ISSN 0147-6882, Scientific and Technical Information Processing, 2016, Vol. 43, No. 1, pp. 20–27. © Allerton Press, Inc., 2016.
Original Russian Text © Z.V. Rodionova, L.K. Bobrov, 2016, published in Nauchno-Technicheskaya Informatsiya, Seriya 1, 2016, No. 1, pp. 21–29.

Protection of the Information Resources of a Library Based on Analysis of Business Processes

Z. V. Rodionova and L. K. Bobrov

Department of Economic Informatics, Novosibirsk State University of Economics and Management, Novosibirsk, Russia
e-mail: z.v.rodionova@nsuem.ru, l.k.bobrov@nsuem.ru

Received September 1, 2015

Abstract—This paper justifies the relevance of the reliable protection of information and the development of measures to reduce information risks in libraries with comprehensive information resources. A brief description of the objects of protection and the main threats, including those that are related to the processing of personal data, is provided. It is alleged that analysis of models of the business processes of a library makes it possible to track the impacts of changes on many aspects of information security. The position of the information system for security analysis of the business process in the overall system of information security is determined. Steps for the formalization and updating of the rights of access to information resources of a library are illustrated. It is emphasized that the basic document for information-security risk management is a threat model that reflects the data on sources of threats and vulnerabilities of the system, impacted objects, and a number of other parameters. A block diagram that illustrates the process of analyzing the threats and vulnerabilities and a knowledge meta-model for the management of information-security risks are provided. It is concluded that based on the relationship of business processes that are reflected in a formal notation it is possible to automatically obtain the data on the degree of influence of security aspects of information objects of a particular sub-process on the results of business processes of a higher level, and as a result, on the achievability of the purposes of an organization.

Keywords: library technologies, business processes, information resources, information threats, information security, threat model, personal data

DOI: 10.3103/S0147688216010032

INTRODUCTION

Information has always played an important role in the life of mankind, while libraries have served as a reliable guide to the world of information. With the advent of the Internet, as shown by the results of J.P. Morgan on the monitoring of information resources [1], libraries took a deserved place in this network (Fig. 1).

The main directions of the state policy in the sphere of culture and mass communications in the Russian Federation up to 2015 include a set of measures to support libraries by creating community-based centers of computer literacy, public reference and educational portals, digital libraries, development of public access to the Internet, introduction of technologies for distance education and a remote information environment [2–4].

The complex of information resources that are available today in libraries is of a hybrid nature because in addition to traditional print editions and microforms, libraries provide a wide range of electronic information resources, including electronic catalogs and archives, as well as open and licensing resources for online access. However, as can be seen based on the example of the Russian National Public Library, in recent years there has been a positive trend to the use of information resources (Fig. 2).

However, due to the fact that information has become publicly accessible, the modern society has become dependent on information resources and technologies, as well as their quality and security. This is occurring against the backdrop of steady growth in the number and types of IT threats, which is supported by many, although somewhat controversial, estimates concerning, for example, malicious software:

- computer viruses are propagating exponentially; in the period from 2010 to 2014 the number of new types of malware increased by almost 40 times and exceeded 10 thousand titles [5];
- in 1994, a new virus appeared once per hour in the world, 2 years later this was once per minute, and by 2011 it was once per second [6];
- in 2014, the Kaspersky Lab detected more than 123 million unique malware objects, identified 1.4 billion web-based attacks, and according to Eugene Kaspersky, more than 325000 of these objects appear in the world every day [7];
- within the period from November 2013 to October 2014, the solutions of the Kaspersky Lab defeated

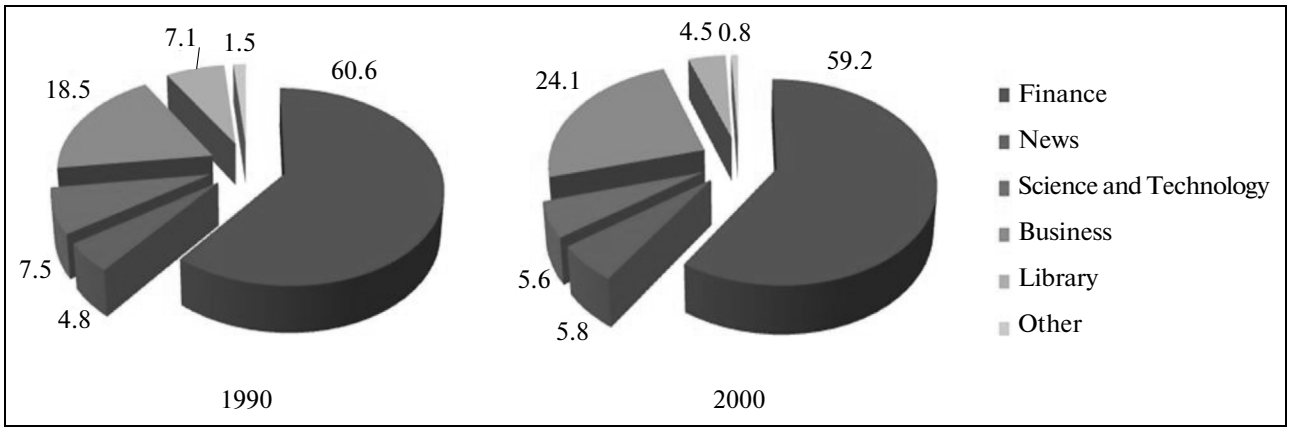


Fig. 1. The share of libraries in a variety of information resources of the Internet.

1432660467 attacks from online resources that were located in various countries around the world [8].

Based on these patterns, it seems quite reasonable that the theses on the future of the digital world [9] include the thought that cyber-terrorism and related offenses and offenders will also develop and present a serious threat to information services, systems, and resources. Therefore, the problems of the protection of information and development of measures to reduce information risks are very important for libraries, whose work is increasingly digitalized [10].

THE PROTECTION OBJECTS AND MAIN THREATS

Libraries are faced with challenges such as the security of data storage and transmission systems, control of their integrity and reliability, access rights to information resources, and protection against distortion, loss, and unlawful copying. Creating the conditions for the security of information resources of a library is aimed at preservation of the national and world cultural heritage, where protection concerns, as a rule, such systems, services, and resources as:

- automated library-information systems, which provide comprehensive automation of library processes (acquisition, cataloging and ordering of literature, creation and maintenance of an electronic catalog and electronic databases, accounting of readers, library funds, etc.);
- library portals;
- library blogs on the Internet and groups (communities) in social networks;
- cloud libraries that provide services via the Internet through cloud computing and cloud services;
- data centers (specialized centers with powerful software and hardware and telecommunication facilities);
- electronic libraries (information system for creating and storing documents in electronic form with the possibility of access to them through computer technology, including information networks, such as NEB, IS EKBSON, and WDL);
- information and telecommunications infrastructure;
- other information systems, services and resources of libraries.

All these objects, services, and resources must be protected under condition of their accessibility (the ability to obtain the required information service within a reasonable time), integrity (the relevance and consistency of information, its protection from destruction and unauthorized changes), and privacy (protection against unauthorized examination).

Increased attention to the problems of information protection in libraries is also associated with the need to protect personal data. As an operator of personal data, the library processes information about its users (readers) and employees. The information systems of personal data (hereinafter ISPDs) of a library include automated library systems (which process cards of users (readers)), information systems of human resources and accounting (information about employees), and electronic document management systems (information about employees and partners).

In accordance with the Government Resolution On Approval of Requirements for the Protection of Personal Data during their Processing in Information Systems of Personal Data from November 1, 2012 no. 1119, it is possible to determine the approximate level of protection of the ISPD of a typical library. The following properties were taken as the initial values:

- actual threats, which are connected to the presence of undocumented (undeclared) capabilities in the application software, as none of automated library information systems (ALIS) on the software market today have a certificate of the Federal Service for Technical and Export Control (FSTEC of Russia) on the absence of undeclared capabilities;
- the category of personal information–biometric personal data, the use of video surveillance, pictures on the card of a user (reader);

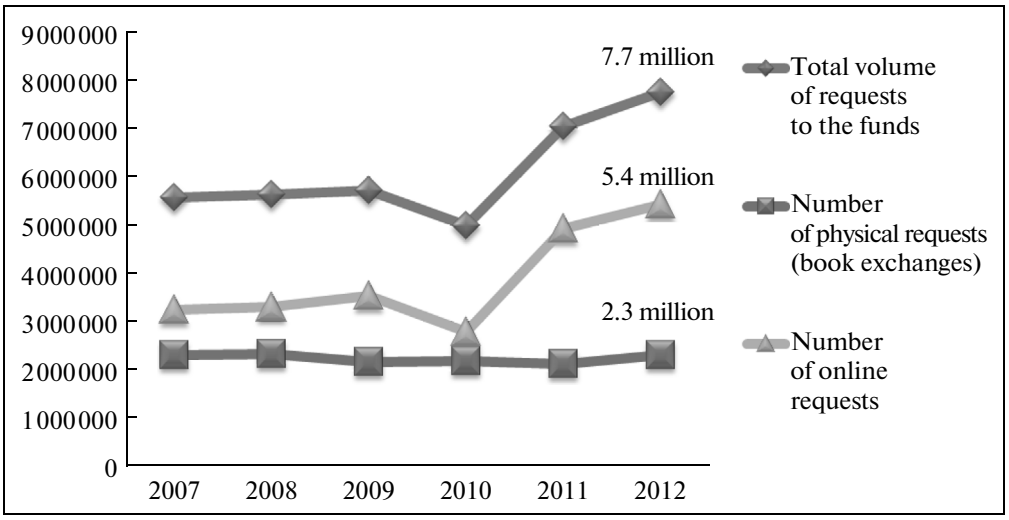


Fig. 2. The dynamics of using the information resources of the Russian National Public Library. http://www.aselibrary.ru/data-docs/Li%20bkom2013/1_Lindeman_Libcom%202013.pps

• the number of subjects of personal data, more than 100000/less than 100000; in connection with the processing of biometric personal data the parameter "number of subjects of personal data" does not affect the determination of the level of protection and can be either more than 100000 or less;

• the personal data of employees are processed.

A large library, in accordance with the above-mentioned Resolution of the Government of the Russian Federation and in accordance with the values of the specified parameters, can be assigned with the second level of ISPD. The requirements for this level of security are as follows:

• the organization of security of the premises that house the information system; this prevents the possibility of uncontrolled penetration or a stay in these premises of persons who are not entitled to access these facilities;

• ensuring the safety of carriers of personal data;

• approval by the head of the organization–operator of a document that defines the list of persons who require access to the personal data that is processed in the information system to implement their official (employment) duties;

• use of information-protection means that have undergone assessment for conformity to the requirements of the legislation of the Russian Federation in the field of information security in the case where the use of such means is necessary to neutralize actual threats;

• the appointment of an official (employee) who is responsible for ensuring the security of personal data in the information system;

• access to the content of the electronic message log must be available exclusively for officials (employees) of the organization–operator or an authorized person who requires the information that is contained in this log to implement their official (employment) duties.

Information-security management is a part of the overall management system based on risk analysis and is intended for the design, implementation, monitoring, maintenance and improvement of measures in the field of information security. The information-security management of a library is aimed at neutralizing threats of various kinds [11]:

• threats to an individual by distributors of methods and data that are harmful to the personality of a citizen (pornography, drugs, cursing, 25th frames, racist remarks, gambling, etc.), manipulation of information (disinformation, concealment, or distortion);

• information threats (violation of the technological processing of information, delayed processing and analysis of incoming data, errors in the processing of information, or improper filling of fields when entering information to the ALIS);

• threats to the system as a whole (natural disasters, fires, industrial accidents, acts of terrorism, theft, eavesdropping, computer crimes, etc.).

Analysis of the threats to the security of information resources in the context of the security triad makes it possible to distinguish the following types:

• when ensuring the confidentiality of information: theft (copying) of information and means of its processing and loss (unintentional loss, leakage) of information;

• when ensuring the integrity of information: modification (distortion), the denial of authenticity, and the imposition of false information;

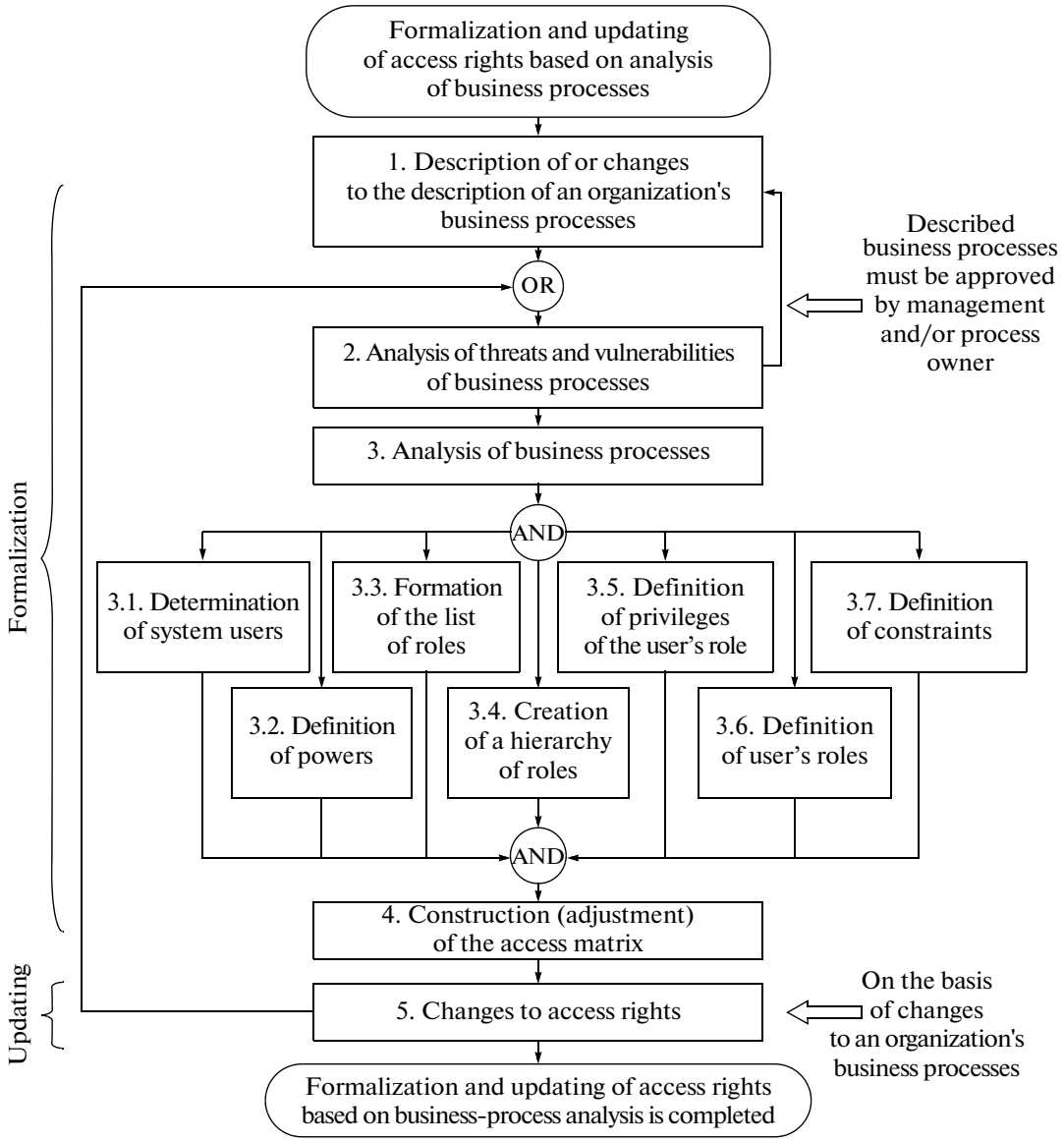


Fig. 3. The stages of the formalization and updating of access rights to information resources [14].

• when ensuring the availability of information: blocking and destruction of information and means of its processing.

An effective information-security management system of a library adapts and modifies the requirements for the protection of resources that depend on the changes in business processes, which in turn are influenced by the external and internal environments. External changes include changes that result from legislation or organization-administrative documents of the parent bodies (ministries, departments, and state regulators). Internal changes may be due to the optimization of business processes, the use of information resources that are shared with other libraries, changes in information processing technology, ALIS, and other factors. This may include all information-security system elements, from information resources, conceptual documents, instructions, and regulations to the configuration of software–technical solutions.

The functioning of the information-security management system of a library should be based on the process of effective risk management. The process of analysis of threats and information-security risks is continuous; the initial data are defined at the stage of creating the information-security system. Then, in the course of its operation the changes in threats and risks are monitored, re-analyzed, and estimated. Typically, the data for this type of work are obtained from the results of interviews and questionnaires of the library

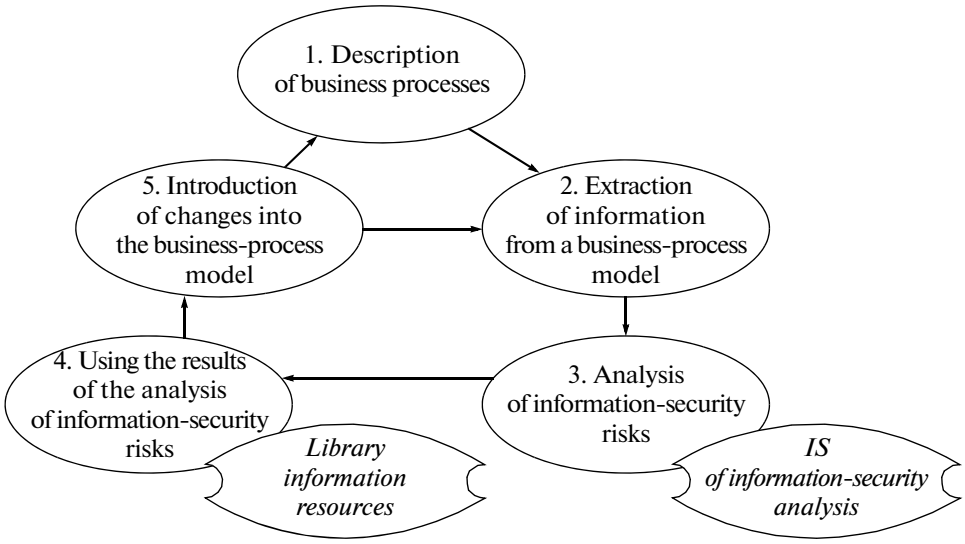


Fig. 4. The position of the information system for security analysis of the business process in the overall system of information security.

staff and external experts at the initial investigation step and subsequent audit.

ANALYSIS OF BUSINESS PROCESSES IN INFORMATION-SECURITY RISK MANAGEMENT

Analysis of models of business processes makes it possible to track the impacts of changes on many aspects of information security. In particular, in [12, 13] the authors proposed an automated approach to the management of access rights (formalization and updating) of users on the basis of analysis of models of business processes in the EPC notation. The content of the stages of formalization and updating of access rights based on the analysis of business processes is illustrated in Fig. 3.

Organization of the risk-assessment process based on the model of the business process requires [14]:

• rules for constructing a model of business processes; these rules ensure the availability and unambiguous interpretation of the data that are contained in this model to identify threats and vulnerabilities and assess the significance of the information resource both in terms of the consequences for the outcome of the process and in terms of the impact of the modified result of the process on the goals of the activities;

• algorithms for extracting the data that are used in the model of the risk analysis from the business processes;

• algorithms for responding to changes that reflect the changes in the parameters of the business process model to the values of the risk-assessment model parameters.

It is advisable to carry out the practical implementation of this approach through the creation of an information system for the analysis of the information security of the process; the position of this system is illustrated in Fig. 4.

As can be seen from Fig. 4, the information system for the analysis of the information security receives data from business-process models for subsequent analysis of information-security risks using various methods. Note that the results of implementing such a system can be used to carry out measures to protect information in both automated information systems and non-automated data processing.

The basic document for information-security risk management is a description of threats (as a result of analysis of the threat model), which contains the data on the sources of these threats, vulnerabilities of the system, affected objects, and a number of other parameters. This document requires constantly updating. Currently, there are a large number of methodologies for the development of such documents: CRAMM, the two-factor method NIST, GRIF, and RiskWatch, which is a method for determining the actual threats to the security of personal data during their processing in information systems of personal data, and other types.

Building a threat model requires knowledge on the following objects:

• information assets;
• the unit an information asset is assigned to;
• the media;
• the information system;
• the user;
• the characteristics of the user's access to information;
• data-transfer channels;
• resources on which information is stored;

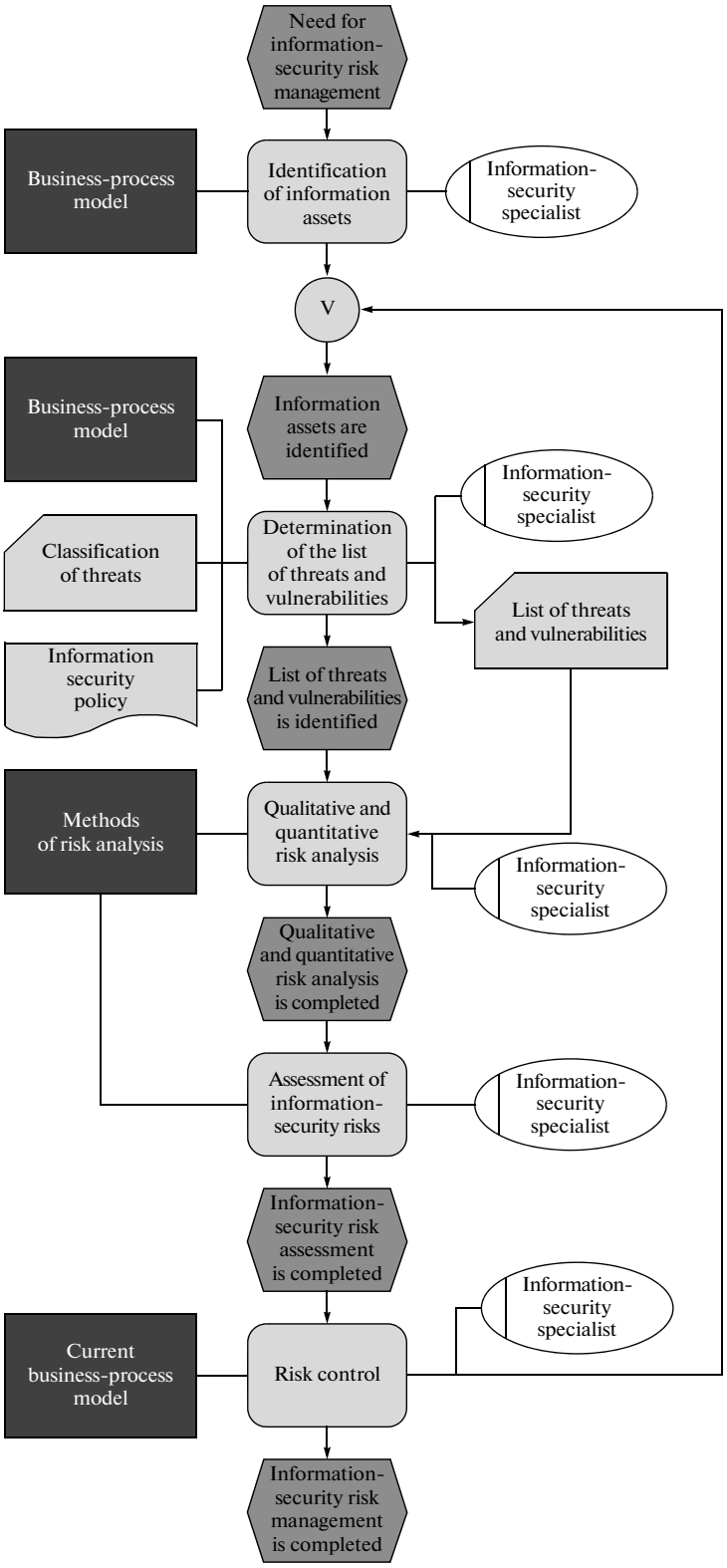


Fig. 5. The process of managing information-security risks.

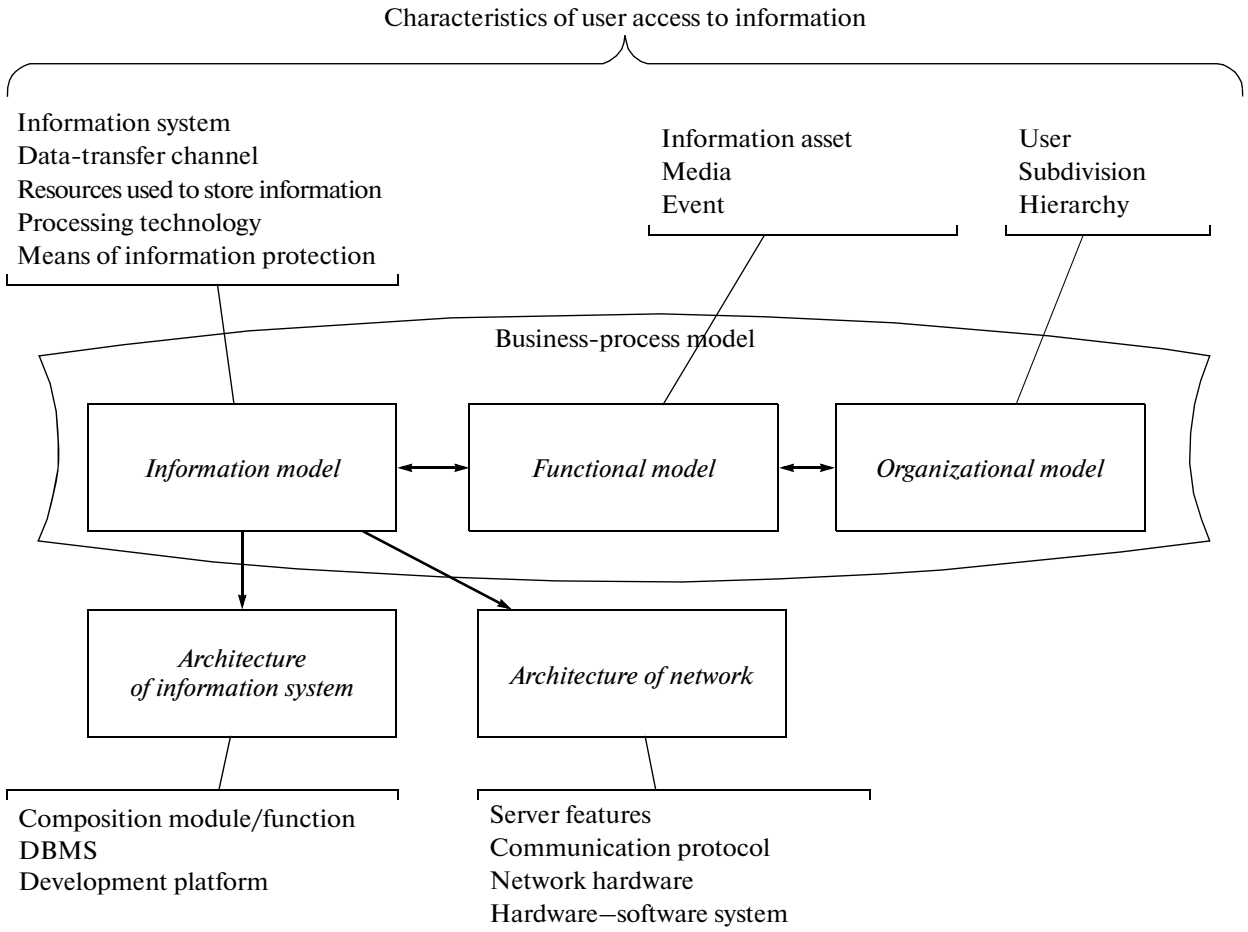


Fig. 6. Knowledge metamodel for managing information-security risks.

- processing technology;
- means of information protection.

This list is not exhaustive and can be extended for a specific method of constructing a model of threats and vulnerabilities.

As an example, Fig. 5 shows a block diagram that illustrates the process of information-security risk management.

A knowledge meta-model, which covers the functional, organizational, and information models and makes it possible to identify and update the information-security risks of the library, is shown in Fig. 6.

The organizational model defines the list of performers of the business process and reflects the duties and responsibilities. A change in this model due to the dismissal, transfer to another position, a new employee, organizational restructuring, etc. through a change-management process will have an impact on processes such as the distribution of duties and responsibilities, data-access control, and the management of risks, incidents, and vulnerabilities [14].

The functional model will increase the awareness of employees on information security, ensure the continuity of the business process, and update the access control model.

The information model reflects the information systems of a library, their modules, and functions, as well as users, and serves as a source of data for the management and monitoring of the information infrastructure and the management of access rights.

Some authors (for example, [15]) have noted the need to review business processes as the main assets of an organization that cover hardware and software means, information resources, staff, and so on, while the solution of information-security problems is not directly linked with the models of business processes. The information about the main business processes from the owners and participants of these processes that is required to identify critical information assets and the technological aspects of their processing, which is later used to draw conclusions about threats and vulnerabilities, is often obtained by means of questionnaires. Thus, as a rule, further evaluation does not involve business processes.

At the same time, analysis of the business-process model makes it possible to extract such data to deter-

mine the boundaries and features of the information system as the content and media of the processed information, the users, the means of data transmission inside and outside this system, and the technology that is used. It is important that these data can serve as a basis for identifying protected assets in connection with the objects of the business process, where:

• each vulnerability can be assigned to an object that defines what method of processing, transmission and/or storage this vulnerability is inherent to;

• each threat is associated with the aspects of information security whose violation the threat can result in (confidentiality, availability, and/or integrity);

• the source of each threat is determined (it may be the executor of the business process or a person who does not participate in the business process, events of a force majeure nature, and other types.)

The business process that is described by the corresponding model can also be regarded as an independent object of protection with certain properties (for example, timeliness of results (output of the process), correspondence of the result to the established requirements, and compliance of the resources that are used within the process to those planned, etc.) whose violation leads to certain negative consequences.

CONCLUSIONS

The construction and maintenance of an effective system of information-security risk management is a complex and continuous process that affects the viability of a library. The complete model of an organization's business processes, as reflected in the formal notation, is a hierarchy of models of various processes and sub-processes that reflects the relationship of processes of different levels of detail. When specifying the causal relationships between the security aspects of information objects on the one hand and the factors and consequences of risks to the relevant sub-processes on the other hand it is possible, based on the relationships of business processes that are reflected in formal notation, to automatically obtain the data on the degree of influence of the security aspects of information objects of a sub-process on the results of processes of a higher level and finally on the prospects of achieving the objectives of the organization.

REFERENCES

1. Chernykh, O., Information services and the organization of the market using Internet technologies. http://citforum.ru/abtec/s2/3.shtm. Cited June 22, 2015.

2. Kulikov, L.V., *Prakticheskoe rukovodstvo po razvitiyu obshchedostupnykh munitsipal'nykh bibliotek: normativnyi podkhod* (Practical Guide to the Development of Public Municipal Libraries: Regulatory Approach), St. Petersburg: RBV, RNB, 2010.

3. Medyankina, I.P., Distance learning technologies: Study of Information Needs of Students, *Vestn. NGUEU,* 2012, no. 1, pp. 236–246.

4. Medyankina, I.P. and Bobrov, L.K., University library in distance education: The use of elements of the Logical Framework Analysis, *Nauchn. Tekh. Bibl.,* 2009, no. 12, pp. 5–11.

5. World history of infections. http://lenta.ru/articles/2014/11/18/virus/. Cited June 12, 2015.

6. Internet: figures and facts (3). http://www.bizhit.ru/index/digital_internet_3/0-563. Cited June 12, 2015.

7. Evgeny Kaspersky on trends in information security. http://www.it-weekly.ru/market/security/74418.html. Cited June 12, 2015.

8. Kaspersky Security Bulletin 2014. https://securelist.ru/files/2014/12/Kaspersky-Security-Bulletin-2014-RU.pdf. Cited May 12, 2015.

9. The Digital World in 2025. http://beta.futureview.ru/files/documents/505966f4379ce1000000001c.pdf. Cited June 10, 2015.

10. Antipov, G., Guzner, I.A., Donskikh, O.A., Ermolenko, S.M., Ivonin, Yu.P., Isakov, S.P., Lesnevskii, Yu.Yu., Lizunova, I.V., Litvintseva, G.P., Makarova, N.I., Muratov, P.D., Os'muk, L.A., Sivirinov, B.S., Smirnova, O.V., et al., Round table: Are libraries without books the inevitability of the future? *Idei i Idealy,* 2011, vol. 1, no. 2, pp. 2–22.

11. Svergunova, N.M., Information security of libraries. http://library.gu-unpk.ru/docs/publ_sotr/Informacionnay%20bezopasnosti.pdf. Cited June 4, 2015.

12. Rodionova, Z.V., Technology of access rights change management based on analysis of business processes, *Vestn. NGUEU,* 2011, no. 1, pp. 16–21.

13. Pestunova, T.M. and Rodionova, Z.V., Information system for managing access rights on the basis of analysis of business processes. Part 2, *Dokl. Tomsk. Gos. Univ. Sist. Upr. Radioelektron.,* 2010, no. 2 (22), pp. 253–256.

14. Pestunova, T.M., Rodionova, Z.V., and Gorinova, S.D., Analysis of aspects of information security based on formal models of business processes, *Dokl. TUSUR,* 2014, pp. 150–156.

15. Astakhov, A.M., *Iskusstvo upravleniya informatsionnymi riskami* (Art of Information Risk Management), Moscow: DMK-Press, 2010.

Translated by K. Lazarev