Probabilistic criterion of information security management system development

© Volodymyr Mokhor[1][0000-0001-5419-9332], © Oleksandr Bakalynskyi[2][0000-0001-9712-2036], © Vasyl Tsurkan[3][0000-0003-1352-042X]

[1] Pukhov institute for modeling in energy engineering of National academy of sciences of Ukraine, Kyiv, Ukraine
[2] Department of formation and implementation of state policy on cyber protection of Administration of State serves of special communication and information protection of Ukraine, Kyiv, Ukraine
[3] Institute of special communication and information protection National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine
v.mokhor@gmail.com, baov@meta.ua, v.v.tsurkan@gmail.com

Abstract. The risk assessment presentation features of information security by the risk maps are considered. The attention is paid to special aspects of such a presentation. The established limit for discreteness and unevenness of changing the step the value of a risk. Using continuous risk maps is proposed to overcome the limit. This is due to income information security events with a continuous flow to consider the analogy information security management system with the queuing system. Therefore, the justification of continuous risk map is led to the probability of occurrence events with risk acceptance. For this, the concept and methods of geometric probability are used. Through this received "unit square" as a reflection of probabilistic geometry which is corresponding to the value normalized quantity of information security risk. The admissibility limit is represented by a hyperbola. With this in mind, use the continuous risk maps is justified.

Keywords: information security, risk, risk assessment, continuous risk map.

1 Introduction

Systemic, visual representation of information security risk assessments is carried out by using maps. Traditionally, they are represented by the coordinate plane whose axes are the risk parameters. For the most part, such parameters are the probability of the threat and the number of losses [1] - [6].

However, in practice, the use of maps is limited to their discreteness and unevenness of changing the step the values of risk [5], [6].

2 Justification for choosing a continuous risk map

Using continuous risk maps is proposed to overcome the limit [5]. Using continuous risk maps is proposed to overcome the limit. They are obtained by increasing the multiplicity of discrete risk maps. This transition is due to income information security events with a continuous flow to consider the analogy information security management system with the queueing system. That's why this process is the best to display by continuous risk maps. That's why effectiveness is confirmed by examples of applications in medicine [5], [7].

2.1 Establish analogies information security management system with the queuing system

To identify the most common analogies between the Information Security Management System (ISMS) and the well-known formal systems, consider the basic characteristics of the ISMS [8]. According to [1], the information security management system is "that part of the overall management system of an organization that is based on risk assessment. It, as part of the overall management system, creates implements, operates, monitors, revises, maintains and improves information security". From this definition, it follows that all and any ISMS can consider as a class of systems that is appropriate to repeatedly solve problems of the same type, in a certain sense.

This interpretation suggests an analogy between the ISMS and the queuing system (QS), in which the requirements for the work performed in the form of information security events.

We should also note that in general, the sequence of service requirements that have the type of information security events/risks is occasional both in terms of the occurrence of events/risks and the type of such events/risks. The occurrence of the sequence of events/risks served by the ISMS is another aspect of the analogy between the ISMS and the QS.

According to ISO/IEC 27001:2013, all information security events could be divided into separate groups depending on which clauses of Appendix A of the standard [2], [3] they are implemented. In particular, this may be, for example, events in the infrastructure of IT-organization, facts of the unauthorized crossing of the security perimeter, personnel problems, non-compliance with certain legislative norms, emergencies. Information security events fall into each of such separate groups is usually handled by specially trained teams of specialists, and sometimes by external organizations, including law enforcement agencies. Each of these certain teams can be considered as a certain channel for servicing information security events/risks, specializing in events/risks of a certain group, but, in principle, able to serve events/risks related to other groups. Thus, the presence of processing channels is traced, and this is the essence of another analogy between the ISMS and the QS.

Those information security events involve consequence represented by damage of a certain size H, the occurrence of which is associated with a certain probability p. At the same time, we've known that the combination of the amount of damage and the probability of its occurrence is a risk which is determined in the simplest case by the ratio

$$R = H \cdot p. \tag{1}$$

In this case, we can say that the ISMS is a QS, in which the requirements for the work performed in the form of information security risks, and the essence of the work performed is the maintenance of these risks following the recommendations of the ISO/IEC 27k series of standards [1], [2].

The service is understood in the sense that the ISMS assesses the level of resulting risks and processes such as them which assessment turns out to be higher than the specified threshold. All other events are documented, but the ISMS does not run into the processing state. In other words, the ISMS simply ignores such events. If in a case of a separated event, let's say zero security, we also consider the absence of any information security events, then it's obvious that such a zero, the event will be ignored in other words. Thus, we can state that the mechanism of risk management in the ISMS should handle all incoming risks, but it involves two non-overlapping classes of service states: processing and ignoring.

The specific number of analogies between the ISMS and the QS is enough to establish the possibility of interpreting the ISMS as the QS. Fundamentally ISMS may assess any risk and another analogy between the ISMS and the QS is appeared [8].

2.2 Evaluation of occurrence probability for acceptable risks

Based on the relation (1), we can form a trivial risk ranking criterion. But, besides, we can assume that based on the relation (1) and the concept of acceptable risk $R = R_0$, one can determine the probabilistic criterion and its value, set as a design requirement in the construction of the ISMS. For this, using the idea of an approach that called "risk maps" which allow "risk-owners" to set acceptable risk levels $R = R_0$ and divide all risks into acceptable and unacceptable by having the appropriate lines on the "risk maps". Such an approach is set out in [2], [4], where the risk map is presented as a two-dimensional table, whose cells at the intersections of the corresponding rows and columns contain the corresponding risk values. At the same time, the risk values are evaluated, for example, on a scale from 0 to 8.

However, it should be noted that the "risk maps" operate with single manifestations of events and do not take into account their possible repeated (multiple) manifestations. The accumulation of the consequences of a set of events, each of which falls into the zone of tolerable, can lead to damage higher than that associated with each of the components of a given level of risk, even without taking into account such phenomena as a provocation by one risk of occurrence other. All this leads to the realization that the level of acceptable risk of a single event cannot be used as a correct design requirement for the construction of an ISMS. In other words, the currently existing methods for constructing an ISMS cannot transform the acceptable risk level set by the owner into the correct formal requirements for building the ISMS. And even if such requirements are formally put forward, then there is no answer to the question of how to make sure that the ISMS, built on the basis of the requirement to ensure a given level of risk, ensures that this requirement is met.

From the thesis stated in the previous paragraph, the conclusion about the non-constructiveness of the project requirement for an ISMS based on the concept "ensure that the level of risk is not higher R_0". Based on established analogies between the ISMS and the QS [8], the correct design requirement should be formulated differently, namely this way [7]: the created ISMS should function as a queuing system that provides the processing of the flow of risk events from levels of risk $R \geq R_0$ and a given probability P_0 of occurrence of such events.

To substantiate the correctness of such a requirement, it is necessary to show the possibility of determining, by a given acceptable risk $R = R_0$, the magnitude of the probability P_0, with which the events associated with the risks occur $R \geq R_0$.

In other words, it is necessary to show the solvability of the following problem: for a given level of acceptable risk $R = R_0$, it is necessary to estimate the probability p_0 of an event with risks $R \geq R_0$. The dual setting of the same task: for a given level of acceptable risk $R = R_0$, estimate the probability p_1 with which events with risks $R < R_0$ may appear. It is obvious that

$$p_0 + p_1 = 1.$$

Probability estimation p_1 can be performed using the concept and methods of geometric probability [7], [8]. First of all, we introduce a two-dimensional Cartesian coordinate system, along the horizontal axis of which we will postpone the values of probabilities p, and along the vertical axis, the values of damage H. It is obvious that the values of probabilities vary in the range from $p = 0$ to $p = 1$, and the values of damage in the range from $H = 0$ to $H = H_{max}$. For uniformity of the range of change in the magnitude of damage with the range of variation of probabilities, we introduce into consideration the normalized amount of damage

$$h = \frac{H}{H_{max}}.$$

Then the normalized damage value will vary in the range from $h = 0$ at $(H = 0)$ to $h = 1$ at $H = H_{max}$.

In Cartesian coordinates (h0p) we define the "unit square" $OACE$ as the locus of points corresponding to any possible values of the normalized risk r:

$$r = h \cdot p, \tag{2}$$

where r is subject to the condition $0 \leq r \leq 1$ due to the fulfillment of the conditions

$$0 \leq h \leq 1$$

and

$$0 \leq p \leq 1$$

Since the length of each side of the square OACE is equal to one, then the square S_{OACE} of the square OACE is equal to one. We set the level of acceptable normalized risk

$$r = r_0.$$

Then from the relation (2) follows the functional dependence OACE

$$h = r_0 \cdot \frac{1}{p}, \tag{3}$$

the geometrical place of the points of the set of all risks is divided into two subsets (see Fig. 1): the figure OABDE determines the geometric location of the points of the set of risk values for which the expression $\mathrm{r} < \mathrm{r}_0$ holds, and the figure BCD defines the geometric location of the points of the set of risk values for which the ratio is satisfied $\mathrm{r} \geq \mathrm{r}_0$.

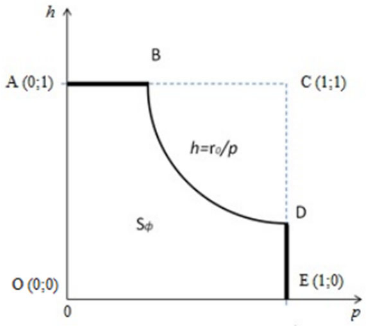


Fig. 1. Geometrical location of points of a set of risk values, divided by hyperbole $\mathrm{h} = (1/\mathrm{p})$

In this case, the probability p_1 that the value of an arbitrary normalized risk r will not exceed the value of a given standardized risk level $\mathrm{r} = \mathrm{r}_0$ is determined by the ratio of the figure area OABDE to the area of the "unit square"

$$\mathrm{p}_1 = \frac{\mathrm{S}_{\mathrm{OABDE}}}{\mathrm{S}_{\mathrm{OACE}}}, \tag{4}$$

where S_{OABDE} is the area of the figure OABDE, and $\mathrm{S}_{\mathrm{OACE}}$ is the area of the "unit square".

Since it was previously shown that $\mathrm{S}_{\mathrm{OACE}} = 1$, then relation (4) takes the form:

$$\mathrm{p}_1 = \mathrm{S}_{\mathrm{OABDE}}. \tag{5}$$

Thus, the probability p_1 that for an arbitrary risk the condition $\mathrm{R} > \mathrm{R}_0$ will be equal to the area OABDE of the figure. It remains to calculate the area of this figure (see Fig. 2)

$$\mathrm{S}_{\mathrm{OABDE}} = \mathrm{S}_1 + \mathrm{S}_1 \tag{6}$$

The area S_1 is calculated as the area of the rectangle with the sides OA and AB. The length of the side OA, as previously stipulated, is equal to 1. And the length of the side AB is determined by the numerical value of the probability coordinate of the point B. The point B is the point of intersection of the line $\mathrm{b} = 1$ with the hyperbola, defined by the relation (3). Then the numerical value of the probabilistic coordinate of a point B can be determined by substituting the value $\mathrm{h} = 1$ in the left side of relation (3):

$$1 = \mathrm{r}_0 \cdot \frac{1}{\mathrm{p}}.$$

From this relation, it follows that the numerical value of the probability coordinate $\mathrm{p} = \mathrm{p}_0$ of a point B is $\mathrm{p}_0 = \mathrm{r}_0$.

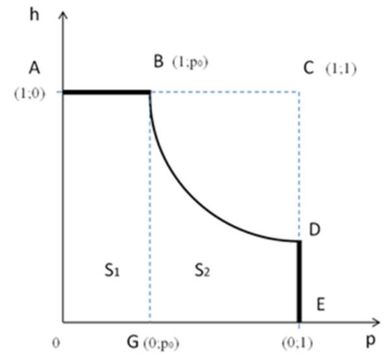


Fig. 2. Splitting a figure OABDE into two figures: a rectangle OABG and a figure GBDE

Then the area $\mathrm{S_1}$ can be expressed by the following relationship:

$$\mathrm{S_1 = 1 \cdot r_0 = r_0}. \quad (7)$$

The area $\mathrm{S_2}$ of the second figure GBDE, which is formed by a hyperbola, defined by the relation (3) and three straight lines: $\mathrm{h = 0}$, $\mathrm{p = p_0 = r_0}$ and $\mathrm{p = 1}$, is calculated as a definite integral using the following formula:

$$\mathrm{S_2} = \int_{\mathrm{r_0}}^{1} \frac{\mathrm{r_0}}{\mathrm{p}} \mathrm{dp} = \mathrm{r_0} \int_{\mathrm{r_0}}^{1} \frac{1}{\mathrm{p}} \mathrm{dp} = \mathrm{r_0} \ln \mathrm{p}|_{\mathrm{r_0}}^{1} = \mathrm{r_0}(\ln 1 - \ln \mathrm{r_0}).$$

Since $\ln 1 = 0$ the formula for calculating the area $\mathrm{S_2}$ takes the following form:

$$\mathrm{S_2} = \mathrm{r_0}(\ln 1 - \ln \mathrm{r_0}) = -\mathrm{r_0} \ln \mathrm{r_0}. \quad (8)$$

Then, to calculate the area of the figure OABDE, we substitute the values (7) and (8) into (6) and get:

$$\mathrm{S_{OABDE}} = \mathrm{S_1} + \mathrm{S_2} = \mathrm{r_0} - \mathrm{r_0} \ln \mathrm{r_0} = \mathrm{r_0}(1 - \ln \mathrm{r_0}). \quad (9)$$

So, taking into account (5), a formula is obtained for estimating the probability $\mathrm{p_1}$ that the normalized values of the magnitude of possible risks will not exceed the specified magnitude of the acceptable risk $\mathrm{r_0}$ (see Fig. 3):

$$\mathrm{p_1} = \mathrm{r_0}(1 - \ln \mathrm{r_0})$$

$$p_1 = r_0(1 + ln\, r_0^{-1}). \quad (10)$$

Looking at the price, there is a list of non-valid cards for the presentation of some risks and information.

2.3 Using continuous risk map in information security

Information security events are sent to the ISMS as a continuous stream according to the analogy of ISMS and QS. That's why this process is the best to image using a continuous risk map. Due to this was chosen to use the Cartesian coordinate system with probability values and losses in the ranges from 0 to 1 to reflect such an idea. As a result, the risk values are within the "unit square" (see Fig. 1), which is created after postponing the maximum value of probability and losses.

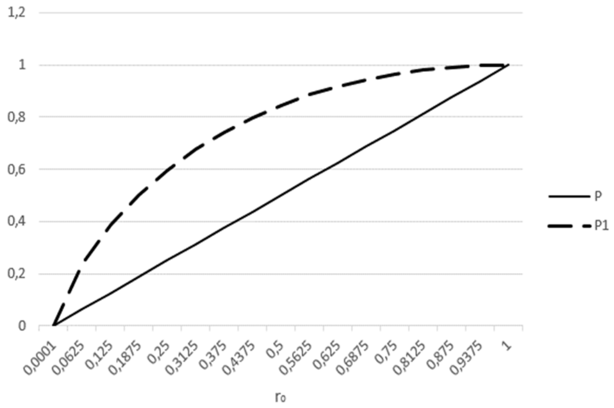


Fig. 3. Position of $p_1 = r_0(1 + \ln(r_0^{-1}))$ function graph relative to the $p = r_0$ function graph

When we are using the usual discrete risk maps, an attempt to reduce the uncertainty of the "distances" between two neighboring risks leads to an increase in the multiplicity of the risk map. Increasing the multiplicity of a discrete card leads to a big amount of unacceptable information security risks when it is developing ISMS. It is difficult to take into account the discreteness of information security risk assessments. Therefore, this restriction is overcome by the use of continuous cards, which are used, for example, in medicine (see Fig. 4) [5], [9].

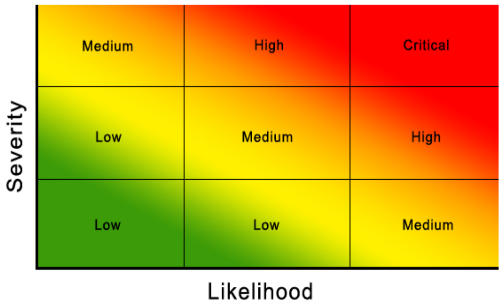
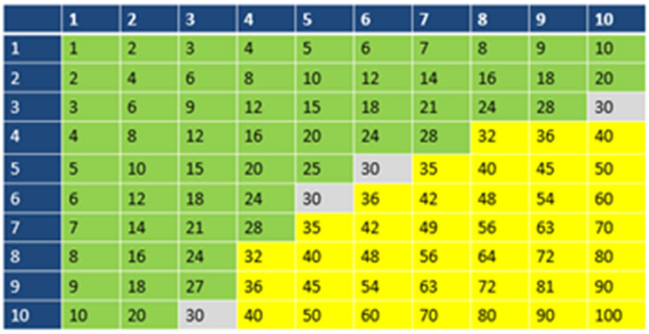


Fig. 4. Type of continuous risk maps

Consider the example (see Fig. 5) to meet the requirement "Take into account all risks between 28 and 32" for nxn maps. For convenience, the values of risks that are less than and equal to 28 are green, the values that are 32 and above are yellow.

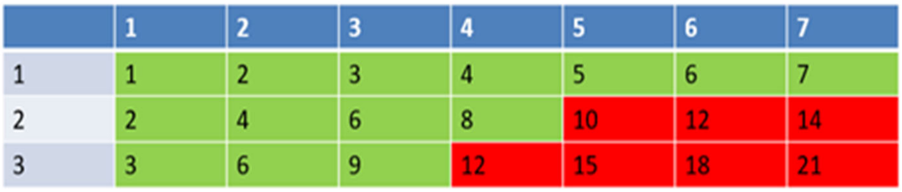
Considering to Fig. 5, it is appropriate to refer four cases corresponding to level "30". But, it is not clear what to do when the risk should be 31? And in the given range from 28 to 32 there are three integers (29, 30, 31), how to take them into account? This problem also has no solution, because, as it was noted, an attempt to increase the table dimension will lead to unjustified time consumption or risk assessment errors [5], [6].



	1	2	3	4	5	6	7	8	9	10
1	1	2	3	4	5	6	7	8	9	10
2	2	4	6	8	10	12	14	16	18	20
3	3	6	9	12	15	18	21	24	28	30
4	4	8	12	16	20	24	28	32	36	40
5	5	10	15	20	25	30	35	40	45	50
6	6	12	18	24	30	36	42	48	54	60
7	7	14	21	28	35	42	49	56	63	70
8	8	16	24	32	40	48	56	64	72	80
9	9	18	27	36	45	54	63	72	81	90
10	10	20	30	40	50	60	70	80	90	100

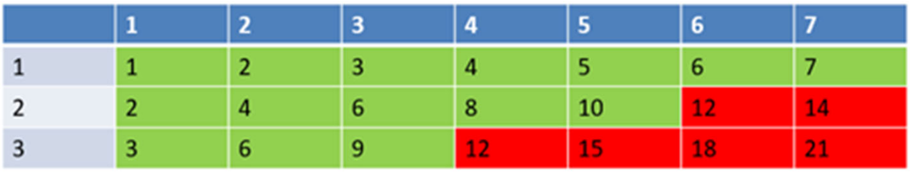
Fig. 5. Take into account all the risks between 28 and 32

In the case of using multi-dimensional "risk maps", we will increase the level of maximum acceptable risk in each following option. For this purpose, we will use the analogy with the previous example and get such values: 1, 3, 9. In Fig. 6 - 9, give an example of defining risks that are greater than "9", "10", "12", "14" [5], [6], [9].



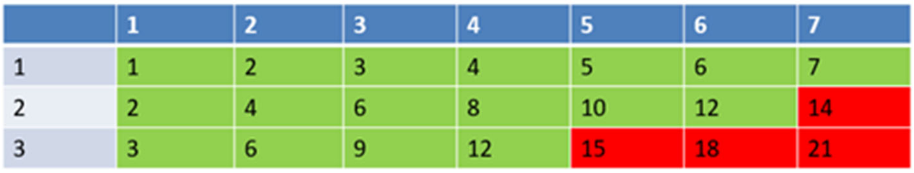
	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7
2	2	4	6	8	10	12	14
3	3	6	9	12	15	18	21

Fig. 6. Requirement: Take into account risks above level "9"



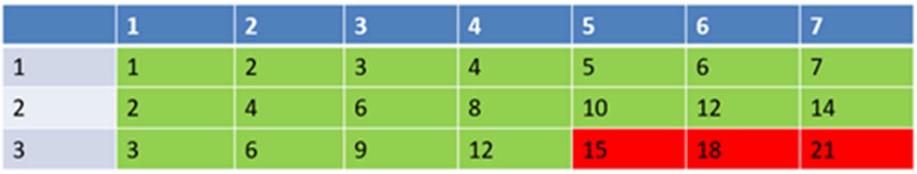
	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7
2	2	4	6	8	10	12	14
3	3	6	9	12	15	18	21

Fig. 7. Requirement: Take into account risks above level "10"



	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7
2	2	4	6	8	10	12	14
3	3	6	9	12	15	18	21

Fig. 8. Requirement: Take into account risks above level "12"



	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7
2	2	4	6	8	10	12	14
3	3	6	9	12	15	18	21

Fig. 9. Requirement: Take into account risks above level "12"

However, to set the levels of acceptable risks, the principle of the task must be changed. For example, the most acceptable risk is each following number, in ascending order, which follows the previous one in table (see Fig. 7-9) – 10, 12, 14. Therefore, in applying this approach, it is necessary to look at all possible options for the magnitude of the risks. First, the value of the acceptable risk for the specific iteration is searched for, and then it is compared with other values. As a result, many unacceptable risks are identified and taken into account when developing an information security management system.

Thus, using risk maps like nxm creates even more difficulties than for equal in size maps. For example, pay attention to Fig. 10 [5]. On the abscissa axis there is a probability value in percent, and on the ordinate axis - probable losses expressed in millions of UAH. Curves on maps distinguish between different risk categories, but how 100% and 16000 are related is not clear. At the same time, the question arises about the possibility of comparing them and the type of curves.

To avoid these difficulties, the risk parameter values are usually normalized. For this purpose, it is necessary to present probability and damage in the same units. For example, if threat realization probability can range from 1% to 100%, it is also advisable to estimate the losses in the same units. Then for example Fig. 10, the value of 100 conventional units is 16,000 million dollars. Thus, one conventional unit is equal to 160 million dollars. The maximum risk value is 100. This approach allows bringing the nxm map to the nxn dimensional map. It is also understood that after obtaining the results of the risk assessment carried out in the normalized values, it is necessary to perform the inverse conversion [5], [9].

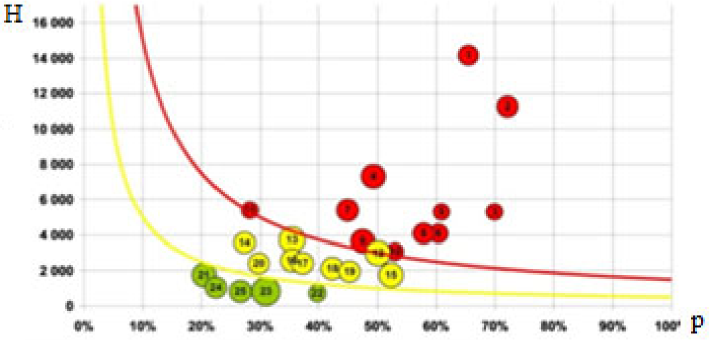


Fig. 10. Example of a multi-dimensional risk map

3 Conclusion

The justification of the continuous risk map is led to the probability of occurrence events with risk acceptance. For this, firstly we establish analogies information security management system with the mass service system; secondly: the concept and methods of geometric probability are used. Particularly, it is introduced a two-dimensional Cartesian coordinate system on which the value of the probability of threat implementation is plotted on the horizontal axis, and the value of the loss is on vertical. The consistency of the change in the value of both ranges is achieved by normalizing the value of the losses. Thanks to this, in the Cartesian coordinate system a “unit square” is obtained. The geometric locus is imaged by this figure which corresponds to the probable value of the normalized value of the risk of information security. By assigning an acceptable value to it the division of the set of risks into a subject of accepted and unacceptable. The admissibility limit is represented by a hyperbola.

It is allowed to income the limit for discreteness and unevenness the value of risk on the map and as a consequence, justifies to use of continuous risk information security maps.

References

1. International Organization for Standardization. (2018, February 07). ISO/IEC 27000. Information technology. Security techniques. Information security management systems. Overview and vocabulary, https://www.iso.org/standard/73906.html, last accessed 2019/09/12.
2. International Organization for Standardization. (2013, Oktober 01). ISO/IEC 27001. Information technology. Security techniques. Information security risk management. Requirements, https://www.iso.org/standard/54534.html, last accessed 2019/09/12.
3. International Organization for Standardization. (2013, Oktober 01). ISO/IEC 27002. Information technology. Security techniques. Code of practice for information security controls, https://www.iso.org/standard/54533.html, last accessed 2019/09/12.
4. International Organization for Standardization. (2018, July 9). ISO/IEC 27005. Information technology. Security techniques. Information security risk management, https://www.iso.org/standard/75281.html, last accessed 2019/09/12.
5. Mokhor, V., Bakalynskyi, O., Tsurkan, V.: Risk assessment presentation of information security by the risks map. Information Technology and Security, vol. 6, iss. 2, 94–104 (2018), doi: 10.20535/2411-1031.2018.6.2.153494, last accessed 2019/09/12.
6. Astakhov, A.: Art of information risk management [Isskustvo upravleniia informatsionnymi riskami]. DMK Press. Moskow (2010).
7. Mokhor, V., Bogdanov, A., Bakalinskii, A., Tsurkan, V.: The Method of the Design Requirements Formation for Information Security Management System, Selected Papers of the XVI International Scientific and Practical Conference “Information Technologies and Security”. Kyiv, 2016, pp. 1-6, http://ceur-ws.org/Vol-1813/paper7.pdf, last accessed 2019/09/12.
8. Mokhor, V., Bakalynskyi, O., Bohdanov, O., Tsurkan, V.: Descriptive analysis of analogies between information security management and queuing systems. Zahist ìnformacìï. vol. 19, № 2, 119–126 (2017).
9. Petrenko S. A., Simonov S. V.: Information risk management. Cost-effective security., DMK Press, Moskow (2004).