УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ/ INFORMATION SECURITY MANAGEMENT

DOI: 10.18372/2225-5036.28.16867

PERSONNEL SELECTION AS INFORMATION SECURITY CONTROLS

Nataliia Kukharska, Andrii Lagun

Lviv Polytechnic National University, Ukraine

KUKHARSKA Nataliia, Candidate of Physical and Mathematical Sciences, Associate Professor
Year and place of birth: 1971, Ternopil region, Terebovlya distric, Zhovtneve, Ukraine.
Education: Ivan Franko Lviv State University (from 1999 – Ivan Franko National University of Lviv), 1993.
Position: Senior Lecturer in the Department of Information Technology Security from 2021.
Scientific interests: Information Security Management, Cryptography, Steganography.
Publications: more than 130 scientific publications, including textbooks, scientific articles, conference abstracts.
E-mail: nataliia.p.kukharska@lpnu.ua.
ORCID ID: 0000-0002-0896-8361.

LAGUN Andrii, Candidate of Technical Sciences, Associate Professor
Year and place of birth: 1969, Lviv, Ukraine.
Education: Lviv Polytechnic Institute, 1993.
Position: Head of Department of Information Systems and Technologies from 2019.
Scientific interests: Information Security Management, Cryptography, Steganography, Information Theory.
Publications: more than 100 scientific publications, including textbooks, scientific articles, conference abstracts.
E-mail: andrii.e.lahun@lpnu.ua.
ORCID ID: 0000-0001-7856-9174.

Abstract. *The article deals with current issues of human resource security in the context of ensuring the organization's information security. The focus is on the procedure of selecting applicants for vacant positions since mistakes made at this stage of personnel management can negatively affect the efficiency of the organization. The list of personal characteristics of employees that are dangerous from the point of view of information security is laid out. Based on the conducted research, recommendations were given regarding the use of non-traditional methods of checking and evaluating candidates for employment, namely: analysis of the applicant's profile in social networks; brainteaser interview; a method based on the use of physiognomy, studying the language of gestures and the body; graphological method; socionic typing method. The verification methods chosen by the organization must comply with the current legislation on confidentiality, protection of personal identification data, and employment. All regulations, moral and ethical standards, business requirements, perceived risks and the organization's information classification scheme must be taken into account, too.*

Keywords: *information security, personnel, candidate for employment, information security management system, brainteaser interview, physiognomy, graphology, socionic typing, social network.*

Introduction

Personnel is one of the most important parts of an organization's activity as well as the most likely and difficult to control the source of security threats to the enterprise. In particular, in 2018-2020 years surveys of enterprise headers were conducted by the international consulting company PwC. According to them, a little less than half (47%) of organizations' financial losses cases had connections with the employees' actions. During this period, each organization experienced an average of 6 incidents of corporate fraud [1].

Analyzing the world experience, we can conclude that the risks in the personnel management system can cause not only financial losses but also reputational losses

of business entities. Of course, this leads to a significant reduction in the market value of the organization's assets and possibly to complete loss of it to owners.

The COVID-19 pandemic has made adjustments to the fight against corporate fraud. The deteriorating financial situation has forced many enterprises to revise their budgets, cutting costs to address security threats to staff. Additionally, the situation was complicated because of the transfer of workers under quarantine restrictions to remote work. Therefore, more than half of the various companies have abolished or simplified control procedures. At the same time, criminals, on the contrary, began to look more actively for additional ways to withdraw funds and assets from organizations.

Thus, in the current conditions of an unfavorable and unstable economic environment, ensuring the necessary personnel security remains a priority and dominant direction in the formation of corporate security of enterprises.

In research related to personnel security, employees of the organization can be considered from two sides. On the one hand, they are the target of threats from outside, for example, from criminal structures or competing companies. On the other hand, employees are the subjects of threats that can harm the organization by their actions (intentional or unintentional). In this case, the objects of a threat are material, intellectual, and information resources of the organization.

Analysis of existing studies

Considering the statistics of enterprises, we can conclude that the negative impact on the information resources of organizations in 80% of cases is caused by people involved in the exploitation of these resources. According to research by the Ponemon Institute in 2020, incidents of unauthorized access to data cost organizations with less than 500 employees an average of $ 7.68 million [2]. These data only indicate that personnel is underestimated as part of the information system by information security services.

It is worth noting that a significant problem in ensuring the information security of the company is the high level of probability of harm to property and non-property interests of the enterprise and the scale of losses in the event of threats caused by personnel.

The object of investigation in this work is the process of selecting personnel for vacant positions in the context of information security of the organization. For *the subject of the study*, we consider methods and approaches to assessing the personal characteristics of job candidates.

In this paper, we consider the essence of the personnel management process, its content, and its place in the information security management system of the company. *The aim* of the work is also to analyze methods of candidates' selection for employment, provide recommendations for their use, and ensure the required level of socio-technical information security.

To achieve the goal of the investigation, the following *main objectives* of the study are identified:

- improving the methods of verifying candidates for employment;
- bringing the company closer to the state of absolute safety and security using the developed methods;
- reducing the information security risks of the organization related to personnel.

The scientific novelty of the obtained research results has created a list of dangers from the point of view of information security personal characteristics of employees and are considered and analyzed non-traditional methods of checking and candidates' estimation for employment.

The practical significance of the research results is the ability to use our analysis of recruitment methods based on the actual situation in the company, namely economic, depending on the traditions, company culture, and position for which the candidate is selected. The organization can choose the methods of selection, the use of which suits it best in terms of obtaining results with the smallest loss of money and time. All selection methods are based primarily on the information security of the company.

The main materials for writing this work were the latest research by experts in the field of threats from personnel to the information security of the organization and the assessment of personnel vulnerabilities.

The main part of the study

In this case, we consider the company's personnel as a threat. The term "personnel" refers not only to employees who are in an employment relationship with the employer but also to applicants for vacant positions. It can also be former employees of the organization, who are obsessed with revenge due to resentment, and anger and may, after dismissal, take certain destabilizing actions against the organization. They can spread negative information about the company, thereby damaging its image, or disclosing confidential information for example.

To eliminate (or minimize) the company's possibility of a risk of leakage, loss, or distortion of information with limited access, it is necessary to build an information security management system. Requirements for its development, implementation, operation, monitoring, analysis, support, and improvement in the context of existing business risks of the company are presented in the international standard ISO/IEC 27001:2013 [3]. Along with measures to solve management problems with the help of technical means, the standard pays great attention to the development of information security policy, and legal requirements, ensuring the continuity of the production process, as well as work with personnel. The use of software and hardware protects information from internal intruders much lesser than organizational measures. Even when the perimeter of the controlled area of the enterprise is securely protected, employees of the organization, endowed with direct access to the information system to perform their duties, continue to be a source of threats to information security.

Rules and methods of information security management are regulated by the International Standard ISO/IEC 27002:2013 [4]. In particular, the seventh section of this standard deals with personnel safety issues. To ensure the confidentiality, integrity, and availability of the enterprise's information assets, the standard recommends applying organizational measures at all three stages of human interaction with the organization: before employment, during employment, and termination or change of employment conditions.

The quality of personnel largely determines the level of resistance and protection of the company from internal threats. The biographical data of all candidates should be carefully reviewed following applicable laws, regulations, and moral and ethical standards before employment, as well as business requirements, classification of information to be accessed, and perceived risks [3]-[4]. The implementation of these measures is necessary for the professional selection of personnel. This procedure is one of the key components in determining the strategy of personnel policy and security of the company.

The search and selection of employees should be approached comprehensively, taking into account all the features of a particular area of activity in compliance with the requirements of laws and regulations, which include:

- international safety standards ISO;
- regulatory documents of public authorities;
- normative documents of internal regulation.

The quality of personnel depends not only on the professional competencies of the company's employees, i.e. the ability to convert their knowledge, skills, and abilities into practice but also on personal and value characteristics. Methods of assessing such characteristics are not considered in information security standards.

Let's highlight the personal characteristics of employees that are undesirable in terms of information security: talkativeness; disability to keep secrets; increased emotionality, imbalance; desire to stand out at the expense of others (careerism, selfishness); love of things, affluent life; increased suggestibility; tendency to manipulation; increased mercantilism; excessive ambition; excessive self-confidence and tendency to overestimate their importance; disinterest in the results of work; excessive resentment, spiteful, vengeance; weakness; inattention.

Employers undoubtfully understand that every candidate for employment makes every effort to conceal biographical information or personal qualities that may compromise him during employer scrutiny. Therefore, there is a need to use special technological procedures: legitimate, semi-legitimate, and illegitimate beside the generally accepted methods of personnel selection.

Legitimate procedures include special testing techniques designed to identify hidden personal qualities, official inquiries to law enforcement, and the use of a polygraph.

With the help of polygraph inspections, are identified (evaluated) the following actions that may harm the work of the enterprise:

- distortion of biographical data and inaccuracy of the presented recommendations;
- reliability, loyalty to the company;
- true motives for employment; the presence of a drug and/or alcohol dependence;
- passion for gambling;
- information on past crimes and misdemeanors;
- availability of big debt obligations;
- links to criminal elements;
- presence of criminal or unfriendly intentions;
- the presence of mental or other chronic diseases.

However, the fact that there are several ways to cheat a polygraph should be taken into account. Those are the following:

- pharmacological (intentional or forced use of inhibitory or stimulant drugs, including large doses of coffee, energy drinks, etc.);
- mental (emotion management: meditation, attempts to bring consciousness into a trance; solving mathematical examples in the mind; complete relaxation, etc.);
- physical (conscious tension of one or more muscle groups, such as arm, leg, abdomen, buttocks; intentional pain by biting the tongue or cheeks, pressing nails into the body; breathing control);
- physiological (excessive physical activity; sleep deprivation, starvation, urinary incontinence);
- psychological method of counteraction (influence on the psychological state of the polygraph examiner).

In addition, polygraph screening is an expensive procedure that not every enterprise can afford.

Legitimate methods also include searching for information about a person by forming a search engine query by last name, first name, and patronymic of the potential applicant.

Semi-legitimate methods may include informal surveys of the candidates for employment relatives, acquaintances, or neighbors, and other means of gathering information that does not conflict with applicable law but may violate moral principles.

Recently, more and more recruitment specialists are resorting to screening potential candidates for employment through social networks. According to the Career Builder survey, 70% of employers use social recruitment in their practice, and this figure is only growing in a pandemic [5]. The profile information cannot be called relevant to the professional qualities of the candidate for employment. The issue of the moral right to use this information is also important. However, a personal web page can tell a lot about a person's life, interests, and moral principles. It allows you to understand whether the candidate is suitable for the company's corporate culture and values.

Let's consider the parameters that most often pay attention to recruiters when viewing the account of the candidate for employment on social networks.

List of groups, pages. Its analysis helps to form an idea of human interests, rhythm of life, level of conflict, as well as the desire to develop, including professionally.

Contents of the questionnaire, photo, and video material. According to the Work.ua survey, 26% of recruiters pay attention to photos in the candidate's profile, and 14% said that candid photos can be the reason for refusal of employment [6].

Publications, comments, and reposts. You can get an idea of the attitude to life of the candidate for the position, the adequacy of his behaviour, and his reaction to criticism thanks to them. Recruiters do not approve of publications of aggressive content and those that contradict the norms of current legislation or openly demonstrate political views. According to research by Work.ua, 33% of employers reject a candidate if he has extremist publications on the page [7]. According to Career Builder, 43% of HR professionals said they rejected candidates if they had negative statements about their former employer on the page. Attention is also paid to a person's literacy, especially if he or she is applying for a position that is related

to content creation. Candidates, who write about their professional activities, publish photos from conferences, and share news related to their profession make a positive impression.

Frequency of publications. It indicates the degree of involvement in the labor process. If a candidate constantly publishes comments or reposts every 10 minutes during working hours, it can be concluded that he is not very interested in the work.

Page privacy level. Different degrees of restriction for different categories of users indicate that the candidate is aware of the need to protect confidential information.

Viewing a candidate's social media is an auxiliary tool that should be in tandem with resume evaluation and interviews. Information obtained from social networks should not be a decisive factor in deciding whether to employ a candidate or not.

Illegitimate methods of collecting and verifying information include measures prohibited by current legislation. Among them are wiretapping, illegal intrusion into the property, and bribery of officials to obtain confidential information.

At present, along with the classic methods of personnel selection (analysis of resumes, biographical and competence interviews, testing), is growing the popularity of non-traditional methods. One of the newest and very interesting methods is Brainteaser interviews. This method tests the candidate's ability to think analytically, as well as identifies his creative potential. The questions addressed to the candidate may be unexpected and even strange, but they all have logical answers.

An example can be separating one counterfeit coin (heavier than the real ones) from nine identical coins for two weightings. It is possible to do. The candidate can find the right solution if he thinks a little. Some questions may not have the only correct answers, such as how many water polo balls can fit in the pool. You can give an approximate estimate in the case of counting the size of a water polo ball and the size of the pool by mathematical calculations. Of course, the answer is not correct, but you can determine whether the candidate has logical thinking.

Another method is to use physiognomy as sign language and body language. It is the science and art of recognizing the peculiarities of character, human inclinations by features and facial expressions, which is a kind of person's business card. Special attention is given to the ability to compose and interpret mutually reinforcing and compensating combinations of physiognomic features. In the United States photos (full-face and profile) of candidates for the vacant position are analyzed according to special physiognomic tables with 198 individual physical characteristics. 80% of applicants for the vacant position are eliminated based on the results of morphological analysis.

People can say one thing and think quite another, so understanding their true condition is very important. Psychologists found that about 60% of information about the interlocutor is shown by our facial expressions and body movements [8]. Other such information is obtained by paralanguage (intonation, tone of voice, pauses, manner of speaking). Thus, part of the direct content is very small. What is conveyed to the candidate verbally is what he considers necessary to say, and all non-verbal information is what is real.

In cases of information security research when working with personnel, it is important to know how long it takes a person to form an opinion about the interlocutor. Different sources say different numbers: from 40 seconds to 6 minutes. This time is not enough to objectively evaluate the candidate in terms of his professional experience, intellectual abilities, and attitude to work. But a person unconsciously tells about his temperament, strong-willed qualities, sociability, and leadership inclinations with the help of non-verbal communication signals. The attention of HR specialists to the language of gestures and movements grows in direct proportion to the level of the position for which the candidate is applying. During filling a position with a low level of responsibility, managers do not pay attention to the nuances; they prefer those who best meet the formal requirements. However, if they employ a person for the position of middle or senior level on enterprise, not to mention the "top" positions, in a big company body language is not ignored.

Another method used to determine the characteristics of candidates for employment is the graphological method. It is based on the study of the relationship between fine motor skills of the hand and the peculiarities of the psychophysical state of persons, their behavior, cognitive, mental, and physiological functions.

In Europe, Israel, and the United States, handwriting analysis is one of the most popular tools in the psychodiagnostic of personality. In France, for example, handwriting research is used as part of personnel policy in more than 70% of companies. Graphology makes it possible to determine a person's intellectual abilities, adaptability in the team, organization, and leadership qualities. Handwriting analysis reveals personal problems that may affect the honesty and reliability of the candidate for the vacant position.

The graphological method can also be used to determine the level of motivation, energy, efficiency, and resilience under stress. It is also worth noting the list of special competencies and qualities determined by graphological analysis, such as IQ, EQ, charisma, moral, material, intellectual, and social values, the composition of thinking, and barriers to excitability.

At the end of our investigation, we note the method of socionic typing. Socionics or information psychology is a non-academic field of psychology that studies the process of human perception of information about everything around him in everyday life. The relationship between people depends on how a person perceives information.

According to the socionic concept, the human psyche can be represented in the form of sixteen possible options for the perception and processing of information that corresponds to a certain type of information metabolism or society. By determining the type of candidates, the recruiter can determine if the job is right for candidates and if candidates will find a relationship with their future colleagues and superiors. Socionics consider not only the behavior of specific individuals but also their interaction in the team, the possibility of growth, and the development of both personal and professional qualities. This makes it

possible to ensure the optimal selection of personnel and their placement, taking into account the moral and psychological compatibility. It is possible to obtain more complete compliance of the employee with the position, as well as the opportunity to create a low-conflict and effective team thanks to the socionic method.

In general, the usage of physiognomy, graphology, or socionics is justified only if there is the extensive practical experience of the personnel selection specialist and his special responsibility in issuing recommendations. Any of these methods is more suitable as an auxiliary method in cases where there is a need to obtain additional information that cannot be obtained in traditional ways.

Conclusions

The permanent increase in the number of information security incidents due to the employees of the organization requires the improvement of methods of working with personnel, including before employment. Assessing the personal and value competencies of applicants for vacant positions can help solve the problem of the human factor in the information security of organizations.

Having considered and investigated non-traditional methods of assessing the personal qualities of candidates for employment, we concluded that there are no bad or good methods, but there are appropriate and inappropriate to the specific organization of the position and situation. Therefore, to form the most high-quality and flexible personnel system, each HR service must choose the tools and methods that meet the goals and interests of the company.

LITERATURE

[1] Fighting fraud: A never-ending battle. PwC's Global Economic Crime and Fraud Survey, 2020. URL: https://www.pwc.com/gx/en/forensics/gecs2020/pdf/global-economic-crime-and-fraud-survey-2020.pdf.

[2] 2020 Cost of Insider Threats Global Report. URL: https://www.exclusive-networks.com/uk/wp-content/uploads/sites/28/2020/12/UK-VR-Proofpoint-Report-2020-Cost-of-Insider-Threats.pdf.

[3] *ISO/IEC 27001:2013 Information technology. Security techniques. Information security management systems. Requirements*. URL: https: // www.iso.org / standard / 54534. html.

[4] *ISO/IEC 27002:2013 Information technology. Security techniques. Code of practice for information security controls. Requirements.* URL: https://www.iso.org/standard/54534.html.

[5] More than half of employers have found content on social media that caused them NOT to hire a candidate, according to a recent CareerBuilder survey. URL: https://www.prnewswire.com/news-releases / more-than - half-of-employers-have-found-content-on-social-media-that-caused-them-not-to-hire-a-candidate-according-to-recent-careerbuilder-survey-300694437.html.

[6] What HR is looking for on your social media? URL:https://www.work.ua/en/atiles/jobseeker/1754/?setlp =en.

[7] Weber J. Should companies monitor their employees' social media? / J. Weber // The wall street journal. URL: https://www.wsj.com/articles/should-companies-monitor-their-employees-social-media-1399648685?KEYWORDS=social+networks+HR.

[8] Butusevich A. Selecting staff: methods and typical errors / A. Butusevich // HR consultant, 2017, No. 23. URL: https://kadrhelp.com.ua/pidbyrayemo-personal-metody-i-typovi-pomylky.

УДК 331.108.37:004.056.5

Кухарська Н.П., Лагун А.Е. Відбір персоналу як захід інформаційної безпеки

Анотація. *У статті розглянуто актуальні питання безпеки людських ресурсів в контексті забезпечення інформаційної безпеки організації. Акцентовано увагу на процедурі відбору претендентів на вакантні посади, позаяк допущені на цьому етапі управління персоналом помилки можуть негативно вплинути на ефективність роботи організації. Визначено перелік небезпечних з погляду інформаційної безпеки особистісних характеристик працівників. На основі проведених досліджень надано рекомендації щодо застосування нетрадиційних методів перевірки та оцінювання кандидатів на найм, а саме: аналізу профілю претендента у соціальних мережах; Brainteaser-інтерв'ю; методу заснованого на використанні фізіогноміки, вивченні мови жестів та тіла; графологічного методу; методу соціонічного типування. Обрані організацією методи перевірки мають відповідати чинному законодавству щодо конфіденційності, захисту персональних ідентифікаційних даних та найму, мають враховувати усі нормативи і морально-етичні норми, а також бізнес-вимоги, усвідомлювані ризики і прийняту в організації схему класифікації інформації.*

Ключові слова*: інформаційна безпека, персонал, кандидат на найм, система управління інформаційною безпекою, Brainteaser-інтерв'ю, фізіогноміка, графологія, соціонічне типування, соціальна мережа.*

Кухарська Наталія Павлівна, к.ф.-м.н., доцент, доцент кафедри безпеки інформаційних технологій, Національний університет "Львівська політехніка".

Kukharska Nataliia, Candidate of Physical and Mathematical Sciences, Associate Professor, Senior Lecturer in the Department of Information Technology Security, Lviv Polytechnic National University.

Лагун Андрій Едуардович, к.т.н., доцент, завідуючий кафедрою інформаційних систем і технологій, Національний університет "Львівська політехніка".

Lagun Andrii, Candidate of Technical Sciences, Associate Professor, Head of Department of Information Systems and Technologies, Lviv Polytechnic National University.

Отримано *26 квітня 2022 року*, затверджено редколегією *21 вересня 2022 року*