Modern Applied Science; Vol. 9, No. 5; 2015
ISSN 1913-1844 E-ISSN 1913-1852
Published by Canadian Center of Science and Education

Research of Human Factors in Information Security

Boris Ivanovich Skorodumov[1], Olga Borisovna Skorodumova[2] & Liliya Fedorovna Matronina[3]

[1] Department of Information Security, Russian new university, Moscow, Russian Federation

[2] Department of Philosophy, Russian State Social University, Moscow, Russian Federation

[3] Department of Philosophy, Sociology and Political Science, Moscow State Technical University of Radio Engineering, Electronics and Automation, Moscow, Russian Federation

Correspondence: Skorodumov Boris Ivanovich, 307 Apartment, 37/21, Marshal Tukhachevsky str., Moscow, 123154, Russian Federation. Tel: 7-916-964-8827. E-mail: bisko2003@list.ru

Received: December 16, 2014 Accepted: December 29, 2014 Online Published: April 7, 2015

doi:10.5539/mas.v9n5p287 URL: http://dx.doi.org/10.5539/mas.v9n5p287

Abstract

The article represents results of research of information security problem in social and human aspects. Authors assume that information sciences are usually focused on detecting and further processing of technical mechanisms and tools for support of information security. However, the analysis of social and human factors influencing growth of criminality in the field of information technologies, search for complex measures and methods aiming to decrease human risks arising from computer criminality is very important as well. One of solutions for information security problem in credit and financial spheres is shown on the example of bank system of Russia. Special attention is drawn to analysis of specificity and dynamics of hacker subculture, its place in cybercrime, taking into account interdisciplinary direction of research of the information security problem. The authors of the article came to the conclusion that early detecting and studying existing and potential threats, notifying system administrators and other technical personnel on such threats and coordinating their activity, as well as cultural and educational policy of states and international communities aiming to create a positive information security expert image, are very important for the information security support.

Keywords: information security, information protection, cybercrime, insider, confidential information, hacker, hackers' subculture, support of information security

1. Introduction

Modern processes of electronic communication development in the society result in need for research of features and development of information technologies (IT) and their influences on all life spheres of society and person. While opening incredible, new opportunities, innovative technologies generate new problems and risks at the same time. Today information security turns to be one of the global problems of humanity getting more and sociological, political, and human character, since necessity to protect a person and a whole society in information sphere increases.

Inherently the problem of information security support is interdisciplinary and requires joint efforts of experts of various scientific directions. "Fighting to close the gap. Key findings from EY's, Global Information Security Survey 2012" and a number of experts' researches in the field of information security (Mitnick et al., 2003; Streltsov, 2001; Streltsov, 2002; Rastorguev, 2009) note that increase in numbers of computer crimes cannot be stopped only by technical means. Many well-known experts in the field of information security including former hackers emphasize the necessity to take into account social and human factors influencing crime dynamics in the field of information security (Mitnick, 2005; Levin, 2006; Appelbaum et al., 2014). Monitoring of hackers' publications on specialized sites (for example Internet portal "Art of information security management ". Hackers' sites. Catalogue: http://www.iso27000.ru/katalog-ssylok/hakerskie-saity), as well as analysis of character and subjects of their presentations at annual international Defcon conference in Las Vegas (USA) allow to determine the trend of expansion of social engineering methods when preparing invasions and break-ins. A. Cole (Cole, 2006), expert in the field of information security technologies (IT) reveals dangers the corporations and state bodies have to face as a result of insider attacks. The expert proposes effective methods for creation of safety system providing protection of enterprise and corporation from possible damage to the organization infrastructure.

The essence of any crime is connected with general social and cultural background, which constrains and/or

provokes criminality. That is why the analysis of information security in a context of specificity of the modern society and its culture is urgent. Definition of features of modern society in scientific literature has a tendency to interpret it like a risk society (Giddens, 1999; Beck & Grande, 2010; Bechmann, 2010). G.Bechmann stresses that the process of revealing preconditions of risk involves the risk caused by activity of people choosing alternative solutions and calculating degrees of outcome's possibility and the risk caused by general social and economic situation. The situation paradoxicality consists in the fact that modern technologies increase both safety and unreliability. The person has to make a decision in conditions of uncertainty. Hence, human assessment of technical and technological innovation and its risky components and possibilities is one of the key problems (Bechmann, 2010).

A number of researches (Grachev, 2009; Astakhova, 2010; Novikov, 2011; Linebardger, 2013) is devoted to analysis of "social hacking" strategy. These researches emphasize the analysis of general strategy using psychological manipulation. Minor attention is drawn to the research of application of these techniques when preparing hacker attacks. Alongside with it the above-mentioned researches study influence of modern society dynamics on formation of hackers' subculture (Castells, 2001; Himanen, 2001; Castells & Himanen, 2002; Gehring, 2004; Skorodumova, 2004). Moreover some authors come to conclusion that hackers' activity meets the interests of society (Gehring, 2004).

Despite of considerable interest from the side of scientists to this problematics there is a number of questions requiring further studying and concerning information security and its human component. This is connected with many difficulties. On the one hand, a borderline character of problematics of both technical and humanitarian knowledge complicates development of information protection measures. On the other hand, it is difficult to get empirical material because there is "closed" information, accessible to information security experts only, subjects of computer crimes (insiders, hackers), and their objects - defrauded enterprises and organizations. As a rule, they do not publish any data neither about motives and techniques of attacks, nor about facts of attacks and their consequences.

Taking into account the level of research of this problem, the focus of the authors on studying of techniques and ways of information protection from insight applied by various corporations, which experience can be used by other organizations. Particularly we present analysis of one method for solving of information security problem in credit and financial sphere on the example of bank system of Russia. Revealing a human component of information security the article contains analytical review of hackers' subculture and assessments of their activity. The role of education in formation of values for experts bearing social responsibility for their activity is determined.

2. Method

The basic methods of research used in the article include both general scientific and particular scientific methods: method of system analysis, method of comparison and analogies, analytical method of operational risks assessment, etc. The executed analysis of information protection of various corporations both in the Western countries and in Russia make it possible to create a number of effective proposals, which have a practical orientation and can be recommended for implementation. At the same time, the authors used a method of historical sociology of concepts developed and actively applied for analysis of society dynamics (Lehmann and Richter, 1999; Bibkov, 2014). The research of dependence between change of concept's semantic content and orientations transformation and value system of hackers was carried out on the base of context use of "hacker" term in scientific editions, mass media, and youth culture. Further correlation between changes of essential attitude of society and activity and motivation of hackers was revealed being supported by functional analysis system technique. Social and culture determinants of increment in hackers' activity were studied and allowed to compose a number of recommendations for introduction of socially focused measures directed on decrease of cyber-crime.

The analysis of human factor of information security was carried out on the basis existing scientific researches in this field and real practical results of using automated systems for prevention of security leakages of some Russian corporations and international organisations. Models and programs of training, as well as tools for increase of awareness about insider risks and for identification of factors, which motivate insiders were determined. Countermeasures for protection of organization against insider attack were proposed (on the example of bank system of Russia). Social and humanitarian factors promoting hackers' subculture were revealed. It was proved that early detection and studying of existing and potential threats, notification of system administrators and other engineering staff about these threats, as well as coordination of their activity are of great importance for solving the problem of information security. Alongside with it cultural and educational policy of states and international communities directed on creation of positive image of information security expert plays critical part as well.

E.Laszlo (Laszlo, 2002) calls transformation of humane processes happening now a "macroshift". The scientist reckons this transformation to be caused by development and wide introduction of information technologies. Researchers note that change of technologies and innovations in a society is accelerated, so programming technologies and technical means get out of date within five years only (Castells, 1996). Experts rate changes in society connected with innovation to be serious, when more than 50 million users use this innovation. On the example of international network of PricewaterhouseCoopers (PwC) company, it was shown that introduction terms of innovative solutions and intellectual changes (Skorodumov, 2004) decrease. The National Intelligence Council (NIS) of the USA published "Mapping the global future: Report of the National Intelligence Council's 2020 Project, 2005" document where special attention was drawn to irreversibility of globalized processes caused by information and technical revolution.

The basis economic activity in the information society is creation and application of information and knowledge used for effective functioning of other kinds of production and consumption. Knowledge and information involved in practical processing of resources become valuable and turn into the intellectual capital used for creation of values (Stewart, 2007). T. Stewart, the American economist and journalist considers the intellectual capital to be the result of interaction between human, structural and consumer capitals reflecting intellectual resources of a certain enterprise. The structural capital is non-material asset (knowledge and information) which belongs to the enterprise and is reproduced and distributed by it. The consumer capital determines relations between the enterprise and consumers, the level of their satisfaction. The researcher especially marks economic value of human capital, which is a source of modifications and progress source when considering intellectual capital. The human capital is shown in the form of brainstorm, laboratory researches, etc.

Formation of global information space is connected with risks constantly. The resolution "Creation of global culture of cyber-safety and protection of critical infrastructure information" was adopted 57th session of General Assembly of the United Nations (21.01.2003). This resolution stresses growing dependence of state structures, business concerns, and individual users from innovations in the field of information technologies when exchanging goods, services, and information. As a result necessity of protection and support of information security increases in process of the growing involving of countries into information society.

Being a social phenomenon, information security designates security of society's information environment. It is directed on support of its formation and development of strategies for the benefit of individual users, enterprises, and states. It is necessary to mention the following issues among the basic problems of information security: prevention of unauthorised access to confidential information; prevention of use of personal data to the detriment of certain person, social group, state; prevention of cyber-crime; protection of copyrights; prevention of mental frustration and technical stress of computer users; prevention of limited access to information and freedom of its distribution, etc.

Unauthorized actions of insiders, i.e. groups of people, employees of a company having access to "protected" information represent threats for the Russian companies in the XXI century. Such people have a wide access to confidential information about company's safety methods, restricted data and computer systems, and pilfer such information. Insider attacks are malicious threats for the company including fraud, pilfering of confidential and commercially valuable information, theft of intellectual property, sabotage of computer systems. Information leakages damage the company in all aspects. Even big and successful companies are not protected against insiders, which are proved by reports about leakages published in print media from time to time (Skorodumov, 2004).

British company Ernst&Young (EY), leader in the field of audit and consultation, made a report "Global Information Security Survey 2005" called "Report on Widening Gap" (2005). The main conclusion, which the experts came to is the fact that risks in the process of business development evolve very quickly, and experts of information security do not always have time to respond to them. A similar publication was published in 2012 - "Fighting to close the gap" (Key findings from EY's, Global Information Security Survey, 2012). Verizon, the American telecommunication company has recently presented another one report about computer safety called "2014 Data Breach Investigations Report (DBIR) <http://www.verizonenterprise.com/DBIR/2014/>". The report combines data about 50 international organizations and contains facts of numerous confirmed security incidents. In DBIR, the experts analyse data about violations in 27 countries in 2013 and come to conclusion that no one is impervious to problems of computer safety. The data presented in DBIR shows that: 1) 50 % of violations were made by the former employees who used old connections or ports, which were not disconnected; 2) more than 70 % of Internet thefts were made by the internal personnel.

The problem of protection of information against leakages is urgent in Russia as well. Authors of research of the Russian company INFOWATCH (Insider Threat, 2013) stated the essential similarity of leakages in the world.

Materials of this enterprise prove that the Russian incidents of information leakages are similar to the American ones. Electronic document circulation in Russia results in the use of another's personal data in own purposes. Many companies and enterprises, which are engaged in information security collect such information from print media and other sources for getting of valid quantitative characteristics of processes happening at informatisation of society. Reviews of incidents happening at business automation serve as a basis for reasoning of specific technical solutions in the field of security. The information analysis contains a set of components: collecting of full statistics, trending, etc. The database consists of public reports on incidents from commercial and non-commercial (state, municipal) organizations. This method of research field formation allows to consider created sample as theoretical, and conclusions of experts and revealed trends as representative for the whole complex. Other companies use similar techniques of information processing, but do not pay due attention to their description. Today the Russian companies pay much more attention to means of control automation and protection against internal information threats or Data Loss Prevention (DLP).

The bank system of Russia is a positive example of complex solution for information security problem. The Russian bank system has recently started to publish materials about incidents while transferring money on open access (Bank of Russia. Analytical review …, 2013). Let us see the incidents in table 1 taken from the specified review, as an example.

Table 1. Share of incidents according to types of their consequences, in percentage of total

	Incident consequence	Share in total of incidents
1.	Influence of malicious code resulted in failure of regular functioning of computer and infringement of money transfer services or delay of money transfer.	0,4%
2.	Actions aiming to create impossibility of money transfer or delay of money transfer.	1,2%
3.	Breach of information confidentiality necessary for operators for confirmation of the right of disposal of money by clients when transferring money.	27,1%
4.	Discredit of critical information of cryptographic means of information protection applied at money transfer.	7,5%
5.	Transfer of money to persons without right of disposal of these money means.	46,8%
6.	Influence of malicious code resulted in incidents	4,4%

Based on requirements of the Federal law "On personal data" and requirements (recommendations) of the Federal Service for Supervision of Communications, the Bank of Russia together with Association of the Russian banks developed branch documents bringing of the bank system to conformity with applicable legal requirements in the field of personal data. A complex of documents in the field of standardization of Bank of Russia was adopted. These documents regulate and normalize assessment methodology for information security incidents. Unnormalised initial data and algorithm of incidents' assessment of various companies lead to scatter of received results and complicate comparative analysis of their final conclusions, but are generally quite sufficient for assessment of trends of processes development (Pyarin et al., 2002; Yarochkin and Buzanova, 2005; Skiba, Kurbatov, 2008). It is assumed that in some years, when factual database of incidents of Bank of Russia becomes mature (representative) and efficient enough, its materials can be used for forecasting of processes. In any case, the presented material forms a good base for information and helps to reason the made decisions. Now we can generalize results from various sources using statistical materials and choosing data with the maximum mutual correlation.

The experience of confidential information protection exists in other countries as well. For example, CERT (CERT/CC) coordination centre was founded and is now working in the USA taking into account necessity of information protection. Thereupon special attention shall be drawn to the brochure published by Software Engineering Institute according to CERT materials with presentation of empirical studies of fighting against insider cyber threats carried out by CERT Insider Threat Centre (Insider Threat, 2013). CERT research project is based on studying of real incidents (Cummings et al., 2012). The presented materials prove that the share of internal threats makes more than 70 % of information security incidents.

Usually when considering illegal use or theft of computer information and cyber-crime as a whole responsibility is laid on hackers. Moreover, at the same time some researchers wonder, "Do hackers render a good service to the society?". Thus, such researches believe the hackers are moved by curiosity, sound scepticism, independence, and responsibility (Gehring, 2004). "Rehabilitation" of hackers proposed by V.Gehring is connected with

distinction between "hackers" whose activity is directed on creation, and "crackers" whose activity is directed on destruction.

When we consider etymology of English word "hack", it is necessary to note that initially it had dual semantic content. On the one hand, it contains sense connected with destruction - to split, to cut to pieces, and on the other hand it is connected with creation - to cut out, to chisel some figure by axe out. This ambivalence was reflected on interpretation of the word "hacker" at initial stages of formation of information technologies experts community and perception of "self" as unitary whole. In 60th of the XX century people called programmers with non-standard, creative solutions connected with change of system in order to open its potential possibilities or solving of complex, unmanageable problems (Barlow, 1996) "hackers". Belonging of early hackers to the upper class of technical intellectuals promoted ideas of chosenness, formed a special consciousness type of "builders" of a new type of free society, virtual environment based on ideas of equality, disinterestedness, collective creativity (Barlow, 1996).

This idealisation of virtual space, belief that accessibility of any information without any restrictions will promote perfection of Internet users, will enrich them intellectually and spiritually, and availability of information resources will make it possible to incarnate direct democracy and to level down stratified differences, in reality proved to be absolutely illusive. Disappointment and realization of impossibility to implement previous ideals led to increase of aggression, protest movements among hackers. The number of hacker invasions into system aiming not to research and improve it, but to damage the system (theft of information and creation of malicious programs) increased already in the late 70th - at the beginning of the 80th of XX century. The extensive use of computers in this period resulted in blurred social structure of hackers. Earlier hacker community consisted, basically, of teachers and students of elite educational institutions. Onwards more and more amateur programmers aimed to boost own social status and prestige even by committing cyber-crimes. Commercialization of the Internet, tough competition among computer enterprises producing incompatible software stimulated growth of cracks' quantity. Hackers' subculture lost unity of world outlook and values, and became amorphous from social and psychological points of view. Increased interest to hackers from mass media, creation of superhero image promoted growth of cracks for the sake of popularity and fame.

Organizational formation of hacker structures, on the one hand, and counteracting state and international organizations on the other hand began in 80-90th of the XX century. The first large hacker organizations, such as "Legion of Doom" (USA) and "Chaos Computer Club" (Germany) were founded. The first hacker manifests (Levy, 1984) were composed. These manifests defined criteria of hacker behaviour: unlimited access to computers allowing to create works of art and to improve the life. There is an ethical problem of contingency of free access to information and possibility to do harm by the actions (wilful or unintentional). At the same time, active fighting against hackers at level of state structures began. Let us see some data. Computer crimes were defined and classified in 1979 in Dallas (USA) for the first time. In 1989, the European Union (EU) agreed upon the "Minimum list of violations" characterizing computer crimes. At the same time, the Federal bureau of investigations (FBI, USA) developed and adopted "Matrix of cyber criminals" which comprehensively classified their types. The task group on cyber-crimes was created in 1991 based on the Interpol. "P" bureau for fighting against cyber-crimes was created at the Ministry of Internal Affairs in 1997 in Russia. In 2001 the National centre of infrastructure protection of the USA published the report "Cyber Protests: The Threat to the U.S. Information Infrastructure" (Grinyaev, 2002). The adopted documents mention increase of coordination of hacker actions, system preparation of cracks, their preparatory modelling and testing, careful development of all details in order to organize as fast invasion as possible and careful deletion of all data about location and person of the hacker. When preparing attacks hackers widely use methods of social engineering: they investigate personality characteristics of system administrators or employees closely connected with attacked system, their cultural and religious orientations, professional dissatisfaction, marital status, foibles in private life, etc. The hackers widely use blackmail, deceit, frame-up, and imitation of rank statuses in order to get necessary information (Mitnick and William, 2003).

The XXI century begins with institutionalization of hackers at a new level. There are large network associations, for example, Anonymous with mobile and flexible structure similar to social networks. The special news media popularising hacker subjects are created: magazines: "Old and New Hackers", "Crypt NewsLetter's Home Page", "Access All Areas", "Chaos Computer Club", "Hacker rings", "Hackzone", etc. Hacker meetings are held regularly and draw attention of both representatives of law enforcement bodies aiming to recruit hackers, and of criminal structures striving to win hackers on their side. Some famous meetings are Defcon in Las Vegas, "Hackers At Large" in Holland, "Chaos Computer Club" in Germany. Mass media promoted popularizations of hackers as well. A great variety of films ("The Fifth Estate", "Live Free or Die Hard", "Hackers", "Skyggen" and

others) present hacker as an admirable hero. Idealisation and attractiveness of hacker's image was caused by the tendency that after jail release many talented hackers were invited to take responsible and well-paid positions at departments of information security of large enterprises. For example, after jail releases Kevin Mitnik became not only a well-known expert in the field of information security, but also popular writer whose books are translated into many languages. The president and founder of "Chaos Computer Club" Andy Muller-Meghan became a member of ICANN organization (Internet Corporation for Assigned Names and Numbers).

One of important factors influencing growth of cyber-crimes is attitude to the risk created in culture of information society. Dynamics of changes, which are typical for modern society lead to demand of risk. Studies of the end of XX - beginnings of XXI centuries devoted to analysis of information epoch specificity determine dependence from risk as one of essential marks of the modern society (Giddens, 1999; Beck & Grande, 2010; Bechmann, 2010). The risk is considered as possibility of innovative break and threat to security at the same time. Nonlinearity and uncertainty of economic and technological processes cause social uncertainty, which is reflected on political instability. Propagation of protest movements in the conditions of developed information infrastructure causes responses in a form of cyber-attack. This trend can be well traced on activity of "Anonymous" - group of hactavists who organized a number of successful attacks to sites of companies counteracting Wikileaks. Hacker attack to the state sites of Estonia in 2007, creation of "Cyber-berkut" in 2014 are also connected with political instability. In many respects the future of hacker activity and methods depend on tension in a society (Olson, 2012; Stryker, 2012). Thus, hacker activity is correlated with a society's condition. In these conditions, decrease of risks for information security is connected with complex measures for improvement of both psychological climate in companies and corporations reducing number of dissatisfied employees, and of large-scale measures for reduction of tension in the world.

Cultural and educational policy creating positive images of information security expert, discrediting a romantic image of hacker are very important. Traditional (classical) education system is significantly transformed in information society. This system shall be directed on formation of an expert who can freely orientate in information, has cognitive abilities and critical mind, and is able to implement his knowledge, to choose proper ways and methods of solution, to create new important forms, to establish relations and contacts, to work in a team. One of critical features of the modern education is its quality, which shall correspond to international and regional educational standards, personal and public requirements. Quality of education turns to be imperative of modern times defining educational attitude of education subjects, goals and tasks in the field of education taking into account their importance in sociocultural context, as well as strategy of training(Tawil et al., 2012; Matronina, 2014). Morale building activities in educational institutions, involvement of teenagers and youth to cooperation with companies on information protection, providing them with possibilities for creativity and status increase can essentially reduce cyber-crimes. This is proved by experience of Finland (Castells & Himanen, 2001). Ease of manufacturing, reliability of projects, efficiency of results etc. form important criteria of any practically reformative activity from the point of view of goal achievement. Nevertheless, such an activity becomes important and valuable only when we consider a social space of human, spiritually moral "climate" promoting development of integrated personality.

3. Results

The undertaken research showed that early detection and studying of existing and potential threats, notification of system administrators and other technical personnel about these threats and coordination of their activity on the one hand, and cultural and educational policy of states and international communities directed on creation of positive image of the information security sphere. On the other hand are of great importance for solving information security problems. When studying prospects of solving of information security problems, it is necessary to mention that this activity is directly connected with development of information sphere as backbone factor of society's life and maintenance of cultural and moral values in the conditions of world globalization. Thus, normative and technical support of information security of a person and society in information sphere, as well as legislative regulation of relations in the field of creation and use of modern information technologies are essential. Problems of formation of integrated personality, spiritual and moral values promoting critical reasoning and creative potential emerge full-blown. Scientific and theoretical analysis of human factor of information security with use of empirical material allowed to create a number of proposals and recommendations with are practical orientated and can be implemented by organizations/corporations interested in protection of information.

Acknowledgments

Authors would like to express special gratitude to colleagues and friends for their helpful comments and critical

remarks concerning this article: Veligura Aleksander Nikolaevich, Malyuk Anatoly Aleksandrovich, Mamykin Vladimir Nikolaevich, Otyutsky Gennady Pavlovich, Skorodumov Oleg Borisovich, Streltsov Anatoly Aleksandrovich.

References

Appelbaum, J., Assange J., Muller-Maguhn, A., & Zimmerman, J. (2014). Cypherpunks. Freedom and future of the Internet. Moscow: Azbuka Biznes, Aznuka-Attikus.

Astakhova, L. V. (2010). Information security: Hermeneutical approach. Moscow: Russian Academy of Sciences

Bank of Russia. Analytical review of incidents connected with violation of requirements for support of information security when transferring money (the first half of the year, 2013). Retrieved from http://www.cbr.ru/PSystem/analytics/analysis_13_1.pdf

Bechmann, G. (2010). Modern society: risk society, information society, knowledge society. Moscow: Logos

Beck, U., & Grande, E. (2010). Varieties of second modernity: The cosmopolitan turn in social and political theory and research. *The British Journal of Sociology, 61*(3), 406-638.

Bikbov, A. T. (2014). Grammar of the order: historical sociology of concepts which changes our reality. Moscow: Higher school of economy.

Castells, M. (1996). The Information Age: Economy, Society and Culture. Vol. I-III. Oxford: Blackwell Publishers.

Castells, M. (2001). The Internet Galaxy. Reflections on the Internet, Business and Society. Oxford UP.

Castells, M., & Himanen, P. (2001). The Hacker Ethic and the Spirit of the Information Age (prologue by Linus Torvalds and epilogue by Manuel Castells). New York, NY.: Random House.

Cole, E. (2006). Insider Threat. Protecting the Enterprise from Sabotage, Spying and Theft. Syngress.

Creation of global culture of cyber-safety and protection of critical infrastructure information (2003). Resolution of General Assembly of the United Nations. Retrieved from http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N02/555/24/PDF/N0255524.pdf?OpenElement

Cummings, A., Lewellen, T., McIntire, D., Moore, A. P., & Trzeciak R. (2012, July). Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector. SPECIAL REPORT. Carnegie Mellon University.

Data Breach Investigations Report. (2014). Retrieved from http://www.verizonenterprise.com/DBIR/2014/

EY Global Information Security survey 2005. Retrieved from http://www.diit.unict.it/users/otomarch/Corsi/Sicurezzaocs/EY_Global_Information_Security_survey_2005.pdf

Gehring, V. V. (Ed.) (2004). The Internet in public life. Rowman & Littlefield Publishers.

Giddens, A. (1999). Runaway World: How Globalization is Reshaping Our Lives. London: Profile.

Global research of leaks of the corporate information in a bank segment (financial and credit institutions) the 1st half-year of 2012. Retrieved from http://www.infowatch.ru/analytics/reports/2758

Grachev, V. (2009). Personality and society: information and psychological safety and psychological protection. Moscow: SE.

Insider Threat (Brochure) (2013). Software Engineering Institute. Retrieved from http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=52375

Internet portal "Art of information security management". Hackers' sites. Catalogue. Retrieved from http://www.iso27000.ru/katalog-ssylok/hakerskie-saity

Key findings from EY's, Global Information Security Survey. Fighting to close the gap. (2012). Retrieved from http://www.ey.com/Publication/vwLUAssets/GISS2012/$FILE/EY_GISS_2012.pdf

Laszlo, E. (2002). Macroshift Navigating the Transformation to a Sustainable World. Berrett, Koehler Publishers.

Levin, M. (2006). Hacker's bible. Moscow: Major.

Levy, S. (1984). Hackers: Heroes of the Computer Revolution. Anchor Press/Doubleday.

Linebardger, P. (2013). Psychological war. Theory and practice of processing of mass consciousness. Moscow:

Tsentropoligraf.

Mapping the global future: Report of the National Intelligence Council's 2020 Project. (2005). University Press of the Pacific.

Matronina, L. F (2014). Quality of education as imperative of the modern times. *Philosophy of education, 1*, 11-19.

Mitnick, K., & Simon, W. L. (2005). The Art of Intrusion. John Wiley & Sons.

Mitnick, K. D., Simon, W. L., & Wozniak, S. (Foreword by) (2003). The Art of Deception: Controlling the Human Element of Security. Wiley Books.

Novikov, V. K. (2011). Information weapon - the weapon of modern and future wars. Moscow: Goryachaya liniya – Telekom.

Olson, P. (2012). We Are Anonymous: Insid the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency. Little, Brown and Company.

Pyarin, V. A., Kuzmin, A. C., & Smirnov, S. N. (2002). Safety of electronic business. Moscow: Gelios ARV.

Rastorguev, C. P. (2009). Bases of information security. Moscow: Akademiya.

Skiba, V. Yu., & Kurbatov, V. A. (2008). Manual for protection against internal threats of information security. St.-Petersburg: Piter.

Skorodumov, B. I. (2004). Information security of modern commercial banks. *Information society, 6*, 41-45. Retrieved from http://emag.iis.ru/arc/infosoc/emag.nsf/BPA/8d73ebf2029e2730c32571780046f676

Skorodumova, O. B. (2004). Hackers as phenomenon of the information field. *Sociological researches, 2*, 70-79.

Stewart, T. (2007). Intellectual capital. The new wealth of organization. Translation from English, Moscow: Pokolenie.

Streltsov, A. A. (2001). The essence of «support of information security» concept. *Information society, 4*, 10-16.

Streltsov, A. A. (2002). Support of information security of Russia. Theoretical and methodological bases. Moscow: MCNMO.

Stryker, K. (2012). Hacking the Future: Privacy, Identity, and Anonymity on the Web. Duckworth Overlook.

Tawil, S., Akkari, A., & Macedo, B. (2012). Beyond the Conceptual Maze. The notion of quality in education. UNESCO Education Research and Foresight. Occasional papers. Retrieved March 2, 2012, from http://unesdoc.unesco.org/images/0021/002175/217519e.pdf

Verizon's 2014 Data Breach Investigations Report (DBIR). Retrieved from http://www.policypatrol.com/verizons-2014-data-breach-investigations-report/

Yarochkin, V. I., & Buzanova, Ya. V. (2005). Audit of enterprise safety. Moscow: Academic project; Korolev: Paradigma.