6. Magnetization reversal of the multilayer magnetic film / Yu. V. Zakharov, K. G. Okhotkin, A. D. Skorobogatov, V. V. Isakova // Magnetism on a Nanoscale (EASTMAG-2007) : Brief outline reports of Euro-Asian symposium Kasan : KSU, 2007. P. 184.

7. Vlasov A. Yu., Okhotkin K. G. Non-linear bend of stiffness-variable compound rod with longitudinal and transversal stress // Physical-mathematical science. 2006. № 1. P. 26–28.

8. Akhiezer A. I., Bariakhtar V. G., Pelemitskii S. V. Spin waves. M. : Nauka, 1967.

V. V. Zolotarev, E. A. Danilova
Siberian State Aerospace University named after academician M. F. Reshetnev,
Russia, Krasnoyarsk

ON APPLICATION OF FACTORIAL ANALYSIS IN PROBLEMS OF SECURITY ESTIMATION OF AUTOMATED SYSTEMS ELEMENTS

The possibility of factorial analysis application in theestimation of the state of information systems security is considered. The procedure of selection and classification of factors as well as calculation of factors influence on the resultant indicator size are described.

Keywords: risk management, information risk, factorial analysis.

Factorial analysis is one of the possible methods of automated systems security analysis. This method of analysis allows both to establish cause-and-effect relations between negative events and to characterize them quantitatively.

Let's consider the application peculiarities of a security estimation factorial model (further a factorial model) in the problem of security estimation of electronic document management system (EDMS). At the same time we will introduce universality elements into the offered model which will allow to use it for the estimation of various elements of both EDMS and other automated systems. We will especially note the applicability of the offered model and the solutions found on its basis for a human factor estimation.

The model description. Let there be an information system *IS* which consists of *N* numbers of *E* elements, each of which in its turn consists of *K* components. A component of each element in a certain period of time can accept *x* of states *s* with probability *r*:

$$IS = \{E_l\}, \qquad E_i = \begin{Bmatrix} s_1^1 & s_2^1 & \dots & s_{x1}^1 \\ s_1^2 & s_2^2 & \dots & s_{x2}^2 \\ \dots & \dots & \dots & \dots \\ s_1^k & s_2^k & \dots & s_{xk}^k \end{Bmatrix},$$

where

$$l \in [1 \dots N]. \qquad (1)$$

Let *x* be the quantity of degrees of a component freedom. It is obvious that in using a similar model of the system it is possible to use the method of a morphological box of Zwicky [1, p. 196] in various variants. At the same time it is possible to calculate the quantity of cause-and-effect relations between the states of information system elements if we calculate them as a number of placings with repetitions:

$$k_{\text{сост}} = \left(\sum_{i=1}^{N} \sum_{j=1}^{K} x_{s_{ij}} \right)^m, \qquad (2)$$

where *m* is the quantity of interlinks between system elements components. During such calculation a number of assumptions was made which is necessary to mention as these assumptions restrict the model application range:

– it is necessary to reduce the quantity of freedom degrees to some uniform value which assumes a standard set of states of system elements components;

– it is necessary to provide the completeness of an initial set of freedom degrees of each system element component which assumes a certain approach to the choice of indicators defining freedom degrees;

– the private function of utility should be calculated for each system element separately, thus resorting to simplification of calculations;

– it is necessary to possess the information about internal connections of analyzed system elements. Without updating such approach is inapplicable for a system with incomplete information about internal connections.

Let's consider basic elements of an applied factorial model:

– the private function of element *E* utility for performing the main task of *IS* system (further – private function of utility):

$$u^*(t) = f(E),$$

where

$$E = \begin{pmatrix} & & \\ r_1^{(1)}(t) & \dots & r_1^{(x)}(t) \\ r_2^{(1)}(t) & \dots & r_2^{(x)}(t) \\ \dots & \dots & \dots \\ r_k^{(1)}(t) & \dots & r_k^{(x)}(t) \end{pmatrix}, \qquad (3)$$

where $r_i^{(j)}(t) = p_i^{(j)}(t)*w_i^{(j)}(t)$, for i-th component in j state according to [2], $i \in [1\ldots K]$, $j \in [1\ldots x]$.

– here $p_i^{(j)}(t)$ characterizes the probability of unfitness of an element component in a certain degree of freedom in a certain period of time for performance of the set function; $w_i^{(j)}(t)$ is the probability of influence of the established security facilities on suitability of an element component in a certain degree of freedom in a certain period of time; as a whole $u^*(t)$, hence, characterizes the ability of a concrete element to resist the influence. The function $f(E)$ essence is the calculation of an average factor allowing to use value u^* for the security estimation of a system element as a whole, instead of the security estimation of its components characterized by values $r_i^{(j)}(t)$. At the same time it is possible to additionally prove the decomposition of a system element, considering it as a set of interconnected components, at the same time keeping the possibility of an inverse operation of decomposition into components, as it will be shown further in an example of use of the offered model;

– directed graph $G(V, E)$, representing the system model. Nodes of the graph–system elements – are characterized by pair $u^*(t)$ and B_e (average cost of security facilities of an element), and tree edges are characterized by value Δu^*, which shows a utility correlation of the related elements;

– the integrated function of utility of a system as a whole:

$$U(t) = \underset{i=1}{\overset{N}{H}} u^*_i(t), \quad (4)$$

where N is the quantity of investigated components; $H = \{*,+, \max\}$ is a set of operations of interconnection. The choice of a concrete operation is defined by a kind of interconnection (or absence of that) of investigated system elements [2].

The following correlation can be used as a criterion function of risk:

$$R(t) = U(t)\sum_{i=1}^{N} B_i(t). \quad (5)$$

Thereby, the utility of work in a certain period of time $[a; b]$ will be equal to (according to Neumann–Morgenshtern function [3]):

$$D = \int_a^b R(t)dt. \quad (6)$$

Taking into account (5) for an optimum configuration:

$$\sum_{\tau \subset T} D_\tau \to \min, \quad (7)$$

where, T is a set of all analyzed periods of time.

Obviously, the offered approach can be supplemented with the criterion of elements connectivity for the choice of the system optimum structure [4] taking into account a prior indicator of elements pairs contents. The considered factorial model together with the offered function of utility allows to solve the problem of optimum distribution of resources.

Then we will consider separate aspects of the offered approach.

Selection and classification of factors. The functioning of any information system occurs in the conditions of complicated interaction of a complex of internal and external factors. A factor is a reason, motive power of any process or phenomenon, defining its character or one of the basic characteristics.

There are various principles of factorial analysis [5]. Deterministic multiple analysis is used to perform the set task.

To solve the problem of the account of all set of factors influencing the information, circulating in EDMS, we suggest breaking it into the basic components. First of all, for each element we will define possible states which it can accept, then we will consider combinations of these states, creating a basic model of all possible private functions of utility and modelling a risk function in the dynamics of system development on the basis of a minimum set of initial data.

Usable model of an element. Let's start with distinguishing the system elements components. Taking into account the fact that the object of this research is to estimate the security of EDMS whose structure can be rather easily described organizationally, technically and by means of functional-logic models, the description of element components becomes the primary goal which defines the efficiency of integrated estimation. Taking into account (2), we will specify the problem as the development of a morphological box of Zwicky satisfying the chosen conditions. So, in view of the definition: an automated system (AS) is a system realizing information technology of performance of the established functions [6] and consisting of personnel and a complex of means automating its activity.

On the basis of the definition, we can distinguish four basic components of each AS element, namely: hardware (HW (fig. 1 and table, 1–ТС)), the software (SW (fig. 1 and table, 1–ПО)), the personnel (Р(fig. 1 and table, 1–Ч)) and organizational measures of information processing and protection (various kinds of instructions, regulations and orders (the ОМ)).

Taking into account model restrictions let the ability of AS element to carry out the set functions be described by a static set of states:

1. Up state (U(fig. 1 and table, 1–Р)) – a state of AS element component when values of all parameters characterizing the ability to carry out set functions correspond to requirements of the specifications and technical documentation and (or) design (project) documentation [7];

2. Down state – a state of AS element component when the value of at least one parameter characterizing the ability to carry out set functions does not correspond to requirements of specifications and technical documentation and (or) design (project) documentation. Let's divide down states of AS element components into three categories:

– failure (F (fig. 1 and table, 1–Отк)) – an event consisting in malfunction of an upstate condition of AS

element component after which a component of AS element stops functioning and demands extraneous intervention for restoration of normal work;

– malfunction (M (fig. 1 and table, 1–C)) – a transient fault or a single fault eliminated by slight intervention of an operator [7];

– error (E (fig. 1 and table, 1–O)) – incorrect or incomplete performance of separate tasks of a component of AS element without loss of its functionality.

Let's set a way of a morphological box formation as investigation of combinations of the listed set of AS element components states. To estimate security it is necessary to define combinations which can negatively influence the change of a productive indicator, i. e. the change of an information system security state. At the same time to exclude the combinations which are of no interest for further research and don't influence the change of an integrated indicator of risk or element utility private function we will introduce some conditions. We will exclude:

– interrelations between the states of one AS element component as we accept that AS element component can be only in one state in some concrete period of time;

– interrelation between up states of various groups of elements as it does not influence the element utility private function negatively.

Let's take into account the dependence on AS element generating state which defines technically impossible combinations of a morphological box states:

– change of a state of organizational measures (ОМ) can be caused only by personnel's (Р(fig. 1, Ч and table)) actions;

– "Failure" (fig. 1 and table, 1–Отк) state of hardware can become a cause of refusal in personnel and/or software, but not simultaneously;

– if hardware is in the state of "Failure" (fig. 1 and table, 1–Отк) the software cannot be in "Upstate" (fig. 1, 1–Р) condition;

– "Failure" (fig. 1 and table, 1–Отк) in personnel's work cannot become a reason of change in the states of other AS elements.

On the basis of introduced restrictions it is possible to define all combinations of AS elements states whose change can lead to the change of AS security state (fig. 1). The total number of such connections can be presented if we exclude some of them according to the conditions set above.

So, we receive 128 combinations with which it is possible to describe all set of influences on AS element, using minimum initial data, that is, failure rate of AS element separate components. Completeness and reliability of the revealed connections between states of AS elements influencing or able to influence the information is reached by way of considering a set of states of all AS element components and, as a consequence, of all factors influencing all AS elements at all stages of information processing [2].

Calculation of the probability of states combination. If the probabilities of occurrence of each state for all components of AS element $P_{sx}(E_i)$ are known to us, then it is possible to represent the probability of occurrence of connected event P_s, as the mutual one, thus applying the following expression, considering (1):

$$P_s = r_{si} r_{sj}, \text{ here } i, j \in [1\ldots x]. \quad (8)$$

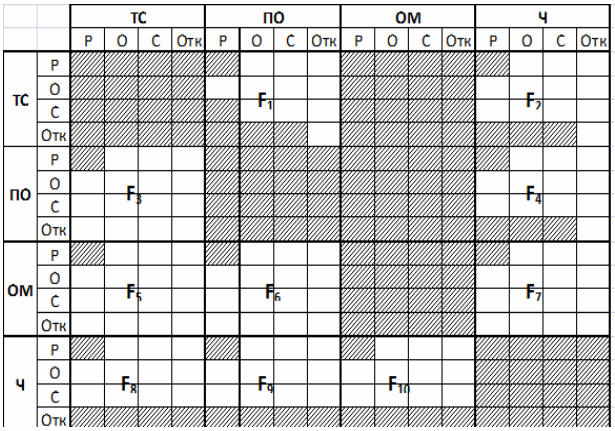

Fig. 1. The morphological box of AS element components states

By means of (8) it is possible to calculate probabilities of occurrence of all 128 connections between AS element components states, presented in fig. 1.

Definition of dependences between AS element components states. Connections between AS element components states can be presented in the form of directed graph *GE*, whose nodes are states of AS element s_{Ei} components, edges of the graph are dependences between them (fig. 2):

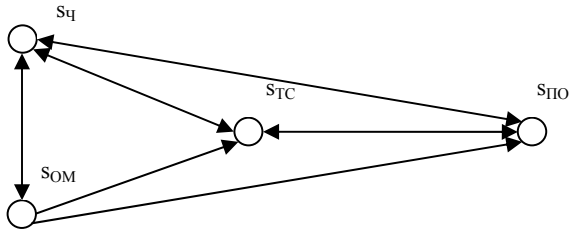

Fig. 2. The graph of dependences between element components of an information system

Having investigated the dependences of the chosen states on each other (fig. 2), we form a private function of an element utility on the basis on factors (average probabilities of sets of the states generated by a concrete component of AS element):

$$u^*_{E_i} = F_1 \cap F_2 \cup F_3 \cap F_4 \cup F_5 \cap \cap F_6 \cap F_7 \cup F_8 \cap F_9 \cap F_{10}, \quad (9)$$

where u^*_{Ei} is a private function of utility of AS element; F_1, F_2, ..., F_{10} are factors influencing the change of AS state; $\cap$ is a symbol of intersection if there is dependence between factors; $\cup$ is a symbol of association if there is no obvious dependence between factors.

Using methods of mathematical logic, it is possible to present (9) as:

$$u^*_{E_i} = F_1F_2 + F_3F_4 + F_5F_6F_7 + F_8F_9F_{10}. \qquad (10)$$

Modelling of investigated AS element security. To carry out the information risks factorial analysis it is necessary to present the object of research – an automated system – as a set of constituent elements. The better the model of research object is studied, the more exactly an integrated function of utility can be defined. Some standard methods of reliability theory, for example, an exhaustive method of states [8] can be used in this process. However it is necessary to remember that modelling the research object should be made from the position of integrity and systematicness, excluding redundant parameters which do not give any useful information for realization of the analysis purposes. The object of research should be considered from the point of view of logic, technical and structural schemes of information processing in an organization. In factorial analysis one can use both each scheme separately and all of them together, which can give fuller information for calculation of a resultant indicator, i. e. the risk level of each element of research object. Thus the risk level of each element of research object is represented from the point of view of factorial indicators (with possible decomposition to separate states of AS element components). On the basis on these data it is possible to draw a conclusion not only about most vulnerable elements, but also to point the concrete reason reducing the level of information safety.

Numerical modelling of security change. Using the offered approach, it is possible to carry out factorial modelling and estimation of security of both separate AS elements and the integrated indicator of security and risk for all research object. Taking (6), (7) and the consequences of the specified correlations into account, it is possible to operate information security of an object, using minimum initial data.

For example, we will consider numerical modelling of security level of the centre of collective access for organization ESDM (that is an AS element in terms of the model) (table), in brackets there is a final state after reaction of an element to introduction of the offered protection measures, nearby there is an initial state of an indicator.

The failure rate was considered for a certain period of time (one operational month, that is 30 days) which was agreed in the course of carrying out of the analysis; intensity calculation was done in terms of 1 day of operational time of the centre of collective access on the basis of reports of technical support services in the organization. Obviously, methods of information protection of ESDM element, applied in this case, have not influenced ESDM as a whole significantly though they were preliminary estimated by an organization management (judging by their influence on concrete components of system elements) as effective ones. You can see from the example that the offered approach allows to specify the complex problems of ESDM element, but does not allow to predict sharp changes and individual security infringements of research object. At the same time the value of the offered approach is obvious both for the solution of operative, short-term problems of information security management and for modelling the systems of protection without taking into account the influence of the information security infringer (preliminary calculation and choice of security facilities and configurations which are optimal form the point of view of cost).

The application of the offered approach takes into account cause-effect relations of processes of information processing which influence the level of information resources security. The use of factorial analysis is a step towards reception of objective quantitative results in information security management.

An example of numerical modelling of AS element security

S_x	P_{sx}	F_1	F_2		u*
P(ТС)	0.84(0.94)	0.0328 (0.302)	0.0567 (0.512)		0.0038 (0.0030)
O(ТС)	0.06(0.03)				
C(ТС)	0.1 (0)				
Отк(ТС)	0 (0.03)				
		F_3	F_4		
P(ПО)	0.68(0.79)	0.0286 (0.0224)	0.0595 (0.0560)		
O(ПО)	0.23(0.09)				
C(ПО)	0.06(0.09)				
Отк(ПО)	0.03(0.03)				
		F_5	F_6	F_7	
P(ОМ)	0.91(0.97)	0.0157 (0.0123)	0.0254 (0.0227)	0.0436 (0.0421)	
O(ОМ)	0.06(0.03)				
C(ОМ)	0 (0)				
Отк(ОМ)	0.03 (0)				
		F_8	F_9	F_{10}	
P(Ч)	0.38(0.51)	0.0564 (0.0520)	0.0620 (0.0594)	0.0540 (0.0487)	
O(Ч)	0.5 (0.4)				
C(Ч)	0.06(0.09)				
Отк(Ч)	0.06 (0)				

References

1. Волкова В. Н., Денисов А. А. Теория систем и системный анализ : учебник для вузов. М. : Юрайт, 2010.

2. Применение факторного анализа и эволюционного алгоритма оптимизации для решения задачи управления информационными рисками систем электронного документооборота / В. Г. Жуков [и др.] // Системы управления и информационные технологии. 2009. № 3(37). С. 41–50.

3. Беллман Р., Калаба Р. Динамическое программирование и современная теория управления. М. : Наука, 1969.

4. Антамошкин А. Н. Алгоритм расчета прогнозируемого трафика при проектировании распределенных систем обработки и хранения информации // Вестник СибГАУ. 2006. Вып. 1. С. 5–10.

5. Сафонов А. А. Теория экономического анализа : учеб. пособие / под ред. Л. В. Моисеевой. Владивосток : Изд-во Владивост. гос. ун-та эконом. и сервиса.

6. ГОСТ 34.003–90. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения. М. : Изд-во стандартов, 1990.

7. ГОСТ 27.002–89. Надежность в технике. Основные понятия. Термины и определения. М. : Изд-во стандартов, 1989.

8. Половко А. М., Гуров С. В. Основы теории надежности. 2-е изд.. перераб. и доп. СПб. : БХВ-Петербург. 2006.

N. N. Zagirov, A. A. Kovalyova, E. V. Ivanov
Siberian Federal University, Russia, Krasnoyarsk

TECHNOLOGY OF PRODUCING FIBROUS STRUCTURE WIRE FROM CHIPS OF ALUMINUM–MAGNESIUM–SILICON ALLOYS

A technological scheme for processing the scrap of aluminum–magnesium–silicon alloy in the form of friable chips into rods and wire is introduced. This scheme is based on the powder metallurgy methods. The characteristic structure and the level of mechanical properties of the produced wire are denoted.

Keywords: friable chips, briquetting, combination of rolling and pressing, drawing, fibrous material, structure, mechanical properties.

A complex composite material is implied in cases when wire is not made of compacted metal material. This material has a metal coating consisting of a hard plastic body and a powder core, which is a friable mixture of heterogeneous particles [1]. During mechanical processing, the metal coating is in a complex interaction with the powder core; this causes complex movement of the powder particles and their elastic-plastic interaction under external load.

According to the suggested technology, making wire from friable fine chips (filing) of aluminum alloy АД31 and putting it into the metal coating is not accomplished. The process of making the final product can be divided into two parts:

– the technological scheme of producing an intermediate workpiece for drawing, which includes the preparation of chips for compacting, briquetting, briquette heating for extrusion, and hot extrusion for the rod of a specified diameter;

– the technological process of making wire consisting of multiple repeated operations of drawing the workpiece through dies and other auxiliary operations.

The method of chip processing in which the quantity of secondary raw material is quite high provides a higher yield ratio of metal chips in comparison with molting. Besides, energy consumption and harmful environmental impact are being reduced, which is a key issue for any type of industry.

It is well known that the suitability of metal chips for making press-items and wire depends on the compressibility during briquetting. The traditional scheme of pressing in rigid molds for making lengthened briquettes of cuboids form with height to width ratio 1 and length to width ratio 10 is not effective (such a ratio is determined by specific character of the equipment and the combination of rolling and pressing). Due to comparatively low briquettes density and cohesion of chips particles there is high probability of fillets rupture (breaking) during the pressing-out.

Briquetting of chips *2* is made in molds (fig. 1) consisting of upper *1* and lower *4* plugs, split matrix *3* and chase *5* with sloping contact surfaces. The experiment shows that briquetting pressures for providing integrated briquette density of 70–80 % must not be lower than 80–100 MPa.

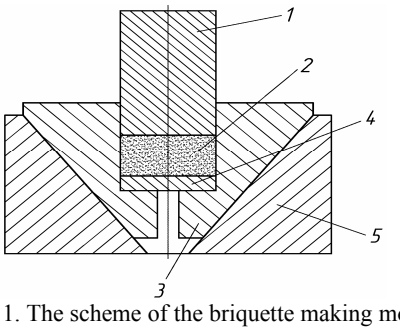

Fig. 1. The scheme of the briquette making mold for combined rolling and pressing