Problems of building an effective policy information security of the enterprise

Andrii Pecheniuk *[1 A]

*Corresponding author: [1] Candidate of Economic Sciences, Associate professor of the Department of Finance, Banking, Insurance and electronic payment systems, e-mail: anvaspe@meta.ua, ORCID: 0000-0002-8348-5044

[A] State Agrarian and Engineering University in Podilya, Kamianets-Podilskyi, 32300, Ukraine

Received: May 17, 2021 | Revised: June 6, 2021 | Accepted: June 30, 2021

DOI: 10.5281/zenodo.4904552

Abstract

The necessity of building an effective information security policy of a modern enterprise is substantiated, the main components of such a policy are highlighted; summarizes the main types of information threats associated with the use of modern computer technology; groups of means of counteraction to threats to information security are systematized; the general characteristic of the basic directions of technical protection of information systems is resulted; the factors on which the organization of effective protection of information system of the modern enterprise depends are analyzed; the list of questions which need to be considered at construction of a policy of information security is offered; offers a number of recommendations to minimize the risks associated with information security of the enterprise.

Key words: information resources, information security, information security policy, information protection, computer technology, software, information security threats, communication channels, information attacks, internet fraud.

Introduction

In Ukraine, as well as around the world, there is a rapid development of the information society, the economic basis of which is the creation and improvement of technical and technological methods and means of production, obtaining and disseminating information based on the creation and use of information and communication technologies, signs of the modern information age.

The effectiveness of modern enterprise management is largely determined by what information is used by management and how it is managed, because it depends on the competitiveness of the firm.

In general, information is so closely related to business that this connection brings to the fore problems that are difficult to overestimate. Among them is the problem of information security of the enterprise.

Losses from the loss of important data or disclosure of confidential information often far exceed the cost of hardware and software used to store them.

Therefore, the preparation and implementation of an effective information security policy is one of the most important tasks to be solved when building an information system of a modern enterprise.

Material and methods

The theoretical basis of the study were the works of Ukrainian scientists on the organization of information security. To achieve the goal of the study used: general scientific methods (abstraction, comparison, generalization, analysis and synthesis) – to reveal the basic concepts of information security; critical analysis and system approach – in the analysis of the components of the formation of information security policy of the enterprise; abstract-logical method – to formulate

research conclusions.

Many researches of modern scientists are devoted to the problems of the organization of information security of the enterprise. In particular, the works of S. Legominova are devoted to the theoretical principles of information security of the enterprise; problems of effective organization of information systems are revealed by A. Batiuk, Z. Dvulit, S. Evseev, O. Korol, K. Obelovska, I. Ogorodnik, S. Ostapov, L. Fabri; features of formation of information security of information and communication systems are presented in publications of M. Zakharchenko; organizational and legal principles of information security were investigated by B. Kuzmenko, A. Nashynets-Naumova, Y. Khokhlachova, G. Nikitin.

However, the problem of building an effective information security policy of the enterprise remains insufficiently studied. Rapid changes in the environment of modern enterprise, the influence of internal and external factors increase the need to improve methods of information security management of the firm, the formation of an effective information security system.

Results and discussion

Information security of a modern firm is an organized activity of its officials (divisions) with the use of permitted forces and means to achieve a state of security of the information environment, which ensures its normal functioning and dynamic development (A. Nashinets-Naumova, 2012).

Information security policy is usually understood as a set of requirements, rules, restrictions, recommendations that regulate the order of information activities in the enterprise and aimed at achieving and maintaining the state of information security of the firm.

The development of such a policy is a very important process of a purely practical nature, which directly applies the knowledge and methods of absolutely all components of information security in a particular situation. Its implementation should be the result of joint activities of technicians capable of implementing its initial technical aspects, and managers of the enterprise interested in the correct policy-making from the financial, legislative and technical side, as well as staff that will now and in the future face information security policy and adhere to them.

It should be borne in mind that the construction of information security at modern Ukrainian enterprises often encounters various confrontations, which must be resolved in the prescribed manner, taking into account the current legislation (A. Nashinets-Naumova, 2017).

Implementation of a rational information security policy is a sign of maturity of a modern firm. The fact that the company clearly regulates its principles and approaches to information security means that serious work has been done in this direction.

Information security policy usually consists of two parts: general principles and specific rules of operation. General principles define the approach to Internet security, rules regulate what is allowed and what is forbidden (rules can be supplemented by specific procedures and instructions). The usual security policy regulates the use of basic network services and informs network users of their access rights, which is the procedure of user authentication (Y. Khokhlachova., 2012).

Information security policy is documented with a division into a number of levels of government. The document, which specifies those responsible for the implementation of the policy, its goals and structure, must be agreed with the highest management of the firm. Detailing of the main document is entrusted to the administrators of information systems security, who must take into account the principles of the enterprise, the availability of resources, as well as the importance of the goals that the company seeks to achieve by implementing information security policy. As a result, a system algorithm is developed, which provides for the use of clearly defined methods of protection of different types of resources (technical, information) and instructions that determine the behavior of employees in

appropriate situations (M. Melnyk, G. Nikitin, K. Mezentseva, 2017).

The information system of the object of protection can be considered protected if all operations are performed in accordance with strictly defined rules that provide direct protection of objects, resources and operations.

Information protection is usually understood as a set of legal, administrative, organizational, technical and other measures to ensure the safety, integrity of information and proper access to it.

It should be noted that the legal regulation of information circulation at the enterprise and liability for offenses in this area is based on the fact that according to Ukrainian law, any documented information is subject to protection, illegal recourse to which may harm its owner, user (A. Nashinets-Naumova., 2012).

The information security policy, in addition to the rules of delimitation of access, establishes management rules. Management functions are entrusted to proxies who are responsible for the security of processed information. These individuals are commonly referred to as computer system administrators.

As a rule, every modern enterprise regulates the rules of working with information. Information security policy is an integral part of the company's overall security policy. It is necessary in modern conditions to develop a list of requirements, threats and risk assessment and a description of the set of measures to combat information threats (M. Zakharchenko, V. Kononovich, V. Kildishev, D. Golev, 2011).

Among the most common types of information threats associated with the use of modern computer technology are:

malicious software;

internet fraud;

unauthorized access to information resources and information and telecommunication systems;

logic bombs (sets of commands that are written to the program and work under certain conditions;

“Trojan horses” (programs that perform certain actions without the knowledge of the owner of the infected system, for example;

send confidential information to a certain address);

different types of attacks that allow you to penetrate the network or intercept its management;

theft of funds;

means of slowing down data exchange in the network;

natural disasters.

The following main groups of means of counteracting information security threats can be distinguished:

legal or legislative (legal framework, regulations of the State Service for Special Communications and Information Protection);

moral and ethical (compliance with the norms of behavior in the information society of the country);

organizational or administrative (regulate the process of functioning of the data processing system, the use of its resources, staff activities, as well as the order of interaction of users with the system);

physical (based on the use of mechanical, electro- or electronic-mechanical devices designed to create physical barriers to possible penetration of potential intruders, their access to system components and protected information, as well as means of visual surveillance, communication and security alarm);

technical (use of various electronic devices and special software) (S. Ostapov, 2013).

Experts identify, for example, the following main areas of technical protection of information systems:

protection of information resources from unauthorized access and use, – power management tool and software download, as well as methods of password protection when logging in;

protection against leakage through secondary channels of electromagnetic radiation and guidance – by shielding equipment, premises, the use of masking noise generators, additional testing of equipment for the presence of compromising radiation;

protection of information in communication channels and switching nodes, – procedures of

authentication of subscribers and messages, encryption and special communication protocols are used;

protection of the legal significance of electronic documents – in a relationship of trust between two business entities and when there is a need to transfer documents (payment orders, contracts) on computer networks – to determine the authenticity of the addressee, the document is supplemented by a “digital signature” (Legominova, 2015).

Analysis of the state of affairs in the field of information security of Ukrainian enterprises shows that in the course of their activities, firms that are victims of “information attacks” do not always turn to law enforcement agencies, or try not to disclose encroachments on their information systems. This is due to the fact that companies do not want to “scare” customers by the fact that their information systems (as well as all the information contained in them) are not well protected.

It should be understood that even if the information security system is built taking into account all modern methods and means of protection, and the company has carefully selected and qualified personnel, it does not guarantee 100% protection of information resources: no security system can long resist targeted actions armed with modern technology. qualified violator (S. Ostapov, 2013).

However, a well-designed information security policy minimizes the relevant risks. In the current conditions, such a policy should be constantly supported: controlled, modernized, updated (A. Batiuk, 2004).

The organization of effective protection of the information system of a modern enterprise depends on:

the level of secrecy and properties of the information to be protected;

specific information processing technology; – hardware and software used by the enterprise;

location of the enterprise;

specifics of activity, etc. (S. Ostapov, 2013).

The task of information security must be solved systematically. This means that information security measures must be applied simultaneously and under centralized management. The components of the system must "know" about each other's existence, interact and provide protection from external and internal threats (S. Severina, 2016).

To build an effective information protection system, the company must answer the questions:

what information resources are subject to protection;

what software can be used on office computers;

disciplinary sanctions and general instructions on conducting official investigations;

to whom the rules apply;

who develops the general guidelines;

who has the right to change the instructions;

accurate description of the powers and privileges of officials;

who can provide powers and privileges;

the procedure for granting and revoking privileges in the field of information security;

completeness and procedure for reporting security breaches and criminal activity;

special responsibilities of management and employees to ensure information security;

date of commissioning and revision;

who and how implemented these rules (B. Kuzmenko).

According to the RFC 2196 System Security Guide “Site Security Handbook” (RFC – Requestfor Comment) there are four main stages of building an information security policy:

1) registration of all resources subject to protection;

2) analysis and creation of a list of potential threats for each resource;

3) assessment of the probability of occurrence of each threat;

4) making decisions that allow you to effectively protect the information system (A. Batiuk, 2004).

To minimize the risks associated with information security, the management of a modern enterprise has:

use effective full-fledged anti-virus software and regularly update virus signature databases.

use a software firewall and standard malware protection.

provide data backup by storing them on removable media, separated by servers;

comply with the requirements of modern methods of creating passwords, ensure their regular change;

do not store authentication data in easily accessible places;

closely monitor the manifestations of Internet fraud;

when using Internet resources (social networks, messaging systems, news, online games) do not follow unknown links and do not download files that have a potentially dangerous extension (for example, .exe, .bin, .ini, .dll, .com, .sys, .bat, etc.).

when connecting removable media to ensure their automatic verification for the presence of malicious software;

regularly raise awareness of the safe use of information technology and countering information threats, for the implementation of which the "human factor" is used (social engineering, Internet fraud).

When building a security policy, it should be understood that it will always be a compromise between the level of security of information resources of the system, which we want to get, how comfortable users will work with the system and, of course, the cost required for its operation (M. Melnyk, G. Nikitin, K. Mezentseva, 2017).

Conclusions

There is no clear answer to the question of how to ensure full protection of the information system. This is due to the presence of a number of factors influencing the decision: the specifics of the activity, security policy, financial capabilities, staff technical training, and so on.

However, to ensure the proper level of competitiveness, a modern enterprise must build a reliable system of information protection, which is one of the most important resources that ensures the development, efficiency and stability of the firm, increases productivity, resource efficiency.

Therefore, the formation and implementation of an effective information security policy is a necessary condition for the transition to a model of sustainable development not only of the individual enterprise, but also the national economy as a whole.

References

Basic course on information security. Available at: http://cert.gov.ua/pdf/Брошура-CERT-UA-Інформаційна-безпека.pdf (accessed 11.03.2021).

Batiuk, A.Ie. & Dvulit, Z.P. & Obelovska, K.M. & Ohorodnyk, I.M. & Fabri, L.P. (2004). Informatsiini systemy v menedzhmenti [Information systems in management]. Lviv: Natsionalnyi universytet «Lvivska politekhnika», «Intelekt-Zakhid», pp. 343-380.

Khokhlachova, Yu. (2012). Polityka informatsiinoi bezpeky obiekta [Object information security policy]. Pravove, normatyvne ta metrolohichne zabezpechennia systemy zakhystu informatsii v Ukraini: naukovo-tekhnichnyi zbirnyk, 2(24), 23-29.

Kuzmenko, B.V. & Chaikovska, O.A. Zakhyst informatsii. Orhanizatsiino-pravovi zasoby zabezpechennia informatsiinoi bezpeky [Information protection. Organizational and legal means of information security]. Available at: http://itman.at.ua/news/kuzmenko_b_v_chajkovska_o_a_zakhist_informaciji_navchalnij_posibnik_ch_1_organizacijno_pravovi_zasobi_zabezpechennja_informacijnoji/2011-03-25-5 (accessed 26.02.2021).

Lehominova, S.V. (2015). Teoretychni zasady informatsiinoi bezpeky pidpryiemstva [Theoretical principles of information security of the enterprise]. Ekonomika. Menedzhment. Biznes, 3(13), 87-92.

Melnyk, M.O. & Nikityn, H.D. & Mezentseva, K.O. (2017). Analiz pobudovy modeli polityky informatsiinoi bezpeky pidpryiemstva [Analysis of building an information security policy of the

enterprise]. Systemy obrobky informatsii, 2(148), 126-128.

Nashynets-Naumova, A.Iu. (2017). Informatsiina bezpeka: pytannia pravovoho rehuliuvannia: monohrafiia [Information security: issues of legal regulation: monograph]. Kyiv: Vydavnychyi dim «Helvetyka», 168 p.

Nashynets-Naumova, A.Iu. (2012). Pytannia zabezpechennia informatsiinoi bezpeky pidpryiemstva [Issues of information security of the enterprise]. Yurydychnyi visnyk, 3(24), 58-62.

Ostapov, S.E. & Yevseiev, S.P. & Korol, O.H. (2013). Tekhnolohii zakhystu informatsii: navchalnyi posibnyk [Information security technologies: a textbook]. Kharkiv: Vydavnytstvo KhNEU, 476 p.

Severyna, S.V. (2016). Informatsiina bezpeka ta metody zakhystu informatsii [Information security and methods of information protection]. Visnyk Zaporizkoho natsionalnoho universytetu, 1(29), 155-161.

Zakharchenko, M.V. & Kononovych, V.H. & Kildishev, V.I. & Holev, D.V. (2011). Informatsiina bezpeka informatsiino-komunikatsiinykh system. Kompleksy zasobiv zakhystu informatsii [Information security of information and communication systems. Complexes of means of information protection]. Odesa: ONAZ im. O.S. Popova, 168 p.