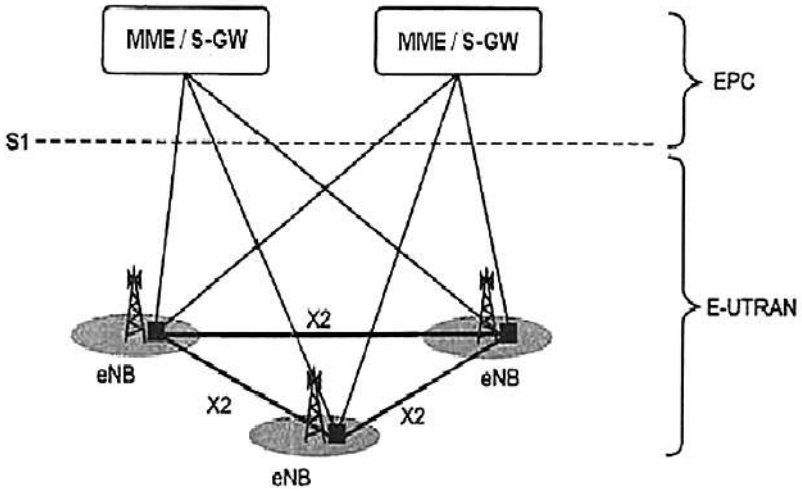


Figure 1. – Simplified network architecture

Data transmission in the EPC network happens only by IP-protocol with packets switching, that's essentially different from LTE from previous generations that used channels commutation between individual elements. This network includes elements that're responsible for management, routing, communication and storage of various data, which will be told more. The E-UTRAN network, that consists of base stations

(eNodeB), assumes functions of radio interface and it is connecting-link between the terminals (UEs) and the EPC network. The main feature that differentiates the LTE network from the networks of other generations, is that the base eNodeB stations, which can transmit information among itself using X2 protocol and assumes management functions. Unlike the GSM standard, where the subsystem of base BSS stations consists of the base BTS receiver and the BSC base station controller, in the LTE network the functions of the transmitter and the controller are combined in one eNodeB element (Fig. 2).

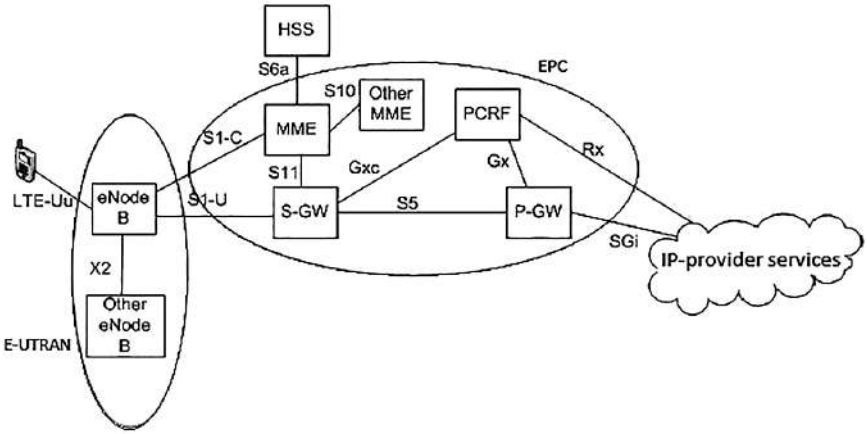


Figure 2. – LTE network architecture

There are two types of traffic in the LTE network: data transmission for user (UP – User Plane) and signal information transmission (CP – Control Plane).

Functions of the main network elements. The base station (BS) (EnodeB) in the LTE network performs the following functions:

- measuring and preparation of relevant reports for managing mobility and dispatching;
- routing in user-defined data-packets plane to the servicing gateway S-GW (Serving Gateway – network gateway, that's responsible for the transmission data for user);
- dispatching and transmitting the calling and speech information received from the Mobility Management Entity MME (the EPS subsystem that manages mobile terminals);
- selecting a Mobility Management Entity (MME) during connection to the network destined for terminal user in the absence of information about the previous connection;
- dispatching and transmission PWS messages (Public Warning System), received from the Mobility Management Entity (MME);

– Radio Resource Management (RRM): distribution of radio channels, dynamic distribution of resources in growing and decreasing directions – so-called dispatching of resources;
– compressing IP packet headers, user plane ciphering.

MME (Mobility Management Entity):

This is the main control element in the LTE network. It only performs the functions of control and does not work with the same data. It has a direct connection to the UE through the signaling protocol out-off NAS access level (Non-access Stratum – the functional stratum of stack the LTE, between ME and the core of the network).

MME performs the following functions:

selecting P-GW and S-GW;

– selecting SGSN (Serving GPRS Support Node – the main component of the GPRS system for the implementation of all packet information processing functions) in case of handover in network of 2G or 3G roaming;
– signaling between EPC and UE;
– signaling in the case of a transition of the mobile terminal between different networks (handover);
– lawful interception of the signalization;
– authentication: during registering the UE in the MME network, it compares its permanent registration number with the number contained in the HSS database (Home Subscriber Server – EPS subsystem that stores information about network users) to verify its identity;
– managing of the channels on the interfaces to other network elements.

S-GW (Serving Gateway):

Designed for processing and routing packet data that's coming from / to the subsystem of the base stations. S-GW routes and directs packets with the same data while acting as a mobility anchor for user data during handover inter the base stations (eNodeB), as well as a mobility management node between the LTE network and the networks with other 3GPP technologies. When UE is free and not engaged, S-GW connects DownLink (DL) and performs UE notification (paging) if necessary to transmission data via DL to the UE. It also provides a copy of the data destined for user within a lawful interception.

S-GW is responsible for the following functions:

– buffering downlink data packets for the UE that's in standby mode and initializing the service request procedure;
– selecting the point of binding ("anchor") Local Mobility Anchor during handover;
– lawful interception of user information;
– routing and redirection of data packets;
– sending various events to PCRF (start of connection, connection ending);
– formation of user accounts and identifier the class of quality for tariffication;
– tariffication of subscribers.

P-GW (Packet Data Network Gateway):

The packet gateway provides a connectivity from the UE to external packet data networks by being the point of exit and entry of traffic for the UE. The UE may have a connection to more than one P-GW for connection to multiple networks. P-GW performs the functions of security, filtering of packets for each user, billing support, lawful interception and packet sorting. Another key role of P-GW is to act like the mobility management node between 3GPP and non-3GPP technologies, such as WiMAX and 3GPP2 (CDMA 1X and EvDO). P-GW provides the following functions:

– marking of transport level packets in the downlink direction;
– distribution IP address for UE;
– lawful interception of user information;
– filtering user's packages;
– tariffication of services, their selection.

PCRF (Policy and Charging Rules Function):

Policy Function can also be divided into 2 functions: gating control and quality control. The control of the gateway is meant timely and error-free determination of such events as the beginning of provision, changing of settings, the end of provision of the service, etc. Quality management includes permanent monitoring and maintenance the quality of service characteristics that are set by subscriber parameters (QoS), besides not only for voice connections, but also for packet sessions. Charging Function (charging fee management) necessarily involves online tariffication, that is, the subscriber and the providers can track the status of the account in real time.

HSS (Home Subscriber Server):

HSS is a large database and is designed for storage of subscriber data. HSS also generates the data needed to perform encryption, authentication etc. HSS intended to store the following information:

– Users identifiers, numbers and address information;
– Users security data: information for access control to the network, authentication and authorization;
– Information about the location of the subscriber at the inter-network level, that is, if even the subscriber leaves the current LTE provider's network, the information about which network he has gone to for search of him in case of an incoming call will be saved in HSS;
– Information about the subscriber's profile;
– User identifiers, numbers and address information.

The LTE network may include one or more HSS. The number of HSS depends on the geographical structure of the network and the number of subscribers.

EPS safety architecture

It is worth noting that the transmission of data in wireless networks has certain disadvantages compared with wired networks, namely:

– openness of the wireless environment: when data is transmission via the airspace, there is no physical barrier preventing it from accessing;
– Limited capacity: although the capacity of the wireless network is increasing, it can not compete with wired technologies;
– complexity of the system: wireless systems more complex because of using mobility and the ability to use the channel effectively;
– Limited computing power: processors installed on wireless devices are not powerful enough to perform intensive processing of information;
– Relatively unreliable connection with the network: during the signal transmission over the radio channel, there are more obstacles than wired ones has.

These restrictions significantly affect the creation of security facilities to provide key information security factors: accessibility, integrity and confidentiality. Before developing the data security facilities for mobile network it worth to discover the threats that my happen.

Information threats in mobile networks may have the following preconditions:
– quantitative insufficiency – a physical lack of one or more elements of the system that cause the failure;
– qualitative insufficiency – imperfection the organization of the system, causing the accidental or deliberate possibility of negative action;
– activity of intelligence agencies – specially organized activities of specific organs professionally oriented on obtaining the necessary information;
– economic intelligence – the secret activity of the organization for the extraction of information that is specially protected from unauthorized leakage or theft, and for creating favorable conditions for itself in order to obtain maximum benefits (unfair competition);
– malicious actions of criminal elements – theft of information or computer programs for the purpose of profit or destruction;
– unconscionable acts of the environment – theft (copying) or destruction of information arrays or programs for certain mercenary motives, and owing to non-observance of set rules of work.

The basic principles of verifying users' authenticity and encryption for mobile networks were formulated during the development of GSM networks. Later, they helped to reduce security problems in earlier wireless telecommunication systems and contributed to the successful commercial distribution of GSM networks around the world. The next-generation UMTS network architecture has retained the good security features that were used in GSM and introduced new ones that include:
– open consideration and discussion of encryption and authentication algorithms;
– inclusion in the specification of the set of algorithms MILENAGE, as an example of algorithms that can be used by providers who are not able to develop their own;

– use 128-bit encryption key (unlike 64-bit used in previous generation networks);
– mutual procedure for authentication and verifying integrity of data between devices in the network.

Overview and relevant specifications

The features and security mechanisms that are part of the GSM and 3G architectures are mostly based and developed according to fairly general principles to be used in a different environment. But the security architectures in GSM and 3G, have mechanisms that are significantly tied to these systems; the security functions have been embedded in the architecture of GSM and 3G to ensure their optimal and efficient work.

The design of the EPS security system follows the same principles of maximizing, in relation of system, merging the security features and the other functions.

The EPS should also be able to interact with the previous systems, so that the adaptation of the mechanisms should be done according to compatibility providing. In addition to adapting the already existing functionality from previous systems, many new extensions and improvements were added with the introduction of the EPS architecture.

The basic properties of EPS architecture security architecture will be presented below (Fig. 3).

After the mobile station (UE / ME) has been identified, the Mobility Management Entity (MME) in the service network request authentication data from the home network. Next, MME initializes the authentication protocol and key agreement with the mobile station. After successful completion of this protocol, MME and the mobile station share the common secret key KASME, where the ASME abbreviation – Access Security Management Entity. In EPS, the role of the security management essence takes the MME. Now MME and UE are able to get other keys from KASME. Two keys are used to protect the confidentiality and integrity of signal traffic between MME and UE. In (Fig. 3). It is labeled as "NAS Protection".

Another key is sent to the base station (eNB). Three more keys are successively received at the base station and mobile station. Two of them are used to protect the privacy and integrity of signal traffic between eNB and UE – "AS protection" on (Fig. 3). The third key is used to protect the confidentiality and integrity of user data between eNB and UE – "AS Protection" in (Fig. 3). In addition to the protection of signal traffic and of user designed data between the terminal and the base station, there is also the protection of the confidentiality and integrity of data between the base station and the core of the network (EPC). Signal traffic is transmitted between the UE and the MME via the interface S1-MME, while the user designed data is transmitted between the UE and the servicing gateway (S-GW) via the interface S1-U. Cryptographic protection used on S1 interfaces – IPsec. IPsec is also used on X2 interfaces between base stations.

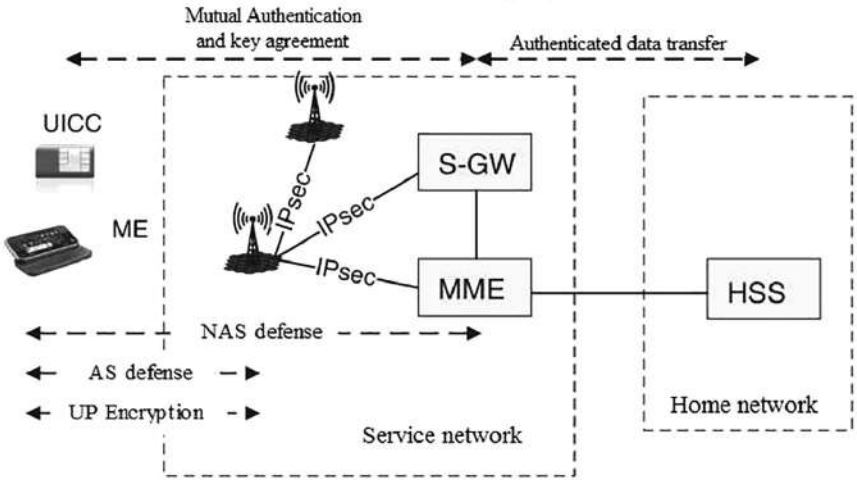


Figure 3. – EPS Architecture

Consider how the mechanisms for provision the confidentiality and integrity of the data are embedded in the EPS stack. On (Fig. 4) Signal traffic protocols are shown. On (Fig. 5) the data protection scheme is shown.

Privacy protection can optionally be integrated into the Packet Data Convergence Protocol (PDCP) – protocol for both signal traffic and user destined data, in the LTE protocol stack. Integrity protection does not apply to protect user destined data between the UE and the base station. For the X2 and S1 interfaces, cryptographic protection is used in the same way as for the corresponding control planes interfaces – using the IPsec protocol.

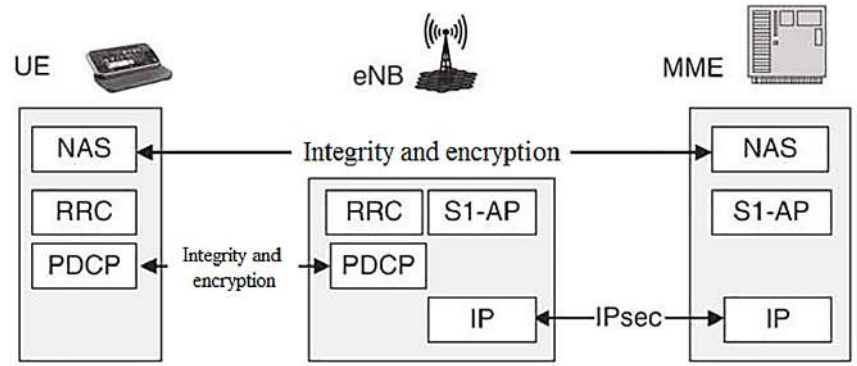


Figure 4. – Protection of the control traffic in the EPS stack protocols

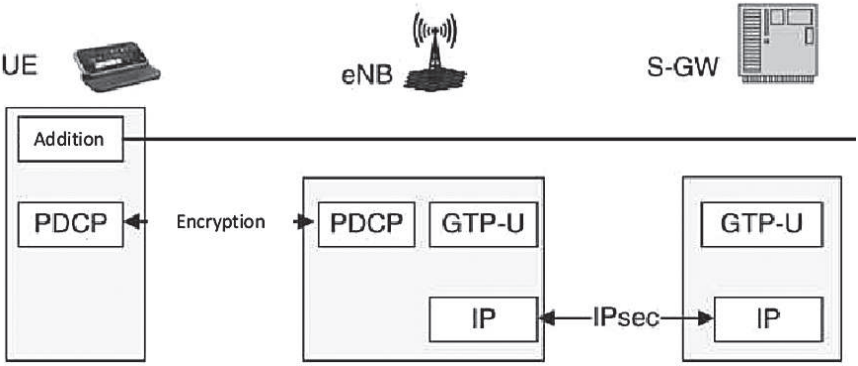


Figure 5. – Protection of user destined traffic in the EPS stack protocols

Specification of EPS security system. The basic specification of the EPS security system is TS33.401 [3]. It contains a description of the EPS security architecture, including all the EPS security features. Also, this document contains a lot of security requirements.

The TS33.401 specification explains the security features for accessing the EPC via E-UTRAN, and covers security system architectures in case of other 3GPP access technologies that are connected to the EPC, such as GERAN (GSM EDGE Radio Access Network, the technology of radio access in the second-generation mobile networks generation) and UTRAN (UMTS Terrestrial Radio Access Network – a ground-based radio access network based on the UTRA radio interface). Security aspects in case of access to EPC through older technologies (eg CDMA) are explained in document TS33.402. Security functions for interfaces between EPS nodes are also very similar to the corresponding features for 3G network nodes. Therefore, the security specifications for network domains – TS33.210 and TS33.310 – are also applied to EPS.

Requirements and properties of EPS security system. As stated above, there are two sources of security requirements for EPS: TS22.278 and TS33.401. The first one provides high-level service requirements, including security requirements, while the second one provides the implementation and security requirements derived from threat analysis. The high-level security requirements of TS22.278 can be formulated the following way:

- (H-1) The EPS security system should provide a high level of security;
- (H-2) Any security issue in one access technology should not affect other types of access;
- (H-3) EPS should provide protection against threats and attacks;
- (H-4) EPS must maintain the authenticity of information between the terminal and the network;
- (H-5) Relevant methods should be provided for traffic protection;
- (H-6) EPS must provide that unauthorized users will not be able to establish connections within (with the help of) the system;

– The TS22.278 security requirements are more related to the services that are provided by the system, can be formulated as follows:
– (S-1) EPS must allow the network to hide its internal structure from the terminal;
– (S-2) Security settings should be controlled by the "home provider";
– (S-3) Security-related solutions should not interact with the provision of services or their transmission in any visible way to the end-user;
– (S-4) The EPS should provide an opportunity for lawful interception of data;
– (S-5) Rel-99 (or newer) USIM (Universal Subscriber Identity Module – Extended SIM standard accepted under UMTS) is required to identify the user in EPS;
– (S-6) USIM shouldn't be used to re-identifying data transmission (or other changes) between EPS and other 3GPP systems, unless the provider requires this;
– (S-7) EPS must support IMS emergency calls (IP Multimedia Subsystem – specification for the transmission of multimedia content in telecommunication based IP protocol).
– The requirements for the protection of personal data can be formulated the following way:
– (P-1) The EPS must provide several appropriate levels of protection for the user's personal data for his communications, location and identity;
– (P-2) The content of communications, point of departure and destination should be protected from the disclosure of unauthorized users;
– (P-3) The EPS should be able to hide personal user data from unauthorized users;
– (P-4) The EPS should be able to hide the user's location from unauthorized users, including those with whom the user communicates.

Threats that endangers EPS. There are many security threats related to communication in general. Most of them endanger EPS. In addition, there are EPS-specific threats that arise from the peculiarities of the EPS architecture, the trust model, the properties of the radio interface etc.

Let's list the most important categories of EPS-related threats and give examples to each of these categories.

– Threats to identify the user. These threats are detailed in requirements P-1 and P-3 above;
– Threats to abuse of network services. For example, filling the network from within (through the compromised elements) or externally (via the Internet);
– Threats of UE tracking. For example, user tracking based on an IP address that can potentially be linked to IMSI (International Mobile Subscriber Identity) or other identities. Also, user tracking, based on redirection of signaling messages;
– Threats relating to base stations and transmission within the "Last mile" (between the base station and the UE). For example, the threat of using

packages directly into the "last mile" connection, as well as the threat of physical damaging to the base stations in dangerous areas;
- Threats that's related to broadband or multiband broadcasting. For example, the broadcasting of false system information, preventing the normal functionality of the network;
- Treats associated with mobility management. For example, the threat of releasing of valuable information about the location of users;
- Threats referring to redirection (user). For example, the forced redirection of a user to a potentially dangerous base station – through a more powerful signal;
- Threats relating to denial of service. For example, jamming the radio signals or performing a distributed attack from a set of UEs towards particular parts of the network or a DoS attack against other UEs;
- Threats relating to radio broadcast protocols. For example, to fake or to change the first messages about the installation of radio contact from the UE side;
- Threats of manipulating the management data. These threats are highlighted in H-4, H-5 and H-6 requirements;
- Other threats to confidentiality. These threats are detailed in the privacy requirements above;
- Threats of unauthorized access to the network. These threats are detailed in H-6 requirements.

It is easy to see that some of the threats are already examine above in the high-level requirements and requirements for protecting private data. Most other threats are examined with more specific requirements. However, there is one type of threat that it is difficult to handle completely. These are Denial of Service (DoS) threats against the network. Indeed, it is extremely difficult to find logical methods of counteraction, for example, jamming the radio signals.

Features of EPS security system. Some of the most important security features come from the LTE security architecture. There can be highlighted the following security features of the LTE security system:

1. Confidentiality of the user and device. This feature ensures the P-1 and P-3 security requirements meeting. The purpose of this feature is to prevent the receiving of information by wiretapped persons, that's enough to identify the sides. This pro feature is copied from 3G and GSM security systems. Details of the mechanism of its work are defined in TS33.102. To protect the device's personal data, some enhancements were created specifically for EPS: device IDs are not sent to the network until security facilities are activated to protect traffic.

2. Authentication between UE and network. This feature provides the executing the high-level requirements of H-2, H-4 and H-6. The purpose of this feature is to check the identity of the interconnected sides. This is the basis of the correct functioning of the whole system, because without authentication users will not be able to securely connect with each other. This feature also allows the UE to verify

the identity of the network to which the connection is made. This feature is also mainly copied from the 3G security architecture (TS33.102).

3. Confidentiality of user and administrative traffic. This feature provides high-level H-5 security requirements as well as P-1 and P-3 security requirements. The purpose of this feature is to encrypt communication in order to make it unobtainable for understanding by wiretapped sides, especially in the radio interface. A similar function is present in the 3G security architecture.

4. Integrity of the administrative traffic. This feature provides high-level H-4, H-5 and H-6 security requirements. The purpose of this feature is to confirm the authenticity of each transmitted message separately, and thus to confirm that the message transmitted has not been modified during the transmission but received in the same form as it was sent to. As with 3G, such integrity protection does not apply to user data.

5. Visibility of security systems and the ability to configure it. This feature is already presented in the architecture of 3G and GSM. Its purpose is to give the user the opportunity to get some information about the security features of the network and use it for his benefits. For the possibility of customizing security systems, the user has the option to enable UICC access control based on the password (PIN).

6. The security of the eNodeB platform. The importance of the security of the EPS base station platforms is especially high because of two reasons:

– eNodeB is the endpoint for the main security mechanisms of EPS;
– eNodeB are expected to be installed in more dangerous locations than 3G base stations when deploying the EPS network.

Similar trends are also presented in the latest versions of 3G technology.

7. Lawful interception of data. This feature meets the requirements of S-4. The purpose of this feature is to provide the law enforcement authorities with access to content and concomitant information such as identifiers of connected persons and time of communications. Lawful data interception (LI) plays a special role in security features, because it limits the set of other security mechanisms in the system. There is a contradiction between the S-4 legal requirement for lawful interception of data and the requirements of the personal data protection. In this sense, data interception is contrary to other security features and should rather be viewed as a controlled exception to other security features. Lawful data interception – one of the EPS system based features., that's in 3G and GSM systems

8. Emergency calls. This is another function that in a way interferes with the operation of other security features. In some countries, legislation requires that emergency calls be possible, even if there are no security conditions for normal calls. For example, when there is no UICC in the terminal. This feature provides the executing of the S-7 service requirement.

9. Security of system interactions. This feature is a kind of "switch" for other security features, but it does not make it less significant than other features. The purpose of this feature is to provide that there are no holes in security when switching from one system to another, for example, when switching from EPS to 3G or vice versa.

10. Network domain security (NDS). This feature is inherited from 3G. Its task is to protect traffic between network elements. Mutual authentication between the involved sides, the confidentiality and integrity of the data – everything included in this feature. Details of this feature are described in TS33.210 and TS33.310.

11. IMS security for voice over LTE. EPS is an IP system based on data packets. Therefore, voice calls must be provided in a way different from the GMS and 3G; that means the methods should be different from the switching channels. A ready-made solution to this problem already exists in 3GPP release 5, namely IP Multimedia subsystem (IMS), based on the SIP protocol (RFC3261). IMS is an overlay system that works with any access technology, including LTE. The fact that IMS does not depend on access technology affects security: IMS security features must exist to ensure its correct functioning, regardless of the security features provided by the (potential) access system. 3GPP security specifications for IMS are contained in TS33.203.

The review of existing methods of LTE security infraction

Below are the different vectors of attack on the LTE radio access network. Some of them are not specific to fourth-generation networks and may be applicable to other radio networks:

1. Interference. The adding of artificial interference to the radio environment can cause the system to stop functioning due to the high level of signal-interference. This kind of attack is easy to implement due to wide availability of equipment. Interference is easily detected by monitoring equipment of the radio channel spectrum.

2. Scrambling. Scrambling – interference is on for a show interval. Directed against certain frames or parts of frames. An attacker may scramble the controlling frames of a particular user in order to stop the service. However, the attacker should be aware of specific frames and temporary slots so that the attack will be successful. This type of attack is difficult to implement.

3. Shutdown. High-speed wireless networks are vulnerable to a simple suppression signal that can block services within the city. The radio channel may be blocked if the transmitter sends a signal at the same frequency. The LTE signal is very complex and consists of many subsystems. if one subsystem fails, then the whole base station will be out of order. The equipment is required for this attack – a laptop, an inexpensive SDR (Software Defined Radio) and a power source.

4. Tracking the location. Detecting user presence within one network cell. Location detection is possible by tracking the combination of C-RNTI (Cell Radio Network Temporary Identifier) with the signals of switching users between base stations. The C-RNTI is transmitted in an open form, so the attacker can determine whether the owner of the given CRNTI is located in this cell or not. The attacker can link the new C-RNTI from the transfer command (Handover Command message) to the old C-RNTI.

5. Key attacks. Key management between the network and mobile stations (MS, Mobile Station) was created to prevent attacks based on receiving response from base stations. ME can detect the aging of the keys received from base stations

(Key Answer message). Both the old and new TEK (Traffic Encryption Key) are transmitted in the corresponding message from the base station. Thus, the attacker can start to often repeat the key update requests to the base station. This will cause confusion on ME and exhaust the resources of the base station.

6. Bandwidth attacks. Measuring the frequencies used by the user device for data transmission. Buffer status reports contain information on scheduling transmissions, load sharing, and access control. Sending the incorrect buffer status report will force the base station to think that the user device does not plan to send any data.

7. Denial of service. A denial of service attack type can be initiated by simply overloading the channel with unauthorized control frames. MS authenticates the base station using RSA. The base station must send its own encrypted public key.

Encryption operation requires a lot of resources. If you overload the base station with erroneous queries, it will fall into the state of constant processing digital signatures without having any time for processing other queries.

8. USIM Cloning. The main task here is to obtain a master key, which is determined by the network provider and is part of a one-to-one correspondence with the IMSI. This key can be restored and used to clone USIM by attacking the physical implementation of mechanisms that implement cryptographic algorithms on the map.

Conclusion

Nowadays, the new line of the wireless networks safety research is the use of the low-budget equipment (software-defined radio systems) to simulate LTE network elements (in particular, base stations). Such approach allows to attack the "man in the middle", which, however, is quite difficult to implement, due to existing security protocols and mechanisms for encryption and protection against repetitions of control traffic. Also, the use of software-defined radio systems allows to track the location of network users and conduct DoS attacks upon the base stations of the network. Another type of threat is related to USIM card cloning. The main task is to obtain a master key, which is determined by the network provider and included in the mutual definitive correspondence with the IMSI. In this case, the main type of the attack, is an attack from the side – by measuring the voltage and temperature indicators on USIM and further analysis of the data, the successfully restoring of the master key can be successful. The protection from such attacks should be improve by improving protection of SIM-cards by manufacturers. The third type of threat is the careless testing of mobile terminals, which are produced. An error in the design and implementation of mobile devices may lead to the appearance of new important security threats to users. To eliminate this kind of threat, it is necessary to search for the vulnerabilities of mobile networks by the side of active users.

References:

1. Morten Tolstrup Indoor Radio Planning: A Practical Guide for GSM, DCS, UMTS, HSPA and LTE .– Wiley India Private Limited, 2014.– 480 p.

2. System Architecture Evolution (SAE) – Security architecture. URL: http://www.3gpp.org/ftp//Specs /archive/ 33_series/33.401/33401-e20.zip.
3. Silke Holtmanns, User Location Tracking Attacks for LTE Networks Using the Interworking Functionality // IFIP Networking. 2016. – P. 315–322.
4. Tihvinski V. O., Yurchuk A. B., Terentyev S. V. LTE mobile communication network. Technology and architecture.– M: Eco-Trends, 2010. – 284 p.

Technology of protection video informational resource in the critical information infrastructure

Yurii Ryabukha
Doctor of Technical Science, Associate Professor
Department of Software Engineering and Management Information Technology
Kharkiv National University of Air Force by named I. Kozhedub
ORCID: https://orcid.org/0000–0001–9821–598X

Andrii Vlasov
Doctor of Philosophy in Technical Sciences, Leading Research Officer
Air Force Science Center
Kharkiv National University of Air Force by named I. Kozhedub
ORCID: https://orcid.org/0000–0001–6080–237X

Abstract. *Is presented technology of the protection video information resource in information and communication component of critical infrastructure that directed toward the development of the technology of processing video information resource for the purpose of the guarantee of its information security, improvement in the protection of resource itself and its service information, based on the development of the complex of the methods of data processing resource components.*

Keywords: *critical information infrastructure, coding, video stream, video frame, semantic significant, processing, compact representation*

Introduction

Modern processes of introducing the latest information technologies, the formation of the information community reinforce the importance of ensuring all components of national security, including information security. Currently, all the basic management processes for objects of critical information structure are not complete without the use of information and communication (infocommunication) systems and systems for collecting, processing and transmitting information.

Critical information infrastructure means a set of automated control systems for the production and technological processes of critical state facilities and for their interaction between information and telecommunication networks, as well as information systems and communication networks designed to solve public administration tasks, ensure defense capability, security and law and order.

Complex application of data of infocommunication systems, allows to increase significantly dynamism, flexibility and management efficiency. Thus, the problem of information security and protection of the processed information resource cannot be solved without improvement of the existing technologies of processing and protection of information resource, and introduction of new technologies.

Actual are requirements: ensuring high-quality providing video data, efficiency of delivery of a video information, ensuring necessary level of safety and protection of

video information resource. At the same time, organizational and technical problems associated with the use of low-speed communication channels, low-quality video equipment, outdated systems for technical protection of information in control systems at objects of critical structure, determine the search for a solution to the problem of ensuring the security of the resource and its protection in the development of new software and hardware solutions while minimizing the economic costs of development and implementation. These solutions should guarantee their simple practical adaptation when introducing hardware of a higher technological level at the critical structure objects.

Thus, as show researches [1–3] by the most significant threats to security to video information resource there are threats of availability and integrity, and from the point of view of ensuring protection – interception, opening and recognition of a resource.

Therefore, the complex problem of protection of a dynamic video information resource in an infocommunication component of control systems of objects of critical structure with simultaneous ensuring information security of this resource, is actual scientific applied research.

Problem solution and results

It is offered to conduct researches and to develop technology of processing of video information resource which will realize the following methods:

- automatic detection and allocation of semantic significant information of the video frames (on the basis of the cascade scheme of processing of a video stream);
- classifications of degree of a semantic saturation of the video frames (or structural unit of a video stream) on the basis of their hierarchical clustering (both in temporary, and in spectral and spatial areas);
- estimates of information intensity of a video stream taking into account its structure and the executed classification semantic video frames saturations (fragments or macro blocks);
- structural processing of the video frames (its macro blocks) with application of selective approaches for decrease in intensity of the transferred video data with use of decisive rules in spectral space (taking into account identification and closing of significant structural units, and also coordination of future code designs);
- differential processing of the transformed submission of the video frames (coding of the video frames with adaptation of parameters depending on a class of a semantic saturation);
- defense of dynamic video information resource with forming of a few channels of treatment and transmission of video stream in obedience to classification of semantic maintenance of macro blocks of video frames;
- reconstruction of a video stream (video images) on the basis of decoding of channels taking into account a class of a semantic saturation of video images (fragments, macro blocks), intra personnel selection of structural units

of a basic shot, the created channel for steganography and the introduced enciphering methods.

Complex development and application of these methods will allow to develop technology of processing of video information resource and to improve protection of video information resource and office information in an infocommunication component of critical infrastructure with providing necessary (not below set) the level of confidentiality and availability of a resource, and also saving (control) of key (semantic significant) information.

Process of formation of a video stream is based on consecutive creation of a chain of the video footage of different type. The type of frames of a video stream is meant as a way of coding and storage of information on the next frame differing from each other in existence or lack of dependences of this frame from previous and the subsequent.

Thus, the video stream consists of consistently created groups of the video frames. Each group of the video frames consists of three types of the video frame: intra (I-frame), predicted (P-frame) and bi-predicted (B-frame) [4].

It is offered to make the analysis and processing of structural unit of a frame for the brightness components, and to carry out procedures of closing (enciphering) and coding for all components (macro blocks) of a frames.

The block diagram is submitted of the offered technology of processing of video information resource in an infocommunication component of critical infrastructure on the (Figure 1).

Processing can be realized at different stages of formation, processing and transfer of video data, namely:

1) encryption of video stream (all operations on the decline of intensity of stream and anti jamming encryption are executed with the already hidden view data);

2) after compression submission of video data is created (before the coded video stream gets to a communication channel);

3) in the course of coding (algorithms of enciphering are integrated into the standardized process on processing of initial video data for decrease in their intensity).

For the removal of lacks of every variant it is suggested to use selective approach (data are closed in the process of their encryption).

Such realization is real to development and introduction in the handling systems of data, where realization of programmatic additions and their integration are assumed in a video codec. For this option, encoding and encryption are performed for the source data as they are received for processing.

To ensure information security and improve the security of the video information resource when meeting the requirements for efficiency, reliability and confidentiality in the critical structure management system, it is necessary to develop the proposed methods based on the improvement of standardized MPEG technologies and cryptographic protection algorithms, methods for forming steganographic channels.

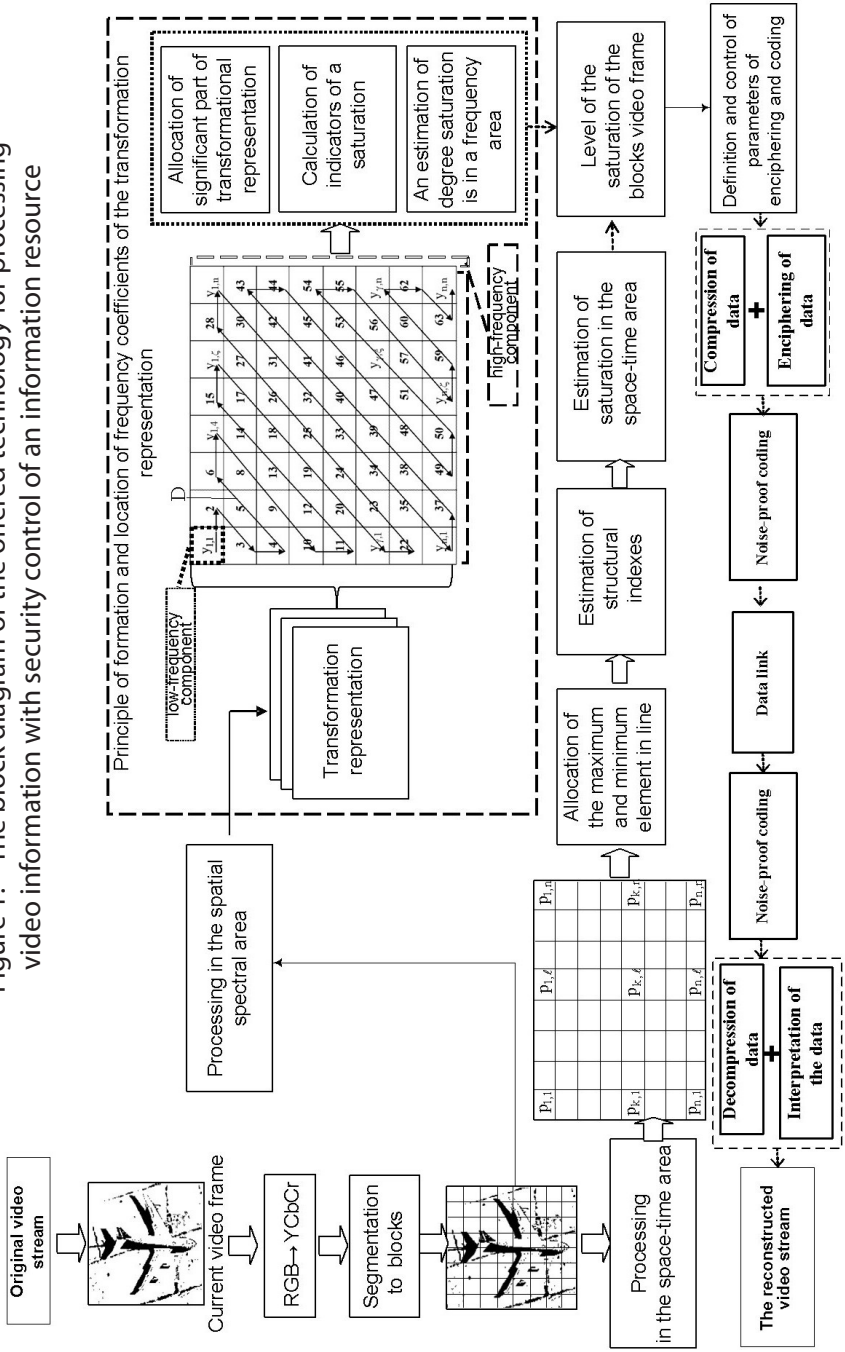


Figure 1. – The block diagram of the offered technology for processing video information with security control of an information resource

It is necessary to first evaluate the information intensity of the video stream in its various transmission and processing options in order to assess the possibilities for improving its processing and protection. General indicator taking into account the correspondence of requirements to the processing methods and the hardware is the bandwidth of the processing channel of the information resource in terms of the initial stream and processing technology (encoding, encryption) and video stream transmission.

From the point of view of the initial stream, the throughput of the channel in question for the information and communication component of the critical structure system will be understood as the total intensity of the closed video stream, which is generated, processed and transmitted in the required time when the conditions for ensuring its safety are fulfilled (by confidentiality and availability, integrity).

In other words, the throughput of a closed video channel refers to the number of source frames for which the system provides security and delivery (processing and transmission) for the required time with the necessary reliability

From the standpoint of processing technology (encoding, encryption) and transmission, the throughput of a closed video channel for the infocommunication component of a critical structure system means the intensity of hidden encoded video data corresponding to the number of frames that need to be processed (from the formation of a hidden container) and transferred in the required time while meeting the requirements security and network bandwidth.

The bandwidth of such a video channel depends on:

Processing time (encoding and encryption) and transmission of the video stream. The shorter the delivery time of the encoded stream, the more frames will be processed and generated in the required time;

Integrity. The lower the peak signal-to-noise ratio for authorized access, the lower the intensity of the encoded stream and the shorter the delivery time. But this violates the requirement to ensure a given level;

The degree of its closure. The lower the peak signal-to-noise ratio for unauthorized access, the higher the degree of closure. The greater the degree of concealment, the more patterns are destroyed during coding and therefore less redundancy is eliminated, and the intensity increases accordingly. This leads to a decrease in the bandwidth of the closed video channel.

The degree of saturation of video frames. The higher the degree of saturation, the greater the number of structural units that are processed and closed (encoded according to a given scheme and algorithm according to the assessment of the degree of saturation), and the smaller the number of structural units that are encoded according to the standard algorithm. This leads to an increase in the total intensity, and therefore, to a decrease in the throughput of this video channel.

Hence, in order to fulfill the bandwidth requirements of a closed video channel, it is necessary to reduce the intensity of video data in the context of reducing transmission time, to ensure their safety, protection and delivery for the required time under the necessary conditions of integrity and confidentiality.

Thus, it is possible to evaluate the throughput of a closed video channel in terms of the initial stream as follows:

$$H_{эк} = N_K \cdot V_K \ : T_{RT} \le T_{DT}; PSNR_{Sac} \ge PSNR_{RSac}; PSNR_{Sunac} \le PSNR_{RSunac},$$

where V – source video frame rate;

N_K – number of video frames that are formed and transmitted under given conditions;

T_{RT} – required delivery time per frame group;

T_{DT} – real delivery time, which includes time for encoding, hiding and transmitting video data;

$PSNR_{Sac}$ – peak signal-to-noise ratio for the delivered video frame with authorized access;

$PSNR_{Sunac}$ – peak signal-to-noise ratio for the delivered video frame during unauthorized access;

$PSNR_{RSac}$ – required peak signal-to-noise ratio for the delivered video frame with authorized access;

$PSNR_{RSunac}$ – required value of the peak signal-to-noise ratio for the video frame during unauthorized access.

To eliminate the maximum amount of redundancy when processing a video stream, it is proposed to use a basic I-frame, since it contains the maximum amount of information, and frames of other types contain up to 70% of the links to it [1, 2].

At the same time, the methods of processing and hiding video data (for the covert channel) that will need to be developed and implemented should be based on hiding only I-frames (intra-frames are called key frames and contain only independently compressed macro blocks).

This ensures complete concealment of the entire video sequence with minimal redundancy.

It is proposed to analyze and process the structural unit of the frame only for its brightness component, and to perform the closing (encryption) and coding procedures for all components (macro blocks) of the frame [1–4].

To eliminate the maximum amount of redundancy in video stream processing, it is proposed to use the basic I-frame, since it contains the maximum amount of information, and other types of frames contain up to 70% of references to it [1, 2].

At the same time, developed methods for processing and hiding video data (for covert channel), will be based on the concealment of only I-frames. Thus, complete hiding of the entire video sequence with its minimum redundancy is ensured.

The processing process can be implemented at different stages of the formation, processing and transmission of video data, namely:

1) before encoding the video stream (encryption algorithms are applied to the newly created (uncoded) source video data; all operations to reduce the intensity of the stream and error-correcting coding are performed with already hidden video data);

2) after the compression representation of the video data has been formed (before the encoded video stream enters the communication channel);

3) in the encoding process (encryption algorithms are integrated into a standardized process for processing the original video data to reduce their intensity (at various stages of compression)).

It is proposed to perform the analysis and processing of the structural unit of the frame for the luminance component, and the closing (encryption) and encoding procedures to perform for all components (macro blocks) of the frame.

The option of encrypting the source data before encoding has the following disadvantages:

– does not take into account the reduction of redundancy in the source video data;
– after encoding, an increase in the initial intensity of the video stream occurs as a result of the destruction of its structure due to pre-encryption;
– an increase in the intensity of encoded encrypted video data entails an increase in the time required to transmit this data in the communication channel.

The option of hiding the video stream after its compression allows reducing the preliminary redundancy of the original video stream and reducing the processing time (including encryption). It provides a high level of information closure, but at the same time they have significant drawbacks:

– error propagation occurs in case of errors in the communication channel;
– cryptographic processing is subject to the entire video information flow, which increases the total processing time of the generated video data on the transmitting side and the processing time of video data on the receiving side.

Therefore, to eliminate these shortcomings, it is proposed to use a selective approach (an option in which data is closed in the process of encoding it). This approach is real to the development and implementation of data processing systems, where it is possible to implement software additions and integrate them into a video codec. For this option, encoding and encryption are performed for the original data as they are received for processing.

In the process of forming a video information stream in the implementation of a selective approach is achieved:

– raising the information content of the transmitted structures and reducing the initial intensity;

– eliminates redundancy (reduces the amount of information) that can be used in cryptanalysis;

– encryption time is reduced by reducing the length of processed messages.

In this case, the encryption time $T_{enT}^{(1)}$ of the original video stream is calculated by the formula:

$$T_{enT}^{(1)} = \frac{\partial(N; R_k; G_k)_{en}^{(r)}}{S_{CC}},$$

where S_{CC} – performance of the computing complex, estimated as the number of operations per second;

$\partial(N;R_k;G_k)_{en}^{(r)}$ – the number of encryption operations, which depends on the encryption algorithm r for used.

The option with encryption of the source data before encoding has the following disadvantages:

- Redundancy reduction in the original video data is not taken into account;
- after encoding, an increase in the initial intensity of the video stream occurs as a result of the destruction of its structure due to preliminary encryption;
- an increase in the intensity of encoded encrypted video data entails an increase in the time it takes to transmit this data in the channel.

The option to hide the video stream after its compression allows reducing the preliminary redundancy of the original video stream and reducing the processing time (including encryption). It provides a high level of information closure, but at the same time it has significant disadvantages:

- with errors in the communication channel, propagation of errors occurs;
- the entire video information stream is subject to cryptographic processing, due to which the total processing time of the generated video data on the transmitting side and the processing time of the video data on the receiving side are increased.

The options considered also have common disadvantages:

- closing the video stream is not in real time;
- the intensity of the closed video stream is often significantly higher than the intensity of the original.

Therefore, to eliminate these shortcomings, it is proposed to use selective technology (a set of methods in which data is closed during encoding). Such an implementation is real for development and implementation in real-time data processing systems, and it is also possible to implement add-ons (software) and their integration into existing video codecs. For this option, encoding and encryption are performed for the source data as they arrive for processing.

The selection mechanism means closing not the entire video frame, but only its significant components.

A significant component is understood to be such a component of a video frame that carries the greatest semantic and structural information content. In the process of automatic selection of significant components, it is proposed to take into account the structural features of video stream formation.

For the selection of significant structural units are invited to identify the most informative, in terms of structural and semantic content, the components of the base frame. Since the luminance component of the video frame carries the most complete information, it is proposed to identify significant structural units on the basis of the luminance components. Therefore, the decision to close the structural unit is proposed to be carried out according to the results

of the analysis of the information component of the aggregate of the blocks of the luminance component.

To determine the energy saturation of blocks, it is proposed to introduce the concept of blocks of three types:

– slightly saturated blocks (blocks in which there are uniform sections of the image);
– average saturation (blocks in which there are minor differences between the pixels, respectively, smooth transitions of contrast are present);
– highly saturated blocks (blocks in which there are sharp transitions of brightness and contrast of the image) [1, 2, 4].

It is proposed to evaluate the structural and semantic information content of the structural unit (macro block) from the standpoint of spectral characteristics [2–4] or on the basis of metrics [5].

A system of indicators has been developed for identifying the most significant blocks of the brightness component of a video frame according to the degree of semantic and structural saturation based on the assessment of indicators: in the space-time domain and in the space-spectral domain [1, 3].

To improve the classification of fragments of video frames (macroblocks), it is proposed to use a two-basis principle, which covers the spatial-temporal and spatial-spectral representation of a video frame.

The mechanism of selection is meant as closing not of all video frames, but only its significant components [3].

The significant component is understood as such component of the video frame which bears in itself the greatest semantic and structural informational content. In the course of automatic selection of significant components it is offered to consider structural features of formation of a video stream [1, 3].

For selection of significant structural units it is offered to reveal the most informative, in respect of the structural and semantic contents, components of a basic frame [1]. As the fullest information is born by the brightness a component, significant structural units are offered to be revealed on its basis. Decision-making on closing of structural unit is offered to be carried out by results of the analysis of information component of set of blocks of the brightness component of the video frame.

For definition of a power saturation of blocks it is offered to enter classification of blocks of three types:

– poorly saturated blocks (blocks at which there are uniform sites of the image);
– an average saturation (blocks in which there are insignificant differences between pixels, respectively are present smooth transitions of contrast);
– strongly saturated blocks (blocks at which there are sharp transitions of brightness and picture contrast) [3].

It is necessary to develop system of indicators for identification of the most significant blocks of the brightness component of the video footage on degree of a semantic and structural saturation on the basis of an assessment of indicators: in space-time area and in spatial spectral area [1, 2, 4].

It is offered to apply selective methods of enciphering to increase of a noise stability of all video stream, and owing to simple realization of these methods and small computing expenses. At unauthorized interception of such video stream with mistakes, in process to interpretation the quantity of these mistakes will only increase.

The analysis of various options of selective enciphering showed that the most effective is enciphering after a stage of transformational transformation [2].

To increase the classification efficiency of fragments of video frames (macro blocks), it is proposed to use the two-basis principle, which covers the spatio-temporal and spatial-spectral representation of the video frame. Then, to evaluate the level of saturation in blocks of video frames, it is proposed to use the following indicators:

1) in the space-time domain – the structural indicator of the block P_{Str}, which determines the most significant elements of the time, is represented by the expression:

$$P_{\text{Str}} = [\log_2(\prod_{i=1}^{n}(p_{k,\max} - p_{k,\min}))]$$

where $p_{k,\max}$ – maximum macro block row element brightness value;

$p_{k,\min}$ – minimum macro block row element brightness value;

i – line number.

2) in the spatial spectral region, the saturation index of the block P_C, which determines the most significant transform coefficients in each designated zone, is represented by the expression:

$$P_{\text{SSR}} = [\log_2(\prod_{\gamma=1}^{D_d}\prod_{\xi=1}^{N_y}(y_{\gamma,\xi}))],$$

where $y_{\gamma,\xi}$ – the frequency coefficient of the transform at the position with coordinates (γ, ξ) relative to the diagonal D;

D_d – the number of diagonals in the estimated area of the frequency coefficients;

N_y – the number of frequency coefficients that correspond to the diagonals in the evaluated area.

It is proposed to determine the energy saturation of blocks after a spatial spectral representation (SSR), for example, a discrete cosine transform (DCT). Using SSR, a transition is made from the spatio-temporal representation of the video frame to the spatially spectral one. The components of the SSR transform (DCT) are integral characteristics of the structural content of the image fragment. Moreover, the integral properties of the components depend on their position in the transform.

It is necessary to develop the main stages of formation of a binary code of the ciphered significant structural unit which are based on three technological components for development of a method of coding of significant structural unit (macro blocks of frame):

– the first component consists in formation of a binary code of value components of transformation representation for the image block;

– the second component consists in formation of a code design of the structural unit of the basic video frame which is subject to enciphering;

– the third component consists in formation of matrixes of a binary code of significant structural unit of the same size, as an enciphering key.

It is proposed to develop the method of the decoding of closed video stream on the basis of the selection (development of the closed significant structural units) of base video frame. for this is proposed to decode the closed base video frame taking into account the determination of the significant structural units.

It is offered to improve a method of a compression of video images on the basis of differential processing of the transformed representation of shots according to the offered classification of semantic significant fragments and to carry out coding with adaptation of parameters of a compression depending on value of a class of a saturation and existence of the built-in steganography container [1, 2].

To assess the integrity of video frames, it is proposed to use proven parameters [5].

As the main parameters, a measure of structural similarity is proposed – SSIM.

For auto-automatic processing systems, the video stream is defined as:

$$\mathrm{SSIM}=\left(\frac{\sigma_{\mathrm{XY}}}{\sigma_{\mathrm{X}}\sigma_{\mathrm{Y}}}\right)\left(\frac{2\overline{\mathrm{XY}}}{(\overline{X}^2)+(\overline{Y}^2)}\right)\left(\frac{2\sigma_{\mathrm{X}}\sigma_{\mathrm{Y}}}{\sigma^2{}_{\mathrm{X}}+\sigma^2{}_{\mathrm{Y}}}\right),$$

$$\overline{\mathrm{X}}=\frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}x_{ij},\ \overline{\mathrm{Y}}=\frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}y_{ij},$$

$$\sigma^2{}_x=\frac{1}{(M-1)(N-1)}\sum_{i=1}^{M}\sum_{j=1}^{N}(x_{ij}-\overline{X})^2,$$

$$\sigma^2{}_Y=\frac{1}{(M-1)(N-1)}\sum_{i=1}^{M}\sum_{j=1}^{N}(y_{ij}-\overline{Y})^2,$$

$$\sigma_{XY}=\frac{1}{(M-1)(N-1)}\sum_{i=1}^{M}\sum_{j=1}^{N}(x_{ij}-\overline{X})(y_{ij}-\overline{Y}),$$

where SSIM – value of a measure of a likeness (integrity) of images (video frames);

X, Y – video frame restored (after processing procedures) and the original;

M, N – video frame size.

A measure of structural similarity SSIM is a comprehensive assessment of the similarity (quality) of images, which has the following components for comparing the input and output images: the correlation coefficient between images, an assessment of the similarity of the average brightness values of the images, an assessment of the similarity of the contrasts of the two compared images. The higher the value of the measure of similarity of images, the better image processing is performed.

This is a criterion that takes into account both the number of discontinuities and the number of missing elements in individual discontinuities, as well as their small displacement. Ranges of values for their criteria-based assessment are formed on the basis of experimental data.

Conclusions

Thus, as a result, the degree of compression and coding is adapted, one-to-one recovery (decoding) depending on the class of semantic saturation of image fragments (video frames) due to the strategy of differential determination (selection) parameters coding of transformants conversion [4]. This provides an increase in the efficiency of compression and coding due to the regularization of the brightness component of images with a given level of integrity of the information resource, namely, the preservation of the original semantic component of video images.

The strategy for selecting compression and coding parameters includes a method for generating these parameters, a quantization matrix, and a mechanism for their adaptation, depending on the class of semantic saturation of the video frame (its fragments). Depending on the class of semantic saturation, the parameters are calculated (or their choice determined earlier empirically based on the processing of experimental data) [4, 5]. The compression and coding process is the transformation of transformant by bitwise processing in accordance with the chosen strategy (implementation of coding methods).

Thus, methodological bases of protection of video information resource in infocommunication component of critical infrastructure the processing of video information resource (development of a complex of the interconnected methods) directed on development technology for the purpose of ensuring its safety, improvement of protection of the resource and office information of all video stream are formulated.

A further area of research is the development of the proposed methods and approaches, their software and hardware implementation, adequacy testing and implementation in the new standards for ensuring the security of information resources.

References:

1. Barannik V. V., Polyakov V. P. The encoding of the transformed image in infocommunication systems. – Kharkiv, 2010. – 212 p.
2. Barannik V., Podlesny S., Krasnorutskyi A., Musienko A., Himenko V. The ensuring the integrity of information streams under the cyberattacks action, 2016 . IEEE East-West Design & Test Symposium (EWDTS). – Yerevan, 2016. – P. 1–5.
3. Vlasov A. V., Lukin V. V., Komolov D. A. Coding of information resources of systems of a video conferencing for increase of their safety // Radio electronics and informatics.2013.– № 2.– P. 44–48.
4. Vlasov A. V., Shiryaev A. V. Method of coding of video images with masking for increase of safety of video information resources // Radio-electronic and computer systems.2013.– № 3.– P. 65–73.
5. Vlasov A. V. Estimation of quality methods disguise images for detection edge contours // Science-Based Technologies.2013.– № 2(18).– P. 193–197.

Cyber safety prevention methods for children

Marharyta Melnyk
Doctor of Philosophy, Associate Professor
Department of Radio Engeneering Divices
Odessa National Polytechnic University
ORCID: https://orcid.org/0000–0003–0619–7281

Serhii Yevseiev
Doctor of Technical Science, Senior Research
Department of Cyber Security and Information Technology
Simon Kuznets Kharkiv National University of Economics
ORCID: http://orcid.org/0000–0003–1647–6444

Abstract. *In the of rapid technological development, it is impossible to imagine the life of a modern person without internet technologies. Therefore, it is important not to avoid those innovations, but to use them correctly. In this article, we want to pay attention to the ways of providing the safety of children and middle school children in internet. We want to offer an educational family game board as a tool for the training of cyber security of children.*

Keywords: *cyber security, cyber safety, internet technologies, internet, devices with internet access, digital security*

Introduction

The internet is not as harmful as it might be seen at first glance. Nevertheless, you need to take care of the safety of the child by following some rules of behavior on the Web.

The problem with young users of smart phones, tablets and other devices with internet access is not only that children can accidentally see, read or download something inappropriate at their age, but also because of insufficient life experience and knowledge, they are very vulnerable to the actions of attackers. Even worse: children can be not only the victims but also a scam tool. What to do with this?

Parents are fully capable of providing children (and, therefore, the whole family) with digital security. It is most reliable to apply an integrated approach combining the educational component and software, then there is a chance to protect children from the cyber threats and, at the same time, keep the opportunity for them to enjoy all the advantages of the digital world. Further, we will give some recommendations that will help you to minimize risks. But first, let's figure out what specifically can pose a threat to a child on the internet.

Let's review some of the most common cybercrime scenarios.

Smart House. A growing number of families use internet devices (IoT) at home: smart doorbells, baby monitors with access to the internet, surveillance cameras, and

other devices. But what will happen if fraudsters gain access to them by penetrating the network through children's devices?

Free public Wi-Fi and School Wi-Fi. Parks, fast-food restaurants and other public spaces with free Wi-Fi are a real bait for teenagers who like to hang out in such places after (or instead of) classes [1, 2].

Untrustworthy applications and viruses. You can pick up virus software not only on adult sites. Malicious code can also be hidden in ordinary applications downloaded from P2P resources or even from Google Play which is also used by children.

Phishing emails. Phishing messages are often disguised as official letters or even come from friends whose accounts have been hacked, so it's not always easy to recognize them even for adults. If you open such kind of a letter, you can get very unpleasant software to your gadget that will steal important information or extort the money.

Excessive dissemination of information on social networks. Critical thinking is not the strongest side of adolescents, so they are not always picky about relationships. Children do not think with whom they are "making friends", how much information they share and what excessive openness in social networks can lead to. And the consequences can vary – from easy embarrassment to large-scale internet harassment.

Materıal and method

Even parents in the families with the most trusting relationships sometimes can't notice the impending danger to the child in time and, moreover, they don't always know how to prevent it.

Here is what parents should pay attention to in order to notice in time that the child has become a victim of cyberbullying/intimidation, humiliation, bullying, physical and mental terror aimed at causing fear and submission in others:

- Restless behavior Even the most reserved student will worry about what is happening and will necessarily betray himself with his behavior. Depression and reluctance to go to school are the most obvious signs that the child is being subjected to aggression.
- Hostility against the internet If the child loved spending time on the internet and suddenly stopped doing it, you should find out the reason. In very rare cases, children are really bored of spending time on the web. However, in most cases, a sudden unwillingness to use the internet is associated with problems in the virtual world.
- Nervousness under receiving new messages A child's negative reaction to the e-mail sound should alert the parent. If your child regularly receives messages that upset him, talk to him and discuss the contents of these messages.

Today the problems of the so-called "internet addiction" (synonyms: internet addiction, virtual addiction) and dependence on computer games ("gaming") are

becoming more and more relevant. The first who came across with them were psychotherapists, as well as companies that use the internet and suffer losses in their activities if employees have a pathological attraction to staying online.

According to Kimberly Young, the harbingers of internet addiction are:

– obsessive desire to constantly check e-mail;
– the anticipation of the next online session;
– increase in time spent online;
– increase in the amount of money spent online.

Recommendation for parents.

And what to do? You should start with a thoughtful conversation with your child: share your concerns, tell about unsafe behavior, give some tips to help him stay safe. At the same time, it is important not to go too far, showing the child that you are driven by anxiety and the desire to protect him, and not the desire to control his life.

It is very important to teach your child not to download malware onto your computer Malicious programs can harm the computer and the data stored on it. They can also slow down the speed of data exchange and even use your computer to spread the virus, send spam on your behalf from an email address or profile of a social network.

Malware collision warning. Install special mail filters and anti-virus systems on all home computers to prevent software infection and data loss. Such applications monitor the traffic and can prevent both direct attacks by intruders and attacks that use malicious applications.

Use only licensed programs and data obtained from reliable sources. Most often, pirated copies of programs, especially games, are infected with viruses. Explain to the child how important it is to use only proven information resources and not to download unlicensed content. Periodically try to fully check your home computers. Regularly back up important data. Try to change passwords time after time (for example, from email) and do not use passwords that are too simple.

What to do if the child is still facing any risks. Establish positive emotional contact with the child, endear him to talk with you about what happened. Tell about your own concern about what is going on with him. The child should trust you and know that you want to understand the situation and help him, and not punish;

Try to listen carefully to the story of what happened, to understand how serious is what happened and how deep it could affect the child;

If the children are upset with something they saw (for example, someone hacked their profile on a social network), or they have fallen into an unpleasant situation (e.g. they spent their own or your money as a result of internet fraud, etc.) – try to calm them down and understand the situation together – what led to this result, what actions of the child were wrong, and where you did not tell them about the safety rules on the internet;

If the situation is related to the violence on the internet in relation to the child, then it is necessary to find out the information about the aggressor, the history of the relationships between the child and the aggressor, to find out if there is an agreement to meet in real life; whether there were such meetings and what the aggressor knows

about the child (real name, surname, address, phone number, school number, etc.), strongly insist on avoiding meetings with strangers, especially without witnesses, check all the new contacts of the child recently;

Collect the most complete information about the incident, both from the words of the child, and using technical means – go to the pages of the site your child attended, review the list of his friends, read the messages. If necessary, copy and save this information – in the future it may be useful for you (for example, for contacting law enforcement agencies);

If you are not sure about the seriousness of what happened with your child, or the child is not open enough with you or is not ready to make a contact at all, or you do not know what to do in such situation. Contact a specialist (helpline, hotline, etc.), where they can give you recommendations on where and in what form to apply if intervention by other duty services and organizations is required (police, for example).

So we also consider it important to mention Karpman Triangle. The Karpman Triangle is the most common model of relationships between people. It was first described by the classic of transactional analysis, Stephen Karpman in 1968. People manipulate each other, depend on each other and get very tired of it. Happiness in such relations is extremely small. Like the forces to make a difference. But there is a way out of this.

Two, three, and entire groups of people can spin in a triangle. But roles in there are always three: a victim, a controller-dictator, a savior. Participants of the triangle periodically change roles, but they are all manipulators and great spoil yourself and loved ones life.

Karpman Triangle using and working in cyberspace. Entry from the Karman triangle is possible. It is important to use preventive measures in order to avoid getting into the triangle.

We know Basic Rules of the safe internet for children:

- do not tell everyone in a row your private information (real name, surname, phone number, address, school number, as well as own photos, family or friends photos);
- do not open email attachments when you don't know the sender;
- do not send spam and "informational dirt";
- do not be rude, nitpick, put pressure – behave impolitely and aggressively;
- do not manage your family's money without the permission of your elders, ask your parents;
- do not meeting the internet acquaintances in real life can be dangerous: a criminal can be hiding behind a pseudonym.

Be careful:

- not everyone writes the truth;
- if you read a lie about yourself on the internet – report it to your parents or guardians;
- invite to chat, play, exchange – check if there is a catch;

– illegal copying of files on the internet it is not good;
– discovered something threatening – don't be afraid to call for help.

Children can:

– use "the nickname" (false name) in correspondence and negotiations;
– respect another user;
– if you use an internet source – make a link to it;
– met on the net and want to meet – take a piece of advice from an adult who you trust;
– open only those links in which you sure;
– the best way to use the internet when there is one of the parents nearby or someone who knows well what the internet is and how to behave in it correctly.

How to protect children from negative information?

Resulting from the development of new technologies in the field of virtual space, including the spread of the internet network, there arose a problem related to the access of minors to information of dubious content and contrary to generally accepted ethics. At present, any person, including a minor, who has knowledge in the field of computer technology, can access data stored on the internet or create his own web resource.

The lack of parental control over the children's use of the internet is one of the reasons for minors to access negative information. As a memo to the parents on the safe use of the internet by children following are the basic rules that will help protect your children from the information of dubious content and contrary to generally accepted ethics:

Rule 1. Parents should know the interests and goals of children who use the internet.

Rule 2. It is recommended that children use the internet in the presence of adults. Access to this information resource should be efficient and safe.

Rule 3. It is necessary to exclude children's access to the internet resources, the contents of which are contrary to the law, that can have a negative impact on minors.

Rule 4. In the case of independent access of children to the internet, parents should control the use of information by minors.

How to limit children's access to negative information on the Internet? To do this, you may need the following set of software:

– a program for parental control, which provides a limitation of screen time, blocking access to sites and applications, as well as the protection of "smart home" gadgets;
– a means of protection against phishing emails and sites that steal personal data, and minimization of the dissemination of information in social networks;
– a tool to protect your smart phone and tablet from email and web threats, as well as from malicious code hidden in applications;

– password manager that will help children (and adults) to create complex passwords and store them in a safe place – even if some of the children's accounts are hacked, the rest will remain protected.

Experimental results

In the era of rapid technological development, it is impossible to imagine the life of a modern person without internet technologies. Therefore, it is important not to avoid those innovations, but to use them correctly. In this work, we want to pay attention to the ways of providing the safety of children and adolescents on the internet.

Educational systems are one of the most dynamically developing types of software, the demand for which in the conditions of development of electronic and distance learning, the introduction of a continuing education system, advanced training, retraining, and digitalization of the educational sphere as a whole is constantly growing. One of the most popular category of educational systems is educational computer games. Environmental friendliness of information and the safety of the internet network should be ensured for all types of activities and occupations of the child (adolescent). We suggest digging into the nature of some presumptions about children and the internet. Some basic myths-speculations are presented in (Table 1).

Table 1. – Basic myths-speculations about Cybersecurity for children

Presumptions	**Clarifications**	**Recommendations**
1	***2***	***3***
Being on the internet is addictive.	Those who feel bad in real life go headlong into the games. If you forbid such a child to play, he will simply look for another way to get distracted.	As soon as in real life the child discovers something more exciting, you will not see him at the computer anymore.
To preserve the mental health of the child, it is better to protect him from the Internet.	The internet is an essential part of the modern world. Parents, restricting children from being online, deprive them of the opportunity to meet basic needs, in this case, social. Subsequently, this situation can cause a child's serious psychological problems.	Conduct outreach. Explain that the internet is useful, but can not be a substitute for real life. Parents' own example should be the main evidence.
Virtual friends can replace real friends.	The computer itself does not affect the growth of interpersonal skills. If the child's time to interact with people is spent	In order to gain important communication skills, children need visual and tactile contact with their parents.

1	*2*	*3*
	on the gadget, in the future it will affect family relationships, communication with other children, attitude to oneself and emotional intelligence.	The child must learn speech, recognize emotions and, finally, just spend time with mom and dad at useful games.
Physical health issues are related to internet technologies.	The use of gadgets stimulates low physical activity, problems with posture and overweight.	It is important to limit the time spent with children not only on the internet but also to limit the use of gadgets Give preference to interactive entertainment: let there be more educational applications than entertaining videos.
Sleep and mental health problems associated with the use of gadgets.	With all these dangers, mobile devices have many advantages for children's formation. Gadgets are the realities of our time and there is no escape from them. Therefore, the issues of the interaction of the child with devices should be approached without fanaticism. But do not forget that without reasonable restrictions, gadgets can serve parents and children poorly.	Children should not be allowed to play with mobile devices several hours before bedtime. Do not give your children a device when they are having a tantrum, and replace personal attention with gadgets.

It is important to offer children (teenagers) an alternative, to explain all the advantages and disadvantages. Explain the value of the time they spend on the computer. The easiest way to learn is the study in the form of a game, the most accessible way to explain is a learning game. For children (adolescents) it is important to carry out explanatory work at the stage of acquaintance and in the process of working with internet technologies.

From the point of view of psychology and the formation of personality structure game and imitation is one of the mechanisms of evolution. Therefore, gaming is one of the most effective tools for acquiring knowledge.

Nowadays, in the ascientific literature more and more attention is paid to the use of the game in order to increase the effectiveness of the educational process, but unfortunately, not all teachers are able to correctly use it in teaching.

The disclosure of the importance of gaming activities was developed by such educators and psychologists as L. Rubinstein, D. B. Elkonin, S. Freud, J. Piaget, and others. The role of the game in the growth of the personality and basic mental functions, in self-administration and self-regulation of the personality, and finally, in the processes of socialization underlie on the adoption and use of social experience by a person, as was investigated and substantiated in their works.

Therefore, explanatory work on the use of internet technologies and a game form of cybersecurity training is an effective tool for raising a mentally healthy generation, as well as preventing cyber addiction in adolescents

The game is a type of activity in conditions of situations aimed at the reconstruction and assimilation of the social experience, in which behavior self-management develops and improves. The therapeutic function of the game is to use it for the means of overcoming various difficulties that a child has in behavior, communication, and learning. The game therapy effect is determined by the practice of new social relationships that the child receives in a role-playing game. It is the practice of new real relationships in which the role-play puts the child with both adults and peers, relations of freedom and cooperation, instead of relations of coercion and aggression, ultimately lead to a therapeutic effect. The correction function is the carrying in of positive changes, additions to the structure of the child's personal indicators. In the game, this process occurs naturally, gently. The entertaining function of the game is perhaps one of its main functions. The game is strategically – only an organized cultural space of entertainment for children, where they go from entertainment to evolution.

Educational games are a large group of methods and techniques for organizing the learning process. The main difference between an educational game and just a game is that the first has an essential feature – a clearly defined learning goal and the corresponding pedagogical result. The symbiosis of science and technology always gives a better effect than the use of knowledge in only one area. Therefore, we believe that the development of an educational game that instructs the cyber safety for children is more effective than outreach. The game will include rules and simulate dangerous situations, ways to avoid dangerous situations and safe exits from such situations. The development of communication skills takes place in a playful way. The use of a desktop educational game is an effective tool for both training cybersecurity and improving the communication of children.

The tool for the training of cybersecurity for children

The choice of teaching methods is first of all determined by the content of the educational material and the learning objectives. The learning process forms the proficiency and skills needed in practical work. Therefore, in the learning process the methods that are suitable to bring children and teenagers closer to the real situation should be used first of all. All these requirements are best met by educational and psychological games [3].

The effectiveness of the game form of training has been proven both by educators and psychologists. An educational game is a form of activity of participants

that imitates real situations and helps to find a way out of them. Thus, the child (teenager) gets the skills to overcome difficult situations, learn to avoid them and improves the level of communication.

We want to offer an educational family game board as a tool for the training of cybersecurity of children and adolescents.

The advantages of the game are as follows:

– imitation of a real situation that can change under the influence of various factors;
– solving of complex problems, so by unraveling of the plot there is a dependence of subsequent actions on previous ones;
– the connection between behavior and communication, as it is based on specific behavior, actions;
– collective, group interaction;
– are functional, affect changes in behavioral factors.

This game complex includes: the theoretical part, a description of the situation (case), examples, illustrations, diagrams, questions, answers, and methodological recommendations.

The technology of the game includes possible game modeling – artificial creation of real situations and helping to get out of them, so the children (teenagers) will be able to resist manipulation if such a situation happens to them in cyberspace

The game as a method of constructing the learning process includes the following components:

– adoption of a role;
– game actions;
– game technology.

Educational game is an imitation of real situations, training to get out of them, teaching the rules of conduct in a cyber environment Thus, the educational game of cybersecurity training of children and adolescents can be an effective tool that will ensure security in cyberspace. The educational game on the cybersecurity training for children and adolescents is a unique mechanism for accumulating and transmitting collective experience and knowledge. With regard to the educational process in the game, practical (mastery of the ways of solving important problems) and ethical (digestion of patterns, rules and norms of behavior in various situations) experience is mastered. The active position of its participants finds its behavioral manifestation in the game.

The purpose of replacing a real event with an experiment (artificially constructed behavioral patterns) is education and training [4,5].

The model of the game is implemented, put into action using its rules. The rules reflect the ratio of all components of the game. They can be transferred to the game from the real situation in which the gameplay unfolds, or they can be invented.

Roles are prescribed to players by the terms of the game. Game actions can be set up in different ways: by a scenario, by the leaders (facilitators) of the game, or formed by the players themselves (children, adolescents) in accordance with their

own vision of the situation and the goals set for them. Therefore, the role actions of individual participants in the game can differ significantly from each other.

The leading component of the game is the role and its adoption. A role is a set of requirements, expectations, presented by a situation to a given person, his behavior. The performance of the role supposes the exact reproduction of human activities in a typical model of the situation in cyberspace. The adoption of the role is carried out at the cognitive, emotional and behavioral levels. Adoption is implemented through the appropriation of external traits and norms of behavior, as well as tasks inherent in the role, its execution.

Conclusion

The symbiosis of science and technology always gives a better effect than the use of knowledge in only one area.

Game form of education is the easiest for children to perceive information. By skillfully connecting the rules and situation simulators, we can ensure the cyber security of children.

The development of communication skills takes place in a playful way. The use of a desktop educational game is an effective tool for both training cybersecurity and improving the communication of children.

Board educational game is one of the effective methods of teaching cybrsecurity for children (teenagers).

References:

1. Ніколаєнко С. М. Якість вищої освіти в Україні: погляд в майбутнє / С. М. Ніколаєнко // Світ фінансів. 2006. – № 3(8). – С. 7–22.
2. Гуляева Е. В. Компьютерные игры в жизни дошкольников / Е. В. Гуляева, Ю. А. Соловьева // Психологическая наука и образование. 2012. – № 2. – С. 5–12.
3. Сурмина Ю. П. Ситуационный анализ, или Анатомия Кейс-метода / Ю. П. Сурмина // Київ: Центр инноваций и развития, 2002. – 286 с.
4. Галимов М. Геймификация в обучении: что, как и зачем / М. Галимов// [Electronic resource]. – Access mode: URL: http://freepublicity.ru/gejmifikacziya-v-obuchenii-chto-kak-i-zachem/
5. Белкин Ф. А. Геймификация в образовании / Ф. А. Белкин // Современная зарубежная психология. 2016. – Том 5. – № 3. – С. 28–34. Doi: 10.17759/jmfp.2016050303

CHAPTER III. DATABASE AND KNOWLEDGE SYSTEMS

Database replication method based on the task of (0,1)-knapsack

Dmytro Holubnychyi
Doctor of Philosophy in Technical Sciences,
Leading Research Officer, Air Force Science Center
Ivan Kozhedub Kharkiv National Air Force University
ORCID https://orcid.org/0000–0003–1719–7586

Viacheslav Tretiak
Doctor of Philosophy in Technical Sciences,
Leading Research Officer, Air Force Science Center
Ivan Kozhedub Kharkiv National Air Force University
ORCID https://orcid.org/0000–0003–2599–8834

Abstract. *Is proposed a parallel computation method based on the ranking approach to its solution the principle of optimization in the direction and strategies for cutting out unpromising decisions for fragmentation of network database data.*

Keywords: *database, fragmentation method, organization, replication, integer linear programming*

Introduction

Analysis [1–3] shows that each of the performance enhancements requires an analysis of the Relational Database (RDB) structure, the flow of solved tasks (Relational Database Management System (RDBMS) queries), and in some cases a detailed analysis of the use of individual RDB fragments (individual tables, their fields, table groups).

For example, managing an index structure requires determining the intensity of using one table and fields. restructuring involves changing the structure of one or more tables. Materialized Impressions (MPs) means a detailed analysis of the sequence of requests and the introduction of special tables for MPs.

Scientific groups under the leadership of leading scientists Y. Foster, Y. Gordon, R. Buya, E. Dilman, D. Tayne, T. Haye, R. Prodan, and also the research of the organization of efficient processing and fragmentation of data as a technology of the CCI of the SBG are actively engaged. A series of studies by Russian scientists

Gorobets V. V. was carried out. Zinkina SA, Kulba VV, Mikrin EA, Kosyachenko S. A., Plutonko A. D., Sokolinsky L. B., Tsvyaschenko E. V.

Setting the task of distributing fragments of the data of the network database

Let's consider the model of placement of fragments of the network database in the computing complex [5]. As the criterion of optimality, let's take the average amount of data sent through the data lines when the request is executed.

Considered n – the number of nodes of the network with an arbitrary structure; m–number of independent fragments of the stem database of data; c – this node of the network; K_j – j fragment of the network database, $j=\overline{1,n}$; F_i -an $i$object of this fragment $i=\overline{1,m}$; L_i – the memory of the node intended for the placement of fragments; b_j – number of request classes (for example, reading, adding, updating, deleting database records); λ_{ij}^k – intensity of requests k-that class to a fragment initiated in a node; α_{ij}^k – the volume of the request of k that class $\left(k=\overline{1,s}\right)$ to the fragment initiated in the node K_j; β_{ij}^k – the amount of data requested when the query of k that class $\left(k=\overline{1,s}\right)$ is performed to the fragment F_i that arrives at the node K_j; p is the number of tables in the network database; M_z z-th table of RBD, $z=\overline{1,p}$; m_z – number of rows of the table M_z; n_z – the number of columns in the table M_z; d_{ij}^z – the cell of the table M_z at the position (line i; column j), $i=\overline{1,mz}; j=\overline{1,nz}$; d_{ijz} – the amount of memory occupied by the cell d_{ijz}.

The volume of data sent in response to the request of that class to the fragment F_i initiated in the node is determined as follows $\left(\alpha_{ij}^k+\beta_{ij}^k\right)\left(1-x_{ij}\right)$. In this case, the values $x_{ij}\left(i=\overline{1,m}; j=\overline{1,n}\right)$ are determined as follows:

$$y_{ijz}^{\sigma}=\begin{cases}1, \text{ if the cell } d_{ijz} \text{ belongs to the fragment } F_{\sigma};\\ 0, \textit{ otherwise}.\end{cases} \tag{1}$$

Since the intensity generates the amount of data that needs to be transmitted, the total amount of data that is required to be transmitted over the communication channels between the nodes due to the functioning of the distributed system over a unit of time is determined by the formula:

$$S=\sum_{i=1}^{m}\sum_{j=1}^{n}\sum_{k=1}^{s}\lambda_{ij}^k\left(\alpha_{ij}^k+\beta_{ij}^k\right)\left(1-x_{ij}\right). \tag{2}$$

If we put that $\lambda=\sum_{i=1}^{m}\sum_{j=1}^{n}\sum_{k=1}^{s}\lambda_{ij}^k$ the target function of the problem of optimal distribution of fragments over the nodes of the computing complex takes the form:

$$V=\frac{1}{\lambda}\sum_{i=1}^{m}\sum_{j=1}^{n}\sum_{k=1}^{s}\lambda_{ij}^k\left(\alpha_{ij}^k+\beta_{ij}^k\right)\left(1-x_{ij}\right). \tag{3}$$

The lower the value, the higher the speed of service queries. All messages arriving at the node's input queues are divided into two types: type 1 – messages that make up queries for processing which the necessary fragments are not contained in the database of the computing complex node, and the responses to these que-

ries; type 2 – messages that make up requests for which the necessary fragments are stored in the database of the corresponding node of the computing complex. In this case, the request of type 1, arrived for its service to the remote node of the computing complex, turns into a request of type 2.

Since each fragment $F_i\left(i=\overline{1,m}\right)$ must be located in at least one node of the computing complex, then the condition

$$\sum_{j=1}^{n} x_{ij} \geq 1, i=\overline{1,m}. \tag{4}$$

In addition, the volume of the local database of each node should not exceed the amount of memory of this node intended for the placement of fragments:

$$\sum_{i=1}^{m} L_i x_{ij} \leq b_j, j=\overline{1,n}. \tag{5}$$

The total volume of all fragments should be equal to the total volume of all tables in the network database, i.e.

$$\sum_{i=1}^{m} L_i = \sum_{z=1}^{p}\sum_{i=1}^{m_z}\sum_{j=1}^{n_z} w_{ij}^{z} \tag{6}$$

At the same time, the volume of the fragment is equal:

$$L_\sigma = \sum_{z=1}^{p}\sum_{i=1}^{m_z}\sum_{j=1}^{n_z} w_{ij}^{z} y_{ijz}^{\sigma} \tag{7}$$

Thus, the problem of allocating fragments of the data of the network database to the nodes of the computing complex is to determine the values x_{ij} of variables where, which $x_{ij}=\{0;1\}\left(i=\overline{1,m}; j=\overline{1,n}\right)$ satisfy conditions (4) (5) and give the minimum of the linear function (3). The obtained mathematical model is intended for solving the problem of integer linear programming.

Method of cutting off unpromising options for problem (0.1) knapsack

The method of cutting off unpromising options for problem (0.1) knapsack put a set of strategies $\{L_w\}$, whose application to the generalized procedures $A0$ lead to the construction of algorithms for solving this problem of integer linear programming with Boolean variables.

The simplest strategy of clipping $L1$ in the formation of $r=r+1$ paths of the next rank in sets m_{sp}^{r+1} based on the procedure $A0$, is the allocation m_{sj}^{r} of paths of maximum length by weight of functional sj whose lengths by weight restrictions do not exceed the magnitude of b_i, $d_a\left(\mu_{sj}^{r}\right)_i \leq b_i$. In this case, the paths that satisfy the properties of ν are called μ_{sj}^{r} paths whose lengths by weight do not exceed the value of b_i. Then, recurrence relations, corresponding to the strategy $L1$, takes the form:

$$\mu_{sp}^{r+1} = \max_{c_j}\left\{\mu_{sj}^{r}\bigcup(j,p)\right\},\ p=\left(\overline{r+1,n}\right),\ j=\left(\overline{r,n}\right), \tag{8}$$

Using the $L1$ strategy does not always provide the optimal solution to the problem.

The occurrence of the screening of paths by the ratio corresponding (8) to the optimal solution of the problem is due to the fact that the paths with a higher value for the functional can gain more length by weight restrictions. Therefore, at some rank there is a situation where, due to restrictions, the paths of the next ranks in the graph $D\Delta$ cannot be constructed, and paths with smaller values of length by weight of the functional having smaller length by weight of constraints discarded by strategy $L1$.

On basis of this, paths of higher rank could be obtained, and, at the expense of this, a greater value by weight of the functional.

Denote $\overset{**\,r=q}{\mu}_{sj=\gamma}$ way rank $r=q$ with a maximum length $d_c\left(\overset{**\,r}{\mu}_{sj}\right)$ of ways $\left\{\overset{*\,r<q}{\mu}_{sj}\right\}$ rank $r<q$, corresponding to local extremes caused by $A0$ procedure using a strategy of $L1$. Then formulate a rule for elimination $L2$-dimensional problem based on the following theorem.

Theorem 1 column $D\Delta$ there is no way that satisfies properties v, rank $r<q$ for which the inequality $d_c\left(\overset{*\,r<q}{\mu}_{sj}\right)<d_c\left(\overset{**\,r=q}{\mu}_{sj=\gamma}\right)$.

Theorem 1 follows a strategy clipping $L2$, allowing mentioned functional way $\overset{**\,r=q}{\mu}_{sj}$ used as an upper estimate for elimination pathways in sets $m_{sj}^{r<q}$ column $D\Delta$. Strategy $L2$ used in constructing multistage algorithms.

Without prejudice strategies $L1$ and $L2$, you can enter additional sets a clipping paths m_{sj}^{r}. Representing strategy $L3$, which is based on the properties of the graph $D\Delta$ and is as follows. From the structure of the graph $D\Delta$ shows that for each of its vertices j, which corresponds to the region Ω_j weight γ_j is the sum of the coefficients sj functional (5), due to the rule:

$$\gamma_j=c_{j+1}+c_{j+2}+...+c_n,\ \gamma_n=0;\ \ j=\left(1,n\text{-}1\right), \tag{9}$$

represents the upper bound value increasing importance in local extremes Ω_j on all these levels.

Reducing the number of shaped paths μ_{sj}^{r} plural m_{sj}^{r} can be achieved if the conditions caused by the following fairly obvious statement 2.

Statement 2. If the total path length $d_c\left(\mu_{sj}^{r}\right)$ a subset of r m_{sj}^{r} w and in weight γ_w. This summit has received less than the maximum length $d_c\left(\mu_{sj=p}^{r}\right)$. Then the next rank ways that are based on μ_{sj}^{r}. Can not determine the optimal solution.

The validity of the assertion 2 follows from the fact that the strategy $A0$ procedure $L1$ selects global extreme of all the local and the maximum length by way of extension μ_{sj}^{r} there is less of a local extreme. Thus, test conditions:

$$d_c\left(\mu_{sp}^{r}\right)+\gamma_p<\max_{\{c_j\}}\left\{d_c\left(\overset{*\,r}{\mu}_{sp}\right)\right\}, \tag{10}$$

where $d_c\left(\mu_{sp}^{r}\right)$ – path length μ_{sp}^{r} the top rank pr weight c_j; avoids this path of further analysis as futile, if the condition is fulfilled. This strategy is based verification $L3$.

As a result of the procedure $A0$ strategies $L1$, $L3$ are set m_{sj}^r. For which $r > q$, and for effective filtration unpromising paths must be functional (5) assessment valuesin fields Ω_j, $j = \left(\overline{1, n^2/2}\right)$ at $r > q$. For this we introduce the strategy of choice from a plurality of paths $L4$, based procedure, which gives a maximum possible paths rank r in column $D\Delta$. It can be implemented if $D\Delta$ determine the shortest path weight restrictions based procedures $A0$ s between the top and all the other vertices of the graph $D\Delta$, and the recurrence relation (6) for a one-dimensional problem takes the following form:

$$\mu_{sp}^{r=r+1} = \min_{a_{ij}} \left\{ \mu_{sp}^r \bigcup (j.p) \right\}, p = (\overline{r+1, n}),\ j = (\overline{r, n}),\ i = 1. \tag{11}$$

It is easy to see that with this strategy, the formation of plural paths m_{sj}^r proposition 2 remains valid and elimination pathways in sets m_{sj}^r you can use the condition (11).

Implementing procedures $A0$ based strategies $L3$, $L4$ allows us to formulate more unpromising strategy $L5$ clipping paths in sets m_{sj}^r, due to the following theorem 2.

Theorem 2. If the set $m_{sj}^r, j = \left(\overline{r_{\max}, n}\right)$, the highest rank $r_{\max}$ built $A0$ procedure strategies $L3$, $L4$, choose the path μ_{sw}^r with the greatest value by weight functional (5) in case of repeated deci- sions outbound enough ways to form the first rank $r = 1$ in the set $m_{sp}^r, p = \left(\overline{1, k}\right)$, where:

$$k = w - r_{\max} + 1, \tag{12}$$

and w – number set m_{sp}^r with a maximum length by weight functional due to the first solution to the problem.

In a theorem 3 we formulate a rule that allows multiple m_{sj}^r provide a way $\overline{\mu}_{sj}^r$ length of $d_c\left(\overline{\mu}_{sj}^r\right)$, in relation to which all paths of length less than the value of the functional weight can be excluded from the analysis as unpromising.

Theorem 3. If you sort the set $m_{sj}^r, j = \left(\overline{r_{\max}, n}\right)$ rank r vectors in descending order by weight functional c_j, then the way in which the length $d_c\left(\mu_{sj}^r\right)$ less than the length $d_c\left(\min_{a_{ij}}\left(\mu_{sj}^r\right)\right)$ can not determine the optimal solution.

This theorem defines the corridor: in one-dimensional corridor set m_{sj}^r the set $m_{sp}^{r=r+1}$ we mean a set of paths μ_{sj}^r, who are between the upper limit set m_{sj}^r and its lower limit satisfying properties ν plural $m_{sp}^{r=r+1}$. The upper limit is determined by the maximum $d_c\left(\mu_{sj}^r\right)$ and the bottom – Theorem 3.

From concept corridor can propose the following strategy $L7$, which represents another strategy of choice routes r is set to from m_{sj}^r rank r in the set $m_{sp}^{r=r+1}$, $p = \left(\overline{1, n}\right)$ next rank choose paths that satisfy properties ν is the maximum weight cj functional and minimal weight restrictions aij, corresponding recurrence relations (9), (12).

A number of $\left\{L_w\right\}$ clipping strategies have been considered for the one-dimensional of integer linear programming with boolean variables. We formulate clipping strategies for m-dimensional problems.

If the solution m-dimensional problems of the most simple strategy is the strategy of choice $L10$, based on the recurrence ratio (9). The principle of forming paths in the identical strategy sets $L1$, except when necessary to carry out checks m times.

The combination strategy with the strategy $L7$, L3 in the case of m-dimensional problem $L11$ form a selection rule, which is to set out m_{sj}^{r} the set $m_{sp}^{r=r+1}$, $p=\overline{(1,n)}$. Next rank choose ways which satisfy properties ν is the maximum weight and minimum functional c_j for each i-th weight restrictions $a_{ij}, i=\overline{(1,m)}$.

The first corresponds recurrence relations (9) and the second is described by the following equation (13), based on the ratio (12):

$$\mu_{sp}^{r=r+1}=\min_{a_{ij}}\left\{\mu_{sj}^{r}\bigcup(j.p)\right\}, p=\overline{(r+1,n)},\ j=\overline{(r,n)}. \tag{13}$$

Enter by analogy with the concept of one-dimensional corridor concept m-dimensional corridor set m_{sj}^{r}.

Let subset of vectors that must remain in the set m_{sp}^{r} after filtering through m_{sp}^{rk}. Recall that the formation of a plurality of paths m_{sp}^{r} always carried out so that the length of the first functional weight are more functional length of the weight of the second and so on. e., that $d_c(\mu_k)\geq d_c(\mu_{k+1})\geq ...\geq d_c(\mu_n)$.

Procedure $A0$ strategies $\{L_w\}$ Kw and regulations can serve as a basis for constructing approximate and exact algorithms for solving the problem of the knapsack is to get different versions $A0$ procedures depending on the combinations used rules clipping $\{L_w\}$ unpromising paths insets μ_{sj}^{r} by applying the principle of optimization direction.

Approximate algorithms for solving the problem integer linear programming with boolean variables

The main qualifying features are the number of steps and the accuracy of the steps of solving the problem. By the first feature, the algorithms are divided into one-stage and multi-stage. This division means that the initial task can be solved one (one-stage) or several times (multi-stage) by different algorithms, the list of which is given in parentheses. The second sign determines the error of the received admissible solution of the problem by the weight of the functional from the optimal solution. If the algorithm is fundamentally unable to give an exact decision about the weights of the functional, then we will call such an algorithm approximate.

Algorithm $A1$. Consideration of approximate algorithms start with a one-dimensional problem. The simplest algorithm $A1$ is that the procedure is based on the $A0$ and implements strategies $L1$ and $L3$. His step description is as follows.

STEP 1. From the top of the set s built paths $m_{sj}^{r=1}$, $j=\overline{(1,n)}$ first rank r, satisfying the properties and determined to set $m_{sj}^{r=1}$ path of maximum length $\left\{\mu_{sj}^{*r}\right\}$ weight functional s_j. For each node j determined weightγj rule (10).

STEP 2. excluded paths $\left\{\mu_{sj}^{r}\right\}, p=\overline{(r,n)}$ plural m_{sj}^{r} current rank r, the length of which $d_c\left(\mu_{sp}^{r}\right)$ satisfying inequality (11).

STEP 3. Formed a set of paths $m_{sp}^{r=r+1}$, $p=\overline{(1,n)}$. next rank satisfying properties based on a plurality of paths m_{sj}^{r} previous rank based on recurrent ratio (9). In educated sets $m_{sp}^{r=r+1}$ distinguish longest path $\left\{\mu_{sp}^{*\,r=r+1}\right\}$ If several ways will be the maximum length, the path chosen among them with a lower value length weight restrictions a_{1j}.

STEP 4. Checks whether all paths set next $r=(r+1)$ rank is empty. If so, proceed to step 5; if not, check $r=(n-1)$. In the case of equality, go to step 5, otherwise increase r 1 and perform step 2.

STEP 5. Select the plural maximum path length and algorithm $A1$ terminates.

Getting close decision is due to the strategy of choice $L1$.

Algorithm $A2$. Another strategy is the strategy of choice routes $L4$, using an algorithm that allows $A2$ obtained by the maximum possible rank r in column $D\Delta$. It can be implemented if the D to determine the shortest path weight restrictions based procedures $A0$ between the top and the rest of s vertices D, using the recurrence relations (12) and, of course, clipping rule $L3$. Step by step description of the algorithm $A2$ is as follows.

STEP 1. From the top of the set s built paths $m_{sj}^{r=1}, j=\overline{(1,n)}$ first rank r, satisfying the properties and determined to set $m_{sj}^{r=1}$ path of maximum length $\left\{\mu_{sj}^{*\,r}\right\}$ weight functional s_j. For each node j determined weightγj rule (10).

STEP 2. Excluded paths a plurality m_{sj}^{r} Current rank r, the length of which $d_c\left(\mu_{sp}^{r}\right)$ satisfying inequality (11).

STEP 3. Formed a set of paths $m_{sp}^{r=r+1}$, $p=\overline{(1,n)}$. next rank satisfying properties based on a plurality of paths m_{sj}^{r} previous rank, who have a minimum value m_{sj}^{r} length weight restrictions based on recurrence relation (12). In educated sets $m_{sp}^{r=r+1}$ distinguish longest path $\left\{\mu_{sp}^{*\,r=r+1}\right\}$

STEP 4. Checks whether all paths set next $r=(r+1)$ rank is empty. If so, proceed to step 5; if not, check $r=(n-1)$. In the case of equality, go to step 5, otherwise increase r 1 and perform step 2.

STEP 5. Select the plural path length and the maximum number tops last w, belonging to this path, then the algorithm $A2$ terminates.

Algorithm $A3$**.** Based on the concept of corridor and $L7$ accordance with the strategy, the following approximate algorithm $A3$ solution which is to set out m_{sj}^{r} a plurality of rank r $m_{sj}^{r=r+1}, j=\overline{(r+1,n)}$ be chosen next rank up to two ways that satisfy properties ν.

The first is the path of maximum weight in functionality (5) (relative recurrence relation (9), and the second – the path with the least weight restriction on $\left\{a_{1j}\right\}$ (relatively recurrence relation (12) that appropriately change the step 3 algorithm $A1$. In another step description of the algorithm $A3$ coincides with the description of the algorithm $A1$. Loss optimum solution due to its falling into the corridor.

Algorithm $A4$. For multidimensional problem can also be similarly effective to construct approximate algorithms. This algorithm $A4$ is based on the strategy of $L10$, who set the current builds in rank rank next set $r=(r+1)$ path with a maximum length weight functional $\{c_j\}$.

This temporal complexity of the algorithm increases 2^m as necessary to execute each vector operations of addition m and m comparisons to ascertain whether satisfying vector corresponding to this path restriction or not. So step and $A4$ for algorithm description coincides with the algorithm $A1$.

Algorithm $A5$. Application strategy $L11$ allowed to build algorithm $A5$, the essence of which is the choice of each set m_{sj}^r Current rank r one way, maximum weight and functional, at worst, m routes, minimum weight limit satisfying properties v. Then, unlike algorithm $A1$, $A5$ algorithm step article describes changes to the following:

STEP 1. From the top of the set s built paths $m_{sj}^{r=1}, j=\overline{(1,n)}$ first rank r, satisfying the properties and determined to set $m_{sj}^{r=1}$ path of maximum length $\left\{{}^{*\,r}_{\mu_{sj}}\right\}$ weight functional. For each node j c_j weight is determined by the rule (10).

STEP 2. excluded paths a plurality m_{sj}^r Current rank r, length which $d_c\left(\mu_{sp}^r\right)$ satisfying inequality (11).

STEP 3. Formed a set of paths $m_{sp}^{r=r+1}$, $p=\overline{(1,n)}$. next rank satisfying properties based on a plurality of paths m_{sj}^r previous rank based on recursive relationships (9), (13). In educated sets $m_{sp}^{r=r+1}$ distinguish longest path $\left\{{}^{*\,r=r+1}_{\mu_{sp}}\right\}$ If you find some ways to the maximum length, the path chosen among them with a lower value length weight limit $\{a_{ij}\}$. If you find a number of ways with a minimum value for the i-th restriction, the chosen one has more weight functional length.

STEP 4. Checks whether all paths set next $r=(r+1)$ rank is empty. If so, proceed to step 5, if not, check $r=(n-1)$. In the case of equality, go to step 5, otherwise increase r on 1 and perform step 2.

STEP 5. Select the plural maximum path length and $A5$ algorithm terminates.

This algorithm has one uncertainty in the case when multiple vectors with maximum length by weight of the functional and with different values by weight of constraints are found in the set, ie, for example, by the weight of the first restriction more than the second vector, by the weight of the second restriction, by the weight of the third – again the second, etc.

Therefore, in order to avoid this uncertainty in the equality of lengths by weight of the functional path is chosen with a smaller value by weight of all restrictions. If this is not possible, then any is selected. It may be that the rejected path will belong to the optimal path. This fact is one of the reasons for the $A5$ algorithm approximation.

To check the correctness and accuracy of the solution by the developed algorithms $A1$ – $A5$ a modified Balash algorithm [3] is chosen as a standard, which takes into account the requirements of the coefficients in the functional. In the future, by D we will understand exactly this algorithm. In the course of

solving the test problems, coefficients were generated using the random number sensor in functional in the range [1÷100] and in the constraints of condition in the range [1÷10]. The choice of other ranges for the functional changed only its absolute value, but did not affect the parameters of the algorithms on average. Changing the range in constraints only affects the rank of the path (path rank is the number of vertices of the graph $D\Delta$ that make up that path).

The structure of the study of each algorithm was as follows. 1000 test problems were solved with given input parameters m and n by the selected algorithm. The performance of the algorithms was calculated during the decision. The values obtained were shown in the least squares approximated graphs.

All algorithms are divided into two groups. The first group consists of one-dimensional algorithms $A1$, $A2$, $A3$, which solve problems ILP with BV. The second group consists of m-dimensional algorithms $A4$, $A5$, that solve the problem.

Research algorithms of the first group. As it turned out, the quantitative values of the selected indicators depend significantly on the rank $\bar{r}$ f the resulting solution, which determines the number of units in the optimal solution. Figures 1 and 2 confirm this, depicting the time dependence of N_{on} algorithms on r with fixed values of input parameters n and $m = 1$.

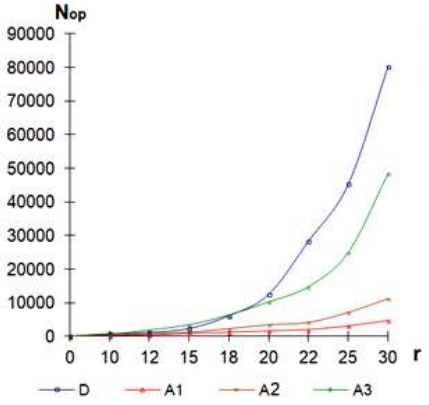


Figure 1. – The dependence of N_{op} on $\bar{r}$ when $n = 15$

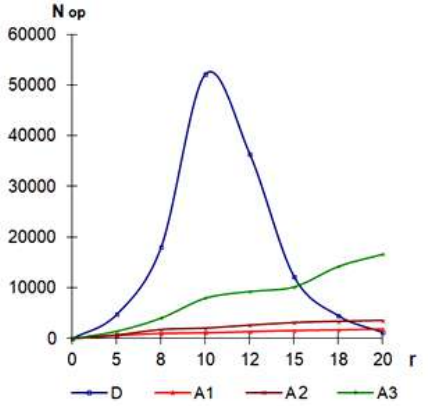


Figure 2. – The dependence of N_{op} on $\bar{r}$ when $n = 20$

The (Fig. 1 and 2) show that the range of variation $\bar{r}$ can be divided into three zones: zone 1 – $\bar{r} = [0 \div n/3]$; 2 zone – $\bar{r} = [n/3 \div 2n/3]$; zone 3 – $\bar{r} = [2n/3 \div n]$. In the first zone, algorithm $D\Delta$ finds the solution quickly, because at the expense of probing the branches of the decision tree corresponding to a single branch are very effectively cut off. Similarly, the fast solution in 3 zone is explained, the vectors in which consist of a large number of unit. The manifestation of all the exponential complexity of algorithm $D\Delta$ occurs in the second zone. For algorithms $A1$, $A2$, $A3$, the increase in the number of N_{on} with

increasing $\bar{r}$ is determined by the number of local areas W that need to be processed. According to the expression the number of regions in the W column $D\Delta$ does not exceed $n^2/2$, so $r \to n$ nop increase in the number does not exceed $c \cdot n^2$, where c = const.

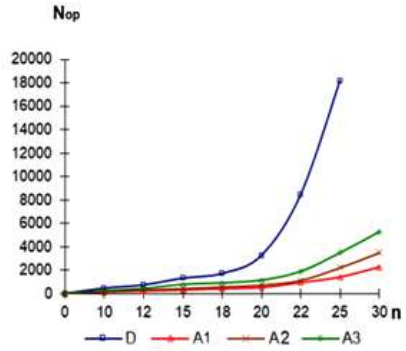


Figure 3. – The dependence of N_{op} on n for zone 1

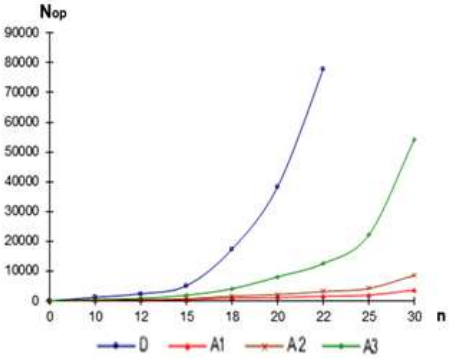


Figure 4. – The dependence of N_{op} on n for zone 2

Thus, for objective comparison of algorithms it is necessary to specify in which zone they belong, that is, what percentage of units (or zeros) contains the optimal solution. According to the division into zones, we plot the dependence of the number $N_{оп}$ on n for each zone. These dependencies for zones 1, 2 and 3 are shown in (Fig. 3–5). Figures 3, 4, 5 show that in order to compare the time indices of the algorithms it is necessary to clearly indicate the belonging to the conditional zones, since the absolute value of these indicators in the zones differs significantly. The hit of a solution of a problem in any zone is precisely determined by the ratio of the range of change of coefficients a_{1j} and the given range for b_1 on the right-hand side of inequality.

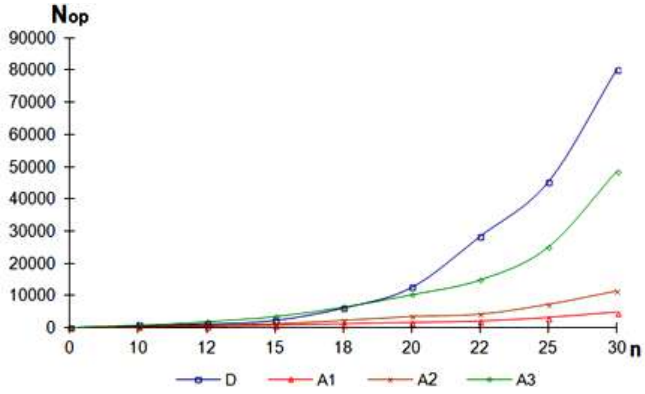


Figure 5. – The dependence of N_{op} on n for zone 3

The amount of RAM V required depends on the specific software implementation. The quantitative values of this indicator, of course, can be changed and directly depend on the skill of the programmer. However, the appearance of the curves does not change due to the nature of the processes they describe.

We show that the amount of RAM required to store the set of m_{sj}^{r} vectors of the graph $D\Delta$ also depends on the average rank of the optimal solution of the test problem. The dependence $V = f(n)$ for the algorithms D, $A1$, $A2$, $A3$ is plotted (figures 6 and 7).

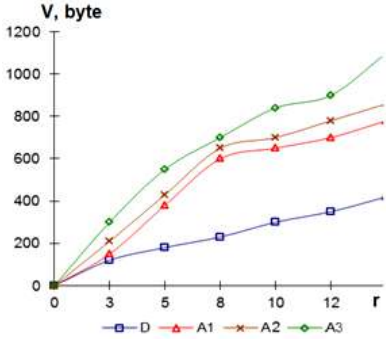


Figure 6. – Effect $\bar{r}$ the V for $n = 15$

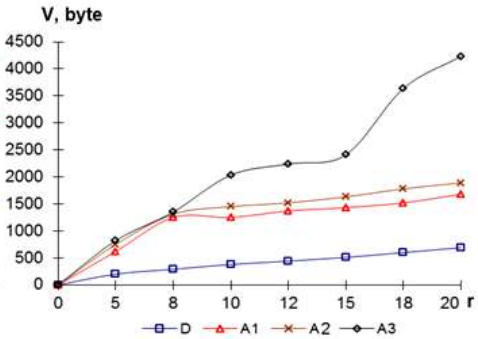


Figure 7. – Effect $\bar{r}$ the V for $n = 20$

The smaller value of the required amount of RAM for algorithm D is explained by the fact that in case of successful probing by the relations (7) and (8) of subsets of alternatives, a new task, and therefore a new record in memory, is not formed because the free list is adjusted vertices for the selected task.

Only the formation of a new branch, which corresponds to step 6 of the algorithm, requires the amount of RAM. For algorithms $A1, A2, A3$ the maximum number of processed vectors stored in the second area.

Therefore, more storage is required than the first zone. The maximum value of the cost is reached in the third zone, since in this case the difference in the weight of the functional within the sets is insignificant, which leads to inefficient screening of vectors according to the strategy $L3$.

The dependence of the value of V on the size of the input parameter n also does not exceed $c \cdot n^2$. The results of this study are shown in (Fig. 8–10), corresponding to zones 1–3.

The temporal complexity of the $A1$ and $A3$ algorithms is easy enough to estimate theoretically. The analysis of each $\vec{x}$ vector involves one addition operation and one comparison operation, that is, two elementary operations.

The maximum number of vectors in the worst case will be in the second rank and is $n^2 / 2$. The number of such ranks in the graph $D\Delta$ is n. Therefore, the time complexity of Algorithm $A1$ will be $O\left(2n \cdot \frac{n^2}{2}\right) = O(n^3)$, to store vectors in the Ω-regions at all ranks will require memory of no more than $O(n^3)$.

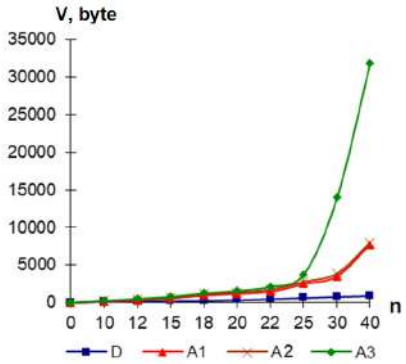


Figure 8. – The dependence of V on n for zone 1

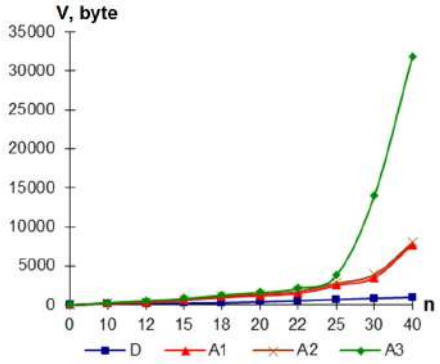


Figure 9. – The dependence of V on n for zone 1

The estimate of the time complexity of the $A2$ algorithm coincides with the estimate for the $A1$ algorithm.

Let estimate the time complexity of algorithm $A3$. The time complexity of algorithm $A1$ is $O(n^3)$. However, in algorithm $A3$ each set will contain, after isolation of the corridor and filtering in the worst case, two ways, which will increase the time complexity of algorithm $A3$ twice and will be $O\left(2 \cdot n^3\right) \approx O\left(n^3\right)$.

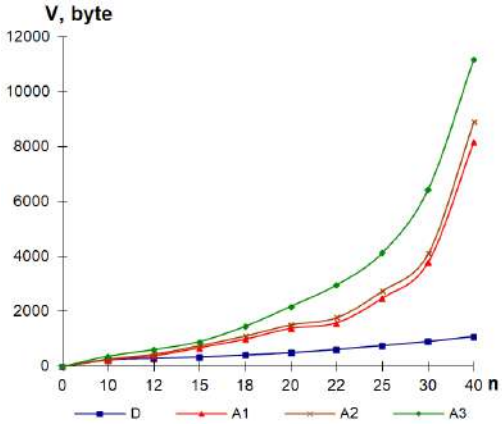


Figure 10. – The dependence of V on n for zone 3

Therefore, hardware costs for storing vectors will also double and add up to $O\left(2 \cdot n^3\right) \approx O\left(n^3\right)$.

One of the important characteristics of approximate algorithms is the relative error Δf, which it gives in the case of solving the problem. From these algorithms approximate are $A1$ and $A3$. The relative error depends on the area in which the optimal solution falls. However, obtaining inaccurate solutions by $A1$ and $A3$ algorithms for different zones proved to be a problematic task on average.

Thus, for zone 1, the exponential growth of vectors in the graph $D\Delta$ encounters a constraint, and therefore in optimal sets the optimal paths will dominate the functional weight In zone 3, the optimal path will be along the higher vertices of $D\Delta$, which will not allow it to be cut off.

Therefore, Figures 11, 12 show the variation of the error f and the K_n factor depending on the dimension n only for the second zone.

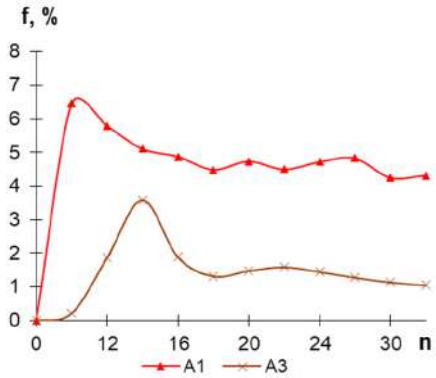


Figure 11. – The dependence of f on n for zone 2

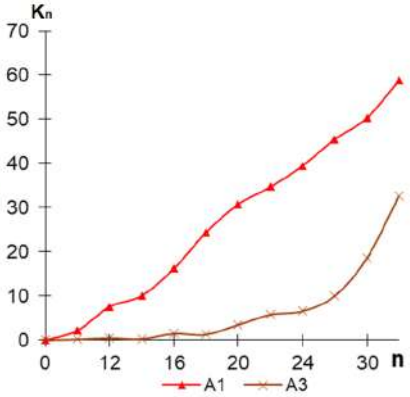


Figure 12. – The dependence of K_n on n for zone 2

As can be seen from (Figures 11, 12) for both $A1$ and $A3$ algorithms the average error f stabilizes: about 5% for the first algorithm and about 2% for the second at $n > 25$.

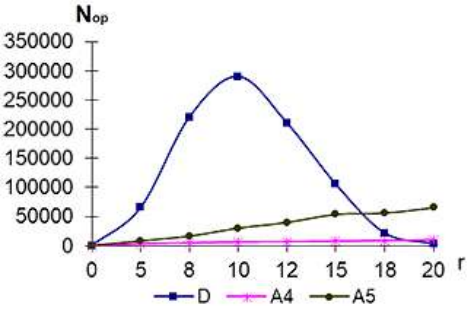


Figure 13. – The dependence of N op on $\bar{r}$ for $n = 20$ and $m = 5$

Research of algorithms of the second group. Let us evaluate the properties of the algorithms of the second group $A4$, $A5$ according to the selected performance indicators. The algorithms $A4$ and $A5$ are approximate. As for one-dimensional tasks, the values of these indicators depend on, $\bar{r}$ which is confirmed by the graph in (Figure 13). The curves in this figure are identical in shape to the corresponding indices of one-dimensional algorithms. Therefore, the division by zones is valid and

for multidimensional algorithms; the dependencies of the selected metrics on n for each zone also coincide with the corresponding dependencies for the one-dimensional algorithms. Due to the need to perform m times of verification of condition, the time complexity of the algorithm $A4$ will be $O\left(2 \cdot m \cdot n^3\right) \approx O\left(m \cdot n^3\right)$.

The time complexity of the algorithm $A5$ due to the chosen strategy $L11$ in m times larger than the time complexity of the algorithm $A4$ and is $O\left(m \cdot n^3 \cdot m\right) = O\left(m^2 \cdot n^3\right)$, since it is necessary to choose from each set according to relation (13), in the worst case, m more vectors. Therefore, the amount of memory hardware used to store the paths will also increase by a factor of m to $O\left(m \cdot n^3\right)$.

When m = 5, the errors of the $A4$ and $A5$ algorithms were investigated. The dependence of f and Kn on n and m for zone 2 are plotted in (Figure 14).

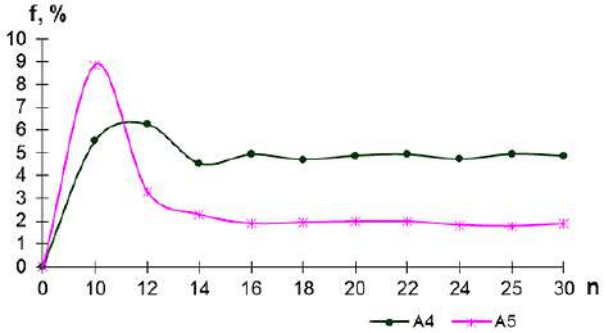


Figure 14. – The dependence of f on *n* for zone 2

Comparing Figure 11 and Figure 14, it can be seen that the relative error f does not depend on m, but depends only on the algorithm selected. Thus, it can be argued that the $A4$ algorithm has an error of 5% and the $A5$ algorithm of 2%.

Conclusions

An official model approach for solving integer programming with boolean variables has been developed Put $A0$ standard procedure that determines the rules of formation sets in box recovered $D\Delta$ and selecting options for solving the problem.

$A0$ procedures clipping for non-promising solutions are formulated based on a strategy that avoids the complexity of NP programming problems with integer boolean variables and provides an approximate solution

References:

1. Listrovoy S. V., Golubnichiy D. Yu., Listrovaya E. S. Solution method on the basis of rank approach for integer linear problems with boolean variables. Engineering Simulation. 1999. – Vol. 16. – P. 707–725.
2. Listrovoy S. V., Tretjak V. F., Listrovaya A. S. Parallel algorithms of calculation process optimization for the boolean programming problems. Engineering Simulation. 1999. – Vol. 16. – P. 569–579.

3. Tretiak V. F., Pashneva A. A. Optimizatsiya struktury khranilishcha dannykh v uzlakh seti infokommunikatsionnoi seti oblachnogo khranilishcha // Sistemy navigatsii i svyazi Poltavskogo natsional'nogo universiteta imeni Yuriya Kondratyuka. – № 4(44), 2017. – P. 122–128.

CHAPTER IV. PROJECT MANAGEMENT AND SOFTWARE ENGINEERING

Static and dynamic models for planning the quality improvement of the software development process

Anna Goloskokova
Doctor of Philosophy in Technical Science, Associate Professor
Department of Software Engineering and Management Information Technologies
National Technical University "Kharkiv Polytechnic Institute"
ORCID: https://orcid.org/0000–0001–9012–7889

Volodymyr Fedorchenko
Doctor of Philosophy in Technical Science, Associate Professor
Department of Information Systems
Simon Kuznets Kharkiv National University of Economics
ORCID: http://orcid.org/0000–0001–7359–1460

Abstract. *In the work the important scientific and practical task for the quality improvement of the software development process is solved based on the maturity model Capability Maturity Model Integration (CMMI) using the rolling planning. The analysis of the current problems in the quality improvement of the software development process has been done. Taking into account analyzed issues, the problem of the method development for the quality improvement of the software development process has been set. The method is based on the rolling planning and allows reducing the dimensionality of the task by the dynamic model simplification, and increasing the accuracy of the result due to the static model. In order to increase the speed of "Kiev broom" algorithm, which is related to the method of the sequential analysis of the alternatives, the technology of oriented search of the alternatives at each algorithm's stage has been improved by solving the set of optimization problems of Boolean programming.*

Keywords: *software development process, maturity model, rolling planning, dynamic model, static model, utility theory*

Introduction

An emphasis was made on the problem of product and service quality at all times. This concept has been changed eventually from the quality of a particular

product or service to the Total Quality Management (TQM). According to the TQM ideology and software engineering, there are four components of the software quality.

1. Quality management of the "input" – the stage of collecting and modeling of the software customer requirements.

2. Quality management of "resources", which are used for software developing – at this stage, it is necessary to allocate financial resources, which are the basis of the technical and organizational support forming, as well as qualified staff.

3. Quality management of the software development process. The first step of problem-solving is to evaluate the initial state of the software development process. Its improvement is the implementation of some set of measures, which are aimed at the software characteristics improvement. Success criteria of these measures are the characteristics of the software development process, rather than the characteristics of the software being developed.

4. Quality management of the "output". The output of the development process is a complete software product or its functionality.

In software engineering, quality metrics are used to measure these components. Metric is a combination of a specific method of the attribute measuring and scale measurement. The ISO / IEC9126–2 standard recommends the usage of five types of scales: nominal, ordinal, interval, relative and absolute.

The important component of the TQM of software development is the software development process itself. The main improving steps of the software systems life cycle (LC) processes are specified in the standard ISO / IEC TR15504–7: initiation of process improvement; assessment of the multiplicity of those processes, the improvement of which can be beneficial; formation of an improving plan-program under the conditions of limited resources; improvements execution according to the plan; confirmation of improvements; support of a new level of LC processes; monitoring of processes execution.

A large number of scientific studies are devoted to the evaluation of SDP state. Some of them evaluate particular LC processes, others estimate the totality of processes, or evaluate the software development process at the level of the software development organization.

However, almost a matter of scientific studies are devoted to solving the problem of the software development process quality improving by mathematical models developing that allow, under the conditions of limited resources, to determine the optimal plan for software development process improvement according to the standard ISO / IEC TR15504–7.

Therefore, the development of the method and models for the quality improvement of the software development process is an actual applied-researched task, which determined the research area of this inquiry.

Statement of the problem

Object of research is a software development process (SWDP).

Subject of research is current planning models, a dynamic model and an information technology for the quality improvement of the SWDP, based on the rolling planning method.

The purpose of this research is the quality improvement of the software development process based on the development of the optimal program for the software development promotion to a higher maturity level of the organization using the maturity model CMMI and the rolling planning method.

To achieve the goal, the following tasks are set:

- to analyze the current state of the SWDP quality improvement problems;
- to develop at the verbal level the method of the SWDP promotion to a higher maturity level of the organization, based on the rolling planning technology;
- to formalize the developing problem of the method for planning of the SWDP quality improvement and to develop appropriate static models for SWDP maturity increasing based on the utility theory;
- to improve the dynamic model and the sequential analysis of the variants method "Kiev broom" in relation to the SWDP quality improvement problem solution by the optimization tasks set solving at each stage.

Analysis of the SWDP quality improvement problems

The analysis showed that the current state of the problem of the program system (PS) quality improvement, and, in particular, of the SWDP is at an initial stage, which corresponds to the verbal description of the well-known maturity models of CMMI, SPICE and other less well-known models that allow evaluation of the SWDP maturity level, hence the PS quality. As an example, the structure of the CMMI model is shown in Fig. 1. By the time being, rather a small amount of scientific researches is devoted to the SWDP quality improvement problem solution based on the development of its mathematical models under the conditions of the limited resources.

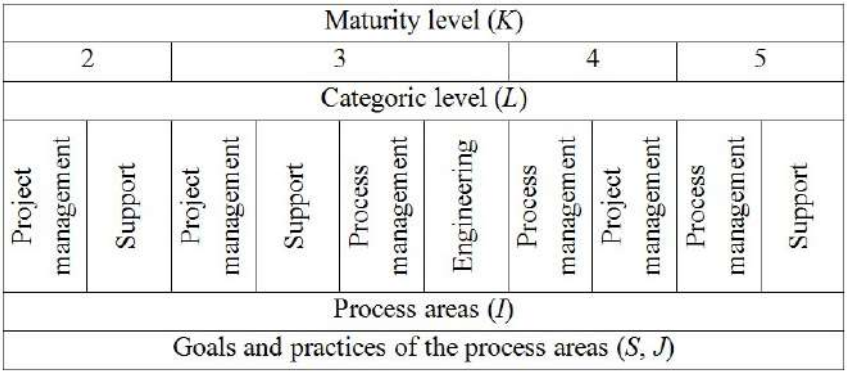


Figure 1. – Structure of the general concepts of the CMMI model

Conducted analysis of the problems, which exist in the software engineering with regard to SWDP quality improvement, showed, that the main models of SWDP quality assessment are CMMI and SPICE, which describe the quality of the SWDP at the verbal level. It does not allow the developing of the mathematical models for quality level increasing, based on them. The first attempts in this direction showed that the developed models and algorithms did not allow to solve the problem at a reasonable amount of time.

Therefore, the task is to study the problems identified during the analysis of the SWDP as a study object. The main of these problems is to increase the adequacy of the developed models to the real SWDP based on the method of rolling planning and to increase the speed of the sequential analysis of the alternatives algorithm.

Static model development of the SWDP quality improvement under current planning

According to the problem statement, it is proposed to consider two problems under paradigm of the sliding method: static and dynamic. In the static statement based on the SWDP initial state and a target profile, taking into account resource constraints, the optimal variant of the organization's progress towards the goal is determined, or a compromise between the achievement degree of the target profile and required resources is found [1]. In dynamically statement the problem of the optimal alternative of the SWDP advancement in a particular planning period [0, T] to a higher quality level arises, where T is the duration of the considered planning period [2]. In the research, the level of quality is characterized by alternative options for the SWDP advancement up to a higher maturity level according to the CMMI model. From the decision making theory point of view, each alternative option for the SWDP quality improvement is determined by three generalized criteria:

1) the degree of the stated objectives achievement, which is connected with a certain target profile of the SWDP;

2) the needed resources to achieve the goal, in the study the financial resources and employees of the company hours worked are considered, which are necessary for the SWDP advancement to a higher level of maturity;

3) the needed time to solve the task.

Based on the structure of the CMMI model (Fig. 1), which is presented in the form of the concepts hierarchy, there are practices at the lowest level, each of which is characterized by a specific capability level. The paper introduces discrete variables $x_{is}^{j}(t)$ that acquire integer values, each of which corresponds to the capability level of the j-th practice in the t-th subperiod, which is involved to ensure the achievement of the s-th goal of the i-th process area. The variable

$$Z_i\left(\left\{x_{is}^{j}(t)\right\}\right) = F_i\left(f_{is}\left(\left\{x_{is}^{j}(t)\right\}\right)\right), \quad (1)$$

in turn, determines the capability level of the i-th process area in the t-th subperiod, where f_{is} – the transforming function of the capability levels of the partial practices, which ensures the achievement of the s-th goal of the i-th process

area, and F_i – is a function of the i-th process area. Further Z_i we will call the criterion.

According to the concepts hierarchy of the CMMI model, the following notation has been introduced:

J_i^s – a set of practices of the s-th goal of the i-th process area;

S_i – a set of goals of the i-th process area;

I_k^l – a set of process areas that belong to the l-th category of the k-th maturity level;

L_k – a set of categories of the k-th maturity level;

K – a set of maturity levels.

Based on (1), the utility functions P_{i1} of the partial criteria at the level of process areas has been formed, which contribute to the achievement of a particular maturity level of the organization SWDP:

$$P_{i1}\left(Z_i\left(\left\{x_{is}^j(t)\right\}\right)\right)=\left(\frac{Z_i\left(\left\{x_{is}^j(t)\right\}\right)-Z_i^H}{Z_i^H-Z_i^H}\right)^{\alpha_{i1}}, \qquad (2)$$

where Z_i^H , Z_i^H – the best and, accordingly, the worst value of the i-th criterion. Z_i^H is determined by the initial state of the SWDP, i.e. $Z_i^H = F_i\left(\left\{x_{is}^j(0)\right\}\right)$. $\left\{\overline{\overline{x}}_{is}^j\right\}=\left\{x_{is}^j(0)\right\}$ for a static statement of a problem. In turn, Z_i^H is determined on the basis of the target profile, i.e. $Z_i^H = F_i\left(\left\{\overline{x}_{is}^j\right\}\right)$. The parameter α_{i1} defines the appearance of the dependence of the utility function: the dependence is convex up, if $0<\alpha_{i1}<1$; it is linear, if $\alpha_{i1}=1$; it is convex to the bottom, if $\alpha_{i1}>1$.

The criterion (2) are related to the SWDP maturity level and determine the achievement degree of the target profile by its particular components. As stated above, two kinds of resources are used to achieve the goal: the financial expenses for transition of the j-th practice of the i-th process area to a higher capability level and time associated with mastering the new skills, tools and technologies used when implementing SWDP.

Thus, the synthesis problem of the criteria and resource utilization of the resource functions is raised. For their formation, the SWDP information is required on the $(t-1)$-th subperiod state $\left\{x_{is}^j(t-1),\ j\in J_i^s,\ s\in S_i\right\}$ and on the t-th subperiod $\left\{x_{is}^j(t),\ j\in J_i^s,\ s\in S_i\right\}$. At the same time for the static statement of the problem $x_{is}^j(t)=\overline{x}_{is}^j$.

For each j-th practice of the i-th process area a set of Boolean variables $\left\{\lambda_{is}^j(v), v\in\left[x_{is}^j(t-1),\overline{x}_{is}^j\right]\right\}$ had been used and its corresponding set of financial resources values $(\tau=2)$ and time resources $(\tau=3)\left\{r_{is}^{j\tau}(v), v\in\left[x_{is}^j(t-1),\overline{x}_{is}^j\right]\right\}, \tau=2,3$, which are required for transition from a specific fixed state $x_{is}^j(t-1)$ to a new state of the j-th practice $x_{is}^j(t)$ under the condition $x_{is}^j(t-1)\le x_{is}^j(t)\le\overline{x}_{is}^j$. The variables $\lambda_{is}^j(v)$ do not have a time index, since they are not used in the dynamic statement of the problem. At that, $\lambda_{is}^j(v)$ equals 1 in the case when a capability level of the j-th practice at the t-th sub-period acquires a value equals v, otherwise it equals

0. If j-th practice at the t-th sub-period does not transit to a new capability level, it means that $v = x_{is}^{j}(t-1)$ and $r_{is}^{j\tau}(v) = 0, \tau = 2,3$.

Essential resourcing for each practice in the transition to a new capability level at the t-th subperiod is written using the mentioned symbols

$$\overline{R}_{is}^{j\tau}\left(\left\{\lambda_{is}^{j}(v)\right\}\right) = \sum_{v=x_{is}^{j}(t-1)}^{\overline{x}_{is}^{j}} r_{is}^{j\tau}(v)\cdot\lambda_{is}^{j}(v), \quad \tau = 2,3; \quad \sum_{v=x_{is}^{j}(t-1)}^{\overline{x}_{is}^{j}} \lambda_{is}^{j}(v) = 1.$$

As a result, in the transition of the i-th process area to a higher capability level resources are spent in such volumes

$$R_{i\tau}\left(\left\{\lambda_{is}^{j}(v)\right\}\right) = \sum_{s\in S_i}\sum_{j\in J_i^s}\overline{R}_{is}^{j\tau}\left(\left\{\lambda_{is}^{j}(v)\right\}\right), \quad \tau = 2,3.$$

By analogy with (2) introduced

$$P_{i\tau}\left(R_i\left(\left\{\lambda_{is}^{j}(v)\right\}\right)\right) = \left(\frac{R_{i\tau} - R_{i\tau}\left(\left\{\lambda_{is}^{j}(v)\right\}\right)}{R_{i\tau}}\right)^{\alpha_{i\tau}}, \quad \tau = 2,3, \tag{3}$$

where P_{i2}, P_{i3} – utility functions, respectively, for the first and second types of resources;

parameters $\{\alpha_{i\tau}\}$ have the same type and purpose as $\{\alpha_{i1}\}$, $R_{i\tau}$ when $\tau = 2,3$ – have the worst maximum values, respectively, for the two types of resources to which the minimum values $P_{i\tau} = 0$, $\tau = 2,3$ are corresponded.

Based on the utility functions of the process areas, the static problem of the planning for the SWDP quality improvement, which has a vector target function, is formalized.

$$\Phi\left(\left\{x_{is}^{j}\right\}, \left\{\lambda_{is}^{j}(v)\right\}\right) = \left\{\widehat{W}_1^{l}\left(\left\{x_{is}^{j}\right\}\right), W_2^{l}\left(\left\{\lambda_{is}^{j}(v)\right\}\right), W_3^{l}\left(\left\{\lambda_{is}^{j}(v)\right\}\right), l\in L\right\} \tag{4}$$

and three groups of constraints.

1. Constraints which are imposed on the model target function variables directly:

$$\underline{\overline{x}}_{is}^{j} \le x_{is}^{j} \le \overline{\underline{x}}_{is}^{j}, \quad x_{is}^{j} \in \{0,1,2,3\}; \tag{5}$$

$$\sum_{v=\underline{\overline{E}}_{is}^{j}}^{\overline{\underline{E}}_{is}^{j}} \lambda_{is}^{j}(v) = 1, \quad \lambda_{is}^{j}(v) \in \{0,1\}. \tag{6}$$

2. Constraints which connect discrete integer variables $\left\{x_{is}^{j}\right\}$ and boolean variables $\left\{\lambda_{is}^{j}(v)\right\}$

$$x_{is}^{j} = \sum_{v=\underline{\overline{x}}_{is}^{j}}^{\overline{\underline{x}}_{is}^{j}} \left(v\cdot\lambda_{is}^{j}(v)\right), \tag{7}$$

where

$$j\in J_i^s, \quad s\in S_i, \quad i\in I_k^l, \quad l\in L_k, \quad k\in K. \tag{8}$$

3. Constrains to the financial resources

$$\sum_{k\in K}\sum_{l\in L_k}\sum_{i\in I_k^l} R_{i2}\left(\left\{\lambda_{is}^{j}(v)\right\}\right) \le R, \tag{9}$$

where R – financial resources, which were allocated for the considered first planning period.

The utility function of the goal achievement degree at the level of a particular l-th category of the CMMI model has the form

$$\widehat{W}_1^l\left(\left\{x_{is}^j\right\}\right)=\sum_{k\in K}\delta_{k1}^l Q_{k1}^l\left(\left\{x_{is}^j\right\}\right),\ \delta_{k1}^l\ge 0,\ k\in K,\ \sum_{k\in K}\delta_{k1}^l=1,\ l\in L,\ L=\bigcap_{k\in K}L_k,$$

where

$$Q_{k1}^l\left(\left\{x_{is}^j\right\}\right)=\sum_{i\in I_k^l}\gamma_{i1}^{lk}P_{i1}\left(\left\{x_{is}^j\right\}\right),\quad \gamma_{i1}^{lk}\ge 0,\quad i\in I_k^l,\quad \sum_{i\in I_k^l}\gamma_{i1}^{lk}=1,\quad l\in L_k,\quad k\in K,$$

$$Z_i\left(\left\{x_{is}^j\right\}\right)=\sum_{s\in S_i}\overline{\beta}_{is}\left(\sum_{j\in J_i^s}\overline{\alpha}_{is}^j x_{is}^j\right),\quad i\in I_k^l,\quad l\in L_k,\quad k\in K.$$

The two subgroups of the second group of utility functions, namely financial expenses and time resources at the level of a particular l-th category of the CMMI model, are written as follows:

$$W_\tau^l\left(\left\{\lambda_{is}^j(v)\right\}\right)=\sum_{k\in K}\delta_{k\tau}^l Q_{k\tau}^l\left(\left\{\lambda_{is}^j(v)\right\}\right),\quad \delta_{k1}^l\ge 0,\quad k\in K,$$

$$\sum_{k\in K}\delta_{k\tau}^l=1,\quad l\in L,\quad L=\bigcup_{k\in K}L_k,\quad \tau=2,3.$$

$$Q_{k\tau}^l\left(\left\{\lambda_{is}^j(v)\right\}\right)=\sum_{i\in I_k^l}\gamma_{i\tau}^{lk}P_{i\tau}\left(\left\{\lambda_{is}^j(v)\right\}\right),$$

$$\gamma_{i\tau}^{lk}\ge 0,\quad i\in I_k^l,\quad \sum_{i\in I_k^l}\gamma_{i\tau}=1,\quad l\in L_k,\quad k\in K,\quad \tau=2,3.$$

The sets of importance weight coefficients $\left\{\overline{\alpha}_{is}^j\right\}$, $\left\{\overline{\beta}_{is}\right\}$, $\left\{\delta_{k\tau}^l\right\}$, $\left\{\gamma_{i\tau}^{lk}\right\}$ are determined on the basis of the collective expert evaluation methodology (CEEM) [3].

Three problems of multicriteria optimization, which are most relevant for practical usage, are considered in this paper. One of them has the following stating. Find the optimal value of the generalized target utility function, which includes the integral target functions of the utility of the two groups of criteria of the CMMI model with weighted coefficients $\overline{\rho}_1$ and $\overline{\rho}_2$, as a result of the following problem solving

$$V\left(\left\{x_{is}^j\right\},\left\{\lambda_{is}^j(v)\right\}\right)=\left[\overline{\rho}_1\cdot\overline{V}_1\left(\left\{x_{is}^j\right\}\right)+\overline{\rho}_2\cdot\overline{V}_2\left(\left\{\lambda_{is}^j(v)\right\}\right)\right]\to\max_{\left\{x_{is}^j\right\},\left\{\lambda_{is}^j(v)\right\}}\qquad(10)$$

with the constraints (5)–(9) and $\overline{\rho}_1,\ \overline{\rho}_2\ge 0,\quad \overline{\rho}_1+\overline{\rho}_2=1$.

The components of the target function (10) are defined as follows:

$$\overline{V}_1\left(\left\{x_{is}^j\right\}\right)=\sum_{l\in L}\eta_1^l\cdot\widehat{W}_1^l\left(\left\{x_{is}^j\right\}\right),\quad \overline{V}_2\left(\left\{\lambda_{is}^j(v)\right\}\right)=\sum_{l\in L}\eta_2^l\cdot\widehat{W}_2^l\left(\left\{\lambda_{is}^j(v)\right\}\right),$$

$$\eta_\tau^l\ge 0,\quad l\in L,\quad \sum_{l\in L}\eta_\tau^l=1,\quad \tau=1,2,$$

$$\widehat{W}_2^l\left(\left\{\lambda_{is}^j(v)\right\}\right)=\mu_2^l\cdot W_2^l\left(\left\{\lambda_{is}^j(v)\right\}\right)+\mu_3^l\cdot W_3^l\left(\left\{\lambda_{is}^j(v)\right\}\right),\ \mu_2^l,\mu_3^l\ge 0,\quad \mu_2^l+\mu_3^l=1,\quad l\in L.$$

The set of importance weight coefficients $\left\{\overline{\rho}_i\right\}, \left\{\eta_i^l\right\}, \left\{\mu_i^l\right\}$ are determined based on the CEEM as previously.

Advancement of the dynamic model and the consecutive analysis of the alternatives algorithm for the SWDP improvement. As well as for the static statement of the problem, the utility function of the two groups of criteria is used: the achievement degree of the target profile and resourcing (the finances and time – working hours of the company employees).

Utility functions of the specific criteria for the achievement degree of the target profile are determined based on (2). Then, the value of the utility function of the increment at the t-th scheduling sub-period for each analyzed process area and, accordingly, a separate category within the k-th maturity level is written as follows:

$$\Delta P_{i1}^t\left(\left\{x_{is}^j(t-1), x_{is}^j(t)\right\}\right) = P_{i1}\left(\left\{x_{is}^j(t)\right\}\right) - P_{i1}\left(\left\{x_{is}^j(t-1)\right\}\right), \quad t \in [1,T];$$

$$\Delta Q_{k1}^{lt}\left(\left\{x_{is}^j(t-1)\right\}, \left\{x_{is}^j(t)\right\}\right) = \sum_{i \in I_k^l} \gamma_{i1} \Delta P_{i1}^t\left(\left\{x_{is}^j(t-1)\right\}, \left\{x_{is}^j(t)\right\}\right), \quad l \in L_k, k \in K, t \in [1,T],$$

and increment values of utility functions, respectively, at the level of certain categories of the model CMMI and at the level of whole SWDP have the form:

$$\Delta W_1^{lt}\left(\left\{x_{is}^j(t-1)\right\}, \left\{x_{is}^j(t)\right\}\right) = \sum_{k \in K} \delta_{k1}^l \Delta Q_{k1}^{lt}\left(\left\{x_{is}^j(t-1)\right\}, \left\{x_{is}^j(t)\right\}\right), \quad l \in L, \quad t \in [1,T];$$

$$\Delta V_1^t\left(\chi(t-1), \chi(t)\right) = \sum_{l \in L} \eta_1^l \Delta W_1^{lt}\left(\left\{x_{is}^j(t-1)\right\}, \left\{x_{is}^j(t)\right\}\right), \quad t \in [1,T],$$

where matrices are introduced to simplify subsequent entries $\chi(t) = \left\{x_{is}^j(t)\right\}, t \in [0,T]$.

To form the utility function of resourcing, as well as the increment value of the transition from $(t-1)$-th to the t-th planning period, two triangular matrixes of resources were introduced, the elements of which $r_{is}^{j\tau}(i,j)$ determine the required financial resources $(\tau = 2)$ and time resources $(\tau = 3)$ when transiting from the capability level $x_{is}^j(t-1)$ to the capability level $x_{is}^j(t)$ (Table 1). The variables $\left\{x_{is}^j(t)\right\}$ acquire the values of integers and satisfy the condition

$$x_{is}^j(t) \in [0,3], \quad j \in J_i^s, \quad s \in S, \quad i \in I_k^l, \quad l \in L_k, \quad k \in K, \quad t \in [0,T]. \qquad (11)$$

The resources that are required when transiting from $(t-1)$-th to the t-th period of the planning period at the level of the i-th process area and the increment value of the corresponding utility function are determined based on the following equation (Table 1):

$$R_{i\tau}\left(\left\{x_{is}^j(t-1)\right\}, \left\{x_{is}^j(t)\right\}\right) = \sum_{s \in S_i} \sum_{j \in J_i^s} r_{is}^{j\tau}\left(x_{is}^j(t-1), x_{is}^j(t)\right),$$

$$\Delta P_{i\tau}^t\left(\left\{x_{is}^j(t-1)\right\}, \left\{x_{is}^j(t)\right\}\right) = \frac{R_{i\tau}\left(\left\{x_{is}^j(t-1)\right\}, \left\{x_{is}^j(t)\right\}\right)}{\left(R_{i\tau} - R_{i\tau}^{\%}\right)},$$

$$\tau = 2,3, i \in I_k^l, l \in L_k, k \in K, t \in [1,T].$$

Table 1. – Resource matrix for the j-th practice

$x_{is}^{j}(t)$ / $x_{is}^{j}(t-1)$	0	1	2	3
0	$r_{is}^{j\tau}(0,0)=0$	$r_{is}^{j\tau}(0,1)$	$r_{is}^{j\tau}(0,2)$	$r_{is}^{j\tau}(0,3)$
1	0	$r_{is}^{j\tau}(1,1)=0$	$r_{is}^{j\tau}(1,2)$	$r_{is}^{j\tau}(1,3)$
2	0	0	$r_{is}^{j\tau}(2,2)=0$	$r_{is}^{j\tau}(2,3)$
3	0	0	0	$r_{is}^{j\tau}(3,3)=0$

The utility function amount of change of a particular category within the k-th maturity level has the form

$$\Delta Q_{k\tau}^{lt}\left(\left\{x_{is}^{j}(t-1)\right\},\left\{x_{is}^{j}(t)\right\}\right)=\sum_{i\in I_k^l}\gamma_{i\tau}\Delta P_{i\tau}^{t}\left(\left\{x_{is}^{j}(t-1)\right\},\left\{x_{is}^{j}(t)\right\}\right),$$

$$\tau=2,3,\quad l\in L_k,\quad k\in K,\quad t\in[1,T],$$

at the level of a separate category of the whole CMMI model, it takes the form

$$\Delta\widehat{W}_{\tau}^{lt}\left(\left\{x_{is}^{j}(t-1)\right\},\left\{x_{is}^{j}(t)\right\}\right)=\sum_{k\in K}\delta_{k\tau}^{l}\Delta Q_{k\tau}^{lt}\left(\left\{x_{is}^{j}(t-1)\right\},\left\{x_{is}^{j}(t)\right\}\right),\tau=2,3,\ l\in L,\ t\in[1,T],$$

and within the limits of the l-th category the integrated resource utility function on the t-th sub-period is written as follows

$$\Delta W_2^{lt}\left(\left\{x_{is}^{j}(t-1)\right\},\left\{x_{is}^{j}(t)\right\}\right)=\sum_{\tau=2}^{3}\mu_t^l\Delta\widehat{W}_{\tau}^{lt}\left(\left\{x_{is}^{j}(t-1)\right\},\left\{x_{is}^{j}(t)\right\}\right),\ l\in L,\ t\in[1,T].$$

As a result, the value of the increment value of the resource utility function at the t-th planning sub-period at the level of whole SWDP is formed.

$$\Delta V_2^t\left(\chi(t-1),\ \chi(t)\right)=\sum_{l\in L}\eta_2^l\Delta W_2^{lt}\left(\left\{x_{is}^{j}(t-1)\right\},\left\{x_{is}^{j}(t)\right\}\right),\quad t\in[1,T].$$

Thus, the additive target function of the medium-term planning model for the SWDP quality improvement has the following form

$$F(\chi)=\sum_{t=1}^{T}\Phi_t\left(\chi(t-1),\chi(t)\right),\tag{12}$$

where

$$\Phi_t\left(\chi(t-1),\ \chi(t)\right)=\xi_t\sum_{\alpha=1}^{2}\overline{\rho}_{\alpha}\Delta V_{\alpha}^{t}\left(\chi(t-1),\ \chi(t)\right),\ \xi_t\geq 0,\quad t\in[1,T],\quad \sum_{t=1}^{T}\xi_t=1,$$

and $\{\xi_t\}$ – vector of the importance weight coefficients of the utility function increments value on the planning sub-periods.

Resource restriction has the form

$$\sum_{t=1}^{\tau}\tilde{R}_t\left(\chi(t-1),\ \chi(t)\right)\leq\sum_{t=0}^{\tau-1}\overline{R}_t=R_{\tau-1},\quad \tau\in[1,T],\tag{13}$$

where

$$\tilde{R}_t\left(\chi(t-1),\ \chi(t)\right)=\sum_{k\in K}\sum_{l\in L_k}\sum_{i\in I_k^l}R_{i2}\left(\left\{x_{is}^j(t-1)\right\},\ \left\{x_{is}^j(t)\right\}\right),\quad t\in[1,T].$$

In this case, the conditions are imposed

$$\chi(t-1)\le\chi(t),\quad \chi(0)=\left\{\overline{=}{}^{j}x_{is}\right\},\quad \chi(T)=\left\{\overline{-}{}^{j}x_{is}\right\},\quad t\in[1,T]. \tag{14}$$

Thus, the dynamic formulation of the medium-term planning problem of the SWDP quality improvement, based on the utility theory [4, 5], is written as follows. Find the optimal matrix value $\chi^{\star}$, that provides the maximum value of the additive utility function (12) under conditions (11), (13), (14).

In order to solve the problem, the idea of the method of sequential analysis of the alternatives based on the "Kiev broom" algorithm is used in the work. The visual interpretation of the algorithm is presented in Fig. 2, where $\sum_t, t=\overline{0,T}$ – the spaces of variables $\chi(t)$, $t=\overline{0,T}$ of the model (11)–(14).

Let's consider the algorithm at the zeroth, t-th, where $t\in[1,T-1]$ and T-th (final) steps.

Zeroth step. A set is formed

$$G_1=\left\{\chi(1):\chi(0)\le\chi(1)\le\chi(T),\tilde{R}_1\left(\chi(0),\chi(1)\right)\le\overline{R}_0\right\},$$

which is discrete and consists of a finite number of elements $\overline{\chi}_k(1)$ whose values acquire $\overline{\chi}_k$. Therefore, we will represent it in the following form

$$G_1=\left\{\overline{\chi}_k(1),k\in\tilde{G}_1\right\},$$

where $\tilde{G}_1$ – set of index values of k elements $\overline{\chi}_k(1)$. Each value $\overline{\chi}_k(1)$ corresponds to $L_1\left(\overline{\chi}_k(1)\right)=\Phi_1\left(\chi(0),\overline{\chi}_k(1)\right),\quad k\in\tilde{G}_1$.

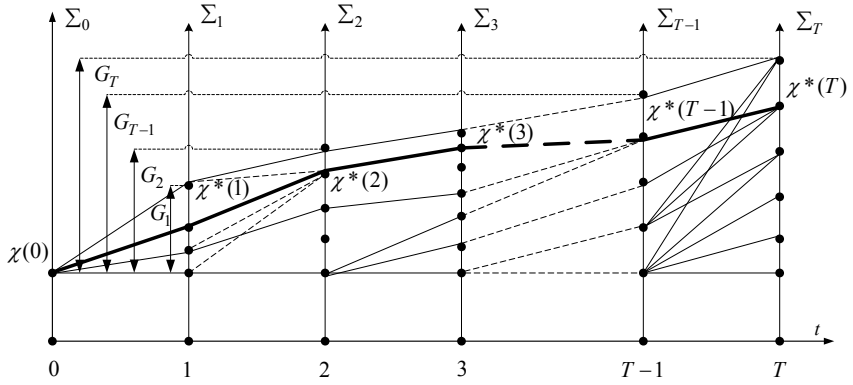


Figure 2 – Visual interpretation of the algorithm

Step $t\in[1,T-1]$. The set is defined

$$G_{t+1}=\left\{\chi(t+1):\chi(0)\le\chi(t+1)\le\chi(T),\ \sum_{\tau=1}^{t+1}\tilde{R}_t\left(\chi(\tau-1),\chi(\tau)\right)\le\sum_{\tau=0}^{t}\overline{R}_\tau\right\}.$$

Then for each $\chi(t+1) \in G_{t+1}$ the sub-set $\overline{G}_t\left(\chi(t+1)\right) \subseteq G_t$ is formed as follows $\overline{G}_t\left(\chi(t+1)\right) = \left\{\chi(t) : \chi(t) \in G_t,\ \chi(t) \le \chi(t+1)\right\}$.

Since the set $\overline{G}_t\left(\chi(t+1)\right)$ is discrete and consists of a finite number of elements whose values acquire $\overline{\chi}_k(t)$, we represent it as follows.

$$\overline{G}_t\left(\chi(t+1)\right) = \left\{\overline{\chi}(t),\ k \in \hat{G}_t\left(\chi(t+1)\right)\right\}$$

where $\hat{G}_t\left(\chi(t+1)\right)$ – an index set of k elements $\overline{\chi}_k(t)$. Each value $\overline{\chi}_k(t)$ corresponds to

$$\overline{L}\left(\overline{\chi}_k(t),\ \chi_k(t+1)\right) = L_t\left(\overline{\chi}_k(t)\right) + \Phi_{t+1}\left(\overline{\chi}_k(t),\ \chi_k(t+1)\right) \tag{15}$$

and the polygonal curve is of the "maximum" length, which connects $\chi(t+1)$ to $\chi(0)$, is determined as follows

$$L_{t+1}\left(\chi(t+1)\right) = \max_{\{\lambda_k(t)\}} \sum_{k \in \hat{G}_t(\chi(t+1))} \left\{\overline{L}\left(\overline{\chi}_k(t),\ \chi(t+1)\right) \cdot \lambda_k(t)\right\}, \tag{16}$$

under the condition

$$\lambda_k(t) \in \{0,1\},\quad k \in \hat{G}_t(\chi(t+1)),\quad \sum_{k \in \hat{G}_t(\chi(t+1))} \lambda_k(t) = 1, \tag{17}$$

where $\{\lambda_k(t)\}$ –boolean variables vector for the t-th step of the algorithm.

At each t-th step, as a result of optimization problems (15) – (17) solving, a set of uncompetitive alternatives is rejected, about which it is known that they are not included in the optimal solution.

T-th step. The set G_T is discrete and consists of a finite number of elements $\overline{\chi}_k(T)$, whose values $\chi(T)$ acquire. Let's represent it in the following form

$$G_T = \left\{\overline{\chi}_k(T), k \in \tilde{G}_T\right\},$$

where $\tilde{G}_T$ – the set of index values of k elements $\overline{\chi}_k(T)$.

Each $\overline{\chi}_k(T)$ corresponds to the polygonal curve of $L_T\left(\overline{\chi}_k(T)\right)$ "length" that connects $\chi(0)$ and $\overline{\chi}_k(T)$. Among all polygonal curves is polygonal curve of the "maximum" length as a result of solving of the Boolean programming optimization problem.

$$L_{\max} = \max_{\{\lambda_k(T)\}} \sum_{k \in \tilde{G}_T} \left\{L_T\left(\overline{\chi}_k(T)\right) \cdot \lambda_k(T)\right\}$$

under conditions $\lambda_k(T) \in \{0,1\},\quad k \in \tilde{G}_T,\ \sum_{k \in \tilde{G}_T} \lambda_k(T) = 1.$

The resulting polygonal curve is the solution to the dynamic problem of mid-term planning for the SWDP quality improvement based on the CMMI model.

As a modification of the approach outlined above to the development of the algorithm "Kiev broom", it was proposed previously not to taken into account the restrictions $\chi(t) \le \chi(t+1)$ when constructing each set $\overline{G}_t\left(\chi(t+1)\right)$, but to enter them into an optimization problem. On the one hand, in this case, the number of variables $\lambda_k(t)$ is increased and an optimization problem with additional constraints is solved, but there is no need to spend time on formation for each $\chi(t+1)$ of $\overline{G}_t\left(\chi(t+1)\right)$ set. This modification is presented in detail in [6].

Conclusion

The conducted research is based on complex usage of: system analysis theory and quality engineering of the software systems, which allow to solve the problem and in terms of TQM to highlight the research object – SWDP as one of the components of quality management software; utility theory, based on which the target functions of static and dynamic models for SWDP improvement were built; mathematical programming (methods: sequential analysis of alternatives, branches and boundaries, multi-criteria optimization), which is used for boolean and discrete programming problems solving, tasks with additive target function, multi-criteria task of the current planning, SWDP quality improvement; decision-making theory and business processes modeling in developing support decision-making information technology under the plan-program formation for the SWDP quality improvement.

The obtained results can be the basis of information technology and applied by the IT company management under real conditions, which will enable them:

- to assess the initial state of the SWDP in terms of "maturity" according to the CMMI model;
- to build an optimal strategy for SWDP maturity level increasing under the limited resources conditions using the target profile within the planning period;
- to determine the optimal sequence of the capacity level increasing of the particular practices and process areas for different resource utilization strategies, according to the SWDP maturity path during the first planning period.

References:

1. Goloskokova A. O. Static planning models synthesis of quality improvement of software development process /A. O. Goloskokova, M. D. Godlevskij // Eastern-European Journal of Enterprise Technologies.– Kharkiv.– № 3/2 (75), 2015.– P. 23–29.
2. Goloskokova A. O. Dynamic planning model of quality improvement of the software development process / A. O. Goloskokova, M. D. Godlevskij, E. U. Rubin // Bulletin of NTU "KhPI". Series: System analysis, control and information technology.– Kharkiv: NTU «KhPI», 2015.– № 55 (1097).– P. 17–22.
3. Gnatienko G. M. Expert technologies of the decisions making / G. M. Gnatienko // Kiev: Maklaut, 2008.– 444 p.
4. Aleskerov F. Utility Maximization, Choice and Preference / F. Aleskerov, D. Bouyssou, B. Monjardet // Berlin: Springer, 2007.– 283 p.
5. Fishburn P. C. Dominance in SSB Utility Theory / P. C. Fishburn // Journal of economic theory.– № 34, 1984.–P. 130–148.
6. Goloskokova A. O. Quality improvement of the software development process based on the sequential analysis of variants method and the method of local optimization / A. O. Goloskokova, M. D. Godlevskij, E. U. Rubin // Bulletin of NTU "KhPI". Series: System analysis, control and information technology.– Kharkiv: NTU «KhPI», 2015.– № 58 (1167).– P. 3–6.

Information support for distributed teamwork knowledge management

Olexander Shmatko
Doctor of Philosophy in Technical Science, Associate Professor
Department of Software Engineering and Management Information Technologies
National Technical University "Kharkiv Polytechnic Institute"
ORCID: https://orcid.org/0000–0002–2426–900X

Mariia Bilova
Doctor of Philosophy in Technical Sciences, Associate Professor
Department of Software Engineering and Management Information Technologies
National Technical University "Kharkiv Polytechnic Institute"
ORCID: https://orcid.org/0000–0001–7002–4698

Abstract. *Several concepts about knowledge management are proposed in the work: knowledge type (tacit knowledge and explicit knowledge, formal knowledge and informal knowledge); knowledge management in software development methods; knowledge management process (knowledge creation, knowledge storage and retrieve), knowledge transferring and knowledge sharing. The framework and implementation of knowledge management system are described. The framework of knowledge management system is illustrated by four elements: roles, product development, structure and forum.*

Keywords: *distributed teamwork, knowledge distribution, knowledge flow, knowledge management, knowledge sharing, software development*

Introduction

Nowadays the distributed software development becomes more and more popular. Not only for the efficiency and effectiveness the distributed teams provide, but also the distributed teams can supply a whole-day works with lower costs. Knowledge management, as a vital component in distributed software development, is responsible to resources creation, storage and retrieval, knowledge distribution and knowledge sharing during the software development process.

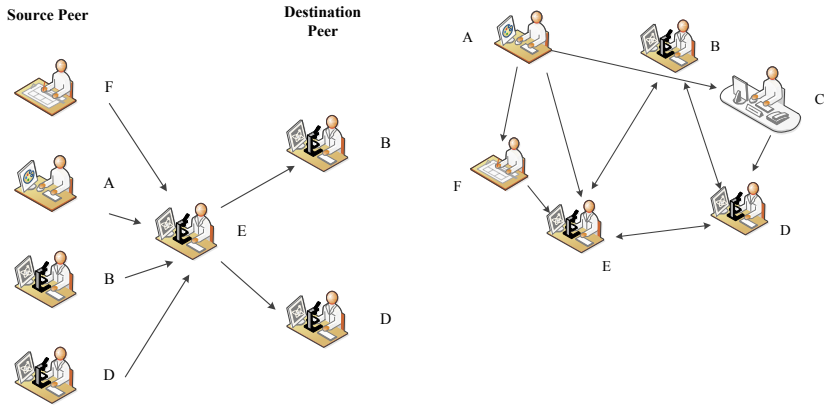
Knowledge sharing model

The process of knowledge sharing involves knowledge creation and import, knowledge capture, knowledge search, and knowledge use, which are equal to the progress of knowledge management. As above debating of knowledge management, in this article both the peer-to-peer (P2P) and C/S (client and server) based knowledge sharing model is considered and an open forum is chose as the description of knowledge contents and sharing.

C/S based architecture is one of the most applied architecture for knowledge management. Under the C/S based architecture, team members as client upload their explicit knowledge to server. Meanwhile, team members can retrieve the knowledge as their requirement from server. C/S architecture belongs to one-to-more or more-to-one mode (more clients correspond to one server), which helps team members obtain various kinds of knowledge from server. For the whole distributed software development team, C/S architecture provides both a safe and convenient centralized knowledge management.

Peer-to-peer architecture is a kind of one-to-one network, which is composed by a series of knowledge nodes. Every knowledge node corresponds to each team member that is the sender or receiver of knowledge flow (or both sender and receiver). Knowledge node generates and requires knowledge in the process of work implementation, which is shown as (Fig. 1).

From the architecture, knowledge sharing is more convenient that every knowledge node can receive knowledge from source peer and send knowledge to destination peer directly. But the peer-to-peer based architecture also brings some troubles: more difficult in management including knowledge retrieval and knowledge selection; more complex in structure of knowledge sharing model. Peer-to-peer based knowledge sharing model is a kind of network topology. Team members with specialization in their domains have different levels and types of knowledge.



1) the knowledge flow of knowledge node (Team member) E

2) knowledge sharing in peer-to-peer model

Figure 1. – Knowledge management under P2P architecture

In the following figure, the peer-to-peer based knowledge sharing model is composed by six knowledge nodes and several knowledge connections with their relevant directions. The knowledge connections with arrows illustrate the direction of knowledge flow. The connection with unidirectional arrow represents that

the knowledge node can just be knowledge sender or knowledge receiver. The connection with bidirectional arrow represents the knowledge node can be both knowledge sender and knowledge receiver. For a knowledge node, there are three modes to demonstrate the correspondence among nodes: one-to-one, a knowledge node corresponds (knowledge sender or knowledge receiver) to a knowledge node (knowledge sender or knowledge receiver); one-to-more, a knowledge node (knowledge sender) corresponds to more knowledge nodes (knowledge receivers); more-to-one, more knowledge nodes (knowledge senders) correspond to a knowledge node (knowledge receiver). For knowledge node named E, it has source peer set (the set of knowledge sender) and destination peer set (the set of knowledge receiver). In this mode, knowledge node B and knowledge node D are both source peer and destination peer, for that the connection has bidirectional arrows.

Knowledge flow out from knowledge node is more abundant than the input from source peer. That is why peer-to-peer based knowledge model is more active than the traditional C/S based knowledge model. Also because of geographical distance, the authority to visit the knowledge server may be limited under the C/S based architecture for distributed team of software development. The peer-to-peer based knowledge management model is more suitable to distributed team of software development than C/S based knowledge management model.

Weighted-similarity calculation among knowledge nodes

Each knowledge node has their profile information that reflects the knowledge resource. The knowledge resource is consisted of a series of features. For distributed team of software development, these features reflect the elementary information of team members including: development experience, skills, ability of system analysis, and model of mentality and so on. The profile information or attributes is described as: $(a_1,a_2,a_3,...,a_n)$, where n is the total number of attributes. For a knowledge node A_i it exists $A_i=\left(\overline{a_{i1}},\overline{a_{i2}},...,\overline{a_{in_i}}\right)$, where $i\in[1,m]$, m is the number of knowledge source (equal to team members); a_{ij} represents the selection j in j -th feature of A_i. For a feature a_i in $(a_1,a_2,a_3,...,a_n)$ it have several selections as $a_i=(a_{i1},a_{i2},a_{i3},...,a_{in_i})$ where n_i is the amount of selections. For every feature, the amount of related selections is identical. The symbol a_{mn} represents the n -th selection in the m -th feature. The set of knowledge network's knowledge resources is described as $KN=\{A_1,A_2,...,A_m\}$. In knowledge network, knowledge node does not need to connect with all of the other nodes. It only should to connect with the knowledge nodes which behavior similarly to it.

The host peer's source peers set should contain the peers that have the similar profile information with host peer [1]. The mathematical formulation to calculate the similarity between two knowledge nodes is:

$$KN_{sim}(X,Y)=\frac{\sum sim(a_{Xi},a_{Yi})}{|X|\cdot|Y|}$$

where $KN_{sim}(X,Y)$ formulation is the similarity between knowledge node X and knowledge node Y;

$sim(a_{Xi}, a_{Yi})$ formulation is the similarity of feature between knowledge node X and knowledge node Y;

$|X|, |Y|$ are the numbers of features in X node and Y node respectively.

As the numbers of features in two knowledge nodes are different, the similarity needs the process of formalization, so the result is divided by $|X| \cdot |Y|$ in last. On the same time, $sim(a_{Xi}, a_{Yi})$ is described as:

$$sim(a_{Xi}, a_{Yi}) = \frac{\sum_j w_{ij} \cdot bina(a_{Xji}, a_{Yji})}{\sum_j w_{ij}},$$

where w_{ij} is the weight of j-th selection in feature i; $bina(a_{Xji}, a_{Yji})$ calculates the binary distance of knowledge features between two knowledge nodes.

The process is described as (Fig. 2).

The feature of software development language	The weight of selection	A	B	C	D
Java	**0.45**	**1**	**1**	**1**	**1**
C	**0.45**	**1**	**1**	**0**	**0**
Python	**0.1**	**1**	**0**	**0**	**0**

Figure 2. – Selections of four knowledge nodes (A, B, C, D) under the feature of software development language

From (Fig. 2), the feature of software development language for team members is different. "1" represents the state of selection is definition while "0" represents the state of selection is default. So for team member A possesses three software development languages: Java, C, and Python. Team member B possesses two software development languages: Java and C.

For software development, not all development languages are equally important. The software system may mainly depend on the Java and C. The weight of Java and C could large than the weight of Python. This regulation is also suitable to other kinds of features. If the similarity in the feature of software development language between A and B, B and C, C and D are:

$$sim(a_A, a_B) = \frac{0.45 \cdot 1 + 0.45 \cdot 1 + 0.1 \cdot 0}{0.45 + 0.45 + 0.1} = 0.9$$

$$sim(a_B, a_C) = \frac{0.45 \cdot 1 + 0.45 \cdot 0 + 0.1 \cdot 0}{0.45 + 0.45} = 0.5$$

$$sim(a_C, a_D) = \frac{0.45 \cdot 1 + 0.45 \cdot 0 + 0.1 \cdot 0}{0.45} = 1$$

Thus the similarity between A and B is 0.9; C and D is 1.0; B and C is 0.5. The similarity calculation between team members A and B shown as (Fig. 3).

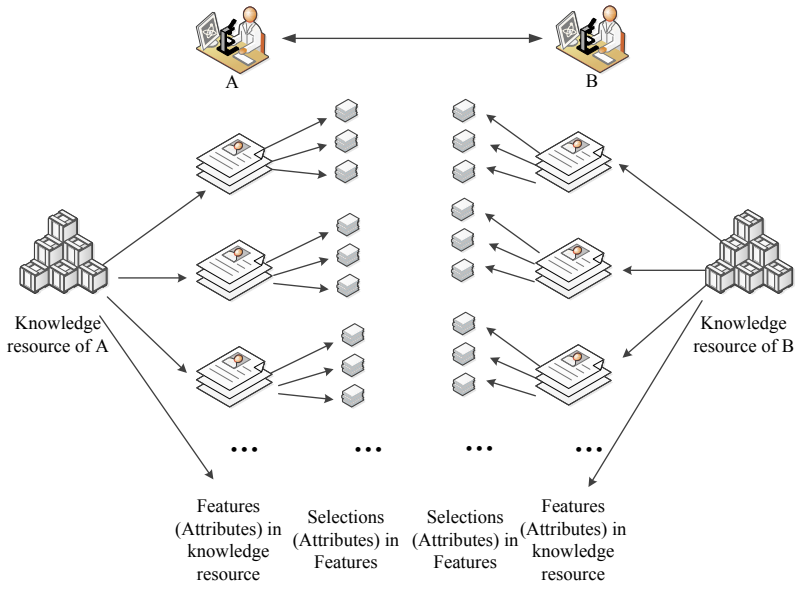


Figure 3. – The knowledge resources of two knowledge nodes (team members)

The process of similarity calculations includes two bottom-up steps: the first step is calculating the similarity of selections in features; the second step is calculating similarity of features. By summary of two steps, the similarity of knowledge resources is obtained. In procedure of knowledge management, the knowledge network initialization and the knowledge network formulation are involving with similarity calculation.

Knowledge network initialization

At the beginning of knowledge network initialization, there are knowledge nodes without connections. To construct the connections, the similarity among knowledge should be calculated at first. Besides the knowledge resource, a knowledge node should equip with source peers set. The source peers set includes the elementary information of source peers and the similarity value among source peers and this knowledge node. Not all team members have a direct relationship during the software development. Thus the size of source peers set is limited to a definite number D. The knowledge node calculates similarity value with other knowledge nodes and selects the D knowledge nodes with the largest value as source peers. There are two ways to initialize the source peers set. The one is global search, which means the knowledge node should search all other knowledge nodes. It costs a great amount of time when the size of network is large. Another is local search. In

this search mode, knowledge node searches some of other peers within a definite scope. The other peers may have a similar work type with this knowledge node.

Knowledge network re-formulation

With the team members leaving and joining or information updating, the knowledge management process is dynamic. The knowledge network updates all the time. Authors in [1] advocated that every time knowledge network reformulation needs to search other peers again for finding the top D most similar peers in current states. Two strategies are proposed below to define the search space.

Equally expending. The search space is constructed by source peers. The knowledge peer extends to its source peers. As the procedure is endless, a fathoming depth is defines to limit the search depths.

Unequally expending. In this strategy, fathoming depths are different according the similarity value among source peers. The higher the similarity value is, the deeper the depth will be, vice versa.

In fact both two strategies has a complex calculation and time cost. Putting the similarity values in the sources peer set corresponding to its source peers is a good choice. When the knowledge node updates its information, it needs to recalculate the similarity with its source peers. If the new similarity rank of knowledge node does not fall into the last one, the formulation of knowledge network is not needed and the whole process' time complexity is linear. If the similarity rank of knowledge node falls into the last one, the knowledge network should re-formulation according to the unequally expending principle. When the knowledge node is deleted, which means the team member leaves the team, its destination peers only need to delete it from their source peers set and find a new source peer outside the source peers set. When the new knowledge node joins the knowledge network, it calculates the similarity with other peers to fill its source peers set at the same time other peers need to decide whether put this node to their source peers set or not by calculating the similarity.

Knowledge flow operations

The knowledge network has been constructed and the most important method to manage the knowledge is by knowledge flow. Team members are linked by all kinds of knowledge flow. Team members can get their desired knowledge by knowledge flow and share their own knowledge to others. In [2], the knowledge flow is regarded as a two dimensional region in knowledge space as type-filed (TF) and level filed (LF). The process among knowledge fields is summarized as:

$$< TF_1, LF_1 > \cup < TF_2, LF_2 > = < TF_1 \cup TF_2, LF_1 \cup LF_2 >$$
$$< TF_1, LF_1 > \cap < TF_2, LF_2 > = < TF_1 \cap TF_2, LF_1 \cap LF_2 >$$
$$< TF_1, LF_1 > - < TF_2, LF_2 > = < TF_1 - TF_2, LF_1 - LF_2 >$$
$$< TF_1, LF_1 > \subseteq < TF_2, LF_2 > \; if \; < TF_1 \subseteq TF_2, LF_1 \subseteq LF_2 >$$

For multiple knowledge flow operations, it exists:

$$< TF_1, LF_1 > \cup < TF_2, LF_2 > \cup ... \cup < TF_n, LF_n > = < TF_1 \cup TF_2 \cup ... \cup LF_n, LF_1 \cup LF_2 \cup ... \cup LF_n >$$

$$< TF_1, LF_1 > \cap < TF_2, LF_2 > \cap ... \cap < TF_n, LF_n > = < TF_1 \cap TF_2 \cap ... \cap LF_n, LF_1 \cap LF_2 \cap ... \cap LF_n >$$

$$< TF_1, LF_1 > - < TF_2, LF_2 > - ... - < TF_n, LF_n > = < TF_1 - TF_2 - ... - LF_n, LF_1 - LF_2 - ... - LF_n >$$

Knowledge flows with one knowledge node is shown in (Fig. 4).

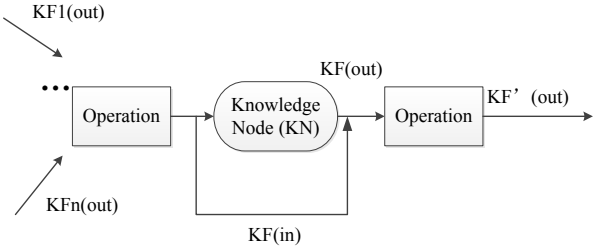


Figure 4. – Knowledge flows with one knowledge node

By logical operation, the input knowledge flows will be integrated into a formalized knowledge flow. The formalize knowledge flow will be input into the knowledge node. The operation within the knowledge node is unclear and new information will be put into the knowledge flow as the output. The operation of knowledge flow also could be not performed.

Framework and structure of knowledge management system

On above sections, it has discussed about characteristics of distributed software development, relationship between knowledge management and distributed software development, types of knowledge, knowledge management process, aims of knowledge management as well as algorithms and models for knowledge sharing and distribution. In this section, it will be introduced a designation of framework and structure for knowledge management system.

The framework of knowledge management system comes along with four processes: knowledge creation (knowledge production and knowledge update), knowledge deposition and retrieve, knowledge distribution (knowledge sharing) and knowledge application (knowledge integration). All four parts is associated with functions (what kind of works the knowledge management undertakes?), roles (what kind of people involves in this process and what kind of reputation they bear?), and events (what kind of achievements the knowledge management can realize?).

The structure of knowledge management system includes function structure (a large function can be divided into several small functions), data structure (attributes of roles and events). Structure of knowledge management system indicates the form of data which is deposited in the database. A complete knowledge management system should satisfy the elementary requirement of distributed software development. It can

edit, deposit, search and integrate knowledge. Besides, a practical system ought to certainty obey the software development modes (such as Agile, Waterfall, RUP etc.). But for a knowledge management system in modern software development mode, these functions are not enough. To enhance the competitiveness of company, a knowledge sharing culture should be constructed within the organization. The knowledge management system should act as a convenient and direct knowledge sharing medium. Team members exchange their thoughts and learn the new knowledge through the system. In view of characteristics of distributed software development, the communications among team members are not ideal. For that different location and time zone, the communications are often asynchronous. The system designs a synchronous mechanism that team members can contact with others by sending instant messages. This mechanism can highly reduce the communication cost and save the time expense.

Framework of knowledge management system

The framework of knowledge management system is shown as (Fig. 5).

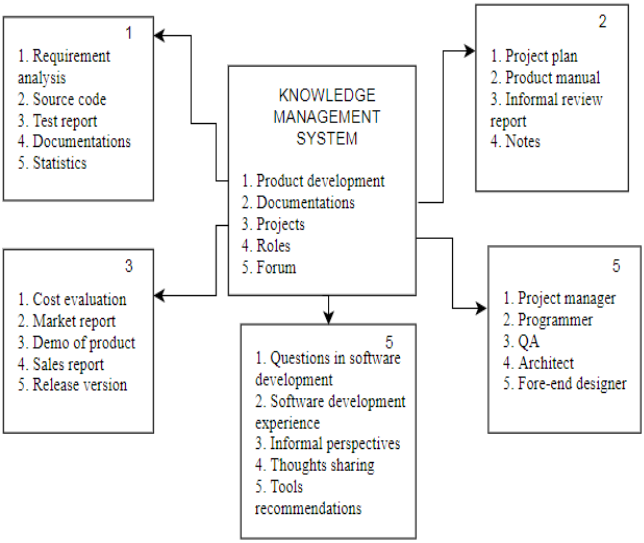


Figure 5. – The framework of knowledge management system

From (Fig. 5), it is clear that knowledge management system is composed to five parts: product development, documentations, project, roles and forum. The details of designs are described as follows.

Product development

Product development is same to the software development, which includes explicit knowledge as: requirement analysis, source code, test report, documentations and statistics etc.

All these explicit knowledge is deposited in different folders. In order to remain old knowledge for revision in the future, the knowledge management system introduces version control. When the team member first uploads files, the system will judge whether the same file has existed. If not, the file will be upload as original; if already existed the same file, the file will be signed with time stamp to distinguish the old version, as Fig. 6 shows.

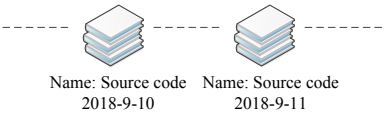


Figure 6. – Documents with version control (Documents with same name and different time stamp)

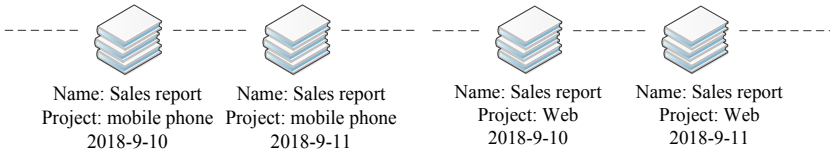
So, in this part only explicit knowledge involves and all explicit knowledge is organized by timeline, which makes framework clear.

Documentations

For distributed software development, documentation includes project plan, product manual, and informal review report and so on. These documentations seem to be useless once it lost effectiveness for a given period of time. However, these documentations still have its effect to be a reference for future works. So the way of deposition for documentations is the same as product development.

Projects

Projects part is the result of product development and documentation. It has cost evaluation, demo of product, market report, sales report, and release version and so on. But the explicit knowledge may belong to different projects. In order to distinct different explicit knowledge from different projects, explicit knowledge in Projects part should have additional remark that points out attributes (Fig. 7).



a) sales report in “mobile phone” project b) sales report in “Web” project

Figure 7. – Explicit knowledge in Project part

Within the same project, explicit knowledge is also remarked with time stamp for distinction. Thus file in Projects parts have two-tuples attributes, which is enough to distinguish every file. This kind of naming mode has many benefits. For new team member, when he/she entered the organization first time, these files with specific identified information can help them learning knowledge precisely. For other team

members, when they want to revise the whole process of project, they can easily and quickly locate the files.

Roles

Roles in knowledge management system indicate people who participate in the distributed software development. Roles include project manager, programmer, architect, quality assurance and fore-end designer etc. Project manager works for communicating with customers, analyzing requirements and then assign tasks to other team members. Project manager can be regard as the medium between customers and project programmers. Architect designs the architecture of project. Fore-end designer contributes to user interface design. Then project programmers are responsible for achieving modules of software project and integrate these modules into a complete project. Once the project is finished, quality assurance begins to make tests (like white-box test and black-box test etc.) of software product and writes the test report.

It seems that roles in the same position (as project programmer to project programmer) have stronger links and more chances to meet other project programmers over the whole distributed software development process. But for roles in different positions, like project manager and project programmers, there is less chance to contact with each other. Once the requirement is defined and tasks are distributed to corresponding project programmers, it is no need to make frequent meet. All in all, knowledge management system constructs profile for each team role. The profile contains personal information, skills, position. In the process of knowledge distribution, sender wants to find appropriate receivers and verse vice. Under this circumstances, profile as a strong tool indicates the similarities and difference among team roles.

Forum

Forum is a kind of electronic community, which is desired to encourage knowledge sharing and transformation from tacit knowledge to explicit knowledge [3]. Like "Quora", it provides a bulletin for team members to online edit; modify their questions. It is a kind of knowledge market letting team members sharing, learning and presenting.

When team member has question about software development, he/she can use online editor describing his/her questions and upload it to bulletin. If someone experts in this aspect, the question can be solved by effective solutions. In this part, questioner solves the problem with the help of expert. On the same time, the expert gains reputation from other team members. This is a win-win mode and motivates the knowledge sharing and knowledge distribution.

Team members can also share their experience in forum about distributed software development. Some team members with similar experience may be triggered and easily solve the similar question. For other purposes, team members could express their own informal perspectives. Different perspectives among team members mix and it is more likely for new creativity creation.

The forum part is also used to recommend software development tools for efficient developing. Team members can share the software development tools that they think is effective and efficient on the forum.

In the conclusion, considered the high value of tacit knowledge, which is not belonging to organization but to individuals, the knowledge management should encourage team members transforming their tacit knowledge to explicit knowledge. By writing a post on the forum, team members communicate with each other by their own experience, activities and skills. It is a process with internalization (from explicit knowledge to tacit knowledge: team members read the post on the forum) and externalization (from tacit knowledge to explicit knowledge: team members write down a new post on the forum). Forum fosters the message exchange among team members. Tacit knowledge, as one of the most valuable fortune, is well exploited through the forum. On the one hand, forum encourages team members to transform individual's knowledge to social knowledge (collective knowledge) as company's explicit fortune; on the other hand, the relationship among team members can be strengthened through the informal conversation.

For distributed software development, team members are in different sites and time zones. Forum is designed to increase the motivation for expressing perspectives of distributed team members. Thus, as consideration of these benefits, knowledge management should provide a space as a forum for team members sharing their perspectives and experiences. Also, it provides the function to comment on the post with sentences and even upload files.

Structure of knowledge management system

Structure of knowledge management system includes two aspects: one is deposition structure (for uploaded files in Product development part) and another is the data structure for elements (profiles of roles, post in the forum and all kinds of uploaded files).

Deposition structure

As above mentioned, when team members upload their files, unstructured principles cause the knowledge management chaos. It is needful to make a clear structure of Project development part in knowledge management system. To clearly manage the knowledge in project development, a tree structure is designed (Fig. 8).

For the project, every kind of part has its own folder to deposit source codes, reports, documentation and statistics. The folder named Source code is the warehouse depositing the source code of the project.

As for a complete project, it has several modules, such as database design, user interface design, and algorithm design and so on. For different module, its explicit knowledge is deposited separately. For example, the source code of the project is deposited in the module called Source code while test reports are stored in the Test report module.

Within the same module, all explicit knowledge is deposit together. In order to discriminate them, a version control mechanism is introduced. Within the same module, all file can have the same name, but they will have different time stamp for distinction.

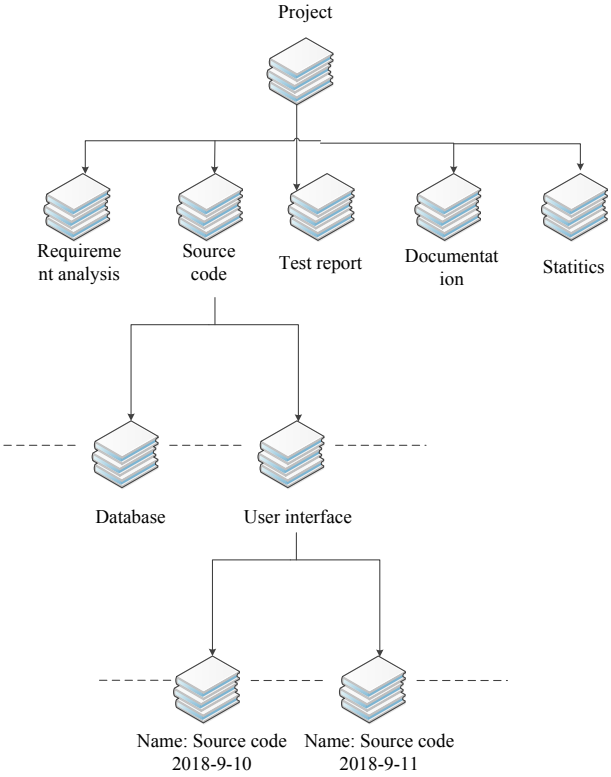


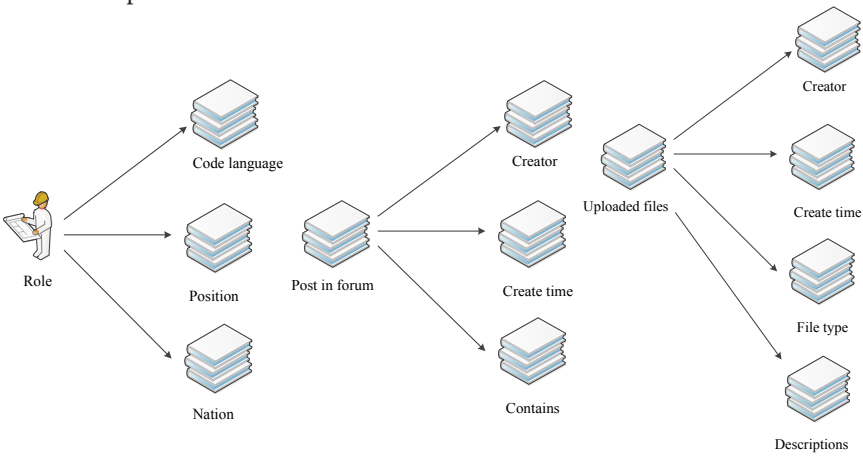
Figure 8. – The tree structure of Project development part

The tree structure makes Project development part clear which can avoid chaos caused by upload files. Additionally, when all the modules is completed, project programmers can easily integrate these modules into a whole project.

Data structure

In knowledge management system, there three elements: role, post in forum and uploaded files. All elements have data structure. The relationship among attributes and elements is described (Fig. 9). File possesses four attributes: upload time, creator, file type and descriptions. To identify a role, the personal profile is needed, which includes: personal information (name, id, create time, create IP and so on), skills (expert in what kind of aspects including program language etc) and position (position in the company, such as project manager, front-end project

programmer, back-end project programmer etc.). The space of database prepared for role is limited. Personal information, skills and position can be described in char. For the post in forum, there also three parts: creator (the name of creator), create time (when the post is created) and contains. Like the role, the attributes of creator is represented in char.



a) role with attributes b) post in forum with attributes c) updated files with attributes attributes

Figure 9. – Data structures of three elements (role, post in forum and upload file)

The create time is described in Date Time type (YYYY-MM-DD, 8 bytes). As the long length of contains, it is indicated by Text type.

The implementation of knowledge management system

This section describes the progress of design and implementation on knowledge management system according to proposed model and framework in last section. At first, the requirement analysis is discussed. Then the details on every module and work flow of knowledge management system are illustrated. After that the structure and tables of system dataset are demonstrated. At last, the implementation and test on knowledge system are shown.

There is a clear requirement that develop an integral knowledge system providing knowledge storage, knowledge retrieval, knowledge sharing and updating, team member matching with high efficiency. Besides, the knowledge management system should give a chance to team members for asking, debating and answering question so as to encourage the knowledge sharing. The details of requirement analysis are described as follows.

The elementary functions of knowledge management system includes: knowledge deposit, knowledge sharing and updating;

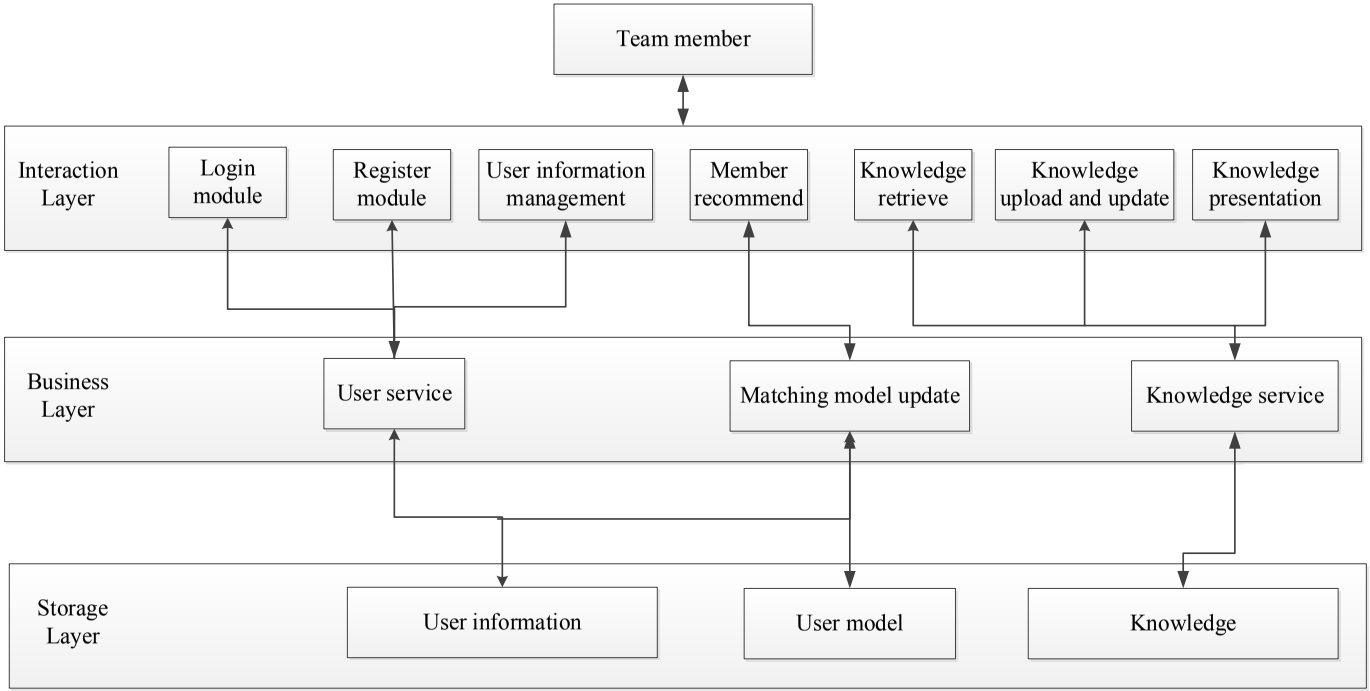


Figure 10. – The structure of knowledge management system

The information of team members is not unchanged. Based on user information the knowledge management system can precisely recommend team members with similar interests for team member matching;

The knowledge management system should provide a function of knowledge retrieval. Team members can find knowledge which they are interested in by using key words;

Because of the distributed software development, the communication between team members is difficult. Thus an effective and convenient medium is necessary.

The knowledge management system is designed by multi-layer and modules, which mainly includes: interaction layer, business layer as well as storage layer. Each layer is consisted of several modules (Fig. 10). The interaction layer provides the interface between user and knowledge management system. Through simple and intuitive interface, the knowledge management collects user information and knowledge. The interactive layer in this system includes: user login module, user register module, user information management module, member recommend module, knowledge retrieve module, knowledge retrieve module, knowledge upload and update module as well as knowledge presentation module.

User login module. Before user enters the knowledge management system, the module will verify the effectiveness of username and password. Only when both username and password is correct, the user is permitted to enter the system and make other operations.

User register module. If the user enters the system at the first time, the user must make the registration. The information of registration includes: user ID, user group ID, email, username and password, created date, position of user, code language and nation, where position, code language and nation are used to make member matching and recommend.

User information management module. The information can be updated by admin so as to make the member recommend precisely.

Knowledge retrieve module. User can find the knowledge in which they are interested by knowledge retrieve module.

Knowledge uploaded and updated module. User can upload their explicit to knowledge management system and update the knowledge in time.

Knowledge presentation module. The knowledge is presented to user. And user can read and download relative knowledge.

The business layer is a connection between interaction layer and storage layer, which satisfy the requirement of users by operating the data from storage. The business layer is consisted of: user service module, matching update module and knowledge service module.

User service module. User service module is applied in user login, user registration and user information management;

Matching update module. This module receives the information from user. Then the similarities between team members are calculated the threshold of similarity

is predefined. Only the similarity is larger than the threshold, the corresponding team member can be recommended to user (Fig. 11).

Knowledge service module. This module is responsible for knowledge management as knowledge upload and update (knowledge creation), knowledge retrieve and knowledge representation (knowledge sharing).

The storage layer is responsible for the persistent storage of system data, providing data support for each module of the business logic layer. The data of storage layer includes: user information and knowledge. The knowledge is classified into two classes: formal knowledge and informal knowledge.

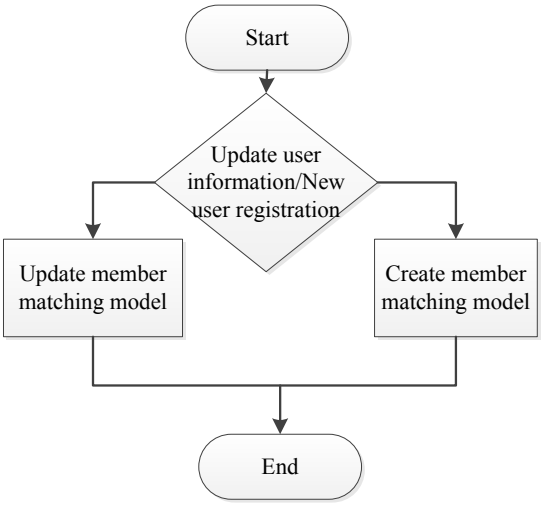


Figure 11. – The work flow of matching update module

For formal knowledge, it includes project codes and relative documents. The informal knowledge is other information in threads and posts. Informal knowledge does not have a fixed format which is more flexible and casual.

The existence of informal knowledge aims to encourage team members to share their software development experience, questions and answers in software development progress or some development tools recommendation etc. In knowledge management system, the informal knowledge has two forms: thread and post. Posts are built based on the threads. The relationship between posts and thread is many-to-one: one thread corresponding to many posts. The contents of posts are associated with the thread.

For each kind of formal knowledge, it has an identical standard and fixed format. For distributed software development, the formal knowledge consists of: cost evaluation, market research report, demo of product, sales report, release version, requirement analysis report, test report, statistics and the source code at last but

not least. The format of formal knowledge is various which depends on the code language (i.e., php file is created by PHP language; c file is created by C language etc) and instrument (i.e., vsd file is produce by Visio; doc file is built on Word etc.).

In knowledge management system, the formal knowledge is expressed in a unified form. It is regarded as the attachment of thread or post. The formal knowledge is created offline by specific language and instrumentation; then it is uploaded to the knowledge management system.

In order to provide an effective approach of communication for distributed software development team, the knowledge management system is implemented based on web. The architecture of web-based knowledge management system is described as (Fig. 12).

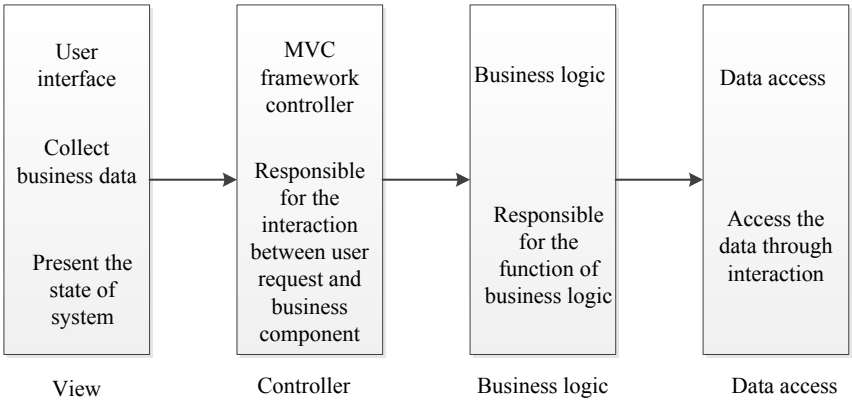


Figure 12. – Architecture of web-based knowledge management system

The first part is responsible for collecting the requirement information from users and presenting business data to user. The function in this part includes: data collection, data representation and data verification. The second part is about the interaction between user requirement and business component. The third part is associated with processing specific user requests and consists of a series of business logic stripping. These business logic objects implement the business logic methods required by the system. The implementation of the business logic methods depends on the data access services provided by the data access layer. The fourth part operates for data access. Separating the number of access operations from other business logics allows the business logic components to focus on the implementation of business logic without having to care about the underlying database access details, making the system more maintainable and portable. The work flow of web-based knowledge management system is described as: in knowledge management system, there are two kinds of users: general user and administrator. For general users,

they can login the system, upload their knowledge to system, sharing knowledge to other team member, get recommendation on similar team members, search for other users and knowledge etc.

For administrator, it possesses all of the same rights as the general user. Besides, administrator can manage the information of users including user registration, user deletion, user information update, distribution of permission, knowledge management and so on. The concrete procedure is shown in (Fig. 13).

Administrator has a higher authority than general user. Besides the rights shown in Fig. 13, the administrator can manage information of users, like user registration, user inform, distribution of permission (Fig. 14).

In order to protect the security of information, the knowledge management system restricts the access of visitors and only the administrator have the right to register a new general user. In addition to other functions administrator can restrict and moderate the right of general user on reading, updating, deleting, uploading, writing, and downloading knowledge in the system. The front-end of web-based knowledge management system adopts BootStrap 4 + JQuery 3 framework while the back-end is designed by the combination of PHP 7 and MySQL 5.6.

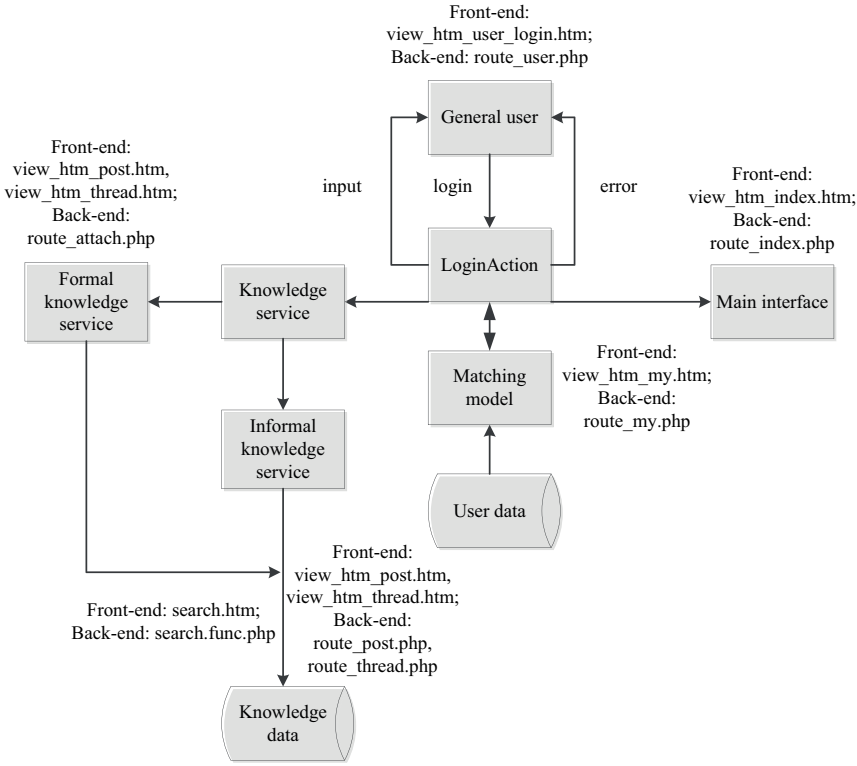


Figure 13. – The concrete work procedure of general user

Test on knowledge management system

This section will execute the test on the elementary function of web-based knowledge management system. The test functions are: login function, registration function, formal knowledge management function, informal knowledge management function, similar team member recommendation function, user/knowledge search function, and permission setting function.

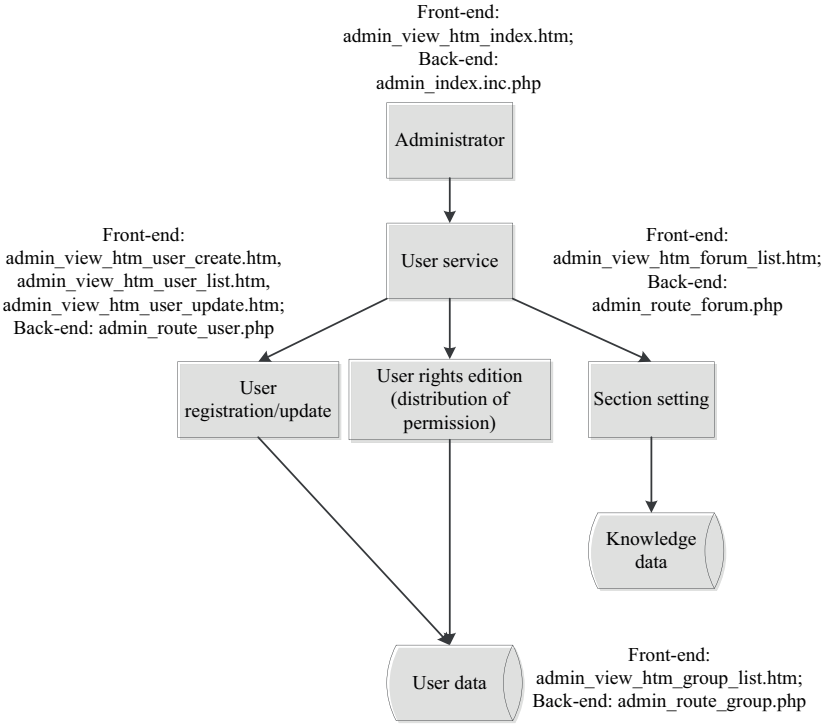


Figure 14. – The specific work procedure of administrator

Table 1. – Login function testing

Input	Input username=”Coder_6”, password=”123456”; Input username=”Coder_5”, password=”1234”; Input username=”Coder_5”, password=”123456”.
Output	Login failed, prompt “User does not exist”; Login failed, prompt “Password Incorrect”; Login successful, jumps to user main interface.
Result	Pass

For login function of the system, design 3 sets of test cases, test cases and test results are shown in Table 1 and the execution procedure is shown in (Fig. 15).

For registration function of the system, design 3 sets of test cases, test cases and test results are shown in (Table 2) and the execution procedure is shown in (Fig. 16).

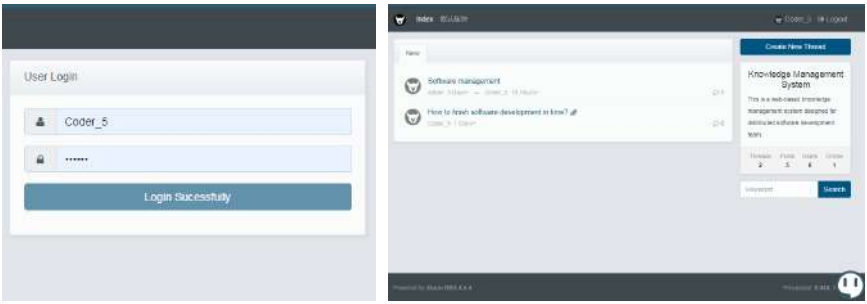


Figure 15. – Login function testing

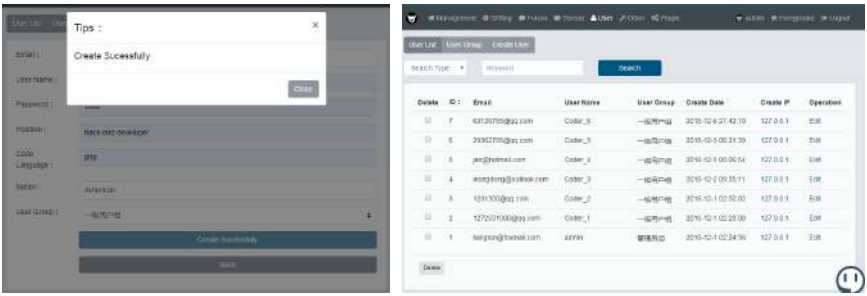


Figure 16. – Registration function testing

Table 2. – Registration function testing

Input	1 Input email = ”69126755” username = ”Coder_6”, password = ”123456” position = ”back-end developer” code language = ”php” nation = ”American”; 2 Input email = 69126755@qq.com username = ”Coder_5”, password = ”123456” position = ”back-end developer” code language = ”php” nation = ”American”; 3 Input email = 69126755@qq.com username = ”Coder_6”, password = ”123456” position = ”back-end developer” code language = ”php” nation = ”American”.
Output	1 Registration failed, prompt “Email format illegal”; 2 Registration failed, prompt “User already exists”; 3 Registration successful, prompt “Create Successfully” then jumps to user list interface.
Result	Pass

Formal knowledge management function includes knowledge upload, knowledge edit, knowledge delete in post and in thread. Test cases and test results are shown in (Table 3) and the execution procedure is shown in (Fig. 17–18).

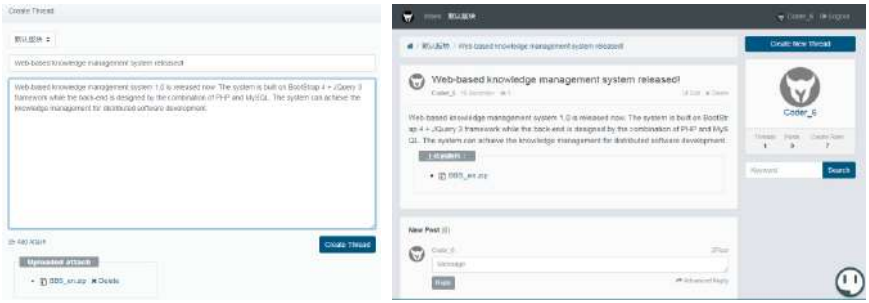


Figure 17. – Formal knowledge management function testing (part 1)

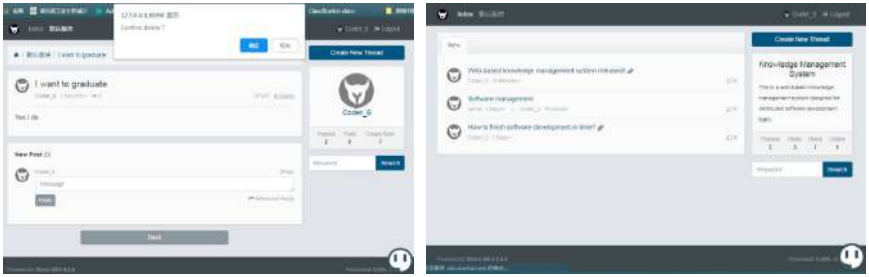


Figure 18. – Formal knowledge management function testing (part 2)

Table 3. – Formal knowledge management function testing

Input and step	1 Create a theme, write a description of the upload knowledge in the edit box, and click the “Add Attach” button; 2 Enter the theme, click the “Edit” button, modify the description of the uploaded knowledge in the edit box, then click the “Upload Attachment” button, delete or re-upload the file, and finally click the “Edit Post”; 3 Enter the theme, click the “Delete” button.
Output	1 Upload successfully, jumps to user main interface; 2 Update successfully, jumps to user main interface; 3 Delete successfully, jumps to user main interface.
Result	Pass

Informal knowledge management function includes knowledge creation as thread and post, knowledge edit, knowledge delete. Test cases and test results are shown in (Table 4) and the execution procedure is shown in (Fig. 19).

Similar member recommendation function can recommend similar team members to user based on personal information (position, code language and nation). Test cases and test results are shown in (Table 5) and the execution procedure is shown in (Fig. 20). User/knowledge search function is used to search relative user or knowledge by key words. Test cases and test results are shown in Table 6 and the execution procedure is shown in (Fig. 21).

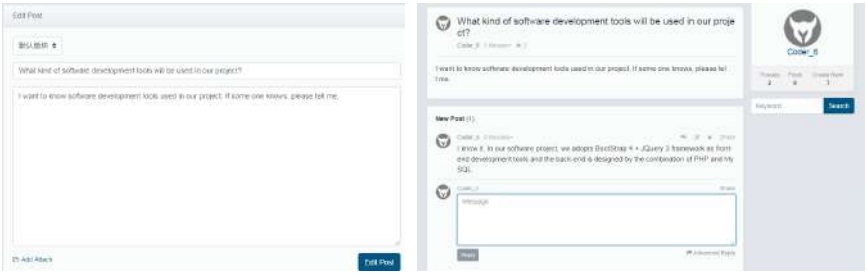


Figure 19. – Informal knowledge management function testing

Table 4. – Informal knowledge management function testing

Input and step	1. Create a thread, write a description in the edit box, and click the "Create Thread" button; 2. Create a post, write a description in the edit box, and click the "Reply" button; 3. Update a thread, click "edit" button, edit a description in the edit box, and click the "Edit Post" button; 4. Update a thread, click "delete" button.
Output	1. Create successfully, jumps to thread main interface; 2. Update successfully, jumps to thread main interface; Edit successfully, jumps to thread main interface; Delete successfully, jumps to thread main interface.
Result	Pass

Figure 20. – Similar team member recommendation function testing

Table 5. – Similar team member recommendation function testing

Input and step	1. Login the system using username “Code_2”, check the personal information; 2. Login the system using username “Code_5”, check the personal information.
Output	1. Recommend the similar team members; 2. Recommend the similar team members.
Result	Pass

Table 6. – User/knowledge search function testing

Input and step	1. Input the uid “2”, and click the “Search” button; 2. Input the uid “7”, and click the “Search” button; 3. Input the word “knowledge”, and click the “Search” button; 4. Input the word “university”, and click the “Search” button.
Output	1. Search failed, prompt “No result”; 2. Search successfully, present the information of user with uid=“7”; 3. Search successfully, present the knowledge associated with “knowledge”; 4. Search failed, prompt “No result”.
Result	Pass

Permission setting function set the scope of operation for users. Test cases and test results are shown in (Table 7) and the execution procedure is shown in (Fig. 22).

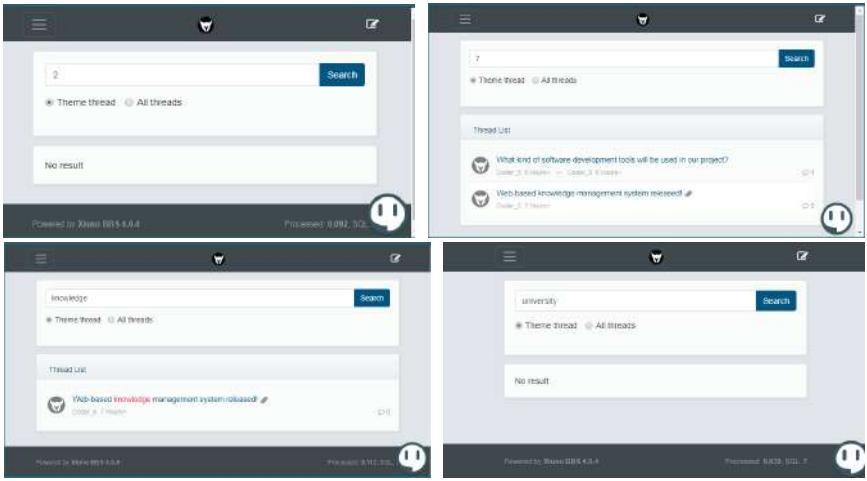


Figure 21. – User/knowledge search function testing

Table 7. – Permission setting function testing

Input and step	1 Set the permission that only team members can read and write the knowledge in the system.
Output	1 Only team member can read and write the knowledge and the visitors is forbidden.
Result	Pass

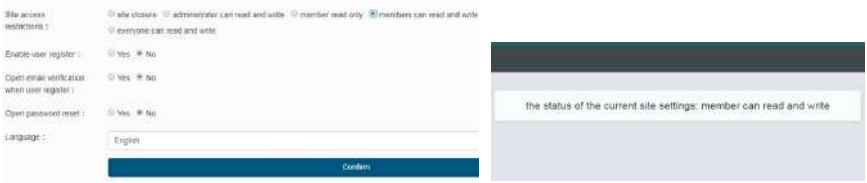


Figure 22. – Permission setting function testing

Conclusions

According to the characteristics and features of distributed software development team, this paper proposed a web-based knowledge management system. Especially, it has been verified that there are a great deal of merits for knowledge transformation from tacit knowledge to explicit knowledge and knowledge sharing. Meanwhile, the knowledge transformation often occurs in the procedure of communication among team members who have similar interests. Thus, this work emphasis the social interaction and devise a similarity calculation model to evaluate the similarity among team members.

In this work several concepts about knowledge management are proposed: knowledge type (tacit knowledge and explicit knowledge, formal knowledge and informal knowledge); knowledge management in software development methods; knowledge management process (knowledge creation, knowledge storage and retrieve), knowledge transferring and knowledge sharing. Finally, the work described the framework and implementation of knowledge management system. The framework of knowledge management system is illustrated by four elements: roles, product development, structure and forum.

References:

1. Zhen L., Jiang Z., Song H. Distributed recommender for peer-to-peer knowledge sharing. Information Science, 180, 2010. – P. 3546–3561.
2. Zhuge H. A knowledge flow model for peer-to-peer team knowledge sharing and management. Expert System with Application, 2002. – P. 23–30.
3. Walsh J. P., Henderson C. M., Deighton V. Negotiated belief structures decision performance: an empirical investigation. Organizational Behavior Human Decision Processes, 42. – P. 194–216.

CHAPTER V. IT-EDUCATION

Automated system for students' knowledge testing

Karina Melnyk
Doctor of Philosophy in Technical Science, Associate Professor
Department of Software Engineering and Management Information Technologies
National Technical University "Kharkiv Polytechnic Institute"
ORCID: https://orcid.org/0000–0001–9642–5414

Natalia Borysova
Doctor of Philosophy in Technical Science, Associate Professor
Department of Intelligent Computer Systems
National Technical University "Kharkiv Polytechnic Institute"
ORCID: https://orcid.org/0000–0002–8834–2536

Abstract. *The solution to improve the quality of the students' knowledge assessing process is proposed. The developed automated information system for knowledge testing, which based on an adaptive testing model, has been described. The positive influence of the information system usage has been proved by the results of experiment.*

Keywords: *information system, adaptive testing model, testing of students' knowledge, fuzzy mathematics*

Introduction

The needs of modern Ukrainian society, the globalization challenges of time, the changes that take place during the European integration of Ukraine, the accession to the Bologna process, are increasingly affecting on Ukrainian education. There is a need for deep and comprehensive modernization of education under such conditions. Therefore, the importance of determining the indicators for objectively assessment the level of educational services is increase. The permanent task in this sphere is the problem of assessing students' knowledge. This problem undoubtedly worries educators and it is one of the most urgent today in Ukrainian education. Formation of knowledge assessment, which corresponds to the level of students' knowledge, is a criterion for the effectiveness of the process of subjective assessment of knowledge. Today the Ukraine educational establishments and the world educational establishments use the new forms and methods of student knowledge control, based on modern information and communication technologies, in particular, computer testing of knowledge. The resolving of such tasks determined the following purpose of the work: improving the quality of the process of assessing student knowledge using an adaptive testing model.

Materials and methods

As the analysis of scientific papers shows, the most important aspect of any educational activity is the system of quality control of knowledge. Traditional evaluation methods suffer from informational unambiguousness, lack of objective measurement indicators, qualitative one-sidedness and subjective influence on the result of control. The subjectivity of knowledge assessment is related, to a certain extent, to the lack of development of controlling methods the knowledge system and the influence of the human factor, which is especially true for young teachers with insufficient pedagogical experience. Often the assessment of knowledge on a course or a separate topic occurs by presenting different requirements with the application for testing individual, often secondary elements, the assimilation of which may not reflect the level of mastering the whole system of the formed knowledge, skills. In the testing of knowledge, an important role is played by psychological factors, general and special training of the teacher, his personal qualities, which definitely occur both in the nature of teaching the material, and in the process of verification and evaluation of knowledge. The most common typical subjective mistakes in the assessment of knowledge include: mistakes of generosity, mistakes of aureole, central tendency, contrast and proximity, as well as logical errors. Pedagogical subjectivity in many cases is an important reason why students prefer computer-test forms of control with minimal participation of teachers.

As a rule, the concept of "test" interpreted among teachers is associated with a simplified version of its definition as "the choice of one answer from several proposed". The traditional test is a standardized method for diagnosing the level of knowledge and skills of students. These are, for example, tasks such as: fill in the gaps; emphasize right; cross out unnecessary; choose from the suggested options, etc.

One of the main questions in the theory of tests – is the question of choosing the best test from all possible ones. Each test differs from the rest by the number of tasks and other characteristics. The optimal one can be considered to have a relatively small number of tasks, but it provides an opportunity for deep checking of knowledge and skills. Therefore, when compiling the tests it is necessary to select the optimal number of tasks, which makes it possible to determine the level of knowledge formation relatively precisely [1].

Test control is a specially prepared control set of tasks that allows reliable, adequate and quantitative assessment of students' knowledge using statistical methods. Tests compared to traditional examinations and control work are often more objective and qualitative means of control. The possibility of standardized testing is also significantly expanded, which makes it possible to compare the level of knowledge of an individual object (student, group, stream) from a specific subject with an intermediate level or with a similar object from the same or another higher educational establishment.

At test control, it is not difficult to ensure comparability for all participants in the conditions, the application of common criteria for the evaluation and interpretation of results.

Testing as an objective standardized definition of the individual level of knowledge has several independent stages: the development (design) of the test, approbation the test, conducting test exams, evaluating individual results (measurements), ranking, that is, determining the place of individual results on a preprepared scale of evaluation, generalized analysis of results (making recommendations), re-testing if necessary.

One of the most important stages in the practice of introducing a testing procedure is the ongoing control of mastering the material in the learning process. Hence, a distinction is made between the assessment of the end result (achievement of the standard) and the periodic current testing to determine the personal achievements of the students (the dynamics of the process of acquiring knowledge) for a certain period. In accordance with the type of control (final or current) the structure of the test is formed indicating the extent of assimilation of the topic, section or the whole course [1].

The widespread use of new information technologies by educational institutions has created the preconditions for using computer testing systems to control students' knowledge at all stages of learning. The urgency of such systems is obvious not only for determining the level of preparedness, but also for monitoring the educational process, for the organization of adaptive learning, distance education.

Computer testing systems are software systems (testing systems) that allow analyzing students' knowledge using modern information technologies. The system of testing knowledge can be used both in independent work of the student and in the work of the student under the guidance of the teacher. A variety of computer testing systems of knowledge are automated testing systems for testing knowledge and skills of students in a specific domain area with the means of possible improvement of knowledge and skills. In such systems, the automatic generation of tasks and the automatic choice of test tasks are carried out based on various test objectives chosen by the teacher or the student. The test result is a numerical evaluation and a model of current knowledge. In some cases, recommendations for sections that need to be repeated or re-examined may be issued. One of the advantages of automated knowledge testing systems is that they can use sophisticated methods of presentation tasks to students, called test strategies. Automated testing systems enable the student to independently assess their level of knowledge, and the teacher to quickly and objectively evaluate real student knowledge, to systematize and simplify the process of knowledge assessment, provide a significant timesaving for the teacher.

In addition, because the development of computer testing systems is associated with the development of modern information technology, there is the possibility of improving these systems. It possible due to the application of new adaptive test control algorithms; using computer multimedia capabilities in tests;

acceleration of calculation of results; simplify administration; increasing the efficiency of testing; reducing the cost of organizing and conducting testing [2].

Thus, the using of automated testing to verify student knowledge not only facilitates the work of the teacher, but also increases the motivation of students' educational activities, while reducing their emotional tension in the control process.

There are many key benefits of computer testing knowledge:

- decreasing the verification time of a large amount of diverse educational material in a large group of students;
- the possibility of regulating a predetermined level of requirements, an automated change in the degree of complexity of questions is allowing;
- the possibility of self-control at the preliminary stage for the purpose of self-evaluation of the results of preparation for the official testing;
- the objective assessment with the exclusion of the human factor;
- the possibility of organizational feedback between a student and a teacher using the Internet;
- the possibility of generating statistical assessments of the results of control and the learning process.

The main disadvantage of computer testing of knowledge lies in the lack of the required number of highly skilled experts and experts who can formulate test tasks.

The basis of computer testing systems is a certain model of testing. The most progressive model now is the adaptive testing model, in which the complexity of the tasks varies depending on the correctness of the previous answers. Nowadays there are three versions of adaptive testing.

The first model is called pyramidal testing. In the absence of preliminary assessments, all person are given a task of middle complexity. Then each task should be easier or more difficult depending on the previous answer.

The second model is flexilevel-control. It starts from definite level of complexity that is chosen by the person who is testing, with a gradual approach to the real level of knowledge.

The third variant of testing model is stradaptive (stratified adaptive). This type of testing is carried out on tasks, divided by levels of complexity. The next task is taken from the upper level if the previous answer was correct, and from the bottom otherwise.

Thus, an automated testing system based on an adaptive model is a kind of automated testing system with known parameters of the complexity of each task ant time for answers.

In this paper, an adaptive testing model based on a fuzzy logic is proposed. The using of fuzzy logic can help both test makers and students undergoing test control.

The creating and using fuzzy characteristics can help for teachers in the development of tasks. It can help for creating tests as well. For example, a teacher can quickly determine whether a task is difficult or not. However, to say definite complexity according to the 100-point scale or to estimate the difference in the complex-

ity of the two questions is difficult task. In addition, the teacher is unlikely to be able to evaluate two tasks with approximate complexity. For example, in the case when tasks have 60 and 62 points, most likely, the teacher will assign those tasks the same complexity of 60 points. Such reasoning refer to the answer time as well.

From the student's point of view, the fuzzy assessment of his knowledge in the form of "excellent", "good", "satisfactory" and "unsatisfactory" is more clear to him than the exact number of points he scored as a result of testing. Thus, the use of fuzzy logic techniques allows for a qualitative description of the characteristics of both individual test tasks and tests as a whole, as well as better interpretation of test results.

Let consider testing algorithm [2, 3]:

1) the student chooses the starting level of tasks' difficulty of his own choice;

2) the system automatically establishes the initial level of knowledge for performing several tasks (from 5 to 10) that do not affect the overall assessment;

3) the testing begins with the average complexity of the tasks.

The number of correct answers increases after the correct answer. After that, the percentage of correct answers is calculated and the complexity of the test tasks varies. The next step is calculating of new level of training S_i as a function of the current level of training (S), the percentage of correct answers, the level of complexity and the time spent on answering the question. It is calculated $G_i = G(S_i)$.

Thus, we obtain the adaptive testing procedure (because the complexity of the tasks varies depending on the correctness of the answers to the previous questions), which uses the fuzzy mathematics (because the concept of the level of preparation, the correct answer to the question, the complexity of the task are fuzzy). It should be noted that the complexity of the task and the level of training are independent and vary independently of each other.

The procedure for changing the complexity of the task also has its own peculiarities. The complexity of questions is reduced under the following conditions:

1) the complexity is higher than "very easy" (that is, it can be reduced);

2) the answer to the question is incorrect;

3) the number of correct answers to questions of one weight complexity category is less than 33% of the critical number and passed more than a third of the questions;

4) the product of the average period of time used to answer a question of a certain weight category and the number of questions remaining before the end of the test, is greater than two-thirds of the time remaining for passing the test.

The complexity of task increases under the following conditions:

1) the complexity is lower than "very difficult", so, it can be increased;

2) answer is correct;

3) the number of correct answers to questions of one weight category of complexity is greater than 66% of the critical number;

4) the product of the average period of time used to answer a question of a certain weight category and the number of questions remaining before the end of the test, is less than a 1/3 of the time remaining for passing the test.

The calculating the new level of training S_i depends of the following parameters: the current level of training – S; the percentage of correct answers – p; the complexity of task – T; the time answer – t. All of these parameters are fuzzy.

Thus, the value of the new level of training is a function $S_i = f(S, p, T, t)$. The above parameters affect on S_i in such way:

1) the higher the percentage of correct answers, the higher the level of training;

2) the higher the complexity of tasks, the higher the level of training;

3) the longer the time answer, the lower the level of preparation.

The time control of the answer to the question is introduced to eliminate the possibility of an independent answer to the question. For example, it makes impossible to find the correct answer in the textbook, the assessment will still be low, even with the correct answers. On the other hand, if the student did not use hints, but thought for a long time, this indicates a lack of training, so the assessment will also be reduced. However, to pass the test, you need to choose the optimal test time $t_{\max}$ so that people have time to read questions and answer options, think and choose the right answer. The response time can be taken in the following way. Result of the answer to the i-th task:

$$R_i = \begin{cases} 1 - \dfrac{(t_{\max} - t_{answ})}{100}, & \textit{if the answer is write}, \\ 0, \quad \textit{if the answer is wrong}. \end{cases}$$

If $R_i > 1$, than $R_i = 1$.

If $R_i < 0$, than $R_i = 0$;

where t_{answ} – the answer time; $t_{\max}$ – the time during which there is no decrease in the rating.

The value of $t_{\max}$ cab be constant for all questions from test or can be calculated depends of task's complexity $t^i_{\max} = f(T_i)$. It is logical because more complicated task requires more time than easer task. In addition, the value of the parameter $t_{\max}$ may depend on the individual characteristics of the student.

Consider the effect of each parameter on the value of the function. The Tables 1–3 show the fuzzy output rules. They are basis for calculating the value of the new level of training. Fuzzy sets describe fuzzy characteristics that can be shown above.

Table 1. – Influence of correct answers percent *p*

Percentage of correct answers	Influence on the function
Very small	Strongly decrease S_i
Small	Decrease S_i
Average	Do not change S_i
Higher than average	To enlarge S_i
Big	To enlarge S_i
Extra large	Greatly increase S_i

Table 2. – Impact of the question complexity *T*

Complexity	Influence on the function
Very easy	Do not change S_i
Easy	Do not change S_i
Average	To enlarge S_i
Higher than average	To enlarge S_i
Complicated	Greatly increase S_i
Very complicated	Greatly increase S_i

The expert-teacher at his discretion can change the functions value of all fuzzy sets. It will entail a change of rules that use this parameter. This allows you flexibly configure the testing system. Based on this description of fuzzy sets and output rules, an active automated testing system was built [2, 4].

Table 3. – Impact of the answer time on the question t

Answer time	Influence on the function
Very small	To enlarge S_i
Small	To enlarge S_i
Average	Do not change S_i
Higher than average	Decrease S_i
Big	Decrease S_i
Extra large	Strongly decrease S_i

The process of designing an information system always begins with the development of requirements, which are presented in the software requirements specification. All requirements are divided into functional and non-functional ones. Functional requirements are divided into business requirements, user requirements, and system requirements. Non-functional requirements are divided into business rules, attributes of quality, constraints and external interfaces. The list of requirements in formal view for the information system is presented in Figure 1 in the form of a requirements diagram.

Let's consider in more detail the functional requirements of the developed system of adaptive testing. Each student at the beginning of the use of the information system must pass the authorization process. This need is determined by the fact that students from different academic groups are available for tests on different disciplines. The student can review the tests available to him after authorization. The student can see the basic information about choosing test and decide whether to pass the test or return to the menu of available tests.

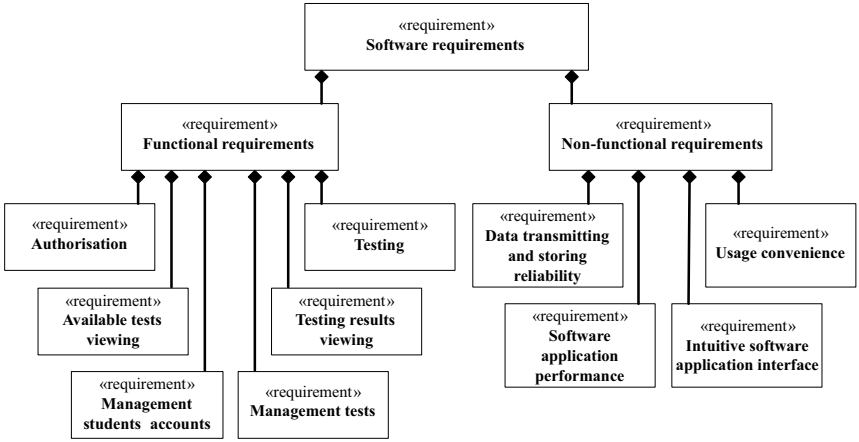


Figure 1. – Requirements diagram

The student has to select the difficulty level of the test questions. Each next question depends on the previous answer. If the student answers correctly on the task, the next question will be a question from a block with complex questions, and from a block with easy questions otherwise. A student may answer the questions or leave them unanswered if the administrator has set this option. The process will continue until the required number of questions is passed, regardless of the answers to them. The student may complete the test before the deadline, in this case the points will be scored only for those questions that were answered, the remaining unanswered questions will be considered incorrect. The response time is limited to the administrator. If the total test time is over, the results are saved and the test is completed. After completing the test, the information system calculates the final student points scored and then compares the points scored with the evaluation table according to the Bologna system. The result of the test is presented on a new page. This information consist of the total number of questions from a certain category, the list of questions, the student's answers with a correct answer, the number of student-scored points on the ECTS scale and the mark on a national four-point scale.

The authorizing administrator has the ability to edit and delete existing tests or create new ones, edit and delete existing student accounts or create new ones, view test results. The admin panel has three related items: management tests, management students' account, and testing results viewing. The possibility management tests has a list of available tests and buttons for deleting or editing the selected test, as well as a button for creating a new test. Management students' account is a list of academic groups that include students. When choosing a particular group, the administrator can view the student list for this group, as well as delete or edit the

certain student account, and create a new account. The Testing Results Viewing section represents the list of academic groups. The administrator can see a table with tests available to students in certain group. After selecting a certain test, the table is displayed in the columns shows the student's surname, name, and patronymic; test results (number of questions, number of correct answers); ECTS Scores; assessment on a national four-point scale; date and time of test start; time spent on execution.

The described functionality and behavior of the information system for a more visual representation can be represented as a use-case diagram (Fig. 2).

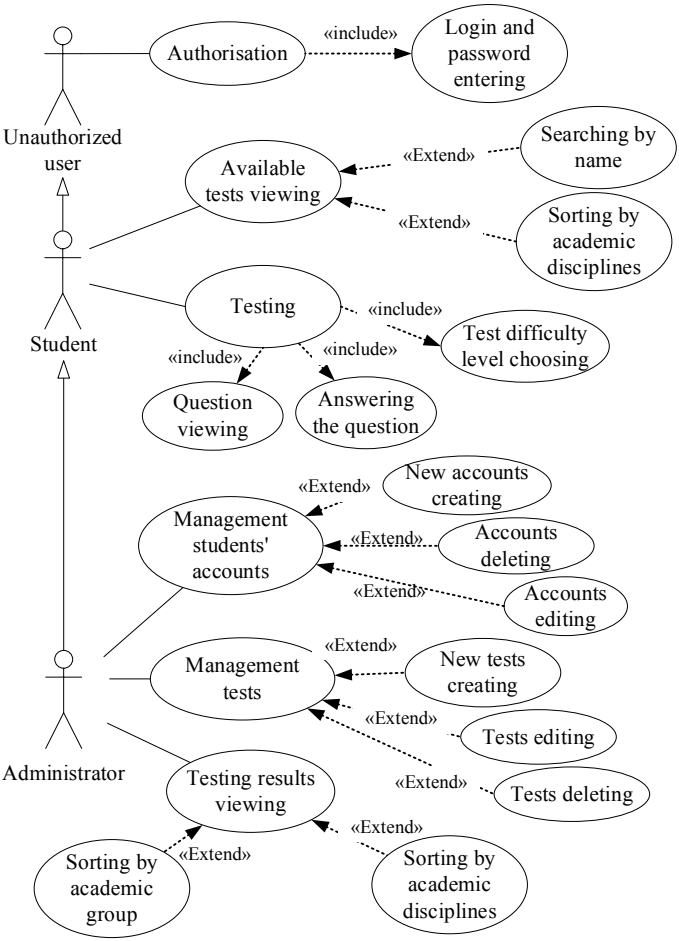


Figure 2. – Use cade diagram

The next stage in the development of any information system is the modeling and description of business processes. With the help of the IDEF0 specification the adaptive testing information system is presented as a set of functional blocks, where each block being responsible for a particular function or task. The (figure 3) shows a business processes for a knowledge testing system in the IDEF0 notation.

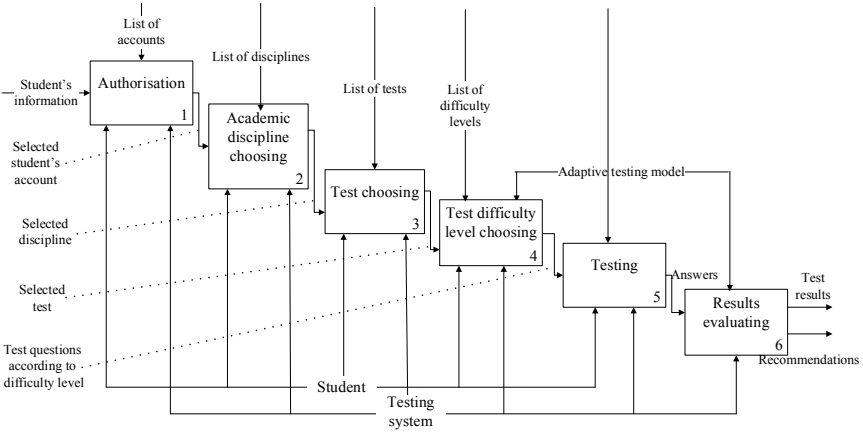


Figure 3. – Modeling the process of adaptive testing

Three-level architecture was chosen for deployment of the information system (Fig. 4). The advantages of the chosen architecture are scalability: this is the ability of the system to expand to increase the performance of this system; configurability: the isolation of levels from each other allows you to quickly reconfigure the system in case of failure; high security level and low requirements for channel speed between clients and application server.

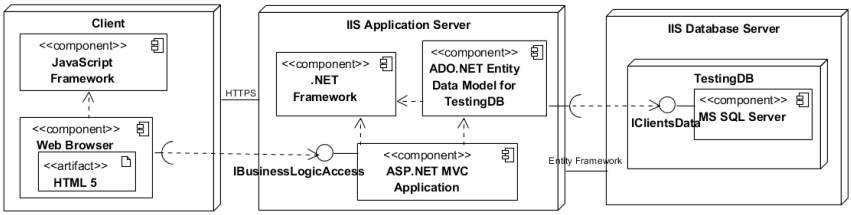


Figure 4. – Deployment diagram of information system

The following components are deployed on the Client node:

1) Web browser is a software that allows you to go to the website being developed;
2) JavaScript framework facilitates interaction with the DOM tree.

The node IIS (Internet Information Services) Application Server is the server on which the development application is deployed with the following components:

1) Web application is ASP.NET MVC web application; it interact with clients by HTTP protocol;

2) Service interfaces are the logic services interfaces of the application being developed;

3) Datamodel for Testing DB is a component that contains classes for working with a data warehouse;

4) Entity Framework is an Object-Relational Mapping that allows you to use a convenient object model for working with a SQL Server database through the standard ADO.NET library;

5) ADO.NET is a standard.NET library that provides tools for working with SQL Server through the ADO driver.

The SQL Server node is the database host site that uses MS SQL Server. This node deploys the database running the IIS node.

One of the main problems in developing almost any software solutions is the task of constructing a data model for a specific subject area, and then effective program implementation in the form of a corresponding database. The database should contain information about person, who wants to check his knowledge. Information about inner structure of each test should be presence as well. In addition, the software should provide convenient way to change list of questions in each tests. So, according to requirements the following model of the database is proposed for storing information about person and his results after knowledge testing (Fig. 5).

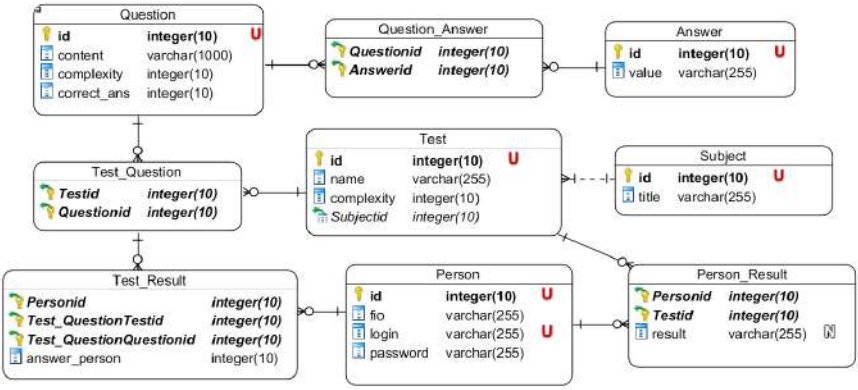


Figure 5. – Database model of domain area

The structure of Database model is consists of nine entities: Subject, Test, Question, Test_Question, Answer, Question_Answer, Person, Test_Result, Person_Result. Detailed description of entities and their attributes are presented in (Table 4).

Table 4. – Description of database model

Entity	Attribute	Attribute description
Subject	Id	Subject's Id
	Title	Subject's name
Test	Id	Test's Id
	Name	Test's topic
	Complexity	Test's complexity
	Subjectid	Which Subject belongs
Question	Id	Question's Id
	Content	Question
	Complexity	Question's Complexity
	Correct_ans	Correct answer to the question
Test_Question	Testid(FK)	Test's Id
	Questionid(FK)	Question's Id
Answer	Id	Answer's Id
	Value	Possible Answer
Question_Answer	Questionid(FK)	Question's Id
	Answerid(FK)	Answer's Id
Person	Id	Person's Id
	Fio	Name and Surname
	Login	User's login
	Password	User's Password
Test_Result	Personid(FK)	Person's Id
	Test_QuestionTestid(FK)	Test's Id
	Test_ QuestionQuestionid(FK)	Question's Id
	Answer_person	The answer for certain question from person
Person_Result	Personid(FK)	Person's Id
	Testid(FK)	Test's Id
	result	The test's result

Entities are storing following information:

– the entity «Subject» represents list of subjects, for which there are tests;

– the entity «Test» describes all possible tests for definite subjects;

– the entity «Question» represents necessary information about question;

– the associative entity «Test_Question» describes the relationship between the entities «Test» and «Question», it shows which questions belong to definite test;

– the entity «Answer» describes all possible answers;

– the associative entity «Question_Answer» represents list of wrong possible answers to definite question;

– the entity of «Person» contains information about person, who performs the test;

– the associative entity «Test_Result» shows all answer for all questions from certain person;

– the associative entity «Person_Result» contains result information about passed tests from certain person.

The created automated adaptive testing system was used in the educational process. To prove the positive influence of using this system on the level of students' professional knowledge formation due to the lack of teacher subjective evaluation and the availability of an individual approach, which provides an adaptive testing model, a pedagogical experiment was conducted. In total, 160 firstyear students were enrolled in the experiment, 80 students were enrolled into the control group, and the same number into the experimental one. In the control and experimental groups, 42 classes were conducted that did not violate the educational process and were not separated from the process of professional training.

At the ascertaining stage of the experiment, the students of both groups were determined the level of basic professional knowledge formation in accordance with the knowledge acquisition normative coefficient, which takes into account: the level of knowledge acquisition, the task complexity, the task performance quality (Table 5).

According to the results of the ascertaining stage of the experiment it was determined that the levels of formation of basic professional knowledge, the students of both groups almost do not differ, the groups are homogeneous. This provided the transparent conditions for the formative stage of the experiment.

Table 5.– Levels of knowledge acquisition

Knowledge acquisition normative coefficient	**Levels of knowledge acquisition**
From 0.90 to 1.00	High
From 0.75 to 0.89	Average
Less then 0.74	Low

At the formative stage of the experiment, taking into account the results of the ascertaining stage, a direct experimental verification was carried out in order to confirm or refute the hypothesis of the study. To ensure control over the level of professional knowledge of students of the experimental group, the developed adaptive testing system was used. In the control group, determining the level of students' professional knowledge formation was carried out by means of oral colloquium polls and conducting traditional written control works (thus, a certain probability of the teacher's influence on the student's assessment remains). The

level of students' professional knowledge formation in the control and experimental groups was assessed on the basis of the results of modular control works and works that assessed the level of self-training. Indicators of student success in experimental and control groups are shown in (tables 6 and 7), respectively.

Table 6. – Indicators of student success in experimental group

Types of tasks	Assessment on a national four-point scale,%				Qualitative success,%	Overall success,%
	5	4	3	2		
Self-training	31	59	10	–	90	100
Modular control work 1	35	55	10	–	90	100
Modular control work 2	66	34	0	–	100	100

Table 7. – Indicators of student success in control group

Types of tasks	Assessment on a national four-point scale,%				Qualitative success,%	Overall success,%
	5	4	3	2		
Self-training	20	60	20	–	80	100
Modular control work 1	23	50	27	–	73	100
Modular control work 2	27	53	20	–	80	100

After analyzing the data of the tables, it was concluded that in the experimental group the level of professional knowledge formation is higher than in the control, which testifies the quality of students' professional knowledge. The average qualitative success in the experimental group is 90%, and in the control group – 77%.

The summary data on the indicators of the level of students' professional knowledge formation by the results of the experiment is presented in (Table 8).

Table 8. – Changes dynamic of indicators of the level of students' professional knowledge formation by the results of the experiment

Level of formation	Control group			Experimental group		
	ascertaining stage,%	formative stage,%	increase/ decrease	ascertaining stage,%	formative stage,%	increase/ decrease
High	33	37	+ 4	31	50	+ 19
Average	37	40	+ 3	38	41	+ 3
Low	30	23	– 7	31	9	– 22

Conclusions

Analysis of the data in the table shows that after the formative stage of the experiment, the values of the levels of the formation of professional knowledge have changed in both groups. But as we see, the increase and decrease rates in the control group differ significantly from those in the experimental group. Thus, the results of the formative stage of the experiment confirmed the hypothesis of the research.

Thus, information system for students' knowledge automated testing is a system that provides satisfaction of the teachers' needs in the instrument for quick and effective students' knowledge assessment, as well as the students' needs in the instrument for unsubjective their knowledge assessment. The purpose of the developed information system is realized through its functions: creation and management tests, testing, management users' accounts etc. The developed information system is based on an adaptive testing model, the most progressive model now, in which the complexity of the tasks varies depending on the correctness of the previous answers. The positive influence of the information system usage has been proved by the results of experiment, which were showed in the increasing of the level of students' professional knowledge formation, because of understanding by students that only the level of their knowledge will influence on their assessment.

References:

1. Wainer H. et al., Computerized adaptive testing: A Primer, 2nd ed. – New York, USA: N. Y. Routledge, 2010.
2. Linden W. J. van der, and Glas C. A. W. Elements of adaptive testing. – New York, USA: Springer-Verlag New York, 2010.
3. Linden W. J. van der. "How to make adaptive testing more efficient?" presented at 1st Annual Conference of the International Association for Computerized Adaptive Testing, – Arnhem. The Netherlands, 2010.
4. Thompson N. A. and Weis D. A. A Framework for the Development of Computerized Adaptive Tests, Practical Assessment, Research and Evaluation, – No. 16(1), – January, 2011. [Online serial]. Available: URL: https://pareonline.net/getvn.asp?v=16&n=1. [Accessed Feb. 2, 2019].

Models and methods of preparing effective schedule in adaptive educational system

Vironika Kalachova
Doctor of Philosophy in Technical Sciences, Senior Research, Associate Professor
Department of Scientific Research
Ivan Kozhedub Kharkiv National Air Force University
ORCID: https://orcid.org/0000–0003–3477–0858

Nataliia Salo
Senior Instructor
Department of Information Technology
M. L. Kropyvnytskyy National Aviation University "Flight Academy of the National Aviation University"
ORCID: https://orcid.org/0000–0003–1422–9853

Abstract. *Kharkiv National Air Force University and Kropyvnytskyy National Aviation University "Flight Academy of the National Aviation University" are conducting research on improving the effectiveness of training and assessment of their personnel. It is based on the use of innovative information technologies; organization and implementation of distance learning (DL); construction of the adaptive and intellectual learning systems, and also quality management training systems. When creating all these systems, the main goal of the developers is to implement an individual learning path. At present, for example, in Kharkiv National Air Force University the one from main information technology for automation of learning which was developed and implemented with the purpose of effective specialists training increase is the complex of designing the academic schedule «CASCAD». Leadthrough of comprehensive analysis of features of development of programm complex, analysis of models and methods of preparing effective schedule in adaptive educational system, estimation of the productivity and advantages in the work of educational department KHNUA after embodiment in daily exploitation of the developed product, and also researches of ways of subsequent development will give «CASCAD» users and target accounts of complex to understand its wide possibilities and powerful internal potential, which are able to promote efficiency work of both educational department and all of higher military educational establishment, in general. Thus, the educational establishment, from the point of view of automation and application in the educational process of modern information technologies fully prepare to integration in educational space of European Union and to implementation of the European norms and standards in education and science Armed Forces of Ukraine.*

Keywords: *information technologie, program complex for designing the schedule, curriculum of lessons, genetic algorithm, NP-difficult task, adaptive learning system, intellectual learning system, quality management training systems, individual learning path*

Introduction

Global informatization, development of telecommunication technologies and facilities of the computing engineering significant changes in the forms of educational process. The role of professional and continuous education is growing, without interruption from the main work activity. All this contributes to the development and implementation based on information technology, distance forms and distance learning systems (DLS) and automation of learning process in general [1].

The introduction of new information technologies in the process of training and retraining of specialists in the educational system of Ukraine is due to a number of reasons: the aspiration of Ukraine to integrate into the European Union and the introduction of European norms and standards in its education and science; the intensity of the development of science requires constant improvement of professional knowledge and skills of specialists of different branches, directions and specialties; only new information technologies for learning are able to provide timely correction of the content of training military specialists at the expense of high speed updating of knowledge in the information and educational environment; high economic efficiency of new forms learning [1–3].

Kharkiv National Air Force University (KhNAFU) and Kropyvnytskyy National Aviation University "Flight Academy of the National Aviation University" (KNAU) are conducting research on improving the effectiveness of training and assessment of their personnel, based on the use of innovative information technologies by analyzing the example of the developed by KhNAFU software complex «CASCAD» of models and methods of preparing effective schedule in adaptive educational system [1–5].

Problem statement, solution and results

Analysis of existing methods for solving the problem of scheduling lessons. Problem solving of scheduling theory presents a known difficulty. In content, these problems belong to the class of combinatorial, for which dimension is essential. As a rule, the dimension of optimal scheduling tasks is so large that it is not possible to solve them by simply looking through the options.

Often, scheduling problems are reduced to problems of integer linear programming (including multi-index), for which methods of clipping or branches and boundaries are used. Traditional methods of operations research for planning problems are combinatorial procedures, simulation modeling, network methods and heuristic approaches.

In an overview of methods such as annealing simulation, graph coloring algorithm, simulation simulation, logical constraint programming, genetic algorithms, linear integer programming is given. Provides a detailed description

of methods for solving discrete optimization problems, namely, heuristic and metaheuristic algorithms, dynamic programming method, graphical method, and some others [1–5].

Methods for solving scheduling problems. Numerical mathematical programming.The task of scheduling can be represented as a problem of integer mathematical programming. In this approach, proposals from the subjects of the educational process are taken into account in the form of constraints or defined optimality criteria.

One of the variants of the mathematical model of the problem of compiling a weekly schedule of distance learning lessons is given in [1]. This model is greatly simplified by reducing the number of classesand the absence of an auditorium.

Let N be a number training groups that are grouped in R flows, r is the stream number ($r = 1...R$); k_r is the number of the training group in stream r, ($k_r = 1...G_r$), G_r – is the number of groups on stream r.

Classes are held on school days. t – number of school days of the week, T – total number of school days of higher education institution (university) ($t = 1...T$). For each group k_r is defined by the set of study days of this group T_{kr}, which is a subset of all the university days of study.

Each school day is broken down into hours (or pairs) beginning with J_s and ending with J_f. The values of J_s and J_f may depend on the working hours of the teachers (regulatory or submitted proposals); j – specific academic hour ($j = J_s \ldots J_f$).

On the basis of the syllabus, a list of S_r lectures is drawn up for each stream, with the number of the specific discipline in the list $s_r = 1 \ldots S_r$. For each k_r group, a list of Q_{k_r} scheduled counseling sessions is compiled, q_{k_r} is a discipline number in the list ($q_{k_r} = 1...Q_{k_r}$). The general Wkr training list for each group will consist of all the disciplines in these lists ($W_{k_r} = S_r + Q_{k_r}$).

Let p be the number (name) of the teacher who conducts the lectures or consultations, and P is the set of all teachers ($p = 1, \ldots, P$).

Boolean variables are introduced for each teacher p [2]:

$$\delta^{p}_{rs_r} = \begin{cases} 1, \textit{ if the } \text{lecture } s_r \textit{ in } \text{learning flow } r \text{ is delivered by a teacher } p, \\ 0, \text{otherwise;} \end{cases}$$
$$\Delta^{p}_{rk_r q_{k_r}} = \begin{cases} 1, \textit{if in } \text{group } k_r \text{ classes } q_{k_r} \text{ is held by a teacher } p, \\ 0, \text{otherwise.} \end{cases} \quad (1)$$

Since the teaching load of the teachers is planned before the schedule of classes, these values are known. Also known load for each teacher p – N_p hours per week.

According to such initial data, the task of scheduling classes is to determine for each class the day of the week and the couple, taking into account the available restrictions.

The following groups of Boolean variables are introduced to find:

$$\varepsilon_j^{tk_r} = \begin{cases} 1, \text{ if } in\ t\ day \text{ the group } k_r \ \ finish \text{ the class at } j \text{ hours}, \\ 0, \text{ otherwise}; \end{cases}$$

$$y_{rtj}^{ts_{rr}} = \begin{cases} 1, \text{ if } in\ t\ day \text{ at } j \text{ hours at the } r \text{ flow } s_r \text{ lecture is delivered}, \\ 0, \text{ otherwise}; \end{cases} \quad (2)$$

$$x_{rk_rtj}^{qk_r} = \begin{cases} 1, \text{ if } in\ t\ day \text{ at } j \text{ hours at the group } k_r \ \ q_{k_r} \text{ consultation is delivered}, \\ 0, \text{ otherwise}; \end{cases}$$

The restriction of "no more than one class can be held for each pair for each group" is as follows [2]:

$$\sum_{q_{k_r}=1}^{Q_{k_r}} x_{rk_rtj}^{q_{k_r}} + \sum_{s_r=1}^{S_r} y_{rtj}^{s_r} \le 1, r = 1 \ldots R, \ k_r = 1 \ldots Gr, t \in T_{k_r}, j = J_s \ldots J_f. \quad (3)$$

Another mandatory condition for scheduling "for each training group during the week must be completed all the types of classes planned" has the following form:

$$\sum_{t \in T_{k_r}} \sum_{j=1}^{J} \left(\sum_{q_{k_r}=1}^{Q_{k_r}} x_{rk_rtj}^{q_{k_r}} + \sum_{s_r=1}^{S_r} y_{rtj}^{s_r} \right) = W_{k_r}, r = 1 \ldots R, \ k_r = 1 \ldots Gr. \quad (4)$$

For specific tasks, the list of restrictions can be extended.

After formalization of the constraints, the criterion for the optimality of the schedule is chosen. This is a difficult question because of the principle of multi-criteria scheduling tasks. In particular, the maximum aggregate workload of teachers can be considered as a criterion. In this case, the criterion is:

$$\sum_{t=1}^{T} \sum_{p=1}^{P} \varepsilon_p z_t^p \to \max, \quad (5)$$

where ε_p – the weighting coefficient, which is determined by the status of the teacher;

z_t^p – is a boolean variable that assumes a value of 0 if teacher p has a lesson on day t, and 0 – otherwise.

The method of branches and borders. The branch-and-bound method [3, 4] is a general algorithmic method for solving optimization problems. It is widely used for such NP-complete tasks as the traveling salesman problem [1] and the backpack task [1–5]. This method is a variation of a complete batch in which subsets of feasible solutions that do not contain optimal values of the objective function are discarded.

The branches and borders method uses two procedures: branching and finding estimates (boundaries).

Through the branching procedure, the set of feasible solutions at each stage is subdivided into subsets of smaller dimension. These sets become nodes of the search tree.

The procedure for finding estimates (boundaries) determines the upper and lower bounds of the optimal value on the subsets of the feasible solutions. If the upper bound for the found node of the search tree coincides with the lower bound, then this value of the objective function is optimal and is reached on the corresponding subset of the feasible solutions.

A formal description of the method for solving problems at a minimum can be given in the following form [2].

Target function set:

$$f(x) \to \min_{x \in D}, \tag{6}$$

where D is the set of feasible solutions.

The function $b(d)$, which corresponds to the set d of splitting it into subsets $d_1, ..., d_N$, $N > 1$, is called branching.

The function $H(d)$ is the lower bound for d if:

a) $H(d) \le \min_{x \in d} f(x)$;

b) on the singular set $\{x\}$, the equality $H(\{x\}) = f(x)$ is true.

An algorithm that implements the branch and boundary method consists of a series of one-step steps. At each step there is a known record of x_0 and subsets of $t_1, t_2, ..., T_L$ of unresolved solutions. At the beginning of the algorithm $L = 1$, $t_1 = D$, x_0 is an arbitrary element of the set D or an empty set.

At each step, the algorithm starts working on checking the elements of the partition. Let the set t_j be checked. The set t_j is cut off in one of two sequentially checked cases:

a) if $H(t_j) \ge f(x_0)$;

b) if $H(t_j) < f(x_0)$ and such element y_j is found to be t_j that $f(y_j) = \min_{x \in t_j} H(t_j)$.

In the second case, there is a change in the record $x_0 = y_j$.

Let $t_1, t_2, ..., T_M$ $(M \le L)$ be the non-truncated sets.

If $M = 0$, the algorithm terminates and a record of x_0 is taken to solve the problem. At $M \ge 1$, the set for a new branch is chosen among the sets $t_1, t_2, ..., T_M$. Suppose that the set t_1. Then branching $b(t_1) = (d_1, ..., d_N)$ is carried out, as a result of which we obtain a list of sets $d_1, ..., d_N, t_2, ..., T_M$. These sets are numbered from 1 to L, and a new step in the algorithm begins.

When solving a particular problem, the methods of constructing the lower and upper estimates, the branching method, as well as the rule for selecting a promising set for partitioning should be determined.

In determining the "promising" element of partitioning, a simultaneous (multilateral) and one-way branching is generally used. With branching simultaneously, function b can be applied to any partition. Often a subset of t_k with a minimum lower bound is chosen as such element:

$$H(t_k) = \min_{1 \le i \le L} H(t_i). \tag{7}$$

In one-way branching, the number of the subset to be partitioned is known in advance.

Method of simulating annealing. Annealing simulation algorithms [1, 3] is a general algorithmic method of solving the global optimization problem; is one example of Monte Carlo methods. In the process of finding the optimal solution, it is likely to go into a state with a higher value of the objective function. This property allows you to get out of the local optima. At the beginning of the algorithm, the probability of moving to a state with a higher value of the objective function must be sufficiently high to allow the transition from the selected initial approximation to any other solution. As the algorithm works, the transition probability gradually decreases.

The algorithm is based on a simulation of the physical process that occurs during crystallization of a substance (with a gradual decrease in temperature), including the annealing of metals. It is assumed that atoms have already lined up in the crystal lattice, but transitions of individual atoms from one cell to another are still permissible. The transition of an atom from one cell to another occurs with some probability, and the probability decreases with decreasing temperature. The stable crystal lattice corresponds to the minimum energy of the atoms, so the atom either enters the state with a lower energy level or remains in place.

By simulating such a process, we look for such a point or set of points at which at least some numerical function $F(\overline{x})$ is reached, where $\overline{x} = (x_1, \ldots, x_m) \in X$. The sequence of points $\overline{x_0}, \overline{x_1}, \ldots, \overline{x_n}$ of space X is introduced. The algorithm sequentially finds the next point on the previous one, starting from the point $\overline{x_0}$ which is the initial approximation. The algorithm stops after reaching the point x_n.

The point $\overline{x_{l+1}}$ on the algorithm is calculated based on the current point $\overline{x_l}$ as follows. Operator A is applied to the point $\overline{x_l}$, which randomly modifies the corresponding point, resulting in a new point $\overline{x^*}$. The point $\overline{x^*}$ becomes a point $\overline{x_{l+1}}$ with $P\left(\overline{x^*}, \overline{x_{l+1}}\right)$ probability that is calculated according to the Gibbs distribution:

$$P\left(\overline{x^*} \to \overline{x_{l+1}} \middle| \overline{x_l}\right) = \left\{ \begin{array}{c} 1, if\ F(\overline{x^*}) - F(\overline{x_l}) < 0 \\ e - \dfrac{F(\overline{x^*}) - F(\overline{x_l})}{Q_i}, if\ F(\overline{x^*}) - F(\overline{x_l}) \geq 0 \end{array} \right\}, \quad (8)$$

where $Q_i > 0$ – elements of an arbitrary, zero-converging positive sequence that sets the analogue of the falling temperature in the crystal.

The descending rate and the descending law are set separately according to the conditions of the solved problem.

The annealing simulation algorithm is similar to the gradient descent algorithm, but due to the randomness of the choice of an intermediate point, it should be less frequent in local minima. The annealing simulation algorithm does not guarantee finding the minimum of the function, however, with the correct generation of a random point in space X, there is usually an improvement in the initial approximation.

Genetic algorithms. Genetic algorithms (GA) [1–5] allow to solve a wide range of complex problems of multicriteria optimization by randomly selecting, combining and changing modeling parameters in ways similar to biological evolution (imitation, mutation, selection). These algorithms are also used to solve graph problems.

Genetic algorithms operate on a set of individuals (populations) that encode one of the possible solutions to the problem. This makes the genetic algorithm different from most other optimization algorithms that operate with only one solution, improving it.

The principle of operation of the genetic algorithm is as follows. With the help of the function of fitness among all individuals, the population distinguishes:

– the most suitable, who are able to cross and give offspring;

– the worst, which are removed from the population and do not give offspring.

Thus, the fitness of the new generation is, on average, higher than the previous one.

There are many modifications to genetic algorithms. But all of them are versatile. That is, the task to be solved depends on the definition of adaptability and the way in which the decisions are coded. The other stages of genetic algorithms are performed equally for any task.

Each step of the algorithm consists of three stages:

1. Generation of an intermediate population by selection of the current generation.

2. Crossing individuals of the intermediate population by crossover, resulting in the formation of a new generation.

3. New generation mutation.

An intermediate population is formed from individuals who have been eligible to reproduce. The most adapted individuals can be recorded there several times, the least adapted individuals are unlikely to get there at all.

There are several ways to implement this selection:

– stochastic sampling. Let the individuals be placed on the roulette wheel so that the size of the sector of each individual is proportional to its fitness. N times when starting the roulette, we select the required number of individuals for entry into the intermediate population;

– remainder stochastic sampling. For each individual, the ratio of its fitness to the average fitness of the population is calculated. The whole part of this relation indicates how many times it is necessary to enroll the individual in the intermediate population, and the fractional indicates its probability to get there again.

After selection, the individuals of the intermediate population are randomly broken into pairs, then crossed with some probability, resulting in two offspring being recorded to the next generation or not crossed, then the new generation is recorded by the couple.

In the classical genetic algorithm, a single-point crossover operator is used: for the parent "genotypes", a section point is randomly selected, descendants are formed by exchanging the cut-off parts:

011010.01010011101 -> 101100.01010011101
101100.10011101011011010.10011101011. (9)

A mutation operator is applied to the resultant selection and crossing of a new generation. In this case, every bit of the "genotype" of each individual population is inverted with some rather small probability.

This process of evolution can go on forever. The criterion for stopping is taken by a given number of generations or population descent.

Climbing is a population state where all lines of a population are in the region of some extremum and are almost identical. That is, the crossover practically does not change the population in any way, and the mutated individuals tend to die out because they are less adapted.

Thus, population convergence means that a close-to-optimal solution is found.

For the solution of the problem take the most adapted individual of the last generation.

Ant algorithm. The ant algorithm [3] (ant colony optimization, ACO) is one of the effective polynomial algorithms for finding approximate solutions to the traveling salesman problem [1–5], as well as similar tasks for finding routes on graphs. The essence of the approach is to use an ant behavior model that looks for ways from colony to power source. The first variant of the algorithm, proposed by Doctor of Sciences Marco Dorigo in 1992, was further developed in [4] and later works.

The classic algorithm is based on the behavior of an ant colony – marking more successful pathways with a large amount of enzyme. The work begins by placing the ants at the vertices of the graph, then moving the ants. The direction of motion is determined by the probabilistic method.

Any ant algorithm, regardless of modifications, consists of the following steps, which are executed cyclically until the exit conditions are fulfilled:

I-stage "Creating ants."

The choice of the initial vertices where the ants are placed and how they are placed depends on the constraints of the task. Ants can be placed in one vertex, in different vertices with repetitions, or without repetitions. At the same stage, the primary pheromone level is set. It is initialized by a small positive number to ensure that the initial step of the transition to the next vertex is not zero.

II-stage "Finding a solution".

The probability of transition from vertex i to vertex j is determined by the formula:

$$P_{ij,k}(t) = \frac{\left[\tau_{ij}(t)\right]^{\alpha} \cdot \left[\eta_{ij}\right]^{\beta}}{\sum_{l \in J_{i,k}} \left[\tau_{il}(t)\right]^{\alpha} \cdot \left[\eta_{il}\right]^{\beta}}, \quad (10)$$

where $\tau_{ij}(t)$ is the pheromone level;

η_{ij} is the heuristic distance;

α, β are constant parameters.

The necessary compromise between these values is experimentally.

III-stage "Pheromone Update".

The pheromone level is updated according to the following formula:

$$\tau_{ij}(t+1) = (1-\rho)\cdot\tau_{ij}(t) + \sum_{k\in\{used(i,j)\}} \frac{Q}{L_k(t)}, \tag{11}$$

where ρ is the intensity of evaporation of the pheromone;
$L_k(t)$ is the price of the current junction for the k-th ant;
Q is the order parameter of the optimal solution price, that is $\frac{Q}{L_k(t)}$, a pheromone, deposited by the k-th ant on the edge (i, j).

IV-stage "Additional actions" (if necessary).

At this stage, the local search algorithm is used, but it can also be applied after finding all possible solutions to the problem.

Several variations of ACO metaheuristic models have been proposed in the literature. The most famous of them are the ant colony system (ACS) [3] and the MAX–MIN ant system (MMAS) [1].

It is advisable to note that many scientific schools conduct research in this relevant area [4]. This, first of all, takes into account the peculiarities of practical application of the developed methods and techniques.

Ant-related algorithms are methods of collective (swarm) intelligence that describe the complex collective behavior of a decentralized, self-organizing system. These methods are considered in the theory of artificial intelligence as a method of optimization.

Basic principles for solving the problem of scheduling in graph theory. The problem of compiling the optimal schedule can be solved by graph theory, in particular by modifying (by taking into account additional constraints when looking for the maximum pairwise combination) the "classical" pairing problem, which solutions are given in various formulations in [2].

Formulation of the classic vapor coupling problem. The solutions to the problem of finding a given coupling of conjugations containing as many edges as possible are based on the alternating chain method proposed by J. Peterson.

The problem of finding the largest coupling in a given bipartite graph is a classic combinatorial problem, also known as the "couple problem" [4]. Let X and Y be the set of men and women respectively, then the expression $\{x, y\} \in E$ (the set of edges of the graph) means that the man x is familiar with the woman y. Then each pairing M corresponds to a possible number of married couples, where each pair consists of a man and a woman who are familiar with each other, with each person participating in only one pair.

You can set the problem as follows [5]. Let us denote the possible conjugations of matrix A, where the terms correspond to men and the columns to women:

$$a_{ij} = \begin{cases} 1, \text{if marriage is possible} \\ 0, \text{if marriage is not possible} \end{cases} \tag{12}$$

where $i = \overline{1,m}, j = \overline{1,n}$;

m is the number of men;

n is the number of women.

We introduce an unknown quantity:

$$x_{ij} = \begin{cases} 1, \text{if the marriage } (i,\ j) \text{ is concluded} \\ 0, \text{otherwise} \end{cases} \tag{13}$$

The value of x_{ij} must meet two more requirements:

$$\sum_{j=1}^{n} x_{ij} = 1, i = 1,...,m \tag{14}$$

(any man is married to only one woman),

$$\sum_{i=1}^{m} x_{ij} = 1, j = 1,...,n \tag{15}$$

(any woman marries only one man).

To maximize marriage, you need to maximize functionality:

$$\sum_{i=1}^{m}\sum_{j=1}^{n} a_{ij}x_{ij} \to \max. \tag{16}$$

Thus, the coupling problem can be solved by means of linear integer (discrete) programming [5]. However, it is recommended to use more efficient algorithms based on graph theory to solve it.

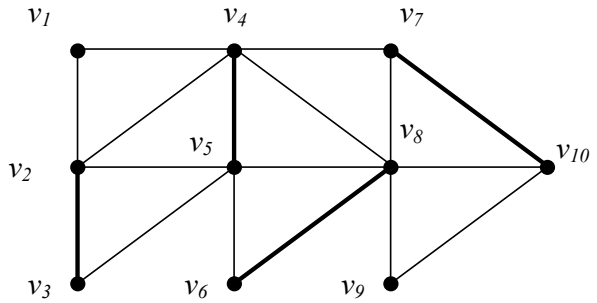


Figure 1. – Coupling on the graph

A subset M of edges of the graph $G = (V, E)$ is called a coupling if no two edges of M have a common vertices. For example, in the graph shown in (Fig. 1), the sets $M_1 = \{[v_2, v_3], [v_4, v_5], [v_6, v_8], [v_7, v_{10}]\}$ and $M_2 = \{[v_1, v_2], [v_3, v_5], [v_4, v_7], [v_6, v_8], [v_9, v_{10}]\}$ are paired. In this case, M_2 is the maximum coupling, since the coupling in G cannot have more than $\frac{|V|}{2} = 5$ edges. The problem of coupling is to find in this graph $G = (V, E)$, the maximum coupling of M. If the coupling power

is equal $\left\lfloor \frac{|V|}{2} \right\rfloor$, the largest possible value for the graph with $|V|$ vertices, then the coupling is called complete.

Consider graph G together with a fixed coupling of M in G. The edges that are in M are called the coupling edges, the other edges are called free. If $[u, v]$ is a coupling edge, then u is called a partner v. Vertices that are not incident to any of coupling edge are called free. The other vertices are combined in pairs. Let $p = [u_1, u_2, ..., u_k]$ be called alternating if the edges $[u_1, u_2]$, $[u_3, u_4]$, ... $[u_{2j-1}, u_{2j}]$ are free, while, when the edges $[u_2, u_3]$, $[u_4, u_5]$, ... , $[u_{2j}, u_{2j+1}]$, are coupling edges. The vertices that are located in odd places in some alternating path starting from the free vertex are called outer vertices. The vertices, located in even places, are called internal.

For graph G and the coupling M_1 presented in (Fig. 1), the paths $p_1 = [v_1, v_2, v_3, v_5, v_4, v_8]$ and $p_2 = [v_1, v_4, v_5, v_6, v_8, v_7, v_{10}, v_9,]$ are alternating. From the fact of the existence of these paths, it follows that vertices v_1, v_3, v_4, and v_5, v_8, v_{10}, are external, since each of them stands in an odd place in one of the paths and vertex v_1 is free. These are not all outer vertices of G with respect to M_1: v_9 and v_6 are also external, since $p_3 = [v_9, v_8, v_6]$ is an alternating path. An alternating path $p = [u_1, u_2, ... , u_k]$ is said to be incremental if both vertices u_1 and u_k are free. In (Fig. 1) the path $p_2 = [v_1, v_4, v_5, v_6, v_8, v_7, v_{10}, v_9,]$ is increasing. The great importance of the magnifying paths for the coupling problem follows from the following fact.

Let P be the set of edges of the increasing path $p = [u_1, u_2, ... , u_{2h}]$ in the graph G with respect to the coupling of M. Then the coupling of M' formed as a symmetric difference of the sets M and P, $(M' = M \otimes P \cdot (M - P) \cup (P - M))$ is the coupling of the power $|M| = 1$.

For example, the magnifying path $p_2 = [v_1, v_4, v_5, v_6, v_8, v_7, v_{10}, v_9,]$ with respect to the coupling of M_1 shown in (Fig. 1), can be used to increase M_1 to $M_3 = M_1 \oplus P_2 = \{[v_1, v_4], [v_2, v_3], [v_5, v_6], [v_7, v_8], [v_9, v_{10}]\}$.

Since M_3 is the maximum coupling (it contains $\frac{|V|}{2} = 5$ edges), it makes no sense to look for magnifying paths in G relative to M_3; there can be no incremental paths relative to the maximum coupling, as such paths could be used to increase this coupling. The reverse is also true.

Berge's theorem. The coupling of M in the graph G is maximal if and only if there is no increasing path in G relative to M.

The definition of maximum couples given in Berge's theorem is similar to the definition of maximum flows. Therefore, for the coupling problem, there may be an analog of the algorithm for constructing the maximum flow: start with an arbitrary coupling (such as an empty one) and find increasing paths. All known coupling algorithms are based on just such an idea, but they have many differences. The most fully cited ideas are used in the problem of coupling in bipartite graphs. In this case, also the most striking analogy with the maximum flow problem.

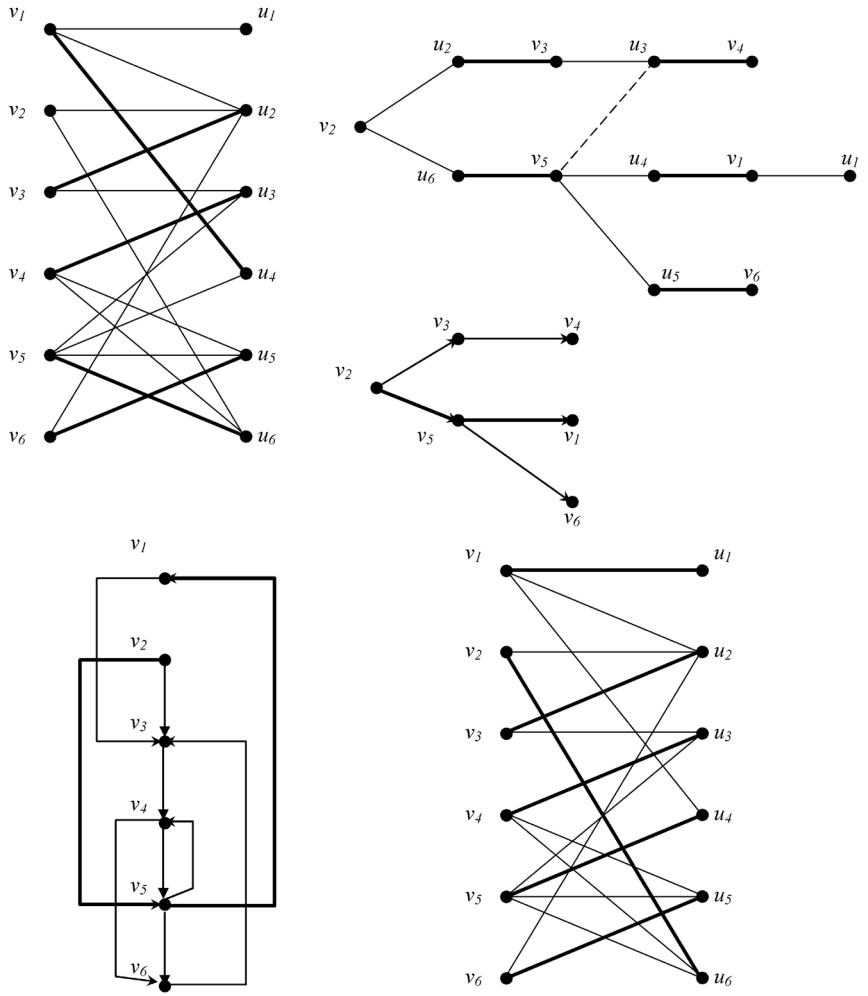


Figure 2. – An example of constructing magnifying paths on a graph

Algorithms for constructing the maximum coupling in a bipartite graph. Since the coupling problem in a two-line graph is a partial case of the coupling problem, it can be solved by repeatedly finding an increasing path p relative to the current pairing M and increasing the current coupling to $M \oplus P$.

Consider graph B and the coupling M represented in (Fig. 2 a).

Finding magnifying paths must begin with the construction of alternating paths. Since one end of the magnifying path must be in V and the other end in U, then, without losing the community, it is possible to begin by magnifying the paths only from the free vertices of the set V (in this example, from the vertex v_2).

You can search for all possible paths alternating with v_2 at the same time, according to the principle of "search wide".

Starting from vertex v_2, one can look for magnifying paths by considering all vertices adjacent to v_2, namely u_2 and u_6 (Fig. 2 b). Since vertex v_2 is free, all its incident edges are also free. By defining the alternating path, it is next necessary to consider the edges of the vapor coming from the vertices u_2 and u_6.

This step is unambiguous, since each vertex has no more than one partner. If one of the vertices u_2 or u_6 were free, the task would be accomplished – a magnifying path would be found. However, this is not the case and therefore vertices v_3 and v_5 should be added to the many alternating paths. By building v_3 and v_5 – the outer vertices. We continue to increase the paths with v_3 and v_5. The edge $[v_5, u_3]$ (Fig. 2 b) is omitted since u_3 is reached from v_3 before viewing the vertex v_5. This algorithm only eliminates unnecessarily magnifying paths. As a result, new outer vertices v_4, v_1 and v_6 are found (Fig. 2 b). The outer vertex v_6 is adjacent to the free vertex u_1. Thus, a magnifying path is found and, using it, it is possible to increase the pairing of M (Fig. 2 d).

The [1–5] provides a detailed description of the Hopcroft and Carp algorithm using the general Dinitz scheme, that is, it consists of phases corresponding to an increase in flow along the shortest increasing paths of a given length. A special kind of network, however, allows both to limit the number of phases and to build a more efficient algorithm for constructing a pseudomaximal flow in each phase. This algorithm builds an auxiliary contourless grid, or rather an auxiliary contourless graph (since the bandwidths of all edges are equal to one). In accordance with graph B is a graph oriented in such a way that all the edges that are in the coupling of M, are oriented from V to U, and all the others – in the opposite direction. First, arcs are built from the source to all the free vertices of the set V, then a search is made in the width in an oriented graph starting from the free vertices V. When finding each free vertex from the set U, an arc u, t is added to the auxiliary contourless graph. Moreover, from the moment of adding the first such vertex in the search process, the vertices that are more than or equal to the distance from s to t are no longer considered. Increasing the existing coupling along the maximum set of shortest magnifying paths with pairwise different sets of vertices is realized by the following procedure. An in-depth search of the auxiliary graph is ongoing, starting with source s. Each time stack t is reached, the stack contains a sequence of vertices, which is an alternating path. Then there is an increase in steam coupling along this path. During the procedure for each vertex, either there is an alternating path that passes through it, or it is found that there is no path that passes through that vertex and does not cross any of the found paths. It follows that the procedure finds the maximum number of shortest alternating paths that do not intersect.

The [5] provides a simple algorithm for constructing a maximum coupling in a two-particle graph based on the following statement: in a graph G, a path that increases relative to a coupling M exists if and only if there exists an (s, t)-path in $\overline{G}$ which $s \in XM, t \in YM$.

The following notation is used: $G = (X, Y, E)$ is a given bipartite graph, M is some coupling in a bipartite graph G, $\overline{G} = (X, Y, A)$ is an auxiliary oriented graph that is matched to the undirected graph G and constructed coupling M: if the edge is part of coupling M, then it is set to an orientation "from X to Y ", if not included – the opposite. XM and YM are the free vertices of the sets X and Y of the vertices of the bipartite graph G.

The general scheme of the algorithm is as follows:

– build an arbitrary coupling of M in graph G;

– we construct an auxiliary graph $\overline{G}$ over graph G and coupling M: all edges of coupling M are given an orientation from X to Y, the other edges of graph v receive the opposite direction;

– perform a search in the graph $\overline{G}$ of the width of the set XM unsaturated vertices of the set YM;

– if one of the vertices of the set YM received a label as a result of the search, then a magnifying path was found. Conduct inversion of edges of the magnifying path relative to the coupling;

– if none of the vertices received a label, then the largest coupling was found.

Substantiation of the choice (development) of the most effective method (algorithm) for solving the problem of scheduling lessons. Considering the fact that a large number of constraints due to objective and subjective factors of the educational process in HEIs have to be taken into account when scheduling training sessions, such tasks have many acceptable solutions that, to varying degrees, satisfy some criterion of effectiveness. Getting the best solution is a crucial part of the scheduling process. The large dimension of the problem and its multi-parameter cause the nonlinear dependence of the efficiency of the obtained solution, which makes it impossible to choose a method of further optimization in order to find the global optimum. However, the main difficulties of applying classical methods of optimization of nonlinear functions [1–5] are related to the problems of local extremum.

A distinctive feature of the classical methods [5] is the high degree of formalization of both the formulation of the problem of scheduling classes and the algorithms of its solution ("rigid" algorithms are used). The application of such methods for scheduling classes in mass education systems is ineffective for the following reasons:

– sharply (exponentially) increasing time costs for finding the best (acceptable) solution with increasing dimension of the solved problem;

– there is no guarantee of obtaining an acceptable solution to the problem;

– it is practically impossible (due to the large dimension, complexity of the mathematical model of the solved problem) to evaluate the influence of constraints on the obtained solution.

A common disadvantage of classic methods is that they are based on an iterative search procedure or an improvement in some initial approximation. This means that the result obtained depends directly on some initial approximation and naturally there is a problem of choosing its value [4].

The application of the method of integer mathematical programming, even for relatively small problems, takes considerable time. When complying with the basic scheduling requirements, the mathematical model should include thousands of constraints and tens of thousands of variables. Therefore, not only the integer, but also the simple linear programming problem of this dimension has no prospects for optimization by exact methods. This fact fully explains why, when comparing the schedule of classes, they usually use heuristic methods in practice [5].

The main disadvantage of the branch and boundary method is the lack of a sign of optimality and, as a consequence, the need to completely solve the linear programming problems associated with each vertex of the feasible solutions. The optimal solution may be obtained long before the algorithm is stopped, but it is generally not possible to detect this, since optimality is only established after the task list is exhausted. For large-scale problems, this requires considerable and, to some extent, unjustified, time-consuming practice. In addition, it may be problematic for specific task types to obtain estimates for the branching procedure.

The task of scheduling training sessions is NP-difficult, that is, for which the algorithm of its solution in polynomial time depending on the dimension is unknown. Similar problems of large dimension cannot be solved by the simple search method. Therefore, approximate methods are used to solve them.

These methods, as a rule, are based on the use of various heuristics or heuristic algorithms [4]. Forming a class schedule using some rules (heuristics) can speed up the search for the "best" schedule, but the use of such algorithms in most cases guarantees finding only an approximate solution (reaching the local extremum). Also relevant is the problem of estimating the closeness of the solution found to the optimal one.

For many NP-heavy problems, the best solutions were obtained by annealing simulations [1]. However, their disadvantage is the high computational complexity. This is due to the fact that to obtain the necessary solution requires a rather slow decrease in the probability of transition to a state with a higher value of the objective function, which leads to a large number of iterations of the algorithm. In [5] it is shown that annealing simulation algorithms can be used to build application schedules at all stages of designing real-time computing systems. However, for the practical application of annealing methods, the problem of reducing the computational complexity of algorithms remains relevant.

Genetic algorithms can be used for a wide range of problems, including large dimensions, and are characterized by their resistance to the local optima of the surface of possible solutions. Another important feature of GA is that they can be used in tasks with a variable environment. It is problematic to use GA in cases of:

- when to find the exact global optimum;
- the execution time of the evaluation function is large;
- you need to find all the solutions to the problem, not one of them;
- the solution coding is too complicated.

Ant algorithms guarantee that the problem is solved, but the time to receive it cannot be determined. Unlike GA, the next iteration uses the memory of the entire colony, not just the previous generation. Usually, additional methods such as local search, etc. are required. For each specific type of task, it is necessary to determine the simulation parameters that can only be obtained experimentally [1–5].

Conclusions

The use of graph theory methods to solve the problem of scheduling lessons, as shown above, has exponential complexity, and for relatively large dimensions in the context of existing, often contradictory, restrictions is not appropriate.

Under uncertainty, evolutionary methods have the highest chance of achieving the desired results. Thus, it is advisable to use the genetic algorithm for the task of scheduling educational classes of HEIs.

References:

1. Distance learning. Fundamentals, concepts, perspectives. (the neck is given to the Ministry of Education and Science of Ukraine letter № 1 / II-10437 dated December 22, 2009) / Romanenko I. O., Sumtsov D. V., Kalachova V. V. , Suk O. P. // Tutorial. – Kharkiv: NTU "KhPI", 2010. – 276 p.
2. Surkov K. Yu. Kalachova V. V., and Kachan M. V. "Metod syntezu adaptyvnoho informatsiynoho seredovyshcha trenazhera pidhotovky dyspetcheriv upravlinnya povitryanym rukhom" [Method of synthesis of adaptive information environment of training simulator of air traffic controllers]. Information processing systems. – No. 1(156). 2019. – P. 118–124.
3. Analysis of the features of development, operation and further development of the complex of programs of the automated system of designing the academic schedule "Cascade" / O. M. Misyura, M. F. Pichugin, S. V. Alekseev, V. V. Kalachova, O. A. Trublin // Systems of information processing.– Kh.: KhNAFU, 2017.– № 4(150). – P. 193–198.
4. Mastering the skills of working with the software complex "Cascade" – as a way to optimize the work of the Secondary Education and European Integration of Higher Education of Ukraine / Kalachova V. V., Misyura O. M., Tretyak V. F., Kuzhel I. E., Trublin O. A., Shigimagha N. V., Shkurupiy S. S. // Educational and methodical collection of KhNAFU.– Kh. KhNAFU, 2018.– № 1(147). – P. 38–47.
5. Features of the development of the interface design of the complex program of the automated system for designing the schedule of classes at the Kharkiv National Air Force University "Cascade" / M. G. Tishchenko, O. M. Misyura, V. F. Tretyak, V. V. Kalachova, O. A. Trublin // Collection of scientific works of KhNAFU.– Kh. KhNAFU, 2018.– № 3(57). – P. 144–151.

Automation of the educational process in Ukraine higher military education institutions

Andrii Trystan
Doctor of Technical Sciences, Senior Research, Chief
Department of Scientific Research
Ivan Kozhedub Kharkiv National Air Force University
ORCID: https://orcid.org/0000–0003–0494–8125

Mykhailo Soroka
Senior Instructor
Department of Information Technology
M. L. Kropyvnytskyy National Aviation University "Flight Academy of the National Aviation University"
ORCID: https://orcid.org/0000–0003–1894–4002

Abstract. *Kharkiv National Air Force University and Kropyvnytskyy National Aviation University "Flight Academy of the National Aviation University" are conducting research on improving the effectiveness of training and assessment of their personnel. It is based on the use of innovative information technologies; organization and implementation of distance learning (DL); construction of the adaptive and intellectual learning systems, and also quality management training systems. When creating all these systems, the main goal of the developers is to implement an individual learning path. For example, at present, the main information technologies for automation of learning and realization of its distance form which were developed and implemented in Kharkiv National Air Force University with the purpose of effective specialists training increase are: the informational and educational environment «DIALOG»; the universal system for the development and conducting of computer tests; the complex of designing the academic schedule «CASCAD». In addition, the learning process successfully uses the distance learning system with the open source code – MOODLE. Thus, the educational establishment, from the point of view of automation and application in the educational process of modern information technologies fully prepare to integration in educational space of European Union and to implementation of the European norms and standards in education and science Armed Forces of Ukraine.*

Keywords: *information technologie, distance learning, computer test, program complex for designing the schedule, distance learning system, automated testing control, adaptive learning system, intellectual learning system, quality management training systems, individual learning path*

Introduction

Global informatization, development of telecommunication technologies and facilities of the computing engineering significant changes in the forms of educational process. The role of professional and continuous education is growing, with-

out interruption from the main work activity. All this contributes to the development and implementation based on information technology, distance forms and distance learning systems (DLS) and automation of learning process in general [1].

The introduction of distance learning in the process of training and retraining of specialists in the educational system of Ukraine is due to a number of reasons: the aspiration of Ukraine to integrate into the European Union and the introduction of European norms and standards in its education and science; the intensity of the development of science requires constant improvement of professional knowledge and skills of specialists of different branches, directions and specialties; only distance learning technologies are able to provide timely correction of the content of training military specialists at the expense of high speed updating of knowledge in the information and educational environment; high economic efficiency of distance learning [1–3].

Kharkiv National Air Force University (KhNAFU) and Kropyvnytskyy National Aviation University "Flight Academy of the National Aviation University" (KNAU) are conducting research on improving the effectiveness of training and assessment of their personnel, based on the use of innovative information technologies [1–5].

Problem statement, solution and results

DLS which do not require direct recognition of the diploma of the sovereign, allow you to improve your knowledge and competency in the relevant subject areas, as well as confirm your qualification, complete your certification. Such a certificate, not being a document about sanctuary, prote, to talk about the knowledge and knowledge of the predecessor, and the need for robotic teachers and assistants. Such DL do not develop only within the framework of national systems of education, but also with commercial companies.

From the organizational and technological point of view, the following models of DL are distinguished:

– is a single media model. It is inherent in the use of any one learning tool and information channel. For example, correspondence training, training radio or television broadcasts. In this model, the dominant learning tool is usually printed material. There is virtually no two-way communication that brings this distance learning model closer to traditional correspondence;

– multimedia model. Various learning tools are being used: printed manuals, computer training programs on different media, audio and video recordings, etc. However, one-way information transfer dominates. If necessary, the elements of full-time study are used – personal meetings of students and teachers, conducting of final training seminars or consultations, face-to-face examinations, etc.;

– hypermedia model. This is a third generation training that involves the use of new information technologies in the dominant role of computer telecommunications. The simplest form is to use e-mail and teleconferences, as well as audio training. In the further development of this model of distance learning involves

the use of a complex of tools such as video, fax and telephone (for video conferencing), while the widespread use of video disks, various hyper-tools, knowledge systems and artificial intelligence.

The mathematical models of the components of distance learning can be attributed to the *DLS* model, the model of the *DL* process, the model of the learner, and the model of the pupil, who formalize the individual objects and subjects of the *DL*.

The mathematical model of *DLS* consists of the following interconnected components [4]: the set of learning process objects – Θ; set of specified operations between objects of the learning process – $L = \{\lambda_1, \lambda_2, ..., \lambda_k\}$ signature of algebraic system); the set of given relationships between the objects of the learning process – $\Omega = \{\omega_1, \omega_2, ..., \omega_l\}$.

Formally, the *DLS* model can be described as an algebraic system:

$$MDLS = \{\Theta, L, \Omega\}. \quad (1)$$

As objects of the *DL* process – Θ- there can be a plurality of *DLS* teachers – *T*; a plethora of learners – *St* and many learning tools – *MnE*.

Means of *DL* can be described by many components: *TlMnE* – technical means of learning; *MdMnE* – methodical learning tools; *EMt* – educational materials; *EMnNTch* – are training tools based on new information technologies; *ESr* – educational services.

Formally, this set of means can be represented as

$$DLMn = \{TlMnE, MdMnE, ESr, EMnNTch, EMt\}. \quad (2)$$

Among all means of distance learning, particular attention is paid to *EMnNTch*, which, in turn, are also many interconnected components: *CCm* – computer communications; *LEn* – learning environment.

The learning environment is also a multitude of components: teaching aids – *TA*; means of knowledge control – *MnKCt*; means of certification – *MnCr*.

This can be formally described as follows:

$$LEn=\{TA, MnKCt, MnCr\}. \quad (3)$$

Components of many teaching aids are interactive tools – *ItMn* and non-interactive tools – *NltMn*, which in turn also have components.

A plurality of IPs consists of all kinds of conferences (*Cn*), mail messages (*MlMs*), interactive hypertext pages (*ItHPg*), and more. Many *NItMn* are electronic textbooks (*ETb*), educational audio and video (*EAVMt*), non-interactive hypertext pages (*NItHPg*), and more.

These sets of components are formally described as follows:

$$TA=\{ItMn, NltMn\}, \quad (4)$$

$$ItMn=\{Cn, MlMs, ItHPg\}, \quad (5)$$

$$NItMn=\{ETb, EAVMt, NItHPg\}. \quad (6)$$

The plurality of set Θ relations $\Omega = \{\omega_1, \omega_2, ..., \omega_l\}$. can be specified on each of the individual subsets *T*, *S*, *MnE* and subsets of the Cartesian product of these sets in any combination.

Considering the set T, you can specify a number of unary relations (properties), such as: $\omega_{i_1}^j$ – scientific degree of *j*-th teacher; $\omega_{i_2}^j$ – academic rank of *j*-th teacher; $\omega_{i_3}^j$ - position of *j*- th teacher; $\omega_{i_4}^j$ – possession of educational material for the *j*- th teacher; $\omega_{i_5}^j$ – methodological abilities of the *j*- th teacher.

Binary relations can be cited as relations $\omega_{i_6}^j$ – the *i*-th teacher is the tutor of the *j*-th student, ($\omega_{i_6}^j \in T \times St$), the relationship "to be a senior by scientific title", "to have a better teaching methodology", which are subsets $T \times T$ and so on.

An example of ternary relations $\omega \in MnE \times T \times S$ is the relation "the *i*-th teacher conducts classes with the *j*-th student using video materials" and others.

The set of given operations $L = \{\lambda_1, \lambda_2, ..., \lambda_k\}$ on Θ is formed from subsets of operations of objects of the process of distance learning *T, St, MnE,* that is to say that

$$L = L_T \cup L_{St} \cup L_{MnN}. \quad (7)$$

Model of the learning process. The learning process can be defined using the "entity-link" method. An entity is defined as an object of interest to the researcher. A connection acts as a connection between two entities. The graphical relation can be represented as the following scheme (Fig. 1).

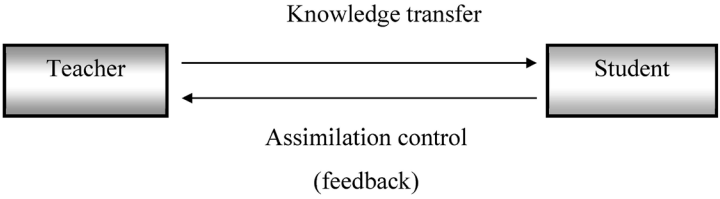


Figure 1. – Scheme of the educational process

You can clearly distinguish the following entities in this subject area:

– teacher – provides the transfer of knowledge from himself to the student (one-way communication);

– student – learns the material (according to the findings of pedagogical psychology there are four phases: perception and understanding, comprehension and memorization, application and control of knowledge [1–5]);

– knowledge control – feedback between the teacher and the subject on the level of mastering knowledge in the learning process.

Modeling of the learning process can be carried out using the following approaches:

– application of object-oriented models;
– application of design information models [1];
– the use of the method of electrical analogy [2];
– application of theoretical information models [3–5].

These models, together with traditional organizational forms of training, use teleconferences, project work, business and imitation games, discussions and more. In these forms the way of representation and assimilation of knowledge, the

form of interaction between teacher and student, which affects the description of the model, changes fundamentally. The model of the learning process takes into account various characteristics:

– assessment of learning;
– evaluation of the success rate;
– assessment of the intensity of the provision of educational information;
– assessment of fatigue in training, etc.

Process distance learning (*PrDL*) can be formally described as:

$$\Pr DL = \langle T, St, CLSm \rangle, \tag{8}$$

where T – is the set of teachers: $T = \{T_1, T_2, \ldots T_n\}$;

St – many students who study: $St = \{St_1, St_2, \ldots St_n\}$;

$CLSm$ – computerized learning system.

The process of learning in a specialty (*PrLSp*) can be represented as a composition of learning processes in all disciplines (*PrLdc*1, *PrLdc*2, *PrLdc*i, ... , *PrLdcn*) curriculum of this specialty:

$$PrLSp = PrLdc1 \circ PrLdc2 \circ PrLdci \ldots \circ PrLdcn. \tag{9}$$

Model tutor. There are several approaches to building a model of the learner [1–5]. One of the more interesting ones is the machine-learning model of the automaton theory.

When forming a model based on the theory of automatons, the methodological apparatus of theories of automatic control, queuing, information, and simulation is traditionally used. Sometimes they propose to use in the learning process an individual model of the learner, which is based on the theory of fuzzy sets. It is assumed that the learning process is a sequential process of development of separate sections of the educational material. Each stage of training ends with testing, which can have different results. The learner can control their learning process by choosing how to learn the material. Under the model of the learner is meant a fuzzy non-deterministic automaton of the form:

$$A = < U, X, Y, S_0, \delta, \vartheta >, \tag{10}$$

where $U = \{U_1, U_2, \ldots, U_m\}$ – finite set of inputs;

$X = \{X_1, X_2, \ldots, X_n\}$ – finite set of states;

$Y = \{Y_1, Y_2, \ldots, Y_p\}$ – finite set of outputs;

$\delta : X \times U \times X \to [0,1]$ – conversion function;

$\vartheta : X \times Y \to [0,1]$ – function of outputs;

S_0 – initial state.

Learning strategies are presented in the form of weighted paths of the graph of the learner model (Fig. 2).

From the initial state in the state of the first step of decision making arcs marked in those ways (*LSg*1, *LSg*2,… *LSgm*) development of educational material, the use of which, according to the learner's forecast, allows to achieve the results of intermediate testing in the first stage of training, characterized by the

highest assessment. Depending on the definition of these arcs and on the basis of the formed pairs "material development method" – "test results" these arcs are conducted from the first to n-th step of training.

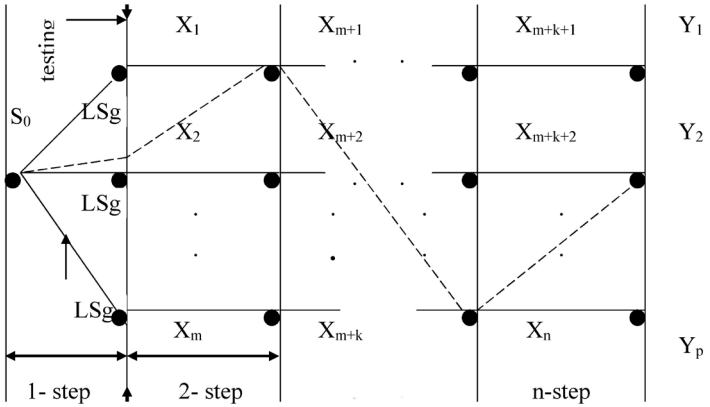


Figure 2 – Learning strategies as weighted graph waysmodels of the automaton-based tutorial

The result is a fuzzy, non-deterministic automaton that simulates the behavior of the learner, with different results of intermediate testing.

By applying the approach used in dynamic programming, it is possible to distinguish classes of instructor strategies.

First of all, the class whose strategies make it possible to achieve the learning goals and are characterized by the highest marks of the relationship between the results of the tests are of interest. To highlight such strategies, many of the final test results are determined by the results relevant to the learning objectives. The following are the results of testing in step n – 1, the transition from which to the target states of the n-th step is characterized by the methods of development of educational material with appropriate assessment.

A similar procedure is carried out for each step of the solution up to state S_0 inclusive. Using the procedure allows you to identify possible learning strategies, which are weighted paths on the graph from vertex S_0 to vertices of the set x_n.

This model allows you to identify ways to automatically correct individual instructor strategies. The peculiarity of the approach is the possibility of transferring the model of the teacher, formed by the teacher at personal contacts, into the educational environment of distance learning.

Model student. Researchers [4, 5] consider the process of distance learning in terms of student interaction with the learning system. Information about the student is given in binary, scalar, vector form, or taking into account the dynamics and nature of changes in the model of knowledge of the student [5].

Construction of specific information-theoretical models (ITM) [3, 5] of the processes of automated learning is based on general theoretical approaches and aimed at the study of two main aspects: processing of educational information aimed at the formation of images and concepts, logical circuits of algorithms, techniques of composition of algorithms, definitions; memorization of factual data and images, descriptions, definitions, algorithms and various methodical and normative materials.

To study the phenomena that arise under conditions of information overload of the user, an ITM is introduced, which describes an algorithmic system, which is a general way of determining algorithms for information transformation by a person and is intended to study the properties of such algorithms. When representing a student as an ITM, we are dealing with a set of interrelated attributes:

$$St_i = \{St_i^A, St_i^s, St_i^P, St_i^U, St_i^Q, St_i^N, St_i^Z\}, \tag{11}$$

where St_i^A – is the initial level of readiness for learning of the *i*-th student;

St_i^s – the ability to learn *i*-th student;

St_i^P – psychological properties of the personality of the *i*-th student;

St_i^U – level of preparation of the *i*-th student to work with the system;

St_i^Q – factors of the *i*-th go student's attitude to the system;

St_i^N – knowledge of the *i*-th student about the applied problem areas;

St_i^Z – the level of readiness of the *i*-th student after completion of study.

All of these attributes are complex, that is, they are simpler.

So in St_i^S can be distinguished: motor skills, linguistic skills, mental abilities, creative abilities of the *i*-th student. In St_i^P can be distinguished: attention, resistance to stress.

User operation in overload modes, unreliable output and incompleteness of input is described by the same model and results in the same results. In this case, data overload and unreliability lead to inaccurate or even erroneous decisions.

Another important approach to modeling the information activity of a user of dialog DLS is to monitor the correctness of the ratio:

$$I_\Sigma = I_{St} + I_R + I_{CS} \le I_B, \tag{12}$$

where I_Σ is the total information flow;

I_{St} – component of the input stream of information sent directly to the user without pre-processing;

I_R – depicted and regulatory information;

I_{CS} – operational information that is that part of the input information stream that is sent through the computing system;

$\overline{G}$ – the maximum amount of information.

The model of the knowledge assessment system (*MAKS*) can be described as follows [1–5]:

$$MAKS = < G, GtMn, Sc >, \tag{13}$$

where G is the set of control objectives: $G = \{G_1, G_2, \ldots G_m\}$;

$GtMn$ – control facilities: $GMn = \{CtMn_1, CtMn_2, \ldots CtMn_{m_2}\}$;

Sc – grading scale: $Sc = \{Sc_1, Sc_2, \ldots, Sc_{m_3}\}$.

The test model (MTt) can be presented at the top three models [59]:

– model of a test system ($MTtS$);

– model of testing system ($MSTt$);

– model of student testing ($TtStM$).

Studying a particular discipline involves learning a number of topics. As a result of the development of the study material, the discipline acquires N test systems. The generated set of test systems $T = \{T_1, T_2, \ldots T_n\}$ is implemented in one of the test systems $S_i = \{T_{i1}, T_{i2}, \ldots T_{in}\}$, where $S_i \in S = \{S_1, S_2, \ldots, S_k\}$. In the general case, there are K test systems at the teacher's disposal.

Testing for the i-th test (T_i) in the j-th test system (S_j) is performed on an array of students $M = \{M_1, M_2, \ldots, M_V\}$, where V is the number of students.

The boundary test is defined as $T = T_1 \cup T_2 \cup \ldots \cup T_n$.

The choice of test system is a fair expression $S = S_1 \cap S_2 \cap \ldots \cap S_k$.

The test model can be described as follows:

$$TtM = \langle V, R, Dn, MrSc \rangle, \tag{14}$$

where V – expert evaluation of the validity of the test: $V = \{V_1, V_2, \ldots, V_n\}$;

R – factors that affect the reliability of test results, including the reliability attributed to this test based on the studies performed: $R = \{R_1, R_2, \ldots, R_{n_2}\}$;

Dn – discriminative, the parameter obtained as a result of studies with the upper and lower bounds: $Dn = \{Dn_1, Dn_2, \ldots, Dn_{n_3}\}$;

$MrSc$ – scale translation scores: $MrSc = \{MrSc_1, MrSc_2, \ldots, MrSc_{n_4}\}$.

The main information technologies for automation of learning and realization of its distance form which were developed and implemented in KhNAFU with the purpose of effective specialists training increase are: the informational and educational environment «DIALOG»; the universal system for the development and conducting of computer tests; the complex of designing the academic schedule «CASCAD». In addition, the learning process successfully uses the distance learning system with the open source code – MOODLE [1–5].

As a result of conducting research on increasing the effectiveness of combat training through the use of distance learning technologies, the informational and educational environment «DIALOG» has been developed, which allows: to plan training by distributing subjects by type of training; to study as a group according to the subjects for which they are studying; organize classes in accordance with the requirements of the orders of the Ministry of Defense of Ukraine regarding the training of military specialists; to carry out automated control of testing of those who learn with automatic fixing of time and results of passing tests; control the process of learning by the average score for the group, the course through the system of statistical data generation (Fig. 3) [2, 3].

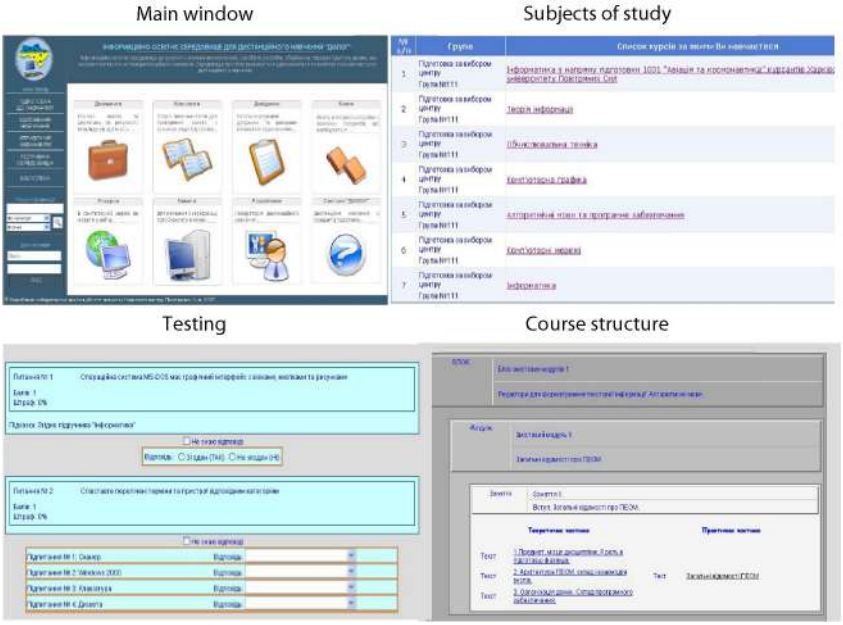


Figure 3. – The specialized informational and educational environment «DIALOG» for distance learning

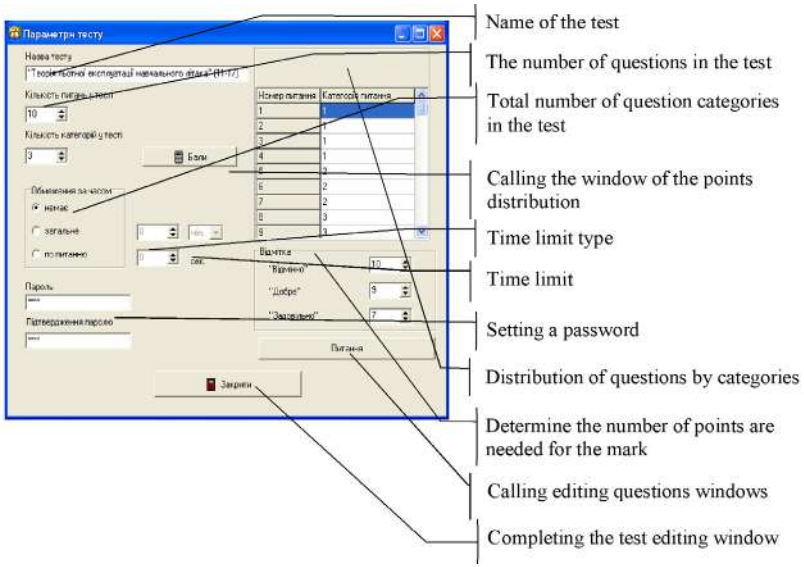


Figure 4. – The window for creating (editing) the test parameters of a universal system for developing and conducting computer tests

The universal system for the development and conducting of computer tests has been developed and implemented. The developed software application allows to solve the following tasks: locally, on separate PCs, to develop computer tests and conduct testing and self-control of those who study; choose the types of answers to questions (with one correct answer, with a few correct answers, with a response in the form of a record); divide the questions by category and type of answers and give the corresponding number of points for the correct answer; to randomly distribute questions by categories; use as a matter of a variety of document fragments (graphic, formulas, etc.) from other programs (MS Word, MS Excel, etc.); enter type of time limit and time limit; to pass the test and return to the questions; at the end of the test, analyze the responses (Fig. 4) [3–5].

Also, the MOODLE (Modular Object-Oriented Dynamic Learning Environment), a modular object-oriented learning environment, also known as a learning management system or a virtual learning environment, is deployed and used by the KhNAFU. To ensure work, it can be installed on a web server on its own computer or hosting company (Fig. 5–6) [1, 2].

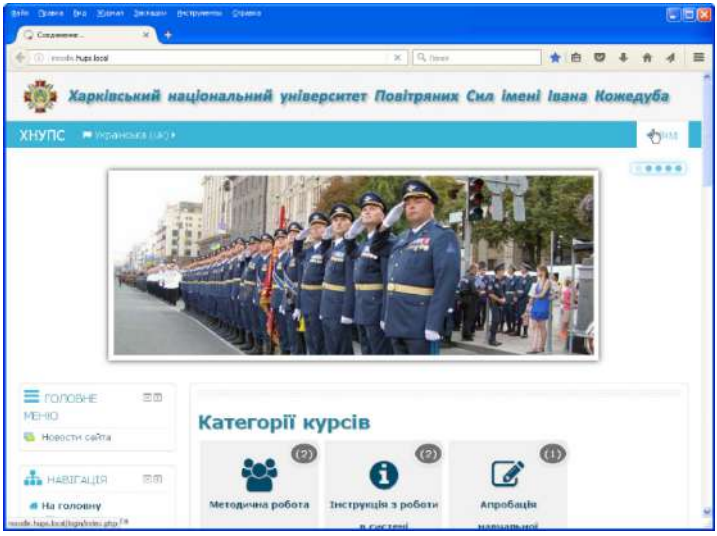


Figure 5. – The system MOODLE, deployed on the server of the university

The main advantages of the software systems developed and actively used at the KhNAFU and responsible for assessing knowledge («DIALOG», the universal system for the development and conducting of computer tests, MOODLE) are: automation of knowledge control processes for those learning; exclusion of "human factor", impartiality of evaluation; automatic fixing of test results; automatic statistical processing of test results and the formation of accounting records for personnel training [1–5].

The developed program complex of the automated system of designing the lessons schedule «CASCAD» is deployed at the work places of the educational departments of the faculties and the department of the university and is successfully used during the planning of the educational process at the university (Fig. 7) [4].

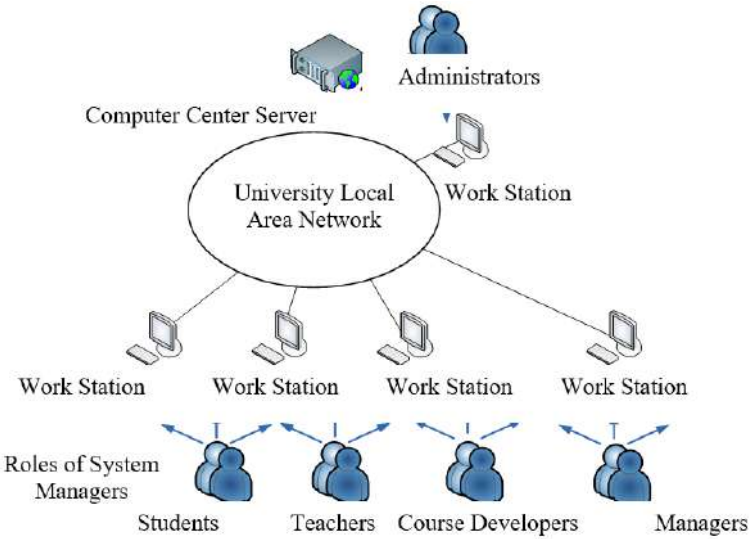


Figure 6. – The system MOODLE scheme of work

The main advantages of the developed software complex are: it is an unique software product, created at the university, which fully corresponds to the content of all stages of the planning of training sessions for the semester; automatic control of the formation lessons schedule according to the defined criterial of the quality of the lessons planning; automatic fixing of all user actions to change data; automated formation of reporting (statistical) documents for the planned learning process.

Perspective directions of improvement of the program complex «CASCAD» are: expansion of the created software complex functionality due to the development of new modules: the account of participants in the educational process; account of the success and ranking of university cadets (students); expansion of the list of accounting documents; development of procedures for the automatic formation of the basic optimized lessons schedule for the semester, taking into account the given restrictions (using genetic algorithms); creation of software modules of management and operative adjustment of curricula directly during the educational process; creation of an complex system of automated control of the Higher Military Educational Institution (based on the integrated components: personnel, logistics, planning and management of the educational process, financial support, etc.) [1–5].

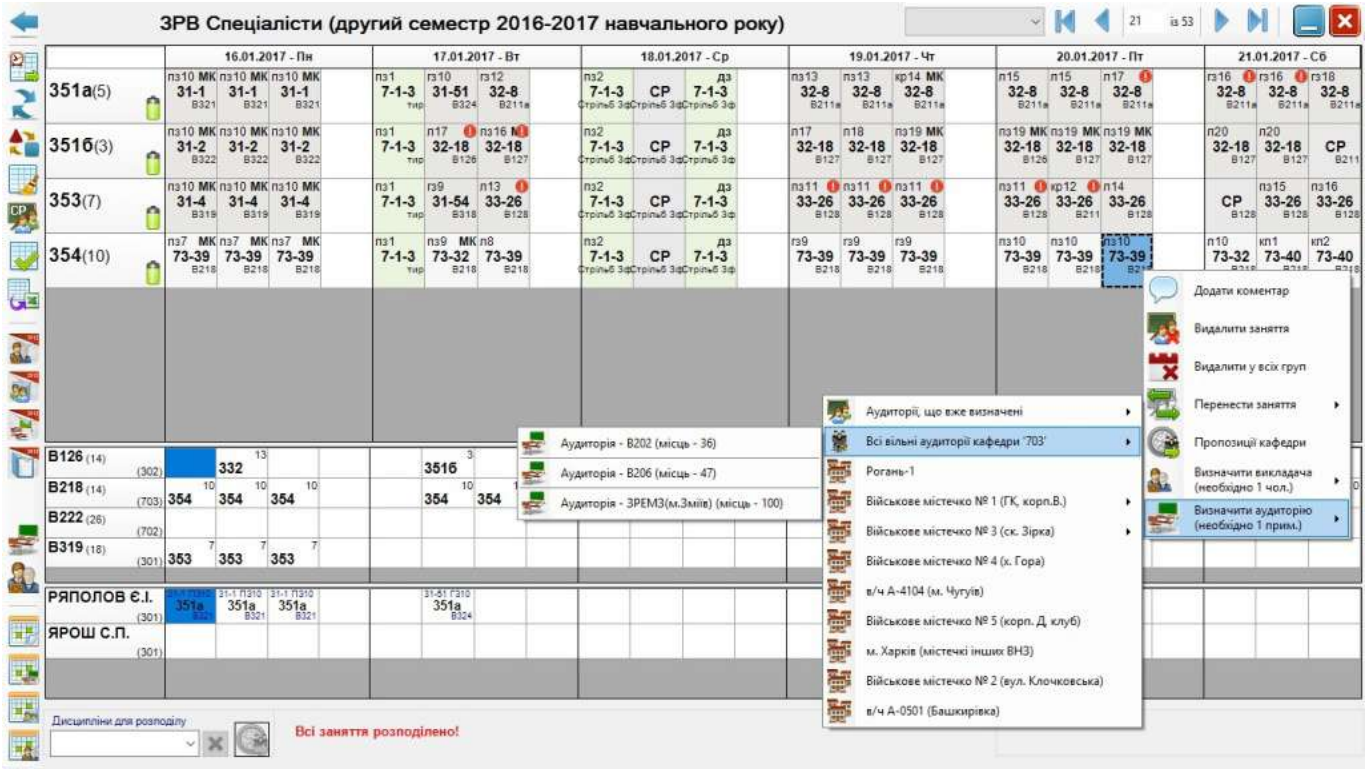


Figure 7. – User interface program complex of automated system of designing the lessons schedule «CASCAD»

Conclusions

Thus, it is necessary to mark that at present in KhNAFU and KNAU exist educational-methodical bases, hardware software and highly skilled scientifically-pedagogical compositions of universities, allow with a complete confidence to talk that educational establishment, from the point of view of automation and application in the educational process of modern information technologies fully prepare to integration in educational space of European Union and to implementation of the European norms and standards in education and science both Armed Forces of Ukraine and the Ukraine in general.

References:

1. Romanenko I. O. Distance learning. Fundamentals, concepts, perspectives. (the neck is given to the Ministry of Education and Science of Ukraine letter № 1 / II-10437 dated December 22, 2009) / Romanenko I. O., Sumtsov D. V., V. V. Kalachova, Suk O. P. // Tutorial. Kharkiv: NTU "KhPI", 2010, – 276 p.
2. Surkov, K. Yu., Kalachova, V.V., Lutsenko, A.S. and Kasatkin, M.V. (2019), "Model nechitkoho vyvodu adaptyvnoyi povitryanoyi obstanovky do rivnya pidhotovky dyspetchera upravlinnya povitryanym rukhom" [Model of fuzzy derive of adaptive air situation to the level of training of the air traffic control manager], Systems of Arms and Military Equipment, Kh.: KhNAFU, No. 1 (57). – P. 34–41.
3. Kalachova V. V. Intelligent Subsystems for Testing Knowledge for Distance Learning of Military Professionals / V. V. Kalachova, M. M. Kolmykov // New technologies – for airspace protection / Eighth scientific conference of KhAFU April 13–14, 2012 Abstracts – Kharkiv: KhAFU, 2012.– P. 132–133.
4. Ruban I. V. Ways of realization of information technology for assessing combat training of military commanders of the Armed Forces / I. V. Ruban, S. S. Tkachuk, V. V. Kalachova, A. M. Nosik, A. M. Tkachov // Science and technology of AFAFU.– Kh.: KhAFU, 2013.– № . 4 (13).– P. 14–17.
5. Tishchenko M. G. Features of the development of the interf301ace design of the complex program of the automated system for designing the schedule of classes at the Kharkiv National Air Force University "Cascade" / M. G. Tishchenko, O. M. Misyura, V. F. Tretyak, V. V. Kalachova, O. A. Trublin // Collection of scientific works of KhNAFU.– Kh. KhNAFU, 2018.– № 3 (57).– P. 144–151.

View publication stats