Object-Oriented Situational Approach to Enterprise Information Security Management

I. Zemtsov[1(✉)] and L. Astakhova[2]

[1] Reshetnev Siberian State University of Science and Technology, 31 Krasnoiarskii Rabochii Avenue, Krasnoyarsk 660037, Russian Federation
9798866@gmail.com

[2] South Ural State University, 76 Lenina Avenue, Chelyabinsk 454080, Russian Federation

Abstract. The article substantiates a method for reducing the cost of an information security management system, developed using a semiotic approach to classifying information security objects, as well as a situational approach to choosing information security methods depending on the object of protection. The method is based on the following criteria for the situational choice of information protection measures: a clear differentiation of the information level, the object of protected information corresponding to this level, and the purpose of its protection. It is shown that each of the information levels (signs, logical structures, meanings, and messages) as an object of protection (material objects, information processes, information, presentation forms), depending on the purpose (confidentiality, integrity, availability, continuity), requires specific protection measures. The choice of these measures depending on the object-target situation of information protection in the organization will ensure the necessary and sufficient level of information security and avoid redundancy of measures and unjustified costs. According to the key principle of information security, economic feasibility, the use of this method (determining not only the need but also the sufficiency of measures) will significantly reduce the cost of information security systems. Based on the developed method, a prototype of a software application was justified, the novelty of which is due to its functionality to automatically determine the composition of information security measures depending on the object and purpose of protection using standards for information security management in the organization.

Keywords: Information · Information security · Management · Situational approach · Semiotics · Information levels · Objects · Goals · Measures · Effectiveness

1 Introduction

Information security (IS) management consists of implementing a list of organizational and technical measures identical to most security objects [1, 2]. For each object of protection, a private set of measures is formed based on the features of the functioning of

A. A. Radionov and V. R. Gasiyarov (Eds.): RusAutoConf 2020, LNEE 729, pp. 591–600, 2021.
https://doi.org/10.1007/978-3-030-71119-1_58

specific information and automated systems, as well as the presence of specific information technologies in these systems. The set of protective measures are the same both for the protection of a single database and for the comprehensive protection of the organization's information infrastructure as a whole. The features of security objects are not taken into account, and the cost of protecting information is unreasonably increased, which contradicts the principle of economic expediency. This explains the relevance of this article, which is aimed at finding a method for selecting information security measures that would take into account the specifics of protected objects. The purpose of our research is to substantiate the object-oriented situational approach to information security management. The objects of information security based on the semiotic approach; we formulate a mechanism for determining the boundaries of the application of security measures; we show the capabilities of a software application to perform the function of selecting security measures based on the proposed approach.

2 Literature Review

Analysis of statistics in the field of information security shows that the effectiveness of modern methods of information protection is not high enough. Over the past ten years, global spending on information security has been growing, but so has the number of incidents [3]. To increase the effectiveness of is, it needs a paradigm shift [4]. There is a need to switch from the number of protective measures to their quality [5].

Standards in the field of information security contain a set of measures abstracted from specific organizations [6]. This is a typical universal set of measures for ensuring information security. The use of multiple measures requires a significant investment of resources. Most of these measures are ineffective because they are typical. Researchers identify factors of effectiveness of an IS management system that are not taken into account by the standards [7]. A review of the literature on IS risk management undertaken by foreign experts has revealed shortcomings in IS management practices that inevitably lead to incorrect decision-making and inadequate security strategies [8]. Therefore, more and more often, a more flexible, adaptive strategy, the strategy of situational management, is being put into the basis of the organization of the information security management process. The development of information security management tools based on a situational approach is very relevant, which is confirmed by Russian and foreign experts [9–15]. Thus, the authors of this article have proposed and experimentally tested a situational approach to IS management [2]. With this approach, each IS system is built individually for each situation.

Some aspects of decision-making based on situational management of dynamic objects have been studied and described in publications. For example, experts concluded that a three-level process and service model of an IS management system is most appropriate for network protection. This model includes processes at the strategic, tactical and operational levels: "risk management, ensuring the integrity of network resources, adjusting the top-level information security policy"; "development and configuration of security procedures, development of the IS system architecture, classification and analysis of the state of IT resources, monitoring and incident management"; "access rights differentiation, network security management, verification of compliance of the is system

with established standards" [2]. Foreign researchers are actively researching situational awareness about cybersecurity. Thus, a cybersecurity situational awareness system has been developed, consisting of seven levels: data assessment, object assessment, situation assessment, impact assessment, process refinement/resource management, user refinement/knowledge management, and mission management [16]. The situational approach to is management has become an object of study in the pedagogical context – in the process of training future specialists in this industry. We paid special attention to the problem of the influence of situational factors on the scope and boundaries of the is management system [17]. We have not found any publications dedicated to information security objects as situational factors of is management.

3 Information Security Protection Objects

Information carriers as protection objects include physical persons or material objects, including physical fields in which information is reflected in the form of symbols, images, signals, technical solutions and processes, and quantitative characteristics of physical quantities. In fact, an information carrier is a material object that is the carrier of the information presentation form. The relationship between information and the representation form is semantic, and the relationship between the representation form and the material object is physical. This provides indirect protection of confidentiality, integrity, and availability of information through the protection of material objects and presentation forms. However, methods for protecting the properties of information, representation forms, and material objects are different due to their different nature. The privacy, integrity, and availability properties of these objects are also not identical. Thus, a violation of the integrity (physical damage to the surface of the transparent layer) of a CD as a material object leads to a violation of the availability of the form of representation of information reflected on it in the physical sense. However, the availability of information in the semantic sense is not affected. On the contrary, compromising (violating the confidentiality) of a material object-the carrier of an electronic signature key-when left unattended may not actually lead to a violation of the confidentiality of the presentation form or information, but, according to established rules, will lead to a violation of the continuity of the information process due to the forced revocation of the certificate. Such arguments give grounds to assert that each of the properties of information, forms of representation, material objects and information processes can be considered as a separate object of protection and, based on the purposes of protection, to allocate one of them.

Review two statements of information security standard [1]:

- Information security – preservation of confidentiality, integrity, and availability of information
- Attack – attempt to destroy, expose, alter, disable, steal, or gain unauthorized access to or make unauthorized use of an asset (information, software, physical, services, etc.)

What information security system needs to protect: information only or all assets? There is no logical proof of reference between information security and asset protection. Understanding, what is information, is the reason.

In this paper, we use the last science researches about information theory. The information has 5 levels: empiric, syntactic, semantic, pragmatic, and social [12]. The empiric level essentially equates information with the signs that are generally said to carry or contain information. We mean as signs signals, gestures, traces, etc. The syntactic level deals with signs and the rules governing them. At this level, information is introduced as logical structures and codes (texts) [13]. The semantic level is concerned with meaning. There are two approaches at this level to understand information, namely objective and subjective. The main idea of the former is that all sorts of signals, primarily physical ones, carry information. Information, in this view, is objective in that it is carried and transmitted whether it is received or understood by anyone or not [12]. The latter theory holds that signs are interpreted differently by different people according to their intentions, beliefs, values, and expectations (meaning). Information, in this view, is the result of interpretation (analyzing what the signs mean) by an individual person. Information on the pragmatic level is the knowledge about the intentions of the message sender, and the effects that the message and its information may have on the receiver(s) [13]. On the social level, similarly to the pragmatic level, information is defined as a message. The difference between this and the pragmatic level is that the message, in this view, has a value for the society, not for the person. The term "message" is not synonymous with "meaning" [14]. For the purposes of our research, we do not need to consider the social level as a separate one. Consider a simple greeting such as "Good day today!". The direct meaning of that sentence is the kind of day. However, the message of that sentence is a proposal to make contact. On the other hand, it could be ironic, if uttered on a rainy and miserable day. As this example shows, a message can have more than one meaning, and several messages can have the same meaning [14].

Thus, we can select four types of information forms to protect: signs, logical structures, meanings, and messages. To achieve the purpose of our research, we create a communication model, which includes a semiotics approach to information and communication. This model introduces the communication process as four steps: access, semiosis, representation, and interpretation [14].

To achieve information security as the preservation of confidentiality, integrity, and availability of information, it is necessary to protect the information properties in all forms of its representation: signs as physical objects, logical structures as representation forms, meanings as the result of direct interpretation, and message as information itself. What form of information does the standard mean [1]? We consider that the answer to this question is different in each situation.

Correctly defining the level of the information in the process of its protection helps to limit the scope and boundaries of applicability of information security measures and the number of employees responsible for information security [15]. This is our hypothesis.

3.1 Protected Information Properties

According to the standard definition [1], the properties of confidentiality, integrity, and availability of information are protection objects. Methods of protecting the properties

of the various information forms are different, due to the different nature of these forms. The privacy, integrity, and availability properties of these objects are not identical.

For example, consider a case where an integrity violation of signs and logical structures does not lead to an integrity violation of meanings and messages. Such cases may be the result of a change of an electronic document format from DOCX to PDF or of a paper document getting wet. In both cases, there is a violation of the physical carrier structure of the sign, but in such cases, it is still possible to read the information.

Thus, it is possible to distinguish 12 information security protection objects: confidentiality (c), availability (a) and integrity (i) of signs, of logical structures, of meanings, and of messages.

3.2 Protection Object as a Situational Factor

Consider the distinctive features of the confidentiality, integrity, and availability properties to determine the scope and boundaries of information security measures of the objects in question.

The main criterion of availability as an information security property is the ability to use information [1]. Thus, the ability to use the sign is the physical access to the sign (empirical access), and the ability to use a logical structure is the ability to read the signs (syntactic access). The ability to use meanings is the correct mapping of signs with designated objects (semantic access). The ability to use the message is to correctly perform the process of interpretation according to the context (pragmatic access). A correct interpretation requires preserving not only the integrity and availability of representation forms, but also the context (including situations of use of the mark), and whether the subject has knowledge about this context [14].

The main criterion of confidentiality property is the unavailability of information to unauthorized entities [1]. The four levels of access (empirical, syntactic, semantic, and pragmatic) use the appropriate access means. The access means management allows to restrict access, i.e. to ensure object confidentiality.

The main criterion for the integrity property is the preservation of the accuracy and completeness of the object [1]. Preservation of integrity is achieved by excluding unauthorized modification of the object (access restriction), control of integrity, and restoration of the object.

Thus, to protect availability the scope and boundaries of information security measures are the appliances and methods of access.

To protect confidentiality, the scope and boundaries of the information security measures are the access control system.

To protect integrity, the scope and boundaries of the information security measures are the appliances of restoration, integrity control, and restriction of access.

3.3 Signs as Protection Object

In its simplest form, information is a sign. A sign is just a thing. The standard [1] defines the following computer security objects: media, networks, information, systems and applications, source code of programs, secure areas, and equipment. A thing containing

computer information is called media. The protection of things and media extends to their storage locations: networks, secure areas, and equipment. Security measures for such objects are quite common and understandable, and in fact constitute physical protection. The means of ensuring security at this level are access control and management systems, as well as enclosing structures of the territory, buildings, or premises.

Measures to protect the availability of signs extend to physical access means. In the case of the material form of the signs, such means include storage places of signs, such as office rooms, boxes, and transportation means. In the case of electronic and optical signs in computer systems, such means include hardware and software means for processing information, such as computers, communication equipment, and networks.

Measures to protect the confidentiality of signs extend to managing access to such media (including physical fields in information systems). These tools include physical and hardware-based access control systems.

Measures to protect the integrity of the signs extend to the sign access control systems, the means of controlling the integrity and restoring the signs. The means of controlling integrity include labels, which signal integrity violation. The means of restoring the signs include tools to create a physical copy of the sign and restore it.

3.4 Logical Structures as Protection Object

Logical structures are objects that allow one to get information from the logical relationship between signs. This relationship is established by the syntactic rules of the language. For a person to "read" the logical structure, they need to know about syntax or have "reading tools", which allow them to present the syntactic connection in a way that is understandable to a person. Logical structures from the set defined by the standard [1] include systems, applications, and program source codes. Security measures for such objects are software systems that restrict access, such as identification, authentication, and authorization systems.

3.5 Meanings as Protection Object

There is a semantic relationship between signs, logical structures, and their meanings. This level is completely ignored by today's information security standards. However, in our opinion, data protection at the means level is quite effective and self-sufficient. The objects of protection at this level are dictionaries and their relationship to dictionaries. Security measures may include using an unknown language or hiding metadata.

Measures to protect the availability of meanings extend to logical means of matching signs and designated objects, as well as to directories containing matching rules (dictionaries). Such means are software algorithms.

Measures to protect the confidentiality of meanings extend to access control systems for the comparison of signs and designated objects and dictionaries.

Measures to protect the integrity of meanings extend to the integrity control systems of programs and dictionaries.

3.6 Messages as Protection Object

Meaning becomes message when it is placed in context. The level of messages is also not considered in today's information security standards. In our opinion, true information protection should first consider this level, since the purpose of information protection is to protect the message. If the attacker does not understand the message of the stolen data, then there is no actual theft of information. The object of protection at this level is the context.

Measures to protect the availability of messages extend to the means of interpretation. These tools include intelligence and meanings generated using symbols in relation to the context.

Measures to protect the confidentiality of messages extend to the means to control the possibility of interpretation (control of relation with the context, the availability of the context).

Message integrity protection measures extend to context integrity control systems.

3.7 Improving the Effectiveness of Information Security

When using the object of protection as a situational factor in information security management, improving the efficiency of information security is achieved by reducing the cost of implementing measures. Let us compare the limits of applicability of information security measures in the current approach [1] to information security management and the use of the situational approach.

In order to protect the confidentiality of current information security management system, it is necessary to implement measures to restrict access to all protection objects: media (A. 8.3.3), networks (A. 9.1.2), information (A. 9.4.1), systems and applications (A. 9.4.2), source code of programs (A. 9.4.5), secure areas (A. 11.1.2), and equipment (A. 11.2.1) [1]. Thus, all these measures should be applied to all information levels (Table 1).

Protection of confidentiality in the situational approach to information security management can be reduced to limiting access to information at the required level according to the purposes of protection. For example, for the level of "message", the method of protection is the anonymization of the data. Other methods do not have to be used, since a sufficient level of confidentiality is ensured by complete anonymization of the data (Table 2).

Proper understanding of the purpose of protection in this approach will help to build an effective information security system by focusing on the target information level.

With an object-oriented situational approach, privacy protection can be reduced to restricting access to information at the required level per the protection goals. So, for the "information" level, the method of protection is "data anonymization", which consists of restricting access to dictionaries and reference books that determine the semantic relationship between representation forms and semantic meaning. However, other methods may not be used, since data anonymization provides the necessary and sufficient level of confidentiality.

Table 1. Comparison of the security boundaries.

Property	Scope and boundaries of information security measures			
	Signs	Logical structures	Meanings	Messages
Availability	Physical access means to signs (media)	Reading means (sensors)	Logical means, dictionaries	Intelligence and context meanings
Confidentiality	Physical and hardware-based access control systems to signs (media)	Software access control systems to information (files) or encryption information or physical access control to reading tools	Access control systems to programs or dictionaries	Access control to relation with context or context
Integrity	Integrity control tools to media, copy tools of signs (media)	Integrity control means, checksum, and backup software	Integrity control systems of programs and dictionaries	Context integrity control systems

Table 2. Confidentiality security boundaries.

Property	Score and boundaries of information security measures			
	Signs	Logical structures	Meanings	Messages
Confidentiality	Media, networks, secure areas, equipment	Systems, applications, source code of programs, information (files), reading tools	Dictionaries, relation with dictionaries (not included in the standards)	Context and relation with the context (not included in the standards)

A comparative analysis of measures to protect the confidentiality of objects in the standard and object-target situational approaches showed a reduction of measures to the necessary and sufficient number, which indicates the advantage of the latter. Based on the research results, we have developed a prototype of a special software application for determining information security measures depending on its level and goals of protection in the organization. Its implementation, along with the application of information security management standards, will contribute to improving the effectiveness of information security systems at the enterprise.

4 Conclusion

The paper presents a justification for the feasibility of an object-oriented situational approach to the selection of necessary and sufficient information security measures to reduce the organization's costs. The scientific novelty consists in the application of two methodological approaches: semiotic (to the classification of information security objects, which allowed identifying different types of specific objects) and situational (to the construction of an information security system, which makes it possible to choose specific adequate protection measures for each type of object). The practical significance of the work lies in the development of a prototype software application for automating the described process of managing the enterprise's information security, which will help reduce the cost of information security and management processes. The research prospects are related to the justification of relevant changes and additions to the standards for information security management.

References

1. ISO/IEC 27002. Information technology – Security techniques – Code of practice for information security controls. International standard (2013)
2. Astakhova, L., Zemtsov, I.: Situational approach to information security. In: Ural Symposium on Biomedical Engineering. Radioelectronics and Information Technology, pp. 136–139 (2018)
3. Infowatch analytics center. Data breach eeport: a study on global data leaks in H1 2018. Infowatch (2019). https://infowatch.com/sites/default/files/report/analytics/Global_Data_Breaches_2018.pdf. Accessed 15 Jan 2020
4. Jan, H.P., Eloff, M.: Information security management: a new paradigm. In: Proceedings of the 2003 Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists on Enablement Through Technology, pp. 130–136 (2003)
5. Baker, W., Wallace, L.: Is information security under control? Investigating quality in information security management. IEEE Security Privacy Mag. **5**(1), 36–44 (2007)
6. Siponen, M., Willison, R.: Information security management standards: problems and solutions. Inf. Manag. **46**(5), 267–270 (2009)
7. Chang, S.E., Ho, C.B.: Organizational factors to the effectiveness of implementing information security management. Ind. Manag. Data Syst. **106**(3), 345–361 (2006)
8. Webb, J., Ahmad, A.: A situation awareness model for information security risk management. Comput. Secur. **44**, 1–5 (2014)
9. Yao, J., Fan, X., Cao, N.: Survey of network security aituational awareness. Cyberspace safety and security. In: Lecture Notes in Computer Science, vol. 11982, pp. 34–44 (2019)
10. ISO/IEC 27000. Information technology – Security techniques – Information security management systems – Overview and vocabulary. International standard (2009)
11. Mingers, J., Standing, C.: What is Information? Toward a theory of information as objective and veridical. J. Inf. Technol. **33**(2), 85–104 (2018)
12. Stamper, R.K.: A semiotic theory of information and information systems. In: Proceedings of the Joint ICL, pp. 1–33 (1993)
13. Danesi, M.: Messages, Signs, and Meanings: A Basic Textbook in Semiotics and Communication Theory. Canadian Scholars Press, Toronto (2003)

14. Pyatkov, A., Zolotarev, V.: About responsibilities distribution for information security. In: Proceedings of the 6th International Conference on Security of Information and Networks, vol. 13, pp. 380–383 (2013)
15. ISO/IEC 27001. Information technology – Security techniques – Information security management systems – Requirements. International standard (2013)