decision making allows to make collecting of statistical material for the subsequent analysis. Use of the program does not cause inconveniences to the user. The program provides maintenance log, which records and stores the date and time of login, username, the number of errors made when entering the password, time and authorization result. The magazine is used for the monitoring of user access. The statistical data obtained by means of the developed program will allow to make number of estimates: informational content of separate characteristics of keyboard handwriting and their different sets, stability in time of characteristics of keyboard handwriting, influence of physical and emotional status of the user on characteristics of his handwriting and others.

Keywords: biometric characteristics, user authentication, keyboard handwriting, password authentication, program of the access permission of the user.

Віктор Леонідович Евецкий, кандидат технічних наук, доцент, доцент кафедри кібербезпеки та застосування автоматизованих інформаційних систем та технологій, Державний заклад "Інститут спеціального зв'язку та захисту інформації Національний технічний університет України "Київський політехнічний інститут", Київ, Україна.

E-mail**:** viktorevetsky@gmail.com.

Іван Вікторович Горнійчук, курсант, Державний заклад "Інститут спеціального зв'язку та захисту інформації Національний технічний університет України "Київський політехнічний інститут", Київ, Україна.

E-mail: knyazhorn@gmail.com.

Виктор Леонидович Евецкий, кандидат технических наук, доцент, доцент кафедры кибербезопасности и применения информационных систем и технологий, Государственное учреждение "Институт специальной связи и защиты информации Национального технического университета Украины "Киевский политехнический институт", Киев, Украина.

Иван Викторович Горнийчук, курсант, Государственное учреждение "Институт специальной связи и защиты информации Национального технического университета Украины "Киевский политехнический институт", Киев, Украина.

Viktor Yevetskyi, candidate of technical sciences, associate professor, associate professor at the cybersecurity and application of information systems and technologies academic department, State institution "Institute of special communication and information protection of National technical university of Ukraine "Kyiv polytechnic institute", Kyiv, Ukraine.

Ivan Horniichuk, cadet, State institution "Institute of special communication and information protection of National technical university of Ukraine "Kyiv polytechnic institute", Kyiv, Ukraine.

UDC 004.056.53

VITALII BEZSHTANKO,
OLEKSANDR MAKAREVYCH

IMPLEMENTATION OF INFORMATION SECURITY MANAGEMENT SYSTEM IN ORGANIZATION

The main objective of paper is the elaboration a common project of implementation information security management systems (ISMS) for organizations. For this, the steps of construction ISMS have been described in accordance with the rules and guidelines of the project management. Thus, in paper, the defined benefits were received by the company as a result of the implementation of an ISMS. The

scope management plan of ISMS was prepared and described. Also, in the work the objectives and tasks of project were identified. The plan for the project time management was suggested. The necessary human resources were defined and plan by for their use was designed. The plan of the communications management between stakeholders and participants was compiled in the project. An algorithm for determining the project cost was proposed. The criteria assessment the quality of the project of implementation ISMS is proposed. The mechanism for monitoring these criteria is developed. The algorithm of risks assessment of the project is defined. The process of the project ending is described. Taking into account the objective of the work, it's creating "a common project for any system..." but it was not possible to finish all phases of the project. Using the project as an example will help to understand what the head of the organization needs to do for the successful building ISMS.

Keywords: information security, information security management, information security management system, project management, implementation.

Introduction. Substantiation of the project. Implementation of selected pro-European vector of Ukraine, the ultimate goal is to join the European Union (EU). The development of international cooperation requires the design and implementation of national standards that take into account the current technical level and experience of the world and achieve compliance at least eighty percent of the national standards documents applicable in the EU.

ISO ISO/IEC 27001: 2010 "Information technology. Methods and means of achieving information security. Information Security Management Systems. Requirements" was adopted and harmonized to achieve these objectives in the field of technical information security which correspond a translation of the international standard ISO/IEC 27001:2005 [1]. Most of the information security management systems in the world are built and operated in accordance with the requirements of the standard, as evidenced by the number of issued certificates For example, at the end of 2013 in some EU countries companies: Bulgaria – 278, Germany – 581; Italy – 901; Romania – 840 have been certified. Recommendations of the ISO/IEC 27001 can be used in organizations with any ownership. It should be noted that a small number of implementation and certification of these standards organizations of private ownership in Ukraine due primarily to lack of funds and low level of their maturity. In organizations with state ownership to information, the protection of which is defined by law, a comprehensive information protection system (CISS) is built. It should be noted that the measures implemented by CISS are designed to protect information designated object information activities, and unlike ISO / IEC 27001 does not cover all the structural elements of the organization. Due to lack of understanding of the purposes of constructing CISS and implement recommendations outlined in standard ISO/IEC 27001 practical advice unused by state organizations. It should be noted that most standard requirements are implemented in the instructions of a structural element of the organization. For example, the requirements of ISO/IEC 27001 for the organization of personnel work outlined in the orders and instructions governing the work of the personnel department. Requirements for the management of the documents - orders and instructions ensure the organization of documents, and more. Thus the introduction of information security management system in compliance with the national standard ISO/IEC 27001: 2010 does not require the abolition of the existing regulatory framework. The recommendations of the standard primarily paid to the implementation of information security management system in the organization. Implementation and performance requirements of national standard ISO/IEC 27001: 2010 will allow organizations to build a complete system of protection that would take into account all aspects of information security based on best practices.

The results of the analysis of existing sources shows that the process of information security management system implementation is described 27000 series of standards, methodology of IT – grundshuts [2], NIST, series 800 [3], and other literature. However, none of the analyzed source does not describe the objectives and tasks, necessary for the implementation system of information security management in the organization. Thus a need for a common implementation of the project ISMS in accordance with established practice [4] exists.

Project benefits. Information Security Management System (ISMS) ensures integration of all employed in the enterprise security and organizational measures in a single real threats to an adequate and managed complex, allowing to achieve the objectives of corporate information security at the level of the enterprise. ISMS levels of integration in common organization are showed on fig. 1. Constructing ISMS allows you to clearly identify how processes and subsystems of information security are interconnected, who is responsible for them, what financial and human resources necessary for their effective functioning, and so on.

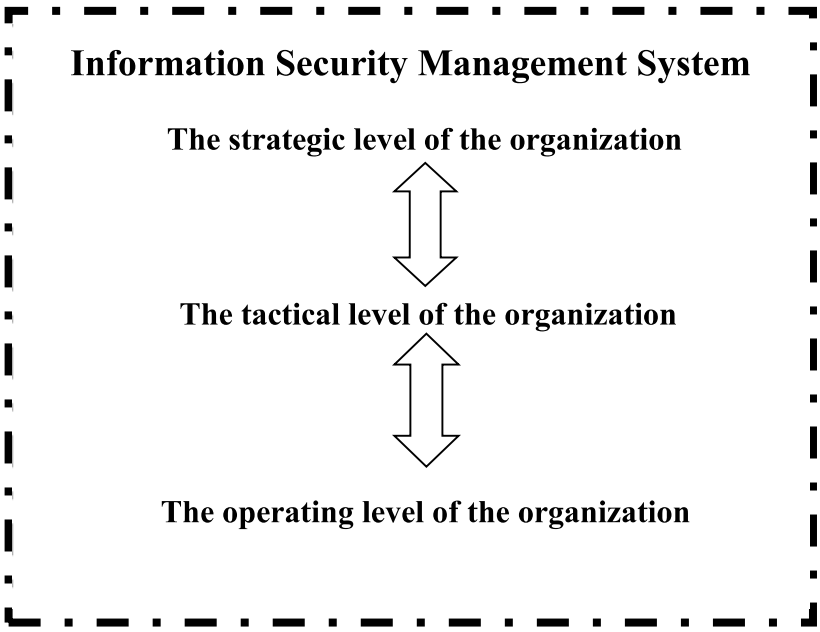

Figure 1 – ISMS levels of integration in common organization

Information security management system is built in accordance with requirements ISO/IEC 27001:2013 international standard and provides the customer a number of benefits from the implementation of the ISMS:

– identify security threats to the processes;

– reducing the financial risks and the risk of direct loss of the organization, increasing the current level of security;

– it is managed and controlled by a system of information security management;

– systematization of processes to ensure information security;

– prioritizing the organization in the field of information security;

– optimization and justification of the information security spending;

– ensuring compliance with information security level legislative, industry, contract, internal corporate requirements;

– increased trust of partners and customers through the organization of demonstrations to ensure a high level of maturity of information security to all stakeholders;

– reducing operational risk (increase of economic efficiency);

– reducing risks for investors (increase of transparency of the processes within the organization).

Goal. Thus, the actual task is the development generalized project information security management system implementation in the organization.

Use this project as an example will help understand what the head of the organization needs to make steps for the successful building ISMS.

Sponsor of the project is the management of an organization interested in building high-quality information security system.

Scope management plan. In order to implement the ISMS it is necessary to achieve the following objectives and tacks.

Objective 1. The officer of information security (manager of project) gets management support for implementation and starting up project.

Tasks:

- showing the result of cost/benefit analyst in another organization for top management;
- be approved of top management organization for implantation ISMS;
- the order to start work on the implementation of the ISMS;
- the appointment of a person responsible for the construction of information security (management representative);
- identify sources of funding.

Objective 2. Greater and training group of implementation ISMS in organization with requirements of standard ISO/IES 27001.

Tasks:

- to create a group for implementation and support of the ISMS;
- to train a group for implementation and support of the ISMS;
- to define the scope of ISMS.

Objective 3. Determine the difference between the current state of security in organization and requirements of standard ISO/IES 27001.

- to analyze the existing ISMS;
- to determine the list of works on refinement of the existing ISMS;
- the definition of the ISMS policy and the objectives of the ISMS;
- to appoint responsible person for ISMS;
- conduct training responsible for ISMS requirements standard;
- to compare the standard requirements with the existing state of affairs in the organization.

Objective 4. Implementation the risk management system.

Tasks:

- to identify and range assets;
- to define responsible for assets;
- to estimate assets;
- to develop procedure for identification of risks;
- to identify threats and vulnerabilities of assets;
- to calculate and range risks;
- to develop the plan for decrease in risks;
- to define inapplicable control (direction) of safety from appendix A;
- to develop the provision on an applicability control.

Objective 5. Implementation information security management system in organization.

Tasks:

- training of heads of divisions in requirements of information security;
- training of heads is carried out already according to existing documents which are actually necessary for work of their divisions;
- training of all personnel is carried out in educational combine according to, as a rule, two schemes, according to the plan of retraining or as induction;
- implementation of the necessary institutional arrangements and technical means of protection based on risk analysis.

Objective 6. Internal audit of the ISMS.

Tasks:

- selection team of internal audit of ISMS;
- planning of internal audit of ISMS;
- carrying out internal audit of ISMS.

Objective 7. The official launch of the ISMS.

Tasks:

– informing clients, partners, mass media on start of ISMS.

As a result introduction the organization gets: organization information security; management assets; aspect of security human resource; physical security; good communication and management networks; access control; system purchase of development and support of information equipment; incident management and another elements of information security.

Time management plan. Planning, that the project will take 82,5 days. Detailed timeline plan is presented fig. 2.

ID	Task Name	Duration	Start	Finish	Predecessors
1	**1 Implementation information security management system in organization**	**82.5 days**	**Tue 5/3/16**	**Fri 8/26/16**	
2	**1.1 The office of information security (management of project) confidence and get management support for implementation and starting up project.**	**7 days**	**Tue 5/3/16**	**Thu 5/12/16**	
3	1.1.1 Showing the result of cost/ benefit analyst in another organization for top management	1 day	Tue 5/3/16	Tue 5/3/16	
4	1.1.2 Showing the advantages of implantation ISMS in organization	1 day	Wed 5/4/16	Wed 5/4/16	3
5	1.1.3 Be approved of top management organization for implantation ISMS	1 day	Thu 5/5/16	Thu 5/5/16	4
6	1.1.4 The order to start work on the implementation of the ISMS	1 day	Fri 5/6/16	Fri 5/6/16	5
7	1.1.5 The appointment of a responsible for the construction of information security (management representative)	1 day	Tue 5/10/16	Tue 5/10/16	6
8	1.1.6 Identify sources of funding	2 days	Wed 5/11/16	Thu 5/12/16	7
9	**1.2 Greater and training group of implementation isms in organization with requirements of standard ISO/IES 27001.**	**4.33 days**	**Fri 5/13/16**	**Thu 5/19/16**	
10	1.2.1 To create a group for implementation and support of the ISMS	0.33 days	Fri 5/13/16	Fri 5/13/16	8
11	1.2.2 To train a group for implementation and support of the ISMS	3 days	Fri 5/13/16	Wed 5/18/16	10
12	1.2.3 To define the scope of ISMS	1 day	Wed 5/18/16	Thu 5/19/16	11
13	**1.3 Establish implications of requirements of ISO/IES 27001 of organization.**	**11 days**	**Thu 5/19/16**	**Fri 6/3/16**	
14	1.3.1 To analyze the existing ISMS	1 day	Thu 5/19/16	Fri 5/20/16	12
15	1.3.2 To determine the list of works on refinement of the existing ISMS	2 days	Fri 5/20/16	Tue 5/24/16	14
16	1.3.3 The definition of the ISMS policy and the objectives of the ISMS	2 days	Tue 5/24/16	Thu 5/26/16	15
17	1.3.4 To appoint responsible for ISMS	1 day	Thu 5/26/16	Fri 5/27/16	16
18	1.3.5 Conduct training responsible for ISMS requirements standard	3 days	Fri 5/27/16	Wed 6/1/16	17
19	1.3.6 To compare the standard requirements with the existing state of affairs in the organization	2 days	Wed 6/1/16	Fri 6/3/16	18
20	**1.4 Implementation of the risk management system.**	**16.33 days**	**Mon 6/6/16**	**Tue 6/28/16**	
21	1.4.1 To identify and range assets	5 days	Mon 6/6/16	Fri 6/10/16	19
22	1.4.2 To define responsible for assets	1 day	Mon 6/13/16	Mon 6/13/16	21
23	1.4.3 To estimate assets	2 days	Tue 6/14/16	Wed 6/15/16	22
24	1.4.4 To develop procedure for identification of risks	0.33 days	Thu 6/16/16	Thu 6/16/16	23
25	1.4.5 To identify threats and vulnerabilities of assets	3.33 days	Thu 6/16/16	Tue 6/28/16	24
26	1.4.6 To calculate and range risks	1 day	Tue 6/21/16	Tue 6/21/16	
27	1.4.7 To develop the plan for decrease in risks	1 day	Wed 6/22/16	Wed 6/22/16	26
28	1.4.8 To define inapplicable control (direction) of safety from appendix A	2 days	Thu 6/23/16	Fri 6/24/16	27
29	1.4.9 To develop the provision on Applicability kontrol	1 day	Mon 6/27/16	Mon 6/27/16	28
30	**1.5 Implementation information security management system in organization.**	**12 days**	**Thu 6/30/16**	**Fri 7/15/16**	
31	1.5.1 Training of heads of divisions in requirements of information security	1 day	Thu 6/30/16	Thu 6/30/16	29
32	1.5.2 Training of heads is carried out already according to ready documents which are actually necessary for work of their divisions	1 day	Fri 7/1/16	Fri 7/1/16	31
33	1.5.3 Training of all personnel is carried out in educational combine according to, as a rule, two schemes: according to the plan of retraining or as induction	1 day	Mon 7/4/16	Mon 7/4/16	32
34	1.5.4 Introduction of means of protection: administrative; educational; technical	6 days	Fri 7/8/16	Fri 7/15/16	
35	**1.6 Internal audit of the ISMS.**	**35 days**	**Fri 7/8/16**	**Thu 8/25/16**	
36	1.6.1 Selection of team of internal audit of ISMS	0.67 days	Fri 7/8/16	Mon 7/18/16	
37	1.6.2 Planning of internal audit of ISMS	3 days	Tue 8/9/16	Thu 8/11/16	36,34
38	1.6.3 Carrying out internal audit of ISMS	5 days	Fri 8/19/16	Thu 8/25/16	37
39	**1.7 The official launch of the ISMS.**	**0.5 days**	**Fri 8/26/16**	**Fri 8/26/16**	
40	1.7.1 Informing clients, partners, mass media on start of ISMS	0.5 days	Fri 8/26/16	Fri 8/26/16	38

Figure 2 – Project WBS and Timeline

Human resource management plan. The responsibility for the construction of information security management system rests with the company management. For this, manager responsible for the construction of information security management system was appointed from among the representatives. Assigning responsible for the implementation the ISMS was documented. To accomplish this, the organization published order. The duties of the person responsible for the implementation of ISMS in an organization among the leadership include:

– the organization and over the development monitoring, implementation and maintenance of the procedures and the processes of an ISMS;

– maintaining liaison with external organizations matters related to the ISMS;

– explanation of personnel of customer requirements for the purpose of their satisfaction;

– support manager of project and project implementation team.

There must be representative of leadership training to understand the project goals and objectives and to pass the course: introduction, implementation and auditing of information security

management system. In the next step a group for the implementation and support of the project must be created. The group includes management representative, project manager, coordinator of project, team of implementation, team of audit, press-secretary.

To do so, an order in an organization on the allocation representatives in the group is issued for implementation and maintenance of the ISMS of the divisions included in the area of building ISMS. For providing redundancy it is offered to assign two persons from every department to the group on introduction. The group should consist of a representative of the leadership, the project manager and the best trained representatives of the organization departments. They carried out the training requirements of the order and of building the ISMS. The training requirements of the standard and order of building the ISMS are carried out with them. At training we focused on the immediate areas of work of each assigned employee. The recommended course of study must include the following modules: introduction; audit; implementation, management representative.

Communications management. Plan. For the organization of close cooperation between the organization's management, the manager, coordinator and team project information security management system implementation is proposed:

1. To conduct the first meeting in the composition of senior management of the organization, department head, coordinator and project manager. To explain the goals and objectives of the project and to enlist the support of ISMS implementation team.
2. To conduct an introductory meeting in the composition of the leadership responsible for the construction of the ISMS project manager and implementation team. To determine the project goals and objectives, and procedure for interaction.

Order of interaction. For the organization of interaction is offered to hold meetings on Mondays at 08.10 and Friday 15.30. The manager, coordinator of the project and implementation team is attracted at the meeting. On Mondays specified set short-term goals, deadlines specified stages of the project, and if it's appropriate to make the necessary changes to the project plan. On Fridays to sum up the results of work done in a week, compares of the current status of the project with the planned. The results of the meeting have to be reported to the manager of the leadership responsible for the implementation the ISMS.

During the works, the personnel perform the project to inform the manager and coordinator of the project about all emerging issues affecting the project. Interaction has the following ways: a personal meeting, a phone call, e-mail, or Skype.

Control. It is necessary to establish and maintain a document which will be recorded arising problem to control the appeals coordinator of the project. The draft of schedule fixing arising problems is shown in tabl. 1.

Table 1 – The draft of schedule fixing arising problems

The members of the project	**Date / heart of the problem, who are made aware, measures taken**		
Member of implementation team	5.05	Fell ill system administrator	09.05 replacement system administrator

To control the interactions between the members of the project, coordinator of the project is to accumulate personal contacts (phone number, e-mail, Skype, etc.) of the project participants. Create a schedule registration of the project participants in the meetings. In case of absence a member of the project team at the meeting to carry out the appropriate registration. The member is required to inform the coordinator and project manager of the cause of absence from meetings.

Project cost management. Determining the cost of the project consists of two phases. The first is determined by the value of human resource costs, as well as, if necessary, the cost of attracted external workers (eg. for carrying network testing). It is planned, that projects involve only employees of the organization. Payment of their work takes place at the rates position. Payment of their work takes place at the rates position.

Residual cost of the project will be known after conducting a risk analysis and determination of required technical equipment and organizational measures protection. Resources used schedule is given in fig. 3.

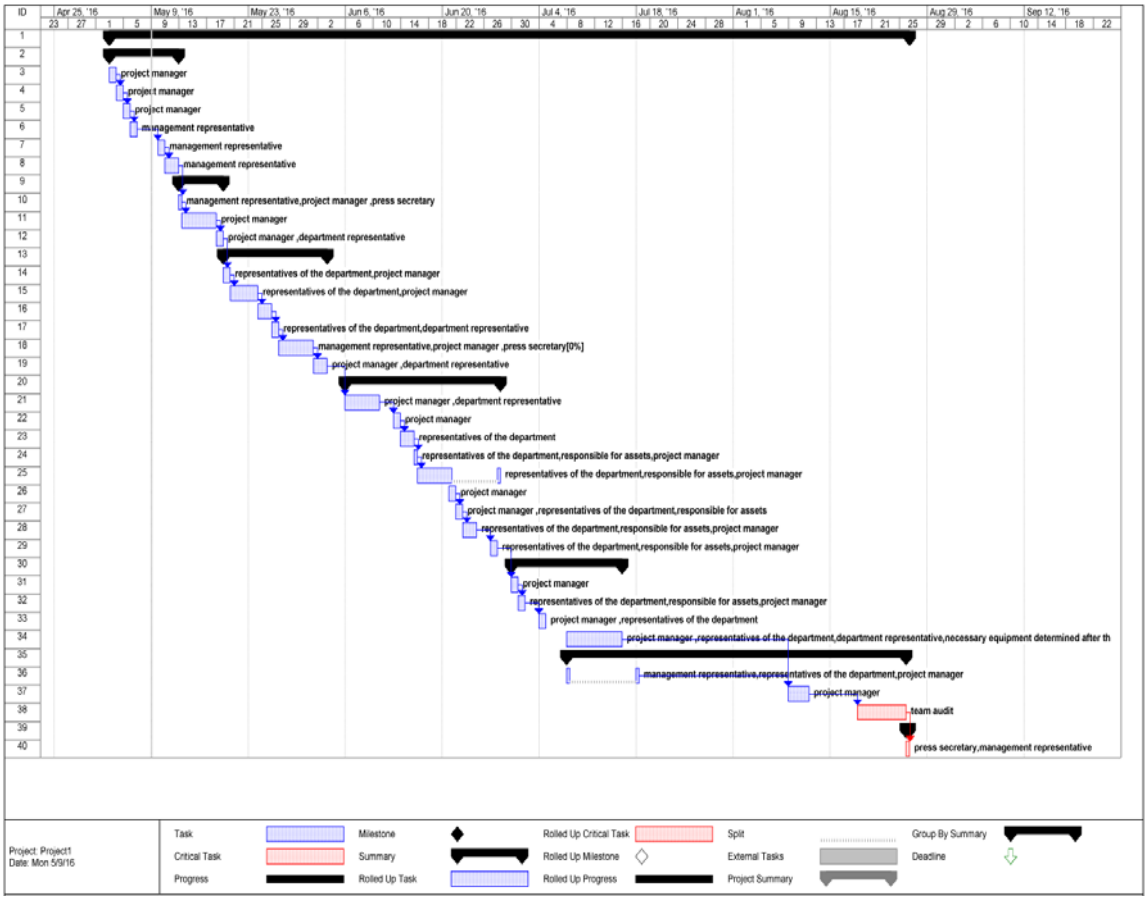

Figure 3 – Resource used schedule

Project quality management. Planning. It is planned that control over the quality of the project implementation of information security management system in the organization will be based on the following criteria:

1. Compliance with the requirements of the activities carried out in annex A of the standard ISO/IEC 27001:2013 "Information technology. Security techniques. Information security management systems. Requirements".

2. Compliance with the planned time schedule of the project and defined tasks. At the initial stage, to deviate from the time the project is not more than 20%.

3. Compliance with the planned budget and real status. A tolerance of finance spent no more than 20% of the planned.

Discussion of criteria and methods for achieving the quality of the project is planned to hold the first general meeting, must be present both stakeholders and project implementers.

Executing. The following actions are performed to ensure the quality of the project:

1) Every Friday, at 15.00, a report of the project coordinator of the extent to which the available jobs, the form set out in the tabl. 2.

Table 2 – Report form of the available jobs

Tasks	The degree of compliance with the plan (0 – 100%)	
	Date of control/Date of completion of the task	Date of control/Date of completion of the task
Task1.1.1.1	Time – (0 – 100%) Budget – (0 – 100%) Complies/does not comply	45% 55% does not comply

2) To verify compliance requirements of Annex A of the standard 27001 at the end of each task, the criterion: complies or does not comply. In case the selected criteria inconsistencies, in the project management plan we make appropriate adjustments (time, budget, tasks).

Monitoring and control. Project monitoring and control is carried out during the execution of the project and at the end of the project:

Throughout the project there is control of the project manager and people who responsible for the tasks according to previously defined criteria. It is immediately corrected by making appropriate adjustments to the project plan.

On completion of the project shall be appointed by order of the organization team of internal auditors. Training of them conducted. Internal audit conduct to determine compliance defined earlier criteria with the requirements of the standard ISO/IEC 27007:2011 “Information technology. Security techniques. Guidelines for information security management systems auditing”. If necessary, the certification organization invited external auditors.

Project risk management. The risks in this project should be divided into two groups:

1) information security risks;

2) the project risks.

The first group includes the risks arising due the implementation of information security threats on information resource. Risk assessment method developed by the project owner of the information asset and by the representative of the project implementation team under the supervision of project manager. Owner of information assets and a member of the implementation team must be members of the same department of the organization.

For the second group of risks is responsible project manager. They developed the approach to the definition of risk. For example, you can use the following method of qualitative risk assessment. So, it is possible to determine the risk = damage × the possibility of implementing the threat. The level of risk for each project is calculated using the following formula:

$$R = S \cdot E,$$

where R – project risk,

S – damage,

E – the possibility of implementing the threat.

Expert approach can be used to determine the probability of losses as shown in tabl. 3.

Table 3 – The frequency (probability) of threats

Threats	The frequency (probability) of threats 1-9				
	There were 4-5 times per year (Very high) 9 – 10	There were 3-4 times per year (High) 7 – 8	There were 2-3 times per year (Middle) 5 – 6	There were 2-3 times per year in the industry (Low) 3 – 4	There have been the historical aspect (Very low) 1 – 2
Threat 1				+	
Threat 2			+		

Levels of damage must be expressed in terms of losses for the organization and recovery time, such as “serious damage to the project, from which the project could not be implemented”. Example is show in table 4.

Table 4 – Table of damage

Level of damage	The criterion of damage	
Very low 1-2	Project delay 2 days	The project cost increased by 100 ₴
Low 3 - 4	Project delay 5 days	The project cost increased by 1000 ₴

Continuation of Table 4

Middle 5 – 6	Project delay 10 days	The project cost increased by 10000 ₴
High 7 – 8	The threat of disruption of project	The project cost increased by 100000 ₴
Very high 9 – 10	The project will not be implemented	The project cost increased by 1000000 ₴

Then, by multiplying the frequency of occurrence the threat and damage is determined the risk, example in tabl. 5.

Table 5 – Table of level risks

The frequency (probability) of threats	Level of damage					
		1 – 2	3 – 4	5 – 6	7 – 8	9 – 10
	1 – 2	Risk 20(4)	Risk 25(3)	Risk 1(5)	Risk 4(14)	Risk 12(9)
	3 – 4	Risk 23(6)	Risk 0(16)	Risk 2(15)	Risk11(21)	Risk16(27)
	5 – 6	Risk18(12)	Risk 24(24)	Risk 17(36)	Risk 3(35)	Risk 19(50)
	7 – 8	Risk 9(16)	Risk 7(32)	Risk 14(48)	Risk 22(56)	Risk 5(70)
	9 – 10	Risk 13(20)	Risk 15(40)	Risk 21(45)	Risk 6(80)	Risk 8(100)

Its value labeled risk numbers in parentheses in the field. Uther, the criteria for risk acceptability established. Assume that 50 units would be in this example. Then all the risks with values less than 50 units are acceptable, above – unacceptable.

Unacceptable risks are handled, the risk of an example of processing shown in the table 5.

Table 5 – Example of processing risk

Number of risk	Values of risk	Name of risk	Owner of risk	Required operation
Risk 22	56	Dismissal of members of implementation team responsible for network security	Manager of risk	Hiring a new specialist

The aim of this work is to establish a common approach to building the ISMS in an organization. It is therefore not carried out an attempt to describe and assess all risks.

Project closeout. Evidence of completion of the project is the order of implementation of information security management system in the organization. It is necessary to hold a final meeting of all employees and management of the organization. The meeting was to analyze all the difficulties arising in the course of work, and how solutions to problems have been found. Mark the best employees. If possible, encourage them. Once again recall that information security is a process that requires permanent employees participate. Announce dates for the internal audit. Also, to announce plans to hold a certification organization for compliance with the requirements of the standard ISO/IEC 27001:2013. Set planned certification deadlines.

Conclusion. Use this common project as an example will help understand what the head of the organization need to make steps for the successful building Information Security Management System.

REFERENCES

[1] International Organization for Standardization. 2013. *ISO/IEC 27001, Information technology. Security techniques. Information security management. Requirements*.

[2] Bundesamt für Sicherheit in der Informationstechnik. 2008. *BSI-Standart 100-2, IT – Grundschutz Methodology.* [Online]. Available: https://www.bsi.bund.de/EN/ Topics/ITGrundschutz/ itgrundschutz_node.html. Accessed on: March, 2, 2016.

[3] “NIST Special Publication”. [Online]. Available: http://csrc.nist.gov/publications/PubsSPs.html #SP 800. Accessed on: March, 2, 2016.
[4] *A Guide to the Project Management Body of Knowledge (PMBOK® Guide).* Philadelphia, Pennsylvania, USA: Project Management Institute, 2013.

The article was received 16.03.2016.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] International Organization for Standardization. 2013. *ISO/IEC 27001, Information technology. Security techniques. Information security management. Requirements*.
[2] Bundesamt für Sicherheit in der Informationstechnik. 2008. *BSI-Standart 100-2, IT – Grundschutz Methodology.* [Online]. Available: https://www.bsi.bund.de/EN/Topics/ITGrundschutz/ itgrundschutz_node.html. Accessed on: March, 2, 2016.
[3] “NIST Special Publication”. [Online]. Available: http://csrc.nist.gov/publications/PubsSPs.html #SP 800. Accessed on: March, 2, 2016.
[4] *A Guide to the Project Management Body of Knowledge (PMBOK® Guide).* Philadelphia, Pennsylvania, USA: Project Management Institute, 2013.

ВІТАЛІЙ БЕЗШТАНЬКО,
ОЛЕКСАНДР МАКАРЕВИЧ

ВПРОВАДЖЕННЯ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ В ОРГАНІЗАЦІЇ

Розробляється загальний проект впровадження системи управління інформаційною безпекою в організацій. Для цього етапи створення ситеми управління інформаційною безпекою описуються відповідно до правил і вимог керівних принципів управління проектами. Зокрема, визначаються вигоди, отримані організацією в результаті впровадження означеної системи. Підготовлено та описано план управління предметною областю створення системи управління інформаційною безпекою. Визначено мету і завдання проекту. Запропоновано план управління часом виконання проекту. Визначено необхідні людські ресурси і план їх використання. Розроблено план управління зв’язками в проекті. Запропоновано алгоритм визначення вартості проекту та критеріїв, за якими оцінюється його якість. Розроблено механізм контролювання цих критеріїв. Визначено основні ризики проекту та алгоритм їх оцінювання. Описано процес закінчення проекту. Його використання, як прикладу, допоможе зрозуміти керівництвом організації обсягу робіт, які необхідно виконати для результативного створення та впровадження системи управління інформаційною безпекою.

Ключові слова: інформація, інформаційна безпека, система управління інформаційною безпекою, оцінювання ризиків, управління проектами.

ВИТАЛИЙ БЕЗШТАНЬКО,
АЛЕКСАНДР МАКАРЕВИЧ

ВНЕДРЕНИЕ СИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ В ОРГАНИЗАЦИИ

Разрабатывается общий проект внедрения системы управления информационной безопасности в организации. Для этого этапы создания системы управления информационной безопасностью описываются в соответствии с правилами и руководящими принципами управления проектами. В частности, определяются выгоды, полученные организацией в результате внедрения такой системы. Подготовлен и описан план управления предметной областью создания системы управления информационной безопасностью. Определены цели и задачи проекта. Предложен план управления временем выполнения проекта. Определены необходимые человеческие ресурсы и план их использования. Разработан план управления

связями в проекте. Предложен алгоритм определения цены проекта и критериев, по которым оценивается качество проекта. Разработан механизм для контроля этих критериев. Определены основные риски проекта и алгоритм их оценки. Описан процесс окончания проекта. Его использование, как пример, поможет понять руководством организации объема работ, которые необходимо выполнить для результативного создания и внедрения системы управления информационной безопасностью.

Ключевые слова: информация, информационная безопасность, система управления информационной безопасностью, оценка рисков, управление проектами.

Vitalii Bezshtanko, candidate of technical sciences, head of laboratory, State institution "Institute of special communications and information protection National technical university of Ukraine "Kyiv polytechnic institute", Kyiv, Ukraine.

E-mail: v.bezshtanko@gmail.com.

Oleksandr Makarevych, postgraduate student, Pukhov institute for modeling in energy engineering of National academy of sciences of Ukraine, Kyiv, Ukraine.

E-mail: amakarevich20@gmail.com.

Віталій Михайлович Безштанько, кандидат технічних наук, начальник лабораторії, Державна заклад "Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут", Київ, Україна.

Олександр Євгенович Макаревич, аспірант, Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України, Київ, Україна.

Виталий Михайлович Безштанько, кандидат технических наук, начальник лаборатории, Государственное учреждение "Институт специальной связи и защиты информации Национального технического университета Украины "Киевский политехнический институт", Киев, Украина.

Александр Евгеньевич Макаревич, аспирант, Институт проблем моделирования в энергетике им. Г.Е. Пухова Национальной академии наук Украины, Киев, Украина.