VILNIUS UNIVERSITY

SAULIUS JASTIUGINAS

INFORMATION SECURITY MANAGEMENT: THE STUDY OF LITHUANIAN STATE INSTITUTIONS

Summary of the Doctoral Dissertation
Humanities, Communication and Information (06 H)

Vilnius, 2012

The thesis was written in 2008–2012 at Vilnius University

Academic Supervisor:
Prof. Dr. Zenona Atkočiūnienė (Vilnius University, Humanities, Communication and Information – 06 H)

Academic Adviser:
Assoc. Prof. Dr. Povilas Abarius (Vilnius University, Humanities, Communication and Information – 06 H)

The dissertation will be defended at the Council on Communication and Information Sciences of Vilnius University:

Chairperson:

Prof. Habil. Dr. Narimantas Kazimieras Paliulis (Vilnius Gediminas Technical University, Social Sciences, Management and Administration – 03 S)

Members:

Prof. Dr. Zenona Atkočiūnienė (Vilnius University, Humanities, Communication and Information – 06 H)
Assoc. Prof. Dr. Rimvydas Laužikas (Vilnius University, Humanities, Communication and Information – 06 H)
Assoc. Prof. Dr. Renata Matkevičienė (Vilnius University, Humanities, Communication and Information – 06 H)
Prof. Dr. Rimantas Petrauskas (Mykolas Romeris University, Social Sciences, Management and Administration – 03 S)

Opponents:

Prof. Dr. Marija Stonkienė (Vilnius University, Humanities, Communication and Information – 06 H)
Prof. Dr. Rimantas Gatautis (Kaunas University of Technology, Social Sciences, Management and Administration – 03 S)

The dissertation will be defended at the public meeting of the Council on Communication and Information on December 20, 2012, at 10 a.m. lecture-hall 315 at Faculty of Communications, Vilnius University.
Address: Saulėtekio al. 9, I building, 10222, Vilnius, Lithuania

The summary of the dissertation was sent out on November 20, 2012.
The dissertation is available for public access at the Library of Vilnius University.

VILNIAUS UNIVERSITETAS

SAULIUS JASTIUGINAS

INFORMACIJOS SAUGUMO VALDYMAS: LIETUVOS RESPUBLIKOS VALSTYBĖS INSTITUCIJŲ ATVEJIS

Daktaro disertacijos santrauka
Humanitariniai mokslai, informacija ir komunikacija (06 H)

Vilnius, 2012

Disertacija rengta 2008–2012 metais Vilniaus universitete.

Mokslinė vadovė:
Prof. dr. Zenona Atkočiūnienė (Vilniaus universitetas, humanitariniai mokslai, komunikacija ir informacija – 06 H).

Mokslinis konsultantas:
Doc. dr. Povilas Abarius (Vilniaus universitetas, humanitariniai mokslai, komunikacija ir informacija – 06 H).

Disertacija ginama Vilniaus universiteto Komunikacijos ir informacijos mokslo krypties taryboje:

Pirmininkas:

Prof. habil. dr. Narimantas Kazimieras Paliulis (Vilniaus Gedimino technikos universitetas, socialiniai mokslai, vadyba ir administravimas – 03 S).

Nariai:

Prof. dr. Zenona Atkočiūnienė (Vilniaus universitetas, humanitariniai mokslai, komunikacija ir informacija – 06 H);
Doc. dr. Rimvydas Laužikas (Vilniaus universitetas, humanitariniai mokslai, komunikacija ir informacija – 06 H);
Doc. dr. Renata Matkevičienė (Vilniaus universitetas, humanitariniai mokslai, komunikacija ir informacija – 06 H);
Prof. dr. Rimantas Petrauskas (Mykolo Romerio universitetas, socialiniai mokslai, vadyba ir administravimas – 03 S).

Oponentai:

Prof. dr. Marija Stonkienė (Vilniaus universitetas, humanitariniai mokslai, komunikacija ir informacija – 06 H);
Prof. dr. Rimantas Gatautis (Kauno technologijos universitetas, socialiniai mokslai, vadyba ir administravimas – 03 S).

Disertacija bus ginama viešame Komunikacijos ir informacijos mokslo krypties tarybos posėdyje 2012 m. gruodžio mėn. 20 d. 10 val. Komunikacijos fakulteto 513 aud.
Adresas: Saulėtekio al. 9, I rūmai, 10222 Vilnius, Lietuva.

Disertacijos santrauka išsiuntinėta 2012 m. lapkričio mėn. 20 d.
Disertaciją galima peržiūrėti Vilniaus universiteto bibliotekoje.

Summary

Relevance of the subject. Information security and its urgency relate to the prime requirements while working with the information. From the early beginning of the writing days people were looking for the means, resistant to time and natural phenomenon in which to record the information. When the need of transmission of information rose, almost simultaneously the need to ensure that it reached only those whom it was intended emerged. Hereby crypto graphical security measures began to develop. The first chroniclers, librarians and workers of the archives can be ascribed to the developers of information security, e.g. they used wax stamps in order to prevent and note illicit approach to the information; codes – to protect from the revealing of information; making of copies – to avoid the loss of information (Denning, 1999; Lomas, 2010; Rusell and Gangemi, 1999).

The content of the information security significantly changed when computers and other information technologies were developed. The first computers, although used inasmuch in national security and in complex commercial matters, were not considered neither the security problem nor its solution. One user for a particular task usually used these computers. Therefore after the user finished the job, the main attention was focused on the physical security of the information medium (magnetic tapes, punch cards) and the premises in which the computer systems were held (the locking up). The first information security problems arose after the nature of the computer usage had changed in 1960 when the first personal computers appeared and new technologies permitted to use the same computer for several users to perform various calculations at the same time and even more after the development of the computer nets (Brinkley and Schell, 1995).

Information security problems in modern society are becoming critical. In the second half of the XXth century the ever rising need to control the information and knowledge with the help of modern technologies and management methods, predetermined that more and more information and every day performance processes migrated into the global electronic space. Dynamic changes transformed the society into an extremely dependant on the reliable functioning of information processing technologies. Any functioning perturbations of these technologies affect not only a single individual or organization, but also the whole social and economic life. Spam, viruses, malware, breaking into the information systems, trouble shooting of web sites, identity or business information thefts, leakage of information (e.g. Wikileaks) or millennium mistake (Y2K) elicited global flurry are becoming a recent point at issue (Amaral, 2007; Atkočiūnienė, 2009; Kuttschreuter, Gutteling, 2004).

Affluence of information security problems evoked the need of security management. Relating documentation was prepared - examples of good practices, assessment methods and recommendations for special business areas, a number of internationally recognized security management standards. Based on these documents organizations are provided a methodological help to apply an integrated and acting in concern information security management methods and technologies to follow the best practices and to correspond legitimate demands (Amaral, 2007; Gorge, 2009; Weise, 2009). The practice shows that individuals or organizations not always are willing or are able to solve the emerging security problems. Thus the public authorities' intervention becomes essential. Countries that recognized the importance of information security issues and their management (e.g. USA, the Great Britain, Japan, Austria and others) identified mandatory information security requirements for organizations or special activity, administering a sensitive information (personal, health, financial or military data, etc). These requirements often are based on entrenched good practices and (or) international information security management standards.

Despite the attempts to solve the arising information security challenges, recent years tendencies show that information security becomes a global issue that can be illustrated by the continually growing number and scale of information security incidents. These incidents threaten not only to separate organizations or countries but to the global cyber space. Worldwide web infrastructure, largest electronic services providers, internet traffic exchange points, domain name systems and other equipment that serves millions of users and billions of inquiries around the world, disorders or purposeful attacks can significantly slow down international dataflow, cut occasional webs sites or their groups and other sources from the remaining users (Ryan, 2007). Tangibility of the problem and possible damage can be illustrated by recent events in Estonia while relocating "bronze warrior statue". This country was attacked by organized global communication infrastructure means. Any possibilities to reach the world, to receive or provide the information about the events that had been happening were cut off. The activities of public authorities and business organizations were paralyzed as well as the possibility to perform business or everyday life needs in electronic space. This incident triggered a wide international discussion, enrolling relevant NATO and European Union structures regarding the present range of violations and the necessity of according collective actions (Janeliūnas, 2007; Lorents, Rain, Rikk, 2009).

Environment changes and the current processes demonstrate that the information security issue specifications can be distinguished on individual or organizational, State or international level. Evaluating the range of information security occurrence and possible

negative impact to any of these levels can be stated that ability to manage the information security must become a strategic objective of any organization, State or States conjoining international alliances and other institutions. Specific information security measures can be sought for each level, but the main responsibility in this context must be within the purview of the States, that provided the given possibilities can and must determine the means ensuring the information security management domestically (i.e. on personal and business level) and influence other States or their constructs to take the security measures and hereby join the problem solving on international level (CIO, CSO and PwC survey, 2012, 2012; Ernst & Young's 12th Annual Global Information Security Survey; NATO, 2010).

Analyzing the discussed global information security management problems context reflection in Lithuania, it can be stated that these global information security problems are also relevant to Lithuania: we had encountered internet banking systems malfunctioning and attacks, inaccessibility of registers and public authorities' information systems, the leakage of personal information from business and public institutions. A breaking into telecommunication services providers' servers, affecting private companies' as well as public authorities' Internet sites and disturbing their work, received a broad resonance (Gamulis, Kiškina, 2009 Janeliūnas, 2007; RRT, 2010). Solving these problems in Lithuania, as in other countries, a range of various strategic documents and other legal instruments adapted, coordinating the information security management. The content of these information security documents has been drawn and is constantly enhanced by information specialists' practices, referring to international good practices and methodologies.

Having discussed the information security problematic development and measures taken managing the information security questions in various levels it can be stated that even though the information security becomes one of the most important priority of action for organizations and countries however the number of information security incidents along with the range of losses they suffer, uncontrollably rises all around the world. These tendencies presuppose that: 1) information security incidents can be marked as the main indicator, signifying the existence of information security issues; 2) the States should take the main responsibility solving information security issues; 3) the information security protection is not duly managed and remains a relevant practical issue.

Thereby the existing situation forces to seek for the deep causes of information security management problems and for possible ways of solutions applicable to Lithuania.

Status of the research on the subject. Many scientific surveys influenced the change in the information security definition. Researching the information security problems attention was focused on the perception of information security (Parker, 1981; Treek, 2006; McCumber, 2005; Zafar and Clark, 2009; D'Archy and Hovav, 2009; Mikučionis, Toldinas and Venčkauskas, 2007 and others), economical (Anderson, 2001; Caelli, 2002; Gordon and Loeb, 2006; Johnson, 2009 and others), management (Abbas et al., 2011; Chang and Lin, 2007; Dlamini, Eloff and Eloff, 2003; Hong et al., 2003; Knapp et al., 2006; Parakkattu and Kunnathur, 2009 and others), communication (Janeliūnas, 2007 and others), implementation of security measures (Kazanavičius et al., 2012; Japertas, Činčikas and Šestavinskas, 2012; Paulauskas, 2009 and others), implementation of standards (Amaral, 2007; Gorge, 2009; Smith et al., 2010; Weise, 2009 and others), psychological (Nohlberg, 2008; Witten and Tygar, 1999; Anderson and Moore, 2009; Asch, 1952 and others), human factor (Ashenden, 2008; Timko, 2008 and others), social engineering (Bakhshi, Papadaki and Furnell, 2009; Workman, 2008; Kelly, 2007; Mitnick and Simon, 2002 and others), legislation and control (Čėsna and Štitilis, 2000; McFadzean, Ezingeard and Birchall, 2007; Paškauskas, 2007; Smith et al., 2010; Štitilis and Paškauskas, 2007 and others), competence and training (Venčkauskas, Krivickienė and Toldinas, 2009; Choi, Kim and Goe, 2008; Chang and Ho, 2006; Tsohou et al., 2008; White, 2009 and others) as well as other aspects of information security.

Analyzing and evaluating the development of information security theory and experience of practical implementation a significant contribution was made by M. Sipponen and H. Oinas-Kukkonen (2007), J. D'Archy and A. Hovav (2009), F. Bjorck and L. Yngstrom (2001), H. Zafar and J. Clark (2009), M. Dlamini, J. Eloff and M. Elloff (2009), von Solms (2010), J. Choobineh, G. Dhillon and M. Grimaila (2007), R. Werlinger, K. Hawkey and K. Beznosov (2009), G. Dhillon and J. Backhouse (2001), E. McFadzean, J. Ezingeard and D. Birchall (2006) and others.

Evaluating theoretical researches and experiences of practical implementation we can assert that information security problematic is quite broad however most of the information security surveys are concentrated on technological issues. There are many studies based on comprehensive scientific and reliable information security ensuring measures yet often due to their technological complexity, economical factors, lack of competence or other reasons, these measures are not properly applied thus a big breakaway is observed between the science and practice. There is a lack of conceptual information security management surveys.

On the grounds of general research context we can presume that the principal purpose (object to be protected) is information, however analyzing the security of information, managed

by technological means, quite often information technologies and information systems actually become a target of security. Seeking for solutions for present information security management issue in this dissertation a presumption is made that the fundamental information security management object is information therefore information security should be researched as a constituent part of information management and other related concepts (information resources management, information systems management, information records management and etc.).

Looking at the academic discourse, history of information security management and information management origins in particular, initial, technical information resource management tasks solving data computing issues can be prefigured. Subsequently these tasks were developing towards effective use of information technologies and became a broad managerial conception, ranging throughout information management to all organizational activities processes and existence of organization. In modern information management context the use of information technologies is valued as specific means (instrument) prepared for effective organizational activity. And to help the organization managing information effectively, optimize all activity processes (bonding them to organizational strategy) and to adapt to environment changes is becoming the objective of information management (Choo, 2002, 2008; Wilson, 1997; Vodacek, 1998; Schlögl, 2005).

Having analyzed the discourse of leading information management academics, we can emphasize the research of T. Wilson (1997), E. Macevičiūtė and T. Wilson (2002), D. Chaffey and S. Wood (2005), D. Chaffey and G. White (2011) in which these authors accent that the information must be safe and delivered to the right person not analyzing information security more explicitly. Studying the process model of information management (Choo, 2002) and model of information ecology (Davenport and Prusak, 1997), we can state that the aspect of information security is not highlighted. Expanding the analysis towards contiguous information management concepts we can discover that emphasizing the technological aspect of information management and having formulated the conception of information resources management in 1970, the issue of information security was analysed in the context of information resources management. Information resources management models, formulated by D. Skyrme (1999), J. Hoven (2001), N. Willard (1993. 2003), Z. Atkočiūnienė and L. Markevičiūtė (2005), also specify the aspect of implementation of information resources security.

Summarizing the analyzed academic surveys of information security, it can be deduced that since the appearance of first computers until these days the approach towards the information security has essentially evolved – narrow understanding of information security as a mere technological issue is expanded by the studies of economical, managerial, psychological,

legal and other aspects' influence information security. A need for the broader viewpoint emerges. It becomes clear that existing information security management measures are no longer sufficient to control the information security. A need for a broader information security concept develops and the flaws of systemic information security management research become apparent. In the context of discussed surveys, comparing the development of information security management and information resource management, we can distinguish parallels of the shifts from technologies towards management in both discourses and predict the links between the objects of research. However in the surveys of information management models, methods and controlling implements the component of information security is not emphasized and information security management is not associated with information management.

The analysis of academic data allowed identifying the flaws of surveys dedicated to defining the information security management entirety and highlighting the cohesion with information management. In researches information is accentuated as a critical resource, inadequate attention is given to the implementation of the security of this resource becomes a pressing issue.

Discussed scientific issue (Research problem). The research field of information security management is not entirely formed, noticeable development of the research, however prevails a discreet analysis of single aspects (especially technological). In administering information security an emphasis on technological aspects is particularly identifiable. It is lacking scientifically grounded thorough information security management concepts that would broaden the field of information security management and determine the implementation of theoretical paradigms solving apparent practical problems of information security management in Lithuania as well as worldwide. It becomes evident that scientifically unevaluated information security management causes problems that become apparent in practical level.

Seeking for solutions to solve the existing information security management problems and making an essential scientific presumption that the object of information security management is the information, it is likely that information security should be a constituent part of information management therefore it could be appropriate to make use of theoretical information management concepts and implements while controlling information security. The use of scientifically grounded information security management implements might help to ensure comprehensive and effective information security management.

It has been observed that even though in scientific acumen information is emphasized as a critical resource, however the attention to ensure the security of this resource is feeble. Up until now the connection between information security management and information

management is not sufficiently developed and proved thus there are no reasonable theoretical grounds to put in practice information management models, methods and management implements in information security management and this becomes a relevant scientific issue.

Having analyzed the problematic spheres of information security management it can be stated that existing information security management means, springing of technological sciences, do not ensure sufficient information security management that would also integrate managerial aspects into it. According to this, the main research problem could be formulated as a question: how to integrate the means of information security management and information management instruments and to ensure thoroughly managed information security in Lithuanian public sector?

Object of the research – information security management.

Aim of the research – to create and substantiate information security management model, suitable for Lithuanian State institutions.

Tasks of the thesis:

1. Assess the prevailing scientific approach to information security and to form the content of information security management.
2. Emphasize the position of information security in the context of information management science; accentuate the means of information management applicable to information security management.
3. Create an integral, scientifically sound information security management model.
4. Form access to information security management assessment and perform an analysis of sources, shaping the requirements for information security management for Lithuanian State institutions.
5. Survey how Lithuanian State institutions implement existing information security management requirements.

Statements being defended:

1. Information security is a constituent part of information management therefore an effective information security management could be ensured invoking information management instruments.

2. Information security in Lithuanian State institutions is not duly controlled because of fragmentation of information security requirements and because of prevailing formal technical approach.
3. Integral information security management model, conjoining information security management means and information management instruments, allows solving present information security management issues, equally broadens the margins of information management and can be successfully used in further theoretical research as well as practically implemented in activities of Lithuanian State institutions.

Research methods

Research methods have been used in theoretical and empirical parts of the work: critical analysis of the literature, document analysis, content analysis, comparison, induction, abstraction, synthesis and generalisation as well as qualitative semi-structured interview and quantitative research questionnaire.

In theoretical part of the thesis forming the versatile outlook to information security subject matter, an analysis of scientific information security issue research as well as the content analysis applying methods of comparison, summarising and synthesis was carried. Comparative analysis was invoked to contextualize the most commonly applied means and contents of information security management. A systemic analysis of information management literature, methods of comparison, abstraction, parallel and generalization allowed highlighting the interconnection between information security and information management, distinguish the means of information management applicable to information security management also formulate an integral model of information security management.

In empirical part of the thesis, in order to identify a practical model of integrated information security management, a compound methods' approach was invoked matching quantitative and qualitative research methods – documents' content analysis, questionnaire survey of institutions and experts' interviews. Coordinating these methods for the vouching and practical realizations of integral academic information security management model it is possible to ensure thoroughly grounded and credible results of the research. To analyse the results of empirical research a consistent procedures' research strategy was applied. Qualitative and quantitative data was collected consistently one after another. Previous research results itemized, broadened and appended using the new information. Access to information security assessment was formed based on theoretical integrated information security management model, distinguished means of information security management and specified assessment criteria. This

access was used for identified sources' that form information security management requirements for Lithuanian State institutions content analysis. Results of analysis were used forming questions to experts and along with their insight (pointed out issues) – forming quantitative research (surveying institutions) questionnaire.

Content analysis of information security documents, regulating information security management in Lithuanian institutions, used to substantiate weaknesses of information security management in Lithuanian State institutions. Results of analysis indicated that information security management of Lithuanian State institutions could be termed a model only with reservation therefore designating present situation a term *discrete* (segregated from a whole) *information security model* should be used. An information security management requirement applied not for whole organisational information, but to its separate information systems defines the content of this model.

Experts' interview method used as means of input of Lithuanian State institutions and their expert context to evaluation of application of content results theoretical integral information security management model to Lithuanian State institutions' documents' content analysis results.

The aim of surveying Lithuanian State institutions was to explore the practical implementation of information security management requirements. To gather quantitative data of how Lithuanian State institutions implement information security requirements an original questionnaire was formed to assess the information security management. Obtained information helped thoroughly evaluate information security management situation in Lithuanian State institutions and form the presumption for the implementation of information security management model.

Novelty and scientific significance of research

Achieved results are substantial to information management science and determine the novelty and academic significance of the thesis. Thesis allowed reducing indeterminacy in information management science, amplify academic information management paradigm in information management highlighting the component of information security management.

Information security management content definition was established and justified having analysed the foresight of information security research, having systematized information security concepts and having established their links as well as having made a comparative analysis of information security management means prevailing at international level.

Specified information security management object discourse and highlighted information as an object of information security management, formed theoretical possibilities to employ the means of information management for information security management. Analysis of these means allowed identifying the means of information management to be used for information security management.

Linking the results of performed research, a theoretical integral information security management model was formed to be applied for further theoretical research as well as for practical use. Practical applicability of integral information security management model tested evaluating information security management in Lithuanian State institutions. Empirical research results confirm the importance of theoretical model providing effective information security management.

The thesis research boundaries

The thesis research confines the creation of information security management model for Lithuanian State institutions. Such boundaries are caused by the following reasons.

1. Current legal requirements on information security management with the broadest approach are implemented exclusively in Lithuanian public authorities therefore; this sector contains the widest area for research. Considering that the Government of the Republic of Lithuania has declared the intention to extend information security management requirements application to other sectors, it is a right time for a thorough scientific evaluation of current situation; justified recommendations could provide a practical value of this scientific work.

2. This sector is chosen also considering the principles of public law which characterize that public sector is authorised only to what is specified, i.e.: 1) public administrative services are authorised only as provided in legislation; 2) public administration services are made compulsory what is provided in legislation, i.e. public sector is bound by these frames and has no freedom of choice on how to react to information security risks. As a result, information security of Lithuanian State institutions are directly dependent from valid information security management requirements, this presupposes that these requirements must be adequately justified.

Basic concepts used in the thesis

This term of information security management is used in the thesis.

Studying the research a lack of coherence of information security concepts' usage was noted. On the level of objective of research in scientific works in English language as well as in

Lithuanian, frequently are used terms information security (*eng*.), *information technology security* (*eng*.) and *information systems security* (*eng*.). There is no consistent differentiation on the level of security process between English concepts *management* and *governance* and their translation into Lithuanian language. It should be noted that there is no strictly established and in this context used translation of English term *security* – security, safety, protection (for example, in the translation of COBIT methodology all three terms are used). Now the term *security* is mostly found in personal data legal protection, privacy context, *safety* – in the context of the State information resources management (registers and information systems), *protection* is used most commonly, as including all the above-mentioned aspects. During the evaluation of discussed context, the concept *of information security management* is the most appropriate with the view to enhance the diversity of information security management context and it was used in the thesis as covering (in the broad sense) security, safety and protection as well as the aspects of management and control.

This term of Lithuanian State institution is used in the thesis:

Lithuanian State institution – institution of representative, Head of the State, executive, juridical authorities, enforcement authorities, auditing, controlling (supervising) institution, other State institution, being financed from the State's budgets and other State money funds and which by the law of public administration is authorized the right to execute the public administration.

The structure of the thesis

The thesis consists of introduction, three parts, conclusions, bibliographical references and annexes.

In the first part of the thesis information security definitions are being analysed and structurized, also disclosed the concept genesis of the information security conception, analysed the scope and problems of Lithuanian and foreign researcher's information security studies. On the basis of this analysis the content of information security management was established.

The means of information security management - international information security management standards, methods and models and the implementation of their comparative analysis are also described in this part.

On the grounds of the assumptions and the content of information security management theoretical research implementation, a prospective research was performed, the documents' content analysis method used to examine the means of information security management for Lithuanian State institutions and the provision of these requirements assessed in a concrete

group of Lithuanian State institutions – in the Ministries of the Republic of Lithuania. The results of this prospective research were capable of supporting the subject-matter of the thesis and the relevance of claimed propositions also to determine the need for further research and directions.

In the second part of the thesis in order to reveal the interconnectedness of information security management and information management, the work of information management scientist has been analysed and evaluated, identified the means of information management which could be applied managing the information security.

Summarising the results of theoretical research, an integral information security management model was composed, which combines the means of information security management and the instruments of information management.

In the third part of the thesis an empirical research of theoretical integral information security management model‘s applicability was performed.

Methodology of research

The object of empirical research – the practical implementation of integral information security management model for information security management in the Lithuanian State institutions.

The aim of empirical research – to determine the practical implementation possibilities of theoretical integral information security management model.

The tasks of empirical research:

1. Formulate an access to information security management assessment, instruments and the evaluation criteria.
2. Determine the sources influencing information security management requirements for Lithuanian State institutions.
3. Research the content of identified sources on the grounds of formulated information security management access instruments and their evaluation criteria.
4. Evaluate how Lithuanian State institutions implement the legal requirements for information security.

Research methods

On the basis of theoretical integral information security management model, an access to information security management evaluation was formed and researched the management of

information security in Lithuanian State institutions. An access of mixed methods was applied to the research, combining document's content analysis, questionnaire of institutions and experts' interview. The results of empirical research allowed identifying weaknesses and formulating proposals on how to manage information security in Lithuanian State institutions on the grounds of integral information security model.

Results of research

According to formulated access to information security management assessment, empirical research was performed at the levels of information security policy, information security strategy, information security audit, and information security maturity and information security operators.

At the level of information security policy it was identified that information security policy in States institutions is defined by the document of institution's security policy and the object of information security management is defined by the information resources (State registers, departmental registers, State information systems and internal administration information systems). At present information security management requirements unambiguously are in force for three sorts of information resource (requirements for the internal administration information systems are not defined). With the help of quantitative research it was identified that only one third of Lithuanian State institutions under research have documents on information security policy which cover all information resources managed by these institutions and define a common organisational information security policy. At the level of non subject to authority, even 63 percent of organisations (most of these organisations control only internal administrative systems) do not have any information security policy documents. Research results allowed to conclude that even though the defined information security management object – the State information resource – has deficiencies (e.g., 48 percent of identified resources are of internal administrative systems and there information security management requirements are not applied), however given the situation that it would require significant financial and organisational resources to alter it, therefore the more appropriate decision – to adopt additional requirements for information security management for internal administration systems and information security documents applied in the integrated way to all information resources administered by a specific institution.

Documents content analysis allowed identifying that the supreme information security management level requirements (laws and the Government decisions) directly cover only two

out of three information security management aims – confidentiality and integrity, however they do not include accessibility.

Experts consider that institutions should have the possibility to set the priorities applying information security objectives with regards to controlled information specification. Quantitative research showed that evaluating overall and individual results institutions haven't singled out any statistically significant information security objectives' difference. Only a small part of State institutions are capable to realistically evaluate and reasonably select the clear methodological recommendations for the choice of priorities.

At the level of information security strategy during theoretical documentary research it was identified that a public authorities' security management document exists, however the implementation has not been ensured yet. Public authorities are not obliged to develop a special information security strategy, however a quantitative research showed that one third of institutions have an approved timely document of information strategy. It is worth mentioning that the cycle of information security processes is not ensured, - a quantitative research shows that 61 percent of State institutions has tried at least once to evaluate the risks and react to environment changes however, only 7 percent of these institutions do it on a regular basis.

Evaluating the content of information security strategy implementation means in the context of information security management dimensions (strategic, human, technological), stated a formal division of information security management responsibilities between the institutions (except the coordination of critical infrastructure security) however, identified an evident insufficiency of real possibilities to implement these responsibilities also it should be mentioned that economic context is not being taken into account while not basing on realistic grounds a mandatory application of expensive technical means.

At the level of information security audit, theoretical research identified obligation to implement information security audit at the State level is indicated in the State information resources law. The importance of such audit was emphasized by the experts, who participated in qualitative research. However, audit at the State level is not fulfilled. At the institutional level the State institutions are obliged to carry out periodical audits however, the quantitative research revealed that only 58 percent of the State institutions have carried out security audit at least once and only 6 percent of them carry out such audit on a regular basis.

At the level of maturity of information security, during the qualitative research the experts almost unanimously emphasized the advantages of determination and evaluation of maturity levels. The means of information security management could be selected according to the maturity level of institution. Institutions controlling more important resources should aim for

accordingly higher maturity level. Documents' content analysis allowed identifying the fact that maturity levels of security and evaluation procedures are not established for State institutions.

Document's content analysis revealed that at the level of information security operators there are designated authorities or institutions, responsible for information security management however, after the analysis of the functions and the list of posts of these institutions it is clear that coordinating institutions are not capable of carrying out their tasks. Similar insights were submitted by the experts, having participated in qualitative research, according to them, even though there are assigned competent authorities, the information security management lacks competence, there is not enough specialists and decision making for appointed tasks is slow.

Quantitative research of information security management in the Lithuanian State institutions helped identifying a serious gap at the institutional level – 78 percent of the institutions have assigned security representatives however, in 60 percent of cases information technology units' staff members or even heads of units are responsible for the management of information security.

Such situation is clearly at odds with the principle of separating the implementation and control functions.

Summarising the information security management in Lithuanian State institutions research results it can be stated that at present only single parts of information security management are controlled. There is a lack of holistic approach. Means which would enable the establishment and maintenance of managed information security as an objective security status are not implemented.

Conclusions

1. Growing information security cases and scope illustrate that the relevance of information security issues becomes critical and present information security means are not sufficient enough to manage information security. Narrow comprehension of information security merely as technological problem is broadened by the research results of economic, managerial, psychological, legal and other related aspects' influence to information security. It becomes apparent that present means of information security management are not sufficient to control the information security. There is a need for a more holistic managerial approach.

2. The scientific information security management problem field is not yet formed. The research area development is observed however, dominates an analysis of single aspects. Managing the information security too much emphasis is put on technological aspects and the lack of scientifically substantiated general information security management concept which

would expand the field of theoretical information security management research and determine the implementation of theoretical paradigms dealing with apparent practical information security management problems. Scientifically unjustified information security management causes problems which become apparent in practice both in Lithuania and globally.

3. In the context of both scientific research and in practical use, observed a rather synonymous use of information, information systems, information technologies and other security objects. Information security management as an objective security status, first of all must have a clearly and unambiguously defined object of management. The designation of an object permits to define the conditions and criteria which allow evaluating whether the object's security is managed.

4. Information is named the objective of information security management in this thesis, and the main objectives of information security management are the assurance of information confidentiality, integrity and accessibility, the aspects, relevant to information security management, grouped into strategic, human and technological dimensions thus the content of information security is defined as an objective to provide information confidentiality, integrity and accessibility, adjusting strategic, human and technological dimensions.

The information security management content is defined as an aim to ensure the information confidentiality, integrity and accessibility sustainably combining strategic, human and technological dimensions.

5. Defining the content of information security management is insufficient, it is necessary to provide the measures that would help to control it. Looking for the solutions for information security management issues and on the basis of the fact that information is the object of information security management, new information security management solutions are searched in the information management sciences.

6. In the view of the fact that information is stressed to be a critical resource in the academic insights, the assurance of the security of this resource is not sufficient addressed in the context of information management science. In the research of information management models, methods and means of application the component of information security management is not highlighted and information security management is not linked with information management.

Comparing the evolution of information security management and information management, the parallels of change from technologies towards the management perceived in both discourses. Also can be noted the security links with the object of the research of information management, information management processes, application, informational technologies and systems as well as with the competences of information management.

Similarly, the security link with information management research object, information management processes, the implementation, information technologies and systems, as well as with the information management competences is identified. Having thoroughly analysed the means of information management it has been stated that given the organization has a clear information policy and strategy, regularly performs an audit, manages all informational processes, promptly reacts to environment changes, designates competitive players and has a high information maturity level, it can reasonably expect to be ensuring the information security management. The main attention to information security at present is given in information management disciplines and in relevant scientific research where the emphasis is placed on the technological information security management aspect, - records management and information resource management spheres. Information security accessibility and confidentiality goals are closely integrated into the information records management and all three management information security objectives are highlighted in the scientific research of information resource.

7. An effective information management is characterised by an appropriate use of means. The key aspects to manage the information security these information management tools are revealed – policy, strategy, audit, maturity and the players. Combining information security content and the main information security means can be reasonably expected to assure the effective information security management (clear information security policy and strategy, regular auditing, management of all information security processes, prompt reaction to environment changes, competitive players are designated and the aim for high maturity level).

Identifying and critical analysis of information management and information security management links, was established a theoretical basis to form an integral information security management model.

8. Theoretical integral information security management model forms an overall approach to the content of information security management, that describes objects and goals should be managed and defines the means of information management which enable to evaluate and assure the complexity of information security management. Therefore implementation of information management tools to information security management allows reinforcement of present weak areas and assurance of effective and integrated management of information security.

9. The requirements regarding the information security management in Lithuanian State institutions are fragmented, a technological approach dominates.

There is no special law in Lithuania regarding information security. Information security policy in Lithuania is regulated by the law on information resources management, in the

institutions – it is a security policy document (data safety regulations). These documents specify that information is an object of information security management, processed by the State information resources (the registers of the State, departmental registers, informational systems of the State and internal administration systems).

Present information security management requirements, applied to single information resources of the State, have deficiencies – this object unambiguously does not cover the whole information, controlled by the institution, mandatory information security management requirements are not adopted by the systems, oriented to internal administration, which constitute 48 percent of total institution's information resources in Lithuania (requirements for these resources are advisory and more than half of Lithuanian State institutions do not comply with the advisory requirements).

Information security management strategy in Lithuania is documented, long time targets, tasks are set, as well as assessment criteria however, it is yet not decided regarding the detail implementation actions and legislation for implementation of operative provisions is not adopted.

A permanent information security management circle is not ensured – only 7 percent of the State institutions apply measures in reaction to environment changes permanently (risk analysis, etc.) and information security management measures are determined without evaluation of economic context (implementation of certain valid means of information security is unduly expensive); also a human factor is underestimated.

Regulatory provisions, relating the information security requirements for Lithuanian State institutions, define the implementation of information security audit. However, the process of information security auditing is not duly specified and implemented, information security policy and its implementation is not being audited, responsible for the information security management coordination institutions‘ referred functions implementation, sufficient control is not provided regarding how the State institutions implement information security management requirements, a real situation in Lithuanian State institutions is unknown, information security management processes are uncontrolled. A significant part of the State institutions only formally apply the current requirements.

A decentralized information security management coordination model is applied in Lithuania – the coordination related functions are designated to several institutions (apart from critical infrastructure security function, which unambiguously is not designated to anyone); a collegiate interinstitutional coordinating body was established – permanent commission. However, institutions, coordinating the information security, are incapable of carrying out their

tasks – institutional competence to organize information security is low and implements assigned tasks rather slow.

60 proc. of the cases information technology units' staff members or even heads of units are responsible for the management of information security. Such situation is clearly at odds with the principle of separating the implementation and control functions and prevents the effective information security management.

One of the most important factors for an effective fulfilment of the targets is maturity; the means of information security management could be selected according to the maturity level of institution. Institutions, controlling more important resources should aim for accordingly higher maturity level. Information security maturity levels and their evaluation procedures are not established for the Lithuanian State institutions.

10. Evaluating information security management in the Lithuanian State institutions, it is concluded that only the single parts of information security are assured, a formal approach dominates; means that would allow creation and maintenance of controlled information security as an objective security state are not implemented.

A dominant formal approach to the information security in Lithuanian public sector materialises through the abundance of confirmed, though not implemented legislation and yet to be defined implementing documents (the lack of law, administrative provisions, necessary for the implementation of the strategies; internal institutional documents are unattended, not renewed, measures provided are not implemented).

A higher maturity noticed of institutions that comply in addition to the requirements of information security management on a long time basis (Ministries, other institutions under the authority of the Government).

11. Aiming for the effective information security management in the Lithuanian State institutions binding information security management requirements must be proved, covering all the State's information resources and laying down that each State institution has one information security management policy document (data safety regulations), that would generally describe all the information resources controlled by that State institution.

The objective of information security management should be – the assurance of the confidentiality, integrity and accessibility of all the State controlled information (at present there is no unambiguously defined accessibility target objective and it becomes especially relevant evaluating last year's tendencies – various cyber space attacks, if successful, information resources become unavailable). Priorities for these objectives must be defined basing on each institution's controlled information specifics, accordingly choosing and applying information

security assurance strategies, human and technical means. With the view to the fact the State institutions lack sufficient competence to set the priorities assuring effective and uniformed information security management process, clear criteria for prioritisation and selection of means should be prepared.

Aiming for the better performance of the State institutions, the coordinating institutions should be strengthened (unambiguously and specifically appointing the responsibility), delegating them to centralize the use of information infrastructure (after inventorying it), provide centralized methodological support to institutions (bringing into collaboration the public, private and academic sectors) and assure a continual information security management evaluation and control, in accordance with uniformed methodology and clear evaluation criteria. For the establishment of definition and evaluation procedures of information security maturity levels, it may be appropriate to refer to the international methodologies and practices.

12. Integral information security management model, constructed at a theoretical level, shows a complex approach towards information security, integrates information management and information security management. Integral information security management model allows indentifying information security management weaknesses in the Lithuanian State institutions, rectifying deficiencies, provide an integrated and efficient information security management. A practical research and obtained results grounded the constructed model's applicability both for further theoretical academic research and for practical application in the Lithuanian State institutions.

The result of theoretical and empirical research allow suggesting that the objective of the thesis is achieved – an integral information security management model, drawn at a theoretical level, is justified, and can be implemented in the Lithuanian State institutions.

Santrauka

Temos aktualumas. Informacijos saugumo svarba ir aktualumas sietini su pirmaisiais poreikiais tvarkyti informaciją. Vos atsiradus raštui, buvo ieškoma laiko ir gamtos reiškinių poveikiui atsparių priemonių informacijai fiksuoti ir išsaugoti. Iškilus poreikiui informaciją perduoti, radosi ir poreikis užtikrinti, kad ji pasiektų tik tuos, kam ji skirta. Tai sudarė sąlygas formuotis kriptografinių saugumo priemonių užuomazgoms. Pirmieji metraštininkai, archyvų bei bibliotekų darbuotojai taip pat gali būti priskirti informacijos saugumo vystytojams, pavyzdžiui, jų naudoti vaško antspaudai buvo taikomi siekiant užkirsti kelią neteisėtai prieigai prie informacijos ir ją pastebėti; kodai – apsaugoti informaciją nuo atskleidimo; kopijų darymas – išvengti informacijos praradimo (Denning, 1999; Lomas, 2010; Rusell ir Gangemi, 1991).

Informacijos saugumo turinys reikšmingai keitėsi pradėjus vystytis kompiuteriams ir kitoms informacinėms technologijoms. Pirmieji kompiuteriai, nors ir buvo naudojami tiek nacionalinio saugumo, tiek sudėtingų komercinių uždavinių sprendimams, nebuvo laikyti nei saugumo problema, nei jos sprendimu. Šie kompiuteriai dažniausiai buvo naudoti vieno vartotojo konkrečių uždavinių sprendimams, todėl vartotojui baigus darbą realiai buvo rūpinamasi tik informacijos laikmenų (magnetinių juostų, perfokortų) bei patalpų, kuriose buvo kompiuterinė sistema, fiziniu saugumu (užrakinimu). Informacijos saugumo problemos pradėjo ryškėti po 1960 metų pradėjus keistis kompiuterių naudojimo pobūdžiui, atsiradus personaliniams kompiuteriams ir technologijoms, leidusioms naudoti tą patį kompiuterį keliems vartotojams įvairiems skaičiavimams atlikti vienu metu, o ypač pradėjus vystytis kompiuterių tinklams (Brinkley ir Schell, 1995).

Šiuolaikinėje visuomenėje informacijos saugumo problemų aktualumas tampa kritinis. XX a. antroje pusėje kylant poreikiui valdyti informaciją ir žinias pasitelkiant modernias technologijas ir vadybos metodus, vis daugiau informacijos ir kasdienės veiklos procesų persikėlė į globalią elektroninę erdvę. Vykstantys dinamiški pokyčiai pavertė visuomenę labai priklausomą nuo patikimo informaciją apdorojančių technologijų veikimo, bet kokie šių technologijų veiklos sutrikimai turi neigiamos įtakos tiek pavienių jos individų, tiek ir organizacijų ar net visos visuomenės socialiniam ir ekonominiam gyvenimui. Aktualiomis informacijos saugumo problemomis tapo nepageidaujami laiškai, virusai, įsilaužimai į informacines sistemas, interneto svetainių sutrikimai, tapatybės pasisavinimas, asmens duomenų ar verslo informacijos vagystės, slaptos informacijos nutekėjimas (pvz., Wikileaks) ar Tūkstantmečio klaidos (Y2K) sukeltas ažiotažas visame pasaulyje (Amaral, 2007; Atkočiūnienė, 2009; Kuttschreuter, Gutteling, 2004).

Aktualių informacijos saugumo problemų gausa lėmė poreikį informacijos saugumui valdyti. Kylančioms problemoms spręsti buvo parengta įvairių dokumentų – gerųjų praktikų pavyzdžiai, vertinimo metodikos, rekomendacijos pavienėms verslo šakoms, sukurtas ne vienas tarptautinį pripažinimą pelnęs informacijos saugumo valdymo standartas. Šių dokumentų pagrindu organizacijoms suteikiama metodinė pagalba kompleksiškai ir suderintai taikyti informacijos saugumo valdymo metodus bei technologijas, laikytis geriausių praktikų, atitikti teisinius reikalavimus ir kitų privalumų (Amaral, 2007; Gorge, 2009; Weise, 2009). Kaip rodo praktika, pavieniai individai ar organizacijos ne visada nori ir gali spręsti kylančias saugumo problemas, čia išryškėja valstybių valdžios institucijų įsikišimo būtinybė. Valstybės, supratusios informacijos saugumo problemų kritiškumą ir valdymo svarbą (pvz., JAV, Didžioji Britanija, Japonija, Australija ir kt.), nustatė privalomus informacijos saugumo reikalavimus organizacijoms, veiklos sritims (sektoriams), valdančioms jautrią informaciją (asmens ar sveikatos duomenis, finansinę ar karinę informaciją ir kitą). Šie reikalavimai dažnai remiasi susiformavusiomis gerosiomis praktikomis ir (ar) tarptautiniais informacijos saugumo valdymo standartais.

Nepaisant bandymų spręsti informacijos saugumo keliamus iššūkius, pastarųjų metų tendencijos rodo, kad informacijos saugumas tampa globalaus masto problema, kurios aktualumą iliustruoja nuolat augantys informacijos saugumo incidentų atvejai ir mastai. Šie incidentai kelia grėsmę ne tik pavienėms organizacijoms ar valstybėms, bet ir globaliai kibernetinei erdvei. Pasaulinės interneto infrastruktūros, kuriai priskiriami didžiausi elektroninių ryšių paslaugų tiekėjai, interneto srautų paskirstymo įranga, vardų sričių saugyklos ir kita milijonus vartotojų bei milijardus užklausų visame pasaulyje aptarnaujanti įranga, sutrikimai ar tikslingos atakos gali smarkiai sulėtinti tarptautinių duomenų srautą, atkirsti pavienius tinklus ar jų grupes bei kitus išteklius nuo likusių vartotojų (Ryan, 2007). Problemos realumą ir galimą žalą parodė įvykiai Estijoje perkeliant „bronzinio kario skulptūrą“. Pasaulinės ryšių infrastruktūros priemonėmis organizuoto puolimo prieš šią šalį metu buvo atkirstos visos valstybės galimybės susisiekti su pasauliu, gauti ar pranešti informaciją apie šalyje vykstančius procesus, paralyžuotas valstybės institucijų ir verslo organizacijų darbas bei galimybė tvarkyti verslo ar kasdienio gyvenimo poreikius elektroninėje erdvėje. Šis įvykis sukėlė plačią tarptautinę diskusiją, į kurią buvo įtrauktos ir NATO bei Europos Sąjungos atitinkamos struktūros, dėl esamų tokio masto pažeidžiamumų ir kolektyvinių veiksmų tokiais atvejais būtinybės (Janeliūnas, 2007; Lorents, Rain, Rikk, 2009).

Aplinkos kaita ir joje vykstantys procesai rodo, kad informacijos saugumo problemų specifiškumas gali būti išskiriamas individo ar organizacijos, valstybės bei tarptautiniame

lygmenyse. Įvertinus informacijos saugumo incidentų mastą ir galimą neigiamą poveikį bet kuriame iš šių lygmenų, teigtina, kad sugebėjimas valdyti informacijos saugumą turi tapti strateginiu tiek organizacijų, tiek valstybių, tiek ir valstybes jungiančių tarptautinių aljansų ar kitų institutų tikslu. Kiekviename lygmenyje galima ieškoti konkrečių informacijos saugumo valdymo įrankių, tačiau didžiausia atsakomybė šiame kontekste turi tekti valstybėms, kurios, pasiremdamos suteiktomis galiomis, gali ir privalo nustatyti priemones, užtikrinančias informacijos saugumo valdymą jų viduje (t. y. individų ir organizacijų lygmenyje), bei turėti įtakos kitoms valstybėms ar jų dariniams imtis informacijos saugumo priemonių ir taip prisidėti prie tarptautinio lygmens problemų sprendimo (CIO, CSO ir PwC tyrimas, 2010, 2012; Ernst & Young's 12th Annual Global Information Security Survey; NATO, 2010).

Analizuojant aptarto globalaus informacijos saugumo valdymo problemų konteksto atspindį Lietuvoje, galima teigti, kad Lietuvai taip pat aktualios globalios informacijos saugumo problemos: esame susidūrę su internetinės bankininkystės sistemų sutrikimais ir atakomis, registrų ir valstybės informacinių sistemų duomenų nepasiekiamumu, asmens duomenų nutekėjimu iš verslo ir valstybinių organizacijų, plataus atgarsio susilaukė įsilaužimai į ryšių paslaugų tiekėjų serverius, kada nukentėjo tiek privačių bendrovių, tiek ir valstybės institucijų interneto svetainės, buvo sutrikdytas jų darbas ir pan. (Gamulis, Kiškina, 2009; Janeliūnas, 2007; RRT, 2010). Sprendžiant šias problemas Lietuvoje, kaip ir kitose šalyse, priimta įvairių strateginių dokumentų ir kitų teisės aktų, reglamentuojančių informacijos saugumo valdymą. Šių informacijos saugumo dokumentų turinys parengtas ir nuolat tobulinamas informacijos saugumo specialistų praktikų, remiamasi tarptautinėmis gerosiomis praktikomis ir metodikomis.

Aptarus informacijos saugumo problematikos raidą bei priemones, kurių imamasi valdant informacijos saugumo problemas įvairiuose lygmenyse, galima konstatuoti, kad nors informacijos saugumas tampa vienu svarbiausiu veiklos prioritetu tiek organizacijoms, tiek ir valstybėms, tačiau informacijos saugumo incidentų skaičius, kartu su dėl jų patiriamų nuostolių mastais, nevaldomai auga visame pasaulyje. Šios tendencijos leidžia daryti išvadas, kad: 1) informacijos saugumo incidentai gali būti įvardyti kaip pagrindinis indikatorius, suponuojantis sisteminių informacijos saugumo problemų egzistavimą; 2) sprendžiant informacijos saugumo problemas, didžiausia atsakomybė turi tekti valstybėms; 3) informacijos saugumo užtikrinimas nėra tinkamai valdomas ir išlieka aktualia praktine problema.

Taigi esama situacija verčia ieškoti giluminių informacijos saugumo valdymo problemų priežasčių bei galimų jų sprendimų būdų, taikytinų Lietuvos atvejui.

Temos ištirtumas. Informacijos saugumo apibrėžties kaitai įtaką darė daugybė mokslinių tyrimų. Tyrinėjant informacijos saugumo problematiką, analizuota informacijos saugumo suvoktis (Parker, 1981; Trcek, 2006; McCumber, 2005; Zafar ir Clark, 2009; Mikalauskienė ir Brazaitis, 2010 ir kiti), įvairūs techniniai (Anderson, 1994; Anderson ir Moore, 2009; D'Archy ir Hovav, 2009; Mikučionis, Toldinas ir Venčkauskas, 2007 ir kiti), ekonominiai (Anderson, 2001; Caelli, 2002; Gordon ir Loeb, 2006; Johnson, 2009 ir kiti), vadybiniai (Abbas et al., 2011; Chang ir Lin, 2007; Dlamini, Eloff ir Eloff, 2009; Eloff ir Eloff, 2003; Hong et al., 2003; Knapp et al., 2006; Parakkattu ir Kunnathur, 2010 ir kiti), komunikaciniai (Janeliūnas, 2007 ir kiti), saugos priemonių taikymo (Kazanavičius et al., 2012; Japertas, Činčikas ir Šestaviskas, 2012; Paulauskas, 2009 ir kiti), standartų taikymo (Amaral, 2007; Gorge, 2009; Smith et al., 2010; Weise, 2009 ir kiti), psichologiniai (Nohlberg, 2008; Whitten ir Tygar, 1999; Anderson ir Moore, 2009; Asch, 1952 ir kiti), žmogiškojo faktoriaus (Ashenden, 2008; Timko, 2008 ir kiti), socialinės inžinerijos (Bakhshi, Papadaki ir Furnell, 2009; Workman, 2008; Kelly 2007; Mitnick ir Simon 2002 ir kiti), teisinio reglamentavimo ir reguliavimo (Čėsna ir Štitilis, 2000; McFadzean, Ezingeard ir Birchall, 2007; Paškauskas, 2007; Smith et al., 2010; Štitilis ir Paškauskas, 2007 ir kiti), kompetencijos ir mokymų (Venčkauskas, Krivickienė ir Toldinas, 2009; Choi, Kim ir Goo, 2008; Chang ir Ho, 2006; Tsohou et al., 2008; White, 2009 ir kiti) bei kiti informacijos saugumo aspektai.

Analizuojant ir vertinant informacijos saugumo teorijos raidą ir praktinio taikymo patirtį daug prisidėjo M. Sipponen ir H. Oinas-Kukkonen (2007), J. D'Archy ir A. Hovav (2009), F. Bjorck ir L. Yngstrom (2001), H. Zafar ir J. Clark (2009), M. Dlamini, J. Eloff ir M. Eloff (2009), von Solms (2010), J. Choobineh, G. Dhillon ir M. Grimaila (2007), R. Werlinger, K. Hawkey ir K. Beznosov (2009), G. Dhillon ir J. Backhouse (2001), E. McFadzean, J. Ezingeard ir D. Birchall (2006) ir kiti.

Išanalizavus teorinius tyrimus ir praktinio taikymo patirtį, galima teigti, kad informacijos saugumo problematika gana plati, tačiau dauguma informacijos saugumo tyrimų koncentruota ties technologinėmis problemomis. Egzistuoja daug išsamiais moksliniais tyrimais pagrįstų, patikimų informacijos saugumo užtikrinimo priemonių, bet dažnai dėl savo technologinio sudėtingumo, ekonominių veiksnių, kompetencijos trūkumo ar kitų priežasčių šios priemonės nėra tinkamai taikomos, taigi stebimas didelis atotrūkis tarp mokslo ir praktikos, stokojama konceptualių informacijos saugumo valdymo tyrimų.

Remiantis bendru mokslinių tyrimų kontekstu, galima daryti prielaidą, kad pagrindinis saugumo tikslas (objektas, kurį siekiama apsaugoti) yra informacija, tačiau, analizuojant informacijos, tvarkomos informacinių technologijų priemonėmis, saugumą, dažnai saugumo

objektu virsta pačios informacinės technologijos ar informacinės sistemos. Šioje disertacijoje, ieškant esamos informacijos saugumo valdymo problematikos sprendinių, daroma esminė mokslinė prielaida, kad svarbiausias informacijos saugumo objektas yra informacija, todėl informacijos saugumas turėtų būti tiriamas kaip sudėtinė informacijos vadybos ir kitų gretimų koncepcijų (informacijos išteklių vadybos, informacijos sistemų vadybos, informacijos įrašų vadybos) dalis.

Žvelgiant į informacijos vadybos mokslų raidą, ypač informacijos vadybos ištakas, taip pat galima įžvelgti pradines, techniškas, informacijos vadybos užduotis sprendžiant duomenų apdorojimo problemas. Vėliau šios užduotys plėstos efektyvaus informacinių technologijų išnaudojimo linkme bei tapo plačia vadybine koncepcija, apimančia informacijos valdymą visuose organizacijos veiklos procesuose ir gyvavimo srityse. Šiuolaikinės informacijos vadybos kontekste informacinių technologijų naudojimas vertinamas kaip konkrečių efektyviai organizacijos veiklai parengtų procesų paramos priemonė (įrankis), o informacijos vadybos uždaviniais tampa siekis organizacijai padėti efektyviai valdyti informaciją, optimizuoti visus veiklos procesus (siejant juos su organizacijos veiklos strategija) bei prisitaikyti prie aplinkos pokyčių (Choo, 2002, 2008; Wilson, 1997; Vodacek 1998; Schlögl, 2005).

Išanalizavus pagrindinių informacijos vadybos teoretikų darbus, galima išskirti T. Wilson (1997), E. Macevičiūtės ir T. Wilson (2002), D. Chaffey ir S. Wood (2005), D. Chaffey ir G. White (2011) mokslinius tyrimus, kuriuose šie autoriai mini, kad informacija turi būti saugi, pristatyta reikiamam subjektui, tačiau detaliau informacijos saugumo nenagrinėja. Nagrinėjant pagrindinius informacijos vadybos procesinį (Choo, 2002) ir ekologinį modelius (Davenport ir Prusak, 1997), galima konstatuoti, kad informacijos saugumo aspektas neišryškintas. Plečiant analizę į gretimas informacijos vadybos koncepcijas, galima aptikti, kad išryškinus informacijos valdymo technologinį aspektą ir apie 1970 m. susiformavus informacijos išteklių vadybos sampratai, šiek tiek plačiau informacijos saugumo problematika nagrinėta informacijos išteklių vadybos kontekste. D. Skyrme (1999), J. Hoven (2001), N. Willard (1993, 2003), Z. Atkočiūnienės ir L. Markevičiūtės (2005) sudaryti informacijos išteklių vadybos modeliai, kaip viena iš informacinės veiklos sričių, išskiria ir informacijos išteklių saugumo užtikrinimo aspektą.

Apibendrinus išanalizuotus mokslinius informacijos saugumo tyrimus, konstatuota, kad požiūris į informacijos saugumą nuo pirmųjų kompiuterių pasirodymo iki šių dienų iš esmės evoliucionavo – siaurą informacijos saugumo, kaip technologinės problemos, supratimą plečia ekonominių, vadybinių, psichologinių, teisinių ir kitų susijusių aspektų įtakos informacijos saugumui tyrimų rezultatai, kyla platesnio vadybinio požiūrio poreikis, tampa akivaizdu, kad

esamos informacijos saugumo valdymo priemonės nebėra pakankamos informacijos saugumui valdyti. Ryškėja platesnės informacijos saugumo valdymo suvokties poreikis ir sisteminių informacijos saugumo valdymo tyrimų trūkumas. Aptartų mokslinių tyrimų kontekste, gretinant informacijos saugumo valdymo ir informacijos vadybos raidą, galima įžvelgti paralelių abiejų diskursų slinktyje nuo technologijų vadybos link, numanyti tyrimų objekto sąsajas, tačiau informacijos vadybos modelių, metodų bei valdymo įrankių tyrimuose neišryškinta informacijos saugumo dedamoji, o informacijos saugumo valdymas nesiejamas su informacijos vadyba.

Mokslinės literatūros analizė leido nustatyti mokslinių darbų, skirtų informacijos saugumo valdymo visumai apibrėžti ir sąsajumui su informacijos vadyba išryškinti, trūkumą. Mokslinėse įžvalgose akcentuojant informaciją, kaip kritinį išteklių, per mažas teoretikų dėmesys šio ištekliaus saugumui užtikrinti tampa aktualia moksline problema.

Sprendžiama mokslinė problema. Informacijos saugumo valdymo mokslinės problemos laukas nėra visiškai susiformavęs, stebėtina tyrimų plėtra, tačiau vyrauja diskretyvi pavienių aspektų (ypač technologinių) analizė. Valdant informacijos saugumą identifikuotinas technologinių aspektų ryškinimas. Stokojama moksliškai pagrįstų sisteminių informacijos saugumo valdymo konceptų, kurie praplėstų informacijos saugumo valdymo teorinių tyrimų lauką bei lemtų teorinių paradigmų taikymą sprendžiant ryškėjančias praktines informacijos saugumo valdymo problemas tiek Lietuvoje, tiek ir globaliu mastu. Tampa akivaizdu, kad moksliškai neįtvirtintas informacijos saugumo valdymas sukelia problemų, kurios išryškėja ir praktiniame lygmenyje.

Ieškant esamos informacijos saugumo valdymo problematikos sprendinių bei darant esminę mokslinę prielaidą, kad informacijos saugumo valdymo objektas yra informacija, tikėtina, jog informacijos saugumas turėtų būti sudėtinė informacijos vadybos dalis, todėl, valdant informacijos saugumą, galėtų būti tikslinga pasitelkti teorinius informacijos vadybos konceptus ir įrankius. Moksliškai pagrįstas informacijos vadybos įrankių pasitelkimas, tikėtina, padėtų užtikrinti visapusišką ir efektyvų informacijos saugumo valdymą.

Pastebėta, kad nors mokslinėse įžvalgose informacija akcentuojama kaip kritinis išteklius, tačiau teoretikų dėmesys šio ištekliaus saugumui užtikrinti yra menkas. Iki šiol informacijos saugumo valdymo ir informacijos vadybos sąsajos nėra pakankamai išplėtotos ir pagrįstos, todėl nėra argumentuoto teorinio mokslinio pagrindo informacijos saugumo valdymui taikyti informacijos vadybos modelius, metodus bei valdymo įrankius ir tai tampa aktualia moksline problema.

Išanalizavus informacijos saugumo valdymo problemines sritis, galima teigti, kad egzistuojančios informacijos saugumo valdymo priemonės, kilusios iš technologinių mokslų, neužtikrina visapusiško, integruojančio vadybinius aspektus informacijos saugumo valdymo. **Disertacijoje keliamas pagrindinis probleminis klausimas – kaip integruoti informacijos saugumo valdymo priemones ir informacijos vadybos įrankius ir užtikrinti visapusiškai valdomą informacijos saugumą Lietuvos valstybės institucijose?**

Tyrimo objektas – informacijos saugumo valdymas.

Tyrimo tikslas – sukurti ir pagrįsti integralų informacijos saugumo valdymo modelį, taikytiną Lietuvos Respublikos valstybės institucijoms.

Tyrimo uždaviniai:

1. Išanalizuoti vyraujančius mokslinius požiūrius į informacijos saugumą ir suformuoti informacijos saugumo valdymo turinį.
2. Išryškinti informacijos saugumo vietą informacijos vadybos mokslų kontekste, išskirti informacijos vadybos įrankius, taikytinus informacijos saugumo valdymui.
3. Sudaryti integralų, teoriškai pagrįstą informacijos saugumo valdymo modelį.
4. Suformuoti informacijos saugumo valdymo vertinimo prieigą ir atlikti šaltinių, formuojančių informacijos saugumo valdymo reikalavimus Lietuvos valstybės institucijoms, turinio analizę.
5. Ištirti, kaip Lietuvos valstybės institucijos įgyvendina galiojančius informacijos saugumo valdymo reikalavimus.

Ginamieji teiginiai:

1. Informacijos saugumas yra sudėtinė informacijos vadybos dalis, todėl informacijos saugumo valdymui pasitelkiant informacijos vadybos įrankius gali būti užtikrintas efektyvus informacijos saugumo valdymas.
2. Informacijos saugumas Lietuvos valstybės institucijose nėra tinkamai valdomas dėl informacijos saugumo reikalavimų fragmentiškumo ir vyraujančio formalaus techninio požiūrio.
3. Integralus informacijos saugumo valdymo modelis, jungiantis informacijos saugumo valdymo priemones ir informacijos vadybos įrankius, leidžia spręsti

esamas informacijos saugumo valdymo problemas, praplečia informacijos vadybos ribas ir gali būti sėkmingai naudojamas tiek tolesniuose teoriniuose tyrimuose, tiek praktinėje Lietuvos valstybės institucijų veikloje.

Tyrimo metodai

Vykdant tyrimą buvo taikyti mokslinės literatūros kritinės analizės, dokumentų turinio analizės, lyginimo, abstrakcijos, analogijos, sintezės, apibendrinimo, anketinės apklausos bei ekspertų interviu tyrimo metodai.

Teorinėse darbo dalyse, formuojant sisteminio požiūrio į informacijos saugumą turinį, atlikta mokslinės literatūros kritinė analizė, lyginimas bei apibendrinimas. Sisteminė informacijos vadybos mokslinės literatūros analizė, abstrakcijos, analogijos ir apibendrinimo metodai leido išryškinti informacijos saugumo ir informacijos vadybos sąsajumą, išskirti informacijos vadybos įrankius, taikytinus informacijos saugumo valdymui, bei suformuoti integralų informacijos valdymo modelį.

Empirinėje darbo dalyje, integralaus informacijos saugumo valdymo modelio praktiniam pritaikomumui nustatyti ir pagrįsti pasitelkta mišrių metodų prieiga derinant kiekybinių ir kokybinių tyrimų metodus – dokumentų turinio analizę, anketinę institucijų apklausą ir ekspertų interviu. Derinant šiuos metodus galima užtikrinti visapusiškai argumentuotus ir patikimus tyrimo rezultatus teorinio integralaus informacijos saugumo valdymo modelio praktinei realizacijai ir pagrindimui. Empirinio tyrimo duomenims analizuoti taikyta nuoseklių procedūrų tyrimo strategija. Kokybiniai ir kiekybiniai duomenys renkami nuosekliai vieni po kitų, renkamais duomenimis detalizuoti, praplėsti bei papildyti anksčiau surinktų duomenų pagrindu gauti rezultatai. Remiantis teorinėje darbo dalyje suformuotu integraliu informacijos saugumo valdymo modeliu buvo sudaryta informacijos saugumo vertinimo prieiga, išskirti informacijos saugumo valdymo įrankiai ir apibrėžti vertinimo kriterijai. Ši prieiga taikyta identifikuotų šaltinių, formuojančių informacijos saugumo valdymo reikalavimus Lietuvos valstybės institucijoms, turinio analizei. Analizės rezultatai panaudoti formuluojant klausimus ekspertams, o kartu su ekspertų interviu įžvalgomis (iškeltais probleminiais klausimais) – sudarant kiekybinio tyrimo (institucijų apklausos) anketas.

Informacijos saugumo dokumentų, reglamentuojančių informacijos saugumo valdymą Lietuvos valstybės institucijose, turinio analizė taikyta pagrįsti informacijos saugumo valdymo Lietuvos valstybės institucijose trūkumus. Analizės rezultatai parodė, kad informacijos saugumo valdymas Lietuvos valstybės institucijose tik su išlyga gali būti pavadintas modeliu, todėl įvardijant esamą būklę naudotina *diskretaus* (atskiro nuo visumos) *informacijos saugumo*

modelio sąvoka, kurios turinį nusako informacijos saugumo valdymo reikalavimų taikymas ne visai organizacijos informacijai, o atskiroms organizacijos informacijos sistemoms.

Ekspertų interviu metodas taikytas kaip pavienių Lietuvos valstybės institucijų ir ekspertinio konteksto įvesties įrankis į atliktą teorinio integralaus informacijos saugumo valdymo modelio taikymo Lietuvos valstybės institucijoms dokumentų turinio analizės rezultatų vertinimą.

Atliekant Lietuvos valstybės institucijų apklausą buvo siekiama ištirti praktinį informacijos saugumo valdymo reikalavimų įgyvendinimą. Kiekybiniams duomenims, kaip Lietuvos valstybės institucijos įgyvendina informacijos saugumo reikalavimus, surinkti, buvo suformuotas originalus informacijos saugumo valdymo įvertinimo valstybės institucijose klausimynas. Surinktų duomenų išsami analizė padėjo detaliai įvertinti informacijos saugumo valdymo situaciją Lietuvos valstybės institucijose ir suformuluoti sudaryto teorinio integralaus informacijos saugumo valdymo modelio įgyvendinimo prielaidas.

Darbo naujumas ir mokslinė reikšmė

Darbo naujumą ir teorinį reikšmingumą lemia pasiekti informacijos vadybos mokslui svarbūs rezultatai. Darbas leido sumažinti neapibrėžtumą informacijos vadybos mokslų sistemoje, išplėtoti teorinę informacijos vadybos paradigmą informacijos vadybos mokslų sistemoje išryškinant informacijos saugumo valdymo dedamąją.

Disertacijoje, išanalizavus informacijos saugumo mokslinių tyrimų įžvalgų kismą, susisteminus informacijos saugumo sąvokas ir nustačius jų ryšius bei atlikus lyginamąją tarptautiniame lygmenyje vyraujančių informacijos saugumo valdymo priemonių analizę, suformuota ir pagrįsta informacijos saugumo valdymo turinio apibrėžtis.

Aptartas informacijos saugumo valdymo objekto diskursas ir išryškinta informacija, kaip informacijos saugumo valdymo objektas suformavo teorines prielaidas informacijos saugumo valdymui pasitelkti informacijos vadybos įrankius. Šių įrankių analizė leido išskirti informacijos vadybos įrankius, taikytinus informacijos saugumo valdymui.

Sujungiant disertacijos teorinėse dalyse atliktų mokslinių tyrimų rezultatus suformuotas teorinis integralus informacijos saugumo valdymo modelis, taikytinas tiek tolesniuose teoriniuose moksliniuose tyrimuose, tiek praktiniam taikymui. Integralaus informacijos saugumo valdymo modelio praktinis pritaikomumas patikrintas vertinant informacijos saugumo valdymą Lietuvos valstybės institucijose. Atlikto empirinio tyrimo rezultatai pagrindė teorinio modelio reikšmingumą efektyviam informacijos saugumo valdymui užtikrinti.

Disertacijos tyrimo ribos

Disertacijos tyrimas apsiriboja informacijos saugumo valdymo modelio Lietuvos valstybės institucijoms kūrimu. Tokias mokslinio darbo ribas lemia dvi pagrindinės priežastys.

1. Lietuvoje galiojantys informacijos saugumo valdymo reikalavimai plačiausiai taikomi išskirtinai valstybės institucijoms, todėl šiame sektoriuje yra didžiausia erdvė tyrimams, o įvertinant, kad Lietuvos Respublikos Vyriausybė yra deklaravusi siekį plėsti informacijos saugumo valdymo reikalavimų taikymą ir visiems kitiems sektoriams, išsamus esamos situacijos mokslinis įvertinimas būtų kaip tik laiku; pagrįstos rekomendacijos galėtų sukurti ir praktinę mokslinio darbo vertę.

2. Šis sektorius pasirinktas atsižvelgiant ir į viešosios teisės principus, nusakančius, kad viešajam sektoriui leidžiama tik tai, kas nurodyta, t. y.: 1) viešojo administravimo subjektams leidžiama tik tai, kas numatyta teisės aktuose; 2) viešojo administravimo subjektams privaloma atlikti tai, kas numatyta teisės aktuose, t. y. viešasis sektorius yra įpareigotas aiškių rėmų ir negali laisvai rinktis, kaip reaguoti į informacijos saugumo rizikas. Dėl šios priežasties Lietuvos valstybės institucijų informacijos saugumas tiesiogiai priklauso nuo galiojančių informacijos saugumo valdymo reikalavimų, o tai suponuoja, kad šie reikalavimai turi būti tinkamai pagrįsti.

Disertacijoje naudojamos pagrindinės sąvokos

Darbe naudojama ši informacijos saugumo valdymo sąvoka:

Nagrinėjant mokslinius tyrimus, pastebėtas naudojamų informacijos saugumo sąvokų nuoseklumo trūkumas. Tyrimų objekto lygmenyje mokslo darbuose tiek anglų kalba, tiek lietuvių kalba dažnai sinonimiškai naudojamos informacijos saugumo (angl. *information security*), informacijos technologijų saugumo (angl. *information technology security*), informacinių sistemų saugumo (angl. *information systems security*) sąvokos. Saugumo proceso lygmenyje nėra nusistovėjusios aiškios takoskyros tarp angliškų sąvokų *management* ir *governance* bei jų vertimo į lietuvių kalbą. Reikėtų pažymėti, kad Lietuvoje nėra griežtai nusistovėjęs ir net šiame kontekste anglų kalboje vartojamo termino *security* vertimas – *saugumas, sauga, apsauga* (pavyzdžiui, COBIT metodikos vertime naudojamos visos trys sąvokos). Šiuo metu terminas *apsauga* dažniausiai sutinkamas asmens duomenų teisinės apsaugos, privatumo kontekste, *sauga* – valstybės informacinių išteklių (registrų ir informacinių sistemų) kontekste, *saugumas* vartojamas plačiausiai, kaip apimantis visus išvardytus aspektus. Vertinant aptartą kontekstą, *informacijos saugumo valdymo* sąvoka labiausiai tinka siekiant atskleisti įvairialypį informacijos saugumo valdymo kontekstą ir disertacijoje buvo naudojama kaip apimanti (bendrąja prasme) saugumo, saugos ir apsaugos bei vadybos ir valdymo aspektus.

Darbe naudojama ši Lietuvos valstybės institucijos sąvoka:

Lietuvos valstybės institucija – atstovaujamosios, valstybės vadovo, vykdomosios, teisminės valdžios institucija, teisėsaugos institucija, auditą, kontrolę (priežiūrą) atliekanti institucija, kita valstybės institucija, kuri finansuojama iš valstybės biudžetų bei valstybės pinigų fondų ir kuriai Viešojo administravimo įstatymo nustatyta tvarka yra suteikti viešojo administravimo įgaliojimai.

Disertacijos struktūra

Disertacija sudaryta iš įvado, trijų dalių, išvadų, literatūros sąrašo ir priedų.

Pirmoje disertacijos dalyje išanalizuotos ir susistemintos informacijos saugumo apibrėžtys, atskleista informacijos saugumo sampratos genezė, išanalizuota Lietuvos ir užsienio tyrėjų informacijos saugumo tyrimų aprėptis ir problematika. Šios analizės pagrindu suformuotas informacijos saugumo valdymo turinys.

Šioje dalyje taip pat aprašytos informacijos saugumo valdymo priemonės – tarptautiniai informacijos saugumo valdymo standartai, metodikos ir modeliai, atlikta šių priemonių lyginamoji analizė.

Remiantis teoriniame tyrime suformuluotomis informacijos saugumo valdymo prielaidomis bei turiniu, atliktas žvalgomasis tyrimas: dokumentų turinio analizės metodu ištirti informacijos saugumo valdymo reikalavimai Lietuvos valstybės institucijoms ir įvertintas šių reikalavimų laikymasis konkrečioje Lietuvos valstybės institucijų grupėje – Lietuvos Respublikos ministerijose. Šio žvalgomojo tyrimo rezultatai leido pagrįsti darbo temos ir ginamųjų teiginių aktualumą, apibrėžti tolesnių tyrimų poreikį ir kryptis.

Antroje disertacijos dalyje, siekiant atskleisti saugumo valdymo ir informacijos vadybos mokslų sąsajumą, išanalizuoti ir įvertinti informacijos vadybos tyrėjų darbai, išskirti informacijos vadybos įrankiai, kuriuos būtų galima taikyti informacijos saugumui valdyti.

Apibendrinus atliktą teorinį tyrimą, sudarytas integralus informacijos saugumo valdymo modelis, jungiantis informacijos saugumo valdymo priemones ir informacijos vadybos įrankius.

Trečioje disertacijos dalyje atliktas teorinio integralaus informacijos saugumo valdymo modelio praktinio pritaikomumo galimybių empirinis tyrimas.

Empirinio tyrimo metodologija

Empirinio tyrimo objektas – integralaus informacijos saugumo valdymo modelio praktinis taikymas informacijos saugumo valdymui Lietuvos valstybės institucijose.

Empirinio tyrimo tikslas – nustatyti teorinio integralaus informacijos saugumo valdymo modelio praktinio pritaikomumo galimybes.

Empirinio tyrimo uždaviniai:

1. Suformuoti informacijos saugumo valdymo vertinimo prieigą, įrankius ir vertinimo kriterijus.
2. Nustatyti šaltinius, formuojančius informacijos saugumo valdymo reikalavimus Lietuvos valstybės institucijoms.
3. Ištirti identifikuotų šaltinių turinį remiantis suformuotos informacijos saugumo valdymo prieigos įrankiais ir vertinimo kriterijais.
4. Įvertinti, kaip Lietuvos valstybės institucijos įgyvendina galiojančius informacijos saugumo reikalavimus.

Empirinio tyrimo metodai

Remiantis teoriniu integraliu informacijos saugumo valdymo modeliu, buvo suformuota informacijos saugumo valdymo vertinimo prieiga ir atliktas informacijos saugumo valdymo Lietuvos valstybės institucijose tyrimas. Tyrimui taikyta mišrių metodų prieiga derinant dokumentų turinio analizės, institucijų anketinės apklausos ir ekspertų interviu metodus. Empirinio tyrimo rezultatai leido identifikuoti trūkumus ir suformuluoti siūlymus, kaip, remiantis integraliu informacijos saugumo valdymo modeliu, efektyviai valdyti informacijos saugumą Lietuvos valstybės institucijose.

Tyrimo rezultatai.

Remiantis suformuota informacijos saugumo valdymo vertinimo prieiga, empirinis tyrimas atliktas vertinant Lietuvos valstybės institucijoms nustatytą informacijos saugumo politiką, informacijos saugumo strategiją, informacijos saugumo auditą, informacijos saugumo brandą ir informacijos saugumo veikėjus.

Informacijos saugumo politiką valstybės institucijose apibrėžia institucijos saugumo politikos dokumentas, o informacijos saugumo valdymo objektas – informaciniai ištekliai (valstybės registrai, žinybiniai registrai, valstybės informacinės sistemos ir vidaus administravimo informacinės sistemos). Šiuo metu informacijos saugumo valdymo reikalavimai vienareikšmiškai galioja trims informacinių išteklių rūšims (neapibrėžti reikalavimai vidaus administravimo informacinėms sistemoms).

Kiekybinis tyrimas leido nustatyti, kad nors per 70 proc. Lietuvos valstybės institucijų turi informacijos saugumo politikos dokumentus, tačiau tik trečdalis tirtų institucijų turi informacijos saugumo politikos dokumentus, kurie nuosekliai apima visus šių institucijų valdomus informacijos išteklius ir nustato bendrą organizacijos saugumo politiką. Nepavaldžių Lietuvos Respublikos Vyriausybei institucijų lygmenyje jokių informacijos saugumo politikos dokumentų neturi net 63 procentai institucijų (dauguma šių institucijų valdo tik vidaus administravimo sistemas).

Tyrimo rezultatai leido konstatuoti, kad nors Lietuvos valstybės institucijoms nustatytas informacijos saugumo valdymo objektas – valstybės informacijos ištekliai – turi trūkumų (pavyzdžiui, beveik pusė valstybės informacinių išteklių yra vidaus administravimo sistemos, o joms informacijos saugumo valdymo reikalavimai nėra taikomi), tačiau jo pakeitimas kainuotų daug finansinių ir organizacinių išteklių, todėl labiau tinkamas sprendimas – patvirtinti trūkstamus informacijos saugumo valdymo reikalavimus vidaus administravimo sistemoms, o informacijos saugumo dokumentus kompleksiškai taikyti visiems konkrečios institucijos valdomiems informacijos ištekliams.

Dokumentų turinio analizė leido identifikuoti, kad valstybės institucijoms galiojantys aukščiausio lygmens informacijos saugumo valdymo reikalavimai (įstatymai ir Vyriausybės nutarimai) tiesiogiai apima tik du iš trijų informacijos saugumo valdymo tikslų – konfidencialumą ir vientisumą, tačiau neapima prieinamumo. Ekspertai išsakė abejones dėl šiuo metu tapačiai taikomų informacijos saugumo tikslų visoms valstybės institucijoms: jų manymu, institucijos turėtų turėti galimybę nustatyti prioritetus šiems tikslams taikyti atsižvelgdamos į institucijoje valdomos informacijos specifiką. Kiekybinio tyrimo rezultatai parodė, kad vertinant tiek bendrus, tiek atskirus rezultatus (pagal institucijų pavaldumo grupes) institucijos neišskyrė jokio statistiškai reikšmingo skirtumo tarp informacijos saugumo tikslų, t. y. tik maža dalis valstybės institucijų sugeba realiai įvertinti ir argumentuotai pasirinkti prioritetus tarp taikytinų informacijos saugumo tikslų. Taigi jei būtų nuspręsta suteikti institucijoms teisę rinktis, kurie informacijos saugumo tikslai joms yra prioritetas, reiktų parengti aiškias metodines rekomendacijas šių prioritetų argumentuotam pasirinkimui.

Teorinio dokumentinio tyrimo metu buvo identifikuota, kad valstybės informacijos saugumo valdymo strategijos dokumentas egzistuoja, tačiau vis dar neužtikrintas jo įgyvendinimas. Valstybės institucijos nėra įpareigotos rengti specialios informacijos saugumo strategijos, tačiau kiekybinis tyrimas parodė, kad trečdalis institucijų turi patvirtintą aktualų informacijos strategijos dokumentą. Pažymėtina, kad strategijai įgyvendinti nėra užtikrintas informacijos saugumo procesų ciklas, – kiekybinio tyrimo rezultatai parodė, kad 61 proc.

valstybės institucijų nors kartą bandė vertinti rizikas ir reaguoti į aplinkos pokyčius, tačiau tik 7 proc. valstybės institucijų tai daro nuolat.

Vertinant informacijos saugumo strategijos įgyvendinimo priemonių turinį, konstatuotas formalus atsakomybių pasidalinimas tarp institucijų, tačiau identifikuotas lėtas paskirtų užduočių sprendimas, taip pat išskirtas nevertinamas ekonominis kontekstas (pavyzdžiui, nustatytas racionaliai nepagrįstų, brangiai kainuojančių techninių priemonių privalomas taikymas) ir per mažas dėmesys žmogiškajam faktoriui.

Teorinis tyrimas leido identifikuoti, kad Valstybės informacinių išteklių įstatyme nustatytas informacijos saugumo audito vykdymas (audito reikšmę pabrėžė ir kokybiniame tyrime dalyvavę ekspertai), tačiau valstybės lygmenyje auditas nevykdomas. Institucijų lygmenyje valstybės institucijos privalo vykdyti periodinius auditus, tačiau kiekybinis tyrimas atskleidė, kad tik apie 58 proc. valstybės institucijų yra nors kartą vykdę saugumo auditą ir tik 6 proc. jų informacijos saugumo auditą vykdo nuolat.

Kokybinio tyrimo metu ekspertai praktiškai vienbalsiai pabrėžė informacijos saugumo brandos lygių nustatymo ir vertinimo privalumus. Pagal institucijų brandos lygį galėtų būti parenkamos informacijos saugumo valdymo priemonės, svarbesnius išteklius valdančios institucijos turėtų siekti atitinkamai aukštesnio brandos lygmens. Dokumentų turinio analizė leido identifikuoti tai, kad valstybės institucijoms informacijos saugumo brandos lygiai nenustatyti, vertinimo tvarka neapibrėžta.

Vertinant informacijos saugumo veikėjus, empirinio tyrimo metu nustatytas decentralizuotas informacijos saugumo valdymo organizavimas ir koordinavimas – pavienės sritys formaliai išdalintos atsakingoms valstybės institucijoms (išskyrus kritinės infrastruktūros apsaugos funkciją, kuri vienareikšmiškai niekam nepriskirta), veiklos tarpinstituciniam koordinavimui įkurta kolegiali koordinacinė komisija. Išanalizavus kompetentingų institucijų funkcijas ir jas palyginus su institucijų struktūra, etatų sąrašais bei pareigybių aprašymais, akivaizdžiai matyti, kad koordinuojančios institucijos nėra pajėgios vykdyti iškeltų joms uždavinių, neturi reikiamų etatų bei specialistų. Panašias įžvalgas kokybinio tyrimo metu pateikė ir ekspertai – jų teigimu, nors yra paskirtos kompetentingos institucijos, tačiau informacijos saugumo organizavimas pasižymi žema institucijų kompetencija, specialistų trūkumu, lėtu paskirtų užduočių sprendimu (pavyzdžiui, Lietuvos Respublikos valstybės informacinių išteklių įstatymas įsigaliojo 2012 m. sausio 1 d., tačiau dauguma jam įgyvendinti reikalingų teisės aktų vis dar neparengta).

Kiekybinis informacijos saugumo valdymo Lietuvos valstybės institucijose tyrimas padėjo identifikuoti rimtą spragą institucijų lygmenyje – 78 proc. institucijų turi už saugumą

atsakingais paskirtus saugos įgaliotinius, tačiau 60 proc. atvejų už informacijos saugumo valdymą paskirti informacinių technologijų padalinių darbuotojai ar net vadovai. Tokia situacija aiškiai prieštarauja vykdymo ir kontrolės funkcijų atskyrimo principui ir trukdo efektyviai užtikrinti informacijos saugumo valdymą.

Apibendrinant informacijos saugumo valdymo Lietuvos valstybės institucijose tyrimų rezultatus, galima teigti, kad šiuo metu valdomos tik pavienės informacijos saugumo užtikrinimo dalys, trūksta visuminio požiūrio, netaikomi įrankiai, kurie įgalintų valdomo informacijos saugumo, kaip objektyvios saugumo būsenos, sukūrimą ir išlaikymą.

Išvados

1. Nuolat augantys informacijos saugumo incidentų atvejai ir mastai iliustruoja, kad informacijos saugumo problemų aktualumas tampa kritinis, o esamos informacijos saugumo valdymo priemonės nėra pakankamos informacijos saugumui valdyti. Siaurą informacijos saugumo, kaip technologinės problemos, supratimą plečia ekonominių, vadybinių, psichologinių, teisinių ir kitų susijusių aspektų įtaka informacijos saugumui.

2. Informacijos saugumo valdymo mokslinės problemos laukas nėra visiškai susiformavęs, stebėtina tyrimų plėtra, tačiau vyrauja diskretyvi pavienių aspektų analizė: pernelyg ryškinami technologiniai aspektai; trūksta moksliškai pagrįstų sisteminių informacijos saugumo valdymo konceptų, kurie praplėstų informacijos saugumo valdymo teorinių tyrimų lauką bei lemtų teorinių paradigmų taikymą sprendžiant ryškėjančias praktines informacijos saugumo valdymo problemas tiek Lietuvoje, tiek ir globaliu mastu.

3. Informacijos saugumo valdymui tirti būtina sąlyga – vienareikšmiškai įvardytas objektas, tačiau mokslinių tyrimų bei praktinio taikymo kontekste nepakankamai aiškiai ir pagrįstai pateikiama informacijos saugumo valdymo objekto apibrėžtis (stebimas informacijos, informacinių sistemų, informacijos technologijų ir kitų saugumo objektų vartojimas).

4. Disertacijoje vienareikšmiškai įvardytas informacijos saugumo valdymo objektas – informacija. Objekto įvardijimas leidžia išskirti informacijos saugumo valdymo tikslus bei informacijos saugumo valdymui aktualius aspektus. Moksliniame darbe pagrindiniais informacijos saugumo valdymo tikslais išryškintas informacijos konfidencialumo, vientisumo ir prieinamumo užtikrinimas, o aspektai, aktualūs informacijos saugumo valdymui, sugrupuoti į strateginę, žmogiškąją ir technologinę dimensijas. Apibendrinus šias įžvalgas, disertacijoje informacijos saugumo valdymas apibrėžtas kaip siekis užtikrinti informacijos konfidencialumą, vientisumą ir prieinamumą subalansuotai derinant strateginę, žmogiškąją ir technologinę dimensijas.

5. Informacijos saugumo valdymui užtikrinti nepakanka suformuoti jo apibrėžtį, būtina numatyti ir priemones, kuriomis informacijos saugumas galėtų būti valdomas. Teigiant, kad informacijos saugumo valdymo objektas yra informacija, informacijos saugumui valdyti pasitelktini informacijos vadybos metodai ir būdai.

6. Efektyvi informacijos vadyba pasižymi suderintu įrankių taikymu. Informacijos saugumui valdyti išskirti informacijos vadybos įrankiai – politika, strategija, auditas, branda ir veikėjai. Jungiant informacijos saugumo valdymo apibrėžtį ir išskirtus informacijos vadybos įrankius, siekiama, kad būtų apibrėžta informacijos saugumo valdymo politika ir strategija, nuolat atliekamas auditas, valdomi visi informacijos saugumo užtikrinimo procesai, operatyviai prisitaikoma prie aplinkos pokyčių, paskirti kompetentingi veikėjai bei siekiamas aukštas brandos lygis. Suderinus šių įrankių taikymą, galima pagrįstai tikėtis, kad bus užtikrintas efektyvus informacijos saugumo valdymas.

Identifikavus ir kritiškai įvertinus informacijos vadybos bei informacijos saugumo valdymo diskursų sąsajas sukurtas teorinis pagrindas suformuoti integralų informacijos saugumo valdymo modelį.

7. Teorinis integralus informacijos saugumo valdymo modelis suformuoja sisteminį požiūrį į informacijos saugumo valdymo turinį, nusakantį objektą, tikslus bei priemones, ir apibrėžia informacijos vadybos įrankius, kurie sudaro sąlygas įvertinti ir užtikrinti informacijos saugumo valdymo kompleksiškumą. Modelio kompleksiškumą išryškina ir tai, kad modelyje integruoti informacijos vadybos įrankiai – politika, strategija, auditas, branda ir veikėjai – yra sietini ir su esamų informacijos saugumo valdymo priemonių trūkumais. Taigi informacijos vadybos įrankių įdiegimas informacijos saugumo valdymui leidžia sustiprinti esamas silpnas vietas ir taip užtikrinti efektyvų ir kompleksišką informacijos saugumo valdymą.

8. *Teoriniame lygmenyje sukonstruoto integralaus informacijos saugumo valdymo modelio praktinį reikšmingumą atskleidžia empirinio informacijos saugumo valdymo Lietuvos valstybės institucijose tyrimo rezultatai:*

- ✓ Specialaus įstatymo, nuosekliai reglamentuojančio su informacijos saugumu susijusius santykius, Lietuvoje nėra. Informacijos saugumo politiką valstybėje nustato Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas, institucijose – saugumo politikos dokumentas (duomenų saugos nuostatai). Šie dokumentai informacijos saugumo valdymo objektu įvardija informaciją, apdorojamą valstybės informaciniais ištekliais (valstybės registrais, žinybiniais registrais, valstybės informacinėmis sistemomis ir vidaus administravimui skirtomis informacinėmis sistemomis).

- ✓ Informacijos saugumo valdymo reikalavimai, taikomi pavieniams valstybės informaciniams ištekliams, turi trūkumų – šis objektas vienareikšmiškai neapima visos valstybės institucijos valdomos informacijos, o privalomi informacijos saugumo valdymo reikalavimai nepatvirtinti vidaus administravimui skirtoms sistemoms, kurios sudaro 48 proc. visų Lietuvos valstybės institucijose valdomų informacinių išteklių (šiems ištekliams reikalavimai yra rekomendacinio pobūdžio, o rekomendacinių informacijos saugumo valdymo reikalavimų nesilaiko daugiau nei pusė Lietuvos valstybės institucijų).
- ✓ Valstybinė informacijos saugumo valdymo strategija dokumentuota, nustatyti ilgalaikiai tikslai, uždaviniai bei šių siekinių vertinimo kriterijai, tačiau vis dar neapsispręsta dėl detalių įgyvendinimo veiksmų bei nepriimti strateginiams nuostatams įgyvendinti reikalingi teisės aktai.
- ✓ Nuolatinis informacijos saugumo valdymo ciklas nėra užtikrintas – tik 7 proc. valstybės institucijų nuolat taiko reagavimo į aplinkos pokyčius priemones (rizikų analizes ir pan.), o informacijos saugumo valdymo priemonės nustatytos neįvertinus ekonominio konteksto (kai kurių galiojančių informacijos saugumo priemonių įgyvendinimas nepagrįstai brangiai kainuoja), taip pat per mažas dėmesys skiriamas žmogiškajam faktoriui.
- ✓ Norminiai dokumentai, formuojantys informacijos saugumo reikalavimus Lietuvos valstybės institucijoms, nustato informacijos saugumo audito vykdymą. Tačiau pats informacijos saugumo audito procesas nėra tinkamai apibrėžtas ir vykdomas, neauditуojama informacijos saugumo politika ir jos įgyvendinimo procesas, atsakingų už informacijos saugumo valdymo koordinavimą institucijų funkcijų vykdymas, neužtikrinama kontrolė, kaip valstybės institucijos įgyvendina informacijos saugumo valdymo reikalavimus, nežinoma reali situacija Lietuvos valstybės institucijose, nevaldomi informacijos saugumo procesai. Didelė dalis valstybės institucijų galiojančius reikalavimus taiko tik formaliai.
- ✓ Informacijos saugumo valdymui koordinuoti Lietuvoje taikomas decentralizuotas modelis – su informacijos saugumo valdymo koordinavimu susijusios funkcijos paskirtos kelioms institucijoms (išskyrus kritinės infrastruktūros apsaugos funkciją, kuri vienareikšmiškai niekam nepriskirta), įkurtas kolegialus tarpinstitucinio koordinavimo organas – nuolatinė komisija. Tačiau informacijos saugumą koordinuojančios institucijos nėra pajėgios vykdyti iškeltų joms uždavinių –

informacijos saugumo organizavimas pasižymi žema institucijų kompetencija, specialistų trūkumu, lėtu paskirtų užduočių sprendimu.

- ✓ Lietuvos valstybės institucijose vyrauja techninis požiūris į informacijos saugumą; tinkamai neatskirtos informacijos saugumo valdymo įgyvendinimo ir kontrolės funkcijos trukdo efektyviai užtikrinti informacijos saugumo valdymą (tyrimo rezultatai atskleidė, kad 60 proc. atvejų valstybės institucijose už informacijos saugumo valdymą paskirti informacinių technologijų padalinių darbuotojai ar net vadovai).
- ✓ Informacijos saugumo brandos lygiai ir jų įvertinimo tvarka Lietuvos valstybės institucijoms neapibrėžti. Branda yra vienas svarbiausių sėkmingo tikslų įgyvendinimo ir valdymo procesų tobulinimo veiksnių, pagal institucijų brandos lygį turėtų būti parenkamos informacijos saugumo valdymo priemonės, svarbesnius išteklius valdančios institucijos turėtų siekti atitinkamai aukštesnio brandos lygmens.

9. *Empirinio tyrimo rezultatai leidžia teigti:*

- ✓ užtikrinant informacijos saugumą Lietuvos valstybės institucijose valdomos tik pavienės informacijos saugumo užtikrinimo dalys, vyrauja formalus techninis požiūris, netaikomi įrankiai, kurie įgalintų valdomo informacijos saugumo, kaip objektyvios saugumo būsenos, sukūrimą ir išlaikymą;
- ✓ Lietuvos viešajame sektoriuje vyraujantis formalus požiūris į informacijos saugumą pasireiškia patvirtintų, tačiau neįgyvendintų teisės aktų ir neparengtų įgyvendinančių dokumentų gausa (trūksta informacijos saugumo reikalavimams, įtvirtintiems įstatymu ir strateginiais dokumentais, įgyvendinti būtinų teisės aktų; institucijų vidiniai informacijos saugumo valdymo dokumentai neperžiūrimi ir neatnaujinami; formaliai įtvirtintų priemonių tinkamas įgyvendinimas nekontroliuojamas);
- ✓ pastebėta didesnė branda valstybės institucijų, kurioms galiojantys informacijos saugumo valdymo reikalavimai jau ilgą laiką yra privalomojo pobūdžio (ministerijos, kitos Vyriausybei pavaldžios institucijos).

10. *Siekiant efektyvaus informacijos saugumo valdymo Lietuvos valstybės institucijose, šalia aptartų trūkumų šalinimo, informacijos saugumo valdymas turėtų būti tobulinamas šiomis kryptimis:*

- ✓ Lietuvos valstybės institucijoms turėtų būti patvirtinti privalomi informacijos saugumo valdymo reikalavimai, apimantys visus valstybės informacinius išteklius ir nustatantys, kad kiekvienoje valstybės institucijoje būtų vienas informacijos

saugumo valdymo politikos dokumentas (duomenų saugos nuostatai), kuriuo būtų bendrai apibrėžiami visi tos valstybės institucijos valdomi informaciniai ištekliai.

- ✓ Informacijos saugumo valdymo reikalavimų tikslas turėtų būti – užtikrinti visos valstybės institucijos valdomos informacijos konfidencialumą, vientisumą ir prieinamumą (šiuo metu nėra vienareikšmiškai apibrėžtas prieinamumo tikslo siekinys, o tai tampa ypač aktualu vertinant pastarųjų metų tendencijas – įvairias kibernetinės erdvės atakas, kurioms pavykus, informacijos ištekliai tampa neprieinami). Šių tikslų prioritetai turėtų būti nustatomi pagal konkrečios institucijos valdomos informacijos specifiką, pagal tai parenkant ir taikomas informacijos saugumo užtikrinimo strategines, žmogiškąsias ir technines priemones. Atsižvelgiant į tai, kad valstybės institucijos neturi pakankamai kompetencijos pačios nusistatyti prioritetų, bendram efektyviam informacijos saugumo valdymo procesui užtikrinti, turėtų būti parengti aiškūs prioritetų nustatymo ir priemonių pasirinkimo kriterijai.
- ✓ Siekiant valstybės institucijų veiklos efektyvumo, reikėtų stiprinti koordinuojančias institucijas (vienareikšmiškai ir konkrečiai paskiriant atsakomybę), joms pavesti centralizuoti informacinės infrastruktūros naudojimą (prieš tai ją inventorizavus), teikti centralizuotą metodologinę pagalbą institucijoms (pasitelkiant viešojo, privataus ir mokslo sektorių bendradarbiavimą) bei užtikrinti nuolatinį informacijos saugumo valdymo vertinimą ir kontrolę pagal vienodą metodiką ir aiškius vertinimo kriterijus. Informacijos saugumo brandos lygiams apibrėžti ir vertinimo tvarkai nustatyti tikslinga pasiremti tarptautinėmis metodikomis ir praktikomis.

11. Teoriniame lygmenyje sukonstruotas integralus informacijos saugumo valdymo modelis atskleidžia kompleksinį požiūrį į informacijos saugumą, integruoja informacijos vadybą ir informacijos saugumo valdymą bei leidžia identifikuoti informacijos saugumo valdymo Lietuvos valstybės institucijose trūkumus, o šiuos trūkumus pašalinus, užtikrinti kompleksišką ir efektyvų informacijos saugumo valdymą. Empirinis tyrimas ir gauti rezultatai pagrindė teoriniame lygmenyje sukonstruoto modelio pritaikomumą tiek tolesniems teoriniams moksliniams tyrimams, tiek praktinėje Lietuvos valstybės institucijų veikloje.

Atliktų teorinių ir empirinių tyrimų rezultatai leidžia teigti, kad disertacijos tikslas pasiektas, – teoriniame lygmenyje suformuotas integralus informacijos saugumo valdymo modelis yra teoriškai bei empiriškai patikrintas ir gali būti taikomas Lietuvos Respublikos valstybės institucijoms.

Publications during the period of writing of the thesis:

Disertacijos rengimo metu paskelbtos publikacijos:

S. Jastiuginas. Informacijos saugumo valdymas Lietuvos viešajame sektoriuje. *Informacijos mokslai*. 2011, t. 57, p. 7–24.

S. Jastiuginas. Integralus informacijos saugumo valdymo modelis. *Informacijos mokslai*. 2012, t. 61, p. 7–30.

S. Jastiuginas. Integralaus informacijos saugumo valdymo modelio taikymas Lietuvos valstybės institucijoms. *Informacijos mokslai*. 2012, t. 61, p. 31–58.

Research carried out during the writing of thesis was presented in the following reports delivered at conferences and seminars:

Disertacijos rengimo metu atlikti tyrimai buvo pristatyti skaitant pranešimus mokslinėse konferencijose ir seminaruose:

2008 m. lapkričio mėn. 7–8 d. Lisabonoje mokslinėje konferencijoje *Skaitmeninio Saugumo Forumas (Digital Security Forum)* pristatytos informacijos saugumo valdymo Lietuvos valstybės institucijose aktualijos, moksliniame seminare aptarta informacijos saugumo ir informacijos vadybos sąsajumo problematika.

2010 m. gruodžio 17 d. Vilniaus universiteto Komunikacijos fakulteto mokslinėje praktinėje konferencijoje „Komunikacijos ir informacijos vadybos raiškos ir modeliai“ skaitytas pranešimas „Informacijos saugumo valdymas Lietuvos valstybės institucijose: problemos ir galimybės“.

2011 m. gruodžio 16 d. Vilniaus universiteto Komunikacijos fakulteto mokslinėje konferencijoje „Informacijos ir komunikacijos teorijos ir praktikos raiškos“ skaitytas pranešimas „Informacijos saugumas informacijos vadyboje: teorija ir praktika Lietuvos viešajame sektoriuje“.

Informacija apie autorių

Saulius Jastiuginas 2000 m. Vilniaus universiteto Komunikacijos fakultete įgijo komunikacijos ir informacijos (informologijos programa) bakalauro diplomą, 2002 m. apgynė komunikacijos ir informacijos (tarptautinės komunikacijos programa) magistro laipsnį. Nuo 2001 metų dirbo informacinės visuomenės politikos formavimo srityje, specializavosi nagrinėjant informacijos saugumo ir elektroninės valdžios problematiką. 2008 m. įstojo į Vilniaus universiteto humanitarinių mokslų srities komunikacijos ir informacijos mokslo krypties doktorantūrą. Nuo 2003 m. dėstė Vilniaus universitete Tarptautiniame žinių ekonomikos ir žinių vadybos (UNESCO) centre, vėliau Vilniaus universiteto Komunikacijos fakultete. Dėstyti Informacijos technologijų ir telekomunikacijų saugos, Informacijos sistemų, Informacijos sistemų audito ir Informacijos saugumo valdymo kursai. Moksliniai interesai: informacinių sistemų sauga, informacinių sistemų auditas, informacijos saugumo valdymas.

Information about the author

Saulius Jastiuginas graduated from Vilnius University, Faculty of Communications in 2000 with the degree of Bachelor of Communication and Information. In 2002, he was awarded the degree of Master of Communication and Information. He has been working in the field of information society development since 2005 and has experience in the e-government and information security management. In 2008, he enrolled in the doctoral studies in the area of the Humanities, the strand of communication and information science, at Vilnius University. He has been teaching since 2003 at the International knowledge economy and knowledge management (UNESCO) center of Vilnius University, later at the Faculty of Communication of Vilnius University. Courses delivered: Information technology and telecommunications security, Information systems, Audit of information systems and Information security management. Research interests: information systems security, audit of information systems, information security management.