Conceptual Information Modelling within the Contemporary Information Security Policies

Aleksandar Klaić*, Marin Golub **
* Office of the National Security Council, Zagreb, Croatia
** Faculty of Electrical Engineering and Computing, Zagreb, Croatia
aleksandar.klaic@public.carnet.hr; marin.golub@fer.hr

Abstract – The contemporary information security policies are analysed in the paper. These policies are characterised by increased similarities among the information security requirements of different sectors of society. Also, they are characterised by the increased differences in comparison with the traditional approach to the security within the closed environment. Key factors of the information security policy: people, process, and technology, are closely related to the requirements and restrictions imposed on certain type of information. In that way the approach to conceptual information modelling becomes one of the central problems of contemporary information security policies. The paper elaborates the approach to the conceptual information modelling, stressing the requirements of both the protection and the sharing of information. It offers the taxonomy of the main terms, which is the base for the development of proposed conceptual model of the information definition and sharing. The conceptual model is based on the standard UML graphical notation that makes it easier to visualize and understand the proposed model and the approach applied in the paper. The proposed model introduces formalized and more structured approach to this field in order to facilitate the development of the solutions that can keep up with the growing complexity of contemporary information security policies.

I. INTRODUCTION

The contemporary information security policies that are used in both the government and private sectors are analysed in the paper. These policies are characterised by increased similarities among the information security requirements of different sectors of society. There are also considerable differences of today's approach to information security in comparison with the traditional approach within the closed environments. Key factors of the information security policy: people, process, and technology, are closely related to the requirements and the restrictions imposed on certain type of information.

Information becomes very important factor within today's cyberspace. The term cyberspace is defined as virtual global environment of mutually connected public and private information systems, in which information, including specific ones that are dominant in the view of information security requirements, are created and transmitted [1]. This development of technology and society makes the problem of the approach to different types of information to become central issue of contemporary policies. Traditionally, information is the key asset that is protected within the information security policies of the government sector [2] [3]. On the other hand, during the last two decades the approach to information security has rapidly developed, and that fact initiated the parallel process of international standardisation. The risk management methods are increasingly applied and that fact has extended the focus of the policies from information and information assets to the wider range of tangible and intangible assets. All these assets have significant values to their owners [4].

The whole range of processes that have security influence on both the government bodies and private companies were caused by the development of society and technology, and followed by the appearance of new threats and vulnerabilities. First it was the development of technology and as a consequence we have today's business processes dependency on information systems and Internet. Actually, it is the dependency on the elements of the cyberspace. Besides that, since the 1990s there were a lot of national processes of liberalization of some sectors such as telecommunications, energy, and transport. That had and still has the influence on national security [5]. All these processes have led to the changes of people's professional and private lives, deeply influencing them through the social networking sites, different internet services, and the new mobile gadget market. The result is the constant and persistent exchange of information within all parts of our professional and private lives [6]. The similar process of constant and persistent exchange of different information including confidential ones is happening on the level of legal entities. Good example is the area of national critical infrastructure, or European Union (EU) critical infrastructure protection program [7].

Closed information systems (isolated, air-gap) are decreasingly applicable even in the traditionally closed environments of government classified information systems. Such changes in the environment necessarily demand changes in the information security policy approach on the two levels. First level is the necessity of adjustment of the new approach to the policies of information system security in order to adapt them to open commercial information and communication resources [3]. Second level is even more sensitive because the approach has to be adjusted in the wider sense of the information security policy as the whole. It is the problem of categorizing different types of information within the contemporary environment based on their security criteria. This is much wider coverage of information comparing to the classified information domain, or trade secret domain for example.

Communication needs today extend the scope of previous information security policies both in the industrial and in government sectors. This includes for example the need to exchange certain information among the entities from different sectors and the demands for handling specific types of information like personal data or intellectual property.

Cyberspace represents significantly changed environment both in the sense of form, amount, and types of information, and in the sense of different and more complex regulatory requirements. Further on, there is the necessity of international cooperation and global information exchange that leads to added complexity both in the approach and in the content of contemporary information security policies. Such growing complexity looks for the new approaches to facilitate practical solutions in this field. So far, the development of information security policies has been mostly based on the best practises and standardisation processes. Such approach has offered adequate solutions within the organisation's local environment [8].

The paper presents the overview of some results of our research in the field of modelling the briefly introduced domain of contemporary information security policies. The focus of interest in the paper is primarily in the information definition and information sharing issues.

II. Conceptual Information Modelling within the Contemporary Information Security Policies

The paper elaborates the approach to conceptual modelling of information within the frameworks of contemporary information security policies, stressing not only the need for protection of information, but also the need for information sharing ("need-to-know" versus "responsibility-to-share"). Conceptual information model is elaborated within the scope of protected national and business assets and through the development of approach to information sharing. In this paper we present the conceptualization of information types and information sharing approaches based on the domain knowledge.

Conceptualization of the domain such as the contemporary information security policies makes it possible to better associate existing knowledge which is available in different forms. Due to these different forms existing knowledge has relatively weak relations among subdomains from the point of view of information security policy. Different forms of existing knowledge are for example knowledge data bases (e.g. threats and vulnerabilities), or procedural knowledge known from the best practises and comprised within some information security standards [4] [28]. According to [25], in order to make specification of conceptualization (the development of the domain ontology), three types of knowledge have to be mapped: declarative knowledge (Know-about Knowledge), procedural knowledge (Know-how Knowledge), and relational knowledge (Know-with Knowledge). Declarative knowledge is represented with the taxonomy terminology, actually the selection of concepts. Procedural knowledge is the description of meaning of such concepts, and finally, relational knowledge is represented by the relations of modelling concepts. Recognizing and mapping of the concepts with the goal to develop ontology in the field of information security policy is the research subject of several research projects [8]. So far, these research projects have been mostly focused on explicit knowledge expressed within certain information security standards [26]. In this paper authors are primarily focused on the conceptualization of implicit and tacit knowledge, contained in different policy frameworks, requirements, and standards for the development of contemporary information security policy.

A. The Issue of the Approach to Different Types of Information

The approach to different types of information within information security policies mostly has characteristics of government or business sector that certain organisation belongs to. The approach is normally adapted to the exchange of the similar type of information with the similar type of organisations. In this approach closed within the sectors there are predefined information categories essential for such approach (e.g. classified information). The sets of minimal protection measures are applied on these predefined information categories. With the approach on the lower level of individual organisational entity (legal entity), the value of certain internal sets of information is assessed. Certain security controls are applied on these sets based on the locally assessed risks. In both cases information sharing is based on the fact that the comparable type of information can be recognized on both sides that want to share information. Besides that, the risk of accepting the same protection measures for their own information, or received information has to be acceptable (reciprocity). This approach is mostly satisfactory within the narrow framework of certain government or business sector.

If we want to extend the described possibilities to cover the approach outside the framework of certain sector, the key problem is incompatibility of locally applied information security policies concerning the access to information („need-to-know"), protection of information (baseline protection or risk management), and the information sharing approach („responsibility-to-share"). Traditional approach to the information security in government sector is focused mostly on the categories of information according to their confidentiality criterion (classified information). On the other hand, regulation requirements are increasingly focused on different types of information (e.g. personal data, intellectual property) that are exposed to the different threats in cyberspace. Also, the information sharing requirements increasingly become the part of regulation demands, e.g. critical infrastructure protection. Furthermore, the increased usage of commercial communication and information resources, lead to the appearance of a range of new types of information that may become security problem to any organization [6].

Within the last few years several governments have initiated the analysis of these issues within their information security policies. The common tendency among these initiatives can be noticed. It is the separation of the domain of unclassified, sensitive, and officially used information from the domain of classified

information. On the one hand the reason for that is the requirement of transparency of work of the government sector. This means that the categories of sensitive information such as "For Official Use Only", "Controlled Unclassified Information", or the introduction of Limited Dissemination Markings, are used in many cases instead of previously used classified information (secret information). On the other hand, these are some of the mechanisms (new categorisation, limitation of distribution etc.) that should facilitate today's information sharing approaches, especially among entities from different sectors. The examples of described initiatives can be seen in a number of countries all over the world, e.g. France [9], Australia [10], or U.S.A. [11]. EU has also this type of unclassified official information marked „Limite" (sensitive but not secret) [12]. For the protection of this type of information EU uses the concept of professional secret [13]. The importance of these initiatives can be seen from the statistical information given by EU that 75% of all the information used within the Council of EU during the year 2010 was marked as „Limite" [12].

Big international organizations such as EU and NATO need to have consistent approach to the information security policy due to their complex organisation. Consistency can be hard to accomplish without certain formalization of the approach and without structured elaboration of the policy requirements and concepts. Good example of such approach is visible in the European Commission plan regarding the new concept of personal data protection in the EU [14]. This new EU regulation will be introduced by 2015 and the key novelty is the unification of the concepts regarding personal data protection across the EU member countries. Primary reason for the change of the approach is to improve consistency of the implemented measures for personal data protection of the EU institutions, EU member countries, and the legal entities registered in those countries. Cooperation of different international, governmental, non-governmental and legal entities within the complex environment of international peace keeping activities is another example of the necessity of certain level of formalization and more structured elaboration of requirements and concepts related to the different types of information. The reason is that all these different participants need to access certain type of classified and sensitive information in the field that in some cases are not recognized by their information security policies.

Conceptual information modelling today is also used in some e-Government projects primarily due to the requirements of interoperability of information systems [15]. In accordance with their purpose the focus of these projects is mostly on the certain architectural view of the system and on the certain specific project goals [16] [17] [18]. There are also researches related to the possibilities of using conceptualization of the decision making process [19], which is partly related to the problems of regulation compliance within the domain of information security policy.

B. Modelling of the Contemporary Information Security Policies

The described security challenges lead to the need of introducing formal methods and structured elaboration of requirements and concepts within more and more complex domain of information security policy. According to [20] the complexity of the security environment is the reason that the issues of the policy should be looked at within much wider context than the certain organisational entity is. Also, in [20] it is concluded that the traditional analytical role of engineers in today's circumstances of fast changes of the security environment should be extended in order to allow engineers to participate in the regulation role (regulation and standardisation, national and international level). That is the only way how to create conditions necessary to set up security relationships in the complex global and local environment according to Fig.1 [20].

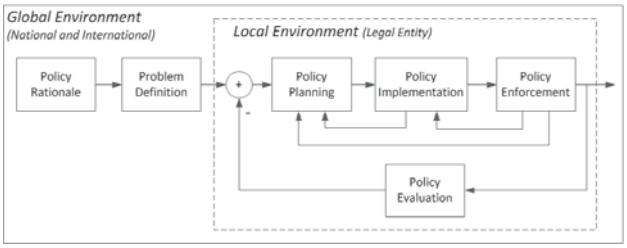

Figure 1. Lifetime phases of the information security policy

During the development process we have transformed the scheme from Fig. 1 according to the model shown in Fig. 2. This model in Fig. 2 represents the domain of contemporary security policies and it gives us the different view on the global and local levels of the policy shown in Fig.1. Fig. 2 shows very important part of the model were the global and local environment are confronted. For the purpose of this paper the term "environment" includes all the elements that are controlled through the information security policy of an organizational system, and the elements that influence on that system and its policy. Model is conceptualized as the set of mutually connected subsystems that describe certain parts of the domain of the information security policy. Conceptual modelling of information is shown through the description of the subsystems tightly related to the information issues. Primarily, it is the information definition within the interface part between the global and local environment of the model, and the information sharing part within the global environment part of the model in Fig. 2.

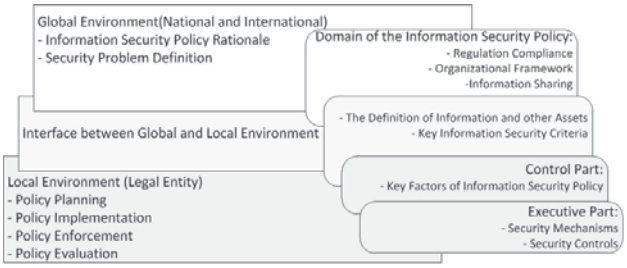

Figure 2. Modelling of the Contemporary Information Security Policies

C. Development of the Taxonomy and the Conceptualisation of the Terms

The hierarchical taxonomy of the terms is defined according to the domain of information security policy defined in [8]. Contemporary requirements and restrictions of handling different kind of information types are also taken into account, both from the point of view of government and private sectors. Taxonomy is used as a classification schema, which structures the knowledge within the domain and creates the hierarchical set of key terms. Further elaboration of taxonomy terms is based on theoretical analysis of the logical terms within the domain, as well as on the available best practises within different sectors and fields of application.

The analysis encompasses the information domains dominant from the point of view of information security (classified information, unclassified information, personal data, and intellectual property). It also encompasses societal and business sectors with specific requirements in the field of information security (e.g. government sector, telecommunication providers, and critical infrastructure protection). Different approaches to the information security policy in government and private sector are also taken into account [2]. The proposed taxonomy is elaborated with a view to future extensions, especially within the executive part of the model from the Fig 2. In that way such taxonomy is a good base for the definition of common terminology necessary in such a complex and heterogeneous field of information security policy.

The requirements imposed on the selection of categories and terms within the proposed taxonomy are used according to [21]:

1. Mutually exclusive categories that do not overlap;
2. Exhaustive categories including all possibilities;
3. Unambiguous and clear categories;
4. Repeatability;
5. Logical and intuitive acceptability;
6. Usefulness for the field of interest.

The structure of the taxonomy is elaborated following these requirements and it is divided into subsystems shown on the right-hand side of the Fig. 2. This paper is limited to the overview of the research results within the part of the taxonomy that deals with information conceptualisation. Hierarchical taxonomy is transformed into tabular view of the concepts and subconcepts in order to facilitate the elaboration of taxonomy terms into model concepts. Model concepts have to be recognized both as the categorization and as the mutual relationships of the domain terms. In this way the first part of the recognition of the basic relations among the domain terms is done. These are the groups of the relations of the type such as "is-a" (generalization), "consists-of" (composition), and "contains" (aggregation). The sample of our taxonomy is shown in tabular view in Table I.

TABLE I. THE ELABORATION OF THE HIERARCHICAL TAXONOMY, SUBSYSTEMS AND CONCEPTS/SUBCONCEPTS VIEW (SAMPLE)

DEFINITION OF INFORMATION AND OTHER ASSETS: Intangible Assets, ...	
Intangible Assets:	Information, Personnel, Software Support, Services, Intellectual Property, ...
Information:	Publicly Available information, Personal Data, Internal Sensitive Information, Confidential Information, Strictly Confidential Information, Classified Information
Personnel:	Qualification, Skills, Experience
Software Support:	Operating Systems, Software Applications, Software Support
Services:	Communication and Information Services, Other Services
Intellectual Property:	Copyright, Industrial Property Rights
Industrial Property Rights:	Patent, Trademark, Trade Secret, ...

The next step in the development process is the further elaboration of the specification of hierarchical taxonomy from Table I. into ontological model that is used for modelling information security policies. As it is already mentioned in the part of introduction of section II of the paper, ontology is treated as the explicit specification of conceptualization and represents the domain knowledge in formal and structured form [22].

One of the problems that have to be solved throughout the conceptualization of the model is the use of appropriate tools [20]. Considering the complex and very heterogeneous domain of contemporary information security policies we propose the use of standard graphical notation of Unified Modelling Language (UML) [23]. Similar approach is recommended in [24], but with the difference of using modified UML elements. UML comply with the ontology requirements in the sense of class definition and relation notation. UML graphical notation facilitates visualization and understanding of the model and the modelling approach in this paper.

D. Definitions of Information and Other Assets

Definitions of information and other assets is the interface between the upper and the lower part of our model from Fig. 2. This is one of the model subsystems that consist of the definition of general organizational assets from the business point of view. Assets are represented through the key information criteria of confidentiality, integrity, and availability.

In the model from Fig. 2 it is necessary to look at this subsystem from the global environment point of view of the requirements that are imposed on certain type of information (e.g. regulation compliance). The model also has to represent the requirements imposed on the key factors of the policy (people, process, and technology). These requirements are imposed on them because the need to handle protected assets. Key factors of the policy are treated through the control part of the model which describes local environment (lower right-hand part of the model on Fig. 2).

Modelling of the concepts in UML is done through the creation of the subsystem metaconcepts which are part of the metamodel of contemporary information security policies (Fig. 3). Metamodel allows the creation of different kind of policies that can be applied to particular organizational entities.

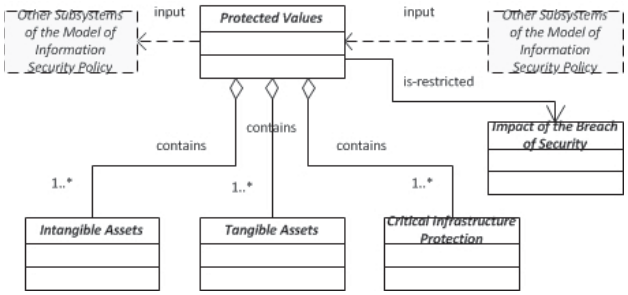

Figure 3. Basic concepts of the subsystem "Definitions of information and other assets" shown in UML class diagram

Information security criteria are generally used for the selection of security controls (assets protection in general) or security mechanisms (classified information protection). Categorisation of information is primarily done according to confidentiality levels (Fig. 4), while other two criteria (integrity, availability) are applied more on the information infrastructure and services that depends on operational needs of organizational entity (local environment). The role of confidentiality (secrecy and privacy) is important in the model as a whole because it depends not only on organizational needs, but also on global requirements (e.g. regulation compliance or information sharing).

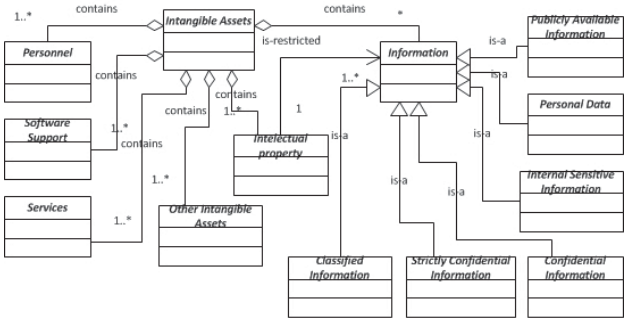

Figure 4. Elaboration of the concept of intangible assets in UML class diagram

The elaboration of the concept "Information" from Fig. 4 incorporates important category of publicly available information (key criteria are integrity and availability) which are further elaborated from the other point of view in the information sharing subsystem (Fig. 6). In Fig. 4 we have introduced the categories such as personal data, classified information, and also internal sensitive information explained in the section II.A of the paper. We encompass in this category 3-level system of classification of sensitive information proposed by [27]. This way of classification is increasingly used throughout private sector and more recently also in government sector (justice, finances, etc.).

E. Information Sharring

The subsystem of information sharing is comprised of basic concepts such as sharing subjects (entities from different sectors), sharing organization, and public information sharing. Sharing subjects are related with the concept of sharing organization according to Fig. 5. Sharing organization implies the organization of subjects in the communities of interest in such a way that there is internal community coordination (domains/users, information meaning, protocols for access) fully aligned with the external community requirements for interoperability rules (organizational, semantic, and technical rules).

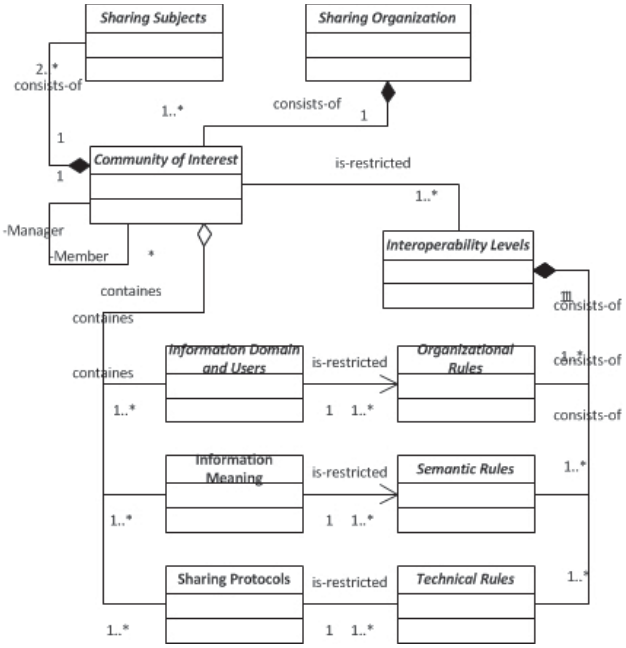

Figure 5. Elaboration of the concept of information sharing organisation in UML class diagram

Concept of public information sharing is one of the key concepts in contemporary information security policies. It is developed and shown in Fig. 6.

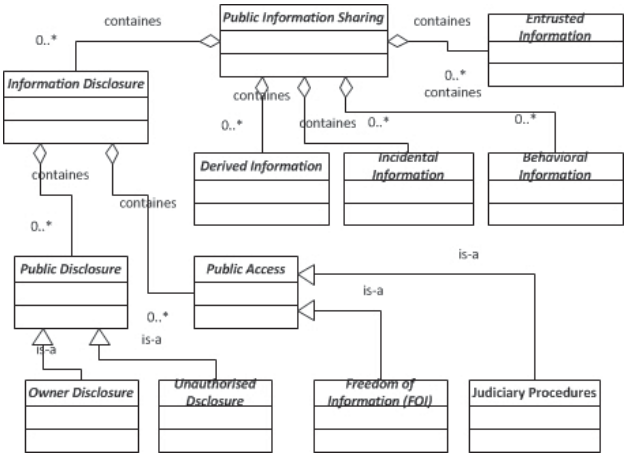

Figure 6. Elaboration of the concept of public information sharing in UML class diagram

Public information sharing concept in Fig. 6 uses several subconcepts according to [6] such as entrusted information. Entrusted information is information which is not under control of its owner because the owner entrusted it to other subjects. There are also behavioural information that is comprised of information collected by the service provider, incidental information that is comprised of what other information owners write or post on somebody or something, and derived information which can be analytically or statistically derived from other publicly available information. Information disclosure concept is further elaborated regarding the public disclosure and

public access concepts. Apart from the information definition and information sharing concepts there are some other concepts related to information in the lower, executive part of the model from Fig. 2. These concepts are not presented in this paper because they primarily present explicit knowledge defined in different regulation and standardization acts [14] [26] [28].

III. CONCLUSION

The paper presents our research related to the modeling approach of the contemporary information security policies, in the part that deals with conceptual information modeling. Presented model introduces formalized and more structured approach in order to facilitate the development of solutions that can keep up with the growing complexity of contemporary information security policies. The approach proposed in this paper consists of the elaboration of hierarchical taxonomy within the information security policy domain, the thorough analysis of the taxonomy terms, the conceptualization of the key terms, and the model development using UML class diagrams.

The proposed approach is illustrated in the paper through the conceptual information modeling that we consider as the central part of the proposed modeling approach. The paper shows the elaboration of hierarchical taxonomy in the part of information definition and sharing, the transformation of taxonomy terms in the tabular view of the concepts and subconcepts, and further elaboration of the concepts in the UML class diagrams.

Further research will be focusing on the development of the complete model of contemporary information security policies based on the approach proposed in this paper.

REFERENCES

[1] A. Klaić, A. Perešin, "The Impact of the National Information Security Regulation Framework on Cyber Security in Global Environment", Corporate Security in Dynamic Global Environment - Challenges and Risks, Institute for Corporative Security Studies, p. 85-96, Ljubljana, 2012

[2] A. Klaić, "Information Security in Business and Government Sectors", MIPRO 2005, Conference Proceedings BIS/DE/ISS, p. 193-198, Opatija, 2005

[3] Council Decision (2011/292/EU of 31 March 2011) on the security rules for protecting EU classified information, OJ L-141, 27.05.2011, p. 17-65, 2011

[4] HRN ISO/IEC 27001:2006 (ISO/IEC 27001:2005), www.iso.org

[5] A. Klaić, F. Turek, "Nacionalna sigurnost i telekomunikacije" (in Croatian), („National Security and Telecommunications"), Međunarodne studije, (1332-4756) II (2002), 4, p. 97-112, Zagreb, 2002

[6] B. Schneier, "A Taxonomy of Social Networking Data", IEEE Security&Privacy,http://www.schneier.com/essay-322.html, 2010

[7] A. Perešin, A. Klaić, „Povezanost koncepata kritične nacionalne infrastrukture i zaštite podataka" (in Croatian), „The Relation between the Concepts of the Critical National Infrastructure and the Data Protection", 3rd International Conference "Crisis Management Days", p. 13-29, Velika Gorica, May 2010

[8] A. Klaić, "Overview of the State and Trends in the Contemporary Information Security Policy and Information Security Management Methodologies", MIPRO 2010, Conference Proceedings Vol. V. DE & ISS & miproBIS &GLGPS &SP, p. 136-141, Opatija, 2010

[9] Secrétariat général de la défense et de la sécurité nationale, „Instruction générale interministérielle sur la protection du secret de la défense nationale" (in Franch), („General Interministerial Directive on the Protection of the National Defence Secret"), Paris, 2010

[10] Australian Government, "Information security management guidelines - Australian Government security classification system", V 1.0, July 2011

[11] The White House, "Executive Order 13556 - Controlled Unclassified Information", November 2010

[12] Council of the European Union, "Handling of Documents Internal to the Council", 11336/11, Brussels, June 2011

[13] Council Decision (2009/937/EU of 1 December 2009) adopting the Council's Rules of Procedure, OJ L-325, 11.12.2009, p. 35-6, Brussels, 2009

[14] European Commission, "Safeguarding Privacy in a Connected World - A European Data Protection Framework for the 21st Century", COM(2012) 9 final, Brussels, 2012

[15] S. Peristeras, K. Tarabanis, S. K. Goudos, "Model-driven eGovernment Interoperability: A Review of the State of the Art", Elsevier, Computer Standards & Interfaces, 31 (2009), p. 613-628, 2009

[16] Federal Enterprise Architecture (FEA) Program, "The Data Reference Model", Version 2.0, USA, November 2005

[17] FEA, "Consolidated Reference Model Document", Version 2.3, USA, October 2007

[18] US Department of Defence, "Guidance for Implementing Net-Centric Data Sharing ", DoD CIO, April 2006

[19] S. Al shayji, N. El Zant El Kadhi, "Building Fuzzy-Logic Ontology for Political Decision-Makers", International Journal of Mathematical Models and Methods in Applied Sciences, Issue 5, Volume 5, 2011

[20] A. Klaić, N. Hadjina, "Methods and Tools for the Development of Information Security Policy – A Comparative Literature Overview", Proceedings of the 34th International Convention MIPRO 2011, Vol. V., Conferences: DE & ISS & miproBIS & GLGPS & SP, p. 190-195, Opatija, 2011

[21] J. D. Howard, T. A. Longstaff, "A Common Language for Computer Security Incidents", Albuquerque, New Mexico, U.S.A.: Sandia National Reports, 1998

[22] T. R. Gruber, "Toward Principles for the Design of Ontologies Used for Knowledge Sharing", International Journal Human-Computer Studies 43, p. 907-928, 1993

[23] Object Management Group (OMG), "Unified Modeling Language Superstructure", V. 2.2, http://www.omg.org, 2009

[24] T. Dillon, E. Chang, M. Hadzic, P. Wogthongtham, "Differentiating Conceptual Modelling from Data Modelling, Knowledge Modelling and Ontology Modelling and a Notation for Ontology Modelling", Australian Computer Society, 5th Asia-Pacific Conference on Conceptual Modelling, Vol.79., Wolongong, Australia, 2008

[25] S. Fenz, A. Ekelhart, "Formalizing Information Security Knowledge", ASIACCS'09, Sidney, NSW, Australia, p. 183-194, ACM, 2009

[26] S. Fenz, G. Goluch, A. Ekelhart, B. Riedl, E. Weippl, "Information Security Fortification by Ontological Mapping of the ISO/IEC 27001 Standard", Dependable Computing, 13th Pacific Rim International Symposium, 2007

[27] Department of Trade and Industry (DTI), "Information Security: Protecting Your Business Assets", November 2004, http://ww.dti.gov.uk

[28] NIST, Special Publication 800-53 Revision 4, Initial Public Draft, Security and Privacy Controls for Federal Information Systems and Organizations, US Deaprtment of Commerce, February 2012