DOI: https://doi.org/10.26642/sas-2025-3(9)-56-60
УДК 355.23:378.2:316.46

Slyusar Vadym
doctor of philosophical sciences, docent
Zhytomyr Polytechnic State University
https://orcid.org/0000-0002-5593-0622

Kondratiuk Yuliia
candidate of sciences (history), docent
Zhytomyr Polytechnic State University
https://orcid.org/0000-0002-5570-5505

Yablonska Nadiya
candidate of sciences (pedagogy)
Zhytomyr Polytechnic State University
https://orcid.org/0000-0002-3368-5929

Vitiuk Iryna
candidate of philosophical sciences, docent
Zhytomyr Polytechnic State University
https://orcid.org/0000-0002-2998-6323

Strategies and philosophy of coaching in the formation of digital resilience of a national security specialist

Abstract. The article is devoted to the analysis of coaching strategies aimed at building digital resilience of national security professionals in the context of global digitalization and growing cyber threats. The study emphasizes the relevance of coaching in the management of human resources in the field of national security. This practice is a tool that promotes the development of professional and personal competencies through a dialogic approach and pragmatism. The authors examine the impact of digital technologies on social and professional processes, in particular in the context of Society 5.0, where the emphasis is on the synergy of humans and artificial intelligence. Digital resilience is considered not only as digital literacy, but also as a set of soft skills and motivational attitudes for adapting to new technologies. The article analyzes coaching techniques, such as the Balance Wheel and the Eisenhower Matrix, which help professionals assess their own competencies and optimize work processes. Coaching is viewed as a method that covers both the training period and self-education, contributing to the development of psychological resilience and critical thinking. The study offers practical recommendations for the implementation of coaching techniques in the training of specialists.

Keywords: digital resilience; national security; information security; professional competence; coaching; soft skills; nineteenth- and twentieth-century philosophy; modern philosophy; media philosophy.

Relevance. Coaching, which is based on the art of building a question-answer system, allows a specialist, with the support of a specialist, to determine the motives for making certain changes (learning new tools for professional activities, mastering new relevant skills, etc. The processes of global digitalization and the adoption of artificial intelligence technologies are affecting the change in strategies for implementing professional activities, which involves learning new tools. At the same time, there is a need to realize the necessity of taking basic actions to protect personal data and prevent cyber threats. If these problems were mainly the subject of research in the technical sciences, the establishment of new social relations analyzed in the Society 5.0 theory shifts the focus of scientific research to the interdisciplinary plane, primarily in the field of humanities, social and military sciences. It is in this area that we are able to carry out comprehensive analyses of the interdependence of the growing role and place of digital technologies at all levels of social life and the corresponding increase in the number of interventions by third parties in various professional and non-professional processes, with their own goals, which are characterized by a predominantly destructive effect. This is also reflected in the implementation of strategic communications through the spread of fake news and disinformation in the media space of a potential or real enemy, harming their national security, economy, politics, and social stability in general. Therefore, specialized educational institutions, including higher education institutions, face the task of effectively building digital resilience in the training of national security professionals who must be able to develop effective strategies for protecting and managing information risks, and quickly and effectively overcome the social and organizational consequences of cyberattacks. One of the effective methods that covers both the training period and self-education is coaching.

The purpose of the article is to analyze the theoretical foundations and identify possible coaching strategies aimed at building digital resilience of national security professionals.

Degree of research of the problem. In our previous studies, we have pointed out the need to pay attention to the formation of digital resilience in the training of specialized professionals to ensure the continuity of national security in the face of rapid technological development and new forms of threats. In particular, we identified prospects for mastering knowledge of strategic communications [10]. The authors also studied coaching technologies as an effective tool to support graduate students in their research activities in the face of modern challenges, including wartime in Ukraine. The authors revealed the experience of applying four coaching techniques – «Balance Wheel», «Powerful Questions», «Eisenhower Matrix» and «Time Blocking» – to unlock the internal potential of applicants [8**Error! Reference source not found.**]. It is important to study the nature of coaching, and in the context of its focus on dialogue, it is worth considering the philosophy of coaching. Significant in this context is the article by Christopher Cashion and Mark Partington, which criticizes the concept of «coaching philosophy» which, in their opinion, is often confused with ideology, reflecting socially constructed beliefs and practices [3]. At the intersection of philosophy, management, and public administration, Ukrainian scholars Petro and Iryna Saukh analyze the concept of Society 5.0, which, using various innovations created in the era of digitalization of the fourth industrial revolution, aims to synthesize the best achievements of the digital and human worlds and the synergy of humans and artificial intelligence [9].

Summary of the main material. The wave of cyberattacks on Estonian public services in 2007 was the beginning of the systematic application of digital resilience mechanisms in the national security system. The attack lasted for three weeks. However, in scientific discourse, this concept is used much more broadly - as any action (not only technical, but also social and technological) that requires the use of digital technologies to overcome its consequences. Digital resilience itself is defined as «building our capacity as a society to use the powerful potential of digital technologies to prepare for and protect against a range of current and future challenges and threats. These could include cyberattacks, disinformation campaigns, natural disasters, emerging infectious diseases, or... war» [5, p. 7]. The problem of managing the country's national security and the skills of specialists to use digital technologies to respond to these challenges comes to the fore.

In addition to digital education, which involves a set of knowledge about relevant modern technologies and skills to apply them in practical life, students should develop psychological attitudes to the permanent development of new technologies in accordance with the dynamics of their emergence and adoption, to overcome information noise, and to de-technologize them. The latter is understood as the application of a set of measures to preserve the humanitarian component in the processes of their implementation. For example, the emergence of large-scale language model technology has led to the effect of mass application in various spheres of human activity, and, as a result, to the competition among developers to improve models. In turn, many social processes are being dehumanized, and human activity is being replaced by algorithms of model programs. As a result, job cuts, the emergence of a class of «superfluous» people, total retraining of personnel, and the destruction of traditional social protection mechanisms transform a person's attitude to life, which is associated not only with the loss of sources of income but also with the loss of life guidelines [9]. A national security professional's digital resilience is designed not only to withstand relevant challenges on their own, but also to be able to detect them in time and develop countermoves.

Scientists S.K. Shandilya, A.Datta, J.Karthik, A.Nagar have developed a number of elements of national security management to build digital resilience, among which they highlight training and awareness (implementation of training programs so that all employees understand their role in maintaining digital resilience), as well as regular updating of technologies and tools that increase security and resilience [4]. Digital resilience is not limited to digital education or digital literacy. Rather, it is about the soft skills that a future national security professional must master, the motivational attitudes to master new knowledge, and the philosophical basis for understanding the trends of digitalization and its impact on social processes. If you realize the need to involve a specialist in self-development, the question of the latter's competence arises. Coaches, according to K.Kashion and M.Partington, usually rely on practical experience and «common sense» rather than on theoretical reflection on their practice, and therefore, in order to identify current trends, the coach must realize that it is true philosophical reflection that can contribute to the transformation of coaching practice, going beyond traditional approaches [3, c. 2].

He basic principles of a coaching session to build digital resilience of national security professionals are as follows: dialogical approach; pragmatism; emphasis on the individual and his or her potential; and belief in the possibilities of self-improvement. Dialogic approach, which has been fundamental to cognitive activity since

Socratic method, and its manipulative nature can be traced back to the conversations of the Sophists, is characterized by the ability to formulate a question so that the answer to it allows the subject of knowledge to determine the boundaries of the known and the unknown in order to ask the next question.

In the twentieth-century philosophy, the idea of dialogicity acquired a conceptual level in the works of M.Buber, L.Wittgenstein, K.-H. Appel, and J.Habermas. Let us pay attention to their emphasis on the role of language and language games. The task of the latter is to clarify language, its functions, and forms of work. That is, a language game appears, first of all, as a set of techniques, skills of awareness that can be learned and taught, in particular through the pedagogy [**Error! Reference source not found.**, c. 20]. Language games, on the one hand, contain ready-made clichés and templates that are contained in the culture and are learned by speakers, and on the other hand, an infinite number of variations of questions and answers that form new games. They can be understood as specific speech acts that are realized in practical activities.

Dialogic approach through «language games» in coaching sessions can explain information security risks in the context of possessing personal competencies to identify them. The coach's task is to help the national security professional determine how his or her existing knowledge and skills relate to those required to work in the modern digital environment, and, most importantly, what specific areas of development he or she needs to identify in order to perform his or her professional activities efficiently. But the main thing is to develop an action plan that the specialist working with the coach plans to realize the goal. And the basic question «What does it mean for you to be resilient to digital challenges?» contains a variety of answers based on your own professional and life experience, level of awareness, and personal characteristics of the specialist. Thus, a language game begins regarding the primary interpretations of the key words in the question, in the interpretation of digital reality. For example, through structured questions, a coach can help a specialist identify how their current knowledge and skills relate to the requirements of the digital environment, as well as identify gaps that need to be developed.

Pragmatism, as another basic principle, complements dialogic, focusing the coaching session on specific, practical results. Back in the modern era, F. Bacon emphasized the unity of knowledge and practice, emphasizing that, «Human knowledge and human power come to the same thing; for where the cause is not known the effect cannot be produced». It is worth adding, according to W.James, that «the only criterion for the truth that is possible for pragmatism is what works best for us, what leads us, what fits best with every part of life, and what fits with the totality of our experience without exception» [6, c. 42]. In this sense, the language games described by Wittgenstein are becoming applied: they are aimed at developing the skills of critical thinking, quick information analysis, and decision-making in the face of uncertainty. For example, a coach can use a dialog to model situations related to cyberattacks or information manipulation so that the session participant can work out response algorithms.

One of the effective coaching techniques that can be used to build digital resilience of national security professionals is the Balance Wheel. This technique allows professionals to objectively assess the current state of key areas of their professional and personal lives, set priorities and plan actions to strengthen resilience to the challenges of the digital environment. In the context of national security, digital resilience implies the ability to adapt to rapid technological change, counter cyber threats, and maintain balance in stressful conditions. The technology of using this technique involves conducting a session in several stages. The first one is preparation for the coaching session. Before applying the Wheel of Balance technique, it is necessary to create a trusting atmosphere, as national security professionals are often stressed by the high level of responsibility, uncertainty in the digital environment, and the need to balance professional responsibilities and personal life. In today's circumstances, particularly in the context of war, these challenges are compounded by the instability and unpredictability of the future. The coach should explain how the technique will help participants assess their current state, identify imbalances, and identify areas for strengthening digital resilience. The main point of using this technique «Wheel of Balance» is to create a visual tool that reflects the level of satisfaction with the main areas of a specialist's life and helps to plan changes. So, at the next stage, the coach begins the session by explaining that the Balance Wheel helps to assess key aspects such as professional activity in the field of national security, digital competence, psychological resilience, health, personal life, self-development, financial stability and work-life balance. This tool allows you to identify areas that need attention and plan actions to improve them, which is critical for building digital resilience. The next stage is the actual creation of the Balance Wheel. To do this, the participant of the coaching session «identifies areas of life». On a piece of paper, they draw a circle divided into 6-8 sectors, each of which corresponds to an important area of life. The recommended set for national security professionals includes the following sectors: «professional activity» (effectiveness in performing tasks related to national security); «digital competence» (knowledge and skills in working with digital technologies, cybersecurity); «psychological resilience» (ability to cope with stress and uncertainty); «health» (physical and mental well-being); «personal life» (family, friends, leisure); «self-development» (education, professional growth, mastering new technologies); «financial stability»; «work-life balance». Participants can adapt this list to their own priorities.

The next stage is self-assessment. Each sector is rated by satisfaction level from 1 to 10. For better visualization, the sectors are colored in percentage of the score. After that, the «Results Analysis» takes place. At this stage, the coach moderates a discussion during which participants analyze the areas with the highest and lowest scores, the cause-and-effect relationships between scores (for example, how low digital competence affects professional performance), the relationships between areas (how lack of rest affects psychological resilience or productivity in the digital environment).

The next stage is reflection and planning. Participants reflect, identifying desired changes and specific steps to achieve them. For example, to strengthen digital resilience, a professional may plan to take cybersecurity training, improve time management skills, or practice regular stress reduction. It is important that in this context, the Balance Wheel technique not only helps national security professionals to recognize their strengths and weaknesses, but also promotes flexibility in the digital world, where rapid change and cyber threats are an integral part of the work.

One of the biggest problems in building digital resilience is the dynamics of technology development, where the development of some tools quickly becomes irrelevant with the emergence and adoption of others. Such technologies include OSINT, which is defined as the methodical collection and use of information from publicly available sources to meet intelligence requirements, i.e. this methodology appears as a discipline of information collection that does not include analysis and dissemination, and therefore OSINT itself is not understood as a final product [2, c. 96]. The biggest challenges for a specialist working with this technology are, first, to choose the most adequate methods from the entire set of regularly updated methods, and second, to optimize production processes due to a significant increase in information flows. The Eisenhower Matrix is an effective coaching tool for national security OSINT professionals who work with a large amount of information and tasks. Its purpose is to help a specialist structure the workflow, optimize time, and focus on priorities that contribute to the achievement of strategic goals, ignoring the state of constant updating.

Conducting an Eisenhower Matrix session to accomplish this task involves first and foremost the development of a task list. The OSINT professional compiles a complete list of current tasks, including data analysis, source monitoring, report preparation, and other professional duties. The next step is to categorize the tasks into squares of the matrix. To do this, tasks are divided into four quadrants based on their importance and urgency. In the first square, «Important and Urgent» are placed. This is where tasks with tight deadlines or crisis situations are identified, such as urgent intelligence analysis to respond to a threat. The second box is used to mark tasks that are «Important but not urgent». These include strategic tasks (e.g., developing new methods of OSINT analysis, planning long-term intelligence operations, or professional training). The third box contains tasks «Not important but urgent». These are primarily tasks that distract from the main goals, such as responding to non-critical requests or standard data processing. And the fourth box is «Not important and not urgent». As a rule, this includes activities that do not contribute to professional goals, tasks that can be avoided altogether because they have no effective value (for example, excessive immersion in non-critical sources or irrelevant activities).

The next step is the prioritization and planning procedure. Its main goal is to focus on tasks from the «Important but not urgent» box, as they have a risk of moving to the «Important and urgent» box. While it is recommended to delegate or optimize tasks from the «Not important but urgent» square, and to eliminate or significantly limit tasks from the «Not important and not urgent» square. The coach helps the specialist to draw up an implementation plan, taking into account resources and workload. To do this, he/she uses a dialogic technique to encourage the participant to identify the reasons for the accumulation of tasks in the first square and the mechanisms for increasing the time spent on the second square; to organize work on setting deadlines for completing the tasks of this square, updating the focus on the productivity of the time spent (for example, hours from 8.00 to 12.00 - only for data analysis). And, finally, he/she establishes feedback in order to periodically review tasks and further adjust his/her work and adapt it to new challenges.

Conclusions. Coaching is an effective tool for building digital resilience of national security professionals, contributing to the development of their ability to adapt to rapid technological changes and counter cyber threats. The use of dialogic approaches with a focus on pragmatism, such as «language games» allows professionals to realize the limits of their knowledge and identify areas for professional development. The Wheel of Balance technique helps to assess key aspects of professional and personal life, identifying areas that need improvement to increase resilience to digital challenges. The Eisenhower Matrix helps to optimize work processes, especially for professionals working with OSINT technologies, helping them to focus on strategically important tasks.

References:

1. Bacon, F. (2000), *The new organon*, Cambridge University Press.
2. Block, L. (2024), «The long history of OSINT», *Journal of Intelligence History,* No. 23 (2), pp. 95–109.
3. Cushion, C. and Partington, M. (2014), «A critical analysis of the conceptualisation of «coaching philosophy»», *Sport, Education and Society,* No. 21 (6), pp. 851–867.

4. Shandilya, S.K., Datta, A., Kartik, Y. and Nagar, A. (2024), «What is digital resilience?», *Digital resilience: Navigating disruption and safeguarding data privacy*, EAI/Springer Innovations in Communication and Computing, Springer, doi: 10.1007/978-3-031-53290-0_1.
5. «The digital front line: 15 actions to boost Europe's digital resilience», *DigitalEurope*, [Online], available at: https://cdn.digitaleurope.org/uploads/2023/03/DIGITALEUROPE-TECHNOLOGYIN-THE-FACE-OF-HYBRID-THREATS-FINAL-WEB-1.pdf
6. Dzheims, V. (2000), *Prahmatyzm*, Vydavnychyi dim Alternatyvy, 144 p.
7. Drotyanko, L.H. (2015), «Filosofiia dialohu v kulturi informatsiinoi ery», *Visnyk Natsionalnoho aviatsiinoho universytetu. Filosofiia. Kulturolohiia*, No. 1, pp. 19–22.
8. Kondratiuk, Yu., Hordiichuk, O., Yablonska, N., and Vitiuk, I. (2025), «Kouchynhovi tekhnolohii v rozkrytti vnutrishnoho potentsialu aspirantiv», *Mizhnarodnyi naukovyi zhurnal «Universytety i liderstvo»*, No. 19, pp. 127–134, doi: 10.31874/2520-6702-2025-19-127-134.
9. Saukh, P.Yu. and Saukh, I.V. (2023), ««Suspilstvo 5.0». Arkhitektonika osvity v umovakh piatoi promyslovoi revoliutsii: vyklyky ta perspektyvy», *Visnyk Natsionalnoi akademii pedahohichnykh nauk Ukrainy*, No. 5 (2), pp. 1–7.
10. Sliusar, V., Yablonska, N., Zaiko, L. and Panchenko, N. (2024), «Formuvannia tsyfrovoi stiikosti u pidhotovtsi fakhivtsiv z natsionalnoi bezpeky ta vchyteliv «Zakhystu Ukrainy»», *Society and Security*, No. 2–3, pp. 106–111.

Слюсар В., Кондратюк Ю., Яблонська Н., Вітюк І.

Стратегії та філософія коучингу у формуванні цифрової резильєнтності фахівця з національної безпеки

Анотація. Стаття присвячена аналізу коучингових стратегій, спрямованих на формування цифрової резильєнтності фахівців з національної безпеки в умовах глобальної диджиталізації та зростання кіберзагроз. Дослідження підкреслює актуальність коучингу в управлінні людськими ресурсами у сфері національної безпеки. Ця практика є інструменту, що сприяє розвитку професійних і особистих компетенцій через діалогічний підхід і прагматизм. Автори розглядають вплив цифрових технологій на соціальні та професійні процеси, зокрема в контексті «Суспільства 5.0», де акцент робиться на синергії людини та штучного інтелекту. Цифрова резильєнтність розглядається не лише як цифрова грамотність, але й як набір soft skills і мотиваційних установок для адаптації до нових технологій. У статті аналізуються коучингові техніки, зокрема «Колесо балансу» та «Матриця Ейзенхауера», які допомагають фахівцям оцінювати власні компетенції та оптимізувати робочі процеси. Коучинг розглядається як метод, що охоплює як навчальний період, так і самоосвіту, сприяючи розвитку психологічної стійкості та критичного мислення. Дослідження пропонує практичні рекомендації для впровадження коучингових методик у підготовці фахівців.

Ключові слова: цифрова стійкість; національна безпека; інформаційна безпека; професійна компетентність; коучинг; soft skills; філософія XIX-XX століття; філософія Нового часу; медіафілософія.

Стаття надійшла до редакції 02.06.2025