2020 International Conference on Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS) | 978-1-7281-8179-0/20/$31.00 ©2020 IEEE | DOI: 10.1109/ITQMIS51053.2020.9322884

# Information Security in the Management of Personnel in a Modern Organization

Elena A. Kirillova[1], Umar M. Yakhutlov, Xi Wenqi, Guo Huiting, Wang Suyu
Institute for Design-Technological Informatics RAS
Moscow, Russia
[1]kea-31@yandex.ru

***Abstract*—Social and managerial mechanisms in ensuring information security are one of the most relevant issues, both in theory and in practice. Therefore, the chosen research direction is timely and necessary in the period of rapid development of information and logistics technologies for enterprise management. Study of the basic and original approaches to information security and logistics services of companies in different industries, the analysis and systematization of the author's points of view on the issue of security in business objects (economic security of motor transport enterprises, security of the supply chain, international security) resulted, in our opinion, some solutions to the problems posed in the article title.Information security is defined as the degree to which information and its processing tools are protected, integrated, and available to the public.**

***Keywords—information security; personnel of a modern organization; security planning and control; information flows***

## I. INTRODUCTION

The problem of ensuring the security of information relations of personnel in a modern organization provides for the solution of a whole range of tasks. They relate to reforming and improving the legal regulation of information security entities, optimizing information networks and flows, ensuring the availability of public information resources, openness and transparency in the activities of public authorities, commercial and non-commercial structures, any organizations and individual employees.

The high speed of transformation and qualitative development of information systems of various classes of General and special purpose on the one hand revealed the urgent need to improve existing and use non - traditional innovative methods and technologies, and on the other-methods and means of protection against various types of threats, primarily unauthorized access to information. If we take into account that these processes are accompanied by intensive globalization of information networks used in the field of management, politics, science, business, Finance and credit, environmental protection, interethnic, cultural, religious communication, etc., then ensuring reliable protection of information flows is a necessary condition for the sustainable functioning of an economic entity [1].

## II. ENSURING EFFECTIVE INFORMATION SECURITY MANAGEMENT OF ALL SERVICES AND ACTIVITIES WITHIN THE PERSONNEL MANAGEMENT OF A MODERN ORGANIZATION

Methods of ensuring information security have the following directions:

1. Organizational and technological,

2. Legal,

3. Economic,

4. Social and managerial. One of the main directions is personnel control and training in the field of information security.

At the present stage of socio-economic development, there is an objective need to create a unified information space that provides timely, comprehensive information security, full-scale protection from computer terrorism and terrorism in General, socio-economic stability of economic entities of all types and forms of ownership, society as a whole and each individual from various threats and risky situations in market conditions. Therefore, it is interesting and socially and economically profitable to apply a logistics approach to solving the problems of improving the efficiency and security of the processes of functioning of information flows (IE) of an enterprise on the basis of micro - and macro-level personnel management.

Information security management is a process that ensures the confidentiality, integrity, and availability of an organization's assets, information, data, and services. Information security management is usually part of an Organizational approach to security Management that has a broader scope than the service provider and includes processing paper documents, access to buildings, phone calls, etc., for the entire organization [2].

The main goal of ISM is to ensure effective information security management of all services and activities within the service Management. Information security is designed to protect against violations of confidentiality, availability, and integrity of information, information systems, and communications.

1. Confidentiality - the state of information, in which access to it is carried out only by subjects who have the right to it.


978-1-7281-8179-0/20/$31.00 ©2020 IEEE

2. Integrity - the state of information in which there is no any change in it or the change is made only intentionally by subjects who have the right to it;

3. Accessibility - the state of information in which subjects who have access rights can implement it freely.

The goal of ensuring information security is achieved if:

1. Information is available when needed, and information systems are resistant to attacks, can avoid them, or recover quickly.

2. Information is only available to those who have the appropriate rights.

3. The information is correct, complete and protected from unauthorized modifications.

4. Exchange of information with partners and other organizations protected.

## III. Social and Managerial Processes in Ensuring the Effectiveness and Integrity of an Organization's Information Security

The organization determines what should be protected and how. At the same time, for the effectiveness and integrity of information security, it is necessary to consider all social and managerial processes from the beginning to the end, since a weak point can make the entire system vulnerable:

- develop, manage, distribute, and enforce information security Policies and other supporting policies that are relevant to information security. Information security policy is a policy that defines an organization's approach to information security management [4].
- understanding the agreed current and future business security requirements;
- use of security controls to implement information security Policies and manage risks related to access to information, systems, and services. The term "security control" is borrowed from the English language and in this context refers to a set of countermeasures and precautionary measures used to cancel, reduce and counter risks. In other words security control consists of proactive and reactive actions;
- documenting the list of safety controls, actions for their operation and management, as well as all risks associated with them;
- manage suppliers and contracts that require access to systems and services. It is performed in interaction with the supplier Management process;
- monitoring all security breaches and incidents related to systems and services;
- proactive improvement of security controls and reduction of information security risks;
- integration of information security aspects into all service Management processes.

The information security policy should include the following:

- implementation of information security Policy aspects;
- possible misuse of aspects of the information security Policy;
- access control policy;
- the policy of using passwords;
- e-mail policy;
- politics of the Internet;
- policy anti-virus protection;
- information classification policy;
- document classification policy;
- remote access policy;
- supplier access policy for services, information, and components;
- asset allocation policy. To ensure and support the information security Policy of the organization's personnel, you must create and use a set of security controls.

There are four stages. The first stage is the emergence of a threat. A threat is anything that can negatively affect or interrupt the personnel management process. An incident is an implemented threat. The incident is the starting point for the implementation of security controls in place. The incident results in damage. Security controls are also used to manage or eliminate risks. For each stage it is necessary to choose the appropriate information security measures:

1. preventive-security measures that prevent the occurrence of an information security incident. For example, the distribution of access rights.

2. recovery-security measures aimed at reducing potential damage in the event of an incident. For example, backup.

3. detecting-security measures aimed at detecting incidents. For example, antivirus protection or intrusion detection system.

4. suppressive-security measures that counteract attempts to implement threats, i.e. incidents. For example, an ATM takes a customer's card after a certain number of incorrect PIN code entries.

5. corrective-security measures aimed at recovery after an incident. For example, restoring backups, rolling back to a previous working state, and so on.

## IV. Key Performance Indicators of the Personnel Information Security Management Process

The following markers can be used as key performance indicators of the personnel information security Management process, for example:

1. protection of the organization and personnel from information security violations:

- percentage reduction of messages about "gaps" in the Service Desk;
- percentage reduction of negative impact on business from "gaps" and incidents;
- percentage increase in information security items in the SLA.

2. creating a clear and consistent information security policy that takes into account the needs of the organization and staff , that is, reducing the number of discrepancies between ISM processes and enterprise information security processes and policies.

3. security procedures that are justified, agreed and approved by the organization's management:

- increasing the consistency and suitability of security procedures;
- increased support from management.

4. improvement mechanisms:

- number of proposed improvements to controls and procedures;
- reduce the number of discrepancies detected during testing and audit.

5. information security is an integral part of ITSM services and processes, i.e. an increase in the number of services and processes that provide security measures.

## CONCLUSIONS

The science and practice of personnel management faces many difficulties and risks in ensuring information security [7] in practice, quite often the management and administration believe that only IT should deal with information security issues. Creating an effective information security system entails high costs, which should be clear to management, since it is they who make the decision on funding. At the same time, it is important to maintain a balance - ensuring information security should not cost more than the most protected information.

## REFERENCES


[1] Basics of logistics: Textbook / Edited By L. B. Mirotin and V. I. Sergeev, Moscow: INFRA-M, 2000, pp. 67-68.

[2] Stepanov E. A. personnel Management: Personnel in the information security system: Textbook / E. A. Stepanov. M.: FORUM: INFRA-M, 2002. - 288 p. - (Ser. "Professional education").

[3] Stepanov E. A. Information security and protection of information: Textbook / E. A. Stepanov, I. K. Korneev. M.: INFRA-M, 2001 .282 p.

[4] Sergeev V. I. Management in business logistics / V. I. Sergeev. M.: inform. - ed. FILIN house, 2007, 772 p.

[5] Christopher M. logistics and Supply Chain Management: Strategies for Reducing Costs and Improving Services. UK: Pitman Publishing, 1992.

[6] Moller C. Johansen.J. Paradigms in Logistics. Department of Production. University of Allborg, Denmark, 1993.

[7] Prasolov, V. I., Kashurnikov, S. N. (2016). Risk-oriented model of the concept of economic security. New science: Experience, tradition, innovation, 1-1, pp. 153-157.

[8] S. A. Sheptunov, M. V. Larionov, N. V. Suhanova, I. S. Kabak, and D. A. Alshynbaeva, "Optimization of the complex software reliability of control systems," 2016 IEEE Conference on Quality Management, Transport and Information Security, Information Technologies (IT&MQ&IS), Oct. 2016. doi:10.1109/itmqis.2016.7751955

[9] T. V. Karlova, S. A. Sheptunov, and N. M. Kuznetsova, "Automation of data defence processes in the corporation information systems," 2017 International Conference "Quality Management,Transport and Information Security, Information Technologies" (IT&QM&IS), Sep. 2017. doi:10.1109/itmqis.2017.8085797

[10] Y. M. Solomentsev, S. A. Sheptunov, T. V. Karlova, A. L. Barashkova, I. V. Vorobiev, A. N. Zapolskaya, R. S. Nakhuchev, U. M. Yakhutlov, and R. M. Glashev, "Popularization of science in online media: Theory and practice," 2016 IEEE Conference on Quality Management, Transport and Information Security, Information Technologies (IT&MQ&IS), Oct. 2016. doi:10.1109/itmqis.2016.7751960

[11] T. V. Karlova, E. A. Kirillova, A. Y. Bekmeshov, A. N. Zapolskaya, and I. A. Mikhaylov, "Analysis of Monitoring Data on the Criteria of Technogenic Safety in Project Activities," 2019 International Conference "Quality Management, Transport and Information Security, Information Technologies" (IT&QM&IS), Sep. 2019. doi:10.1109/itqmis.2019.8928381

[12] T. V. Karlova, A. Y. Bekmeshov, and N. M. Kuznetsova, "Protection the Data Banks in State Critical Information Infrastructure Organizations," 2019 International Conference "Quality Management, Transport and Information Security, Information Technologies" (IT&QM&IS), Sep. 2019. doi:10.1109/itqmis.2019.8928412

[13] A. Evstrapov, V. Kurochkin, D. Petrov, and S. Sheptunov, "Microfluidic Devices for Molecular Diagnostics in Medical and Biological Research," 2018 3rd Russian-Pacific Conference on Computer Technology and Applications (RPC), Aug. 2018. doi:10.1109/rpc.2018.8482169

[14] Inozemtsev, V. E., Kulikov, M. Y., Larionov, M. A., Krukovich, M. G., & Sheptunov, S. A. (2017). The conception of surface quality formation for metal detail's shaping through layered growing. In Proceedings of the 2017 International Conference "Quality Management, Transport and Information Security, Information Technologies", IT and QM and IS 2017 (pp. 730–733). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ITMQIS.2017.8085929

[15] Kolontarev, K. B., Pushkar, D. Y., Govorov, A. V., Sidorenkov, A. V., Osipova, T. A., & Sheptunov, S. A. (2017). Significance of the −2propsa index and the prostate health index in patients with prostate cancer: A literature review and data of the Russian prospective study. 2017 International Conference "Quality Management,Transport and Information Security, Information Technologies" (IT&QM&IS). doi:10.1109/itmqis.2017.8085839

[16] T. V. Karlova, E. A. Leonov, S. M. Roshchin, Y. M. Kazakov, A. V. Averchenkov, and D. V. Gritsev, "Analysis automation of the software user interfaces," 2017 International Conference "Quality Management,Transport and Information Security, Information Technologies" (IT&QM&IS), Sep. 2017. doi:10.1109/itmqis.2017.8085796

[17] Averchenkov, A. V., Averchenkova, E. E., Gorlenko, O. A., & Miroshnikov, V. V. (2017). Machine-building Enterprise Fuzzy Model as the Interrelated Factor Complex System. Journal of Physics: Conference Series, 803, 012009. doi:10.1088/1742-6596/803/1/012009