UDC 681.3.06

**A.V. POTIY[1], D.Y. PILIPENKO[2], I.N. REBRIY[1]**

*[1]Kozhedub Air Force University, Kharkiv*
*[2]Kharkiv national University of Radioelectronics, Kharkiv*

# THE PREREQUISITES OF INFORMATION SECURITY CULTURE DEVELOPMENT AND AN APPROACH TO COMPLEX EVALUATION OF ITS LEVEL

*The problems of Information Security Culture promotion are more and more recognized by researchers working in the field of Information Security. ISC can be considered as an essential component of Information Security Management systems today. The prerequisites to development of Information Security Culture are investigated in this paper. The main factors that affect Information Security Culture are discussed, namely attitude to IS requirements, standards of behavior and normative beliefs. An approach to complex qualitative evaluation of ISC using convolution matrices is proposed.*

***Keywords:*** *information security culture, information security requirements, evaluation, convolution matrix.*

## Introduction

Obviously more and more organizations develop a much deeper understanding of the relationship between Information Security (IS) and dominant business goals [1]. A wide range of ready-made software, firmware and hardware IS solutions enables the reduction of IS incidents, which are mainly caused by external threats. At the same time the quantity of internal threats usually caused by human factor has increased in number.

IS incidents occur not only due to deficiency or inadequacy of IS policies, practices or procedures. Non-compliance is often the reason. IS requirements are usually considered by organization members to be limitations and obstacles preventing them from day-to-day activities. Poor understanding of IS function and its goals also leads to low subjective perception of risk, which in-turn leads to negligence. The lack of positive attitude towards IS requirements results in promotion of poor Information Security Culture (ISC). IS policies, practices and procedures can lose their efficacy considerably without high quality ISC promoted.

It's essential to note that a set of guidelines towards development of ISC was released by Organization for Economic Co-operation and Development (OECD) in 2002 [2]. This document aims to address security issues via promotion of ISC. These Guidelines include nine complementary principles, which should be read as a whole: Awareness, Responsibility, Response, Ethics, Democracy, Risk assessment, Security design and implementation, Security management, Reassessment. The principles listed above concern every participant in both strategic and operational dimensions.

Investigation of factors that develop positive attitude towards IS requirements, prerequisites to ISC development and design of complex method of assessment is thus considered to be a matter of great interest in the field of Information Security.

## 1. The development of attitude towards IS requirements

The investigation of human factors in the field of Information Security increasingly draws attention of researchers. According to the survey presented in [3], the majority of employees are quite confident that responsibility for integrity of information assets rests solely on IS staff, and their major task consists of eliminating mistakes and IS incidents aftereffects. As an example, the author mentions an organization, whose Service of Infosecurity carried out an awareness campaign (on their own initiative) via corporate e-mail. The main goal of this delivery was to make employees aware of IS functions and to inform them about the changes in IS policy. This initiative was unsuccessful, since the majority of employees deleted the messages without reading them due to low quality ISC. At the same time, the survey of Service of Infosecurity staff revealed that the main cause of IS incidents is regular non-compliance to IS requirements and single system failures. In other words, organizations still suffer from casual or intentional employee errors despite the presence of valid IS policies and technologies.

There are two possible solutions to the issue of non-compliance to IS requirements:

1. The first one is to implement a strict inspection system, which also defines system of penalty fines and disciplinary actions in case of non-compliance. This solution is capable of producing quick results, though its negative perception by employees makes its effect non-

durable. Apart from this shortcoming, continuous supervision inevitably leads to the growth of expenditures, which can be completely unsuitable for small organizations.

2. The other solution is to develop a high level of ISC. Though this option is rather long-term result oriented, it promises a long-lasting effect in case of success.

ISC is incentive in its nature, since it consists of standards of behavior and behavioral patterns established in an organization. Still, the first step toward the development of ISC is the presence of positive employee *attitude* towards the goals of IS and its role in organization's activities. First of all, let us understand the meaning of the term "Attitude". An attitude is liability of individual to a certain course of action in a particular situation. Speaking of IS, an attitude can be positive in case of compliance to IS requirements, or negative otherwise. An attitude can be represented as a ternary structure, composed of affective, cognitive and behavioral components [4].

***Affective component*** is usually referred to some phenomenon, event or particular person within an organization. That's the way of human to evaluate objects and phenomena around him and to create a perceptive image. This image contributes to the development of ISC and consolidates an overall attitude as well. For example, recognition of supervisor's authority or subjective importance of sensitive information can be considered as affective component. Employee prejudice will inevitably influence an attitude in negative way.

***Cognitive component*** represents the knowledge about some object towards which an attitude is formed. The resultant belief will greatly influence an attitude depending on the accuracy of underlying knowledge. Cognitive component (unlike affective component) does not have strongly pronounced emotional character. This means it's possible to change cognitive component via rational evidence. For example, basic IS training can lead to awareness and competence growth, which by-turn reduces the probability of IS incidents caused by the lack of basic knowledge.

***Behavioral component*** defines the aptitude of individual to act in a certain way. This component contributes the most, since its activity nature, and due to the influence of the other components. For example, a negative experience of personal involvement in IS incident can make an employee realize the importance of IS. This also develops a new knowledge, which improves awareness and makes employee perform their routines in more secure manner.

Though employee awareness and competence (cognitive component) are crucial in terms of IS requirements compliance, it gives no guarantee of stability in this behavior. An employee should possess an intention (behavioral component) apart from basic knowledge to comply with IS requirements and perform daily routines in secure manner [5]. The value of circulating information is quite dissimilar for individual employee or organization department. If employee behaves as rational egoist, then they put as much effort to protect information as is their subjective estimate of the value of this information [6]. Thus both knowledge and correct behavioral choice equally affect the compliance of IS requirements. IS policies, practices and procedures can be considered effective only in case they are followed in real-life, in operational dimension particularly.

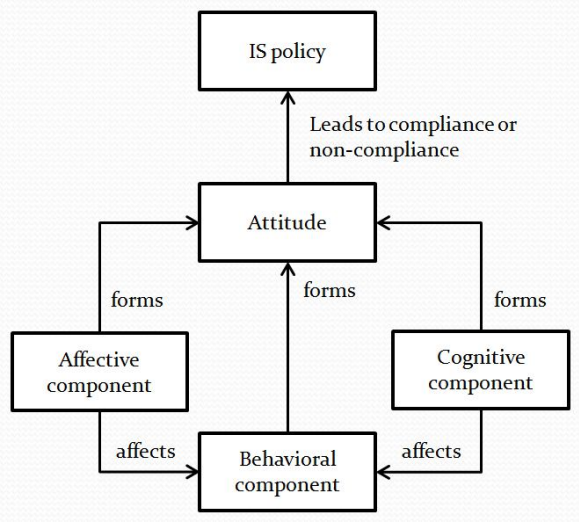



Fig. 1. The development of attitude towards IS requirements

This problem raises an obvious question – which factors influence the mentioned above components and the intention to perform daily activities in secure manner. Many researchers agree that even adequate IS policy is not enough to guarantee the absence of IS incidents, caused by employees [5, 7]. Another survey of organizations revealed that utmost correspondence between the formal IS policy and day-to-day activities showed organizations, whose management addressed the issues of ISC promotion [8]. The desired standards of behavior were stated by management, so their regard for such issues served as a straightforward signal of the importance of ISC.

## 2. Information Security Culture

It is essential to note that no common definition of Information Security Culture is used today. And a certain number of variations in the definition and interpretations of the "Information Security Culture" term among different researchers exist as well [3, 5, 7]. Summarizing different definitions we can say that *ISC is a set of values, human beliefs, opinions and behavioral patterns, that provide a certain degree of compliance*

*with IS requirements in an organization*. According to Organizational Behavior Theory each member of an organization from CEO to average executive possess a set of needs, expectations and desires, as well as beliefs, principles and opinions towards some object [9]. So it is fallacious to suggest the total absence of ISC in an organization. On the contrary, ISC is always present in certain degree with inevitable positive or negative impact on an organization. As an example, we can analyze a hypothetical organization with IS requirements compliance issues. In a rough approximation we can suggest that such ISC is rather ineffective and impacts organization in a negative way.

Drawing a line between acceptable and inadmissible behavior, ISC demarcates employee standards of behavior. There is a straightforward relation between behavioral choice and knowledge of an employee, which is represented in Fig. 2.

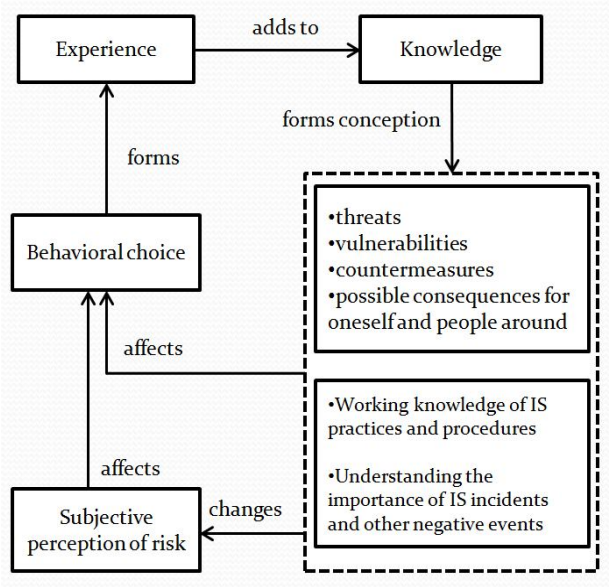



Fig. 2. Relation between behavioral choice and knowledge

As mentioned above, neither basic knowledge, nor behavioral choice can solely establish a high level of ISC. Even an advanced repertoire of knowledge cannot guarantee the possession of desire or intention to perform one's duties in secure manner. By the same token, it is a nontrivial task to change ISC using only behavioral component without proper knowledge. As shown in Fig. 2, a competent employee possesses a clear idea of IS threats and vulnerabilities; understands a probable consequence of IS incidents against himself, his colleagues and the whole organization. A repertoire of knowledge can be developed via learning or in practice, as a form of experience. A more sound understanding IS functions and goals can affect behavioral component of an employee, which facilitates the compliance of IS requirements. At the same time the growth of knowledge affects the subjective perception of risk. Without adequate knowledge base an employee is unable of objective risk assessment, which leads to negligence. Performing certain actions an employee acquires experience and consolidates ISC as well, since typical behavior transforms into standard, normal behavior over time. There are some other factors that affect behavioral choice, namely normative beliefs and established standards of behavior. The following fig. represents the relation between these factors:

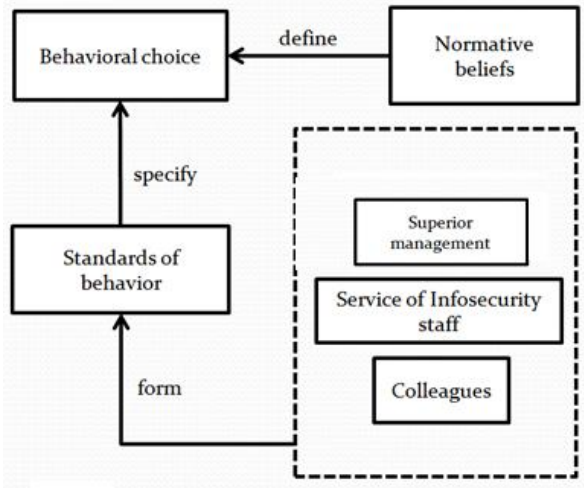



Fig. 3. The influence of normative beliefs and standards of behavior in behavioral choice

*Normative belief* is an individual's perception about the importance of the judgment by significant other of his particular behavior. *Standards of behavior* are established by typical behavior of colleagues, supervisor and Service of Infosecurity staff, etc. In other words, if there's a rule that states the performance of day-to-day activities in secure manner, it works as a signal, that indicates the necessity of IS requirements compliance.

The new employees find themselves in the phase of adaptation and are guided by established standards of behavior at first, gradually adopting the way that community behaves itself. Employees' activity is thus regulated through acceptance of organizational culture. However a certain paradox should be mentioned: while regulating activities, ISC itself can be considered as a product of personnel activity. If the process of ISC promotion is carried out spontaneously, this makes the standards of behavior become more profound (without conscious control). This fact means a negative effect in case of low quality ISC. An employee develops an idea of acceptable and improper behavior during the process of socialization. The process mentioned helps an employee to adopt the established patterns of behavior, values and standards of an organization (regardless of their compliance to IS requirements). The socialization

process in case of using a proper approach can be a powerful tool of creating desirable compliance. This process effectively facilitates enhancement of ISC in case of superior management support. Fig. 4 represents how superior management, employees and the present ISC affect this process.

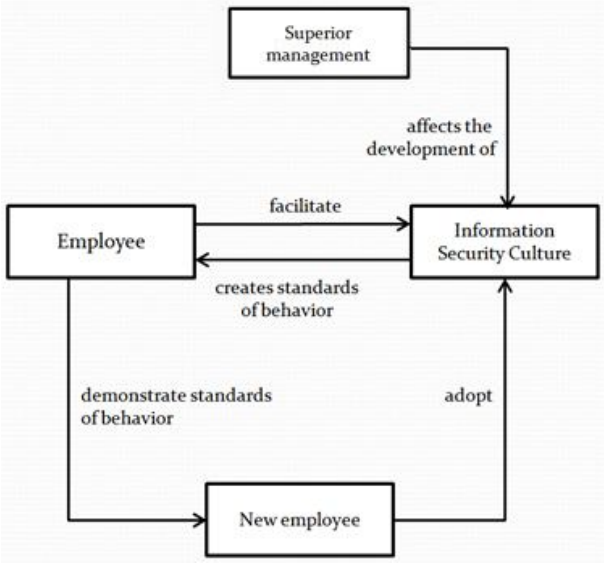



Fig. 4. The process of socialization

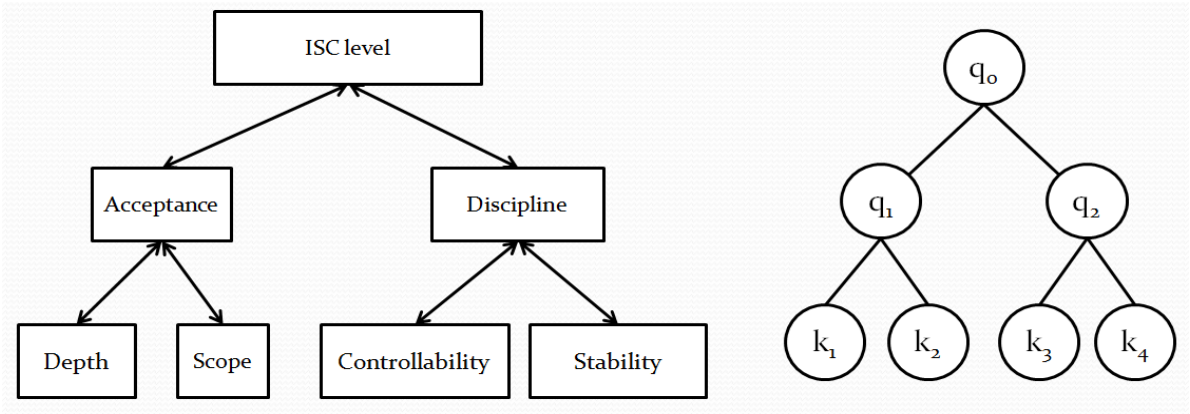
## 3. A method of complex evaluation of ISC

In spite of a certain interest to this problem, there has not yet been proposed a method of qualitative or quantitative evaluation of ISC in whole.

We suggest applying one of the methods of complex evaluation, which enables convolution of several indicators to an integrated one for system description.

Let the final result of evaluation be an integrated indicator "ISC level", which in turn is defined by local indicators of "Acceptance" and "Discipline". The "Acceptance" indicator is defined by lower indicators of "Depth" and "Scope". The "Discipline" indicator is similarly defined by lower level indicators of "Controllability" and "Stability". Thus we get the goal tree presented in Fig. 5 a. In general, this tree-based structure can be described by the block diagram presented in Fig. 5, b.

The value of node $q_0$ is defined by aggregating of local indicators $q_1$ and $q_2$. The nodes $q_1$ and $q_2$ represent the aggregated values of lower level indicators $(k_1, k_2)$ and $(k_3, k_4)$ respectively. The mentioned diagram is stated by the following dichotomous representation of complex indicator:




a b

Fig. 5. a – The goal tree of ISC; b – The block diagram of the goal tree

$$q_0 = f(q_1, q_2) = \varphi_1[(\varphi_2(k_1, k_2), \varphi_3(k_3, k_4))]$$

This procedure is a step-by-step process of criteria convolution; notice that only two of criteria are aggregated in each step. The nature of dichotomous representation allows us to solve the problem of complex evaluation involving $n$ criteria by means of solving two criteria problem. One of the unquestionable advantages of this method is its simplicity, which facilitates an effective evaluation process using an arbitrary scale. Most experts in the field of Organizational Management are confident, that decision maker is able to solve a finite number of problems efficiently due to the limit of his personal capabilities. Since we solve a problem involving no more than two criteria, such evaluations are much more efficient.

It is suggested to evaluate the extent of goal achievement for $q_i, i = \overline{0,2}$ and $k_i, i = \overline{1,4}$ using discrete scale, consisting of four possible values: poor (1), average (2), good (3) and excellent (4). Given matrix $A = \| a(i, j) \|$, where $a(i, j)$ is a convolution of values $i$ and $j$. Fig. 6 illustrates an example with such matrices.

Assume we get the value of "Depth" and "Scope" indicators equal (2) and (3) respectively, which in turn convolutes to $q_1$ indicator, which equals (3). In much

the same way we calculate the value of $q_2$ indicator, which equals (2). Acquiring values for $q_1$ and $q_2$ indicators allows us to calculate the desired integrated indicator $q_0$ "ISC level".

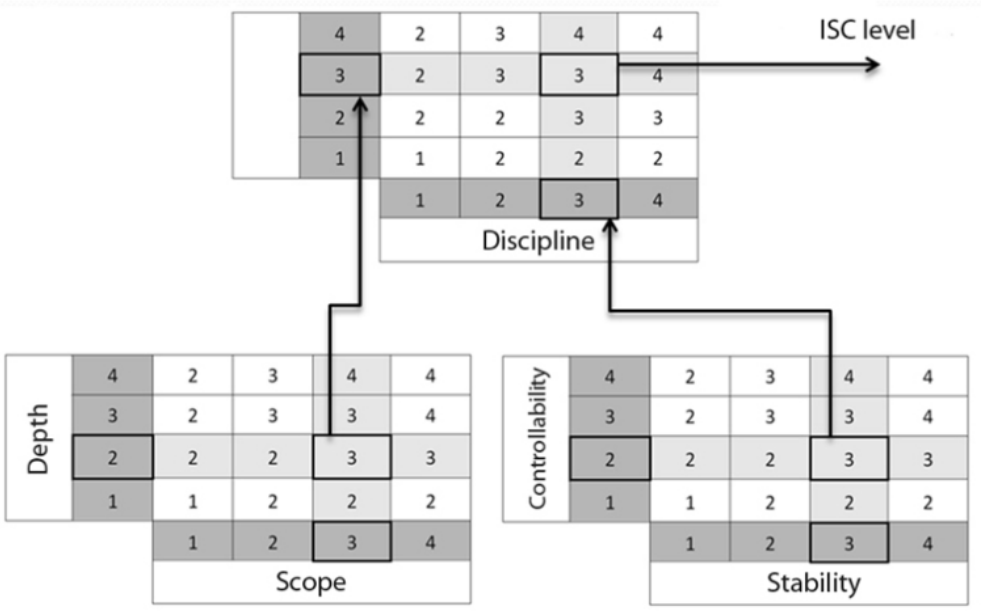



Fig. 6. Convolution matrices

The process of indicator aggregation is relatively simple, still there are two main difficulties: to generate adequate convolution matrices and to obtain valid values for lower level indicators $(k_1,k_2)$ and $(k_3,k_4)$. The responsibility for generation of convolution matrices rests upon the decision maker (in our case the role of decision maker can be granted to Chief Security Officer).

It is suggested to follow monotonicity condition while generating convolution matrices, i.e. the aggregated value should not be less than the initial one. It is essential to note, that one cannot fully abstract from subjective judgments during this process, so this nuance is required to be considered as well [10].

## Conclusion

The problems of Information Security Culture promotion are more and more recognized by researchers working in the field of Information Security. ISC can be considered as an essential component of Information Security Management systems today.

The development of organizational culture is very spontaneous in nature; therefore this process should be managed. As the component of every organizational system, ISC is always present somehow. As a matter of fact, low quality ISC has negative influence over IS policies and their execution in operative dimension. But it is utterly difficult to obtain an unconstrained compliance of IS requirements without it. From this point of view, ISC can be considered as important entity within the process of development of employee behavior, as well as a powerful tool of facilitating IS policy compliance.

Due to the immaturity of this concept a number of issues exist: an issue of complex evaluation of ISC level as well as evaluation of its degree of influence over IS policies compliance in organizational environment. A more detailed research on this subject appears to be a promising direction.

## References

*1. Потий, А.В. Концепция стратегического управления информационной безопасностью [Текст] / А.В. Потий, Д.Ю. Пилипенко // Радіоелектронні і комп'ютерні системи. – 2010. – № 6 (47). – С. 53 – 58.*

*2. OECD guidelines for the Security ofInformation Systems and Networks: Towards a Culture of Security [Electronic resource]. – Access mode: http://www.oecd.org. 8.03.2012.*

*3. Alfawaz, S.M. Information security management : a case study of an information security culture [Text] / S.M. Alfawar // PhD thesis. Queensland University of Technology. – 2011.*

*4. Майерс, Д. Социальная психология [Текст] / Д. Майерс. – СПб.: Питер, 1997. – 688 с.*

*5. Van Niekerk, J.F. Fostering Information Security Culture through Integrating Theory and Technology [Text] / J.F. Van Niekerk // PhD thesis. Nelson Mandela Metropolitan University. – August 2010.*

*6. Biri, K. Corporate Information Security governance in Swiss Private Banking [Text] / K. Biri,*

*G.M. Trenta // Master's Thesis. Executive MBA Program of the University of Zurich. – July 2004.*

*7. Alnatheer, M. Proposed Framework for Understanding Information Security Culture and Practices in the Saudi Context [Text] / M. Alnatheer, K. Nelson // Proceedings of the 7th Australian Information Security Management Conference, Perth, Western Australia, 1–3 December 2009.*

*8. Abu–Zihen, S. Success Factors of Information Security Management: A Comparative Analysis between Jordanian and Finnish Companies [Text] / S. Abu-Zihen // PhD thesis. The Swedish School of Economics and Business Administration, Hanken. – 2006.*

*9. George, J. Understanding and Managing Organizational Behavior [Text] / J. George, G. Jones. – Prentice Hall; 4th edition, November 13, 2004.*

*10. Новиков, Д.А. Теория управления организационными системами [Текст] / Д.А. Новиков. – М.: МПСИ, 2005. – 584 с.*

*Поступила в редакцию 12.03.2012*

**Рецензент:** д-р техн. наук, проф., зав. каф. И.Д. Горбенко, Харьковский национальный университет радиоэлектроники, Харьков, Украина

## ПЕРЕДУМОВИ ФОРМУВАННЯ КУЛЬТУРИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА МЕТОД КОМПЛЕКСНОГО ОЦІНЮВАННЯ ЇЇ РІВНЯ

***О.В. Потій, Д.Ю. Пилипенко, І.М. Ребрій***

Проблеми просування культури інформаційної безпеки все частіше розглядаються дослідниками, що працюють у сфері інформаційної безпеки. ISC може розглядатися як істотний компонент адміністративної системи інформаційної безпеки. В роботі досліджуються передумови формування культури інформаційної безпеки. Розглянуто ключові фактори, що впливають на формування культури інформаційної безпеки, а саме: психологічна настанова по відношенні до вимог інформаційної безпеки, норми поведінки та нормативні переконання. Запропоновано комплексний метод якісного оцінювання рівня культури інформаційної безпеки за допомогою матриць згортки.

**Ключові слова:** культура інформаційної безпеки, вимоги інформаційної безпеки, оцінювання, матриця згортки.

## ПРЕДПОСЫЛКИ К ФОРМИРОВАНИЮ КУЛЬТУРЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И МЕТОД КОМПЛЕКСНОГО ОЦЕНИВАНИЯ ЕЕ УРОВНЯ

***А.В. Потий, Д.Ю. Пилипенко, И.Н. Ребрий***

Проблемы продвижения культуры информационной безопасности все чаще рассматриваются исследователями, работающими в сфере информационной безопасности. ISC может рассматриваться как существенный компонент административной системы информационной безопасности. В работе исследуются предпосылки формирования культуры информационной безопасности. Рассматриваются ключевые факторы, оказывающие влияние на формирование культуры информационной безопасности, а именно: психологическая установка по отношению к требованиям информационной безопасности, нормы поведения и нормативные убеждения. Предложен комплексный метод качественного оценивания уровня культуры информационной безопасности на основе матриц свертки.

**Ключевые слова:** культура информационной безопасности, требования информационной безопасности, оценивание, матрица свертки.

**Потий Александр Владимирович** – д-р техн. наук, профессор, начальник кафедры радиоэлектронных систем пунктов радиосвязи управления Воздушных Сил Харьковского университета Воздушных Сил им. И. Кожедуба, Харьков, Украина, e-mail: potav@ua.fm.

**Пилипенко Дмитрий Юрьевич** – аспирант кафедры безопасности информационных технологий Харьковского национального университета радиоэлектроники, Харьков, Украина.

**Ребрий Инна Николаевна** – доцент кафедры иностранных языков Харьковского университета Воздушных Сил им. И. Кожедуба, Харьков, Украина.