BRAIN. Broad Research in Artificial Intelligence and Neuroscience
ISSN: 2068-0473 | e-ISSN: 2067-3957
Covered in: PubMed.gov; IndexCopernicus; The Linguist List; Google Academic; Ulrichs; getCITED; Genamics JournalSeek; J-Gate; SHERPA/RoMEO; Dayang Journal System; Public Knowledge Project; BIUM; NewJour; ArticleReach Direct; Link+; CSB; CiteSeerX; Socolar; KVK; WorldCat; CrossRef; Ideas RePeC; Econpapers; Socionet.

2020, Volume 11, Issue 1, pages: 96-120 | https://doi.org/10.18662/brain/11.1/17

Scheme of Evaluating Information System Effectiveness of the Border Guard Service

Mykhailo STRELBITSKYI[1], Valentyn MAZUR[2], Yuriy IVASHKOV[3], Andrii KARPUSHYN[4], Serhii SERKHOVETS[5], Serhii SINKEVYCH[6], Ihor BLOSHCHYNSKYI[7]

[1] Doctor of Technical Sciences, Associate Professor, Communication, Automation and Cyber Security Department, Bohdan Khmelnytskyi National Academy of the State Border Guard Service of Ukraine. m.strelb@ukr.net

[2] Doctor of Military Sciences, Associate Professor, Institute of Advanced Training, Bohdan Khmelnytskyi National Academy of the State Border Guard Service of Ukraine, vumazur154@gmail.com

[3] Doctor of Military Sciences, Associate Professor, National Security (Border Protection) and Management Department, Bohdan Khmelnytskyi National Academy of the State Border Guard Service of Ukraine. yuriy-ivashkov@ukr.net

[4] Software engineer, Communication, Automation and Cyber Security Department, Bohdan Khmelnytskyi National Academy of the State Border Guard Service of Ukraine, andrew.karpushyn@gmail.com

[5] Candidate of pedagogical sciences, Associate professor of the Canine Department, Bohdan Khmelnytskyi National Academy of the State Border Guard Service of Ukraine. ssv_1986@ukr.net

Abstract: *The analysis of the State Border Guard Service Information and Telecommunication Systems, which provide the activity of the information and analytical units of the Border Guard Agency, has been carried out. The peculiarity of such systems lies in the requirement of true-time operation. Moreover, even a minor malfunction or a halt in operation can result in serious national scale damages. Thus, the modernization process quality evaluation will allow to choose among the many available options the most efficient and consecutively to increase the effectiveness of administrative decision-making while protecting Ukraine's borders. Based on the analysis of the researches in the field of information and telecommunication systems quality assessment, the theory of effectiveness of goal-oriented processes is proposed to use. This approach most accurately describes the system effectiveness concept as the standard to achieve the system's goal. To describe the approaches to quality assessment, the semantics of the input parameters of the effectiveness evaluation scheme has been developed and the indicator of the effectiveness of the Information and Telecommunication System functioning has been justified, on the basis of which the effectiveness evaluation scheme has been evolved.*

Keywords: *effectiveness indicator; information and analytical system; information and telecommunication system; information resource; special software.*

How to cite: Strelbitskyi, M., Mazur, V., Ivashkov, Y., Karpushyn, A., Serkhovets, S., Sinkevych, S., & Bloshchynskyi, I. (2020). Scheme of Evaluating Information System Effectiveness of the Border Guard Service. *BRAIN. Broad Research in Artificial Intelligence and Neuroscience, 11*(1), 96-120. https://doi.org/10.18662/brain/11.1/17

[6] Candidate of Pedagogical Sciences, Associate Professor of the General Military Disciplines Department, Bohdan Khmelnytskyi National Academy of the State Border Guard Service of Ukraine. sinkevich76@i.ua

[7] Doctor of Pedagogical Sciences, Professor, Head of the English translation department, Faculty of foreign languages and humanities, Bohdan Khmelnytskyi National Academy of the State Border Guard Service of Ukraine. i.bloshch@gmail.com

Introduction

The geopolitical location in central-eastern Europe is a significant factor to prioritize which security system should be built. Recently, resistance to various political, military and economic threats to national security has become urgent. These include illegal migration and trafficking in human beings, cross-border drug trafficking, smuggling of goods, illicit trade in bioresources in the exclusive (maritime) economic zone, illicit arms trafficking, international terrorism. Crisis zones and armed conflicts in and near the region, as well as their recurrent escalation, also increase the threats in the border area. All this requires an adequate response, relevant analysis and forecasting of changes to make a sound decision on counteracting those threats. Information and analytical support for decision-making on the issues of the state border protection is performed by the State Border Guard Service's Information and Telecommunication System (ITS).

Currently, information has been one of the most valuable resources that determines the level of national security of the state. With advances in information technology and increasing importance of technical means of communication, information is exposed to an increasing number of threats that, if realized, could lead to national losses. Under these conditions, the effectiveness of law enforcement bodies depends largely on the ability to adapt existing information and telecommunication systems to the present-day challenges.

This is especially true for the Border Guard Agency, which is largely related to the peculiarities of organizing protection of the state border. This includes, inter alia, state border crossings, the specifics of managing the administrative border and the demarcation line in the Joint Forces Operation area.

Automated control systems, ITS of national security entities are installed mainly on the intranet networks of the relevant agencies and have a large number of subsystems distributed throughout the state. Such systems require true-time operation and that is the major peculiarity. Moreover, even a minor flaw or delay in operation can cause serious national scale damage.

One of them is the Border Guard Agency's Integrated Information and Telecommunication System. It consists of many information systems as well as information and telecommunication systems that collaborate as a single entity, and in the common data field.

These systems can be divided into three groups that determine their functional peculiarities as well as the possibility to stop and upgrade them.

The first group includes real-time systems that are characterized by the practical lack of any possibilities to stop their functioning. The ITS automation of information-analytical systems for admission of persons, and vehicles across the State border is an example of such a system. To stop such a system for even a short period of time is unacceptable as it can lead to national losses.

The second group comprises partial stop systems, which are characterized by greater possibilities for the upgrading process. One of them is the automated data system of daily activities. These systems generally operate during the day working hours.

The third group involves full stop systems. They are distinguished by the maximum feasibility for the upgrading process. This type of system is limited only by its operational lifetime.

As far as the second and third groups concern, no significant problems during the upgrading phase ought to arise as they can be stopped to renew all the system elements.

The problem occurs with the first group ITS upgrading, which in practice is carried out element-by-element (and randomly) until the upgrading of all components is completed. In this situation it is necessary to take into account that there are thousands of elements of such a system (automated workplaces, software and technical complexes, etc.) in the border guard agency along the whole state border. Thus, at the upgrading stage of the ITS, both the old and the upgraded versions of the special software function simultaneously in the shared data field. At the same time, it is assumed that separately old and new versions of special ITS software do not create destabilizing factors. Destabilizing factors occur only in the course of joint operating old and new versions of special software in the common data field.

The key aspects in making a decision based on information processing in real-time systems are the timeliness and reliability of the user's request. At the stage of upgrading the information system, a violation of its properties may occur due to the discrepancy of special software versions.

The above requires the managers of this type of systems to clearly understand the scale of the risks involved in upgrading. One-way of identifying rational ways to modernize ITS is to evaluate the effectiveness of their functioning at the upgrading stage. Thus, defining approaches to assessing the effectiveness of functioning the Border Guard Agency’s information and analytical systems will allow taking into account the features of the upgrading process, which determines the relevance of the research.

Literary Data Analysis and Problem Statement

Defining quantitative and qualitative indices of the effectiveness of ITS functioning at the upgrading stage is quite a challenging task. It depends on: purpose of the system, conditions of its operation, information circulating in it, etc. In general, the ITS effectiveness, as a complex set of software-hardware, technical, organizational and other methods and measures, is the ability of the system to withstand the negative effects of destabilizing factors.

The majority of the researchers' study information systems only in stationary operation processes, in particular Al Rababah, (2019) provides a general analysis of the subsystems, on which the effectiveness of the information system as a whole without their mathematical modeling depends on. In the study of Cao et al. (2018), only the isolated nodes (elements) of the information system are evaluated without taking into account the cross-impact of other elements. An attempt to consider the life cycle in describing the functioning of the ITS is realized by Caniëls and Bakens (2012), which will allow to evaluate its effectiveness in general, and not only at the isolated stages.

The approaches available to assess the ITS operation effectiveness are based on two categories: quantitative and qualitative evaluation. Qualitative evaluation methods are applied in case of considerable uncertainty and are generally grounded on the experts' experience in the field. More accurate are the quantitative evaluation methods, in consequence of a thorough description of the research subject area, ITS operation detailed modeling. The use of these methods makes it possible to determine the specific significance of the evaluation of the research process and subsequently optimize it.

Maslova (2008) realizes an analysis concerning the criteria types encountered in practice. They include:

- "effect-cost" criteria type, which allows evaluating the achievement of the system operation goal at the predetermined costs, in other words-economical effectiveness;
- criteria that allow to evaluate the quality of the system by the some indicators and exclude versions that do not satisfy the established limits, using multicriteria optimization methods and discrete programming methods;
- artificially formed criteria, which evaluate the integral effect.

The above criteria make up a variety of methods and techniques that describe the process of evaluating the ITS operation effectiveness, indicating that there is no single methodological approach to solving the problem. In addition, the components of this system type introduce complex subsystems whose operation effectiveness depends on its elements and is usually described by a set of criteria with antagonistic characteristics.

The first approach to evaluating the ITS functioning effectiveness involves quality indices that operates in the "better- worse" categories. One of the methods of this approach is the expert assessment methods as a way of forecasting and estimating future results of actions on the basis of experts' predictions (International Carnahan Conference on Security Technology, 1990). The effectiveness of using this method depends on the expert's professional and intelligent level.

Another group of expert assessment methods includes multi-expert methods that ensure shaping common views owning to experts' team-work (Kupalova, 2008). Among these methods are distinguished the following: commissions, Delphi, remote evaluation, conference of ideas and others. The advantage of these methods lies in the ability to engage professionals with a comprehensive range of knowledge of theory and practice.

One more group of qualitative evaluation is a formal approach. The reference documents that regulate the evaluation procedure are evolved on the basis of previously developed standards for assessing the ITS effectiveness, practical experience of operating such systems, emergence of the new threats to the information resource and counteraction methods.

The next approach to evaluation is a quantitative approach, implemented through the use of stochastic methods and formal models. Using this approach allows to objectively determine the system quality indicators value.

Among the stochastic methods we can distinguish the following: frequency, statistical, and probabilistic ones. The frequency method of assessing the ITS effectiveness is based on the statistical material analysis and is used to determine the loss from the realization of a specific threat (Domarev, 2002).

Getting a necessary amount of statistical materials is its major disadvantage. The statistical method determines the occurrence of some threat over a certain period of time, i.e. the statistical processing of potential threats. The probabilistic method of the stochastic group determines the plausibility of the system failure as a result of destabilizing factors.

Another group of qualitative evaluation is the use of formal models, namely: matrix, multilevel, multicriteria, and optimization ones.

Some authors (Artemov, 2015) offer to apply matrix or formal models. According to this approach, the properties of the system are described by three parameters: subjects, objects and access rights. An analogue of this approach is the discretionary access model, which similarly describes the procedure for granting users of a system that act within the model as entities or processes running on their behalf, as well as the Graham-Denning model (Shcheglov, 2004). The method of determining effectiveness indicators is aggregated in the research of Maslova (2008). Its essence lies in determining the parameters; drawing up a three-dimensional matrix of relations; transformation of the relation matrix into a two-dimensional table; determination of qualitative and quantitative indicators values.

An optimization or combinatoric approach uses methods of discrete programming (discrete optimization) where the value of a function must be maximized (minimized). This approach uses linear, convex programming tools and more.

Using only one of the proposed approaches has some disadvantages. For example, using only expert evaluation methods puts at risk the final decision, which can be influenced by certain patterns and stereotypes. On the other hand, using exclusively mathematical methods requires clear source data, which are not usually available. In order to determine the ITS operation quality under ambiguity of the source data, mixed methods are proposed to use. One of such methods is comparative multidimensional analysis, the essence of which is to determine the degree of mutual influence of threats and the causes of their occurrence (Harasymchuk & Kostiv, 2011). The use of this method requires the formation of a matrix of features, for which the expert evaluation method is used. The method allows to evaluate the impact and interaction of the threats generated by experts and to rationalize the ITS upgrading processes on this basis.

One of the mixed nature approaches is risk management as an activity aimed at making and executing management decisions in order to reduce the probability of a negative result and minimize the potential losses caused by its implementation (Alekseyev, 2010). The most well-known algorithms that help optimize forces and resources in managing risks are the CRAMM and RiskWatch methods.

Using the described methods for evaluating the ITS operation effectiveness requires objective impartial data, including statistics, that may be problematic. However, the nature of the destabilization factors caused by the upgrading stage in the ITS operation is probabilistic. For this reason, this approach is considered to be the most valid one for describing the process of evaluating the ITS operation effectiveness.

A number of researches are devoted to the study of this approach, in particular (Pihur & Pohrebennyk, 2013) but only in some of them (Gribunin

& Chudovskiy, 2009) it is suggested to use the theory of effectiveness of purposeful processes. In our opinion, this approach most accurately describes the concept of system effectiveness as the degree of goal achievement by this system. However, the use of this approach is limited by the following reasons: a high degree of uncertainty in the input data, and the complexity of formalizing the operation processes.

The analysis of work in the field of evaluating the ITS effectiveness showed a sufficiently wide range of methods used. However, the use of each of them requires taking into account the probabilities of destabilization factors caused by the modernization stage. Moreover, a number of methods cannot fundamentally take into account the factors that are caused by the cooperation of border guard personnel with the ITS undergoing modernization.

Thus, existing approaches to assessing the ITS operation effectiveness do not allow taking into account the specific features:

- ITS functioning;
- ITS application in different conditions of the environment;
- the emergence of destabilizing factors regarding the ITS operation at the upgrading stage;
- the occurrence of destabilizing factors in relation to the information resource caused by the joint operation in the common data field of special software different versions.

The above needs to solve a number of problems that will allow us to reasonably come up to the development of approaches concerning the ITS operation effectiveness evaluation at the upgrading stage.

The Purpose and Objectives of the Research

The **purpose** of the research is to develop approaches to evaluating the State Border Guard Service's information and analytical systems' operation effectiveness at the upgrading stage.

To achieve this goal, the following tasks were set:

- to develop semantic aspects of input parameters formation to the estimation scheme of ITS operation effectiveness;
- to substantiate the indicator of the ITS operation effectiveness;
- to develop a scheme for evaluating the ITS operation effectiveness;
- to investigate the results of applying approaches to evaluating an experimental sample of the State Border Guard Service's Information and Analysis System operation effectiveness at the upgrading stage.

Semantics of Input Parameters of Evaluating the Scheme of Information and Telecommunication System Operation Effectiveness

Information and analytical systems of the agency-level integrated and information system operate critical assets for decision-making by border guards. Compliance with the information resource and ITS properties is generally the main task in terms of their adaptation to the current challenges. Some sources (Benmoussa et al., 2018) focus on meeting the needs of the system users. The concept of observing the ITS information resource properties or its security insurance presupposes the activities aimed at preventing unauthorized actions against this information in the system. The foregoing allows us to formulate the concept of ITS functioning as a goal-oriented process with the sole (that is fundamental) purpose - to prevent violations of the information system's properties as well as information resource in it throughout the ITS life cycle. It should be noted that in this definition the system is considered in isolation from the external environment, namely from the conditions of the system operation and the system exploitation.

Some authors (Chen et al., 2010) consider the ITS functioning effectiveness from the perspective of information system strategies, such as: ITS compliance with the organization strategy, functional development and the system impact on the organization. This approach over-complicates the process of assessing the ITS effectiveness due to the expansion of the subject area and the complexity of its formalization.

Some researches (Kavun et al., 2008) use the concept of the external environment as a basic condition for ensuring the ITS functioning. The quality of the system functioning depends not only on the degree of its properties observance and the information resource characteristics, but also on the ability to prevent the negative impact of the environment. Basically, all researchers who consider the concept of "external environment", evaluate only its negative impact on the system operation quality. The external environment is seen as a source of threats: the activities of organizations (individuals), the impact of natural disasters, the upgrading process, and so on. This approach to this concept consideration is reasonable, it actually makes sense to count only the negative impact, since the positive one does not broadly reduce the quality of ITS functioning. At the same time, the environmental impact can also have a positive effect on the ITS functioning or offset the negative effects on its quality. As part of this approach, the ITS external environment is considered not only the negative side but also as an uncontrolled influence on the whole system functioning.

It should be noted that the State Border Guard Service's information systems are vulnerable, first of all, to such information resource properties, as accessibility and integrity. It is the quality of the service performance by ITS in compliance with the information resource properties that significantly affects the effectiveness of the border guard agency's ITS exploitation and, in turn, the state national security. The peculiarity of the State Border Guard Service's Information Systems functioning is the employment of leased communication channels for the data transmission to the border protecting bodies and units. Therefore, for example, reducing the channel bandwidth or short-term channel cutoff by the owner cannot be classified as unauthorized actions against the system information, but such violation is an information destabilizing influence on the quality of ITS functioning. Such actions fall under the category of "external environment".

Let us define the concept of "external environment", which is a set of objects that neither make up the ITS, nor directly perform its functions, but affect the system goal achievement. Hereinafter, the term "external environment" will be savvied as a set of the ITS operating and exploiting conditions.

Basically, the ITS functioning can be imagined as a complex man-machine (ergatic) system with many possible states, which communicates with the external environment and manages its own resources in order to achieve the goal.

When it has to do with ITS, "external environment" is considered to be the system application conditions, which are subject to various types of destabilizing factors of an objective nature, as well as the management system and the developer's upgrading.

The management system (ITS manager) does not directly belong to the ITS, but has a direct impact on the system resources availability, determines the exploiting conditions and the functioning conditions through the ITS manager. For instance, the Border Guard Agency's ITS manager is the Administration of the State Border Guard Service. When ITS is created, the technical conditions of the specified system deployment are defined, and the resources for its creation are allocated by the manager.

When the administrative function is implemented, the Administration, through appropriate authorizing documents, establishes the procedure for the ITS usage in state border protecting bodies. Getting feedback through evaluating ITS operation effectiveness allows the Administration to adjust the operation conditions and the system exploitation as a whole. If an existing system needs to be upgraded, the manager sends a requirement description to the developer for its upgrade. The developer, in turn, having received the task to upgrade the system, takes into account the usage conditions and makes changes in the system. Upgrading ITS components leads to a change of the system operation effectiveness indicator, which, after its evaluation, is compared with the normative value. On the grounds, a decision is made by the management system to introduce the changes, alter the system operating conditions or determine the acceptable conditions for the ITS usage. It also takes into account the ability to regulate the resources allocated to ensure ITS functioning in order to comply with the effectiveness indicator to a given criterion.

Thus, ITS modernization can be considered as a set (sequence) of actions, coordinated over a period of time, aimed at achieving the goal of this process. When evaluating effectiveness, it is important to pay attention to the fact that this is a property of the process, not of the system itself. Therefore, from this point on the concept of the ITS functioning effectiveness will be considered as a complex property of a goal-oriented process, which is characterized by the degree of its achievement.

In assessing the quality of the system functioning described by n - a measurement vector indicator $Y_{\langle n \rangle}$, it is necessary to determine a set of criteria, which belong to the matching criteria class $\{G\}$, the mathematical formulation of which is the following [17]:

$$G : \left(Y_{\langle n \rangle} \in \left\{ Y_{\langle n \rangle}^{A} \right\} \right), \qquad (1)$$

where $Y_{\langle n \rangle}$ - indicator of quality of ITS functioning; $\left\{ Y_{\langle n \rangle}^{A} \right\}$ - a set of permissible entries of the functioning quality indicator.

Thereby, the system, for which the condition (1) is fulfilled, fits the goal and performs its functions.

Among the many system properties there are those that determine the quality of its functioning. The normative documents define the functional criteria, which describe the functioning requirements that ensure the correct ITS operation. In particular, it is the adherence to the requirements concerning the system information resource: confidentiality, integrity, availability, accountability, which determines many types of quality indicators (properties of the information resource):

$$p = \{i, c, a, u\}, \qquad (2)$$

where i - integrity; c - confidentiality; a - availability; u - accountability.

At the same time, some resources are required to make the system function at a given effectiveness level. Thus, ITS can be characterized by three properties at any time:

- effectiveness - the property of the system to ensure the fulfillment of information processing tasks;
- resource-intensiveness, which is characterized by the consumption of system resources (logistical, time, etc.);
- efficient response - the ability of the system to perform information processing tasks within a specified time period.

From the above we can conclude that the quality of ITS can not be characterized by isolated properties, but is determined only by the battery of the three properties.

Let us introduce these properties identifiers:

$V\langle n_1 \rangle$ - an effectiveness indicator;

$R\langle n_2 \rangle$ - a resource-intensiveness indicator;

$T\langle n_3 \rangle$ - time indicator,

where n_1, n_2, n_3 the corresponding vector dimensions.

Then, an indicator of ITS quality will be n - a measurement vector containing three groups of properties:

$$Y_{\langle n \rangle} = \left\langle V_{\langle n_1 \rangle}, R_{\langle n_2 \rangle}, T_{\langle n_3 \rangle} \right\rangle, \qquad (3)$$

where $n = n_1 + n_2 + n_3$.

The partial indicators within the groups may be wound up by entering generalized indicators. So, in most cases, the resource-intensiveness can be cost-effective, and then (3) will acquire the form:

$$Y = \langle v_i, v_c, v_a, v_u; r; \tau \rangle, \qquad (4)$$

where v_i - the integrity indicator; v_c - confidentiality indicator; v_a - availability indicator; v_u - accountability indicator; $r = \sum_{r_i \in R} r_i$ - the resource-intensiveness indicator; τ - time indicator.

It is necessary to take into account that the generalized indicator loses physical value, when heterogeneous indicators are converged. So, it is correct to wind up the indicators only within the groups of result indicators in multicriteria analysis. Convergence of the systems functioning quality indicators in different groups is unacceptable.

The physical sense of the effectiveness indicators, which provides information resource properties, lies in determining the time during which its property will not be violated.

The physical sense of the time indicator is to determine the operating time of all ITS components, which ensures the normative level of their functioning. In terms of reliability, this is a failure experience and is described by the well-known functional dependencies of the reliability theory. This indicator is a component in the formation of effectiveness indicators and can be curtailed in them.

Similarly, the resource-intensiveness also depends on the time the system is running. However, the ITS information and intelligence units' deployment involves the consumption of certain resources but in case of their deficiency the permission to operate them is refused. Therefore, this indicator does not require research and can be excluded from the vector of quality indicators of the system functioning and be taken into account separately when comparing two systems with the same values of quality indicator.

Thus, the vector of quality indicators of ITS functioning (4) will take the form

$$Y = \langle v_i, v_c, v_a, v_u \rangle. \qquad (5)$$

It is worth noting that the components of the vector are quantitative characteristics of the quantitative results of the process of the system functioning. We will assume that their qualitative characteristics are provided in advance before its exploitation begins. The same remark applies to the qualitative characteristics of the resource.

Substantiation of the Effectiveness Indicator of Information and Telecommunication System Functioning

To evaluate the information and analytical system functioning, it is necessary to develop the effectiveness indicator of its functioning, which must meet the basic requirements (Petukhov & Yakunin, 2006):

demonstrability (adequacy), criticality (vulnerability), complexity (completeness), stochasticity and simplicity.

Demonstrability allows us to evaluate the ITS operation effectiveness in terms of its main task performance. Therefore, the system goal should be clearly stated in the system effectiveness indicator. The criticality of the indicator shows how sensitive it is to changes in the characteristics of the ITS functioning process. The complexity of the indicator permits us to solve the problem of determining the system effectiveness without involving its other characteristics. Stochasticity will allow taking into account uncertainty of system functioning conditions, influence of destabilizing factors, which have the random character. The simplicity of the effectiveness indicator contributes to its accessibility, as well as to the analysis of the quality of its functioning.

Let us draw attention to the fact that the effectiveness indicator, which will be considered below, meets all of these requirements. It is known that effectiveness is a complex property of the system functioning process, which characterizes its ability to achieve the goal by the system. Let us consider that the quality of the tasks performed by the system is determined not only by the final effect, but also by the resources that are spent to achieve the system goal (including time resources). Together with the above, the indicator takes into account the conditions of the system operation and exploitation.

The effectiveness indicators of the system are influenced by external and internal factors, which are determined by its environment. Each of the components of the vector depends on the characteristics of the system and its organization, the conditions of the system operation and usage.

$$Y = Y\left(A_1, A_2, B_1, B_2\right), \qquad (6)$$

where A_1 - the ITS characteristics; A_2 - characteristics of the process organization of ensuring the system functioning; B_1 - characteristics of the ITS operating conditions; B_2 - characteristics of the ITS application conditions.

On the other hand, the components of the vector Y^A of acceptable values also depend on the conditions of the system usage and are determined by the control system

$$Y^A = Y^A\left(B_2\right). \qquad (7)$$

In the general case, the ITS characteristics, its organization, operation and application conditions are affected by a number of random factors, which determine these variables as stochastic. However, the acceptable values of the vector Y^A, which depends on the conditions of the system usage are a priori random, since it is not known in advance what the results of the ITS operation should be in order to ensure the necessary level of its functioning. Some researches assume the worst case scenario (in terms of ensuring the correct ITS functioning) when the conditions of the system usage and functioning are determined, that is, the magnitudes B_1 and B_2 are not accidental. This assumption leads to unreasonable high resource expenses.

All constituents of the vector of quality indicators of the ITS functioning are probable, therefore

$$\begin{aligned}\hat{Y} &= Y\left(\hat{A}_1, \hat{A}_2, \hat{B}_1, \hat{B}_2\right),\\ \hat{Y}^A &= Y^A\left(\hat{B}_2\right).\end{aligned} \qquad (8)$$

As a result of the actual the ITS operating conditions, the suitability criterion (1) will emerge

$$G:\left(\hat{Y} \in \left\{\hat{Y}^A\right\}\right). \qquad (9)$$

From formula (9) we can conclude that the ITS suitability is a random event that does not directly reflect the quality of the process. Therefore, the characteristics of the ITS functioning quality is the accidental probability

$$P_g = P\left(\hat{Y} \in \left\{\hat{Y}^A\right\}\right). \qquad (10)$$

To determine the effectiveness indicator, the desired distribution function of a random vector should be specified, a universal form emerges as:

$$F_{\hat{Y}}(Y) = P\left[\left(\hat{v}_i \le v_i\right) \wedge \left(\hat{v}_c \le v_c\right) \wedge \left(\hat{v}_a \le v_a\right) \wedge \left(\hat{v}_u \le v_u\right)\right]. \qquad (11)$$

As far as this problem concerns, namely the vector components of the quality indicators of the ITS functioning, the physical value of which is the time, when the information resource properties will not be violated, more convenient and informative form of integral distribution rule can be expressed like this:

$$\Phi_{\hat{Y}}(Y)=P\left[(\hat{v}_i>v_i)\wedge(\hat{v}_c>v_c)\wedge(\hat{v}_a>v_a)\wedge(\hat{v}_u>v_u)\right], \qquad (12)$$

the physical value of which lies in the likelihood of observing the information properties within a specified time frame.

The above allows us to lay down the full probability formula to achieve the ITS goal in the following way:

$$P_g=P\left(\hat{Y}\in\left\{\hat{Y}^A\right\}\right)=\int\limits_{-\infty}^{\infty}\int\limits_{-\infty}^{\infty}\int\limits_{-\infty}^{\infty}\int\limits_{-\infty}^{\infty}\Phi_{\hat{Y}}(Z)\,dF_{\hat{Z}}(Z), \qquad (13)$$

or

$$P_g=\int\limits_{-\infty}^{\infty}\int\limits_{-\infty}^{\infty}\int\limits_{-\infty}^{\infty}\int\limits_{-\infty}^{\infty}\Phi_{\hat{Y}}(Z)\,f_{\hat{Z}}(Z)\,dv_i^A dv_c^A dv_a^A dv_u^A, \qquad (14)$$

where $f_{\hat{Z}}(Z)$ is the probability density distribution of a random vector $\hat{Z}$.

Therefore, P_g probability is an ITS effectiveness indicator, which determines the degree to which it performs its functional tasks. On its basis, the criterion of system suitability is formed, i.e. $P_g \geq P_g^{st}$.

Scheme Development for Evaluating the Information and Telecommunication System Functioning Effectiveness

The semantic aspects of the input parameters describe the components of the vector $V\langle n_1\rangle$ as indicators of ITS effectiveness, which are quantitative characteristics only of the quantitative results of the system. It should be noted that such an interpretation is permissible only if the qualitative characteristics of the performance components are observed. That is, the quality of ensuring the ITS functioning is provided even before the system "starts". The above requires evaluating the effectiveness of the security process in two stages (Fig. 1).

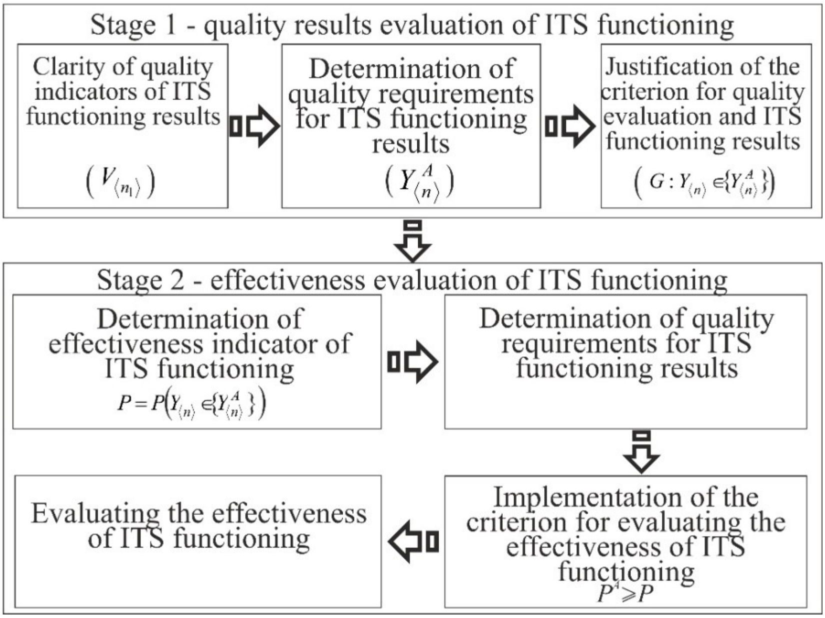
Stage 1 - quality results evaluation of ITS functioning
Clarity of quality indicators of ITS functioning results
$\left(V_{\langle n_1 \rangle} \right)$
Determination of quality requirements for ITS functioning results
$\left(Y^{A}_{\langle n \rangle} \right)$
Justification of the criterion for quality evaluation and ITS functioning results
$\left(G : Y_{\langle n \rangle} \in \{ Y^{A}_{\langle n \rangle} \} \right)$
Stage 2 - effectiveness evaluation of ITS functioning
Determination of effectiveness indicator of ITS functioning
$P = P\left(Y_{\langle n \rangle} \in \{ Y^{A}_{\langle n \rangle} \} \right)$
Determination of quality requirements for ITS functioning results
Implementation of the criterion for evaluating the effectiveness of ITS functioning
$P^{A} \geqslant P$
Evaluating the effectiveness of ITS functioning

Fig. 1. Steps of evaluating the effectiveness of ITS functioning

At the stage of evaluating the quality of the ITS functioning results:

- the quality indicator of the ITS functioning results is determined through the vector of quality indicators of its functioning;
- the quality requirements for the ITS functioning results are determined through the set of allowable values of the ITS quality indicator;
- the quality evaluation criterion of the results of ITS functioning is grounded.

At the stage of evaluating the ITS effectiveness:

- the effectiveness indicator of the ITS functioning is determined as the probability of the goal achieving by the system;
- the requirements for the effectiveness of ITS functioning are determined due to the minimum permissible value of the probability of the system goal achievement;
- the effectiveness evaluation indicator of ITS functioning is implemented as a matching criterion;
- the direct evaluation of the ITS effectiveness is carried out.

Generally, the ITS operation effectiveness is proposed to be determined by the probability of the functional tasks performed by the system under the conditions of both external and internal destabilization factors. Defining the vector of quality indicators' values is carried out in accordance with the ITS structure.

Discussion of the Results of Application of Effectiveness Evaluation Scheme of Information and Telecommunication System Functioning

In order to determine the type of distribution function of the ITS quality indicators at Bohdan Khmelnytskyi National Academy of the State Border Service of Ukraine, an ITS experimental version of the Border Guard Agency units was launched. Conducting research of the process of upgrading special software (SSW) allowed us to determine the specific type of distribution functions of each of the quality indicator components of the system functioning.

Fig. 2 shows the dynamics of changing the probability that data arrive at an ITS element from another version of the special software.

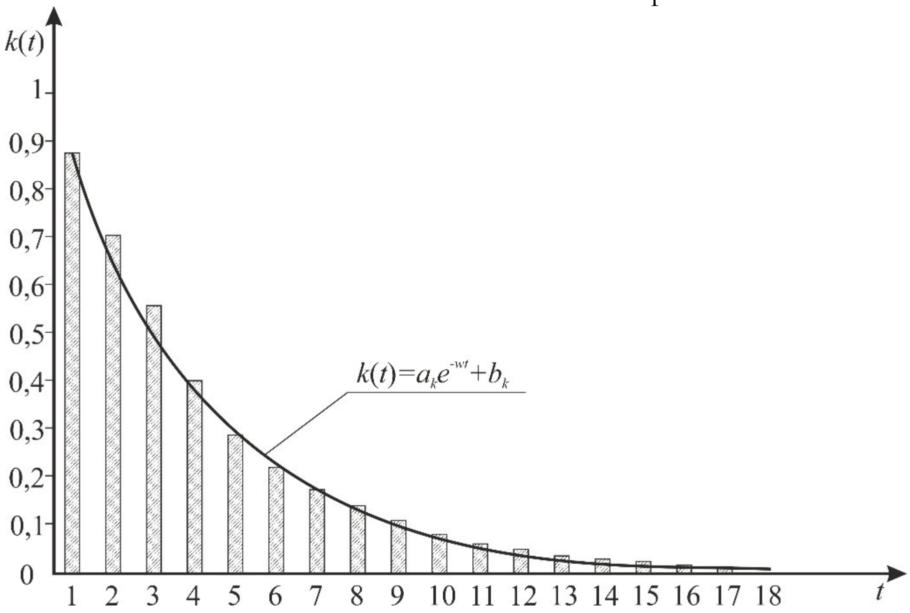

Fig. 2. Dynamics of changing probability of data entry into ITS element from other version of special software: $k(t)$ is an upgrading part, t - upgrading time, w, a_k, b_k are parameters of realization speed of upgrading ITS components

Data analysis allowed us to determine the functional dependency of the change in the elements number of the old version relative to the total number of elements during the upgrade period, which has the following look

$$k(t) = a_k e^{-wt} + b_k, \tag{15}$$

where w, a_k, b_k are the parameters of the upgrading speed of ITS components.

This made it possible to determine the probability of data entering an ITS element from a different SSW version, namely:

$$P_{dis}(t) = \frac{\lambda_{old}\left(a_k e^{-wt} + b_k\right)}{\lambda_{new} a_k \left(1 - e^{-wt}\right) + \lambda_{old}\left(a_k e^{-wt} + b_k\right)}, \tag{16}$$

where λ_{old} is the value of the information flow of the ITS old version; λ_{new} is the value of the information flow of the ITS new version.

Analysis (16) showed the invariance of the probability values of the data flow into an ITS element from another SSW version from a number of ITS elements under the condition of the equality of information flows of the old and new versions. However, in general, this assumption is not mandatory. Due to differences in the information flows of dissimilar ITS versions, P_{dis} value changes according to fig. 3.

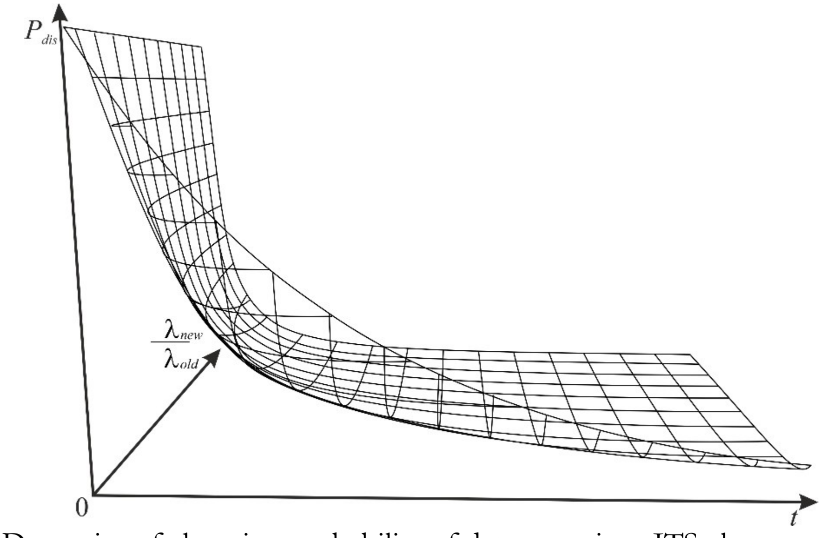

Fig. 3. Dynamics of changing probability of data entry into ITS element of another SSW version with divergences of information flows of different ITS versions: P_{dis} means probability that data arrive at ITS element from another

SSW version, t is upgrade time, λ_{new} - information flow value of the new IS version, λ_{old} - information flow value of the old IS version

The dynamics analysis of changing the probability of data entry into an ITS element from another version of the SSW with discrepancies in the information flows of different ITS versions showed a faster decrease of the specified probability in case of increasing the information flows of the new version.

Thus, the new versions of SSW introduction with a reduced amount of information flow, compared with the old version, leads to an increase in the probability of properties violation of the information resource. This factor must be taken into account when upgrading ITS. At the same time, the reverse situation leads to a decrease in the intensity of destabilizing factors of the information resource properties violation caused by discrepancies of SSW versions at the ITS upgrading stage.

For the sake of clarity of dynamic changing values of probability to perform functional tasks aimed at providing information and analytical activity units, we fix some components of the functional dependence. Figure 4 shows the effect of regulatory values of norminative indicators on the performance of ITS functional tasks.

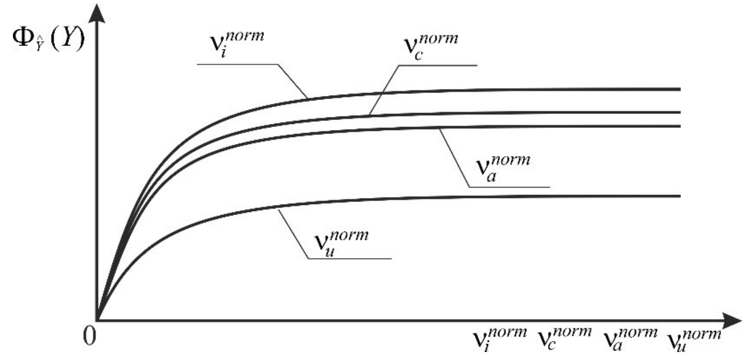

Fig. 4. Dynamic changes of probability values of performing functional tasks at partial changes of normative values: $\Phi_{\hat{Y}}\left(Y\right)$ is an effectiveness of performing ITS functional tasks, ν_i^{norm} - normative value of the integrity indicator, ν_c^{norm} - normative value of the confidentiality indicator, ν_a^{norm} - normative value of the accessibility indicator, ν_u^{norm} - normative value of the observation indicator

The normative value of the integrity indicator exerts the greatest impact on the system effectiveness because of its greater influence on the observation indicator. Post-run by impact are confidentiality and accessibility metrics that are of similar importance. The observation indicator exerts the least influence.

Therefore, as the values of regulatory effectiveness indicators increase, the average value of the probability of completing the ITS task to an accomplished standard at the upgrading stage increases, too. The physical value of this phenomenon is explained by the gradual decrease of destabilizing factors caused by the upgrading process.

The dynamic change of the average value of probability of fulfilling ITS functional tasks at the upgrading stage with fixed values of normative results and change of a number of functional blocks of information processed by the system is shown in Fig. 5.

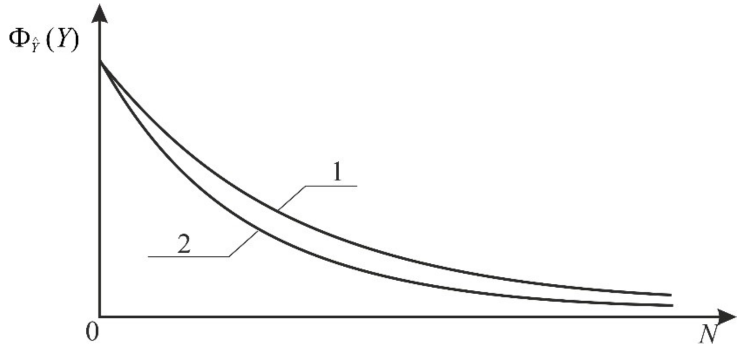

Fig. 5. Dynamic change of values of probability of completing functional tasks at change of a number of functional blocks of information (1) and a number of automated ITS jobs (2): $\Phi_{\hat{Y}}(Y)$ is effectiveness of accomplishing ITS functional tasks, N - a number of functional blocks of information / a number of automated ITS jobs

Analysis of the impact of a number of blocks of information revealed an exponential effect on the effectiveness of the system, that is, the increase in the amount of information. The information that is processed at automated ITS workstations, significantly reduces the probability of completing the tasks by the system. The above will allow making recommendations for upgrading information systems, namely the normative reduction of the number of information blocks or conducting upgrade at their minimum values. Moreover, the increase of a number of ITS automated jobs has less impact than the amount of information.

The analysis of the influence of P_{vm}, P_{cd} and P_{bp} probabilities change on the final effectiveness of the system functioning (Fig. 6), showed that the increase of the values of and probabilities does not lead to a complete loss of system effectiveness.

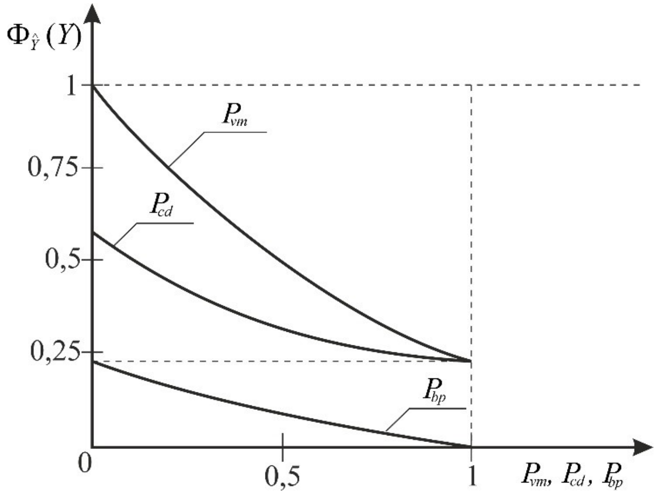

Fig. 6. Dynamic change of values of probability of performing functional tasks by the information system at separate components change: $\Phi_{\hat{Y}}\left(Y\right)$ is an effectiveness of completing ITS functional tasks, P_{vm} - probability of SSW versions mismatch, P_{cd} - probability of a certain category data delivery in ITS, P_{bp} - probability that certain category data come into the general field of an ITS element from the old or new SSW versions with broken properties

In this case, the final effectiveness is reduced only to a certain threshold. As can be seen from fig. 6, the minimum value of the system functioning at the maximum values P_{vm} and P_{cd} corresponds to the minimum value P_{bp} and the increase of the latter results in incompleting system functional tasks. Thus, when an ITS element from an old or new SSW data version with a defective property come into the general field, the system cannot perform its task. This circumstance leads to the loss of the probable component of the violation of the information resource properties and makes this fact deterministic.

Conclusions

1. To describe the semantics of the scheme input parameters for evaluating the effectiveness of information and telecommunication systems functioning, the characteristic features of the tasks performed by the border guard agency were determined. The influence of destabilizing factors on the components of the information resource of this type of systems is taken into account. In describing the approach to effectiveness evaluation, the real conditions for the ITS functioning were determined, which in turn required the formulation of the concept of "external environment". The provided aspects have defined a generalized mathematical view of the approach to the quality evaluation of the system functioning.

2. To evaluate the effectiveness of the information and analytical system operation, the effectiveness indicator of its functioning has been developed. The developed indicator takes into account the ITS characteristics, the features of the organization of the process of ensuring the system functioning, the characteristics of the conditions of ITS functioning, as well as the characteristics of the conditions of ITS exploitation. The above functional dependencies allow to form the indicator itself on the basis of the approach to assessing the quality of the system functioning and to determine the suitability criterion.

3. Taking into account the conducted researches the effectiveness evaluation scheme of Information and Telecommunication Systems functioning was developed. The adequacy of the description is confirmed by the above physical justification, the point of which is the probability of observing the information properties within the specified terms.

4. The new SSW versions introduction with a reduced amount of information flow, compared to the old version, leads to an increase in the likelihood of violation of the information resource properties, which must be considered when upgrading ITS. It is safe to say that with increasing values of regulatory effectiveness indicators, the average value of the probability of completing the task that ensures the quality of ITS functioning at the upgrading stage increases. The physical value of this phenomenon is explained by the gradual decrease in the flow of destabilizing factors caused by the upgrading process.

References

Al Rababah, A. A. (2019). Assurance quality and efficiency in corporate information systems. *International Journal of Computer Science and Network Security*, *19*(4), 87-95. Retrieved from https://www.researchgate.net/profile/Ahmad_Alrababah/publication/333176169_Assurance_Quality_and_Efficiency_in_Corporate_Information_Systems/links/5d6b6a6a299bf1808d5cca53/Assurance-Quality-and-Efficiency-in-Corporate-Information-Systems.pdf

Alekseyev, A. (2010) *Upravleniye riskami. Metod CRAMM. [Risk Management. CRAMM Method.]*. IT Expert.-Elektron. dan.-M.: ZAO IT Ekspert. [Internet source].- Retrieved from http://www.itexpert.ru/rus/ITEMS/ITEMS/_CRAMM.pdf [in Russian]

Artemov, A. V. (2015). Informatsionnaia bezopasnost. Kurs lektsiy [Information Security. Lecture Course]. Retrieved from https://fictionbook.ru/author/a_artemov/informacionnaya_bezopasnost_kurs_lekciyi/ [in Russian]

Benmoussa, K., Laaziri, M., Khoulji, S., Kerkeb, M. L., & El Yamami, A. (2018). Impact of system quality, information quality and service quality on the efficiency of information system. *Proceedings of the 3rd International Conference on Smart City Applications (Sca'18)*. https://doi.org/10.1145/3286606.3286818

Caniëls, M. C. J., & Bakens, R. J. J M. (2012) The effects of project management information systems on decision making in a multi project. *International Journal of Project Management, 30*(2), 162-175. https://doi.org/10.1016/j.ijproman.2011.05.005

Cao, Y., Wang, Y. P., Tang, X. M., & Zhao, X. F. (2018). An evaluation method for network communication system efficiency based on multi-source information fusion. In: *37th Chinese Control Conference (CCC)*, Wuhan, China. pp. 4305-4309. https://doi.org/10.23919/ChiCC.2018.8483552

Chen, D. Q., Mocker, M., Preston, D. S., & Teubner, A. (2010). Information systems strategy: Reconceptualization, measurement, and implications. *MIS Quarterly, 34*(2), 233-259. Retrieved from https://www.academia.edu/28954954/Chen_et_al._Information_Systems_Strategy_INFORMATION_SYSTEMS_STRATEGY_RECONCEPTUALIZATION_MEASUREMENT_AND_IMPLICATIONS_1

Domarev, V.V. (2002). *Bezopasnost informatsionnykh tekhnologiy. Metodologiya sozdaniya sistem zashchity [Security of information technologies. Methodology of creating security systems]*. Kiev, Ukraine: OOO "TID "DS". [in Russian]

Gribunin, V. G., & Chudovskiy, V. V. (2009) *Kompleksnaia sistema zashchity informatsii na predpriiatii [Integrated system of information security in an enterprise]*. Moscow, Russia: Izdatel'skiy tsentr Akademiya. Retrieved from: https://academia-moscow.ru/ [in Russian]

Harasymchuk, O. I., & Kostiv, Yu. M. (2011). Otsinka efektyvnosti system [Estimation of system effectiveness].*Visnyk KNU im. M. Ostrohradskoho.-*

Kremenchuk: KNU imeni M. Ostrohradskoho, 1(66), Chastyna 1. Retrieved from http://www.kdu.edu.ua/PUBL/main.php. [in Ukrainian]

International Carnahan Conference on Security Technology, October 10-12, 1990. [in English]

Kavun, S. V., Nosov, V. V., & Mazhay, O. V. (2008). Informatsiina bezpeka. [Information Security] Navchalnyi posibnyk. CH.1 - Kharkiv: Vyd. KHNEU. Retrieved from http://www.repository.hneu.edu.ua/bitstream/123456789/3105/1/%D0%9D%D0%B0%D0%B2%D1%87%D0%B0%D0%BB%D1%8C%D0%BD%D0%B8%D0%B9%20%D0%BF%D0%BE%D1%81%D1%96%D0%B1%D0%BD%D0%B8%D0%BA.%20%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B0%20%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0.%20%D0%A7.%202%20%D0%9A%D0%B0%D0%B2%D1%83%D0%BD%20%D0%A1.%D0%92..pdf [in Ukrainian]

Kupalova, H.I. (2008) *Teoriya ekonomichnoho analizu [Theory of economic analysis]*. Kiev, Ukraine: Knowledge [in Ukrainian].

Maslova, N. A. (2008). Metody otsenki effektivnosti sistem zashchity informatsionnykh sistem [Methods of effectiveness evaluation of information systems protection]. *Iskusstvennyy Intellect [Artificial Intelligence], 4*, 253-264. [in Russian]

Petukhov, G. B., & Yakunin, V. I. (2006) *Metodologicheskiye osnovy vneshnego proiektirovaniia tselenapravlennykh protsessov i tseleustremlonnykh sistem. [Methodological foundations of external design of targeted processes and purposeful systems]* M.: AST. Retrieved from: https://www.twirpx.com/file/1179860/ [in Russian]

Pihur, N. V., & Pohrebennyk, V. D. (2013). *Otsiniuvanniya efektyvnosti kompleksnykh system zakhystu informatsii. [EvaluatingiIntegrated information security systems effectiveness]*. Retrieved from http://ena.lp.edu.ua:8080/bitstream/ntb/23063/1/45-61-61.pdf [in Ukrainian]

Shcheglov, A.Yu. (2004). *Zashchita kompiuternoy informatsii ot nesanktsionirovannogo dostupa [Protecting computer information from unauthorized access]*.Sankt Petersburg, Ukraine: Nauka i tekhnika [Science and technology]. [in Russian]