Incidents Correlation Mechanism for Assessing Average and Total Criticality Level of Situation in the Infosphere

Andrii Gizun [1] [0000-0002-2974-6987], Alexey Pisarchuk [1] [0000-0001-5271-0248],
Vladyslav Hriha [1] [0000-0002-1408-5805], Volodymyr Buriachok [2] [0000-0002-4055-1494]
and Rat Berdibayev [3] [0000-0002-8341-9645]

[1] National Aviation University, Kyiv, Ukraine
[2] Borys Grinchenko Kyiv University, Kyiv, Ukraine
[3] Almaty University of Power Engineering and Telecommunications, Almaty, Kazakhstan
andriy.gizun@gmail.com

Abstract. Today, the methods of incidents / potential crisis situations detecting and their criticality level assessing are proposed. However, these methods do not describe simultaneous occurrence of several crisis situations and determining of the average and total criticality level. In this paper the correlation issues of several events - security incidents – are reviewed and the mechanism for calculating an average and total criticality level of incidents is proposed. A mechanism basis of events correlation, as well as crisis management methods itself, includes Delphi methods and fuzzy logic model. Proposed mechanism appliance will allow the simultaneous occurrence of several incidents to be taken into account and assess their average and total impact on the information system.

Keywords: crisis situation, information security management, correlation, business continuity management concept, mechanism, criticality level, impact, fuzzy logic.

1. Introduction

The onrush of information technology (IT), along with an increase of communication and information processing capabilities, generates a significant increase in the number of incidents / potential crisis situations, which are described in international statistical reports and materials [1].

Crisis situations (CS) response problem in IT field is extremely important, though not yet sufficiently understood. Today, the role of crisis phenomena response systems in the process of managing and maintaining the enterprises viability, institutions and organizations of all ownership forms is constantly increasing. At the same time, protection not from catastrophic, but, more likely, emergency situations becomes more and more actual.

In [2-4] describes methods for detecting, identifying incidents / potential crisis situations (IPCSs), and assessing the incidents criticality level based on fuzzy logic and Delphi methods. Fuzzy logic methods for solving similar problems are also used

CybHyg-2019: International Workshop on Cyber Hygiene, Kyiv, Ukraine, November 30, 2019.

in [5]. Paper [6] describes the integrated model of IPCS representation. On the basis of these methods a computing complex [7], which implements IPCS control processes, is developed. In addition, it is worth noting that a system with a similar mechanism of work, described in [9].

However, these works do not take into account the simultaneous occurrence situation of several (two or more) IPCSs, their reconciling and determination of the average and total criticality level. Therefore, the main purpose of this article is to develop a mechanism for correlating information security incidents and to determine an average and total criticality level of their impact on information system using fuzzy logic methods.

2. Incidents correlation mechanisms, average and total criticality level determination

For the formalization of forecasting, detection, identification and assessing processes, we introduce the following set of IPCSs: $\mathbf{IKS} = \{\bigcup_{i=1}^{n} \mathbf{IKS_i}\} = \{\mathbf{IKS_1}, \ldots, \mathbf{IKS_n}\},\ (i = \overline{1,n})$, where n determines the number of potential i CS, in other words incidents. that can lead to a crisis state, each of which is represented as a generalized six-component tuple [6]: $\mathbf{IKS_i} = < IKS_i,\ \ \mathbf{P_i},\ \mathbf{T_i^e},\ \underset{\sim}{\mathbf{P}}_\mathbf{i}\mathbf{,}\ \mathbf{ER_i},\ LCS_i >$, in which: IKS_i – identifier of i -th IPCS, which is (or may become) the cause of CS occurrence; $\mathbf{P_i}$ – a subset of possible parameters used for forecasting or identification of i -th incident; $\mathbf{T_i^e}$ – a subset of all possible fuzzy (linguistic) standards that reflect the standard states of the corresponding parameters from the $\mathbf{P_i}$ subset; $\underset{\sim}{\mathbf{P}}_\mathbf{i}$ – a subset of the parameters current values for a certain period of time; $\mathbf{ER_i}$ – a subset of heuristic rules (similar to [8]) based on fuzzy parameters that are used to detect / identify the i -th IPCS; LCS_i – situation criticality level, caused by i -th IPCS.

A detailed description of the procedure for detecting, identifying the IPCS, is described in [3].

The revealed situation refers to the crisis one only if its criticality level is higher than average or bigger, that is $LCS_i \underset{\sim}{\geq} BC^e$. Otherwise, the incident either remains out of place (at a sufficiently low criticality level) or is responding to it in order to control and eliminate it as a normal information security incident.

Each incident is characterized by a criticality level that is given by a set $\mathbf{LCS} = \{\bigcup_{i=1}^{n} L\underset{\sim}{C}S_i\} = \{L\underset{\sim}{C}S_1, \ldots, L\underset{\sim}{C}S_n\},\ (i = \overline{1,n})$. Criticality level is determined by the parameters of a situation criticality assessing, taking into account their weight coefficients, that is $L\underset{\sim}{C}S_i = \sum_{e=1}^{E} (\Omega_e * \underset{\sim}{\mathrm{L}}_\mathrm{e})$. It is established that a criticality level can be described by taking into account the functional dependencies between $\underset{\sim}{\mathrm{L}}_\mathrm{e}$ –

parameters of criticality level assessing. A detailed method for criticality level assessing and the set of estimated parameters are described in [2].

The disadvantage of this model is a failure to take into account the mutual influence of incidents, which coincide in time, on the information system environment. Since one or another IPCS is characterized by a set of critical parameters that determine the degree of incident impact on the environment in a certain aspect, each one of IPCSs can increase the overall level of influence on the system depending on the magnitude of their correlation with each other. Thus, the correlation coefficient establishes dependency between different IPCSs and can reach values from 0 to 1. Moreover, IPCSs that have a homogeneous effect on the controlled environment have a correlation coefficient of 1, and IPCSs that affect the environment in various aspects and their interdependence is not manifested at all in the general criticality level determination, have the correlation coefficient value of 0. Therefore, correlated IPCSs increase the effect of each other's influence on the environment, which can be represented as the average and total criticality level with taking into account their interdependence, and not correlated IPCSs cause impact, the level of which can be assessed only separately for each incident.

Proceeding from these positions, we will propose application in the IPCS model and method for criticality level assessing of the correlation mechanism for a current situation. This mechanism is based on certain common criteria of criticality level for different IPCSs, additionally the higher the number of identical parameters is, the higher the correlation coefficient will be.

So each incident can be estimated by applying a general set of criticality level estimation parameters that are proposed in [2]. The number and composition of the characteristic parameters for each IPCS can have different values and is determined by the experts.

Mechanism itself has several stages, in particular:

1) Determination of the IPCS number, with which operations are performed, and sets of evaluative parameters for each of them.

2) Determination of the main and dependent IPCSs. In this case, write ordering of IPCSs set varies is in such a way that the main incident has the 1st number.

3) Determination of the correlation coefficients for each dependent and main IPCSs respectively.

Let’s consider each of these steps.

The main element of the integrated IPCSs representation model is an IKS_i identifier that binds a $\mathbf{IKS}$ set element to a specific incident, which is determined by its corresponding name. For example, if *n=5* we obtain $\mathbf{IKS} = \{\bigcup_{i=1}^{5} \mathbf{IKS_i}\} = \{\mathbf{IKS_1},\ \mathbf{IKS_2},\quad \mathbf{IKS_3},\ \mathbf{IKS_4},\ \mathbf{IKS_5}\} = \{\mathbf{A}, \mathbf{B}, \mathbf{C}, \mathbf{D}, \mathbf{E}\}$, where **A**,**B**,**C**,**D**,**E** – incidents names. Accordingly each of these incidents is characterized by its sets of evaluation parameters $\mathbf{L_i} = \bigcup_{i=1}^{N} \left\{ \bigcup_{e=1}^{E} \underset{\sim}{L}_e \right\} = \bigcup_{i=1}^{N} \{\underset{\sim}{L}_1, \underset{\sim}{L}_2, ..., \underset{\sim}{L}_E\},\ e = \overline{1, E}$, where E – number of parameters. For example, under conditions study for an incident **A** at E=15,

$$\mathbf{L}_{\mathbf{A}} = \left\{ \bigcup_{e=1}^{15} \underset{\sim}{L}_e \right\} = \{ \underset{\sim}{L}_1, \underset{\sim}{L}_2, \ldots, \underset{\sim}{L}_{15} \} = \{ TR,\ DVF,\ GS,\ OS,\ OLED,\ RD,\ RTLH,\ RM,\ F,\ DDI,\ CRT,\ CRP,\ LM,\ DIEPF,\ DVChS \}.$$

In order to determine dependency between IPCSs, we introduce two categories of events: the main and dependent incidents. There are two ways to allocate and assign the value of the main and dependent events, such as:

1) by time - the IPCS, which was detected first, acquires the status of the main while all the others - dependent IPCSs;

2) by the criticality level - the status of the main IPCS is assigned to the incident with the highest criticality level or selected by an expert or system operator, the user, based on the position of which CS aspects he considers the most threatening. For example, if human life is a priority, then IPCS that is most threatened in this aspect or criticality of information systems operation - IPCSs which interrupt these processes or reduce the quality of their provision, will be selected as the main one.

Of course, the 2nd method is more prioritized, since in that case there is no danger of ignoring the critical aspects of the IPCS influence on the controlled environment.

Correlation coefficient shows same aspects of the impact of different IPCSs and is determined by the number of common parameters between main and dependent events. Proposed mechanism is based on a consistently determined coefficient of correlation between the main and each dependent IPCSs using the formula

$$K_{IKS_{\text{осн}} IKS_{\text{зал}_i}} = \frac{|(\mathbf{L}_{\mathbf{осн}} \cap \mathbf{L}_{\mathbf{зал}_i})|}{|\mathbf{L}_{\mathbf{зал}_i}|}, \qquad (1)$$

until all dependencies between IPCSs are taken into account, and moreover $\mathbf{L}_{\mathbf{осн}}$ is a set of evaluation parameters of main IPCS and $\mathbf{L}_{\mathbf{зал}}$ is a set of estimation parameters of dependent IPCSs.

Next, let's unravel the problem of determining the average and total criticality levels for a set of detected IPCSs. Note that each of these procedures can be carried out both by taking into account the correlation between incidents and without it.

Thus, an average criticality level can characterize the situation formed from the point of view of its development in the time perspective, in particular for the formation of forecasts for longer development. To determine an average criticality level of a situation that arose from several simultaneous incidents influence we will use the following formulas:

- without taking into account a correlation coefficient

$$L\underset{\sim}{C}S_{\text{сер}} = \frac{1}{N} \sum_{i=1}^{N} L\underset{\sim}{C}S_i\ , \qquad (2)$$

where $L\underset{\sim}{C}S_{\text{сер}}$ is average criticality level of several IPCSs with taking into account a dependancy between them, $L\underset{\sim}{C}S_{\text{осн}}$ is criticality level of a main IPCS, $L\underset{\sim}{C}S_i$ - is criticality level of *i*-th IPCS, N - is total number of incidents.

- with taking into account a coefficient of correlation, which will allow to assess criticality level in a particular aspect of identified IPCSs manifestation

$$L\underset{\sim}{C}S^{K}_{\text{сер}} = \frac{1}{N} (L\underset{\sim}{C}S_{\text{осн}} + \sum_{i=2}^{N} K_{IKS_{\text{осн}} IKS_{\text{зал}_i}} * L\underset{\sim}{C}S_i)\ , \qquad (3)$$

where $L\underset{\sim}{C}S_{\text{сер}}$ is an average criticality level of several IPCSs with taking into account a dependency between them, $L\underset{\sim}{C}S_{\text{осн}}$ is criticality level of a main IPCS, $L\underset{\sim}{C}S_i$ - is criticality level of other (dependent) IPCSs and $K_{IKS_{\text{осн}}IKS_{\text{заг}_i}}$ is a correlation coefficient between a main and corresponding dependent IPCSs, N - is total number of incidents.

Schematically, the process of finding an average IPCS criticality level and a corresponding correlation coefficients is shown in Figure 1.

Total criticality level of the situation that arose as a result of a set of incidents impact is important for choosing the appropriate responses to them. This is due to the fact that countermeasures selected for only one IPCS will not be sufficient to neutralize a set of them, since each incident brings its part to a general growing level.

If criticality level of a single incident is estimated between 0 to 100 points, then the total amount is likely to exceed 100 points. This situation is unacceptable. Obviously, in this case, the definition of a total level can not be carried out by the banal addition of individual IPCSs criticality levels.

Let's use this Shortliffe formula, which is used to determine the degree of trust for two or more interconnected evidences in decision-making performed by expert systems. Having replaced the "measure of confidence" in it with "criticality level", we can use it for our problem.

We determine the formula for n-value of IPCS criticality level. So, for 2 IPCSs we will have $L\underset{\sim}{C}S_{12} = L\underset{\sim}{C}S_1 + L\underset{\sim}{C}S_2(1 - L\underset{\sim}{C}S_1)$ or because the formula is symmetric $L\underset{\sim}{C}S_{12} = L\underset{\sim}{C}S_2 + L\underset{\sim}{C}S_1(1 - L\underset{\sim}{C}S_2)$. For 3 IPCS - $L\underset{\sim}{C}S_{123} =$ $L\underset{\sim}{C}S_3 +$ $L\underset{\sim}{C}S_{12}$ $(1 - L\underset{\sim}{C}S_3)$. Substituting in the last expression an analytical records of finding $L\underset{\sim}{C}S_{12}$, and having carried out algebraic transformations we obtain an expression for the calculation of a total criticality level of 3 IPCSs

$$LCS_{123} = LCS_4 + +LCS_2(1 - LCS_3)(1 - L\underset{\sim}{C}S_4) + L\underset{\sim}{C}S_1(1 - L\underset{\sim}{C}S_2)(1 - L\underset{\sim}{C}S_3)(1 - L\underset{\sim}{C}S_4) .$$

By summarizing and systematizing we will formulate a formula for determining a total criticality level for n incidents (potential crisis situations) without a correlation between them

$$L\underset{\sim}{C}S_{\text{сум}} = L\underset{\sim}{C}S_N + \sum_{i=1}^{N-1} L\underset{\sim}{C}S_i \prod_{i=i+1}^{N} (1 - L\underset{\sim}{C}S_i) , \qquad (4)$$

where $L\underset{\sim}{C}S_{\text{сум}}$ - is total criticality level of several IPCSs without taking into account a dependency between them (correlation), $L\underset{\sim}{C}S_i$ is criticality level of *i*-th IPCS, N is total number of incidents.

Similarly to an average criticality level value we can apply mechanism of events correlation to the detected IPCSs. Then a criticality level, with taking into account a dependency between individual incidents in the aspect of their influence, is calculated by the formula

$$L\underset{\sim}{C}S^K_{\text{сум}} = L\underset{\sim}{C}S^K_N + \sum_{i=1}^{N-1} L\underset{\sim}{C}S^K_i \prod_{i=i+1}^{N} (1 - L\underset{\sim}{C}S^K_i) , \qquad (5)$$

where $L\underset{\sim}{C}S^K_{\text{сум}}$ is total criticality level of several IPCSs with taking into account a correlation between them, N is total number of incidents, $L\underset{\sim}{C}S^K_i =$ $K_{IKS_{\text{осн}}IKS_{\text{заг}_i}}$ *

$\underset{\sim}{LCS}_i$, $i = \overline{2,N}$ is criticality level of correlated *i*-th IPCS , $\underset{\sim}{LCS}_1^K = \underset{\sim}{LCS}_{\text{осн}}$, N is total number of incidents.

3. Experimental research of correlation mechanisms, average and total criticality level determination

Let’s consider the work of events correlation mechanisms and assessting of the situation total and average criticality levels, which was formed under the influence of several IPCSs in an example.

Let A, B, C, D and E be the identifiers of incidents, where A – Change of climatic conditions in the server, B – Network denial of service attack, C – Theft of equipment and media, D – Network hack by the violator, E – Flood. First, we need to define the sets of estimation parameters that correspond to each of them in order to detect a dependency between these IPCSs.

Thus the change of climatic conditions in the server is characterized by such a set of estimating parameters: $\mathbf{L_A} = \{\ TR - L_1; DVF - L_2; OS - L_4; OLED - L_5; DDI - L_{10}; CRT - \ L_{11}; CRP - L_{12}\ \}$. Similarly for a network denial of service attack: $\mathbf{L_B} = \{\ TR - L_1;\ DVF - L_2;\ OS - L_4;\ OLED - L_5;\ F - L_9;\ DDI - L_{10};\ CRT - L_{11}; CRP - L_{12};\ DVChS - L_{15}\ \}$. For stealing of equipment and media: $\mathbf{L_C} = \{\ DVF - L_2; OS - L_4;\ OLED - L_5;\ F - L_9;\ DDI - L_{10};\ DVChS - L_{15}\ \}$. Network hack by a violator is characterized by a set $\mathbf{L_D} = \{\ TR - L_1;\ DVF - L_2;\ OS - L_4;\ F - L_9; CRT - L_{11};\ CRP - L_{12}; DVChS - \ L_{15}\ \}$. And the last IPCS is a flood: $\mathbf{L_E} = \{\ TR - L_1; DVF - L_2;\ GS - L_3;\ OLED - L_5;\ RTLH - L_7;\ F - L_9;\ DDI - L_{10};\ RTLH - L_7; CRP - L_{12}\ \}$.

During the experimental research IPCSs were simulated and evaluated using the CSAS software [7] in a fuzzy and crisp form as shown in Table 1.

Table 1. IPCS assessment results

IPCS	Criticality level	FN
A	60 points or 0,6	0/0,4; 1/0,6; 0/0,8
B	80 points or 0,8	0/0,6; 1/0,8; 0/1
C	30 points or 0,3	0/0,1;1/0,3;0/0,5
D	40 points or 0,4	0/0,2; 1/0,4; 0/0,6
E	50 points or 0,5	0/0,3; 1/0,5; 0/0,7

Let’s assume that expert has selected a theft of equipment and media as the main IPCS, since the main emphasis in the organization's activities is to ensure the information confidentiality. Then $\underset{\sim}{LCS}_C = \underset{\sim}{LCS}_{\text{осн}} = \underset{\sim}{LCS}_1$, $\underset{\sim}{LCS}_A = \underset{\sim}{LCS}_{\text{зал}_2} = \underset{\sim}{LCS}_2$, $\underset{\sim}{LCS}_B = \underset{\sim}{LCS}_{\text{зал}_3} = \underset{\sim}{LCS}_3$, $\underset{\sim}{LCS}_D = \underset{\sim}{LCS}_{\text{зал}_4} = \underset{\sim}{LCS}_4$, $\underset{\sim}{LCS}_E = \underset{\sim}{LCS}_{\text{зал}_5} = \underset{\sim}{LCS}_5$.

Let’s calculate the correlation coefficients for the selected dependent events using the expression (1):

$K_{12} = K_{CA} = K_{IKS_{осн}IKS_{зал_2}} = \frac{|(\mathbf{L}_{\mathbf{осн}} \cap \mathbf{L}_{\mathbf{зал}_2})|}{|\mathbf{L}_{\mathbf{зал}_2}|} = \frac{|(\mathbf{L}_\mathbf{C} \cap \mathbf{L}_\mathbf{D})|}{|\mathbf{L}_\mathbf{D}|} = \frac{4}{7}$, $K_{13} = K_{CB} = K_{IKS_{осн}IKS_{зал_3}} = \frac{|(\mathbf{L}_\mathbf{C} \cap \mathbf{L}_\mathbf{B})|}{|\mathbf{L}_\mathbf{B}|} = \frac{6}{9} = \frac{2}{3}$, $K_{14} = K_{CD} = K_{IKS_{осн}IKS_{зал_4}} = \frac{|(\mathbf{L}_\mathbf{C} \cap \mathbf{L}_\mathbf{A})|}{|\mathbf{L}_\mathbf{A}|} = \frac{4}{7}$, $K_{15} = K_{CE} = K_{IKS_{осн}IKS_{зал_5}} = \frac{|(\mathbf{L}_\mathbf{C} \cap \mathbf{L}_\mathbf{E})|}{|\mathbf{L}_\mathbf{E}|} = \frac{3}{8}$.

Thus, all correlation coefficients for this set of 5 IPCSs are calculated.

Let’s calculate an average criticality level without taking into account the interdependencies between individual IPCSs, using the formula (2).

$\underset{\sim}{LCS}_{сер} = \frac{1}{5}(\underset{\sim}{LCS}_1 + \underset{\sim}{LCS}_2 + \underset{\sim}{LCS}_3 + \underset{\sim}{LCS}_4 + \underset{\sim}{LCS}_5) =$ (1/5) * ({0/0,1;1/0,3;0/0,5} + {0/0,2; 1/0,6; 0/0,8} + {0/0,6; 1/0,8; 0/1} + {0/0,2; 1/0,4; 0/0,6} + {0/0,3; 1/0,5; 0/0,7}) = (1/5)({0/0,3; 0/0,7; 0/0,9; 0/0,5; 1/0,9; 0/1,1; 0/0,7; 0/1,1; 0/1,3}+{0/0,6; 1/0,8; 0/1} + {0/0,2; 1/0,4; 0/0,6} + {0/0,3; 1/0,5; 0/0,7}) = (1/5)({0/0,7; 1/0,9; 0/1,1}+{0/0,6; 1/0,8; 0/1} + {0/0,2; 1/0,4; 0/0,6} + {0/0,3; 1/0,5; 0/0,7}) = (1/5)({0/1,3; 0/1,5; 0/1,7; 0/1,5; 1/1,7; 0/1,9; 0/1,7; 0/1,9; 0/2,1}+{0/0,2; 1/0,4; 0/0,6} + {0/0,3; 1/0,5; 0/0,7}) = (1/5)({0/1,5; 1/1,7; 0/1,9}+{0/0,2; 1/0,4; 0/0,6} + {0/0,3; 1/0,5; 0/0,7}) = (1/5)({0/1,5; 1/1,7; 0/1,9}+{0/0,2; 1/0,4; 0/0,6} + {0/0,3; 1/0,5; 0/0,7}) = (1/5)({0/1,7; 0/1,9; 0/2,1; 0/1,9; 1/2,1; 0/2,3; 0/2,1; 0/2,3; 0/2,5}+ {0/0,3; 1/0,5; 0/0,7}) = (1/5)({0/1,9; 1/2,1; 0/2,3}+ {0/0,3; 1/0,5; 0/0,7}) = (1/5)({0/2,2; 0/2,4; 0/2,6; 0/2,4; 1/2,6; 0/2,8; 0/2,6; 0/2,8; 0/3}) = (1/5)({0/2,4; 1/2,6; 0/2,8}) = {0/0,48; 1/0,52; 0/0,56} or after defuzzification $\underset{\sim}{LCS}_{сер} = 0{,}52$ or 52 points on a 100-point scale.

In order to determine the average value of criticality level for a particular aspect, it is usually necessary to apply a correlation mechanism on some particular most important characteristic. Since the system [7] allows us to present results in a fuzzy and crisp form, we will continue to make calculations to simplify computations using the instrument of ordinary (crisp arithmetic). Let’s determine an average criticality level of the current situation by the expression (3).

$\underset{\sim}{LCS}^{K}_{сер} = \frac{1}{5}(\underset{\sim}{LCS}_1 + \sum_{i=2}^{5} K_{IKS_{осн}IKS_{заг_i}} * \underset{\sim}{LCS}_i) =$ (1/5)* (0,3 + (4/7)*0,6) + (2/3)*0,8 + (4/7)*0,4 + (3/8)*0,5) = 0,32 or 32 points on a 100-point scale.

Let's analyze the correctness of a mechanism usage for determining a total criticality level of a situation depending on taking in account the mutual incidents correlation.

Let’s calculate a total criticality level without taking into account the interdependencies between individual IPCSs, using the formula (4).

$\underset{\sim}{LCS}_{сум} = \underset{\sim}{LCS}_5 + \sum_{i=1}^{4} \underset{\sim}{LCS}_i \prod_{i=i+1}^{5} (1 - \underset{\sim}{LCS}_i) =$ 0,5 + 0,3 ((1-0,6)(1-0,8)(1-0,4)(1-0,5)) + 0,6 ((1-0,8)(1-0,4)(1-0,5)) + 0,8((1-0,4)(1-0,5)) + 0,4 (1-0,5) = 0,5 + 0,0072 + 0,036 + 0,24 + 0,2 = 0,9832 or 98 points on a 100-point scale.

Let’s apply a mechanism of incidents correlation in order to determine a total criticality level of a situation as a result of their complex influence. Let’s determine a total criticality level of a current situation in terms of expression (5), and a correlation coefficients apply the same as in a previous example, and the input data from Table. 1 Accordingly $\underset{\sim}{LCS}_2^K = K_{12} * \underset{\sim}{LCS}_2$, $\underset{\sim}{LCS}_3^K = K_{13} * \underset{\sim}{LCS}_3$, $\underset{\sim}{LCS}_4^K = K_{14} * \underset{\sim}{LCS}_4$, $\underset{\sim}{LCS}_5^K = K_{15} * \underset{\sim}{LCS}_5$ i $\underset{\sim}{LCS}_1^K = \underset{\sim}{LCS}_1$.

Thus $\underset{\sim}{LCS}_{сум}^K = \underset{\sim}{LCS}_5^K + \sum_{i=1}^{4} \underset{\sim}{LCS}_i^K \prod_{i=i+1}^{5} (1 - \underset{\sim}{LCS}_i^K)$ = *(3/8)0,5 + 0,3((1-(4/7)0,6)(1-(2/3)0,8)(1-(4/7)0,4)(1-(3/8)0,5)) + (4/7)0,6 ((1-(2/3)0,8)(1-(4/7)0,4)(1-(3/8)0,5)) + (2/3)0,8((1-(4/7)0,4)(1-(3/8)0,5)) + (4/7)0,4(1-(3/8)0,5) = 0,1875 + 0,0577 + 0,1003 + 0,3343 + 0,1857 = 0,8655* or *87* points on a *100*-point scale.

As we can see, a total and average criticality level value with taking into account a correlation between incidents is lower than without taking into account, which is explained by the allocation of a specific aspect of impact assessment, under the experimental conditions - preserving the information resources confidentiality. Thus, the effect that generates a violation of other characteristics in these calculations is not taken into account.

To check a proposed mechanism adequacy, let's check the results correctness in output as a form of criticality levels input data of all detected incidents, which are 0 (minimum level) and 1 (maximum level) (Tab. 2).

Table 2. IPCS assessment results

IPCS	Criticality level minimum	Criticality level maximum
A	0	100 points or 1
B	0	100 points or 1
C	0	100 points or 1
D	0	100 points or 1
E	0	100 points or 1

Obviously when a criticality level of all IPCSs will be 0 points, then $\underset{\sim}{LCS}_{сер}$ = $\underset{\sim}{LCS}_{сер}^K = 0$ and $\underset{\sim}{LCS}_{сум}$ = $\underset{\sim}{LCS}_{сум}^K = 0$.

Let's consider the situation that arises under the incidents influence with criticality maximum. We calculate an average (by the formula (2)) and a total (by formula (4)) criticality level of the situation without taking into account correlation coefficients of incidents in this case:

$\underset{\sim}{LCS}_{сер} = \frac{1}{5}(\underset{\sim}{LCS}_1 + \underset{\sim}{LCS}_2 + \underset{\sim}{LCS}_3 + \underset{\sim}{LCS}_4 + \underset{\sim}{LCS}_5)$ = *1/5(1+1+1+1+1) = 1* or *100* points and $\underset{\sim}{LCS}_{сум} = \underset{\sim}{LCS}_5 + \sum_{i=1}^{4} \underset{\sim}{LCS}_i \prod_{i=2}^{5} (1 - \underset{\sim}{LCS}_i)$ = *1 + 1 ((1-1)(1-1)(1-1)(1-1)) + 1((1-1)(1-1)(1-1)) + 0,8((1-1)(1-1)) + 1(1-1) = 1* or *100* points..

Let's perform similar calculations with taking into account an incidents correlation interdependence according to formulas (3) and (5), respectively:

$\underset{\sim}{LCS}_{сер}^K = \frac{1}{5}(\underset{\sim}{LCS}_1 + \sum_{i=2}^{5} K_{IKS_{осн} IKS_{заг_i}} * \underset{\sim}{LCS}_i)$ = *(1/5)* (1 + (4/7)*1) + (2/3)*1 + (4/7)*1 + (3/8)*1) = 0,64* or *64* points on a *100*-point scale and

$\underset{\sim}{LCS}{}^{K}_{сум} = \underset{\sim}{LCS}{}^{K}_{5} + \sum_{i=1}^{4} \underset{\sim}{LCS}{}^{K}_{i} \prod_{i=2}^{5} (1 - \underset{\sim}{LCS}{}^{K}_{i})$ = *(3/8)* + *(1-(4/7))(1-(2/3))(1-(4/7))(1-(3/8))* + *(4/7)(1-(2/3))(1-(4/7))(1-(3/8))* + *(2/3)(1-(4/7))(1-(3/8))* + *(4/7)(1-(3/8))* = *0,375* + *0,038265* + *0,05102* + *0,178571* + *0,357143* = *1* or *100* points on a *100*-point scale.

As can be seen, the obtained results are quite correct and do not exceed the scope of admissible values $[0; \quad 1]$, which confirms the adequacy of developed mechanisms.

4. Conclusions

The proposed correlation mechanism, the main stages of which are: 1) selection of IPCS and estimating parameters sets from the general set which characterize their influence on the environment; 2) the choice of the main and dependent IPCSs, as well as the corresponding change in the incidents numbering in a system; 3) determination of the correlation coefficient of each dependent IPCSs with the main one, that determines the interdependence between them.

The obtained correlation coefficients can be used to calculate the average and total criticality levels of a situation that arose under the influence of several interrelated and simultaneous incidents (potential crisis situations). The basis of the mechanism, as well as in the methods of detection and evaluation of IPCSs, are methods of fuzzy logic and Delphi method.

The correlation coefficients determine the common impact features of each incident on the protected system or environment and are determined by comparing the criticality level assessment parameters of each IPCS.

The practical and scientific significance of this mechanism is the ability to evaluate the simultaneous impact of several IPCSs in a certain aspect on the state of the controlled environment.

In addition, the determination of the average criticality level will allow to assess the situation from the statistical point of view and make forecasts for its further development. A total criticality level allows to choose a countermeasures that is adequate to a level of risk. And the application of incidents correlation mechanism allows to calculate a situation criticality level in a specific aspect of information, national or other security [21-24].

References

1. Gizun, A., Hriha, V., Roshchuk, M., Yevchenko, Y., Hu, Z. (2019). “Method of informational and psychological influence evaluation in social networks based on fuzzy logic”. 4th International Scientific-Practical Conference Problems of Infocommunications Science and Technology. pp. 444-448.
2. A. Korchenko, V. Kozachok, A. Gizun, “Method of criticality level assessment for crisis management systems”, Ukrainian Information Security Research Journal, 2015, Vol. 17, №. 1, p. 86-98.

3. Pisarchuk, A. A., Bondarenko, Y. L., Melnik, A. L. (2008). “Method of forming optimum structure of direction finding network by nonlinear chart of compromises”. Journal of Automation and Information Sciences, № 40(5), pp. 68-79.
4. A. Gizun, V.Gnatyuk, N.Balyk, P. Falat, “Approaches to improve the activity of computer incident response teams”, Proceedings of the 2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2015, p. 442-447, 2015.
5. Manjunatha K.C., Mohana H.S, P.A Vijaya,"Implementation of Computer Vision Based Industrial Fire Safety Automation by Using Neuro-Fuzzy Algorithms", IJITCS, vol.7, no.4, pp.14-27, 2015. DOI: 10.5815/ijitcs.2015.04.02.
6. Hu, Z., Gizun, A., Gnatyuk, V., Kotelianets, V., & Zhyrova, T. (2017). “Method for rules set forming of cyber incidents extrapolation in network-centric monitoring”. 4th International Scientific-Practical Conference Problems of Infocommunications Science and Technology, PIC S and T. pp. 444-448.
7. A. Gizun, “Computer complex for detection and evaluation of crisis situations in information sphere”, Ukrainian Information Security Research Journal, Vol. 18, №. 1, p. 66-73, 2016.
8. Zaied, Abdel Nasser H., Samah Ibrahim Abdel Aal, and Mohamed Monir Hassan. "Rule-based expert systems for selecting information systems development methodologies." International Journal of Intelligent Systems and Applications 5.9 (2013): 19.
9. Qi Cheng, Lei Yu,”Operational Mechanism and Evaluation System for Emergency Logistics Risks ", IJISA, vol.2, no.2, pp. 25-32, 2010.
10. Layton, T. (2007). Information Security: Design, Implementation, Measurement, and Compliance. Boca Raton, FL: Auerbach publications
11. Coombs W.T. “Conceptualizing crisis communication Handbook of crisis and risk communication". New York : Routledge, 2009. P. 100 – 119.
12. Harris S. „CISSP Certification All–in–One Exam Guide". McGraw–Hill Osborne Media, 2010. 5th edition. 1216 p.
13. Killmeyer Jan. “Information Security Architecture: An Integrated Approach to Security in the Organization". Auerbach Publications, 2006. 424 p.
14. SEVA4A: An ontology for emergency notification systems accessibility / A. Malizia, T. Onorati, P. Dias [et al.], Expert systems with Applications. (2010). Vol. 37. Is. 4. pp. 3380 – 3391.
15. Weber P. “Complex system reliability modeling with Dynamic Object Oriented Bayesian Networks (DOOBN)", Reliability Engineering and System Safety. Volume 91. Issue 2. (2006). PP. 149-162.
16. Da Veiga A., Martins N. “Improving the information security culture through monitoring and implementation actions illustrated through a case study", Computers & Security. (2015). vol. 49. pp. 162-176.
17. Soomro Z. A., Shah M. H., Ahmed J. “Information security management needs more holistic approach: A literature review", International Journal of Information Management. (2016). vol. 36. №. 2. pp. 215-225.
18. Shameli-Sendi A., Aghababaei-Barzegar R., Cheriet M. “Taxonomy of information security risk assessment (ISRA)", Computers & Security. (2016). vol. 57.pp. 14-30.
19. Safa N. S. Information security conscious care behaviour formation in organizations. „Computers & Security", (2015). vol. 53. pp. 65-78.
20. de Gusmão, A. P. H., e Silva, L. C., Silva, M. M., Po- leto, T., & Costa, A. P. C. S. (2016). “Information security risk analysis model using fuzzy decision theory", International Journal of Information Management, 36(1), 25-34.

21. Gnatyuk S., Akhmetova J., Sydorenko V., Polishchuk Yu., Petryk V. Quantitative Evaluation Method for Mass Media Manipulative Influence on Public Opinion, CEUR Workshop Proceedings, Vol. 2362, pp. 71-83, 2019.
22. Fedushko, S., Ustyianovych, T., Gregus, M. (2020) Real-time high-load infrastructure transaction status output prediction using operational intelligence and big data technologies. Electronics (Switzerland), Volume 9, Issue 4, 668. DOI: 10.3390/electronics9040668
23. A. Peleschyshyn, T. Klynina, S. Gnatyuk, Legal Mechanism of Counteracting Information Aggression in Social Networks: from Theory to Practice, CEUR Workshop Proceedings, 2019, Vol. 2392, pp. 111-121.
24. S. Gnatyuk, M. Aleksander, P. Vorona, Yu. Polishchuk, J. Akhmetova, Network-centric Approach to Destructive Manipulative Influence Evaluation in Social Media, CEUR Workshop Proceedings, Vol. 2392, pp. 273-285, 2019.