UDC 004.415.2
DOI: 10.24025/2306-4412.3.2023.288836

A SYSTEMATIC APPROACH TO THE AUTOMATION OF THE PROCESSES OF ENSURING PERSONNEL COMPETENCE AT CRITICAL INFRASTRUCTURE FACILITIES OF THE DEFENSE FORCES OF UKRAINE

Sergii Chumachenko
Doctor of Technical Sciences, Senior Researcher
Head of the NGO Association of Civil Protection Specialists
https://orcid.org/0000-0002-8894-4262, e-mail: s.chumachenko@rnbo.gov.ua
Valerii Popel
Head of the Department of Scientific and Technical Expertise
State Research Institute of Cybersecurity Technologies and Information Protection
https://orcid.org/0000-0001-5544-3544, e-mail: v.popel@cip.gov.ua

Abstract. The publication is devoted to the problems of automation of the system of selection and assessment of personnel compliance, which should ensure the safety of critical infrastructure facilities of the Defense Forces of Ukraine. The article examines the main regulatory documents, requirements for personnel, and ways of assessing the appropriateness of their knowledge, skills, and competencies. The requirements of professional standards developed for the sphere of critical infrastructure of the Defense Forces of Ukraine and information protection are taken into account. This work aims to identify the basic problems associated with the selection of qualified personnel, assessment of their compliance and determination of the quality of work in activity processes. The materials of the article refer specifically to the objects of the critical infrastructure of the Defense Forces of Ukraine and consider the features related to the processes of ensuring the security of the critical infrastructure. The results obtained as a result of the analysis of personnel problems in the field of ensuring the security of critical infrastructure facilities should help the heads of institutions, organizations, enterprises, as well as HR units in the formation and staffing of units, training and placement of personnel. When preparing the publication, the main normative acts regulating the processes of critical infrastructure protection, the experience of developed countries, primarily the USA and the European Union, security standards (DSTU ISO/EN 27001, NIST Special Publication 800-181) and recommended practices were considered.

The conclusions contain recommendations regarding the automation of the system of selection, training and advanced training of personnel in the field of protection of critical infrastructure objects, as well as its information and cybersecurity. Recommendations are given for improving the automation of personnel selection and placement procedures, planning professional development, and creating a professional training system based on the knowledge management system.

Keywords: automation, management systems, critical infrastructure protection, personnel competence, information security standards, knowledge, skills, competencies, knowledge management.

Formulation of the problem

In the conditions of Russian military aggression, one of the primary tasks of the state is to ensure the protection of the critical infrastructure (CI) of the Defense Forces of Ukraine. The basic principles and principles of CI protection are determined by the Law of Ukraine "On Critical Infrastructure" (2021). In the context of the practical organization of protection, the

DOI: 10.24025/2306-4412.3.2023.288836

Law provides for the introduction of an automated security system of the CI of the Defense Forces of Ukraine. Its construction and provision of an adequate level of protection face problems that have a direct impact on both the state of system security and the resource needs, including financial ones, required for their solution. One of the most urgent and key in this sense is the problem of personnel competence, which ensures the protection and restoration of infrastructure facilities. It is on the level of competence and qualification of personnel that both the amount of resources and the response time to security incidents depend, which directly affects both the defense capability of the country and the quality of life of the population.

Protection of CI objects is a vital task in the conditions of military aggression for the Defense Forces of Ukraine (DF). The exceptional need to organize the protection of critical infrastructure is reflected in legislation (On Critical Infrastructure, 2021; On the Basic Principles, 2019; On Approval of General Requirements, 2019). At the moment, the characteristics of critical infrastructure objects (CICs), the procedure for their identification, accounting, unification into management sectors, and the procedure for managing each sector, including in the context of organizing the protection of the identified objects, have been determined.

Taking into account the legally established organizational uniting of the SOU OKI into a complex hierarchical structure, which has a state-appointed authority in the field of critical infrastructure protection (On Critical Infrastructure, 2021), we will consider the actual aspects of automating the system of training and improving the competence of personnel involved in ensuring the protection of both individual OKI and of the entire CIS as a whole.

Analysis of recent research and publications

Personnel management system, according to the classics of this field of research, activity and use (Armstrong, Barnard, Drucker, Karloff, Maslow, Mescon, Taylor, Follet, Fayol, etc.), consists of the following closely related and interdependent elements of technologies (Figure 1):

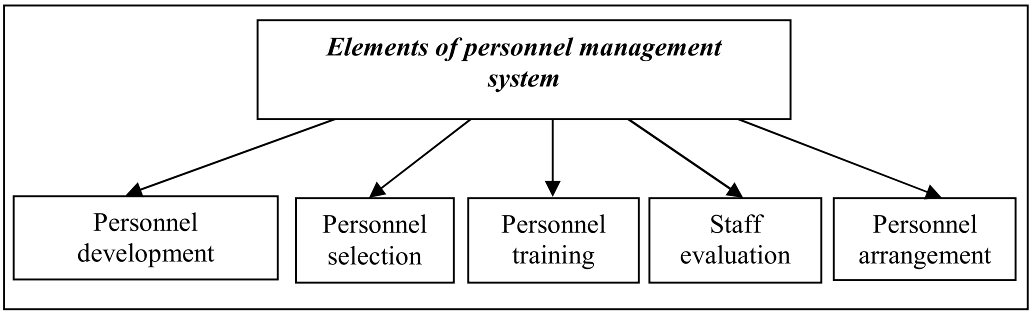


Figure 1. Component systems of personnel management

With, it is impossible to categorically separate the elements of the personnel management system from each other. They form a single whole, since it is impossible to carry out the selection, training and placement of personnel without personnel evaluation; personnel training without selection and evaluation; staffing without personnel selection, evaluation and training. Therefore, the main technology of personnel management is the assessment of personnel, which determines their quality, their suitability for the performance of relevant duties and tasks for the protection of KI SOU.

The concept of "human-centeredness" was first reflected in philosophical science, and later, with the development of the human resources management system, it was also spread in personnel management.

DOI: 10.24025/2306-4412.3.2023.288836

As noted by the President of the Academy of Pedagogical Sciences of Ukraine, Academician V.G. Kremen, "...the philosophy of human-centrism is not just another philosophical and anthropological teaching, but the transformation of philosophizing from humanistic considerations as such into a new type of metaphilosophy and worldviews directly related to the higher meanings of being, which act through life and living thinking. Turning to the problems of spirituality, morality and the unity of the inner world of a person, anthropocentrism, as a principle of holistic understanding of the person, corresponds to the search of modern socio-philosophical thought.

People-centeredness meets the requirements and demands of modern post-industrial civilization, which is looking for an experienced, creative, proactive and at the same time innovative thinking person" (Kremen, & Ilin, 2022).

For many years, the principle of people-centeredness has been at the center of the activities of personnel management bodies, personnel services, and personnel bodies of the armies of the leading countries of the world.

Qualitative selection of the personnel of SKI SOU should be decided with the help of methods that make it possible to determine the degree of suitability of this or that citizen to perform the duties of professional activity or the degree of his suitability for a new position for him. Determining the degree of suitability (conditional suitability, unsuitability) of a person (person) to perform military professional duties is possible only when using technologies of professional psychological selection for military service, for a new position (Vetrov, & Vraneshych, 2020).

The analysis of professional activity is carried out within the framework of professionography, on the basis of professional studies, the study of the content of each individual position (specialty) (Andreeva, 2005).

Strategic approaches to the use of personnel management technologies in the areas of personnel management and career management in the military organizations of NATO member states have been used since the beginning of the 20th century.

The system of promotion in the NATO armies has been developed over many years of application and the corresponding legal framework: in the USA (1947, 1981), Germany (1971), France (1976), Spain (1999), Hungary (2002) (The Army Strategic Planning Guidance, 2023; On Adopting the Regulations, 2001; Official bulletin of the French Armed Forces, 2009; On the Organization of Personnel, 1999).

The entire system of promotion of officers of the Armed Forces (AF) of the United States is built on the cultivation of the spirit of competition according to the principle: the higher the military rank and position, the stricter the selection criteria should be (Study of the problems, 2018). It mainly ensures fair selection in the officer corps. Terms of service in each military rank are strictly observed. It is believed that an officer cannot "sit" without advancing through the official ladder, and if the established terms are exceeded, he must be dismissed as unpromising. This is how, for example, they will do with a captain who has more than 16 years of service (4+two captain's terms of 6 years each), or a colonel with 30 years of service (25+5 years of the maximum colonel's term), who have no prospects for further promotion. Uniform minimum terms of military service (service) have been established for officers in all branches of the US Armed Forces to receive the next military rank: to receive the rank of 1st lieutenant - 2 years, captain - 4, major - 10 years, lieutenant colonel - 15 years, colonel - 22 years.

Many works of domestic scientists are devoted to the formation of a high-quality and professional management staff: G. Atamanchuk, N. Nyzhnyk, A. Obolonskyi, V. Oluyko, E. Okhotskyi, I. Surai, O. Turchynov, and others (Study of the problems, 2018). The first impetus and the greatest influence on the development of the direction of creation and ensuring the level of professionalism of the management units of the SKI contributed to the

DOI: 10.24025/2306-4412.3.2023.288836

works of the classics of management in general and personnel management in particular. The classics of this direction are M. Armstrong, M. Weber, A. Maslow, S. Taylor, E. Meskon, P. Drucker, and others.

During research in this direction, the first standards of professional service were created, which were based on the "system of merits and merits", which, in turn, required the determination and approval of accounting for the necessary business and personal qualities when appointing and promoting to managerial positions of any level of SKI, regardless of race, skin color, religion, gender, marital status, age. The main criteria were the greatest competence, high moral and ethical standards.

The personnel services of the NATO member states determine that the selection of a candidate for the position of SKI SOU should be:

objective and based on the evaluation of the merits (achievements) of each candidate;

competitive, but to be carried out according to processes and indicators that should be understandable to any serviceman - soldier, sergeant or officer;

evaluation of the candidate is a key part of the selection both for the members of the selection commissions and for the officers who carry out the initial selection of candidates in units (compounds);

the selection must take into account issues related to the individual, personal preferences of the candidate for the nature of the type of activity of the appointment, assignment of a military rank, referral to training and training (On Approval of the List of Works, 1994; Andreeva, 2005; Obolonsky, 2001; Krill, 2018).

The purpose of the article is a scientific justification for the use of modern information technologies for the automation of the personnel training system for the protection of the OSI, as an integral organic addition to the basic toolkit of the automated security management system of the OSI.

Presenting main material

The requirements for the organizational support of OKI are determined, including, by Resolution of the CMU dated June 19, 2019 No. 518 "On approval of General requirements for cyber protection of critical infrastructure objects" (p. 2). The requirements provide for both the creation of appropriate units and the inclusion of specialists in them, who must perform actions to ensure the safety of OKI SOU. At the same time, at the level of the object itself, it is quite difficult to find both the necessary personnel and to determine the degree of their compliance and readiness to perform the relevant job duties.

When carrying out work on the selection and training of personnel, it is important to clearly understand what knowledge, skills and competencies a specialist should possess. The content of such training stems from the concept of CI protection, which is largely borrowed from the experience of developed countries that have gone a long way in creating a CI protection system and have stable experience. The general approach in the organization of the protection of CSI is that the protection of CSI is based on the management system, and, accordingly, on the information infrastructure, as the basis of the functioning of any management system. Therefore, the main practice of protection is based on the DSTU standard ISO/EN 27001 (Information Security, 2022), which defines the requirements for the information security management system. This standard is based, in turn, on DSTU ISO/EN 9001, and is essentially a quality system, the implementation of which allows to ensure the protection of information in the organization. According to the concept of the standard, information that is determined by the organization as valuable, as well as information that needs to be protected by the law, is subject to protection. Thus, the requirements of the standard regarding information affect all business processes and aspects of the organization's

DOI: 10.24025/2306-4412.3.2023.288836

activities, organization management, internal and external interactions, technologies and personnel. Personnel requirements are defined in section 7 of the standard, and define the organization's responsibility for ensuring that personnel are competent, have the appropriate education, training or experience.

In (Information Security, 2022), a comparative analysis with standards and methods in working with personnel in the field of CI security of other countries is given, and best practices are considered. The requirements of the standards are taken into account, including DSTU ISO/EN 27001 "Information Security, Cyber Security and Privacy Protection - Information Security Management Systems - Requirements" (2022), NIST Special Publication 800-181 "Workforce Framework for Cybersecurity (NICE Framework)" (n.d.).

In particular, it is possible to highlight some important competencies, knowledge and skills:

- personnel must be competent in identifying potential CI threats and be able to prevent them. This may include studying methods of cyber protection, physical security and other aspects of the security of OKI SOU;
- personnel must be trained to respond to a variety of incidents, such as natural disasters, man-made accidents, or cyber attacks. It is important to be able to quickly and effectively respond to danger and ensure the safety of personnel and OKI SOU;
- competent personnel must know how to ensure the uninterrupted operation of the OKI SOU in the event of a crisis or incident. This may include working with backup power sources, water supply, security systems, information technology, etc.;
- staff must understand and comply with the laws and regulations related to the safety of OKI SOU. Failure to comply with legal requirements may result in serious legal consequences;
- threats and technologies are constantly changing, so personnel must be ready to learn and constantly update their knowledge and skills, both in the field of security and in the field of other functionality.

All these aspects, requirements, areas of competence are aimed at forming the ability of personnel to ensure the reliable and safe work of OKI SOU and protect them from possible threats.

Proper training of personnel, which must ensure the protection of critical infrastructure, requires the creation of an appropriate concept. Such a concept should provide a certain unification, in particular, in terms of the subject area - ensuring the safety of the OKI SOU, in terms of the requirements for a specialist - the application of professional standards, in terms of the procedure - to apply typical methods and procedures at the level of the corporation - SKI.

In order to apply the best practices in the field of SCI protection, it is necessary to take into account the complexity of the problem, requirements for applicability, flexibility and level of generalization of methods, limitations in resources, especially in time. To the greatest extent, when forming a system of working with personnel, the task of organizing CI protection is met by the concept of knowledge management (Malikhin, & Yarmolchuk, 2020, pp. 1-3), since it has the ability to compensate for resource limitations by more active application of the intellectual component. This concept is based on the definition of knowledge as a value and an asset, as well as taking into account in this asset the practical skills, abilities, etc., that individual specialists of OKI SOU have. According to the concept, knowledge is an important element of SKI resources, and the management of these resources will provide additional opportunities when organizing actions in extreme conditions of accidents, aggressor terrorism, attacks and liquidation of the consequences of SOU OKI.

Application of the concept does not require the creation of new functions or changes in business processes. It is seen that this concept operates at the level of understanding by the

DOI: 10.24025/2306-4412.3.2023.288836

heads (managers) of the organization of the main principles of the concept and the application of these principles in the conduct of usual activities. These include:

1. Creating a knowledge base. The procedure of creating knowledge is largely based on the identification of knowledge, the selection of useful knowledge, the creation of a knowledge base and the delivery of this knowledge to the members of the team to whom this knowledge applies. For this, the search and implementation of processes that contribute to the creation of new knowledge can be carried out. This may include stimulating working groups to share ideas, holding briefings and trainings to build a knowledge base.

2. Identification and documentation of knowledge. In order to ensure the possibility of taking knowledge into account, applying and managing it, it is necessary to define knowledge, if possible document it - describe it, add it to the knowledge base and connect it with processes and specialists. It is advisable to involve the entire team of OKI SOU in this process. To ensure motivation on the part of specialists, it is advisable to introduce incentives for employees to share their knowledge and experience. Documenting knowledge is an important element of the concept, as knowledge that is not documented is easily lost. Various tools, instructions, knowledge base procedures can be used for the purpose of documentation. In the existing version, it can be maintaining a database or an internal portal for storing and distributing information for OKI SOU.

3. Dissemination and transfer of knowledge. The organization must develop an automated training system that takes into account and applies the principles of the concept of knowledge management. Such a system can include the creation of a training and development program that helps employees acquire new knowledge and skills, foresee the use of effective training methods, such as trainings, webinars, online courses and mentoring.

4. Knowledge, as a valuable asset, should be available to those members of the OKI SOU team who can use it. This requires shared access to information. This access can be organized by creating centralized information systems for accessing and sharing information between employees, using secure networks or special software for sharing access to resources.

5. The key element of implementing the concept of knowledge management is providing motivation for joint learning. The motive can be both material and moral encouragement, a correctly built career model, participation in the results of the SKI activity. Creation of motivational systems and rewards for those who actively share knowledge and teach others, encouragement of collective learning and exchange of experience should be ensured.

6. Knowledge, as a valuable asset, must be protected. Knowledge protection can be ensured by implementing confidentiality and protection of valuable information, developing policies to restrict access to certain types of knowledge, introducing relations in the organization that include the element of knowledge protection in the corporate culture of OKI.

7. Knowledge management, as a process, requires control and analysis. For this purpose, it is possible to introduce monitoring and evaluation of the results of knowledge base management, including measuring the impact of the implemented measures on the productivity and results of OKI SOU.

8. The culture of relationships in the team of OKI SOU (corporate culture) is an element of the automated management system (including knowledge base management) and is largely the result of the implementation of the knowledge management concept. Corporate culture will strengthen the organization's potential if it is based on openness and cooperation. The management of OKI SOU should encourage the spread of a culture in which employees feel that their opinions and ideas are important and their contributions are valued. This creates a favorable environment for the exchange of ideas and free communication.

Knowledge management in the field of information security and AI protection can face a number of problems and challenges. These include the rapid change in technologies and threats, as the security field is constantly evolving, and new technologies and threats to OSI

DOI: 10.24025/2306-4412.3.2023.288836

are emerging very quickly. This makes it difficult to constantly update the knowledge of the staff and train them in new methods of information protection, but at the same time it increases the importance of the very task of security of OKI SOU. Some staff members may not fully understand security threats or consider them to be serious. Such a situation may lead to insufficient compliance with security policies and rules for the use of information.

Insufficient funding for training and development of personnel in the field of security of OKI SOU leads to a systematic limitation of access to resources and training programs. Insufficient communication, insufficient exchange of information and knowledge between different parts of the organization can cause underestimation of threats and loss of opportunities for timely response to incidents of OKI SOU. Lack of clear and efficient automated knowledge management processes can lead to confusion and wasted time. Different SOU OKIs have different corporate cultures and structures, in organizations with a higher level of hierarchy, it is usually more difficult to implement knowledge base management initiatives that require an open exchange of information. Table 1 shows examples of the application of the concept of knowledge management at the level of the organization's development strategy.

Table 1. Application of the knowledge management system in the organization

Company	**Implemented knowledge management system (KMS)**	**Implementation results**
Microsoft	Own knowledge management solutions such as SharePoint and Microsoft Teams	These tools help teams work together on projects, share knowledge and documents, which increases work productivity
Siemens	A knowledge management system has been implemented, which covers knowledge sharing, employee training and collaboration between different departments	The organization increased innovativeness and ensured the efficiency of new product development. The system facilitates quick search and exchange of knowledge, improves communication and cooperation between departments and various business units of the company
IBM	IBM uses an advanced KM strategy to support its global teams, including forums, virtual communities and e-learning systems	This allows the company to quickly adapt to market changes, effectively manage projects and improve the qualifications of employees
Daimler AG	Developed a specialized platform for sharing knowledge and best practices between in-house engineers and third-party developers	More effective use of innovative technologies and solutions in various projects and company products is ensured
Novo Nordisk (Denmark)	Novo Nordisk actively invests in training and development programs for its employees, including internal academies and training centers	Professional development and development of employees' skills takes place, which has a positive effect on the company's productivity and innovation
Santander Bank (Spain)	The bank uses analytics and intelligent data analysis tools to better collect and process information about customers, products and market trends	Increasing efficiency in decision-making, improving the quality of customer service and optimizing the bank's internal processes
ABB (Switzerland)	ABB implements knowledge management solutions to integrate different databases, design systems and engineering tools to facilitate collaboration between specialists	More effective coordination of projects, reduction of time for development of new products and improvement of the quality of solutions

DOI: 10.24025/2306-4412.3.2023.288836

Leading international companies are actively implementing knowledge management strategies to increase efficiency, promote innovation, strengthen communications and improve decision-making processes. In each case, the strategies are adapted to specific business processes and the company's corporate culture, which ensures the maximum benefit from their implementation.

From the analysis of the materials in Table 1, it follows that knowledge management is the process of creating, distributing, using and storing knowledge in the organization in order to increase its capacity in all aspects of activity. The analysis shows that modern knowledge management systems are usually based on the use of automated information systems that are integrated into the organization's business processes. Successful implementation of the knowledge management strategy in the organization requires a systematic approach, management support and active participation of all employees. A correctly chosen and implemented knowledge management strategy is a powerful tool for increasing efficiency and achieving the strategic goal of OKI SOU.

Compliance monitoring and assessment systems should be implemented for all CAIs in the system. Methodical and educational materials should also be developed, as well as support measures should be implemented, under which a training system will emerge and be able to function, which will ensure the training of various specialists in a single paradigm of SKI.

The totality of these measures forms a system of personnel training in general for the CI protection system. At the moment, the system that is successfully operating in the USA belongs to the most developed systems for the protection of critical infrastructure. Its detailed description can be found in the document "National Infrastructure Protection Plan (NIPP)" (2013) on the website of the specialized government organization CISA (an agency within the structure of the US Department of Homeland Security responsible for the protection of critical infrastructure). The NIPP is a document that defines strategic goals, priorities and approaches to protect critical infrastructure such as energy systems, transport, communications and other critical sectors from various threats, including cyber attacks, natural disasters and acts of terrorism. The plan includes a description of the structure of governance and cooperation between the public and private sectors, as well as defines methods of risk analysis and measures to reduce them. It is regularly updated to take into account current threats and technological changes. It also defines the basic requirements for personnel involved in the performance of critical infrastructure protection tasks.

The advantage of the US critical infrastructure protection model is also that a series of national standards and frameworks (NIST, FISMA and others) have been developed for it, which contain a sufficient set of requirements and practices to cover most elements of CI protection.

It is possible to highlight the following features of this system:

1. The requirements for qualifications, knowledge and skills of specialists are based on the NIST standard 800-181 "Workforce Framework for Cybersecurity (NICE Framework)" (n.d.).
2. The specialties for which professional standards are developed in accordance with the general requirements of the standard are defined.
3. Separate functions are allocated for specialties, for which specialized training courses can be created, training and knowledge testing for which are implemented on automated training and testing systems.
4. Assessment centers are used to assess the suitability of specialists, and assessments of both the state and some non-state training centers (such as Cisco, Microsoft and some others) are valid.

DOI: 10.24025/2306-4412.3.2023.288836

Ukraine is currently implementing approximately the same model. NIST standards are recommended for use by the authorized body. Based on the NICE Framework standard, six professional standards have been developed and another fifteen professional standards are being prepared. A specialized Qualification Center was created and accredited, the task of which is to determine the compliance of qualifications with the requirements of professional standards in the field of information security. Measures are being taken to implement other important elements of the personnel training and evaluation system for the field of CI protection. It is possible to use automation tools in the training system itself. There are many training and testing systems for face-to-face and distance learning. Such systems function in most educational institutions, so there is no need to provide a detailed description of the example.

The main component of such an automated system is the training courses that they offer to the staff of OKI SOU. Such training courses should provide knowledge and skills that meet the qualification requirements of professional standards. The division of the profession into modules, each of which corresponds to a certain production function, will allow the formation of a flexible system of professional development, which can consist of 1-2 annual plans, according to which specialists will have the opportunity to obtain the necessary knowledge in full without a significant break from production.

Such centers can have a centralized knowledge base on methodical materials, accumulate exam materials, be connected to a network, contain monitoring elements and process training statistics, forming objective data on the state of professional readiness of the personnel of the entire segment of SKI.

Software can ensure the implementation of modern approaches to learning, include practice on simulation simulators, provide elements of the knowledge management system.

To improve productivity and automate personnel processes, primarily related to monitoring and selection, selection and promotion of OKI SOU personnel, hundreds of software and analytical platforms have been created on them.

Structurally, a typical training and testing center consists of the following blocks: a training and testing system and a training and testing class. The training and testing system is connected to an external network with network protection through a router. The central element of the training and testing system includes: a network management system, a software and technical system of training and testing, a video surveillance system for the testing process. The training and testing class has separate workplaces for methodologists and examiners, as well as for persons undergoing testing under video surveillance.

The basis of such software is business intelligence (BI) analytical systems, which are defined as computer methods and tools for organizations that provide the translation of transactional business information into a form accessible to users, suitable for business analysis, as well as tools for mass work with such processed information (Prokopenko *et al.*, 2020).

Leading positions in software development in this field belong to well-known leading companies: SAP, ORACLE, ADP, IBM. Also recently, a large number of new companies have been involved in this process.

The latest trends in the development of special analytical software for Business intelligence are the use of advanced information technologies based on cloud computing, which provides advantages in their use on various types of workstations and mobile devices.

In addition to the main list of functions for processing a large array of data (Big Data), some software and analytical applications may include the following opportunities for innovation:

DOI: 10.24025/2306-4412.3.2023.288836

1. Testing and assessment of personnel competence - intended for preliminary assessment of knowledge, abilities, skills, acquired qualifications of applicants for the position in order to select the best of them. The most popular software, which is in demand among many global companies in this field, is software and analytical platforms and services:

HackerRank - a platform for evaluating the competencies of labor resources by recruiting organizations for the selection and hiring of employees with the necessary qualities;

Pymetrics - a service that uses unbiased algorithms to find suitable candidates using gamified neurobiological tests. The service is on the market relatively recently, but has already proven itself well;

Self Management Group - human resource management software and analytics with integrated diagnostics and assessments to attract, manage and evaluate candidates.

2. Use of artificial intelligence. Use of artificial intelligence (AI) technologies in automated business analytical processes. The best services include:

Ideal - uses AI technologies to select candidates, analyzing complex information about them: resumes, evaluations and data on their performance;

Textio - a global system for the unification according to a single standard of the text data of published resumes of candidates, written according to different presentation and structure, and automatic correction of possible grammatical and syntactic errors in the text. The main feature offered by the system is the ability to detect patterns in language, helping personnel agencies to better select candidates.

3. Use of Applicant Tracking Systems (ATS) - candidate tracking system:

Bullhorn - a specialized analytical application designed for searching and selecting candidates;

SAP SuccessFactors - special software and information and analytical support for human resources management. The system uses technologies based on talent management methodology;

iCIMS - a complex of software for optimizing the work of personnel managers involved in the processes of personnel recruitment, promotion and career management;

Oracle Taleo Cloud Service - special software and information and analytical support for searching, recruiting, promotion and retention of qualified specialists with the help of a multifunctional software package;

Workday - a software system that combines accounting, personnel management and planning in a single cloud ERP system to improve business efficiency;

SmartRecruiters - special software and information and analytical support, which, due to the use of AI and social networks, allows personnel managers to effectively search for candidates and select qualified specialists in any part of the world.

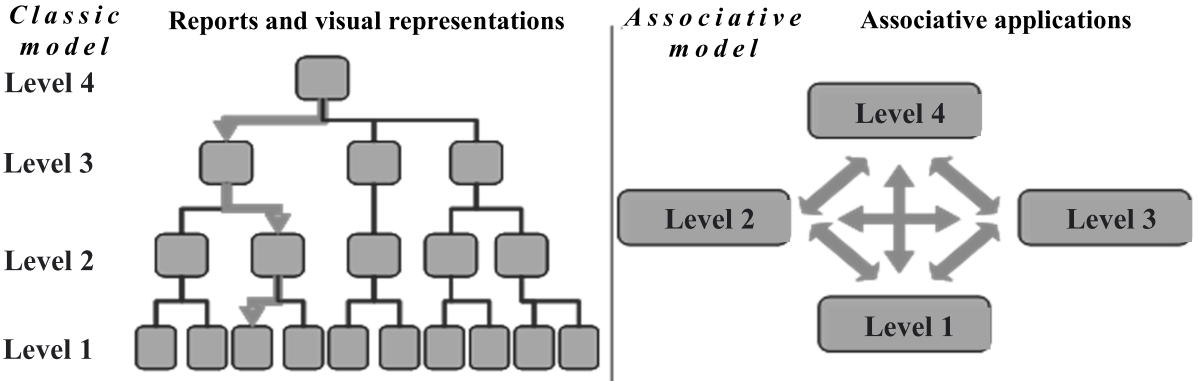
In addition to BI-systems narrowly directed in the field of personnel management, there are universal systems, the capabilities of which allow conducting Big Data analysis in any field of activity. The most powerful business intelligence tools, according to the Gartner publication for 2020 and previous years, include the software products of Tableau, Qlik and Power BI companies.

Their main difference from ready-made BI solutions is slightly different approaches to the order of data processing, as well as their adaptability to any organizational requirements regarding the construction and implementation of dashboards at automated workplaces.

Information panels is an integral part of a BI system designed to visualize a large array of information that is analyzed in the form of graphs, charts and other forms of displaying quantitative information, which, in turn, simplifies awareness and helps management assess the real state of affairs and make an informed decision.

DOI: 10.24025/2306-4412.3.2023.288836

The use of in-memory processing technology (conducting analysis and calculations in RAM) and Business Discovery (business research module) in Qlik software products is quite functional, which allows analyzing business information at any level, avoiding time-consuming and expensive work from the construction of repositories and multidimensional OLAP cubes. Any calculations of the Qlik BI system are performed instantly even with very large volumes of information when a large number of users work simultaneously, which significantly increases work efficiency. Algorithms for building analytical models, their advantages and disadvantages are shown in Figure 2.



– linear, determined by the algorithm
– limited choice of the following actions, which complicates understanding
– depends on the developer
– data storage/ hardware and software complex

– the user decides where to start and where to end
– all data is always available
– knowledge-oriented
– processing in RAM and working with Big Data

Figure 2. Algorithms for building analytical models

The associative architecture of the model will allow managing the relationships between data not at the application level, but at the level of the platform's internal mechanisms. The software in which this is implemented stores separate data tables and associative relationships between them in RAM, where each value of each field is related to all other values of the associative model. When creating new samples, the user sees: how the data is related to his request, data that is not included in the sample. This allows the user to work as comfortably as possible, answering new questions independently without the help of information technology specialists (Study of the problems, 2018).

The Qlik Business Discovery service allows you to analyze information in different information sections (by update time) and regardless of the automated personnel management systems in which this information is stored, to quickly deploy and scale even when using a large number of data sources, it includes joint analytics tools in real time.

Special attention during the construction of BI-systems is paid to their implementation. The main idea of this stage is that the implementation of the system should not take place at the final stage of its creation, but should be carried out in parallel from the very beginning of the creation of the system. The world's leading software developers are recommended to start development with a simple version, quickly put it into practice, and gradually improve and expand the automated system based on the experience gained from the interaction between the user, the system and the one who designs it.

DOI: 10.24025/2306-4412.3.2023.288836

So, for many organizations in the world of use BI-systems for processing large data sets (Big Data), designed for effective personnel management, especially aimed at finding, selecting and retaining qualified specialists, are increasingly becoming the norm every year, without which it is impossible to run an effective business to obtain maximum profits.

The use of special software and analytical support in the activities of personnel services of the OKI Secondary School at all levels of management of the organizational hierarchy will allow solving a number of problematic issues related to the acceleration of the pace of professionalization of the Defense Forces of Ukraine, improving the quality of staffing, transparency, objectivity and justification of personnel decisions of the OKI Secondary School, qualitative selection and promotion of the best candidates for key positions.

Based on the results of the assessment and determination of the required number of candidates for the Reserve for the respective positions, a rating is compiled (by majors, specializations, positions, ranks). Rating - a list of candidates compiled based on the results of the competitive selection based on the quantitative indicator of the points scored by them according to the principle of higher score to lower.

When compiling the rating, it is necessary to take into account:

N-th number of parameters (indicators, evaluation criteria);

the weight of each parameter and its possible influence on the overall result;

the number of members (number of votes) participating in the compilation of the rating;

the weight of each vote depending on the status of the member of the commission (chairman, expert in a given field, specialist of the highest category in the field of activity, boss, colleague, subordinate).

In theory, the rating is the lower bound of the Wilson confidence interval for the Bernoulli parameter, which can be determined by the formula:

$$\left(\hat{p}+\frac{z_{a/2}^{2}}{2n}\pm z_{a/2}\sqrt{\left[\hat{p}(1-\hat{p})+z_{a/2}^{2}/4n\right]/n}\right)/\left(1+z_{a/2}^{2}/n\right)$$

where: p is the share of positive evaluations; z – quantile of the standard normal distribution (an indicator characterizing the distribution of a random variable relative to the median); n is the total number of assessments.

According to this formula, the lower limit of the share of positive evaluations is estimated under the conditions of taking into account only positive and negative evaluations (that is, without taking into account the 5-point evaluation system).

At the same time, another mathematical apparatus known as Bayesian estimation (named after the author Thomas Bayes) can be used to determine the rating when applying statistical dependencies. This evaluation involves taking into account not only the average arithmetic value of the evaluations provided by the members of the commissions, but also their number:

$$\frac{\textbf{the number of votes}}{\textbf{the number of votes}+n}\times \textbf{GPA}\times\frac{\boldsymbol{n}}{\textbf{the number of votes}+n}\times 7.2453$$

where 7.2453 is some average value that is taken as the basis of the method.

Compiling a rating of candidates is the main task of the commissions regarding the results of the evaluation in the selection process (Krill, 2018; Workforce Framework, n.d.; Prokopenko *et al*., 2020).

Thus, the existing automated system makes it possible to ensure staffing at the necessary level to perform the tasks of OKI SOU as assigned.

DOI: 10.24025/2306-4412.3.2023.288836

Conclusions

Thus, for the successful management of the knowledge base in the field of critical infrastructure protection, when implementing knowledge management as a system for improving the qualifications of SOU personnel, it is important to implement strategies based, on the one hand, on the requirements of standards (Information security, 2022; Workforce Framework, n.d.), on the other - on implementation of knowledge base management principles as a process to which process management rules are applied. This may include ongoing training, building a safety culture, collaboration with other organizations and internal communication, and improving knowledge base management processes.

Implementation and compliance with the rules must be ensured and participated by the management of OKI SOU, all possible technologies and technical means must be applied, the knowledge base management process itself must be deeply integrated into the organization's business processes.

The staff should be motivated, have a desire for knowledge due to the possibility of obtaining career prospects and material remuneration. The listed conditions, combined into an automated system, will allow to increase the efficiency of the organization's activities and ensure the protection of OKI SOU under the condition of limited resources.

Acknowledgements

None.

Conflict of interest

None.

References

Andreeva, T. (2005). Motivation of people at work. *Personnel management,* 4.12.

Information Security, Cyber Security and Privacy Protection – Information Security Management Systems – Requirements: State Standard of Ukraine DSTU ISO/EN 27001:2022.

Kremen, V.H., & Ilin, V.V. (2022). Philosophy of human-centrism in the system of anthropological studies. *Anthropological Measurements of Philosophical Research,* (21), 5-14. Retrieved from https://doi.org/10.15802/ampr.v0i21.260429.

Krill, M. (2018). Meritocracy as the kingdom of reason. Retrieved from http://cloudwatcher.ru/analytics/3/view/35/.

Malikhin, O.V., & Yarmolchuk, T.M. (2020). Current learning strategies in the professional training of information technology specialists. *Information technologies and teaching aids,* 76(2).

NIPP 2013 Partnering for Critical Infrastructure Security and Resilience (n.d.). Retrieved from https://www.cisa.gov/resources-tools/resources/2013-national-infrastructure-protection-plan.

Obolonsky, A.V. (2001). Personnel policy in the federal civil service of the USA: History and modernity. *Social sciences and modernity,* 3. 41-61.

Official bulletin of the French Armed Forces (2009). Nov. 13, No. 44, permanent part of the General Staff.

On Adopting the Regulations for the Evaluation and Promotion Process: Royal Decree (document No. 2). (2001). Sept. 28, No. 1064.

DOI: 10.24025/2306-4412.3.2023.288836

On Approval of General Requirements for Cyber Protection of Critical Infrastructure Objects: the Resolution of the Cabinet of Ministers of Ukraine. (2019). June 19 No. 518. Retrieved from https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text.

On Approval of the List of Works Where There Is a Need for Professional Selection: the Order of the Ministry of Health (1994). Sept. 23, No. 263/121.

On Critical Infrastructure: the Law of Ukraine (2021). Document 1882-IX. Editorial from 05.12.2022. Retrieved from https://zakon.rada.gov.ua/laws/show/1882-20#Text.

On the Basic Principles of Ensuring Cyber Security of Ukraine: the Law of Ukraine. (2019). Document 2163-VIII. Editorial from 08/17/2022. Retrieved from https://zakon.rada.gov.ua/laws/show/2163-19#Text.

On the Organization of Personnel in the Armed Forces of Spain: the Law (document No. 1) (1999). Chapter II of Chapter VII "Evaluation Process" and Chapter I of Chapter VIII "Procedure for Promotion". May 18, No. 17.

Pan, L.V., Sysenko, N.V., & Abramovych, O.K. (2004). The concept of knowledge management as a new direction of organization management. *Proceedings, Economic Sciences,* 30.

Prokopenko, O.S., Rybydaylo, A.A., & Vasyukhno, S.I. (2020). Application of controlling technology for career management of military personnel. *Collection of scientific works of the Center for Military and Strategic Studies of the National Defense University of Ukraine named after Ivan Chernyakhovsky,* 1(68). 66-73.

Study of the Problems of Managing the Career of Military Personnel, Taking into Account the Requirements for Candidates for Positions in the Armed Forces of Ukraine: Report on the GDR (code "Passport"). (2018). Kyiv: NMC KP MOU.

The Army Strategic Planning Guidance 2006-2023 (2023). Retrieved from https://www.hsdl.org/%3Fabstract%26did%3D443218+&cd=2&hl=ru&ct=clnk&gl=u.

Vetrov, V.I., & Vraneshych, O.V. (2020). Model of personnel management. *Defense Bulletin,* 3, 16-21.

Workforce Framework for Cybersecurity (NICE Framework): NIST Special Publication 800-181. (n.d.) National Institute of Standards and Technology.

DOI: 10.24025/2306-4412.3.2023.288836

СИСТЕМНИЙ ПІДХІД ДО АВТОМАТИЗАЦІЇ ПРОЦЕСІВ ЗАБЕЗПЕЧЕННЯ КОМПЕТЕНТНОСТІ ПЕРСОНАЛУ НА ОБ’ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ СИЛ ОБОРОНИ УКРАЇНИ

С. М. Чумаченко
Доктор технічних наук, старший науковий співробітник,
голова ГО Асоціації фахівців цивільного захисту
https://orcid.org/ 0000-0002-8894-4262, e-mail: s.chumachenko@rnbo.gov.ua
В. А. Попель
Начальник відділу науково-технічної експертизи
Державний науково-дослідний інститут
технологій кібербезпеки та захисту інформації
https://orcid.org/ 0000-0001-5544-3544, e-mail: v.popel@cip.gov.ua

Анотація. Публікація присвячена проблемам автоматизації системи підбору та оцінки відповідності персоналу, що має забезпечувати безпеку об’єктів критичної інфраструктури Сил оборони України. В статті розглянуто основні нормативні документи, вимоги до персоналу та шляхи оцінки відповідності його знань, умінь і компетенцій. Враховані вимоги професійних стандартів, розроблених для сфери критичної інфраструктури Сил оборони України та захисту інформації. Ця робота має на меті визначити базові проблеми, пов’язані з добором кваліфікованого персоналу, оцінкою його відповідності та визначенням якості роботи в процесах діяльності. Матеріали статті стосуються саме об’єктів критичної інфраструктури Сил оборони України і розглядають особливості, пов’язані з процесами забезпечення безпеки критичної інфраструктури. Результати, отримані внаслідок проведеного аналізу проблем персоналу в сфері забезпечення безпеки об’єктів критичної інфраструктури, мають допомогти керівникам установ, організацій, підприємств, а також службам HR при формуванні та комплектуванні підрозділів, підготовці та розстановці кадрів. Розглянуто основні нормативні акти, що регулюють процеси захисту критичної інфраструктури, досвід розвинених країн, в першу чергу США та Європейського Союзу, стандарти безпеки (ДСТУ ISO/EN 27001, NIST Special Publication 800-181) та рекомендовані практики. Висновки містять рекомендації щодо автоматизації системи добору, підготовки та підвищення кваліфікації персоналу в сфері захисту об’єктів критичної інфраструктури, а також її інформаційної та кібербезпеки. Наведено рекомендації щодо удосконалення автоматизації процедур добору та розстановки кадрів, планування підвищення кваліфікації та створення системи професійної підготовки, що базується на системі управління знаннями.

Ключові слова: автоматизація, системи управління, захист критичної інфраструктури, компетентність персоналу, стандарти інформаційної безпеки, знання, навички, компетенції, управління знаннями.

Дата надходження: 20.08.2023
Прийнято: 10.09.2023

DOI: 10.24025/2306-4412.3.2023.288836