КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (20), 2023
ISSN 2663 - 4023

DOI 10.28925/2663-4023.2023.20.3544
UDC 005.95/.96:004.056

Kukharska Nataliia
Candidate of Physical and Mathematical Sciences, Associate Professor, Senior Lecturer in the Department of Information Technology Security
Lviv Polytechnic National University, Lviv, Ukraine
ORCID ID: 0000-0002-0896-8361
nataliia.p.kukharska@lpnu.ua

Lagun Andrii
Candidate of Technical Sciences, Associate Professor, Head of the Department of Information Systems and Technologies
Lviv Polytechnic National University, Lviv, Ukraine
ORCID ID: 0000-0001-7856-9174
andrii.e.lahun@lpnu.ua

HUMAN RESOURCES MANAGEMENT AS A COMPONENT OF ORGANIZATION INFORMATION SECURITY

Abstract. The cyber threat landscape has undergone major changes in recent years. Compared to any period since the beginning of the information age, it is more diverse and broad. First, the Covid-19 pandemic, namely the resulting transition of organizations to remote work and then the full-scale invasion of Ukraine by the Russian Federation, made adjustments to the information security strategy. Today, most organizations are aware of security threats and the need to create a reliable information security management system to ensure their effective operation in an information environment that is aggressive both technically and socially. An important area of information security in an organization is human resource management since, according to statistics from a number of reputable analytical centers, employees are the weakest link in any data security system. The organization's human resources management includes a thorough recruitment process, fostering a responsible attitude to work in compliance with the requirements for protecting restricted information, developing a corporate culture of information security and dismissal procedures.
The article provides a list of documents of the regulatory framework, namely, international security standards, regulatory documents of public authorities, and internal documents of an organization regulating the rules and methods of work with personnel. The main motives for the unlawful behavior of an internal attacker are highlighted, and the organizational measures recommended in the context of ensuring information security at all three stages of interaction between a person and an organization: employment, employment, and dismissal are described. There is also indicated the expediency of using psychoanalysis, psychology, management ethics and conflictology methods in the field of personnel management for forecasting and prevention of informational threats.

Keywords: personnel management; information; information security; human resource security.

INTRODUCTION

Recently, global cybersecurity has been facing an increasing number of threats. In 2020, in connection with the transition of enterprises to remote work mode due to the Covid-19 pandemic, cybercriminals took advantage of the vulnerabilities of misconfigured networks. According to research by AAG (a provider of IT support services), the number of malware attacks increased by 358% in 2020 compared to 2019. During 2021, the number of cyberattacks worldwide increased by 125% [1].

Russia's invasion of Ukraine has affected the cyber threat landscape. Since the beginning of the full-scale war, the number of Russian phishing attacks on electronic mailboxes of

European and American companies has increased 8 times. Also, in the first quarter of 2022, almost 3.6 million Russian Internet users were attacked, which is 11% more than in the fourth quarter of 2021 [1].

It is clear, that the rate and the average cost of data breaches have also increased. Since 2001, the number of data breach victims has increased from 6 victims per hour to 97, a 1517% increase in 20 years. In 2001, the average hourly cost of a data breach for individuals was $2054. Since then, the hourly loss rate has increased and in 2021, it already amounted to $787671 [1].

Problem formulation. According to the survey by AAG [1], 73% of small and medium-sized enterprises realize that for their effective activity in the conditions of a fairly aggressive information environment, both technically and socially, it is necessary to create a reliable system for ensuring of information security. It will prevent and counter various information threats. Although the term “information security” is defined in different ways, most companies focus on protecting information using software, hardware, and software-hardware solutions. However, as practice shows, such tools do not guarantee 100% protection, and all because the weakest link in the chain of ensuring the company's information security is the employee. He has access to confidential information and may intentionally or unintentionally violate its security (confidentiality, integrity, or availability). In 70% of cases (until an incident occurs), organizations do not suspect the existence of an internal threat, which makes difficult to prevent and respond to it [2]. Insider threats are difficult to detect and hard to protect information resources from, as insiders quite often have authorized access to the systems and data on which they direct their actions under their official duties. They can be stealing and leaking confidential data, sabotaging systems or networks, or simply abusing access to them to disrupt normal business operations. There is a high probability that insiders are familiar with the organization's security procedures and, therefore, can easily bypass them without arousing any suspicion.

Even a seemingly imperceptible violation of an organization's information security by an employee can lead to a large-scale data leak, which is extremely difficult to contain. And this can lead to the loss of customers, dissatisfaction among shareholders, and a decrease in share prices. In the worst-case scenario, which is not entirely excluded, the company will be forced to cease operations due to huge losses caused by the attack. As the 2022 Cost of Insider Threats: Global Report [3] reveals, insider threat incidents have risen 44% over the past two years, with costs per incident up more than a third to $15.38 million. The cost of credential theft to organizations increased 65% from $2.79 million in 2020 to $4.6 million in 2022.

Since about 82% of information security violations are committed by employees of the organization [1], an important area of IS provision is personnel management. It includes careful selection of candidates for employment; formation of employees by training them to have a responsible attitude to work in compliance with information protection requirements; education of a reliable and dedicated labor team; development of the corporate culture of information security; dismissal of employees.

Analysis of recent research and publications. A large number of works by such scientists as V. Bezbozhnyi, Z. Zhivko, I. Kernytskyi, O. Kyrychenko, G. Kozachenko, O. Lyashenko, I. Migus, V. Ortynskyi, Yu. Pogorelov, V. Sidak, V. Panchenko, N. Shvets, and others are devoted to the research of personnel security as a component of economic security [4]-[7].

The purpose of the article is to develop recommendations on personnel management in the context of ensuring the organization's information security.

RESEARCH RESULTS

Normative and legal basis of personnel management

Personnel management is carried out in compliance with the requirements of legislative and normative legal acts. In Ukraine, they include the following ones.

1. International safety standards:

- ISO/IEC 15408 “Information security, cybersecurity, and privacy protection. Evaluation criteria for IT security”;
- ISO/IEC 27001 “Information technology. Security techniques. Information security management systems. Requirements”;
- ISO/IEC 27002 “Information technology. Security techniques. Code of practice for information security controls”;
- ISO 31000 “Risk management. Principles and guidelines”.

2. Regulatory documents of state authorities:

- Constitution of Ukraine;
- Economic Code of Ukraine;
- Criminal Code of Ukraine;
- The Civil Code of Ukraine;
- Labor Code of Ukraine;
- Law of Ukraine “On State Secrets”;
- Law of Ukraine “On Information”;
- Law of Ukraine “On information protection in automated systems”;
- Law of Ukraine “On protection against unfair competition”.

3. Normative documents of internal regulation:

- charter;
- Regulations on structural subdivisions;
- job instructions for employees;
- employment contract;
- provisions on commercial secrecy;
- obligations to not disclose information that constitutes restricted access information;
- nomenclature of officials and employees who have access to commercial secrets;
- a list of information that is a commercial secret of the enterprise;
- internal work schedule of the enterprise;
- staff list;
- Regulations on personnel;
- Regulations on labor discipline;
- Regulations on official record keeping;
- Regulations on the conduct of official investigations.

International Standard ISO/IEC 27002:2013 “Information technology. Security techniques. Code of practice for information security controls” (clause 7) [8] regulates the rules and methods of working with personnel to ensure the confidentiality, integrity, and availability of information assets at the enterprise. This standard recommends applying organizational measures at all three stages of human interaction with the organization: hiring, employment, and dismissal. Their comprehensively ensure security related to personnel and to reduce the risk of theft, fraud, or misuse of information processing facilities.

The goal of working with employees during employment is to ensure that they understand their responsibilities and are capable of fulfilling their intended roles. The goal of working with employees during employment is to inform personnel about threats and problems related to information security, about the extent of their responsibility and obligations, as well as equip them with everything necessary to support the security policy of the organization, which reduces the risk of the human factor. The goal of working with employees during dismissal is to ensure that employees leave the organization or change positions in a way that does not affect the security of information assets in the enterprise.

Although the quality of personnel depends not only on the business and professional competencies of the organization's employees but also on moral qualities and psychological characteristics, the information security standards do not consider methods of their assessment.

Typology of insider motives

CISA defines an insider threat as the potential for an insider to use their authorized access or special understanding of an organization to harm that organization. This harm can include malicious, complacent, or unintentional acts that negatively affect the integrity, confidentiality, and availability of the organization, its data, personnel, facilities, and associated resources [9].

Personal characteristics of employees, which are undesirable from the point of view of information security, we considered earlier in [10]. Let's highlight the motives for the illegal behavior of an internal attacker:

- selfish interest (receiving material benefit);
- coercion by third parties;
- personal interest caused by family and other close relationships or certain obligations to third parties;
- revenge;
- self-affirmation;
- curiosity;
- game motive (thrill-seeking, adventurism);
- the distorted sense of justice;
- the desire to fulfill official duties at any cost;
- careerism;
- hooligan motives;
- envy;
- ideological considerations;
- enmity;
- the subject's desire to hide compromising facts (violations, information about himself or loved ones);
- dissatisfaction with various aspects of personal life or work relations;
- drug or alcohol addiction.

When you ask any businessman what qualities their dream partner, employee, or assistant possesses, competence, reliability, and decency are most often mentioned. The search for people capable of becoming the personnel core of the company is mainly focused on the selection and placement of personnel.

Pre-hire candidate screening

The use of the candidates screening procedure for a vacant position helps to make a balanced decision on hiring an employee. In particular, it allows to:

- make sure that the candidate for the position is sufficiently qualified;
- protect the company from hiring fraudsters, dishonest employees, etc.;
- prevent the leakage of important information, which is a commercial secret or know-how.

Each company has its own approved procedure for screening candidates for employment, which depends on the size of the company and the availability of the necessary specialists in the staff. It is correct if two divisions are engaged in this at once:

HR Department posts information about open vacancies, then collects feedback from candidates and primary information about them, conducts interviews, evaluates professional qualities, transfers data to the security department, forms a dossier on each applicant, and transmits information to the immediate supervisor, who makes the final hiring decision.

Security Service is engaged in checking the reliability of the data provided by the data collector, assessing the candidate's trustworthiness, and drawing up a psychological portrait. It can be both a full-fledged unit and one employee. If the company does not have this department, then the entire recruitment process falls on the recruiter. If there is no such employee either, the manager hires new people on his own.

How deeply and thoroughly a candidate should be vetted depends on the position he is applying for. The more responsibility a new employee will have in the company, the more thoroughly he will be vetted before a decision is made.

It is possible to single out the following stages of screening candidates before hiring, which are used in all large companies in Ukraine.

1. Creating a job description to understand who is needed in the company at a specific moment in its development.
2. Placing job announcements on various resources.
3. Accepting resumes from applicants, and filling out a standardized questionnaire for a certain position.
4. Selection of suitable candidates and the invitation to an interview. A short telephone interview is possible.
5. Interview with a recruiter. In some cases, a specialist who is competent in the field where the new person is needed is additionally invited to the so-called technical interview.
6. Testing for professional suitability, intellectual abilities, and personal qualities.
7. Verification of the authenticity of the provided documents. A visual assessment of the provided documents can be supplemented by inquiries into the relevant structures about their authenticity.
8. Request for additional information from the candidate or former places of work. You can contact the applicant's former manager and colleagues, clarifying the reason for dismissal and asking them to tell as much as possible about the person.
9. Request about the presence of criminal records, as well as about being registered in a psychiatric clinic or drug hospital.
10. Analysis of the received information.
11. Interview with the manager who makes the final hiring decision.
12. Job offer to the candidate. At this stage, the applicant can refuse to fill the vacancy, and then the recruiter needs to conduct the work again to find a new person

With each new stage, the number of candidates decreases. By the 7th or 8th stage, there are only a few applicants left who continue to be screened further.

In some cases, especially for managerial positions and those employees who will have access to material and technical assets or trade secrets, the security check does not end even after the hiring process. It can continue during the internship when all the decisions made by the person are recorded to obtain a complete portrait of him or her. Also is monitored person's behavior: compliance with the work schedule, and reaction to various events in the company.

The use of multi-stage technologies that involve the sequential use of several recruitment methods, both classical and non-traditional, can improve the quality of personnel selection [10].

The difficult economic conditions caused by the Covid-19 pandemic have forced managers to switch from the generally accepted model of office-based work to remote work, adapting the way they do business.

Today, despite the success of remote work and the challenge of replacing the best employees who left their organizations during the pandemic, many executives want their employees back in the office. At the same time, two-thirds (67%) of executives surveyed by A.Team and MassChallenge said that the traditional hiring process needs to be revised because it takes too long and is too expensive. 62% of executives state that it takes an average of 4 months to hire talented professionals [11].

73% of the surveyed executives have experience working with “mixed” teams consisting of full-time and part-time employees. 71% of executives are convinced that engaging freelancers or independent workers to work in an organization during a period of economic uncertainty is the right decision, as it gives the business more flexibility [11].

Security measures during the hiring process

Insider activity can be unintentional and intentional.

The most common channels of leakage are classified as unintentional disclosure of information and occur due to negligence, ignorance, or indiscipline of employees. Negligent insiders unwittingly, with absolutely no intention of harming the organization, can expose it to external threats. The threats they cause are often the result of their mistaken actions. For example, an employee may accidentally send a confidential email to the wrong person, or again by accident, leave a file on a shared network drive that is not intended for public viewing, falls for a phishing attack, or lose a work device with confidential information of the organization due to negligence. Other, no less damaging, threats can be caused by incorrect employee setup of databases, poor administrator credentials, and improper disposal of confidential company documents.

Intentional “information leakage” is much less common but in this case, information is “merged” purposely and with the most dangerous consequences for the organization.

To detect and identify potential intentional insider threats, you need to pay attention to employees who exhibit suspicious behavioral and digital activity. Such individual observations can be combined with the use of network monitoring tools.

There are several behavioral indicators, that signal the presence of insider threats, including:

- an employee, contractor, supplier, or partner expressing dissatisfaction;
- repeated attempts to bypass security;
- regular work of an employee outside of normal working hours;
- conflicts with colleagues or management;
- systematic violation of labor discipline;
- consideration of resignation and new opportunities related to it;
- and several digital indicators:
- an employee's access to resources that are not related to his or her job duties or to which access is prohibited;
- access to data that is not within the employee's area of competence;
- unauthorized use of corporate programs and access to the network at unusual times. For example, if an employee is found to be authorized to log on to the network at 3:00 a.m. without a management order, this is cause for concern;
- unusual spikes in network traffic may indicate that someone is trying to copy large amounts of data over the network;
- use of devices not authorized by the organization, such as USB drives;

- scanning the network and deliberately looking for confidential information;
- sending confidential information related to the organization's business by email.

Regular risk assessments of potential insider threats, including those related to potential internal threats, help identify vulnerabilities and address issues with access control policies, authentication protocols, user access privileges, and employee training programs.

Security measures related to the termination or change of employment conditions

When dismissing an employee who had access to confidential information, it is recommended to take the following measures:

- make a backup copy of the user's files;
- find out the reason for dismissal declared by the employee;
- try to find out the real reason for the employee's decision, analyze and decide whether to retain or dismiss him/her;
- find out about the employee's future place of work;
- determine the level of motivation and loyalty to the organization;
- determine the amount of confidential information known to the employee;
- organize the transfer of cases;
- Identify possible risks of confidential information disclosure and take measures to neutralize them;
- change access codes, computer passwords, and cryptographic protection keys that were known to the resigning employee;
- make sure that the employee surrenders the sources of confidential information he or she has;
- analyze the activities of the unit where the employee worked: whether there have been any recent cases of missing or lost documents with commercial information, samples of finished products, keys to offices and safes, or other confidential items;
- conduct a special briefing of the dismissed employee on the obligation and responsibility to keep confidential information secret after dismissal;
- identify those employees with whom the resigning employee maintained friendly relations. These employees should receive special training and be monitored, as they may leak information or take other negative actions against the organization;
- hold a conversation with the staff to explain the reasons for their colleague's dismissal;
- notify all employees of the organization, as well as partners, regular customers, and other persons with whom the employee cooperated, that the employee has been dismissed.

CONCLUSIONS AND FUTURE WORKS

Ensuring information security is a multifaceted problem and working with people is one of its most challenging areas. The article considers behavioral indicators, as well as describes digital indicators of internal threats, and provides recommendations for personnel management in the context of ensuring the information security of an organization. Prospects for further research on building an effective system of information security management of an organization are seen in the development of approaches to personnel management based on the application of psychoanalysis, psychology, and ethics of management and conflictology methods.

REFERENCES

1 The Latest 2023 Cyber Crime Statistics (updated February 2023). https://aag-it.com/the-latest-cyber-crime-statistics/.

2 The Reality of Insider Threats in Cybersecurity. https://www.threatintelligence.com/insider-threats.

3 2022 Cost of Insider Threats Global Report. https://protectera.com.au/wp-content/uploads/2022/03/The-Cost-of-Insider-Threats-2022-Global-Report.pdf.

4 Ortynskyi, V.L., Zhyvko, Z.B., Kernytskyi, I.S. (2009). Ekonomichna bezpeka pidpryiemstv, orhanizatsii ta ustanov [Economic security of enterprises, organizations and institutions]. Kyiv: Pravova yednist.

5 Liashenko, O.M., Pohorielov, Yu.S., Bezbozhnyi, V.L., Kozachenko, H.V. (2010). Systema ekonomichnoi bezpeky: derzhava, rehion, pidpryiemstvo [System of economic security: state, region, enterprise]. Luhansk: Elton-2.

6 Sidak, V.S., Mihus, I.P. (Ed.). (2012). Kadrova bezpeka subiektiv hospodarskoi diialnosti: menedzhment insaideramy [Personnel security of business entities: management by insiders]. Cherkasy: Maklaut.

7 Panchenko, V.A. (2018). Mistse kadrovoi bezpeky v systemi ekonomichnoi bezpeky pidpryiemstv [The place of personnel security in the system of economic security of enterprises]. *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Seriia: Mizhnarodni ekonomichni vidnosyny ta svitove hospodarstvo, 21*(2), 53-60.

8 ISO/IEC 27002:2013 Information technology. Security techniques. Code of practice for information security controls. Requirements. https://www.iso.org/stand-ard/54534.html.

9 Insider Threat Mitigation Guide.

10 https://www.cisa.gov/sites/default/files/publications/Insider%20Threat%20Mitigation%20Guide_Final_508.pdf.

11 Kukharska, N., Lagun, A. (2022). Personnel selection as information security controls. *Ukrainian Scientific Journal of Information Security, 28*(1), 21-25.

12 2022 Tech Work Report. https://assets.website-files.com/60aedfe8d838fc583e6d9cd7/6318e48c376c58335d410009_2022_TechWorkReport_090722-compressed.pdf.

Кухарська Наталія Павлівна
Кандидат фізико-математичних наук, доцент, доцент кафедри безпеки інформаційних технологій
Національний університет “Львівська політехніка”, м. Львів, Україна
ORCID ID: 0000-0002-0896-8361
nataliia.p.kukharska@lpnu.ua

Лагун Андрій Едуардович
Кандидат технічних наук, доцент, завідуючий кафедрою інформаційних систем і технологій
Національний університет “Львівська політехніка”, м. Львів, Україна
ORCID ID: 0000-0001-7856-9174
andrii.e.lahun@lpnu.ua

УПРАВЛІННЯ ЛЮДСЬКИМИ РЕСУРСАМИ ЯК СКЛАДОВА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЇ

Анотація. Ландшафт кіберзагроз в останні роки зазнав серйозних змін. У порівнянні з будь-яким періодом з початку інформаційної епохи він є більш різноманітним і широким. Спершу пандемія Covid-19, а саме зумовлений нею перехід організацій на віддалений режим роботи, а згодом повномасштабне вторгнення Російської Федерації в Україну внесли свої корективи у стратегію забезпечення інформаційної безпеки. Сьогодні більшість організацій мають усвідомлення безпекових загроз та необхідності створення надійної системи управління інформаційною безпекою для забезпечення ефективної їх діяльності в умовах агресивного як у технічному, так і в соціальному планах інформаційного середовища. Важливим напрямком забезпечення інформаційної безпеки в організації є управління людськими ресурсами, оскільки, як свідчать статистичні дані низки авторитетних аналітичних центрів, саме працівники є найбільш слабкою ланкою у будь-якій системі безпеки даних. Управління людськими ресурсами організації включає в себе процедуру ретельного відбору кандидатів на найм; формування у працівників відповідального ставлення до роботи з дотриманням вимог захисту інформації з обмеженим доступом; розвиток корпоративної культури інформаційної безпеки; а також процедуру звільнення працівників.

У статі подано перелік документів нормативно-правової бази, а саме: міжнародних стандартів безпеки, нормативних документів органів державної влади та внутрішніх документів організації, що регламентують правила і методи роботи з персоналом. Виділено основні мотиви протиправної поведінки внутрішнього зловмисника та описано рекомендовані у контексті забезпечення інформаційної безпеки організаційні заходи на всіх трьох стадіях взаємодії людини з організацією: працевлаштування, зайнятості та звільнення. А також вказано на доцільність застосування у сфері управління персоналом для прогнозування та запобігання інформаційним загрозам методів психоаналізу, психології, етики управління та конфліктології.

Ключові слова: управління персоналом; інформація; інформаційна безпека; безпека людських ресурсів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 The Latest 2023 Cyber Crime Statistics (updated February 2023). https://aag-it.com/the-latest-cyber-crime-statistics/.

2 The Reality of Insider Threats in Cybersecurity. https://www.threatintelligence.com/insider-threats.

3 2022 Cost of Insider Threats Global Report. https://protectera.com.au/wp-content/uploads/2022/03/The-Cost-of-Insider-Threats-2022-Global-Report.pdf.

4 Ортинський, В.Л., Керницький, І.С., Живко, З.Б. (2009). Економічна безпека підприємств, організацій та установ. Київ: Правова єдність.

5 Ляшенко, О.М., Погорєлов, Ю.С., Безбожний, В.Л., Козаченко, Г.В., ред. (2010). Система економічної безпеки: держава, регіон, підприємство. Луганськ: Елтон-2.

6 Сідак, В.С., Мігус, І.П., ред. (2012). Кадрова безпека суб’єктів господарської діяльності: менеджмент інсайдерами. Черкаси: Маклаут.

7 Панченко, В.А. (2018). Місце кадрової безпеки в системі економічної безпеки підприємств. *Науковий вісник Ужгородського національного університету. Серія: Міжнародні економічні відносини та світове господарство, 21*(2), 53-60.

8 ISO/IEC 27002:2013 Information technology. Security techniques. Code of practice for information security controls. Requirements. https://www.iso.org/stand-ard/54534.html.

9 Insider Threat Mitigation Guide.

10 https://www.cisa.gov/sites/default/files/publications/Insider%20Threat%20Mitigation%20Guide_Final_508.pdf.

11 Kukharska, N., Lagun, A. (2022). Personnel selection as information security controls. *Ukrainian Scientific Journal of Information Security*, *28*(1), 21-25.

12 2022 Tech Work Report. https://assets.website-files.com/60aedfe8d838fc583e6d9cd7/6318e48c376c58335d410009_2022_TechWorkReport_090722-compressed.pdf.