

DOI: 10.17323/2587-814X.2026.1.29.40

A comprehensive approach to building an intelligent system for proactive personnel risk assessment in critical infrastructure*

Denis Nikolaevich Biryukov 

E-mail: vka@mil.ru

Andrey Sergeevich Dudkin 

E-mail: vka@mil.ru

Alexander Viktorovich Frolov

Email: vka@mil.ru

A. F. Mozhaysky Military-Space Academy, St. Petersburg, Russia

* The article is published with the support of the HSE University Partnership Programme

Abstract

Modern challenges in organizational security, particularly within critical infrastructure sectors (energy, transportation, finance, IT), necessitate innovative solutions to mitigate risks associated with hiring unreliable personnel. This requires a shift from conducting fragmented checks to the creation and implementation of comprehensive systems for proactive risk assessment. The urgency of developing such systems is driven by the high frequency and catastrophic consequences of insider incidents, coupled with the inability of traditional methods to detect complex, multi-stage threats originating from employees. However, building intelligent systems that semantically integrate heterogeneous data (biographical, behavioral, financial, digital) presents new systemic challenges. The aim of this article is to analyze the key methodological, ethical-legal, and architectural requirements for designing such systems. The work sequentially examines: 1) ethical and legal dilemmas (fairness, privacy, the right to explanation) and the constraints imposed by personal data legislation; 2) specific cyber threats targeting the compromise of the knowledge base and system logic, along with architectural countermeasures based on Security by Design principles; 3) a comparative analysis of the technological components of a multi-level assessment system (documentary verification, psychometric testing, AI analysis), justifying the necessity for their integration. The scientific novelty lies in a synthetic approach that forms a holistic methodology, considering not only technological efficiency but also fundamental legal constraints and information security requirements. The practical significance of the work consists in formulating systemic requirements for the design of secure, lawful, and socially responsible intelligent decision support systems for personnel security.

Keywords: proactive assessment of personnel risks, intelligent decision support systems, ontological modeling, semantic integration, psychometric testing in personnel security, AI analysis of behavioral and biographical data, ethical and legal restrictions on personal data processing, cyber resilience of personnel assessment systems

Citation: Biryukov, D. N., Dudkin, A. S., & Frolov, A. V. (2026). A comprehensive approach to building an intelligent system for proactive personnel risk assessment in critical infrastructure. *Business Informatics*, 20(1), 29–40. <https://doi.org/10.17323/2587-814X.2026.1.29.40>

Introduction

The problem of insider threats in critical infrastructure organizations (energy, transportation, finance, IT) is not new [1] and remains one of the most acute problems in the field of modern security. Research data indicates that a significant portion of incidents, including data leaks, sabotage, and corruption, is caused by the actions of insiders [2]. The

scale and complexity of these threats have multiplied with the development of digital technologies. According to IBM Security, most data leaks in the energy sector are related to the human factor, including employee errors and malicious actions [3]. In Russia, according to a study by “Rostelecom-Solar,” 45% of companies face incidents caused by unreliable personnel, with 22% of these incidents leading to catastrophic consequences [4].

In response to growing threats, states are tightening regulatory requirements. In the EU, Directive NIS2 obliges companies to implement employee vetting systems, including social media analysis and polygraph tests. In Russia, Federal Law No. 152-FZ “On Personal Data” and Government Decree No. 1119 regulate the collection and processing of candidate information but leave gaps regarding the use of AI algorithms. In the USA, for example, the Cybersecurity Act requires companies in the energy sector to conduct annual personnel audits for connections with extremist groups. In Russia, as noted by “HeadHunter,” every second organization conducts preliminary candidate checks, yet only 27% have an in-house security service [5].

Traditional candidate assessment methods, such as resume analysis, interviews, or reference checks, prove ineffective in identifying complex, multi-stage, and intentionally concealed threats. Their key limitation is the fragmentation of data and the lack of semantic integration of heterogeneous information sources: biographical, behavioral, financial, and digital traces of a candidate. This leads to a reactive, rather than predictive, approach to personnel security, which, given the high cost of insider incidents (including both direct and reputational losses), becomes an unacceptable risk to the sustainable functioning of organizations.

In response to this challenge, technological solutions using artificial intelligence (AI), psychometric testing, and automated data verification are emerging in scientific literature and on the market [6–10]. However, their application often remains isolated, failing to solve the problem of comprehensive candidate assessment. Moreover, the creation of centralized intelligent systems aggregating confidential personal data generates new, systemic risks. These include both ethical-legal dilemmas – questions of fairness, discrimination, privacy, and the right to explanation of automated decisions [11, 12] – and unique cyber threats aimed at compromising the semantic knowledge base and assessment algorithms themselves.

Thus, the relevant scientific and practical task is the development not just of another vetting tool, but of a holistic methodology for designing systems for proactive personnel risk assessment. Such a methodology should ensure the semantic integration of heterogeneous data to identify complex threat scenarios, while being embedded within strict ethical-legal frameworks and considering cybersecurity requirements for the designed system itself.

The aim of this article is to analyze the key methodological, ethical, legal, and architectural requirements for building an intelligent risk assessment system for personnel recruitment in critical infrastructure facilities. The focus is not on a detailed description of the internal ontological model (which is the subject of a separate study), but on the systemic constraints and conditions under which its implementation would be correct, safe, and lawful.

The scientific novelty of the work lies in the synthesis of three aspects usually considered in isolation:

- 1) a comparative analysis of the technological components of a multi-level assessment system (AI, psychometrics, data verification);
- 2) a comprehensive analysis of ethical-legal dilemmas and regulatory requirements;
- 3) proactive modeling of cybersecurity threats inherent to the ontological system itself and the formulation of architectural countermeasures based on Security by Design and Privacy by Design principles.

The structure of the article reflects the logic of the sequential formation of system requirements. The first section examines the ethical and legal aspects that define the fundamental design boundaries. The second section is dedicated to analyzing new vectors of cyber threats and the resulting architectural requirements for system security. The third section contains a comparative analysis of existing technological assessment methods (documentary verification, psychometric testing, AI analysis), justifying the need for their inte-

gration within a unified methodology. The conclusion formulates the main findings and defines directions for further research.

1. Ethical and legal aspects of applying an ontological approach in candidate assessment

The shift to comprehensive candidate assessment systems based on semantic integration of heterogeneous data and artificial intelligence methods gives rise to a number of ethical and legal dilemmas [13]. Balancing organizational security with the protection of individual rights requires careful analysis prior to the design and implementation of such systems.

Key moral and ethical dilemmas.

The principle of fairness and non-discrimination. Automated systems based on historical data can reproduce and amplify existing societal biases. For example, identifying “potentially unreliable” candidates based on analysis of social activity can lead to discrimination based on indirect attributes (political views, religious affiliation, social status). This contradicts both ethical norms and labor legislation.

The right to privacy and digital autonomy. Integrating data from open sources (social networks, forums, etc.) with data from corporate and state databases contributes to creating an exhaustive digital profile of an individual without their explicit consent for creating such a profile and without informing the potential candidate about it. The question arises about the boundaries of permissible surveillance: where does the employer’s legitimate interest in a candidate’s reputation end, and where does unacceptable intrusion into private life begin?

The right to explanation. A hiring decision based on the output of an ontological model and AI algorithms may, not without reason, be perceived by a candidate as unfair and unexplainable, as most machine

learning models operate as “black boxes.” In accordance with evolving legal doctrine (e.g., the “right to explanation” in GDPR), a candidate should have the opportunity to challenge an automated decision and receive a meaningful explanation of its reasons.

System requirements and constraints imposed by legislation.

Transparency and controllability of ontological tools. In the context of Russian legislation (Federal Law No. 152-FZ “On Personal Data”), data processing must be specified, limited to stated purposes, and understandable to the data subject. This generates a systemic requirement for the ontology: its structure and key logical rules must be available for review by both the candidates themselves (in the part concerning them) and regulatory bodies. An organization may be required to disclose not the specific settings of generative AI (as a trade secret), but at least the principles, categories, and attributes upon which the assessment is built.

Limitations on the content and structure of ontologies. Legislation does not directly regulate the structure of ontologies, but the basic principles of personal data processing (lawfulness, purpose limitation, and data minimization) impose serious constraints on it:

- ◆ the ontology should not include redundant classes and properties that do not have a direct and provable relation to professional qualities and risks for a specific position (e.g., sexual orientation, philosophical beliefs, etc.);
- ◆ logical rules and the risk scenarios themselves must be justified and documented by research or statistics to exclude arbitrary and discriminatory interpretation.

The requirement of human control. The final hiring decision, especially one based on an assessment of “unreliability,” cannot be fully automated. The system should provide results as a recommendation, and the final decision must be made by a human (HR specialist or manager), who bears responsibility for it.

The established ethical-legal frameworks define conceptual constraints for the ontological model. However, their practical implementation and ensuring compliance with the requirements that an intelligent decision support system for personnel recruitment must satisfy are impossible without considering a new class of applied tasks – namely, the tasks of ensuring the cybersecurity of the designed intelligent system itself. A centralized knowledge base accumulating confidential personal profiles becomes, in itself, an object of critical importance and generates unique attack vectors. A comprehensive analysis of these threats and the architectural countermeasures necessary to protect the integrity, confidentiality, and availability of the ontology constitutes the subject of separate consideration in the next section.

2. Current threats and additional requirements for ensuring information security in the implementation of ontological modeling

Creating a unified ontological knowledge base, accumulating confidential biographical, financial, and behavioral data about candidates, transforms the threat landscape for an organization. The integrated ontology, being the core of the decision support system, itself becomes a holistic object of high value and, consequently, a priority target for cyberattacks. This imposes specific constraints on its architecture, content, and management processes.

Classification of new vectors of cyber threats.

Compromise of the ontology. Unlike fragmented data, a compromised ontology allows a malicious actor to:

- ◆ make unauthorized changes to ontological relationships between specific concepts to systematically and purposefully reduce the system’s sensitivity to certain threats;

- ◆ add false facts or entire scenarios to the ontology aimed at discrediting specific candidates (targeted “black PR”) or, conversely, concealing their real risks.

Leakage of the confidential semantic network – the foundation of the ontology. The theft of the knowledge base is equivalent to obtaining a structured dossier on all candidates who have undergone vetting. In this case, not only candidate attributes (experience, education) are disclosed, but also logical connections between them (e.g., “Candidate A is connected to Company B, which participated in a dubious tender”), which also represents a leakage of contextual information.

Insider misuse of access to the ontology. A security service employee or knowledge engineer with rights to modify the ontology can manipulate it for corrupt or other unlawful purposes, remaining “in the shadows” due to the complexity of verifying semantic changes.

Architectural constraints and countermeasures. To counter the indicated threats, the system architecture must be based on the “Security by Design” principle (an approach to software development where security is built into the product at the concept stage, not added post facto [14]):

- ◆ all operations modifying the ontology (adding classes, properties, individuals, rules) must be recorded in a structure resistant to tampering. The use of blockchain technologies or similar distributed ledgers to create a verifiable and irrefutable change log can be recommended, which directly contributes to proving insider actions within the organization’s infrastructure [15]. This imposes an architectural constraint: the ontology management system must be integrated with a secure logging module;
- ◆ the ontology itself should be used to model security policies. It is necessary to introduce, for example, classes such as AuditEvent, SystemUser, AccessRole and relationships like hasPermission, performedAction. This should allow, using the same ontology, to describe, control, and audit data access within

the system, implementing the RBAC (Role-Based Access Control) concept;

- ◆ personal data, being particularly sensitive, should be stored in encrypted form, and the ontology should operate only with their cryptographic hashes or tokens to establish semantic links, without the need for constant decryption and access to the semantics of facts.

Cybersecurity requirements directly affect the implementation of ontological modeling as well. The ontology should not contain redundant data. For example, to establish a fact of “financial unreliability,” in some cases, the presence of the attribute “hasCreditDelinquencyStatus = true” may be sufficient, without the need to store detailed delinquency history in the ontology itself. This reduces the damage in case of its compromise.

It is also recommended to design the ontology as several linked but physically or logically separated modules. Public data (from social networks and other publicly available resources) can reside in one module, while sensitive data (polygraph results, connections with law enforcement) – in another, with stricter access control. This limits potential risks and damage in case of compromise.

The ontology population process should include a stage of mandatory verification of scenarios and features entered by expert analysts. A cross-validation system is proposed, where a new inference rule, scenario, or class is activated only after confirmation by several independent experts. This should counteract the risk of “semantic sabotage.”

Thus, the design of an ontological system for risk assessment in personnel recruitment must take into account that the designed tool for risk management itself becomes a source of new, systemic vulnerabilities, creating the possibility of new cyber threats. The response to this challenge is the implementation of a multi-layered security architecture based on the prin-

ciples of continuous and comprehensive auditing, strict access segregation, end-to-end encryption, and minimal sufficiency of ontological models. Only such comprehensive protection should make it possible to mitigate the risks inherent in centralized repositories of confidential data and intelligent decision support systems based on them.

The proposed ontological approach should be implemented not as a closed system in terms of the methodology for making decisions to reject a candidate, but as a transparent decision support tool embedded within ethical-legal frameworks. This requires designing the ontology considering “Privacy by Design” principles (an approach where privacy and data protection considerations are integrated into the design phase of any system, service, product, or process), implementing explainability mechanisms (Explainable AI, XAI), and ensuring the ability to audit all its modifications. Only under these conditions can a balance be achieved between the operational security of an organization and fundamental human rights.

3. A multi-level system for personnel risk assessment in critical infrastructure: an ontological approach, psychometric testing, and AI analysis

Without claiming universality, the focus should be on the following key risks associated with hiring new employees:

1. *Professional incompetence.* According to Checker, 78% of candidates provide false information about skills and experience, increasing the risk of errors in critical projects.
2. *Connections with criminal structures.* Undetected employee connections can lead to data leaks or sabotage.
3. *Drug and other addictions.* Employees with addic-

tions more frequently violate security protocols, as confirmed by Russian Ministry of Internal Affairs statistics.

4. *Financial problems.* Indebtedness makes candidates vulnerable to corruption, as noted in studies by credit bureaus.

Review of existing approaches: documentary verification and psychometric testing. Modern personnel vetting methods can be divided into two main categories: documentary verification and psychometric testing. Various technological solutions can be applied in this context.

Documentary verification.

Verification of work history and education. Using state databases (Pension Fund, Ministry of Internal Affairs) and university APIs. For example, the “SearchInform” platform automates requests to 98% of Russian educational institutions, reducing verification time from 7 to 2 days. In Russia, 67% of companies use the Unified Register of Diplomas from the Ministry of Education and Science, which allows detecting 18% of forged documents. However, the system has limitations: universities often process requests for up to 14 days; 32% of educational institutions do not update information about graduates. In 2023, 12% of resumes contained false data about education, as noted in the 2023 report on resume falsifications by the Russian Union of Industrialists and Entrepreneurs.

Direct contact with previous employers helps clarify actual achievements. According to MIT, 30% of references contain hidden negative assessments.

Social Media Monitoring. Various tools can be applied for social media monitoring (depending on countries, social networks, etc.). For example, platforms like SocialIntelligence Corp analyze publications for radical views. In 2023, 7% of candidates in the energy sector were screened out due to posts on Telegram supporting extremist groups.

Psychometric testing.

MMPI and BigFive questionnaires. The MMPI-2 has been used for quite some time [16] and identifies tendencies toward manipulation (Scale L) and aggression (Scale Pd). In an MIT study, the test identified 80% of candidates with criminal inclinations. For instance, 9.7% of those convicted for terrorism showed clinical scales above the norm. Big Five: the assessment of Conscientiousness correlates with employee reliability ($r = 0.62, p < 0.01$) [17].

Stress resistance assessment. Application of case techniques simulating emergency situations. For example, a case method from “Media Netology” facilitates predicting behavior in crisis situations, and the “Crisis Management” test from PwC reduced staff turnover by 25% in the energy sector.

Various technological solutions with certain advantages and disadvantages can be applied during documentary verification and psychological testing. Some of them are considered below.

Ontological models.

These models [11, 18] can be used for semantic analysis of resumes and cross-referencing their data with incident databases. The Palantir system is used in the USA to identify candidates connections with terrorist organizations, demonstrating 85% accuracy, and can also correlate candidates’ employment periods, for example, with cyber incidents in the CISA database.

AI-algorithms.

NLP analysis of resumes [12] allows, for example, identifying contradictions in dates and facts (IBM Watson algorithms reduce errors by 40% and detect date contradictions with 93% accuracy).

Computer vision: analysis of video interviews [19] for micro-expressions (e.g., the HireVue platform analyzes micro-expressions (frequent blinking (>20 times/min) correlates with secretiveness ($r = 0.71$)) predicts candidate reliability with 78% accuracy).

Polygraph.

Used for candidates with “red flags” [20, 21].

In some cases, conducting additional in-depth checks may be required:

- ◆ verification of professional competence (e.g., the CISSP exam for cybersecurity specialists confirms knowledge of security standards);
- ◆ analysis of credit (financial) history (Equifax and NBKI services identify financial vulnerability of candidates. A Deloitte study shows that 33% of employees with a credit burden >50% of income are involved in fraud and/or corruption. In 40% of cases, debts exceeding income are identified);
- ◆ blockchain for transaction verification (the Chainalysis service tracks candidates cryptocurrency transfers. In 2023, 5 cases of money laundering among top managers, 12 candidates with connections to sanctioned wallets were identified), as well as for logging and proving insider actions within the organization’s infrastructure [22].

At the same time, it should be noted that, at present, there is a lack of integration between the considered methods. For example, AI does not consider polygraph results, leading to fragmented assessment; ontological models are rarely used and even more

rarely integrated with psychological tests. Polygraph examinations are quite expensive per candidate and are inaccessible for small businesses.

Comparative analysis of approaches. A comparative analysis of the effectiveness of candidate assessment methods was conducted during the research (*Table 1*). The data presented in *Table 1* were obtained as a result of a comprehensive analysis of open scientific publications, reports from consulting companies, and the HR technology market, and the approximate implementation cost was estimated based on an analysis of the average service cost on the market in 2025 [23–28]. Naturally, within the analysis that was conducted, the complexity of the methods (e.g., MMPI, Big Five questionnaires) and the need to involve qualified specialists to interpret the results were not assessed. It is well known that the quality of polygraph examinations heavily depends on the expert conducting them, which certainly affects the final implementation cost. When conducting AI analysis, it is difficult for a non-specialist to correlate the quality of the applied models and candidate testing results, so the average market service cost must be considered. However, it was revealed that ontological models are not popular, and their implementation cost cannot be estimated as there are no similar offerings on the service mar-

Table 1.

Comparative analysis of approaches

Method	Accuracy, %	False positives, %	Implementation cost, USD/cand.
Documentary verification	60–68	22–28	8–15
Psychometric testing	75–80	15–20	18–50
AI analysis	85–90	8–12	50–100
Polygraph	81–91	12–18	70–110

ket, which limits the understanding of their contribution to identifying unreliable employees.

Various combinations of the approaches we considered are successfully applied by organizations in different countries. For example, the CLEAR system for civil servants (USA) combines credit history and social media checks and reduced hiring risks in the public sector by 40% (CLEAR Program Annual Report. U.S. Department of Homeland Security). In China, social credit scores are analyzed alongside transaction analysis on Alipay; however, this approach is criticized for privacy violations (in 2019, over 10,000 officials voluntarily confessed to corruption under pressure from the system). In Germany, the Xayn platform uses Federated Learning to analyze data without centralization, complying with GDPR.

Conclusion

This research was dedicated to solving the relevant task of forming systemic foundations for designing intelligent systems for proactive personnel risk assessment in critical infrastructure organizations. The work justifies the necessity of shifting from fragmented checks to a comprehensive approach capable of identifying complex insider threats.

The main results obtained within this article are as follows:

1. Key ethical-legal frameworks have been defined, serving as mandatory context for any technological development in this field. Dilemmas of fairness, privacy, and explainability, as well as specific legislative requirements imposing constraints on the collection, processing, and interpretation of candidate data, have been analyzed.
2. Specific cybersecurity requirements arising from the creation of a centralized ontological knowledge base have been formulated. A set of architectural countermeasures based on Security by

Design and Privacy by Design principles is proposed to protect the integrity, confidentiality, and availability of the assessment system itself.

3. A comparative analysis of technological components (documentary verification, psychometric testing, AI analysis) has been conducted, and the methodological necessity of their deep semantic integration for transitioning from reactive to predictive risk assessment models has been proven.

Thus, the practical significance of the work lies in creating a comprehensive set of requirements and constraints for architects and developers of intelligent systems for proactive personnel risk assessment in organizations. The proposed approach allows us to design systems where technological efficiency does not contradict legal norms, ethical principles, and fundamental information security requirements.

Directions for future research. Further work involves transitioning from the formulated systemic requirements to concrete implementation, focusing on developing and verifying a formal ontological model intended for semantic data integration and identifying risky candidate behavior scenarios. For this, it is necessary:

- ◆ to classify suspicious actions of candidates for vacant positions and types of threats originating from them;
- ◆ to develop a methodology for constructing scenarios based on justified ontological relations;
- ◆ to consider issues of integrating the model with the upper-level UFO ontology to ensure methodological rigor.

As envisioned, this will allow us to move from the conceptual foundations outlined in the article to creating practical tools for intelligent decision support systems for proactive personnel risk assessment in critical infrastructure organizations. ■

References

1. Reason, J. (1990). *Human error*. Cambridge University Press. <https://doi.org/10.1017/cbo9781139062367>
2. Greitzer, F. L., & Hohimer, R. E. (2011). Modeling human behavior to anticipate insider attacks. *Journal of Strategic Security*, 4(2), 25–48. <https://doi.org/10.5038/1944-0472.4.2.2>
3. IBM. (2024). *Cost of a Data Breach Report 2024*. Armonk, NY: IBM Security.
4. Solar Group. (2025). *Cyber-attacks on the credit and financial industry in 2025*. <https://rt-solar.ru/analytics/reports/6391/>
5. hh.ru. (2025). *Screening candidates for hiring: Research*. <https://hh.ru/article/301430>
6. Tuan, A. C., Dang, M. T., Do, H. N., Solanki, V. K., Torres, J., Gonzalez Crespo, R., & Nguyen, T. N. A. (2024). Ontology and its applications in skills matching in job recruitment. *Applied Ontology*, 19(3), 287–306. <https://doi.org/10.3233/ao-240019>
7. Miranda, S., Orciuoli, F., Loia, V., & Sampson, D. (2017). An ontology-based model for competence management. *Data & Knowledge Engineering*, 107, 51–66. <https://doi.org/10.1016/j.datak.2016.12.001>
8. Wanyonyi, E. N., Abeka, S., & Masinde, N. (2023). A systematic review on machine learning insider threat detection models, datasets and evaluation metrics. *International Journal of Network Security & Its Applications*, 15(6), 37–56. <https://doi.org/10.5121/ijnsa.2023.15603>
9. Alzaabi, F. R., & Mehmood, A. (2024). A review of recent advances, challenges, and opportunities in malicious insider threat detection using machine learning methods. *IEEE Access*, 12, 30907–30927. <https://doi.org/10.1109/access.2024.3369906>
10. Gharibi, S. J., BagheriFard, K., Parvin, H., Nejatian, S., & Yaghoubyan, S. H. (2024). Ontology-based recommender system: a deep learning approach. *The Journal of Supercomputing*, 80(9), 12102–12122. <https://doi.org/10.1007/s11227-023-05874-0>
11. Sebuli, O., Zlotnikova, I., & Hlomani, H. (2023). Ontology-driven semantic enrichment framework for open data value creation. *Data Science Journal*, 22(1), 40. <https://doi.org/10.5334/dsj-2023-040>
12. Zheng, F., Zhao, C., Usman, M., & Poulouva, P. (2024). From bias to brilliance: The impact of artificial intelligence usage on recruitment biases in China. *IEEE Transactions on Engineering Management*, 71, 14155–14167. <https://doi.org/10.1109/tem.2024.3442618>
13. Ilyina, V. A., & Ilyina, N. A. (2020). Ontologicheskiiy podkhod k poznaniyu sistemy tsennostey yuridicheskoy psikhologii [An ontological approach to understanding the value system of legal psychology]. *Psikhologiya i pravo [Psychology and Law]*, 10(1), 143–151 (in Russian). https://psyjournals.ru/journals/psylaw/archive/2020_n1/112944
14. Kotov, A. A., & Sokolov, D. V. (2021). Postroenie sistemy upravleniya informatsionnoy bezopasnost'yu ontologicheskikh modeley predmetnykh oblastey [Building an Information Security Management System for Ontological Models of Subject Domains]. *Informatizatsiya i svyaz' [Informatization and Communication]*, 3, 124–128 (in Russian). <https://cyberleninka.ru/article/n/postroenie-sistemy-upravleniya-informatsionnoy-bezopasnostyu-ontologicheskikh-modeley-predmetnyh-oblastey>

15. Venderevsky, M. A., & Pilipenko, A. P. (2019). *Sovremennyye metody i sredstva informatsionnoy bezopasnosti: uchebnoye posobiye [Modern methods and means of information security: A textbook]*. Moscow: Solon-Press (in Russian).
16. Zapata, A., Kreuch, T., Landers, R., Hoyt, T., & Butcher, J. (2009). Personality assessment in personnel selection using the MMPI-2: A cross-cultural comparison. *International Journal of Clinical and Health Psychology*, 9, 287–298.
17. Soto, C. J., & Jackson, J. J. (2013). Five-factor model of personality. *Psychology*. <https://doi.org/10.1093/obo/9780199828340-0120>
18. Fazel-Zarandi M., & Fox M. S. (2009). Semantic matchmaking for job recruitment: An ontology-based hybrid approach. Proceedings of the *3rd International Workshop on Service Matchmaking and Retrieval*. Washington, D.C.
19. Almomani, H., Alsarhan, A., AlJamal, M., Aljaidi, M., Alsarhan, T., Khassawneh, B., Samara, G., Singla, M. K., & BaniMustafa, A. (2024). Proactive insider threat detection using facial and behavioral biometrics. *25th International Arab Conference on Information Technology (ACIT)*, 1–7. <https://doi.org/10.1109/acit62805.2024.10876972>
20. Synnott, J., Dietzel, D., & Ioannou, M. (2020). Open Access: A review of the polygraph: history, methodology and current status. *Reviewing Crime Psychology*, 50–74. <https://doi.org/10.4324/9780429346927-5>
21. National Security and Intelligence Review Agency (2024). *Review of the communications security establishment's use of the polygraph for security screening*. <https://nsira-ossnr.gc.ca/wp-content/uploads/NSIRA-Final-Redacted-Polygraph-Review-EN.pdf>
22. Hu, T., Xin, B., Liu, X., Chen, T., Ding, K., & Zhang, X. (2020). Tracking the insider attacker: A blockchain traceability system for insider threats. *Sensors*, 20(18), 5297. <https://doi.org/10.3390/s20185297>
23. Committee to Review the Scientific Evidence on the Polygraph, National Research Council (2003). *The polygraph and lie detection*. Washington: National Academies Press.
24. Schmidt, F. L., & Hunter, J. E. (1998). The validity and utility of selection methods in personnel psychology: Practical and theoretical implications of 85 years of research findings. *Psychological Bulletin*, 124(2), 262–274. <https://doi.org/10.1037/0033-2909.124.2.262>
25. CheckPRSN (2025). *Checking employees* (in Russian). https://checkprsn.ru/check_applicant
26. HT-Lab (2025). *Price list of services* (in Russian). <https://ht-lab.ru/ceny/>
27. Kwork (2025). *Resume analysis using AI* (in Russian). <https://kwork.ru/script-programming/39958948/analiz-rezyume-s-ispolzovaniem-ai>
28. Yandex.Uslugi (2025). *Services: undergo a polygraph* (in Russian). [https://uslugi.yandex.ru/10174-saint-petersburg-and-leningrad-oblast/category?text= пройти+полиграф](https://uslugi.yandex.ru/10174-saint-petersburg-and-leningrad-oblast/category?text=пройти+полиграф)

About the authors

Denis Nikolaevich Biryukov

Doctor of Sciences (Technology), Professor;

Head of Department, Department of Information Collection and Processing Systems, A. F. Mozhaysky
Military-Space Academy, 13 Zhdanovskaya St., St. Petersburg 197198, Russia;

E-mail: vka@mil.ru

ORCID: 0000-0003-1300-2470

Andrey Sergeevich Dudkin

Candidate of Sciences (Technology), Associate Professor;

Deputy Head of Department, Department of Information Collection and Processing Systems, A. F. Mozhaysky
Military-Space Academy, 13 Zhdanovskaya St., St. Petersburg 197198, Russia;

E-mail: vka@mil.ru

ORCID: 0000-0003-0283-9048

Alexander Viktorovich Frolov

Applicant for Department, Department of Information Collection and Processing Systems, A. F. Mozhaysky
Military-Space Academy, 13 Zhdanovskaya St., St. Petersburg 197198, Russia;

E-mail: vka@mil.ru