UDC 004.056
doi:10.31799/1684-8853-2023-1-41-50
EDN: MFUKDX

Articles

Information security audit for a manufacturing company

S. V. Shirokova[a], *PhD, Tech., Associate Professor, orcid.org/0000-0001-9384-1877*
O. V. Rostova[a], *PhD, Econ., Associate Professor, orcid.org/0000-0001-6581-3473, O.2908@mail.ru*
M. V. Bolsunovskaya[a], *PhD, Tech., Associate Professor, orcid.org/0000-0001-6650-6491*
L. A. Dmitrieva[a], *Junior Researcher, orcid.org/0000-0003-3831-7137*
T. O. Almataev[b], *PhD, Tech., Associate Professor, orcid.org/0000-0003-2373-9732*
[a]*Peter the Great St. Petersburg Polytechnic University, 29, Politekhnicheskaia St., 195251, Saint-Petersburg, Russian Federation*
[b]*Andijan Machine-Building Institute, 56, Bobur Shoh St., 170019, Andijan, Uzbekistan*

Introduction: *The number of information attacks on company information systems has now increased significantly. The unintended consequences of such attacks are both financial and reputational losses. To increase the effectiveness of information protection, a sound analysis of the level of information system security is necessary.* ***Purpose:*** *To justify the need and describe the information security audit procedure for a manufacturing company.* ***Results:*** *We have analyzed business operations of a certain company and collected the necessary information for an information system security audit. Having analyzed the approaches to threat identification and countermeasure techniques, as well as the specifics of the company in question, we have chosen a combined approach. The study of different risk analysis methods has allowed to substantiate the choice of FRAP methodology. As a result of the audit procedure the compliance of the information system to the information security standards has been assessed.* ***Practical relevance:*** *Recommendations for reducing risks associated with threats to information security have been developed. The implementation of the developed countermeasures to eliminate information security vulnerabilities will allow the company to avoid possible financial losses and avert the damage to the company's reputation.*

Keywords *— digital transformation, information systems security, project, information security standards, business process, audit.*

For citation: Shirokova S. V., Rostova O. V., Bolsunovskaya M. V., Dmitrieva L. A., Almataev T. O. Information security audit for a manufacturing company. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2023, no. 1, pp. 41–50. doi:10.31799/1684-8853-2023-1-41-50, EDN: MFUKDX

Introduction

The relevance of information protection is due to the widespread use of information systems for the transmission, storage and processing of significant amounts of information, especially given the global trend towards an increase in the number of information attacks that lead to significant financial and reputational losses [1, 2]. For effective protection against attacks, organizations need a sound analysis of the security level of the information system, especially taking into account the ongoing digital transformation [3, 4]. This is exactly what security audits are used for.

The purpose of this study was to substantiate the need and describe the information security audit procedure for a manufacturing company, as well as to develop recommendations based on the analysis. In accordance with this goal, the following tasks were set:

1. Gather all necessary information about the company, the information system used, important business processes and the current information security system.
2. Investigate the types of information security audits and methods used to identify threats, vulnerabilities and countermeasures. Compare them and select the most appropriate ones for the company under investigation.
3. Conduct a security audit of the company's information system using the selected methods.
4. Develop recommendations to eliminate or minimize the identified information security risks of the company.

Drawing up an audit plan is not a trivial task, as it requires the auditor to be experienced in the methods of constructing such plans, and also depends on the objectives of the audit and the features of the audited object. Information security audits can be conducted according to a number of criteria, including requirements defined on the basis of one or more standards, as well as policies and requirements established by stakeholders.

Security audit of the company's information assets allows you to get an idea of the security status of the infrastructure and information security management processes. An information security audit is a test of the ability to successfully counter information security threats. Conducting an independent audit allows you to identify risks in a timely manner and objectively assess the compliance of the parameters characterizing the information security regime with the required level [5, 6].

According to the type of threats, it is possible to distinguish natural, associated with the impact of natural physical processes, and artificial, caused by the impact on the human information environment. Artificial threats can be unintentional (system failures, computer and communication equipment failures, employee errors) and intentional (caused by deliberate actions of people).

All sources of threats to information security are divided into three main groups [7]:

1) threats caused by the actions of subjects. These sources can be predicted and appropriate measures taken;

2) threats caused by technical means (man-made sources);

3) natural sources of threats. Such sources of threats are completely unpredictable, and therefore measures against them should always be applied.

It is the type of threat that determines the nature and features of anti-risk measures.

Rationale for auditing information security

A company engaged in the production of textile materials uses a CRM (Customer Relationship Management) system in its activities. The company uses a CRM-system, namely vTiger CRM, an open source customer relationship management system. The vTiger CRM-system has been specially modified in accordance with the requirements and objectives of the company. It has added modules, reports and functions that are not provided in the standard system solution.

In order for each employee to have access only to the information that he needs to perform his duties, roles are created in the information system. Available modules and available actions with records of these modules are installed for each role.

For the effective operation of the company, it is necessary that the data from the information system be accessible to employees who have access to it, so that this data is reliable, not distorted and confidential. To do this, it is necessary to ensure the security of the company's information system.

Since the CRM-system was recently implemented, it was necessary to conduct a study of possible threats to the security of the information system. The purpose of the information security audit was not only to reveal vulnerabilities and identify risks, but also to describe possible consequences and develop countermeasures to improve the current level of information system security.

Comparative analysis of information security audit types

There are different classifications of audit types. In the work, a study of different types of information security audit depending on the methods and means used was conducted and their distinctive features were identified, which are presented in Table 1 [8–10].

■ ***Table 1.*** Comparison of the types of audit

Audit type	Criteria		
	Verification tools and methods	Result of the test	The ideal with which the result of the test is compared
Hardware audit	Conducting real attacks on the information system by experts using special software and special methods	It is aimed at identifying and fixing the vulnerabilities of the system's software and hardware	Set of known vulnerabilities in the software and the expected test result
Expert audit	Collection and analysis of information on IS, analysis of organizational and administrative documents and information flows of the enterprise	Identifying global errors in the corporate network topology, using security tools, identifying vulnerabilities of information system	Requirements of the company's management for protection, as well as the auditor's own experience
Audit of compliance with standards	Collection and analysis of information on IS and subsequent comparison with the description of the standard	The degree of compliance of the tested IS with the selected standards, as well as recommendations for bringing the security of the IS in accordance with standards	Abstract description of the state of information security which given in the standards
Complex audit	Depends on the set of procedures that will be implemented during this audit		

Regardless of the type of audit used, in general, the information system security audit process consists of the following stages:

— initiation of the audit procedure;

— collecting the audit information;

— data analysis;

— making recommendations and preparing an audit report.

Recommendations are determined by the approach used, the characteristics of the information system being audited, the state of information security in the company, and the level of detail used during the audit.

The use of different types of auditing can be done individually or in combination, it depends on the needs of the company.

The information security standards approach to data analysis begins with selecting the standard that will form the basis, or a set of additional standards. The standards define a core set of information security requirements.

The ISO / IEC 27001 standard assumes the use of a process approach to create, implement, support the information security management system (ISMS). The implementation and use of a set of processes within the company that are interrelated. When creating the processes of the ISMS, the Deming cycle (PDCA) can be used, which is considered in the standard. The Fig. 1 shows the process of creating managed information security, where the process input is submitted to the requirements and expected results in the field of information security of the parties concerned, and on the output we receive managed information security. If desired, to enhance their reputation in the eyes of customers, companies can be certified for compliance with the requirements of ISO / IEC 27001.

For the company in question, a comprehensive information security audit was selected, which includes the following steps [12, 13]:

— analysis and construction of a model of interaction of components of information systems used in the provision of business processes of the organization;

— identification and determination of the value of information assets that are most important for ensuring the functioning of business processes. This stage allows you to take into account the unique structure of the system and the point of view of the company's management on critical assets and threats;

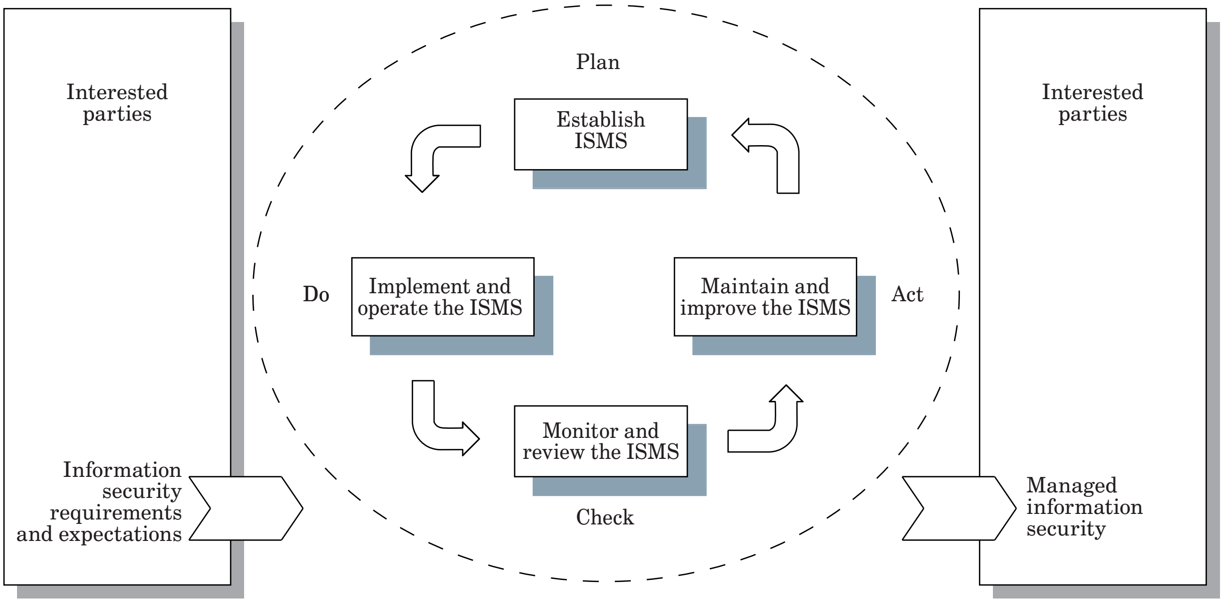
— study of the features of the existing information security system, analysis of the settings of standard security tools in the company, server operating systems and communication equipment;

— conducting penetration tests into the company's information environment;

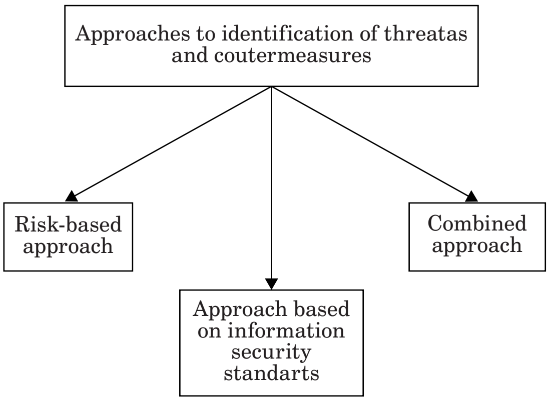
— identification of threats to the most significant information assets, assessment of their level, probability of manifestation and development of recommendations taking into account the requirements and standards of information security formed at previous stages.

The description of the stages is due to the need to specify this procedure for auditing information security in the company in question.

Depending on the selected audit type, different approaches are used to identify threats and countermeasures [14–16]. Variants of existing approaches to identify threats and countermeasures, depend-


Interested parties
Information security requirements and expectations
Plan
Establish ISMS
Do
Implement and operate the ISMS
Maintain and improve the ISMS
Act
Monitor and review the ISMS
Check
Interested parties
Managed information security

■ ***Fig. 1.*** Stages of building and using the ISMS [11]


Approaches to identification of threatas and coutermeasures
Risk-based approach
Combined approach
Approach based on information security standarts

■ ***Fig. 2.*** Types of approaches to identification of threats and countermeasures

ing on the selected audit approach, are presented in Fig. 2.

Let's describe each approach in more detail.

– The information security standards approach. In this approach, an information security standard is selected, compliance with which will be verified by the information system.

– Risk-based approach. This approach uses risk analysis methods to determine an individual set of information system security requirements [17, 18].

– Combined approach. A basic set of security requirements applicable to an information system is defined by a standard. Additional requirements, are formed on the basis of risk analysis.

For the company in question, a combined approach was chosen.

In addition, it should be noted that information security risk management methods for standard information system implementation projects and pilot projects, when high-tech solutions with a high degree of uncertainty are implemented, will differ significantly [19].

Information security risk analysis methods

Risk analysis is a study of information system security, in order to determine the key IT assets that are important to the company, as well as to identify threats against which they need to be protected. Key assets may include: information resources that support business processes; electronic media: system and application software; hardware; paper media. The importance or value of an asset is determined by the amount of damage that would occur if the confidentiality, availability, or integrity of the asset were to be compromised.

The development of adequate countermeasures to protect these assets occurs during risk management. At the same time, one must consider the fact that the value of the information security system should not exceed the value of the information being protected. The cost of the information security system includes the one-time costs of its development and implementation, as well as the operational costs of maintaining it. Detailed cost items, as well as an assessment of the effects of implementation are presented in detail in the publications [20, 21].

In the course of risk assessment and analysis, the following stages are distinguished:

1) identifying the key assets of the organization;

2) analyzing which key assets need to be protected;

3) creation of a list of expected threats and vulnerabilities that may lead to the emergence of these threats;

4) assessing the likelihood that security threats will materialize;

5) assessing the level of impact with employee involvement;

6) qualitative or quantitative risk assessment;

7) interpretation of the obtained results.

Qualitative or quantitative risk analysis can be done. Most companies usually choose a qualitative risk assessment because it is an easier way to assess risks. In this case, also qualitatively assess the levels of damage from the implementation of the attack, as well as the level of probability of threat of the attack itself.

In order to more reasonably choose a method of information security risk analysis for the enterprise in question, a comparative analysis of the most well-known and popular methods was made: CRAMM, RiskWatch, FRAP, OCTAVE.

This list presents methods that perform qualitative, quantitative, and comprehensive risk assessment. It will also describe one method that is used only in the framework of internal audit. Let's describe each of the methods a little.

1. *CRAMM* is based on an integrated risk analysis approach, i.e. Qualitative and quantitative assessments are used simultaneously [22]. Also, the method is considered universal, because Suitable for companies of different sizes and working in different areas. In addition, this technique allows you to justify the costs of building or upgrading the information security system and prevents unnecessary costs.

CRAMM divides the procedure of risk analysis into three stages.

In the first stage, the research boundaries are first defined, then within the boundaries, the system resources are identified and their value is determined. After this, the critical resources of the information system are determined on the basis of the data obtained. If the level of criticality of system resources is low enough, then this information system is considered to require a basic level of protection, and this level does not require a detailed assessment of information security threats, therefore, the second stage of the procedure is skipped.

At the second stage, security threats are identified for the system resources under consideration, as well as an analysis of the probability of their occurrence and threat analysis. On the basis of available information, risks of threats are calculated. It should be noted that countermeasures existing in the company are not taken into account in order to avoid an incorrect evaluation of the effectiveness of countermeasures.

At the third stage, a list of adequate countermeasures is developed to reduce risks and develop recommendations for working with them. The auditor also justifies the proposed countermeasures. Further, the company's management analyzes the information received, assesses the labor costs and material costs of implementing or improving the protection system, benefits the business and decides which of the recommended will be implemented.

The merits of this method include:

— availability of a software tool that implements this method;

— well-tested.

The disadvantages of the CRAMM method include:

— sufficient time-consuming procedure;

— requires a high level of qualification of the auditor.

CRAMM is suitable for existing information systems, not for those that are under development.

2. The *RiskWatch* methodology is based on a quantitative risk assessment. Risk is estimated through a numerical value, in this case through the size of annual loss expectancy and an estimation of return on investment [23]. The procedure for risk analysis based on the RiskWatch method consists of four stages.

At the first stage, a description of the research object is given: the type of organization in question, the requirements for the security of the information system, and the structure of the information system.

The second stage provides a detailed description of system resources, losses, and incident classes. In this case, incident classes themselves are obtained after comparing the loss category and resource category.

At the third stage of this procedure, a quantitative risk assessment is carried out. The effect of using the recommended protection is determined using the return on investment indicator.

At the fourth stage, reports with analysis results are generated. When analyzing risks, the RiskWatch method uses special estimates, called LAFE (Local Annual Frequency Estimate) and SAFE (Standard Annual Frequency Estimate).

The merits of this method of risk analysis include:

— in the course of this procedure, in addition to the risk assessment, the effectiveness of the implemented information security measures is calculated;

— a report is generated, on the basis of which a decision can be made about the necessity and expediency of introducing the recommended means of protection;

— there is appropriate software that implements this method.

Disadvantages of RiskWatch is:

— it is difficult to adapt to Russian companies;

— it is quite problematic to obtain estimates of LAFE and SAFE for our conditions.

3. The *FRAP* methodology is based on a qualitative assessment of the risks of implementing information security threats [24]. At the same time, it is based on the principle that an unprotected information system is assessed, which makes it possible to evaluate the effectiveness of new implemented information security tools, i.e. At the initial stage of the analysis, we believe that there is no protection system.

The risk assessment procedure should consist of the following steps:

Identification of the resources to be protected. Information can be obtained by interviewing company employees and by analysing documentation accompanying the information system.

Identification of possible threats. A list of possible threats can be used, in which company representatives mark what they believe to be the most likely threats to the resources in question. In addition, threats can be identified based on statistics for the information system in question or for similar systems.

Risk assessment. The probability of each threat and the damage it can cause is determined. A final risk assessment is then carried out.

Development of countermeasures to eliminate risks or reduce them to a level acceptable by the company's management. The incremental cost of acquiring and implementing the proposed information security tools is identified.

Preparation of analytical reports.

Advantages of the FRAP methodology:

— a detailed description of how to obtain the information required for system and vulnerability analysis;

— the scales used to assess the likelihood of threat occurrence and the level of damage are simplified in this case, as they contain only three criteria.

The disadvantages are that this methodology requires an auditor with a very high level of expertise.

4. The *OCTAVE* method is a method of rapid assessment of critical threats, assets and vulnerabilities [25]. This method of analysis and risk management is used for internal audit by employees of

the company, i.e. It is planned to create a certain group of company employees (technical specialists and management units). This technique qualitatively assesses the risks of information security.

The OCTAVE method consists of eight steps:

At the first step, it is necessary to define qualitative indicators for risk assessment, for example, the level of costs for information security, criticality of information resources.

The second step is the identification of key resources, as well as the compilation of profiles for each of them. The profile implies a description of the characteristics and characteristics of the resource in order to identify security requirements for it.

At the third step, the storage locations for the resources in question are identified, the security of these places is analyzed, bottlenecks are identified.

At the fourth step, critical information security locations are identified to detect the obvious threats as quickly as possible.

At the fifth step, a tree of threat scenarios is compiled.

At the sixth step, a risk is defined for each resource to assess its criticality.

At the seventh step, possible damage from the threat to risk prioritization is calculated.

Countermeasures are being developed at the eighth step.

The advantages of OCTAVE include:

— the methodology is designed to organize different areas;

— ease of use;

— suitable for regular use.

The disadvantages include the following:

— calculated only for internal audit;

— does not involve any residual risk management mechanisms.

Based on the analysis of existing risk analysis methods, FRAP was chosen because it is suitable for external auditing (unlike OCTAVE), and because it is based on a qualitative risk assessment (unlike RiskWatch and CRAMM), which is easier to use, and because in this case a qualitative risk assessment is sufficient.

Audit results

At the first stage, a basic set of requirements was formed based on information security standards, which were divided into the following groups:

1) physical access control and premises monitoring;

2) hardware information system;

3) network support for the information system;

4) system software;

5) application software;

6) organizational support.

The report described the current state of the information security system, optimal structure, identified remarks and threats, measures to reduce threats.

The next stage was the formation of additional requirements, taking into account the specific functioning of the information system on the basis of risk analysis. This approach is quite time consuming and requires a high level of auditor skills. In the course of using this method, an individual set of requirements for the security of the information system is determined.

To determine the key resources of the company, the method of "brainstorming" the company's employees was used. As a result of the discussion, the assets were determined, we will consider some of them:

— servers on which all important information for the company is stored and processed (data about customers, orders, etc.);

— database, where all the information necessary for the functioning of the organization is stored;

— electronic media, on which copies of contracts and agreements with customers and suppliers are stored.

Assets with different levels of criticality were selected for greater visibility of the method.

Identification of possible threats

Possible threats to information security for previously defined resources were identified by brainstorming the company's employees. As a result of the discussion, possible threats to each of the resources were identified. Let's look at them in more detail.

Possible threats to servers:

– malicious server damage or destruction;

– server failure due to technical reasons;

– destruction of the server by a natural disaster, such as fire.

Possible threats to the database where all the information necessary for the organization's operation is stored:

– unintentional modification or deletion of information from the database by company employees;

– leakage of confidential information as a result of copying information from a database using an external electronic medium.

Possible threats to electronic media that store copies of contracts and agreements with customers and suppliers:

– destruction or damage of electronic media by an attacker, resulting in data loss;

– destruction of electronic media due to fire.

At the next stage, a qualitative assessment of the likelihood of threats and an assessment of damage in case of their manifestation was carried out (Table 2).

According to the methodology applied, each level of risk corresponds to a specific response: A — risk

■ ***Table 2.*** Qualitative assessment of the probability of the implementation of threats and assessment of damage

Threats	Probability	Damage	Risk
Malicious server damage or destruction	Low	High	B
Server failure due to technical reasons	High	High	A
Destruction of the server by natural cataclysm, for example, by fire	Average	High	B
Unintentional modification or deletion of information from the database by employees of the company	High	Average	B
The leakage of confidential information as a result of copying information from the database using an external electronic medium	Average	Average	B
Destroying or damaging an electronic medium by an attacker, which results in data loss	Low	Low	D
Destruction of the electronic carrier in consequence of a fire	Average	Low	C

action should be taken immediately on a mandatory basis; B — risk action should be taken; C — monitoring of the situation is required; D — no action is required at this time.

Recommendations

After the audit of the company's information security, a list of recommendations was compiled.

On the basis of the table obtained, one can see that only one of the risks under consideration is a critical level: server failure due to technical reasons.

To reduce this risk it is recommended:

— use of RAID technology (fault tolerance technology);

— maintaining a constant temperature, through the use of air conditioning (main, backup);

— reservation of important information to separate servers or external storage media;

— conduct a continuous check of the server room to detect breakdowns or malfunctions.

To reduce risks in case of inadvertent modification or deletion of information from the database, company employees should implement the following:

— reservation of important information to separate servers or external storage media;

— implementation of the functionality of storing the history of database changes.

The risk associated with the leakage of confidential information as a result of copying information from the database using an external electronic medium is high enough to reduce it:

— implementation of the DLP (Data Leak Prevention — Information Leakage Prevention System), which will analyze the data streams along the protected perimeter;

— introduction of organizational and administrative documents, which will describe: what information is confidential, the requirements for working with such information, as well as the appropriate sanctions for their failure to comply;

— implementation of active monitoring systems for employee workstations.

To reduce the risk associated with the destruction of electronic media that stores copies of contracts and agreements with customers and suppliers, you can use the same information security tools as to protect servers from fire, but this is not mandatory, because the damage from the threat is estimated as low and most likely the cost of implementing protection will be higher than the damage caused.

The risk of destruction or damage to electronic media by an attacker, resulting in data loss, is low. The damage is also assessed as low, so there is no need to take any measures to manage this risk at this time.

At the organizational level, it is recommended:

— regularly review the security policy when making changes to the company's system;

— include in the job responsibilities of all employees the task of ensuring information security;

— the IT service checks the personnel being hired;

— remind an employee of the company that they have signed an agreement to comply with the trade secret regime;

— regularly send information about incidents and viruses to all employees of the company;

— when creating a company's information security system, you need to consider the option that the company's employees have sufficient knowledge to perform unauthorized access to information when they have the opportunity;

— place the equipment in rooms that cannot be accessed by persons who are not connected with the maintenance of this room;

— in the event of a hard disk failure, call a representative of the supplier and inspect the damage in the presence of responsible representatives of the company;

— update antivirus databases every day;

— conduct regular third-party security audits of the company, as well as penetration tests performed by independent experts

— regularly use the vulnerability scanner to track changes in the security of the company's information system;

— ensure that the company's information system meets any published security standard;

— use only certified local and network security tools in the company;

— exclude the presence of service personnel in the company's office without the presence of controlling persons;

— develop a list of documents and recommendations on non-disclosure of confidential information by employees.

Conclusions

The study substantiated the feasibility of implementing an information security system at a manufacturing enterprise, and described in detail the procedure for auditing information security in a particular organization. In accordance with the goal, the following tasks were solved.

Collected and analyzed information about the company. Important business processes of the company include the processes of production of products (fabrics). Special attention is paid to the technological process of production. For effective operation of these business processes, up-to-date information from the information system is necessary, access to which should not be difficult for authorized persons. Also, the information must be securely protected from access by unauthorized persons. To ensure these requirements, it is necessary to conduct a security audit of the information system.

Possible types of information system security audits are analyzed. A review of methods for identifying threats and countermeasures is made: an approach based on risk analysis, an approach based on information security standards, and a combined approach. We selected a comprehensive audit with a combined approach to identifying threats and countermeasures. The ISO/IEC 27001 standard was chosen as the information security standard, which describes the requirements for information security. FRAP was chosen as the risk analysis method.

The company's information system security audit was conducted taking into account the selected procedure. Existing threats to information security were identified and analyzed. The most important of them are: server failure due to technical reasons, as well as copying information to external removable media for further disclosure.

Developed recommendations to eliminate existing threats to information security for the company. The most important implementation recommendations are the purchase and installation of an air conditioning and fire alarm system in the server room, as well as the implementation of a DLP-system designed to prevent leaks of confidential information outside the corporate network. In addition, the cost of all recommended information security measures for threats found was 183,000 rubles, which is included in the company's acceptable information security budget of 210,000 rubles. If these recommendations are implemented (organizational and software-technical), the security of the information system will increase, and the risks of threats found will decrease, which will allow the company to avoid financial and reputational losses in the future.

Financial support

The research is funded by the Ministry of Science and Higher Education of the Russian Federation under the strategic academic leadership program "Priority 2030" (Agreement 075-15-2021-1333 dated 30.09.2021).

References

1. Whitman M. E. In defense of the realm: understanding the threats to information security. *International Journal of Information Management*, 2004, vol. 24, no. 1, pp. 43–57. doi:10.1016/j.ijinfomgt.2003.12.003
2. Anisimov V. G., Anisimov E. G., Saurenko T. N., Zotova E. A. Models of forecasting destructive influence risks for information processes in management systems. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2019, no. 5, pp. 18–23. doi:10.31799/1684-8853-2019-5-18-23
3. Babash A. V., Baranova E. K. *Aktual'nye voprosy zashchity informacii* [Actual issues of information protection]. Moscow, INFRA-M Publ., 2017. 111 p. (In Russian). doi:10.12737/monography_58dbc380aa3a4
4. Amirova E. F., Voronkova O. Yu., Zakirova N. R., Stepanenko O. G., Doguchaeva S. M., Murzagalina G. M. Internet of things as a tool for development of russias digital economy. *International Journal of Mechanical Engineering and Technology*, 2019, vol. 10, no. 2, pp. 1011–1019.
5. Anisimov V. G., Zegzhda P. D., Suprun A. F., Anisimov E. G. The problem of innovative development of information security systems in the transport sector. *Automatic Control and Computer Sciences*, 2018, vol. 52, no. 8, pp. 1105–1110. doi:10.3103/S0146411618080035

6. Shmeleva A. S., Suloeva S. B., Rostova O. V. Use of agile management tools in projects of information security systems implementation. *Problems of Information Security. Computer Systems*, 2021, no. 4, pp. 123–136. doi:10.48612/jisc/5zkx-22b9-8 kam

7. Vostretsova E. V. *Osnovy informacionnoj bezopasnosti* [Fundamentals of information security]. Yekaterinburg, Ural'skij universitet Publ., 2019. 204 p. (In Russian).

8. Astahov A. *Audit of Information Systems Security.* Available at: http://iso27000.ru/chitalnyi-zai/audit-informacionnoibezopasnosti/audit-bezopasnosti-informacionnyh-sistem (accessed 25 August 2022).

9. *Audit informacionnoj bezopasnosti* [Information security audit]. Available at: https://intuit.ru/studies/courses/600/456/lecture/10226 (accessed 15 September 2022).

10. Maksimova E. A. Audit of information security. *Information Protection. Inside*, 2006, no. 6(12), pp. 64–65 (In Russian).

11. State Standard R ISO/IEC 27001-2006. *Information technology. Security techniques. Information security management systems. Requirements.* Moscow, Standartov Publ., 2008. 31 p. (In Russian).

12. *Kompleksnyj audit* [Comprehensive audit]. Available at: http://www.pointlane.ru/security_a/complex (accessed 24 September 2022).

13. Sabillon R., Serra-Ruiz J., Cavaller V., Cano J. A comprehensive cybersecurity audit model to improve cybersecurity assurance: The CyberSecurity Audit Model (CSAM). *2017 Intern. Conf. on Information Systems and Computer Science (INCISCOS)*, 2017, pp. 253–259. doi:10.1109/INCISCOS.2017.20

14. Pandey S. K. A comparative study of risk assessment methodologies for information systems. *Bulletin of Electrical Engineering and Informatics*, 2012, vol. 1, no. 2, pp. 111–122.

15. Hashim N. A., Abidin Z. Z., Puvanasvaran A. P., Zakaria N. A., Ahmad R. Risk assessment method for insider threats in cyber security: A review. *International Journal of Advanced Computer Science and Applications*, 2018, vol. 9, no. 11. doi:10.14569/IJACSA.2018.091119

16. Shirokova S., Kislova E., Rostova O., Shmeleva A., Tolstrup L. Company efficiency improvement using agile methodologies for managing IT projects. *ACM Intern. Conf. Proc. Series (DTMIS 2020)*, 2020. doi:10.1145/3446434.3446465

17. Kuzminykh I., Ghita B., Sokolov V., Bakhshi T. Information security risk assessment. *Encyclopedia*, 2021, vol. 1, no. 3, pp. 602–617. doi:10.3390/encyclopedia1030050

18. Baranova E. K., Chernova M. V. Comparative analysis of programming tools for cybersecurity risk assessment. *Problems of Information Security. Computer Systems*, 2014, no. 4, pp. 160–168.

19. Zharova M., Shirokova S., Rostova O. Management of pilot IT projects in the preparation of energy resources. *E3S Web of Conf.*, 2019, vol. 110, 02033. doi:10.1051/e3sconf /201911002 033

20. Anisiforov A. B. *Metodiki ocenki effektivnosti informacionno-tekhnologicheskih proektov v biznese* [Methods of evaluating the effectiveness of information technology projects in business]. Saint-Petersburg, Politekhnicheskij universitet Publ., 2018. 127 p. (In Russian).

21. Grozdova A., Shirokova S., Rostova O., Shirokova A., Shmeleva A. Rationale for information and technological support for the enterprise investment management. *Lecture Notes in Networks and Systems*, 2022, vol. 387, pp. 181–190. doi:10.1007/978-3-030-93872-7_15

22. Yang T., Berger E. D., Kaplan S. F., Moss E. B. CRAMM: Virtual memory support for garbage-collected applications. *Proc. of the 7th USENIX Symp. on Operating Systems Design and Implementation — OSDI'06*, 2006, pp. 103–116.

23. Kouns J., Minoli D. *Information Technology Risk Management in Enterprise Environments: A Review of Industry Practices and a Practical Guide to Risk Management Teams.* 2010. doi:10.1002/9780470558133

24. Nurul A. H., Zaheera Z. A., Puvanasvaran A. P., Zakaria N. A., Ahmad R. Risk assessment method for insider threats in cyber security: A review. *Int. J. Adv. Comput. Sci*, 2018, vol. 9, no. 11, pp. 126–130. doi:10.14569/IJACSA.2018.091119

25. Jufri M. T., Hendayun M., Suharto T. Risk-assessment based academic information system security policy using octave Allegro and ISO 27002. *Proc. of the 2nd Intern. Conf. on Informatics and Computing, ICIC 2017*, 2018. doi:10.1109/IAC.2017.8280541

УДК 004.056
doi:10.31799/1684-8853-2023-1-41-50
EDN: MFUKDX

Аудит информационной безопасности производственной компании

С. В. Широкова[а], канд. техн. наук, доцент, orcid.org/0000-0001-9384-1877
О. В. Ростова[а], канд. экон. наук, доцент, orcid.org/0000-0001-6581-3473, O.2908@mail.ru
М. В. Болсуновская[а], канд. техн. наук, доцент, orcid.org/0000-0001-6650-6491
Л. А. Дмитриева[а], младший научный сотрудник, orcid.org/0000-0003-3831-7137
Т. О. Алматаев[б], канд. техн. наук, доцент, orcid.org/0000-0003-2373-9732
[а]Санкт-Петербургский политехнический университет Петра Великого, Политехническая ул., 29, Санкт-Петербург, 195251, РФ
[б]Андижанский машиностроительный институт, Бобур шох ул., 56, Андижан, 170019, Узбекистан

Введение: количество информационных атак на информационные системы компаний в настоящее время значительно увеличилось. Нежелательные последствия таких воздействий заключаются как в финансовых, так и в репутационных потерях. Для повышения эффективности защиты информации необходим обоснованный анализ уровня безопасности информационной системы. **Цель:** обосновать необходимость и описать процедуру аудита информационной безопасности для производственной компании. **Результаты:** проанализирована деятельность компании, собрана необходимая информация для проведения аудита безопасности информационной системы. На основе анализа подходов к выявлению угроз и контрмер, а также специфики рассматриваемой компании был выбран комбинированный подход. Исследование различных методов анализа рисков позволило обосновать выбор методологии FRAP. В результате проведения процедуры аудита даны оценки соответствия информационной системы стандартам информационной безопасности. **Практическая значимость:** разработаны рекомендации по снижению рисков, связанных с угрозами информационной безопасности. Внедрение разработанных контрмер по устранению уязвимостей информационной безопасности позволит компании предотвратить возможные финансовые потери и ущерб репутации компании.

Ключевые слова — цифровая трансформация, безопасность информационных систем, проект, стандарты информационной безопасности, бизнес-процесс, аудит.

Для цитирования: Shirokova S. V., Rostova O. V., Bolsunovskaya M. V., Dmitrieva L. A., Almataev T. O. Information security audit for a manufacturing company. *Информационно-управляющие системы*, 2023, № 1, с. 41–50. doi:10.31799/1684-8853-2023-1-41-50, EDN: MFUKDX
For citation: Shirokova S. V., Rostova O. V., Bolsunovskaya M. V., Dmitrieva L. A., Almataev T. O. Information security audit for a manufacturing company. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2023, no. 1, pp. 41–50. doi:10.31799/1684-8853-2023-1-41-50, EDN: MFUKDX