INFO-2226 UDK: 336:316.42:004
Primljeno/Received: 2020-05-03 Original Scientific Paper /Izvorni znanstveni rad

https://doi.org/10.32914/i.53.3-4.3

ISSUES OF ENSURING BUDGET SECURITY AS A LEGAL CATEGORY IN THE DIGITAL AGE

PITANJA OSIGURANJA PRORAČUNSKE SIGURNOSTI KAO PRAVNE KATEGORIJE U DIGITALNOM DOBU

Juliia V. Abakumova[1], Halyna S. Andrushchenko[2], Olga O. Semchyk[3], Ievgeniia A. Ananieva[4], Roman I. Samsin[5]

Vladimir Stashis Institute of Law, Classical Private University, Zaporizhzhya, Ukraine[1]; Departament of Financial Law, Taras Shevchenko National University of Kyiv,Kyiv, Ukraine[2]; Department of State Governance and Administrative Law Issues, V.M. Koretsky Institute of State and Law of National Academy of Sciences of Ukraine Kyiv, Ukraine[3]; Department of Legal Support of Economic Activity Kharkiv National, University of Internal Affairs, Kharkiv, Ukraine[4]; Department of Private Law Disciplines, Kyiv International University, Kyiv, Ukraine[5]

Pravni institut Vladimir Stashis, Klasično privatno sveučilište, Zaporožje, Ukrajina[1]; Odjel za financijsko pravo, Nacionalno sveučilište Taras Ševčenko, Kijev, Ukrajina[2]; Odjel za državnu upravu i upravnopravna pitanja, V.M. Korecinski institut za državu i pravo Nacionalne akademije znanosti Ukrajine, Kijev, Ukrajina[3]; Odjel za pravnu potporu gospodarskim djelatnostima, Harkovsko nacionalno sveučilište, Harkov, Ukrajina[4]; Odjel za privatno-pravne discipline,Kijevsko međunarodno sveučilište, Kijev, Ukrajina[5]

Abstract

The digital development of society is determined by the fact that all aspects of the development of the technical environment and the formation on this basis of an equilibrium process of social development can be singled out as a structural feature of national security. The budget as a source of social development has a tax, social and social foundation under it. All this is determined by the necessity for additional research on issues related to the formation of the possibility of maintaining the vector of development of society. The novelty of the study is that all legal research is limited to the formation of only framework conditions, which in turn affect such aspects as the development of deterrent mechanisms. In the work, the authors determine the possibility of development and formation of the budget security category on the basis of a model that is provided not only by legal conditions, but also regulated by information components. The article provides a component model, which is determined by the fact that it forms a protective mechanism based on a legal decision. The practical significance of the

Sažetak

Digitalni razvoj društva određen je činjenicom da se svi aspekti razvoja tehničkog okruženja i formiranje na toj osnovi ravnotežnog procesa društvenog razvoja mogu izdvojiti kao strukturno obilježje nacionalne sigurnosti. Proračun kao izvor društvenog razvoja ima porezne, socijalne i socijalne temelje. Sve je to određeno potrebom za dodatnim istraživanjem pitanja vezanih uz formiranje mogućnosti održavanja vektora razvoja društva. Novost studije je da su sva pravna istraživanja ograničena na stvaranje samo okvirnih uvjeta, koji zauzvrat utječu na aspekte kao što je razvoj mehanizama odvraćanja. U radu autori utvrđuju mogućnost razvoja i formiranja kategorije proračunske sigurnosti na temelju modela koji je predviđen ne samo zakonskim uvjetima, već i reguliran informacijskim komponentama. Članak daje komponentni model, koji je određen činjenicom da čini zaštitni mehanizam zasnovan na zakonskoj odluci. Praktični značaj studije određuje činjenica da se proračunska sigurnost ističe ponajprije kao komponenta društvenog razvoja i može se razmatrati u svrhu poboljšanja i oblikovanja održivog razvoja društva u cjelini.

study is determined by the fact that budget security stands out primarily as a component of social development and can be considered in order to improve and shape the sustainable development of society as a whole.

Introduction

Considering that one of the components of national interests in the legal sphere contains the development of the information industry, including the industry of means of informatisation, telecommunications and communications /**1**/, improper handling of which could harm their owner, user or other a person – an assessment of the security of state information resources in information /**2**/, telecommunication and information and telecommunication systems and their level is a priority task and, moreover, is of practical importance /**3**/. Given such a solution to the problem of the legal category, this will make it possible to assess the state and level of security of state information resources in information, telecommunication, and IT systems /**4**/. For this, the following particular problems must be solved:

– based on the totality of the most dangerous threats, which should be addressed as the primary protection measures, – to form the totality of the "threat-vulnerability" pairs;

– based on the totality of the generated "threat-vulnerability" pairs – to determine the security index of information resources and calculate a comprehensive indicator of their security status.

The ability of ITC to counteract attempts to violate the integrity, confidentiality and accessibility of information that circulates and/or is processed in them is understood As the state of information security in ITC /**5**/. The assessment of the information security in ITC is a set of measures aimed at identifying threats to information in ITC and preventing unauthorised actions against it /**6**/.

Materials and methods

Obviously, the main increase in the level of security of budgetary security is an integrated approach, which is based on the organisational and technical structure of the information security system in ITC /**7**/. The creation of such a highly efficient system requires solving a set of optimisation problems and, in particular, choosing appropriate criteria for optimising the state of budget security.

Recent studies in this field, as well as an analysis of the organisational and technical structure of the security system as an economic criterion for optimising the state of budget security, allow to choose a multi-component criterion **(F)**, the objective function and security restrictions are presented below /**8**/:

$$F = f\ min\ a_c \tag{1}$$

Where

$$a_c = \underset{k\,=\,1}{\overset{N}{}} c_k \tag{2}$$

$$F\ R_i \leq F^*(R_i) \tag{3}$$

In this case, $F\ R_i$ – the probability of occurrence of special situations in ensuring the protection of information, which are normalised by regulatory documents (*if i*=1, …, 4) – is the rationing index.

Given this, the basic economic principles for ensuring the necessary level of budget security can be the following principles:

– firstly, minimising costs while ensuring a standardised level of protection;

– secondly, minimising costs corresponding to a given change in the level of protection.

Given the multi-component nature of the selected criterion, the optimal control effects on the state of budget security are always complex and the improvement of one of its components is accompanied by the deterioration of the other /**9**/.

The current state of budget security is determined by a set of processes and is described by a vector in n -dimensional space. Thus, the basis for making a decision about the state of budget security in the ITC is the technical state of the protection system, which, first of all, is determined when diagnosing the object of protection using the protection system by identifying (recognising) the state of the object and developing control decisions that determine the state of security, ensuring the fulfilment of the conditions of formula 2.

The protection system (PS) of the budget for OID is denoted by the symbol "A". Other symbols are the stages of IS maintenance, namely: b – the stage of research of PS in order to obtain the necessary information; c – the stage of analysis of existing IS support processes; d – the stage of development of proposals for optimising the processes of ensuring information security; e – the stage of development of the necessary organisational and administrative documents; f – the stage of refinement of existing means of information protection and the introduction of new ones.

Then for the life cycle of PS in general form there is:

$$Y_a = b, c, d, e, f \tag{4}$$

For the budget security management process, it is possible to formulate a relationship between the set $P_i$of values i -th of reliability indicators and the set $D_j$of values j -th of diagnostic indicators of the state of budget security, the set P_i of reliability indicators and the corresponding stages of IS provision:

$$R_k \rightarrow P_i, D_j \leftrightarrow B_k \leftrightarrow Y_0 \tag{5}$$

Obviously, this ratio should ensure the fulfilment of condition 3.

Based on the foregoing, the basic principle of optimal compliance with the state of the information security system in ITC is formulated: the optimal budget protection system should provide adequate conditions according to expression 4 while minimising the objective function 1 and fulfilling constraint 2. Therefore, it is advisable to select and evaluate the consequences of control actions on the basis of simulation models, which for some functional budget protection systems have now been developed.

A legal apparatus for assessing the state of budget security under the influence of current threats and vulnerabilities is proposed for consideration **/10/**. In a formalised form, this task reduces to determining the probability of a decrease in the security of the budget complex and the formation of a model of budget security **/11/**. The authors consider the mathematical method and model the form of legal protection on the basis of the mathematical apparatus, since budgetary security and its legal expression should be based on a comprehensive consideration of signs and threatening phenomena, which in turn can only be determined mathematically **/12/**.

There is some known ordering in the direction of increasing the coefficient of significance of the actual threats that form the reference sample $\gamma = \gamma_{zagr1}, \dots, \gamma_{zagri}, \dots, \gamma_{zagrQ}$. At the same time, $i = \overline{1, Q}, , Q$ – the number of threats in the reference sample. Each of these threats has a priority established by a certain rule and is characterised by corresponding indicators – $''j''$ $\left(j = \overline{1, L}\right)$ and vulnerabilities.

It is necessary, according to the totality of indicators, the set of relevant threats from the reference sample and relevant vulnerabilities of the IS, to determine the state of information security in ITC, that is, the ability of ITC to resist attempts to violate the integrity, confidentiality, accessibility and observability of information at the impact time of each actual threat on budget security **/13/**.

The solution comes down to the implementation of such successive stages:

– development of a procedure for the formation of many pairs of "threat-vulnerability" according to a reference sample of current threats to information security with the determination of the time of the impact of current threats on the information resource;

– the formation of a technology for assessing the security status of information resources under the influence of current threats and vulnerabilities, based on the set of "threat-vulnerability" pairs established in the reference sample of current threats.

Results and discussion

Based on the fact that the relationship between a pair of objects $x\,F\,X$, $y\,F\,Y$ is traditionally expressed in the form of an ordered pair (x, y), a condition is introduced according to which each vulnerability from the current list of vulnerabilities $Y = y_1, y_2, \dots, y_m, m = \overline{1, M}$corresponds to a threat with the longest budget exposure time from the reference sample of threats $Z = Z_{zagr1}, Z_{zagr2}, \dots, Z_{zagrk}, k = \overline{1, Q}$ and the conditions for which this vulnerability can be implemented (Table 1).

Table 1. An example of the formation of "threat-vulnerability" pairs

An example of threats	An example of vulnerabilities
Physical damage / Loss of building / Loss of information /	No fire alarm Lack of fire extinguishing system Permission to smoke indoors The presence of flammable materials The presence of a malicious arsonist Staff negligence Staff ignorance Criminal acts

As a rule, such relations are determined by the direct (Cartesian) product of sets $XiY{:}XFY$ according to rule 1:

Rule 1: Pair = [threat] due to [vulnerability]

Given this, the set of all possible combinations of threats and vulnerabilities, which are the Cartesian product of the set $T$and consisting V of ordered pairs z_k, y_m, are defined:

$$R = ZFYF\ z_1, vy_1, z_1, y_2, \dots, z_k, y_mF \qquad (6)$$

Next, a fuzzy set of threat-vulnerability pairs is defined:

$$R = F\ z_1, y_1/ij\ z_1, y_2/1F, \dots, z_k, y_m/kmF \qquad (7)$$

As it can be see, a set R is a set of tuples, the first component of which are elements z_iF ..., the second – elements y_jEY, and the third – elements $ijFM$. A set R is a universal set of sets, and a set $M$is a set of values of a membership function from the range 0.1

The meaning of a fuzzy set of values of belonging of an ordered pair from set R to set R – the subjective expression of an expert in the fact that for a given information system a threat z_i is realised through a vulnerability y_i.

In this case, it is not about the likelihood of a threat being realised through a vulnerability. Probability characterises the share of this threat realisation during the functioning of the information system in a given period of time. Belonging characterises a subjective measure of how an ordered pair (z_i, y_j) responds to the expert's opinion – this threat is realised through this vulnerability. In other words, regardless of the probability values of occurrence of threats from the set Z, it is evaluated how legitimate the statement that the threat $z_1$is realised through the vulnerability y_j. The legal definition and purpose of the probability of a threat are related to the collection of statistics; the legal definition and purpose of affiliation are associated with the prevailing views of a lawyer on the character of the threats and vulnerabilities being studied, that is, with his personal experience.

Of course, statistical patterns identified by a lawyer at one time may also influence the personal experience accumulation /**14**/. However, a lawyer almost never directly identifies and compares statistical laws, calculates probability values, etc. /**15**/. Knowledge corresponding to his experience is formed, generally speaking, in the form of images that do not have clear boundaries. To a certain extent, it can be said that these images are a kind of metadata that, at a qualitative level, represent absolutely all the quantitative results of experiments, which serve as the basis for the formation of personal experience, including statistical observations /**16**/. Further, when making a decision, a lawyer refers specifically to images, such as the probability of this event occurring is huge (a linguistically given probability value), – most likely, there is a relationship between these two objects (a linguistically given binary relation), – of the two objects, the first more significant than the second (linguistically given preference relation), etc. /**17**/

For this reason, the described procedure for representing the relationship between threat and vulnerability may be more effective than the model based on the probability of events /**18**/. The model allows a more accurate description of processes that violate the security of the budget, without losing the time associated with the collection of facts /**19**/.

In many issues related to the organisation and ensuring information security, quite often there are tasks associated with the need to select and justify the time required to perform a certain action. An example of such tasks is the task of legal competition, in which each side seeks to delay their actions as much as possible and get some gain from this, but at the same time can suffer significant losses as a result of waiting.

In general, the function of winning or victory in such tasks can be written as follows:

$$M(x,y) = \begin{array}{c} Kx,\ \ if\ x < y \\ Ix, if\ x = y \\ Lx,y,\ \ if\ x > y \end{array} \qquad (8)$$

where functions K, I, L may be subject to various restrictions determined by the specific conditions of the problem being solved.

Denote the distribution function $P(x)$, which has a jump in the value$a$ at zero, a jumpβ in unity, through $Px = (\alpha I_0, \rho_{ab}x, \beta I_1)$, where the distribution $\rho_{ab}(x)$ is completely continuous over the entire interval $[a, b] \subset [0,1]$.

Based on the foregoing, the following theorem is true.

Theorem 1. Let the payoff function of a continuous legal task have the form:

$$M\Bigl(x, y = \begin{array}{l} K\ x, y,\ \text{при}\ x \le y; \\ L\ x, y,\ \text{при}\ x \ge y; \end{array} K\ x, x = L\ x, x \qquad (9)$$

where the functions K, L satisfy the following conditions: in their domains of definition, the functions $K(x,y), L(x,y)$ have continuous third partial derivatives; derivatives $K_{xx}(x,y)$, $K_{yy}(x,y)$ strictly negative for$x \le y$, and derivatives $L_{xx}(x,y)$ and $L_{yy}(x,y)$ strictly negative for $x \ge y$; the function $K(x,y)$ strictly increases in $y$and strictly decreases in x, and the function $L(x,y)$ strictly increases in x and strictly decreases in y.

Then both sides have such a single optimal mixed strategy:

$$Fx = \alpha I_0, fx, \beta I_1 \qquad (10)$$

$$Gy = \gamma I_0, gy, \delta I_1 \qquad (11)$$

where the functions $f(x)$ and $g(y)$ are absolutely continuous in the entire interval [0,1] and come out as single solutions to a pair of integral equations:

$$\alpha p_1 + \beta p_2 = f + T_f \qquad (12)$$

$$\gamma q_1 + \delta p q_2 = q + R_q \qquad (13)$$

Where:

$$T_f = {}_0^y \frac{K_{yy}(x,y)}{K_y y,y - L_y(y,y)} \times fxdx + {}_y^1 \frac{L_{yy}(x,y)}{K_y y,y - L_y(y,y)} \times fxdx \qquad (14)$$

$$R_q = {}_0^q \frac{L_{xx}(x,y)}{L_x x,x - K_x(x,x)} \times qydy + {}_x^1 \frac{L_{xx}(x,y)}{L_x x,x - K_x(x,x)} \times qydy; \qquad (15)$$

$$p_1 = -\frac{K_{yy}0,y}{K_y y,y - L_y y,y}; p_2 = -\frac{L_{yy}1,y}{K_y y,y - L_y y,y}; \qquad (16)$$

$$q_1 = -\frac{L_{xx}x,0}{L_x x,x - K_x x,x}; q_2 = -\frac{L_{xx}x,1}{L_x x,x - K_x x,x} \qquad (17)$$

Constants α, β, δ are denoted under the following conditions:

$${}_0^1 fxdx = 1 - \alpha - \beta, 0 \le \alpha, \beta \le 1; \qquad (18)$$

$${}_0^1 qydy = 1 - \gamma - \delta, 0 \le \gamma, \delta \le 1; \qquad (19)$$

Thus, the solution of such problems as, for example, determining the moment in time of the impact of current threats on the budget, can be reduced to solving a number of integral equations. The following theorem follows from this.

Theorem 2. Let the payoff function of a continuous game problem have the form:

$$M(x,y) = \begin{matrix} Kx,y < \quad if\ x < y \\ Ix, if\ x = y \\ Lx,y,\ if\ x > y \end{matrix} \tag{20}$$

where the functions K, I, L satisfy the following conditions: $K(x,y)$ and $L(x,y)$ are defined and have continuous second partial derivatives, respectively, on closed triangles $0 \le x \le y \le 1$ and $0 \le y \le x \le 1$; the value $I(1)$ is located between $K(1,1)$ and $L(1,1)$; the value$I(0)$ is located between $K(0,0)$ and; and $L(0,0)$; $K_x(x,y) > 0$ and $L_x(x,y) > 0$ in the corresponding closed triangles with possible exception $L_x(1,1) = 0$; $K_x(x,y) < 0, L_x(x,y) < 0$ in the corresponding closed triangles with possible exception $K_x(1,1) = 0$.

Then both sides have optimal strategies of the form $Fx = (\alpha l_0, f_{a1}, \beta I_1), Gy = (\gamma l_0, q_{a1}, \delta I_1)$, where distribution densities are defined as solutions of the following integral equations:

$$f_{a1}(t) - {}_{a}^{1}T_{a1}x,t \times f_{a1}xdx = ap_1 + \beta p_2 t; \tag{21}$$

$$g_{a1}(u) - {}_{a}^{1}U_{a1}u,y \times g_{a1}ydy = \gamma q_1 u + \delta q_2 u; \tag{22}$$

$$T_{al}x,t = \begin{matrix} \frac{-K_y(x,y)}{Kt,t-L(t,t)},\ if\ \alpha \le x \le t \le 1, \\ \frac{-L_y(x,t)}{Kt,t-L(t,t)},\ if\ \alpha \le t \le x \le 1 \end{matrix} \tag{23}$$

$$U_{al}u,y = \begin{matrix} \frac{-L_x(u,y)}{Ku,u-L(u,u)},\ if\ \alpha \le y \le u \le 1, \\ \frac{-L_y(x,t)}{Kt,t-L(t,t)},\ if\ \alpha \le u \le y \le 1 \end{matrix} \tag{24}$$

$$p_1 t = \frac{-K_y(0,t)}{Kt,t-L(t,t)}, p_2 t = \frac{-L_y(1,t)}{Kt,t-L(t,t)}; \tag{25}$$

$$q_1 u = \frac{-L_x(u,0)}{Ku,u-L(u,u)}, q_2 u = \frac{-L_y(u,1)}{Kt,t-L(t,t)}. \tag{26}$$

Remark 1. It is clear from expression (17) that if $K(1,1) < L(1,1)$, then the point $x = 1, y = 1$ is a combined point for $M(x,y)$. This follows from the conditions of Theorem 2.

Corollary 1. In the case when $l(x) = 0, K(x,y) = L(x,y)$, then the game problem is called symmetric. The symmetric game problem is investigated for the case when the function $M(x,y)$in the domain $0 \le x \le y \le 1$ is continuous in both variables and has continuous first-order partial variables $M_x(x,y), M_y(x,y)$ such that $M_x(x, y \ge 0), M_y(x,y) \le 0\ if\ x \le y$ the set of points for which $M_x(x,y) = 0$ or $M_y(x,y) = 0$ does not contain any interval of the form $x = const, \beta_1 < y < \beta_2$ or $y = const\ \alpha_1 < x < \alpha_2$.

If $K(1,1) \le 0$, the optimal unity strategy will look like:

$$Fx = I_1 = \begin{matrix} 0 \text{ при } 0 \le x \le 1, \\ 1 \text{ при } x = 1 \end{matrix} \tag{27}$$

If $K(0,1) > 0$, the optimal strategy will be:

$$Fx = I_0 = \begin{matrix} 0\ if\ x = 0 \\ 1\ if\ 0 \le x \le 1 \end{matrix} \tag{28}$$

In the case $K(0,1) < 0 < K(1,1)$, it is possible, without loss of generality, to consider $K(x,x) > 0$ when $0 < 0 \le 1$. Then there is uniquely some interval of the form $[a, 1], 0 \le a \le 1$ such that the optimal strategy has the form:

$$Fx = \begin{matrix} 0\ if\ x = 0 \\ \alpha\ if\ 0 < x < \alpha \\ \alpha + {}_{0}^{x}f_{a1}\xi d\xi\ if\ \alpha < x \le 1 \end{matrix} \tag{29}$$

where f_{a1} – a continuous positive function; the parameter α is a jump$F(x)$) at zero, and is determined from the normalisation condition:

$${}_{\alpha}^{1}f_{\alpha 1}\xi d\xi = 1 - \alpha \tag{30}$$

From Theorem 2 it follows that the optimal strategy $F(x)$ for a symmetric game problem in this case exists only when it is possible to find numbers $\alpha, \alpha(0 \le \alpha, \alpha < 1)$ and such a continuous function$f_{\alpha 1}(x)$ denoted $\alpha < x < 1$ and

$$\alpha K0,y + {}_{\alpha}^{y}Kx,yf_{\alpha 1}xdx - {}_{y}^{1}Ky,xf_{\alpha 1}xdx = 0\ (\alpha < y < 1) \tag{31}$$

Remark 2. The case of a function $M(x,y)$growing in y and decreasing in x, with the help of substitution

$$\xi = 1 - x, \eta = 1 - y \tag{32}$$

$$\xi = 1 - x, \eta = 1 - y \qquad (33)$$

and reduced to the case of growth in x and decrease in y, considered in Theorem 2.

Remark 3. If in Theorem 3, instead of condition (20), to assume that

$$K_y y, y - L_y(y, y) > 0 \qquad (34)$$

$$K_x x, x - L_x(x, x) > 0, \qquad (35)$$

then it is possible to show that the optimal strategies of both sides will have the form of distribution functions

$$Fx = (\alpha I_a, f_{ab}(x), \beta I_b), Gy = (\gamma I_a, g_{ab}(y), \delta I_b), \alpha, \beta, \gamma, \delta \geq 0, \qquad (36)$$

$$Fx = (\alpha I_a, f_{ab}(x), \beta I_b), Gy = (\gamma I_a, g_{ab}(y), \delta I_b), \alpha, \beta, \gamma, \delta \geq 0 \qquad (37)$$

and the functions $f_{ab}, g_{ab}(y)$ come in the form of Neumann series in terms of the eigenfunctions of the connected integral equations:

$$f_{ab}(t) - {}_{a}^{b}T_{ab}x, t \times f_{ab}xdx = ap_1t + \beta p_2(t) \qquad (38)$$

$$g_{ab}(u) - {}_{a}^{b}U_{ab}u, y \times g_{ab}ydy = \gamma q_1u + \delta q_2(u) \qquad (39)$$

Now consider a special class of symmetric game problems for which $M(x, y)$ is not necessarily continuous in the aggregate of variables at points (0. 0) and (1.1) and it is only required that there are restrictions taking into account:

$$K\ 0,0 = lim_{y\to 0}K\ 0, y; K\ 1,1 lim_{x\to 1}K\ x, 1; \qquad (40)$$

Assume that

$$K\ x, y = k\frac{x}{y} \qquad (41)$$

where the function $k(u)$is continuously differentiable in $0 \leq u \leq 1$, and its derivative $k'(u)$ in this interval does not change sign, and the set of points $u$for which$k'(u) = 0$ does not contain any interval.

It is easy to see that when $k'(u) \geq 0$, the optimal strategy is $Fx = I_1\ if\ k1 \leq 0, Fx = I_0\ if\ k(u) \geq 0$. The proof of this fact is based on the principles of the search for sustainable strategies. To do this, the equation is written:

$$E_1F, 0 = E_1F, 0 + \alpha K\ 0,0 = E_1F, 0 + \alpha K\ 0 \qquad (42)$$

whose correctness is established using (31).

For $\delta > 0$ there is:

$$E_1F, \delta = {}_{0}^{\delta - 0}Kx, \delta dFx - {}_{\delta}^{1}K\delta, xdFx \qquad (43)$$

$$E_1F, 0 = -{}_{\delta}^{1}K0, xdFx \qquad (44)$$

Such that

$$E_1F, \delta - E_1F, 0 = \alpha K\ 0, \delta + {}_{0}^{\delta - 0}Kx, \delta dFx - {}_{\delta}^{1}K\delta, xdFx + {}_{\delta}^{1}K0, xdFx; \qquad (45)$$

heading towards$\delta \to 0$ when $\alpha K(0,0)$. To evaluate the integrals in (45), choose from the given $\varepsilon > 0$ such η that the total variation $F(x)$ in $[0, \eta]$ is less

$$\varepsilon/4K_0, K_o = Sup[K(x, y)]. \qquad (46)$$

Then the first integral is less than $\varepsilon/4$, and the last two are represented as:

$${}_{0}^{\eta}K0, \delta dFx - {}_{0}^{\eta}K\delta, xdFx + {}_{\eta}^{1}K0, x - K\delta, xdFx = J_1 + J_2 + J_3 \qquad (47)$$

This shows that $J_i \leq \frac{\varepsilon}{4}, i = 1,2,3$. This proves the validity of expression (44). Let first $\alpha = 0$. C $E_1F, y = 0$ when $\alpha < y < 1$ follows that $E_1F + 0 = 0$. When $\alpha > 0$, $E_1F, 0 = 0$ should be; by virtue of $k(0) < 0$, this contradicts (42). On the other hand, if $\alpha = 0$ there is:

$$E_1F, +0 = -{}_{0}^{1}k0fxdx = -k(0){}_{0}^{1}fxdx = -k(0) > 0 \qquad (48)$$

which, obviously, is impossible. If further $\alpha > 0$, then with $E_1F, \alpha = 0$ there is a strict decay of the function

$$E_1F, y = ak0 - \frac{1}{a}k\frac{y}{x}f(x)dx \qquad (49)$$

in the interval$0 < y \leq a\ E_1F, +0 > 0$ follows. If $\alpha > 0$ and $E_1F, 0 = 0$, then from expression (37) $E_1F, +0 = \alpha k0 < 0$ is obtained that is a contradiction. Accordingly $\alpha > 0, \alpha = 0$. In this case, equation (28) $E_1F, y = 0$ is equivalent in the interval $(\alpha, 1)$ provided $E_i^1F, y = 0$. Hence, to determine the density$f(x)$, the integral equation is obtained

$$2k1fy = {}_{a}^{y}\frac{x}{y^2}k'\frac{x}{y}fxdx + {}_{y}^{1}\frac{f(x)}{x}k'\frac{x}{y}fxdx, \ (a < y < 1) \qquad (50)$$

The condition must be met ${}_{a}^{1}fxdx = 1$.

Remark 4. For the case $k\text{'}(u) \leq 0$, it can be shown that optimal strategies have the form $Fx = \alpha I_0 + \beta I_1$. Thus, it is easy to verify the validity of the following formulas:

$$Fx = \alpha I_0 x + \frac{I_1(x)}{I_0 x} 1 - I_1 x \begin{array}{ll} if & k(0) < 0 \\ if\ k0 = 00 \leq \alpha \leq 1 & \\ if & k(0) > 0 \end{array} \tag{51}$$

The analysed situations showed that a reasonable choice of threats to the budget from the reference sample, which have the longest action time on the information resource in conditions of conflict and uncertainty, should contribute to the application of game theory with payoff functions. As a result, this will make it possible to solve the difficult task of identifying the time moment of a threat's impact on the budget and, thus, reduce the time it takes to make a decision on the localisation and legal opposition to a detected threat.

Tasks like assessing the state of budget security under the influence of legal threats and vulnerabilities belong, as is known, to the multicriteria class. For their collegial solution in conditions of uncertainty and conflict among existing methods of mathematical modelling, methods of forming and studying generalised quality indicators using graphoanalytic and similar approaches, legal methods for solving complex problems of evaluation and selection of objects, including special purposes, as well as analysis and forecasting situations with a large number of significant factors, the most rational and determining are precisely legal methods. They provide an opportunity to more deeply study the phenomena that significantly affect the level of protection of both the state as a whole and individual objects of its information infrastructure from the influence of internal and external threats, to identify the most important and essential in these processes, without omitting those details and relationships, without which a model of the studied situation cannot be built. An increase in the effectiveness of the application of expert methods is usually facilitated by the assessment of legal consequences:

– conducting a reasonable selection of a group of highly qualified lawyers whose activities are related to conducting research in the areas selected for the conduct and whose positions correspond to the requirements for those in the chosen branch of knowledge;

– timely familiarisation of lawyers for the purpose of research and explaining to them the content of the work that they must perform;

– questionnaire survey of lawyers taking into account all stages of the examination of each event to ensure IS of a state or individual objects of its infrastructure regarding certain requirements for the established indicators and their respective indicators.

Given this recent widespread use among well-known methods of legal assessment, allowing directly to use the judgments and intuition of lawyers in any formalised structure to solve problems with social, political or military content, the questionnaire method has been obtained, then you should use it. When solving the problem of assessing the state of security of information resources under the influence of current threats and vulnerabilities, its essence will be revealed from the point of view of one lawyer. As the initial data, the system of actual threats will be used that has developed in the reference sample of the many threat-vulnerability pairs and the set of indicators (criteria) of existing threats that characterise the possibility of violating confidentiality, integrity, availability and observability of information. The solution to this problem is to determine the security index of information resources and calculate a comprehensive indicator that characterises the state of elimination of legal consequences from violation of the regime.

The budget security index will be considered a dynamic quantitative and qualitative characteristic that indicates the organisation's ability to provide its own information security and maintain the safe functioning of the objects of their information structure in the context of existing threats to information resources. Its determination is carried out on the basis of identifying deviations from the normal operating mode, IT systems and networks, as well as software and hardware, by analysing four main categories, namely:

1) impact on integrity;

2) effects on confidentiality;

3) impact on accessibility;

4) effects on observation.

Each of these categories falls under the influence of threat/vulnerability (ZY) pairs formed in the reference sample and current information security threats. Such pairs can be pairs like:

1. Obtaining unauthorised logical access to information by external attackers/lack of a policy for using network services ($ZY1$):

– there is no list of networks and network services to which access is allowed;

– there are no authorisation procedures to determine who is allowed access and to which networks and network services;

– there are no security measures and control procedures to protect access to network connections and network services;

– means used to access networks and network services (for example, conditions for allowing telephone lines to access the services of an Internet provider or a remote system).

– the policy of using network services should not contradict the policy of controlling business access.

2. Lack of recovery options/lack of backup information ($ZY2$):

– the necessary level of information backup has not been determined;

– the volume and frequency of backups does not reflect the business requirements of an organisation, the security requirements for the information involved and the criticality of information for the continuous operation of an organisation;

– backups are not stored in a remote place, at a sufficient distance, thereby avoiding any damage from natural disasters in the main room is not achieved;

– backup media is not tested and cannot be trusted in the event of an emergency;

– confidential backups are not protected by encryption;

3. Disclosure, sale, fraudulent copying of information/lack of procedures for handling information ($ZY3$):

– no mechanisms have been introduced to restrict access to information to prevent access to personnel who do not have sanctions;

– the registry of authorised data recipients is not supported;

– protection of the uploaded data awaiting withdrawal is not ensured at a level that does not contradict their confidentiality;

– storage of media in accordance with the manufacturer's specifications;

– distribution lists and lists of authorised recipients are not reviewed at regular intervals;

– no clear labelling of all copies of media has been introduced.

4. Violation by staff of organisational measures to ensure information security/lack of information security policy ($ZY4$):

– the information security policy does not contain requirements regarding compliance with legislative, regulatory and contractual requirements;

– the information security policy contains the basics of setting goals for security measures and security measures themselves, including the structure of risk assessment and risk management;

– the information security policy contains requirements for the education, training and awareness of security personnel;

– the information security policy contains explanations of the consequences of violation of the information security policy;

– the information security policy contains the definition of general and special responsibilities for managing information security, including reporting on information security incidents;

– the IS policy is revised as planned or when significant changes (there are revision marks) a revision of the information security policy takes into account the results of views from the management in accordance with a specific review procedure from the side of the management, including the schedule or frequency of reviews, registration of views from the management is supported.

5. Uncontrolled modification of an information resource/lack of cryptographic protection measures ($ZY5$):

– the absence of the identified desired level of protection, taking into account the type, stability and quality of the necessary encryption algorithm;

– lack of use of encryption to protect confidential information that is transported on mobile or removable media, devices or through communication channels;

– there is no approach to key management, including methods related to the protection of cryptographic keys and the recovery of encrypted information in case of lost, compromised or damaged keys.

Based on the above indicators characterising an organisation's ability to provide information security and maintain the safe functioning of its own information structure objects, a hierarchical scheme of their indicators will be developed in which the values of the previous i-th level are determined by the value of the corresponding indicators of the i-th level (Table 2).

Table 2. Hierarchical diagram of the state of budget security

The level of information security criticality																				1st level
Impact on integrity			Impact on confidentiality							Impact on accessibility					Impact on observability					2nd level (categories)
ZY1	ZY2	ZY3	ZY4	ZY5	ZY1	ZY2	ZY3	ZY4	ZY5	ZY1	ZY2	ZY3	ZY4	ZY5	ZY1	ZY2	ZY3	ZY4	ZY5	3rd level (indicators)
$A1_1$ $A1_2$ $A1_3$ $A1_4$ $A1_5$	$A2_1$ $A2_2$ $A2_3$ $A2_4$ $A2_5$	$A3_1$ $A3_2$ $A3_3$ $A3_4$ $A3_5$ $A3_6$	$A4_1$ $A4_2$ $A4_3$ $A4_4$ $A4_5$ $A4_6$	$A5_1$ $A5_2$ $A5_3$	$B1_1$ $B1_2$ $B1_3$ $B1_4$ $B1_5$ $B1_6$	$B2_1$ $B2_2$ $B2_3$ $B2_4$ $B2_5$	$B3_1$ $B3_2$ $B3_3$ $B3_4$ $B3_5$ $B3_6$	$B4_1$ $B4_2$ $B4_3$ $B4_4$ $B4_5$ $B4_6$	$B5_1$ $B5_2$ $B5_3$	$C1_1$ $C1_2$ $C1_3$ $C1_4$ $C1_5$ $C1_6$	$C2_1$ $C2_2$ $C2_3$ $C2_4$ $C2_5$	$C3_1$ $C3_2$ $C3_3$ $C3_4$ $C3_5$ $C3_6$	$C4_1$ $C4_2$ $C4_3$ $C4_4$ $C4_5$ $C4_6$	$C5_1$ $C5_2$ $C5_3$	$D1_1$ $D1_2$ $D1_3$ $D1_4$ $D1_5$ $D1_6$	$D2_1$ $D2_2$ $D2_3$ $D2_4$ $D2_5$	$D3_1$ $D3_2$ $D3_3$ $D3_4$ $D3_5$ $D3_6$	$D4_1$ D D $D4_4$ $D4_5$ D	$D5_1$ $D5_2$ $D5_3$	44th level (figures)

At the same time, a set of specific indicators are into compliance with categories, which in turn are described by elementary characteristics, which are called figures. Each category of the 2nd level, each indicator of the 3rd level and each figure of the 4th level of the hierarchy with a certain rule, by means of an expert survey, can be associated with a certain number (Table 3). A prerequisite for this is the following: the sum of the weights of categories, indicators and figure of one level should always be equal to one.

Table 3. Values of categories and indicators of the criticality level of budget security

Designations of criticality categories and indicators	Designations of weights of categories and indicators	Values of weights of categories and indicators	Sum of indicator weights
Impact on integrity	$g1$	0.26	
$ZY1$	$a1$	0.13	1.0
$ZY2$	$a2$	0.31	
$ZY3$	$a3$	0.15	
$ZY4$	$a4$	0.12	
$ZY5$	$a5$	0.29	
Impact on confidentiality	$g2$	0.25	
$ZY1$	$b1$	0.20	1.0
$ZY2$	$b2$	0.18	

$ZY3$	$b3$	0.29	
$ZY4$	$b4$	021	
$ZY5$	$b5$	0.12	
Impact on accessibility	$g3$	0.26	
$ZY1$	$c1$	0.21	1.0
$ZY2$	$c2$	0.25	
$ZY3$	$c3$	0.17	
$ZY4$	$c4$	0.18	
$ZY5$	$c5$	0.19	
Impact on observability	$g4$	0.23	
$ZY1$	$d1$	0.20	1.0
$ZY2$	$d2$	0.19	
$ZY3$	$d3$	0.20	
$ZY4$	$d4$	0.17	
$ZY5$	$d5$	0.24	

In this, the meaning of categories and quality indicators are determined as follows.

Impact on the integrity of threat/vulnerability pairs:

$$\langle Z\rangle a1\langle ZY1\rangle, a2\langle ZY2\rangle, a3\langle ZY3\rangle, a4\langle ZY4\rangle, a5\langle ZY5\rangle \quad (52)$$

$$\langle ZY1\rangle = a1_1A1_1 + a1_2A1_2 + a1_3A1_3 + a1_4A1_4 + a1_5A1_5 = \sum_i \quad a1_iA1_i; i = \overline{1,5} \quad (53)$$

where $a1_1, a1_2, a1_3, a1_4, a1_5$ – weight coefficients of figures of 4th level for $A1_1, A1_2, A1_3, A1_4, A1_5, a1_1 + a1_2 + a1_3 + a1_4 + a1_5 = \sum_i \quad a1_i = 1$;

$$\langle ZY2\rangle = a2_1A2_1 + a2_2A2_2 + a2_3A2_3 + a2_4A2_4 + a2_5A2_5 = \sum_i \quad a2_iA2_i; i = \overline{1,5} \quad (54)$$

where $a2_1, a2_2, a2_3, a2_4, a2_5$ – weight coefficients of figures of 4th level for $A2_1, A2_2, A2_3, A2_4, A2_5, a2_1 + a2_2 + a2_3 + a2_5 = \sum_i \quad a2_i = 1$;

$$\langle ZY3\rangle = a3_1A3_1 + a3_2A3_2 + a3_3A3_3 + a3_4A3_4 + a3_5A3_5 + a3_6A3_6 = \sum_i \quad a3_iA3_i; i = \overline{1,6} \quad (55)$$

where $a3_1, a3_2, a3_3, a3_4, a3_5, a3_6$ – weight coefficients of figures of 4th level for $A3_1, A3_2, A3_3, A3_4, A3_5, A3_6, a3_1 + a3_2 + a3_3 + a3_4 + a3_5 + a3_6 = \sum_i \quad a3_i = 1$;

$$\langle ZY4\rangle = a4_1A4_1 + a4_2A4_2 + a4_3A4_3 + a4_4A4_4 + a4_5A4_5 + a4_6A4_6 = \sum_i \quad a4_iA4_i; i = \overline{1,6} \quad (56)$$

where $a4_1, a4_2, a4_3, a4_4, a4_5, a4_6$ – weight coefficients of figures of 4th level for $A4_1, A4_2, A4_3, A4_4, A4_5, A4_6, a4_1 + a4_2 + a4_3 + a4_4 + a4_5 + a4_6 = \sum_i \quad a4_i = 1$;

$$\langle ZY5\rangle = a5_1A5_1 + a5_2A5_2 + a5_3A5_3 = \sum_i \quad a5_iA5_i; i = \overline{1,3} \quad (57)$$

where $a5_1, a5_2, a5_3$ – weight coefficients of figures of 4th level for A$A5_1, A5_2, A5_3,, a5_1 + a5_2 + a5_3 = \sum_i \quad a5_i = 1$;

Impact on confidentiality of threat-vulnerability pairs:

$$< K \geq b1\langle ZY1\rangle, b2\langle ZY2\rangle, b3\langle ZY3\rangle, b4\langle ZY4\rangle, b5\langle ZY5\rangle \quad (58)$$

where $b1, b2, b3, b4, b5$ – weight relevant coefficients of figures of 4th level, moreover $b1 + b2 + b3 + b4 + b5 = 1$

$$\langle ZY1\rangle = b1_1A1_1 + b1_2A1_2 + b1_3A1_3 + b1_4A1_4 + b1_5A1_5 = \sum_i \quad b1_iA1_i; i = \overline{1,5} \quad (59)$$

where $b1_1, b1_2, b1_3, b1_4, b1_5$ – weight coefficients of figures of 4th level for $A1_1, A1_2, A1_3, A1_4, A1_5, b1_1 + b1_2 + b1_3 + b1_4 + b1_5 = \sum_i \quad b1_i = 1$;

$$\langle ZY2\rangle = b2_1A2_1 + b2_2A2_2 + b2_3A2_3 + b2_4A2_4 + b2_5A2_5 = \sum_i \quad b2_iA2_i; i = \overline{1,5} \quad (60)$$

where $b2_1, b2_2, b2_3, a2_4, a2_5$ – weight coefficients of figures of 4th level for

$A2_1, A2_2, A2_3, A2_4, A2_5, b2_1 + b2_2 + b2_3 + b2_4 + b2_5 = \sum_i \quad b2_i = 1;$

$$\langle ZY3\rangle = b3_1A3_1 + b3_2A3_2 + b3_3A3_3 + b3_4A3_4 + b3_5A3_5 + b3_6A3_6 = \sum_i \quad b3_iA3_i; i = \overline{1,6} \tag{61}$$

where $b3_1, b3_2, b3_3, a3_4, a3_5, a3_6,$ – weight coefficients of figures of 4th level for $A3_1, A3_2, A3_3, A3_4, A3_5, A3_6, b3_1 + b3_2 + b3_3 + b3_4 + b3_5 + b3_6 = \sum_i \quad b3_i = 1;$

$$\langle ZY4\rangle = b4_1A4_1 + b4_2A4_2 + b4_3A4_3 + b4_4A4_4 + b4_5A4_5 + b4_6A4_6 = \sum_i \quad b4_iA4_i; i = \overline{1,6} \tag{62}$$

where $b4_1, b4_2, b4_3, a4_4, a4_5, a4_6,$ – weight coefficients of figures of 4th level for $A4_1, A4_2, A4_3, A4_4, A4_5, A4_6, b4_1 + b4_2 + b4_3 + b4_4 + b4_5 + b4_6 = \sum_i \quad b4_i = 1;$

$$\langle ZY5\rangle = b5_1A5_1 + b5_2A5_2 + b5_3A5_3 = \sum_i \quad b5_iA5_i; i = \overline{1,3} \tag{63}$$

where $b5_1, b5_2, b5_3$ – weight coefficients of figures of 4th level for $A5_1, A5_2, A5_3, b5_1 + b5_2 + b5_3 = \sum_i \quad b5_i = 1;$

Impact on accessibility of threat/vulnerability pairs:

$$< D \geq c1\langle ZY1\rangle, c2\langle ZY2\rangle, c3\langle ZY3\rangle, c4\langle ZY4\rangle, c5\langle ZY5\rangle \tag{64}$$

where $c1, c2, c3, c4, c5$ – weight coefficients of relevant indicators of 3rd level, moreover $c1 + c2 + c3 + c4 + c5 = 1$

$$\langle ZY1\rangle = c1_1A1_1 + c1_2A1_2 + c1_3A1_3 + c1_4A1_4 + c1_5A1_5 = \sum_i \quad c1_iA1_i; i = \overline{1,5} \tag{65}$$

where $c1_1, c1_2, c1_3, c1_4, c1_5$ – weight coefficients of figures of 4th level for $A1_1, A1_2, A1_3, A1_4, A1_5, c1_1 + c1_2 + c1_3 + c1_4 + c1_5 = \sum_i \quad c1_i = 1;$

$$\langle ZY2\rangle = c2_1A2_1 + c2_2A2_2 + c2_3A2_3 + c2_4A2_4 + c2_5A2_5 = \sum_i \quad c2_iA2_i; i = \overline{1,5} \tag{66}$$

where $c2_1, c2_2, c2_3, c2_4, c2_5$ – weight coefficients of figures of 4th level for $A2_1, A2_2, A2_3, A2_4, A2_5, c2_1 + c2_2 + c2_3 + c2_4 + c2_5 = \sum_i \quad c2_i = 1;$

$$\langle ZY3\rangle = c3_1A3_1 + c3_2A3_2 + c3_3A3_3 + c3_4A3_4 + c3_5A3_5 + c3_6A3_6 = \sum_i \quad c3_iA3_i; i = \overline{1,6} \tag{67}$$

where $c3_1, c3_2, c3_3, c3_4, c3_5, c3_6,$ – weight coefficients of figures of 4th level for $A3_1, A3_2, A3_3, A3_4, A3_5, A3_6, c3_1 + c3_2 + c3_3 + c3_4 + c3_5 + c3_6 = \sum_i \quad c3_i = 1;$

$$\langle ZY4\rangle = c4_1A4_1 + c4_2A4_2 + c4_3A4_3 + c4_4A4_4 + c4_5A4_5 + c4_6A4_6 = \sum_i \quad c4_iA4_i; i = \overline{1,6} \tag{68}$$

where $c4_1, c4_2, c4_3, c4_4, c4_5, c4_6,$ – weight coefficients of figures of 4th level for $A4_1, A4_2, A4_3, A4_4, A4_5, A4_6, c4_1 + c4_2 + c4_3 + c4_4 + c4_5 + c4_6 = \sum_i \quad c4_i = 1;$

$$\langle ZY5\rangle = c5_1A5_1 + c5_2A5_2 + c5_3A5_3 = \sum_i \quad c5_iA5_i; i = \overline{1,3} \tag{69}$$

where $c5_1, c5_2, c5_3$ – weight coefficients of figures of 4th level for $A5_1, A5_2, A5_3, c5_1 + c5_2 + c5_3 = \sum_i \quad c5_i = 1;$

Impact on observability of threat/vulnerability pairs:

$$< C \geq d1\langle ZY1\rangle, d2\langle ZY2\rangle, d3\langle ZY3\rangle, d4\langle ZY4\rangle, d5\langle ZY5\rangle \tag{70}$$

where $d1, d2, d3, d4, d5$ – weight coefficients of relevant indicators of 3rd level, moreover $d1 + d2 + d3 + d4 + d5 = 1$

$$\langle ZY1\rangle = d1_1A1_1 + d1_2A1_2 + d1_3A1_3 + d1_4A1_4 + d1_5A1_5 = \sum_i \quad d1_iA1_i; i = \overline{1,5} \tag{71}$$

where $d1_1, d1_2, d1_3, d1_4, d1_5$ – weight coefficients of figures of 4th level for $A1_1, A1_2, A1_3, A1_4, A1_5, d1_1 + d1_2 + d1_3 + d1_4 + d1_5 = \sum_i \quad d1_i = 1;$

$$\langle ZY2\rangle = d2_1A2_1 + d2_2A2_2 + d2_3A2_3 + d2_4A2_4 + d2_5A2_5 = \sum_i \quad d2_iA2_i; i = \overline{1,5} \tag{72}$$

where $d2_1, d2_2, d2_3, d2_4, d2_5$ – weight coefficients of figures of 4th level for $A2_1, A2_2, A2_3, A2_4, A2_5, c2_1 + c2_2 + c2_3 + c2_4 + c2_5 = \sum_i \quad c2_i = 1;$

$$\langle ZY3\rangle = c3_1A3_1 + c3_2A3_2 + c3_3A3_3 + c3_4A3_4 + c3_5A3_5 + c3_6A3_6 = \sum_i \quad c3_iA3_i; i = \overline{1,6} \tag{73}$$

where $d3_1, d3_2, d3_3, d3_4, d3_5, d3_6$ – weight coefficients of figures of 4th level for $A3_1, A3_2, A3_3, A3_4, A3_5, A3_6, d3_1 + d3_2 + d3_3 + d3_4 + d3_5 + d3_6 = \sum_i \quad d3_i = 1;$

$$\langle ZY4\rangle = d4_1A4_1 + d4_2A4_2 + d4_3A4_3 + d4_4A4_4 + d4_5A4_5 + d4_6A4_6 = \sum_i \quad d4_iA4_i; i = \overline{1,6} \tag{74}$$

where $d4_1, d4_2, d4_3, d4_4, d4_5, d4_6$ – weight coefficients of figures of 4th level for $A4_1, A4_2, A4_3, A4_4, A4_5, A4_6, d4_1 + d4_2 + d4_3 + d4_4 + d4_5 + d4_6 = \sum_i \quad d4_i = 1;$

$$\langle ZY5\rangle = d5_1A5_1 + d5_2A5_2 + d5_3A5_3 = \sum_i \quad d5_iA5_i; i = \overline{1,3} \tag{75}$$

According to the formulas (43-47), (49-53), (55-59), (61-65), using the data of the lawyer's questionnaire, which regulates the values of indicators and their weight coefficients, the values of indicators of the 3rd level such as:$\langle ZY1\rangle; \langle ZY2\rangle; \langle ZY3\rangle; \langle ZY4\rangle; \langle ZY5\rangle$.

Using formulas (42), (48), (54) and (60) and the values of previously obtained indicators of the 3rd level, the values of complex indicators (categories) of the 2nd level are calculated, such as:

– impact on integrity$\left(G_1^{fakt}\right)$;

– impact on confidentiality$\left(G_2^{fakt}\right)$;

– impact on accessibility$\left(G_3^{fakt}\right)$;

– impact on observability$\left(G_4^{fakt}\right)$.

A comprehensive indicator of the state of budget security G_{zaxich}^{fakt} from the point of view of law can be calculated by the formula:

$$G_{sec}^{fakt\left(\sum_{i=1}^{n} \quad g_iG_i^{fakt}\right)} \tag{76}$$

where g_i – weigh coefficients of categories of the second level of the hierarchy G_i^{fakt}; n – the number of categories (in this case$n = 4$).

The decision on the ability of the public sector to withstand incidents was made on the basis of the following rule, empirically derived:

– if $90 \leq G_{sec}^{stan}$, then the state of budget protection from the risk of the implementation of threat/vulnerability pairs is considered high enough to maintain the safe functioning of objects of the state information structure;

– if $45 \leq G_{sec}^{stan}$, then the state of protection of the public sector from the risk of the implementation of threat/vulnerability pairs is considered acceptable to maintain the safe functioning of the information structure objects;

– ifG_{sec}^{stan}, then the state of protection of the public sector from the risk of the implementation of threat/vulnerability pairs is considered insufficient.

Conclusion

A procedure has been developed for the formation of many pairs of current threats to information security of the budget, the application of which allows, by direct (Cartesian) product of sets$X$ and Y, to determine the set of all possible combinations of threats and vulnerabilities, as well as more accurately describe the processes that violate the security of assets without losing time associated with the facts collection. A technology has been developed for assessing the state of security of information resources of budgets, the use of which, based on the prevailing set of threat-vulnerability pairs and the set of indicators (criteria) of existing threats characterising the possibility of violating confidentiality, integrity, accessibility and observability of information, allows to determine the security index of information resources and calculate the values of a complex indicator characterising the state of their security. The application of this method will enable legal departments of state control to obtain a numerical characteristic of a comprehensive indicator for assessing the level of security of the public sector in the ITC and decide on its compliance with specified requirements.

Notes

/1/ Mott, C.A., Skellern, D.J. (1987): Design of digital satellite communication links using interactive link budgeting software. *Journal of Electrical and Electronics Engineering, Australia*, 7(1), 36–44.

/2/ Wetherbe, J.C., Dickson, G.W. (1979): Zero-based budgeting: An alternative to chargeout systems. Information & Management, 2(5), 203–213. https://doi.org/10.1016/S0378-7206(79)80004-X

/3/ Martinez, J., Newsome, K. L., Sheble, M. A. (1998): Planning and budgeting the transition to a digital tomorrow. *Serials Librarian*, 34(3–4), 353–360. https://doi.org/10.1300/J123v34n03_15

/4/ Touchton, M., Wampler, B., Spada, P. (2019). The digital revolution and governance in Brazil: Evidence from participatory budgeting. *Journal of Information Technology and Politics*, 16(2), 154–168. https://doi.org/10.1080/19331681.2019.1613281

/5/ Khin, E.W.S. (2010): Comparative study of the budgeting process reforms within two international accounting organisations: Malaysia and Australia perspectives. *Australian Journal of Basic and Applied Sciences*, 4(9), 4142–4150.

/6/ Robinson, K.M. (2017): Can we afford that?: One library's transition to a data-rich acquisitions environment for e-resource budgeting and forecasting. *Technical Services Quarterly*, 34(3), 257–267. https://doi.org/10.1080/07317131.2017.1321377

/7/ Hudák, M. (2015): Sustainability of digital public spaces. *Quality Innovation Prosperity*, 19(1), 103–111. https://doi.org/10.12776/QIP.V19I1.381

/8/ Pozzebon, M., Cunha, M.A., Coelho, T.R. (2016): Making sense to decreasing citizen eParticipation through a social representation lens. *Information and Organization*, 26(3), 84–99. https://doi.org/10.1016/j.infoandorg.2016.07.002

/9/ Iasulaitis, S., Nebot, C.P., Da Silva, E.C., Sampaio, R.C. (2019): Interactivity and policy cycle within electronic participatory budgeting: A comparative analysis. *Revista de Administracao Publica*, 53(6), 1091–1115. https://doi.org/10.1590/0034-761220180272x

/10/ Stortone, S., De Cindio, F. (2015): Hybrid participatory budgeting: Local democratic practices in the digital era. *Citizen's Right to the Digital City: Urban Interfaces, Activism, and Placemaking*, 177–197. https://doi.org/10.1007/978-981-287-919-6_10

/11/ Breul, J.D. (2017): The growing use of performance information in the budget process in the United States: The convergence of performance budgeting and the digital transformation. In *Open to the Public: Evaluation in the Public Sector.* Available at: https://www.taylorfrancis.com/books/e/9781315125770/chapters/10.4324/9781315125770-11

/12/ von Fröhlich, S. (2013): The journey is its own reward! design and implementation of digital archive projects. *VOEB-Mitteilungen*, 66(1), 132–144.

/13/ Stortone, S., De Cindio, F. (2014): BiPart of participatory budgeting. A software platform for new political practices. *Innovation and the Public Sector*, 21, 30–39. https://doi.org/10.3233/978-1-61499-429-9-30

/14/ Halawa, M., Olcoń-Kubicka, M. (2018): Digital householding: calculating and moralizing domestic life through homemade spreadsheets. *Journal of Cultural Economy*, 11(6), 514–534. https://doi.org/10.1080/17530350.2018.1486728

/15/ Flint, E., du Plooy, S. (2018): Extending risk budgeting for market regimes and quantile factor models. *Journal of Investment Strategies*, 7(4), 51–74. https://doi.org/10.21314/JOIS.2018.103

/16/ Korachi, Z., Bounabat, B. (2019): Integrated methodological framework for digital transformation strategy building (IMFDS). *International Journal of Advanced Computer Science and Applications*, 10(12), 242–250.

/17/ Haugh, M., Iyengar, G., Song, I. (2017). A generalized risk budgeting approach to portfolio construction. *Journal of Computational Finance*, 21(2), 29–60. https://doi.org/10.21314/JCF.2017.329

/18/ Cunha, M.A.V.C.D., Coelho, T.R., Pozzebon, M. (2014): Internet and participation: The case of digital participatory budgeting in Belo Horizonte. *RAE Revista de Administracao de Empresas*, 54(3), 296–308. https://doi.org/10.1590/S0034-759020140305

/19/ Limao, J.P. (2018): Participatory budgeting in the regional press: A case study. *Estudos Em Comunicacao*, 2(26), 93–104. https://doi.org/10.20287/ec.n26.v2.a07