Evaluating the efficiency of mitigation tools against negative external actions on the information system

Yu Yu Gromov¹, V I Sumin², S S Kochedykov³ and V I Novoselcev³

¹Department of Information Systems and Information Protection, Tambov State Technical University, Sovetskaya 106, Tambov, Russia
²ET Department, Voronezh Institute Federal Penitentiary Service of Russia, 1a Irkutskaya Street, Voronezh, RU

E-mail: infosec36@mail.ru

Abstract. An approach is proposed to solve the problem of evaluating the efficiency of parrying negative external influences on the information system using the methodological foundations of the efficiency theory of purposeful processes.

1. Introduction
To evaluate the efficiency of the tools used by the information system (IS) to mitigate negative external actions (NEAs), one can use the methodological foundations of the efficiency theory of purposeful processes [1-4].

Out of the many properties inherent in any process, only its operational properties (attributes) that determine the quality of this purposeful process (PP) as a research object are essential for description of the purposeful process of the system functioning (PPSF) [5-7].

Most of these properties are characterized by the results of the operation, i.e. by the effects resulting from this operation, and, therefore, are indirect characteristics of its quality [5]. The specific physical meaning of such indicators is determined by the nature and objectives of the operation, as well as the conditions for its application. An example of a direct indicator of an operation property can be its duration, i.e., the time it takes to achieve the goal of the operation.

2. Statement of the problem
In general, the quality of an operation includes its proper and improper components, the components of the first one are the operation duration and the level of achievement of its objective, and the components of the second one are the quality of the various characteristics of its results (effects). Therefore, two levels of evaluation of the operation quality should be distinguished: evaluation of the quality of the operation results and evaluation of the quality of the operation itself, which is called efficiency [6].

The second level of evaluating the operation quality is the dominant one (the main one), since the operation can be considered qualitative (efficient) if and only if all the results (without exception) possess the required qualities. In this case, the criteria for evaluating the operation qualities and its results should be chosen independently of each other.
In the course of an operation, resources (materials, time, etc.) are used to achieve its objective [6-7]. The ability (or rather, the suitability) of an operation to best convert the consumable resources into the output effects is its main (inherent only to the operations) property.

Generally speaking, the actual result of the operation is the purposeful effect (i.e. the result for which the operation was performed). However, from a formal point of view, the resource consumption corresponding to this effect should also be considered as the result of the operation (or as its side effect). Thus, the properties of the operation results that determine their quality are expedient to divide into two groups: purposeful (functional) and supportive (operational–technical).

This classification is somewhat arbitrary, since one operation may be aimed to support another operation of a larger scale or a higher level (superoperations). In addition, the objectives of an operation may change during its conduct. However, from a methodological point of view, such a classification is always useful, since it makes it possible to structure the research objective and to identify factors that have a decisive influence on the success of the operation (on the quality of its results – effects).

Quality is a property or a set of essential properties of an object that determine its suitability for its intended use. In the case of the PP, its similar properties – attributes – are called operational ones.

These include: productivity, resource capacity, operativity.

Together, these properties comprise a complex property of the PP – the efficiency inherent only in operations.

The productivity of the PP is characterized by the resultant effect. It is determined by the ability of the operation to produce the desired effect (i.e., the result for which the operation is performed).

The resource capacity of the PP is characterized by the expenditure of operational resources of all types (materials, equipment, energy, information, time, finance, labor, etc.) needed to conduct the operation and obtain a targeted effect.

The operativity of the PP is characterized by the consumption of the operating time, i.e., the time it takes to achieve the goal of the operation.

To date, many efficiency indicators have been proposed. There is a set of general requirements that any indicator of the operation efficiency must be suitable for its purpose. The most important of these requirements are [7] representativeness (adequacy), criticality (sensitivity), complexity (completeness), stochasticity, and “simplicity”.

The representativeness (adequacy) indicator assesses the efficiency of the operation to achieve its main objective. The objective of the operation must have its direct mapping in the indicator of its efficiency.

The criticality (sensitivity) indicator is sensitive to changes in the investigated characteristics of the PPSF. The higher is the sensitivity, the better.

The complexity (completeness) indicator is used to solve the problem of investigating the operation efficiency without attracting its other characteristics.[8]

The stochasticity indicator takes into account the uncertainty of the operation conditions, caused by the impact of random factors, and always accompanying the study of the operation and its efficiency.

The efficiency indicator must be quite “simple” (while being complex) so that its computation and subsequent analysis of the operation efficiency could be implemented in a reasonable time and would have a visual interpretation.

The following indicator of the operation efficiency satisfies all the above requirements

By definition, efficiency is a complex operational property (“quality”) of the PPSF, which characterizes its fitness to achieve the objective of the operation implemented by the system (to accomplish the task facing the system).[9]

For a comprehensive study of the efficiency of the PP (operations), the quality indicator $Y_n$ should be defined in a canonical form and include three groups of components – three aspects:

$$Y_n = \left\{ Y_n^{(1)}, Y_n^{(2)}, Y_n^{(3)} \right\} = \left\{ V_{\langle n_1 \rangle}, R_{\langle n_2 \rangle}, T_{\langle n_3 \rangle} \right\}$$

characterizing virtual objective effects, resource costs
and time costs, respectively, i.e. at least three components.

It seems quite obvious that the situation is similar to assessing the quality of the PP results when assessing the quality of any object. Indeed, a priori, i.e. at the stages of development and creation, as well as before the application of the object, both its quality and the requirements to it, conditioned by the situation in which the object will perform its functions are random and, therefore, the suitability of the object for its intended use is a random event. Therefore, the most objective and informative a priori evaluation of the object quality is the probability of its suitability.

Since the quality of the operation results cannot be directly used to evaluate its quality, a probabilistic formulation of the problem is necessary, according to which the evaluation of the operation efficiency (“quality”) should be carried out at two levels and implemented in two stages.

At the first level (1st stage):

1.1 the indicator of virtual quality of the operation results – the vector \( \hat{Y}_i \) of indicators \( \hat{v}, \hat{r}, \hat{\tau} \) of its particular results (effects) is determined;
1.2 the requirements to the quality of the operation results – the region \( \hat{Y}_d \) of permissible values \( \hat{v}^d, \hat{r}^d, \hat{\tau}^d \) of the quality indicators of its results \( \hat{v}, \hat{r}, \hat{\tau} \) are determined;
1.3 the criterion is formulated for evaluating the quality of the results of an operation - 2n – argument (6-argument) predicate

\[
G_1: \hat{Y}_i \in \left\{ \hat{Y}_d \right\} \approx U. \tag{1}
\]

At the second level (2nd stage):

2.1 the indicator of the operation efficiency – the probability of achieving its objective is determined (calculated, “estimated”):

\[
P_1 = P_2 = P \left( \hat{Y}_i \in \left\{ \hat{Y}_d \right\} \right); \tag{2}
\]

2.2 the requirements for the operation efficiency – required (minimum acceptable) or optimal (maximum) value \([ P_3 \text{ or } P_4 ]\) of probability \( P_i (P_2) \) of achieving the goal of the operation, in our case, counteracting negative external actions \( P^*_i (P^*_2) \) are determined (justified, set, presented).

2.3 one of the “selected” (justified) criteria for assessing the efficiency of the IS mitigation tools against NEAs – single predicates is formulated (justified, constructed) and implemented:

– suitability criterion
\[
G_2: \begin{cases} 
P_1 \geq P_3; \\ P_2 \geq P_4. \end{cases} \tag{3}
\]

– optimality criterion
\[
G_3: \begin{cases} 
P_1 = P^*_1; \\ P_2 = P^*_2. \end{cases} \tag{4}
\]

2.4 The actual evaluation of the operation efficiency is performed.
When evaluating the effectiveness of an operation described by an n-dimensional vector indicator, a set of criteria is implemented, each of which in general can belong to one of the three classes: class \( \{G\} \) of suitability criteria; the class \( \{O\} \) of optimality criteria; class \( \{S\} \) of excellence criteria.

Let us give their mathematical formulations. Let

\[
\{y_i^j\}_{i=1}^n, \quad j = (1) m \]

is the indicator of the \( i \)-th property of the \( j \)-th tool for NEA mitigation tools, i.e. the efficiency index of the \( j \)-th mitigation tools is a vector \( Y_n^j = (y_1^j, y_2^j, ..., y_n^j) \).

- \( \{y_i^d\} \) is set (range) of admissible values of an indicator \( y_i^j \) or in the vector form \( \{Y_i^d\} = \{(y_1^d, y_2^d, ..., y_n^d)\} \).

Then the criteria of the classes listed above have the following definitions.

Suitability criterion:

\[
G: \bigcap_{i=1}^n \left( y_i^j \in \{y_i^d\} \right) \equiv U, \quad [j = (1) m], \quad (5)
\]

where \( U \) is an authentic event (true proposition), \( \cap \) is the symbol of the Boolean intersection of events (the conjunction of propositions). In the vector form, criterion (1) takes the following form:

\[
G: \quad \left( Y_n^j \in \{Y_n^d\} \right) \equiv U, \quad [j = (1) m], \quad (5')
\]

where \( \{Y_n^d\} \) is a range of permissible values of the efficiency indicator of suitable mitigation tools.

The NEA mitigation tools, for which the conditions \( (5), (5') \) are satisfied, are suitable for their intended use. At the same time, they all have the same efficiency.

For the case \( n = 2; m = 5; \{Y_2^d\} = \left[ y_1^1, y_1^2 \right] \times \left[ y_2^1, y_2^2 \right] \) criterion (5') is illustrated in figure 1.

As can be seen from Fig. 1, in the above example, the 1st, 2nd, 3rd and 5th objects are suitable, but the 4th one is not suitable, i.e., \( \{Y_2^d\} = \left\{ Y_2^1, Y_2^2, Y_2^3, Y_2^5 \right\} \).

Optimality criterion:

\[
O: \bigcap_{i=1}^n \left( y_i^j \in \{y_i^d\} \right) \cap \bigcap_{k < (1) n} \left( y_k^j = y_k^{0(j)} \right) \equiv U, \quad [n_0 = (1) n; \ j = (1) m], \quad (6)
\]
where $y_{k}^{Opt}$ is optimal value of the indicator of the $k$-th property, $n_{0}$ is the volume of the set $\{k\}$ a-numbers (number) of optimized properties of the object. In vector form, the criterion (2) takes the form

$$ O: \bigg( Y^{j}_{n} \in \big[ Y^{d}_{n} \big] \bigg) \cap \bigg( Y^{Opt}_{n} = Y^{j}_{n} \bigg) \approx \bigg( Y^{j}_{n} \in \big[ Y^{d}_{n} \big]^{Opt} \bigg) \approx U, [j = 1(1)m] .$$

where $y_{k}^{Opt}$ is range of permissible values of the efficiency indicator of the optimum object.

By definition, the mitigation tools for which condition (6') is satisfied is called the optimal for the $k$-th property, that is, for $n_{0}$ properties. It is clear that such mitigation tools must be suitable as well.

For the case $n_{0} = 1; k = 1; \big[ Y^{d}_{(2)} \big] = \big[ y_{1}^{Opt}, y_{2}^{Opt} \big]$ criterion (6') is illustrated in figure 2.

![Figure 2. Optimality criterion.](image)

As can be seen from Fig. 2, in the example given, the 1st and 3rd mitigation tools against NEAs are optimal for the first property (indicator $y_{1}$), i.e. $\big( y_{1}^{d} \big)^{Opt} = \big[ y_{1}, y_{2} \big]$.

Excellence criterion:

$$ S: \bigg( \bigcap_{j=1}^{n} \big( y^{j}_{n} \in \big[ y^{d}_{n} \big] \big) \cap \bigg( \bigcap_{i=1}^{n} \big( y^{i}_{n} \geq y^{j}_{n} \big) \bigg) \approx U, [l = 1(1)m] .$$

where $l$ is the number of excellent mitigation tools.

In vector form, criterion (3) takes the form

$$ S: \bigg( \bigcap_{j=1}^{n} \big( Y^{j}_{n} \in \big[ Y^{d}_{n} \big] \big) \cap \bigg( \bigcap_{i=1}^{n} \big( Y^{i}_{(n)} \geq Y^{j}_{(n)} \big) \bigg) \approx \big( Y^{l}_{(n)} \in \big[ Y^{d}_{(n)} \big]^{Ex} \big) \approx U ,$$

where $\big( Y^{l}_{(n)} \geq Y^{j}_{(n)} \big) \approx \big( \bigcap_{j=1}^{n} \big( y^{j}_{n} \geq y^{j}_{n} \big) \big)$ is the range of admissible values of the quality score of excellent mitigation tools. By the definition, the mitigation tools for which the condition (7) is satisfied, surpasses in quality all other mitigation tools. If $\big( \bigcap_{j=1}^{n} \big( y^{j}_{n} = y^{j}_{n} \big) \big) \approx U$, then the quality of the 1st and j-th mitigation tools are recognized as identical. If at least one of the conditions (7) is not satisfied, then this means that a given set of property indicators does not allow finding mitigation tools that outperforms all the others in quality.
Criterion (7) is illustrated by figure 3, from which it follows that on a given set of mitigation tools, the 3rd means is optimal by the criterion of excellence, in spite of the relation \( y_2^3 > y_2^4 \), since the 4-th mitigation tools. It is not suitable and therefore not competitive compared with the rest.

The optimality criterion is a particular case of the suitability criterion

\[
\{Y_{(n)}^d\}_{Opt} = \{Y_{Opt}^{n}\} \times \prod_{i=1}^{n-1} \left[ y_i', y_i \right]
\]

Under the conditions of the examples given, expression (8) takes the form

\[
\{Y_{(2)}^d\}_{Opt} = \{y_{Opt}\} \times \left[ y_2^1, y_2^3 \right] = \{y_{(2)}^1, y_{(2)}^3\}
\]

figure 2 can serve as an illustration of the expression (9), which shows that for the optimality criterion the region \( \{Y_{(2)}^d\}_Opt \), turning into the region \( \{Y_{(2)}^d\}_Opt \), degenerates into a straight line segment (and on a finite set \( m \) of mitigation tools, into a two-point set \( \{Y_{(2)}^1, Y_{(2)}^3\} \)).

In turn, the criterion of excellence is a special case of the optimality criterion, since expression (7) means

\[
\prod_{i=1}^{n} \left( y_i' \geq y_i' \right) \approx \prod_{j=1}^{n} \left( y_i' = y_i^{Opt} \right)
\]

or in the vector form

\[
\{y_{(2)}^d\}_Ex = \prod_{j=1}^{n} \{y_j^{Opt}\}
\]

Under the conditions of the examples given, expression (6 ') takes the form

\[
\{y_{(2)}^d\}_Ex = \{y_1^{Opt}\} \times \{y_2^{Opt}\} = \{y_{(2)}^{Opt}\}
\]

figure 3 can serve as an illustration of the expression (11), which shows that for the excellence criterion the region \( \{Y_{(2)}^d\}_Ex \), turning in to the region \( \{Y_{(2)}^d\}_Ex \), degenerates into the point \( \{y_1^3, y_2^3\} \).

Thus, in assessing the quality of mitigation tools, the suitability criterion G is dominant and universal and is defined by expression...
\[ G^{(K)}: Y_{\{n\}} \in \left\{ Y^{d(K)}_{\{n\}} \right\} \cong U, \quad (12) \]

where \([K] = S, \text{Opt}, \text{Ex}\) is index of the criterion class; \(Y^{d(K)}_{\{n\}}\) is valid vector value \(Y_{\{n\}}\) for the criterion of the \(K\)-th class.

The study of the operation efficiency is a three-pronged problem: the problems of assessing (measuring) the operation efficiency; the problem of analyzing the operation efficiency, the problem of the optimal synthesis of the efficient operation.

The first two problems are often combined under the general name of the direct problem, and the third one is called the inverse problem. An approximate scheme for classifying the problems of investigating the operation efficiency is shown in figure 4.

![Figure 4. Classification of the problems of evaluation of the operation efficiency.](image)

Although the direct and inverse problems have independent meanings, the ultimate goal of their solutions, as a rule, is to optimally design the IS, ensuring the achievement of the objective of the operation (mitigation of NEAs) with the greatest probability, i.e. in solving the synthesis problem. Nevertheless, their first links are problems of evaluating and analyzing the efficiency of an operation, the goals of which are achieved by: constructing mathematical models of the investigated IS; determination (justification) of IS performance indicators; evaluation of the efficiency of mitigation; analysis of the influence of the IS mitigation tools against the NEAs on its efficiency.

Since all operations are carried out and proceed under the conditions of the action of a set of a priori unknown, and therefore random factors, their rather adequate description can be given only on
the basis of stochastic models. As for deterministic models and quasi–regular models, they should be considered only as some approximations of stochastic models and the validity of their application should be justified in each concrete case.[10]

Thus, the methodological foundations for investigating the efficiency of operations are as follows: evaluating the efficiency of the mitigation tools against the NEAs; analysis of the effect on the efficiency of mitigating NEAs; the IS synthesis ensuring the achievement of maximum IS security.

References

[1] Gromov Yu Yu 2011 Methods and means of providing security in the design of information systems: a textbook for students of higher education institutions in 220100 "System Analysis and Management", 230400 "Information Systems and Technologies" (Tambov: Gos. obrazovatel'noe byuzdhetnoe uchrezhdene vyssh. prof. obrazovaniya "Tambovskij gos. tehknicheskij un–t") p 296

[2] Shheglov А Yu 2004 Protection of computer information from unauthorized access (SPb.: Science) p 384

[3] Gromov Yu Yu, Ivanovskij M A, Didrikh V E, Didrikh I V and Gubskov Yu A 2010 Mathematical modeling of states of information security of an organization Engineering Physics vol 3 (Moscow: Nauchtechizdat) pp 8-10

[4] Gromov Yu Yu, Minin Yu V, Ivanova O G and Morozova O N 2018 Models of multidimensional discrete distribution of probabilities of random variables in information systems IOP Conf. Series: Journal of Physics: Conf. Series p 973

[5] Petukhov G 1989 Bases of the theory of efficiency of purposeful processes. Part 1. Methodology, methods, models (Moscow) p 140

[6] Gromov Yu Yu, Karpov I G, Minin Yu V and Ivanova O G 2016 Generalized probabilistic description of homogeneous flows of events for solving informational security problems Journal of Theoretical and Applied Information Technology Vol 87 №2 p 250-254

[7] Gromov Yu Yu, Karpov I G, Didrikh V E, Minin Yu V and Ivanova O G 2016 Application of linear pure birth-death processes for network-centric information systems modeling Journal of Theoretical and Applied Information Technology Vol 85 №1 p 69-73.

[8] Dushkin A V, Kochedykov S S and Novoseltsev V I 2017 Tool and algorithmic diagnostic devices of operability of actuation mechanisms of automated control systems Proceedings. 2017 2nd International Ural Conference on Measurements (UralCon) South Ural State University (national research university), Chelyabinsk, Russian Federation DOI: 10.1109 URALCON 8120709 pp 193-198

[9] Dushkin A V, Kochedykov S S, Noev A N and Gubin I A 2018 Method of optimum channel switching in equipment of infocommunication network in conditions of cyber attacks to their telecommunication infrastructure International Conference Information Technologies in Business and Industry IOP Conf. Series: Journal of Physics: 1015 032101. DOI:10.1088/1742-6596/1015/3/032101 pp 187-193

[10] Dushkin A V, Kasatkina T I, Novoseltsev V I and Ivanov S V 2018 An improved method for predicting the evolution of the characteristic parameters of an information system Conference Information Technologies in Business and Industry IOP Conf. Series: Journal of Physics: 012031. DOI:10.1088/1742-6596/973/1/012031 pp 180-187