ISSN 0147-6882, Scientific and Technical Information Processing, 2015, Vol. 42, No. 2, pp. 41–52. © Allerton Press, Inc., 2015.
Original Russian Text © L.V. Astakhova, 2015, published in Nauchno-Technicheskaya Informatsiya, Seriya 1, 2015, No. 4, pp. 1–13.

Information Security: Risks Related to the Cultural Capital of Personnel (Review)

L. V. Astakhova

South Ural State University, Chelyabinsk, 454080 Russia

e-mail: lvastachova@mail.ru

Received October 6, 2014

Abstract—Based on the analysis of such current trends in the field of information security and the post-industrial economy as the paradigm of "security through development," the culture of information security as a necessity to reduce information-security risks, and the approach that considers a person as capital, the concept of the cultural capital of corporate information security as an integral part of the cultural capital of an organization is justified. A procedure is developed for the risk assessement of personnel in information security, based on the index of confidence as the ratio of the individual cultural information-security capital to the corporate cultural information-security capital.

Keywords: information security, risks, vulnerability, cultural capital, personnel

DOI: 10.3103/S0147688215020021

INTRODUCTION

A modern economy cannot exist outside of culture; therefore, the cultural capital of a man, which is his cultural values, is converted to socio-economic benefits during any activity, including information security.

The high rates of information development in Russia and the scale of digital-information resources in all areas of public life have modernized the problem of information security. However, it is becoming clearer that the most advanced software, hardware, and technical security means, even with such a rapid dynamics of their development as occurs today, cannot provide a solution to these problems.

The reason for this is the underestimation of people as the most important links of a socio-technical system, which is the system of information security of an organization. These are the eloquent figures: for the first half of 2014 the InfoWatch Analytical Center recorded 654 cases of leakage of confidential information, which is 32% more than for the same period in 2013. As well, 71% of those who leaked information were employees of companies, current or former (69.2% and 1.4%, respectively) [1].

We cannot say that this problem has not been reviewed by science.

In the theory of information security of the post-Soviet period, a person as a source of threats to the protected information of an organization was the subject of the multi-direction research of A.A. Aleksentsev. This scientist not only identified people as the most widespread, diverse and dangerous source of destabilizing impacts on protected information, but also revealed different categories of people that may have this impact, and developed a detailed classification of the threat on different grounds: natural manifestations, causes and circumstances, conditions, methods of implementation, and results [2]. Today, a person is the main focus of attention in the study of organizational problems of information security, personnel security, and personnel management.

Much less attention in science and practice is paid to the assessment of a person in the context of the reduction of information-security risks, due to the complexity of the formalization of the process, as well as the interdisciplinary nature of the problem.

In the simulation of the threats and vulnerabilities of information security, the human factor can be taken into account; however, in the state regulator's methods of identification and evaluation of personnel, information-security vulnerabilities are not represented. Procedures for personnel evaluation exist in international and Russian standards. A. Prozorov noted that the "human factor" receives more attention in modern standards, such as ISO 27001/22301/20000, COBIT 5, ITIL, PMBOK 5, and NIST. Thus, COBIT5 focuses on the requirements of communication management, leadership and team building, identifying features of behavior, knowledge and skills, understanding the motives, expectations, values and goals of people, and raising awareness and training [3]. The ISO 27001 international Standard specifies requirements for the management of information security to demonstrate an organization's ability to protect its information resources [4]. According to this

standard, the analysis of organizational vulnerabilities includes, among other tools, interviews of personnel.

The security of human resources is included in the list of standard information-security vulnerabilities that is presented in section 8 of the ISO/IEC 27002 International Standard, which includes the following vulnerabilities: lack of safety training, lack of awareness of security issues, lack of monitoring mechanisms, lack of correct policies on telecommunications and messaging, no cancelation of access rights after dismissal of an employee, lack of procedures that guarantee the return of resources after such a dismissal, unmotivated or disgruntled personnel, and unsupervised work by attending or off-duty personnel [5].

The ISO/IEC 31010-2011 standard "Risk management. Methods of risk assessment" (Moscow, 2012) defines the following general (not only for information security) risk-assessment methods based on the identification and analysis of threats and vulnerabilities: brainstorming; structured or semi-structured interviews; the Delphi method; checklists; Preliminary Hazard Analysis (PHA); Hazard and Operability Study (HAZOP); Hazard Analysis and Critical Control Point (HACCP); the Structured What-If Technique (SWIFT); scenario analysis; Business Impact Analysis (BIA); Root Cause Analysis (RCA); Failure Mode and Effects Analysis (FMEA); Fault Tree Analysis (FTA); Event Tree Analysis (ETA); analysis of the causes and consequences; causal analysis; Layers Of Protection Analysis (LOPA); the Monte Carlo simulation method; Bayesian analysis and the Bayesian network; FN curves; risk indices; effects and probability matrixes, and other methods [6].

As well as the above methods, there is the method of the influence of human factors, Human Reliability Assessment (HRA), which may be used not only in a qualitative but also in a quantitative manner. Thus, a qualitative assessment of an operator's actions can be used to identify his possible errors and their causes. The HRA method may also be used to obtain quantitative data on failures associated with operator error.

A great contribution to the development of the theory of human vulnerabilities and methods of identification and assessment was made by the Central Bank of Russia by the developing a system of industry standards for information security. The STO BR IBBS-1.0-2014 standard "Information security of organizations of the banking system of the Russian Federation. General Provisions" emphasizes the priority of anthropogenic sources of threats. This standard is characterized by requirements for so-called "confidence in personnel."

Thus, in Sec. 7.2. "General requirements for information security in appointment and role assignment, and ensuring confidence in personnel," the general requirements include the following: the selection and documentation defining the role of employees; personification and determination of responsibility; documentary definition of the employment procedures that affect information security (authentication of documents that are submitted, claimed qualifications, the accuracy and completeness of biographical facts, verification of skills and professional suitability); regular verification (with documentary fixation of the results) of skills and professional suitability of employees, as well as unscheduled inspection of employees (with documentary fixation of the results) in the case of their abnormal behavior, participation in information-security incidents or suspicion of such behavior or participation; written commitment of employees of confidentiality, and commitment to the rules of ethics, including the requirement to prevent conflicts of interest [7, p. 18]. Specific requirements (Sec. 8.9) apply to the development and organization of educational programs that raise awareness in the field of information security [7, p. 34].

Such a keen interest of the developers of standards in employees as a source of anthropogenic threats to information security is certainly reflected in the methodology of its assessment.

It is quite natural that the CBR STO BR IBBS-1.2-2014 standard "The information security of organizations of the banking system of the Russian Federation. Methods of assessment of the conformity of the information security of the organizations of the banking system of the Russian Federation to the requirements of STO BR IBBS-1.0-2014," names the group indicator M1 "Information security in appointment and role assignment, and ensuring confidence to personnel," which describes the particular indicators that correspond to the above requirements, as well as denoting the compulsion of their performance. The structure of the indicators, besides the M1 indicator that is associated with confidence in personnel, includes the M18 group indicator "Development and organization of educational programs, raising the awareness in the field of information security," which contains traditional protective measures associated with increasing of skills [8].

The recommendations for harmonization of standards RS BR IBBS-2.2-2009 "Methods of risk assessment of violation of information security," which groups the main sources of information-security threats into seven classes. Sources that are related to the activity of insiders have been attributed to the fifth class, and social engineering, along with terrorism, industrial espionage and blackmail, to the second class. The method is based on determining the risk of violation of information security depending on the possible implementation of risk (PIR) and severity of the consequences (SC). The recommendations also propose a methodology for risk assessment of violation of information security in a quantitative (monetary) form [9].

Due to the fact that standards in Russia are advisory in nature, in practice the need for risk assessment

is either denied, or risks are assessed intuitively, or on the basis of general considerations. To determine the levels of human vulnerability in information security, as a rule, expert judgment is used, which certainly affects the objectivity of the results. Trying to find more accurate methods, e.g., to derive formulas, to construct models, so far has not led to a result that would be viable in practice. Therefore, in the scientific world there is increasing interest in the problem of evaluation of human factors in information security. Researchers from the St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences (SPIIRAS) have undertaken a serious development of methodologies for the assessment of a person as an object of socio-engineering attacks [10, 11]. A.S. Zaitsev and A.A. Malyuk, using the insider model, have developed a technique that can solve such problems as the problem of the formalization of a human factor in the system and the problem of the lack of statistical material for the construction of analytical and management systems in the field of information security [12]. An information system that solves the problem of formalizing the assessment of employee loyalty and reducing the information-security risks of an organization was created by M.Y. Rytov and E.V. Leksikov [13]. This problem is being paid close attention by the leading experts in the field of information security. Thus, A.V. Lukatskii identified indicators of the awareness of internal clients in the field of information security [14]. In our publications the problem of the assessment of human vulnerability of an organization information security was also solved in the methodological aspect [15].

However, with all the advantages of the above methods, we should state that some of the important factors were considered sufficiently.?The first factor is based on the evolution of the security paradigm from the "defensive" to the "developing," from threat protection to the paradigm of "security through development." This paradigm is secured in the following recent official Russian documents: "The National Security Strategy of the Russian Federation until 2020," "Strategy for Information Society Development in Russia" and others. The ideal information security is related today to the development of personnel, society, business entities, and the state. It is well known, however, that the development of organizations, society, or the state is impossible without the development of people, thus, modern assessments of the human vulnerability of an organization should be based on the comprehensive development of their employees.

The second factor is the development of scientific knowledge in the field of information security, expressed in active humanitarian studies of this process, including its cultural aspects. The most important object of the study is the culture of information security; its subject is people. This idea is attributed to K.M. Dolgov, who insists that people are the subject and the object of culture, which has always determined other spheres of life. According to Dolgov, "the disadvantage of all the political systems and all political regimes, both in Western Europe and Russia, by now, is that they are not based on the highest cultural standard. If so, it is impossible to develop the political will of either the ruling strata or the people, because neither the ruling strata nor the people have faith in what they do and should do. A lack of faith is due to a lack of culture, which is the basis of all social constructions and all social modernization" [16].

A similar position is held by the Japanese professor D. Ikeda, who, relying on the experience of the "Japanese miracle," claims that any innovations, including democracy and the market economy, should emerge in each case in the depths of culture, grow in urgent need, and tactfully adapt to traditions, customs, and national mentality; it is important to have a careful approach and a carefully thought-out strategy, with initiatives emanating from the nation itself.

This is the culture that determines the country's economic prosperity and political independence. An excursion into the history of Russian philosophical thought convinces scientists that the problems of morality, the moral health of society, and human values in general, acquire an economic aspect, because the relationship between values and economic development and their mutual influence are considered to be proven [18, p. 128]. Therefore, the evaluation of human factors in information security today cannot be developed outside the cultural context.

The third factor is related to the evolution of methodological approaches to a person in an organization and its evaluation in economic science. In the first half of the 20th century a person was considered as a resource and evaluated through costs, while in the 1940s–50s as an employee, and the assessment was focused on his motivation. Starting from the 1960s, people have been included in the capital structure and evaluated by cost performance [19]. Human capital is the set of specific characteristics of a person that may bring income to an organization. The dependence of company income on employees has become axiomatic.

If human-resource management achieves the business goals of a company, management of human capital ensures a constant growth of individual, corporate, and public wealth. Meanwhile, all of the existing techniques for the assessment of human vulnerability of information security ignore this modern approach. Thus, in the ISO/IEC 27002: 2005 standard a resource-based approach is applied to human vulnerabilities; Section 8 is named "Safety of human resources" [5]. For clarifying the motivation of personnel, the approaches of the middle of the last century are based on the techniques of A.S. Zaitsev and A.A. Malyuk [12], M.Yu. Rytov, and E.V. Leksikov [13], among others.

It is obvious that we need an approach that combines all these factors. This approach, we believe, is

based on cultural capital. The development of the cultural information-security capital of a company as a factor of its maintenance and development is the vector of human vulnerability assessment that is provided by the current trends of science and practice. The higher the level of the development of the cultural capital of a company is, the lower the risk is to its information security.

THE CONCEPT OF CULTURAL CAPITAL

In recent years, the concept of cultural capital has taken a stable place in the scientific discourse. Bourdieu was the first to determine it as a separate form of capital. He defined cultural capital as capital that under certain conditions may be converted into economic capital and may be institutionalized in the form of educational qualifications [20].

Cultural capital was also investigated by N.V. Bol'shakov [21], S.V. Gorbunova [22], E.A. Kos'mina [18], V. Radaev [23], I.S. Samarina [24], and others. Thus, according to I.S. Samarina, cultural capital is a system-based socio-economic category that reflects quantitative and qualitative socio-cultural characteristics of different groups of the working age population [24]. N.V. Gorbunova, using a value approach to culture, defines cultural capital as a person's wealth in the form of basic values, norms, principles, education, intellectual, moral and social characteristics that determine professional competence and are implemented in his social activities, bringing additional socio-economic benefits and legitimizing status, role, and power [22]. It is easy to see that the latter definition almost blurs the boundaries between culture as a system of values and cultural capital. What, then, is the difference between cultural capital and culture?

The answer to this question was given by D. Throsby, who argues that only under certain conditions of active use do the cultural values embodied in a person change his professional status and transform into cultural capital. In this case, the main condition is social action, in which an individual is the subject of work and has a professional niche that is appropriate to his cultural level, which provides not only social professional status, but also access to additional income, exceeding the cost of the simple reproduction of the worker and his family [25].

Cultural capital is also different from human capital. According to D. Thorsby, human capital means knowledge as a formal human professional competence.

Cultural capital focuses on the human characteristics that a person obtains as a consequence of membership in a particular social group, such as, language, dress style, tastes, or hobbies. Cultural capital enables people who are not familiar with each other and belong to the same social group to recognize each other and to enter into communication [25].

The concepts of culture and human capital are not the same. Cultural values in themselves, embodied in people's minds as culture itself (a set of stable forms of social interaction) are not human capital. They are merely a potential form of the manifestation of human capital [25].

The structure of cultural capital is interpreted differently by scientists. Its classical interpretation is the classification of Pierre Bourdieu [20], according to which cultural capital can act in following three states: the institutionalized state (diplomas and titles or sports titles), the objectified state (the possession of cultural objects) and the incorporated state (expertise, skills, understanding of the aesthetics, pronunciation, etc). The incorporated type of capital is a so-called habitus. A habitus includes a set of dispositions, models of perception and actions that an individual acquires in the socialization process, incorporating a set of ways of thinking, feeling, and action. These dispositions are stable. Habitus is a consequence of assimilation (interiorization) of objective social relationships and at the same time a subjective source of agents, i.e., a kind of mechanism that gives rise to various social practices. These practices include aesthetic tastes, manners, speech patterns and pronunciation, body language, writing styles, preferences in food and beverages, and educational success. V. Furs argued that habitus is inscribed on the social structure of the human body, i.e., the social structure becomes human "nature" [26].

According to other researchers, the basic structural foundations of cultural capital are humanistic capital and intellectual capital. They rank religious and moral potential, moral values and moral potential among the forms of humanistic capital. Intellectual capital is considered as a set of human capital (professional competence) and structural capital, which consists of organizational and customer capital [18, p. 45].

The theory of human capital is developing intensively in science. I. Soboleva concluded that "Today broad interpretations of human capital more popular. Its composition includes a broad set of personal qualities, worldviews, and values, which may have an indirect effect on the results of productive activities" [27].

However, the nature of intellectual capital can be defined much more precisely if we interpret it as "a productive form of human productive and creative forces in the information and network economy that is adequate to the modern information stage of the development of human society; its elements receive monetary and non-monetary assessment, capitalization, become intellectual property, come to the market, increase productivity, generate additional revenue, improve the quality and standard of living, and provide sustainable innovative economic growth and social stability in society" [28]. Scientists include the three following components in intellectual capital: human capital, structural (or organizational) capital, and client capital.

ASSESSMENT OF CULTURAL CAPITAL

In the domestic economy, works have been published devoted to the assessment of cultural capital. Thus, the basis of the assessment technique of cultural capital that was developed by a team of the authors [18] consists of imperatives for the assessment of humanistic and intellectual capital. However, most economic studies are focused on the assessment of one of the components of cultural capital.

The existing methods in economic literature for the assessment of intellectual capital may be grouped into five aggregated groups: (i) direct intellectual-capital methods; (ii) market capitalization methods; (iii) return on assets methods; (iv) method scorecard methods; and (v) information intellectual capital methods.

In contrast to the law of diminishing returns in the traditional economy, in the modern information and intellectual economy there is a law of increasing returns on intellectual capital. Thus, G.M. Tolstobrov proposed a component and investment type method for the assessment of intellectual capital that is based on the overall assessment of all types of carried out and accumulated investments in the relevant components of intellectual capital, taking the differences in the type of investment, investing time, and the duration of the employee's work into account [28]; E.A. Kos'mina, S.E. Meteleva, and A.D. Kosmin proposed to assess intellectual capital using Tobin's Q ratio, which is the ratio of the market price of a company to the price of its real assets. [18]

The analysis of assessment techniques of human capital and efficiency of investment in human capital that exists in economics shows a wide variety of approaches that can be divided into two main groups, viz., the cost-is-no-object and income approaches. The cost-is-no-object approach is based on the summation of the total expenditures on education, vocational training and other costs of society that are usually attributable to investment in human capital. The profit approach supposes the evaluation of employee income, which reflects the return on the funds that were invested in the educational and qualification levels. K.V. Markaryan added a third method to these two methods, the method of sales comparison, which is a market method for determining the value of human capital on the basis of a comparative analysis of the current supply and demand for similar human capital [29].

The comparative analysis of the techniques for assessing human capital showed that the basis of the calculations is the evaluation of the investment in human capital and the capitalization of the return on these investments, as well as natural indicators. However, the problem of the calculations remains in the form of incomplete baseline data and the great likelihood of double counting in the case of the development of a single technique for all elements of the proposed categories. Therefore, the most appropriate technique, as recognized by Yu.M. Kastryulina, is the approach that is based on investment accounting, although the investment value does not always correspond to the direct impact at the level of human capital [30], with which we fully agree. This allows us to agree as well with N.M. Pliskevich, who associates the imperfection of human capital assessment with the use of purely formal statistical categories, as well as abstraction from the quality of cultural capital as a total human capital base [31].

In most of the techniques the authors overlook certain important aspects, which leads to distortion of the results of empirical research. According to I. Sobol-eva, the largest discrepancies are typical for transformational economies, including the Russian economy. The data are less contradictory for countries with well-developed competitive labor markets. Technical roadblocks and the exhausted capabilities of the cost evaluation of human-capital reserves lead to a change in the direction of research: from direct measurement of its volume to identification of trends and correlations in the analysis of human capital [27].

In addition, in the course of the analysis of approaches to the evaluation of human capital, scientists have shown the contradictions between: (i) the transformation of human qualities into major factors and the value of development and (ii) worsening of the natural limitations and increased anisotropy of human capital. In this context, the further progress of post-industrial trends and globalization transforms itself into an anthropogenic problem [29].

In this regard, the work of N.N. Shash [32] is interesting; he determined the contradictory process of the development of the human capital of an organization that, on the one hand, promotes the intellectual and labor potential of personnel (i.e., improves the quality of working life), and on the other hand, leads to increased intensification of labor and, consequently, increased exploitation of employees who are involved mainly in intellectual work. Therefore, we agree with the author of [32], that it would be wrong to unambiguously interpret the development of a company's human capital as the basis for a real improvement of the living standards of its employees. By definition, the quality of working life is characterized by the level of well being of a person, as well as their social and spiritual development, through their activities in an organization; thus, the intensification of labor may lead to disloyalty to an organization by these employees [32], which means an increase in information-security risks.

This point of view is also supported by V.G. Puzikov [33], who argued that "human capital is not an abstract concept but a concrete embodiment of human nature, the primary element of which is specific individuals." Society as a system involves in its development an implementation of the target function of the system as a whole and its individual elements.

The objective meaning of the human system is a person himself. We agree with the author that the meaning of human life is not to ensure the growth of GDP, or, for example, to create as many weapons as possible for their own destruction. A person can and should live in order to develop and realize his spiritual and intellectual potential, with a simultaneous increase in consciousness and physical perfection.

These contradictions in the studies of human capital are resolved by themselves as soon as we consider human capital as the cultural capital of an organization. It is the cultural essence of a person (values, ethics, etc.) that creates a valuable and humanistic space, which must impact the organization at which that person is an employee.

Taking the above drawbacks of approaches to the assessment of cultural capital in economics in account, we turn to more value-laden sociological, philosophical, and psychological studies, which also attempt to develop techniques for the assessment of cultural capital. Thus, N.V. Bol'shakov has developed a comprehensive technique for the assessment of cultural capital in the three following states defined by Bourdieu: incorporated, objectified, and institutionalized. N.V. Bol'shakov used the following indicators, on whose basis a single index for each state was established: scientific degrees, diplomas, certificates, and publications (institutional state); recognizable signs and symbols that are contained in material objects (objectified state); the ability to understand meaning, knowledge, vision, knowledge of foreign languages, cultural and linguistic competence, characteristics of the environment in which the individual's socialization took place, and their place of residence during their school years (incorporated state) [21].

Much attention is paid by scientists to the assessment of the individual components of cultural capital, such as humanistic (valuable) capital and intellectual (human and structural (organizational) capital). Thus, in the context of a study of human capital Babenko [34] proved that for modern sociological studies the traditional interpretation of human capital as a set of knowledge and skills that were acquired in the course of study and work is insufficient. In the context of structural functionalism human capital is an element of the socio-economic system that contributes to its reproduction, fulfilling the social function of human and social development. Within the framework of social constructivism human capital is a product of not only social but also cultural construction, including a set of knowledge, skills, ideas, and values, that are accumulated in the process of education and training. The author also highlights the peculiarities of the institutionalization of the use of human capital for the purpose of human capital in the modern period, the processes of transition from equality to differentiation in consumption; from orientation to survival to focusing on having fun; from meeting the requirements of a population to meeting effective demand; from the pseudo-efficient to the quasi-efficient use of human capital; from quasi-fair to pseudo-fair payment; and from formal assessment of human capital to financial assessment [34]. Obviously, in these circumstances, the urgent problem is the values in labor relations.

The question of the measurement of values as the core of humanistic capital is the most difficult problem, which doesn't adequately solve the notorious question of the human factor. Today, this is actively developed in social philosophy and social psychology. There is an interesting study by M.P. Danilkova [35], who settled the definition of value through the degree of application of human effort, i.e., through human activities.

Danilkova showed that the subject of activity creates value or experiences something else depending on the cost of the work, creative power, and energy that are aimed at the creation or development of external realities in their objectification or disobjectification. Interpretation of the values that were provided by the author "as a measure of costs," where the measure is the dialectical unity of quantity and quality, gives the value of the practical content. The principle of measurement of values was formulated by Danilkova as follows: the higher and worthier the value is, the more effort it takes for creation or implementation. At the same time, the dependence of real values on the degree of the effort to create them has a directly proportional nature and the spiritual and institutional values are determined not so much by the costs that are incurred in their creation, but by the degree or scale of their consumption, i.e., this dependence has an inversely proportional nature [35]. This approach to the assessment of values seems to be quite heuristic in order to identify the attitudes of employees to different values in the field of information security.

The psychological context has great importance in the research on cultural capital. In the context of the assessment of organizational culture, the psychological aspect of the problem of value assessment was considered by E.N. Molodykh [36], who proved that one's attitude towards ethical standards of business behavior plays a key role in the moral regulation of business behavior. The author convincingly proved that, on the one hand, business behavior is caused by the subjective experiences and personal characteristics of employees, and on the other hand, is subject to change in accordance with the accepted values, norms, and basic ideas about the nature of morality, i.e., is determined by the moral component of organizational culture and its subjective interpretation. One of the mechanisms for the subjective assessment of organizational culture is, according to E.N. Molodykh, a projection mechanism of its own ideas about the "ideal" culture.

The particular interest that was justified by Molodykh is a conceptual approach to the value assessment of the employees of an organization due to the

fact that she justified preferences of a particular type of organizational culture by the features of need and the motivational sphere of the employees. An interesting result was obtained during an empirical study, which shows the relationship between ethical standards of business behavior and the motivation of employees. For example, the need for social contact and close ties with colleagues who deal with a wide range of people is associated with the willingness to be less tolerant and adherence to principles in business behavior. The more people tend to feel popular and have interesting and socially meaningful work, the more likely they are to be guided by the principle of fairness to their colleagues and business partners.

The need for high wages, entitlements, to win recognition from other people, and the desire for a feeling of one's own importance are associated with a low level of readiness for responsibility in business behavior. With the increasing need for improvement, growth, and development, one's readiness for responsibility increases. The patterns that were identified by this scientist [36] may also be used in the assessment of human capital in the field of information security.

N.M. Lebedeva and A.N. Tatarko [37] proposed a new theoretical and methodological approach to the psychological constellation of cultural values of Schwartz questionnaire based on an approach to the values from the perspective of an individual, rather than that of society, from the perspective of individual solutions to the major problems of his life in society. According to the results of factor analysis using World Values Survey and subsequent theoretical understanding of it, the authors identified the following options for addressing the three major problems faced by the people in culture: the stability of life–self-realization, dominance–equality, and the pursuit of pleasure–spirituality. The authors tied certain values to each of the poles, thus identifying the values that have a positive impact on economic development. These values, in their opinion, are the values of self-realization (independence, skills, a choice of one's own goals, intelligence, curiosity, success, open-mindedness, ambition, and responsibility), spirituality (the world of beauty, unity with nature, spiritual life, environmental protection, creativity, mature love, and solitude), the search of pleasure (pleasure, an interesting life, diversity of life, true friendship, pleasure, and self-indulgence) [37]. Identifying these values that contribute to economic development once again stresses the need for the study of human capital in the cultural context.

In the shaping of the cultural capital in different social strata I.S. Samarina [38] identifies a number of common features: (i) the growth of the incorporated cultural capital (the development of knowledge and skills that are potentially obtained and used by some social group); (ii) realization of the process of the modernization of objectified cultural capital, a modernizing of the symbolic forms of culture (paintings, books, dictionaries, the appearance of actors, and their style of labor interaction); and (iii) the improvement of institutional cultural capital (progressive updating of the rules, concepts, and principles of behavior of social groups). However, the functioning of cultural capital in various fields has specific characteristics. Therefore, having defined the concept, structure, and some heuristic approaches to the assessment of cultural capital, let us move to the justification of the details of its operation in the field of information security.

THE CONCEPT OF THE CULTURAL CAPITAL OF INFORMATION SECURITY AND ITS STRUCTURE

The need to use the concept of cultural capital in the process of assessment of personnel risks in information security is confirmed by the words of the Russian philosopher Nikolai Berdyaev, who as early as in the 1930s in the article "Man and Machine" named three types of human life, viz., natural, cultural, and that related to mechanisms. If the first type prevails, a society remains at a primitive level, if the third type prevails, a society loses its spirituality and dies. Only culture connects the natural and mechanical types, maintaining harmony [19, p. 10]. Therefore, for organizations to achieve information security, they should focus not only and not so much on the technical means of the process, but on the culture and the people who are involved in it directly and indirectly.

As cultural capital is culture embodied in production, it is logical to assume that cultural capital in the field of information security is a projection of the culture of information security.

We have determined the culture of information security from the position of the functional active approach as a specific method for the organization and development of the information activity of a person, as realized in value-oriented models of information exchange as a data sender and recipient, in which the person determines and controls the unity of existence and development of information objects in their cognitive and communication manifestations [39]. The peculiarity of the new definition is that the essence of the culture of information security as a requirement of the modern developing information society manifests itself when we use a functionally active technological concept of culture, a protective and developing concept of security, and ambivalence of information, its ideal material nature, as the embodiment of dualistic monism in the context of a realistic philosophy.

Of particular importance is the fact that the proposed definition is based on the understanding of culture that was justified by E.S. Markaryan as a part of his technological concept in the 1970s. The starting point of his argument was the recognition of the fact that any system, from a simple living organism to a

society, tends to self-preservation and self-reproduction. If the system loses the ability to develop mechanisms that prevent an increase in entropy processes, it disintegrates. Such a mechanism as applied to society is culture as a result of the activities of a special kind, which manifests the social nature of man. This approach emphasizes the particular embodiment of culture in the field of information security, as self-preservation and self-reproduction reflect the nature of culture through the processes of security and development, which corresponds to the paradigm of "security through development."

If an individual achieves this path, his culture of information security will capitalize as individual cultural information-security capital, bringing him an income in the form of his personal security privacy and protection from manipulation of his mind from the negative impacts of information; this allows harmonious development and career growth, as well as material and spiritual well being not only within an organization but also outside it.

Thus, individual cultural information-security capital (ICCIC) is all of the cultural resources of an individual as a data recipient and sender in the process of information exchange (basic values, norms, principles, intellectual, moral, ethical and social qualities, and value oriented behaviors), which determine his ability to organize and develop information activities during which he reveals and controls the unity of existence and development of information objects in their cognitive and communication forms, and allowing him to receive additional socio-economic benefits and to legitimize his status, role, and power.

The task of an organization in achieving the goal of its information security is to convert the formed individual cultural information-security capital of an employee into corporate cultural information-security capital. Corporate cultural information-security capital (CCISC) is all of the cultural resources that are used by an organization that contains the employees of the organization and the organization as a whole, as data senders and receivers in the process of information exchange (basic values, norms, principles, intellectual, moral, ethical and social qualities, and value-oriented behaviors), which determine the ability of an organization to develop information activities in the course of which an organization defines and controls the unity of existence and development of information objects in their cognitive and communication forms and allows an organization to obtain additional socio-economic benefits and legitimize its status, role, and power.

Based on the definitions of the "culture of information security," "cultural capital," and the "cultural capital of an organization's information security," we include in the structure of corporate cultural information-security capital the following:

1. Incorporated cultural information-security capital:

1.1. Humanistic capital: A holistic system of views on social life (information worldview).

1.2. Intellectual capital:

• human capital: awareness of an employee of information security, the ability to understand the meaning of information security, the ability to develop and adapt in the field of information security, the ability for the specific language of communication in the field of information security, and reputation in the field of information security (lack of information-security incidents);

• structural capital (institutional and market): the professional competence of a head of the department of information security in the field of information security, awareness among employees of an organization in the field of information security, costs (financial and time) for training, retraining, and professional development, including raising of awareness on information security, employee turnover, communication with customers and partners in the field of information security, reputation in the field of information security, the strength of the brand, employee's feeling of satisfaction, his work in the organization, the organizational culture, and other factors.

2. Objectified cultural information-security capital:

2.1. Humanistic capital: personal and corporate values, ideals, principles, criteria of good and evil, implemented in communication, etc.

2.2. Intellectual capital: human capital (personal patents, programs, publications, techniques); structural capital (institutional and market): corporate patents, programs, publications, techniques, etc.

3. Institutional cultural information-security capital:

3.1. Humanistic capital: a professional code of honor, a corporate code of honor.

3.2. Intellectual capital:

• human capital: a system of individual certificates of employees in the field of information security (degrees, licenses, and certificates), types of educational institutions and total duration of training on information security for each employee, etc.;

• structural capital (institutional and market): a system of corporate certificates in the field of information security (degrees, licenses, and certificates), types of educational institutions and total duration of training on information security of all employees, the organization's membership in professional societies on information security.

ASSESSMENT OF THE CULTURAL INFORMATION-SECURITY CAPITAL OF AN ORGANIZATION

There are no techniques for the assessment of the cultural capital information security of organizations,

although it is obvious that this process can be performed separately or together with the assessment of other types of cultural capital of an organization. Thus, N.I. Pirozhkova [40], in developing a technique for the assessment of human capital, introduces a special group of costs associated with the disloyalty of employees, as well as coefficients that reveal the factors that increase loyalty. Such costs are divided into five groups: the replacement cost upon the sudden dismissal of an employee; loss of revenue from a customer due to the incorrect behavior of an employee; losses from deliberate sabotage to destroy or damage the property of a company; loss of employee time for a subjective reason (in monetary terms); and financial losses from the disclosure of confidential information by the employees of a company.

To assess the cultural information-security capital of an organization within the determined frames, we can use, for example, a technique for assessment based on Lazarfeld's Latent Structure Analysis (LSA) [12, 41, etc.]. Each of the variables—attributes of the incorporated, objectified, and institutionalized cultural capital of the organization's information security must have its own total value that is determined by expert evaluation.

For poorly formalized criteria for assessing the cultural information-security capital, which includes values, it is advisable to use the approach of E.N. Molodykh, who has convincingly proved the relationship between the attitude of employees to the organizational culture of a company and its attitude towards fulfilling ethical standards of business behavior [36]. The validity of this estimation will be much higher, as the employee will be a subject of estimation of not his own culture of information security or his cultural information-security capital, but organizational culture or capital of the organization. It is no coincidence that specialists in personnel management who develop techniques for the assessment of employee loyalty have found it useful to apply indirect estimations.

It is important to emphasize that through this approach we can carry out the monitoring of the cultural capital of an organization, as soon as the subjective interpretation of the organizational culture changes via changes in its moral values. In the case of the detection of the evolution of the assessments, we can take corrective actions relating to either the human or structural capital.

THE RELATIONSHIPS OF TYPES OF CULTURAL CAPITAL AS AN ASSESSMENT TECHNIQUE FOR THE HUMAN VULNERABILITY OF THE INFORMATION SECURITY OF AN ORGANIZATION

In terms of corporate cultural information-security capital, we cannot assess the level of individual cultural information-security capital and vice versa. This is due to the fact that: (i) not everyone in an organization has the ability and desire to use his cultural values in the production activity and (ii) not every organization is able to use for its own purposes cultural capital of each of its employees. This is confirmed by the ideas of I.S. Samarina [24] on the dual qualitative characteristics of cultural capital. On the one hand, the potential form of cultural capital is the features of cultural competency, knowledge, skills, values, social norms, principles, moral and ethical priorities, the labor motivations of the actors; on the other hand there is a real form of the accumulated cultural capital, cultural human potential used in the labor process that legitimizes social work status, power, and career dynamics.

Existing in such a dynamically ambivalent form, the cultural capital of an organization's information security always has a synergistic effect, which summarizes the effect of the interaction of these two types of cultural capital. It is this emergence, which means the inequality of all of the properties of cultural capital of organization's information-security system to the sum of the properties of its components, that is able to increase the level of information security.

Trust in an organization refers to such synergistic emergent properties of cultural information-security capital (CCIS) as trust of employees in managers and in each other, trust of managers and employees in partners and customers, etc. Trust is a relationship to the actions of another person and to oneself that is based on the belief in faithfulness, integrity, honesty, and sincerity [42]. The need for such a culturally capacious concept has always existed in the area of information security in the area of secrets and mysteries.

It is no coincidence that to this day this term is used as a target and is the result of data protection in relation not only to individuals but also to technical objects, which is reflected even today in the standards of information security. A high degree of confidence is the result of the full synergistic unity of individual and corporate cultural information-security capital. Confidence is evaluated today at an intuitive level by subjects of information relationships and is the guarantor of information security in interpersonal and corporate communications.

On this basis, it's reasonable to assess cultural information-security capital through the index of confidence in the employees (Dpers), which depends on the ratio of personal cultural information-security capital (ICCISpers/n) and corporate cultural information-security capital of a person (ICCISpers/corp/n), i.e., a personal capital, which an employee invests in a company. The lower the ratio is, the more the personal cultural capital of an employee is converted to corporate information-security capital (IS), the lower the level of personnel vulnerability is. A simple average of the trust in all of the employees of an organization may be indicative of the confidence index in all of the

employees of an organization. The product of the confidence index in the index of the structural capital of an organization is the cultural capital of the organization's information security. Let us take a closer look.

1. Identification of the level of individual cultural information-security capital of each employee, ICCISpers/n:

$$\text{ICCISpers/n} = \text{GCpers/n} + \text{HCpers/n}, \quad (1)$$

where ICCISpers/n is the level of individual cultural information-security capital of each employee, n;

GCpers/n is the humanistic capital of each employee, n;

HCpers/n is the human capital of each employee, n.

2. Identification of the level of corporate cultural information-security capital of each employee ICCISpers/corp/n:

$$\text{ICCISpers/corp/n} = \text{GC pers/corp/n} + \text{HC pers/corp/n}, \quad (2)$$

where ICCISpers/corp/n is the corporate cultural capital of IS of a person that is invested by him in the organization;

GC pers/corp/n is the humanistic cultural capital of IS of a person;

HC pers/corp/n is human cultural capital of IS of a person;

3. Determination of the confidence index for each employee as the ratio of the two identified indicators for each employee:

$$\text{Dpers/n} = \text{ICCISpers/n: ICCISpers/corp/n}, \quad (3)$$

where Dpers/n is the employee confidence index, n;

ICCISpers/n is individual cultural information-security capital of a person, n, outside the organization;

ICCISpers/corp/n is the corporate cultural information-security capital of a person, n, inside the organization.

4. Determination of the average value of the confidence index of the employees:

$$\text{Dpers/1} - \text{n} = (\text{Dpers/1} + \text{Dpers/2} + \ldots \text{Dpers/n}): \text{n}, \quad (4)$$

where Dpers/1 – n is the confidence index of the employees;

Dpers/1 is the confidence index of employee 1;

Dpers/2 is the confidence index of employee 2;

Dpers/n is the confidence index of employee n;

n is the number of employees.

Note that the confidence index is not the same as the amount of cultural information-security capital. Cultural information-security capital is a product of the index and the index of the structural capital of organization, the indicator of the volume of the efforts that an organization undertakes to convert individual cultural information-security capital into the corporate type:

$$\text{CCISC} = \text{Dpers/1} - \text{n*SC}, \quad (5)$$

where CCISC is corporate cultural capital of the IS of an organization;

Dpers/1 – n is the revealed confidence index for all of the employees of an organization;

SC is the volume of the capital structure of the organization.

The higher the ratio of the capitals is, the less the employee invests his capital in the organization; this means that less capital is converted into the cultural capital of an organization's information security and consequently a lower level of trust in the employee, as well as the higher personnel vulnerability of an organization from this employee.

As one can see, the dependence of human vulnerability of information security on the cultural information-security capital is inversely proportional. The higher the level of cultural capital is the lower the probability is of threats to information security. Managing cultural information-security capital is able to transform it into new revenue of an organization. It is no coincidence, for example, that knowledge management, which is so intensively studied at present and put into practice, is a strategy that transforms all kinds of intellectual assets into higher productivity and efficiency, new value and increased competitiveness [43].

The advantage of the proposed technique, which can be called "a technique for the relationships of cultural capitals," is based on the process of assessment of human vulnerability of information security of organization grounded on integration of personal and corporate cultural capitals. There is a person, on the one hand, with his cultural information-security capital and the opportunity to convert his cultural capital in the information security of an organization in order to gain an advantage; on the other hand there is an organization with an opportunity to convert the cultural capital of employees into the cultural capital of the organization, and then, into its economic capital. The process of conversion is a complex process of the formation and development of structural capital and knowledge management in the field of information security, but due to the synergistic property of cultural capital, the process of the conversion of an organization's information security allows it to provide a steady growth of not only corporate, but also individual and social wealth.

CONCLUSIONS

1. This analysis of the existing approaches to the assessment of the human factor that reduce the risk to the information security of an organization has identified the interdisciplinary nature of the problem of the assessment of the human factor, reducing the risk to the information security of an organization and the weak formalization of the evaluation of the human factor, which complicates the search for its solution.

At the same time, some experience in studying this problem has been accumulated in domestic science. However, most studies do not take the current trends in the fields of security, information security, and economics that are caused by social and cultural post-industrial transformations into account.

2. A conceptual approach based on cultural capital has great heuristic capacity for solving this problem. We justify the concept of the cultural capital of corporate information security as an integral part of the cultural capital of an organization and its structure, which is based on humanistic and intellectual (human and structural) capitals.

3. The approach to the assessment of the human vulnerability of information security based on its cultural capital allows us to take the main current trends of social and economic practices (the paradigm of "security through the development"; the culture of information security as an imperative to reduce the risk of information security; the approach to a person as capital) into account and implement them in relation to the field of organizational information security as follows:

• To consider the development as an imperative of culture as an essential factor in ensuring information security, which is ultimately aimed at achieving the goals of the economic development of an organization, increasing its competitiveness. This allows one to consider cultural capital, and, therefore, cultural competency features of personnel as an argument to the function of economic development of people, organizations, and society;

• To consider the conversion of the culture of information security of employees in the cultural capital of an organization, focusing on the process of objectification of subjective characteristics of employees. This allows us to see the high heuristic value of information-security culture and the process of its transformation into the cultural capital of an organization;

• To consider a person in the light of current trends of the post-industrial society as capital, to develop on this basis a technique for the assessment of the human vulnerability of information security. This allows one to overcome stereotypes about the low-grade validity of the assessment techniques of the human factor, which result in an attempt to assess a person as a human production resource or as an employee with his motivations.

4. The technique for the assessment of the human vulnerability of information security, based on the confidence index as the ratio of the cultural information-security capital of individuals and organizations enables one to monitor these types of capital and the gap between them and assess the necessary directions of the development of a company's capital structure to reduce the risk of information security with respect to each employee at any time.

REFERENCES

1. Study of leaks of confidential information in the first half of 2014. http://www.infowatch.ru/report2014_half.
2. Aleksentsev, A.I., The nature and relations between the concepts of "protection of information", "security of information", and "information security", *Bezop. Inf. Tekhnol.*, 1999, no. 1, pp. 44–47.
3. Prozorov, A., The human factor in information security standards. http://www.slideshare.net/AndreyProzorov/ss-27026263.
4. GOST (State Standard) *R ISO/MEK 27001:2006 Information Technology. Methods and Means of Ensuring of Security. Management Systems of Information Security. Requirements*, 2008.
5. ISO/IEC 27002:2005, BS 7799-1:2005,BS ISO/IEC 17799:2005. *Information technology. Security techniques. Code of practice for information security management*, 2005.
6. GOST (State Standard) *R ISO/MEK 31010-2011. Risk management. Risk assessment methods*, 2012.
7. *Standart TsB RF STO BR IBBS-1.0-2014. Obespechenie informatsionnoi bezopasnosti organizatsii bankovskoi sistemy RF. Obshchie polozheniya* (Standard TsB RF STO BR IBBS-1.0-2014. Ensuring of Information Security of Russian Federation Bank System Organization. The General Positions), Moscow, 2014.
8. *Standart TsB RF STO BR IBBS-1.2-2014. Obespechenie informatsionnoi bezopasnosti organizatsii bankovskoi sistemy RF. Metodika otsenki sootvetstviya informatsionnoi bezopasnosti organizatsii bankovskoi sistemy Rossiiskoi Federatsii trebovaniyam STO BR IBBS-1.0-2014* (Standard TsB RF STO BR IBBS-1.0-2014. Ensuring of Information Security of Russian Federation Bank System Organization. Methodology of Estimation of Information Security of Russian Federation Bank System Organization Correspondence to STO BR IBBS-1.0-2014 Requirements), Moscow, 2014.
9. *RS BR IBBS-2.2-2009. Obespechenie informatsionnoi bezopasnosti organizatsii bankovskoi sistemy Rossiiskoi Federatsii. Metodika otsenki riskov narusheniya informatsionnoi bezopasnosti* (Ensuring of Information Security of Russian Federation Bank System Organizations. Methodology of Estimation of Risks of Violation of Information Security), Moscow, 2009.
10. Tulup'eva, T.V., Tulup'ev, A.L., and Azarov, A.A., Psychological aspects of information safety assessment in the context of socio-engineering attacks, *Med.-Biol. Sots.-Psikhol. Probl. Bezop. v Chrezvych. Sit.*, 2013, no. 1, pp. 77–83.
11. Azarov, A.A., Tulup'ev, A.L., Solovtsov, N.B., and Tulup'eva, T.V., Acceleration of information system users' security assessment calculations due to elimination of unlikely trajectories of socio-engineering attacks, *Tr. SPIIRAN*, 2013, no. 2(25), pp. 171–181.
12. Zaitsev, A.S. and Malyuk, A.A., Study of the insider problem, *Vestn. Ross. Gos. Gum. Univ.*, 2012, no. 14(94), pp. 114–134.
13. Rytov, M.Yu. and Leksikov, E.V., Formalization of the process of evaluation of staff's loyalty to reduce information security risks, *Inform. Besop.,* 2014, vol. 17, no. 2, pp. 276–279.

14. Lukatskii, A.V., How to evaluate the awareness enhancing program? http://lukatsky.blogspot.ru/2011/08/blog-post_19.html.

15. Astakhova, L.V., Problem of identification and assessment of human resources vulnerability in the information security of the organization, *Vestn. Yuzhn. Ural. Gos. Univ. Ser. Komp'yut. Tekhnol., Upravl. Radioelektron.*, 2013, vol. 13, no. 1, pp. 79–83.

16. Dolgov, K.M., Human capital and culture, *Vestn. MGIMO-univ.*, 2013, no. 3(30), pp. 135–136.

17. Kuz'minov, Ya., Bendukidze, K., and Yudkevich, M., How the science of markets becomes a science about society, *Vopr. Ekon.*, 2005, no. 12, p. 73.

18. Kos'mina, E.A., Metelev, S.E., and Kos'min, A.D., *Kul'turnyi kapital obshchestva v real'nom materiale funktsioniruyushchei organizatsii* (Cultural Capital of the Society in a Real Material of a Functioning Organization), Moscow: Ekonomika, 2007.

19. Tikhomirova, O.G., *Organizatsionnaya kul'tura: formirovanie, razvitie i otsenka* (Organizational Culture: Formation, Development, and Evaluation), SPB: Izd-Vo ITMO, 2008.

20. Bourdieu, P., Forms of the capital. http://gtmarket.ru/laboratory/expertize/2009/2601.

21. Bol'shakov, N.V., Measurement of the cultural capital: from theory to practice, *Monit. Obshchestv. Mneniya: Ekon. Sots. Peremeny*, 2013, no. 6(118), pp. 3–12.

22. Gorbunova, S.V., Accumulation of the human capital in real economy workers, *Cand. Sci. (Econ.) Dissertation*, Yekaterinburg: In-t Ekon. UrO RAN, 2009.

23. Radaev, V.V., The concept of the capital, forms of the capital and their conversion, *Ekon. Sots.*, 2002, vol. 3, no. 4.

24. Samarina, I.S., Cultural capital of students in the conditions of Russia's transition to the innovative type of development: *Cand. Sci. (Soc.) Dissertation*, Saratov: Sarat. Gos. Sots.-Ekonom. Un-t, 2010.

25. Trosbi, D., Cultural capital, *J. Cult. Econ.*, 1999, no. 12.

26. Furs, V., Social theory in a changing world: Towards a dynamic concept of social? in *Sochineniya*, 2 vols., Vilnus: EGU, 2012, vol. 1, pp. 412–432.

27. Soboleva, I., Paradoxes of measuring the human capital, *Vopr. Ekon.*, 2009, no. 9, pp. 51–70.

28. Tolstobrov, G.M., Formation and evaluation of the intellectual capital in the information economy, *Cand. Sci. (Econ.) Dissertation*, Sankt-Peterburg, 2010.

29. Markaryan, K.V., Human capital in the post-industrial economy, *Extended Abstract of Doctoral (Econ.) Dissertation*, Moscow, 2005.

30. Kastryulina, Yu.M., Analysis of methods for assessing the human capital of economic entities, *Nauchn. Zh. NIU ITMO. Ser. Ekon. Ekol. Menedzhm.*, 2013, no. 1, p. 19.

31. Pliskevich, N.M., *Chelovecheskii kapital v transformiruyushcheisya Rossii* (Human Capital in Transforming Russia), Moscow: Institut Ekonomiki RAN, 2012.

32. Shash, N.N., Development of human capital in organization: Theory and methodology, *Doctoral (Econ.) Dissertation*, Saratov, 2006.

33. Puzikov, V.G., Person: Socio-cultural criteria of measurement, *Nauka o Cheloveke: Gum. Issled.*, 2013, no. 4(14), pp. 111–118.

34. Babenko, I.A., Institutionalization of human capital in the current socio-economic system of Russia, *Cand. Sci. (Soc.) Dissertation*, Belgorod, 2012.

35. Danilkova, M.P., The concept of the value theory from the standpoint of dialectical methodology, *Cand. Sci. (Philos.) Dissertation*, Novosibirsk, 2008.

36. Molodykh, E.N., Relationship of estimates of the organizational culture and attitudes of staff to comply with ethical standards of business behavior, *Cand. Sci. (Psychol.) Dissertation*, Moscow, 2009.

37. Lebedeva, N.M. and Tatarko, A.N., Values and social capital as a basis for socio-economic development, *Zh. Inst. Issled.,* 2010, vol. 2, no. 1, pp. 17–34.

38. Samarina, I.S., Cultural capital of students in the conditions of Russia's transition to the innovative type of development, *Cand. Sci. (Econ.) Dissertation,* Saratov, 2010.

39. Astakhova, L.V., The concept of the information-security culture, *Sci. Tech. Inf. Process.*, 2014, vol. 41, no. 1, pp. 22–28.

40. Pirozhkova, N.I., Assessment of the human capital of the enterprise, *Cand. Sci. (Econ.) Dissertation*, Moscow, 2012.

41. Tolstova, Yu.N., *Izmerenie v sotsiologii: uchebnoe posobie* (Measurement in Sociology: Textbook), Moscow: KDU, 2007.

42. Zinov, V.G., *Upravlenie intellektual'noi sobstvennost'yu* (Intellectual Property Management), Moscow: Delo, 2003.

43. Gaponenko, A.L. and Orlova, T.M., *Upravlenie znaniyami: Kak prevratit' znaniya v capital* (Knowledge Management: How to Turn Knowledge into Capital), Moscow: Eksmo, 2008.

Translated by A. Kolemesin