

<https://doi.org/10.15407/scine22.04.126>

KRYSHTANOVYCH, M. F.¹ (<https://orcid.org/0000-0003-1750-6385>),
PASICHNYK, V. M.¹ (<https://orcid.org/0000-0002-2447-2374>),
BONDARENKO, L. P.¹ (<https://orcid.org/0000-0002-3313-3569>),
DANCHAK, L. I.¹ (<https://orcid.org/0000-0001-8768-7543>),
and SHCHEKHOVSKA, L. M.² (<https://orcid.org/0000-0002-6119-166X>)

¹ Lviv Polytechnic National University,
 1, S. Bandera St., Lviv, 79000, Ukraine,
 +380 32 258 2282, coffice@lpnu.ua
² State University "Kyiv Aviation Institute,"
 1, L. Guzara Ave., Kyiv, 03058, Ukraine,
 +380 44 406 7901, post@kai.edu.ua

CONCEPTUAL FUNCTIONAL MODELING OF THE ASSESSMENT OF REGIONAL INNOVATION POTENTIAL IN THE NATIONAL SECURITY SYSTEM

Introduction. Innovation is a critical condition for the resilience and recovery of Ukraine's regions, even in the face of the COVID-19 pandemic and the full-scale armed invasion of the Russian Federation, as it directly strengthens the security of sovereignty, territorial integrity, and democratic constitutional order. Each region has its own innovation and security potential, which should be revealed through a systematic assessment as a starting point for prioritizing investments and aligning with national security goals.

Problem Statement. There is no generalized, easy-to-use and reproducible methodological approach that comprehensively reflects the process of assessing innovation potential precisely in the context of ensuring national security, which leads to resource dispersion, duplication of efforts and slow implementation of solutions. It is necessary to develop a functional assessment model based on IDEF0, which structures inputs, outputs, management and mechanisms, ensuring coordinated management decisions and transparent project selection criteria.

Purpose. The purpose of the study is to substantiate and build, based on functional modeling IDEF0, a decomposition of the phased process of assessing the innovation potential of the region in the national security system for making coordinated and most effective management decisions.

Citation: Kryshchanovych, M. F., Pasichnyk, V. M., Bondarenko, L. P., Danchak, L. I., and Shchekhovska, L. M. (2026). Conceptual Functional Modeling of the Assessment of Regional Innovation Potential in the National Security System. *Sci. innov.*, 22(4), 126—138. <https://doi.org/10.15407/scine22.04.126>

© Publisher PH "Akademperiodyka" of the NAS of Ukraine, 2026. This is an open access article under the CC BY-NC-ND license (<https://creativecommons.org/licenses/by-nc-nd/4.0/>)

Materials and Methods. We use functional modeling IDEF0 (Integration Definition for Function Modeling) with the construction of a context diagram and hierarchical decomposition of functions, based on the principles of the ICAM program.

Results. A methodological approach based on IDEF0 with the ICOM model and stages A1—A3 has been proposed. It enables generating standardized data, agreed metrics, a capability profile, a ranked portfolio of solutions, and roadmaps for their implementation.

Conclusions. Assessing the region's innovation potential is a necessary condition for strengthening national security, as it directly translates strategic goals into manageable, verifiable actions.

Keywords: national security, model IDEF0, innovation, innovation potential, regions, war in Ukraine.

Assessing the region's innovation potential is gaining critical importance, even despite the consequences of the COVID-19 and the full-scale armed invasion of Ukraine by the Russian Federation. Thus, the COVID-19 pandemic and the full-scale war have significantly exposed the vulnerability of infrastructure, logistics, energy, healthcare, and risk management systems, showing that resilience and adaptability directly depend on the ability to generate, absorb, and scale innovations. At the same time, in the context of Ukraine's national security, which should be understood as the protection of state sovereignty, territorial integrity, democratic constitutional order, and other national interests of Ukraine from real and potential threats, innovations are not only a source of technological advantage, but also a mechanism for the rapid restoration of critical functions, economic diversification, and mobilization of local resources. Any region of Ukraine has a unique combination of scientific, entrepreneurial, educational, industrial and creative assets that form innovation and security potential, which must be revealed through competent planning, but above all through careful assessment, as mentioned above (Fig. 1).

Today, innovations serve as a powerful foundation for proactive responses to emerging threats. This is achieved through the ability to create new formats of interaction between the state, the private sector, and the public, increasing independence, optimizing resource use, and improving cybersecurity and societal resilience. It should be noted that in this context, the regional dimension may be particularly significant, as clusters, supply

chains, higher education institutions, laboratories, and innovation-driven enterprises capable of quickly transforming theoretical R&Ds into applied solutions for security and recovery are concentrated at the regional level. Given this, an effective and well-thought-out assessment of each region's innovation potential should be the initial step in prioritizing investments, optimizing support programs, creating project portfolios, and aligning development policies with strategic national security goals.

The purpose of the study is to substantiate and build, based on functional modeling IDEF0, a decomposition of the phased process of assessing the innovation potential of the region in the national security system for making coordinated and most effective management decisions. The object of the study is the processes and information flows of the regional innovation ecosystem that ensure the formation, measurement and use of innovation potential in connection with national security goals.

The available scholarly research and practical literature outlines several interconnected information fields in which the security goals of the state converge with innovation development [1—10]. These fields are connected not only by a common strategic orientation toward resilience, but also by a shared need for standardized assessment procedures, transparent prioritization criteria, and coordinated institutional interaction. In this context, the assessment of regional innovation potential should be understood not as a descriptive inventory of resources, but as a management tool that links regional capabilities with concrete national

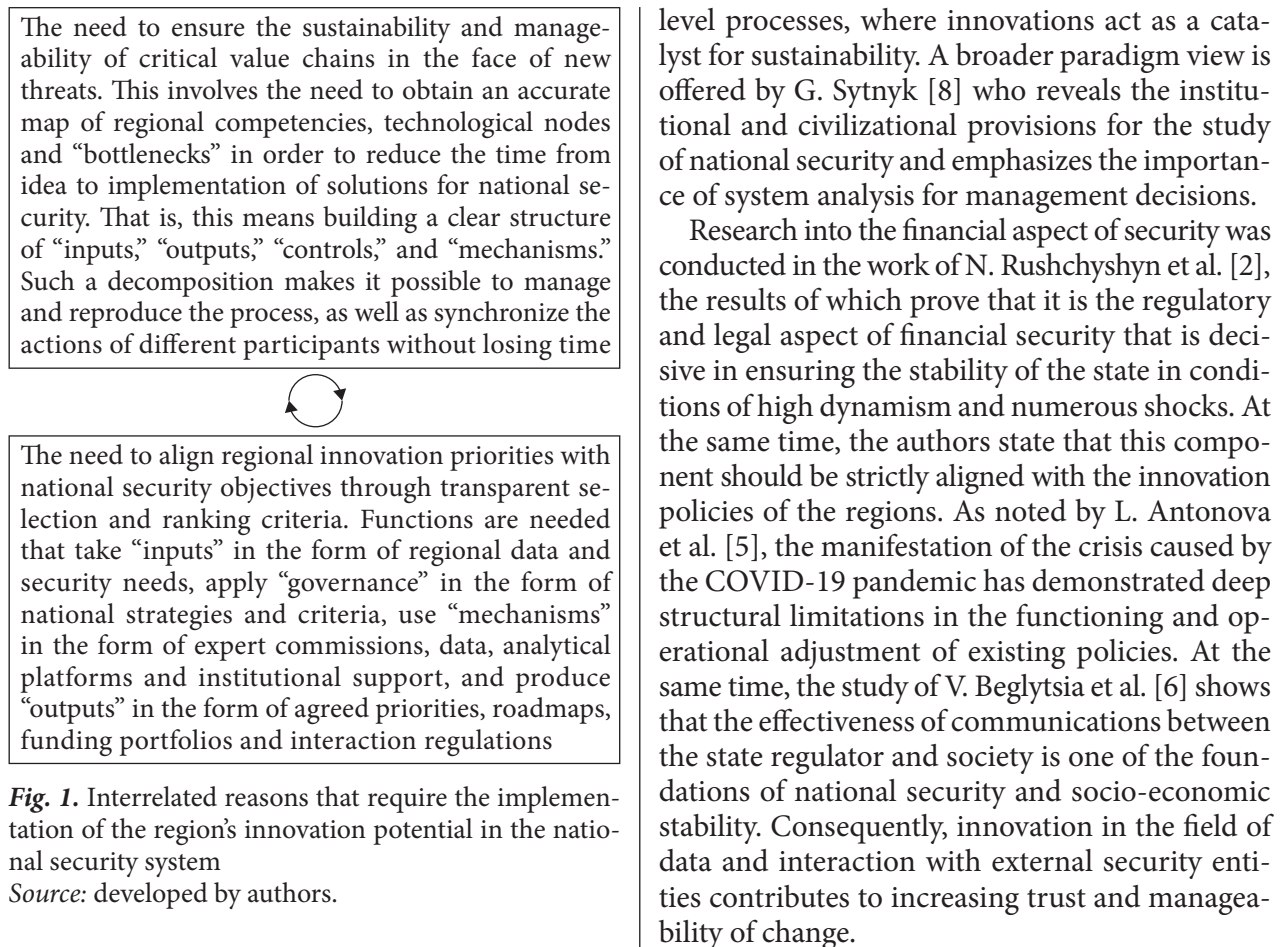


Fig. 1. Interrelated reasons that require the implementation of the region’s innovation potential in the national security system
Source: developed by authors.

security needs, implementation constraints, and the expected effects of public decisions [11–26]. For example, as emphasized by R. Prav [1], increasing the effectiveness of mechanisms for ensuring national security requires the adaptation of European experience, institutional capacity and a clear process approach, which directly correlates with the need to measure and strengthen innovation potential at the regional level. At the same time, V. Avdeev et al. [4] argue for the importance of modern directions of legal support for national security, emphasizing that the regulatory framework should be flexible enough not to inhibit the implementation of innovations in critical sectors. S. Kruk [7] draws attention to the macro aspect of the issue, stating that the development of public administration in the security sector should be based on the ability of authorities to coordinate multi-

level processes, where innovations act as a catalyst for sustainability. A broader paradigm view is offered by G. Sytnyk [8] who reveals the institutional and civilizational provisions for the study of national security and emphasizes the importance of system analysis for management decisions.

Research into the financial aspect of security was conducted in the work of N. Rushchyshyn et al. [2], the results of which prove that it is the regulatory and legal aspect of financial security that is decisive in ensuring the stability of the state in conditions of high dynamism and numerous shocks. At the same time, the authors state that this component should be strictly aligned with the innovation policies of the regions. As noted by L. Antonova et al. [5], the manifestation of the crisis caused by the COVID-19 pandemic has demonstrated deep structural limitations in the functioning and operational adjustment of existing policies. At the same time, the study of V. Beglytsia et al. [6] shows that the effectiveness of communications between the state regulator and society is one of the foundations of national security and socio-economic stability. Consequently, innovation in the field of data and interaction with external security entities contributes to increasing trust and manageability of change.

It is precisely the assessment of regions through the prism of security that is proposed by T. Panfilova et al. [3], who substantiate local approaches to optimizing state regulation in the field of business security. Therefore, this directly refers to the need to map regional competencies, clusters and innovation infrastructure so that regulatory support mechanisms are targeted and effective precisely where the greatest return on national security is possible. As emphasized in O. Polishchuk et al. [10], the formation of a security ecosystem requires the integration of technological, organizational and information solutions, which is naturally consistent with the assessment of the innovation and security potential of regions.

The role of information support is clearly defined in the work of M. Dumchykov et al. [9], which demonstrates that cybercrime poses a significant

threat to national security for the Baltic countries and Ukraine. The results place particular emphasis on the need for institutional readiness for the dynamics of technological development. At the same time, V. Yemanov [12] believes that the use of information and analytical methods to improve the effectiveness of technical intelligence requires the presence of high-quality integration of data, algorithms, and decision-making procedures at the initial stages. At the regional level, this means stimulating and supporting investment in competence, infrastructure, and interaction standards. The author's conclusions emphasize the inextricable link between the innovation capacity of regions and the efficiency and accuracy of security decisions.

It should be noted that human capital and personnel management in the public sector today represent a separate element of risks and opportunities. In this context, L. Melnychuk et al. [11] believes that countering threats to effective human resource management requires new approaches to assessing competencies, incentives, and organizational practices. At the regional level, this means that the category of innovation potential cannot be equated solely with tools or startups, but must include the ability of teams to create, integrate, and scale solutions for interaction between public and non-public partners.

Separately, it is necessary to clarify the conceptual and categorical framework of our study. Thus, summarizing the scientific achievements of our predecessors [13–15], we believe that the innovation potential of the region should be understood as the combined ability of the territorial community and its institutions to create, adapt and scale new knowledge, technologies and organizational solutions, transforming them into measurable socio-economic results. In turn, national security should be understood as the state of security of the state, society and citizens, in which the authorities, resources and legal order are able to prevent, deter and neutralize internal and external threats to the key interests and development of the country.

At the same time, the international theoretical field is broader than the initially reviewed regional-

security literature and should be considered explicitly. OECD regional innovation analytics and the associated regional innovation policy framework emphasize cross-regional comparability, multidimensional indicator systems and the role of territorial capacities in innovation diffusion [21, 22]. The European Innovation Scoreboard adds a robust logic of composite indicator construction, normalization and benchmarking across countries and regions [23]. Capability Maturity Model studies are also important because they interpret institutional capacity as a staged developmental process rather than as a static stock of resources [24]. Finally, recent MCDA research, including applications in public security, demonstrates that transparent weighting, ranking and sensitivity analysis are essential when policy decisions involve competing criteria and scarce resources [25, 26].

To emphasize the scientific and applied relevance, we note that even despite a significant body of work on institutional, legal, and technological aspects of security, there is still a lack of a holistic framework that links the innovation potential of regions to specific national security goals and provides a reproducible assessment procedure (Table 1).

Thus, our task is to make it possible to close the above-mentioned gaps through the proposed functional modeling of the assessment of the innovation potential of the region in the national security system.

Our methodology is based on the application of the functional modeling method from the IDEF family. Thus, the IDEF0 toolkit itself is a more formal approach to building functional models, which is described as a clear system that converts resources into results under the influence of rules and constraints. Functions are displayed in the form of certain blocks, which can be conditionally designated as “A,” connected by arrows, which allows us to clearly show cause-and-effect relationships, decision points, data dependencies and standards. We start with a context diagram of level A0, where the system boundaries, key inputs, controls, mechanisms and expected outputs are established, after which the model is sequentially

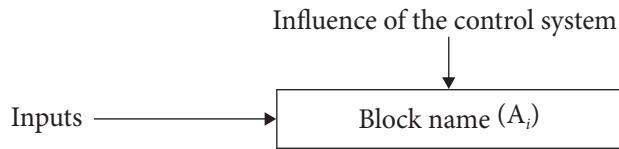


Fig. 2. Interrelated reasons that require the implementation of the region's innovation potential in the national security system

Source: developed by authors.

detailed, revealing complex functions into sub-functions in the form of a hierarchy (Fig. 2).

Along with this, the ICAM method should also be taken into account. The auxiliary method ICAM (Integrated Computer Aided Manufacturing) is used because it was within this program that the IDEF0 logic was formed as a disciplined way of describing functions, flows and resources in complex organizational and technological systems.

It should be emphasized that IDEF0 is a functional method for describing complex systems, in which each process is modeled not as a “black box,” but as a function of transforming inputs according to certain rules into measurable outputs with the involvement of specific execution capabilities. Formally, the process A_i is represented by a tuple (1):

$$A_i \equiv \langle I_i, C_i, O_i, M_i, f_i \rangle, \quad (1)$$

In a multilevel representation, the upper process A_0 is decomposed into subprocesses $A_1, \dots, A_3$ with the condition of balancing interfaces (2):

$$A_0 = \bigotimes_{k=1}^3 A_k. \quad (2)$$

ICAM sets a culture of standardization, interoperability and documentation, forces to clearly record requirements, constraints, roles and artifacts at each stage of modeling. Thanks to this, IDEF0 is not reduced to “process pictures,” but turns into a controlled cycle of analysis and design, suitable for both production systems and public administration.

From a theoretical point of view, IDEF0 is preferable here to BPMN, System Dynamics and standalone MCDA because the core research problem is the formal structuring of assessment functions and governance interfaces, rather than only event sequencing, dynamic simulation or ranking. BPMN is highly effective for describing executable workflows and event-driven coordination, but it is less explicit in separating inputs, controls, outputs and enabling mechanisms for analytical governance. System Dynamics is powerful for feedback loops, delays and scenario simulation, yet it presupposes a deeper level of parameter calibration than is currently available for a first-stage regional security assessment framework. MCDA remains essential,

Table 1. Main Gaps in the Scholarly Research and Practical Literature

Main gap	Consequences
Lack of a unified, reproducible methodology for assessing the region's innovation potential specifically in the context of national security	Split resources, incommensurability of results between regions, weak prioritization and slow decision-making
Insufficient integration of institutional, legal, organizational, and technological dimensions (predominance of “silo” analysis)	Inconsistency of policies with real security needs, regulatory barriers to innovation, loss of time for coordination
Lack of standardized data and metrics at the regional level (capability indicators, level of technological readiness, personnel competencies, financial viability)	Limited monitoring and comparison capabilities, high risk of errors in the selection of projects and support mechanisms
Imperfect logic for managing a portfolio of projects and dual-purpose solutions (civilian/defense), lack of transparent ranking criteria	Duplication of initiatives, underfunding of critical areas, weak accountability and transparency for stakeholders

Source: developed by authors.

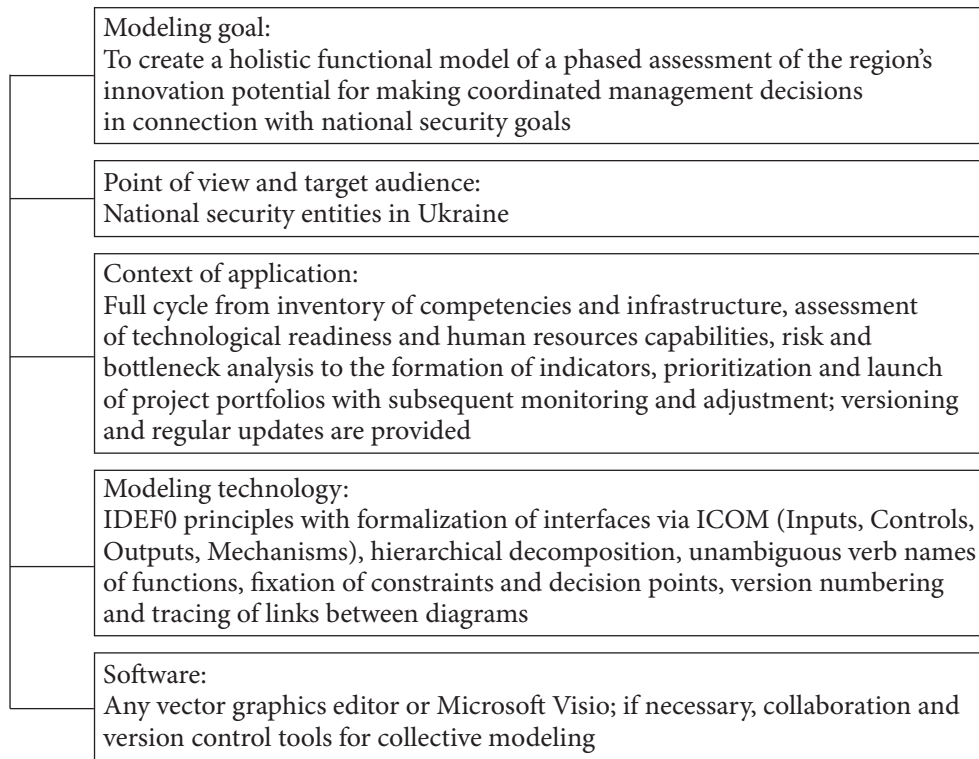


Fig. 3. The main basic conditions for developing a functional model for ensuring the implementation of the assessment of the innovation potential of the region in the system of ensuring national security

Source: developed by authors.

but mainly at the stages where already validated indicators and alternatives must be weighted and prioritized. For this reason, we see IDEF0 as the primary architectural language.

To begin with, let's form A0 in the context of further functional modeling. Thus, in our case, A0 models the managed process "Assess the innovation potential of the region in the system of ensuring national security," which covers the full cycle. For reproducibility, versioning of diagrams, clear tracing rules between levels A0 → A1—A3 and regular updating of the model in accordance with changes in the external environment are assumed. Let's highlight the main basic conditions for developing a functional model for ensuring the implementation of the assessment of the innovation potential of the region in the system of ensuring national security (Fig. 3).

Next, we form the ICOM (Inputs–Controls–Outputs–Mechanisms) model as an introductory framework for IDEF0 functional modeling. Thus, it clearly captures what exactly feeds the evaluation process (inputs), what norms and strategies it is guided by (control), what measurable results it should generate (outputs), and who and with what (mechanisms) ensures the performance of functions (Fig. 4).

Next, we provide a description of the stages (A1—A3) of the IDEF0 model for assessing the innovation potential of the region in the national security system:

A1. Data identification and normalization, setting criteria and system boundaries. The first stage involves the formation of a complete register of data sources and activities. This also includes measures to define the boundaries of analysis and stan-

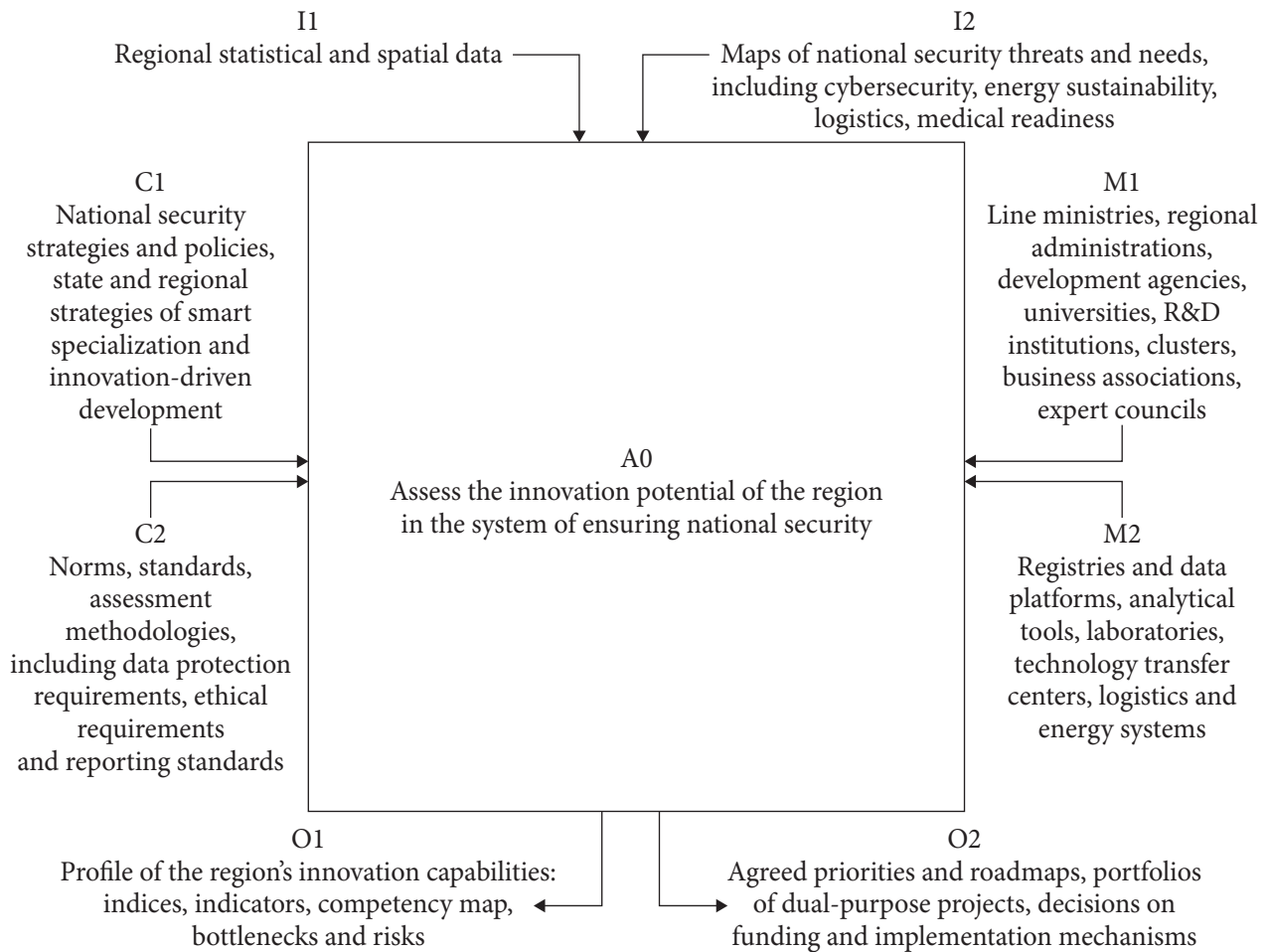


Fig. 4. The main basic conditions for developing a functional model for ensuring the implementation of the assessment of the innovation potential of the region in the system of ensuring national security
Source: developed by authors.

dardize terms, formats, and rules for accessing information, which shape the information security paradigm. In parallel, criteria and metrics for assessing innovation potential in the context of national security are being developed. The final result of A1 is a validated and transparent set of “inputs” and “controls” for a number of steps, such as a data catalog with descriptions of quality and sources, a dictionary of indicators for calculation methods, and a register of standards and strategies.

A2. Assessment of capabilities and problem areas, building a profile of the region. The second stage transforms the collected “inputs” into a structured

profile of the region’s innovation capabilities, using criteria agreed with A1. Analysis is performed at the level of functions and subfunctions. For each block, strengths, “bottlenecks,” risks, as well as capabilities for rapid conversion and scaling of dual-purpose solutions are determined. The output is an integral index and thematic sub-indices, a map of competencies and dependencies, a matrix of risks and readiness for implementation, reflecting the cause-and-effect relationships between the region’s innovation activity and national security goals.

A3. Prioritization and list of solutions, roadmaps and rules of engagement. The third stage transla-

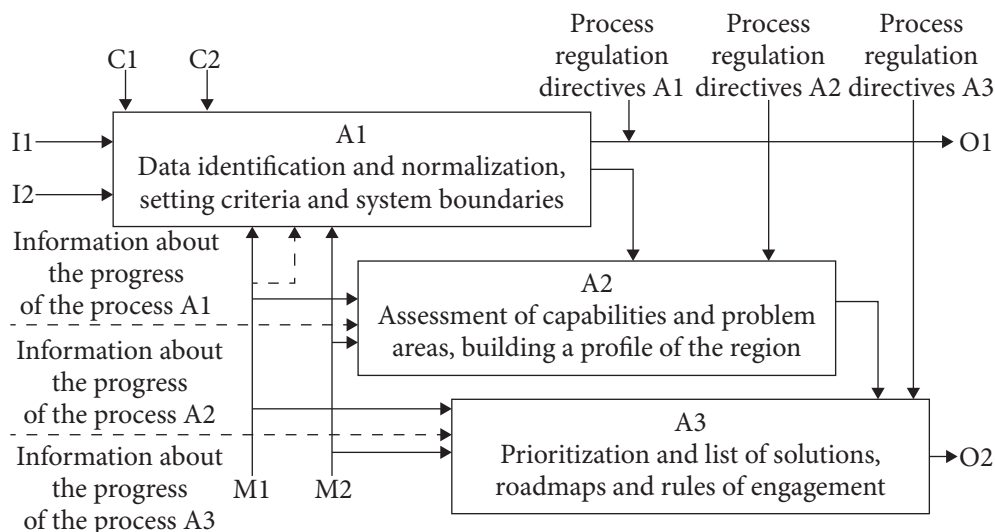


Fig. 5. Decomposition of the first level of the IDEF0 context diagram for ensuring the implementation of the assessment of the innovation potential of the region in the system of ensuring national security
Source: developed by authors.

tes the capability profile into specific management actions. Thus, a ranked portfolio of projects and reforms is formed with transparent criteria. Roadmaps with milestones, resource models, responsible institutions and co-financing mechanisms are developed. The “outputs” of A_3 are, in essence, agreed priorities, a portfolio of dual-function initiatives, a set of performance indicators and implementation rules to directly ensure the achievement of A_0 (Fig. 5).

Directives and process information are needed to transform the assessment from a one-off analytical exercise into a manageable, repeatable and accountable cycle. Together, they provide a common “language” for all participants, reduce the risk of errors and conflicts of interpretation, accelerate decision-making, and allow for comparison of results across regions and over time (Table 2).

The advantage of IDEF0 is that any block A1—A3 can be formally detailed to the second and further levels, revealing a complex function into subfunctions with clear “inputs,” “controls,” “mechanisms” and “outputs.” This kind of decomposition allows us to localize responsibility, accurately specify the

necessary data and standards for each substep. We demonstrate this for A2 (Fig. 6).

A21. Calculating indicators and merging data into a single analytical set. In sub-step A21, we transform the sources prepared in A1 into a unified analytical array. The result is a verified dataset at the region-sector-function level, ready for capability profiling, with full formula traceability and a data quality log.

A22. Mapping capabilities and identifying threats. A22 transforms an array of analytical data into a structured system of ideas about real possibilities. The result is a regional capabilities atlas, listing the strengths, risks, and specific threats associated with individual institutions and response timeframes.

A23. Integral assessment and expert validation of the region's profile. At A23, we aggregate normalized indicators into thematic sub-indices and an integral index of innovation capabilities, perform sensitivity analysis to weights and thresholds, and form a matrix of readiness for implementation. The output is an approved regional capabilities passport.

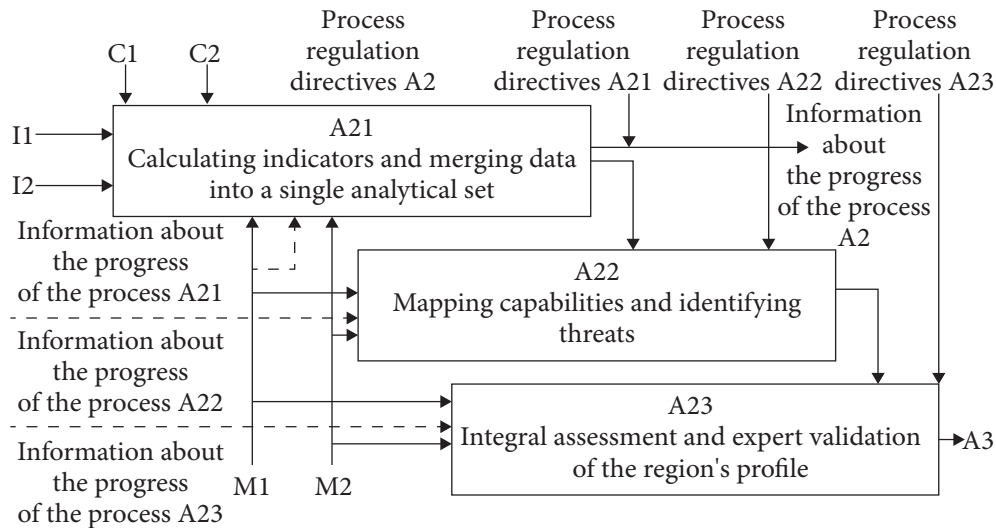


Fig. 6. Decomposition of the second level (A2) of the IDEF0 context diagram for ensuring the implementation of the assessment of the innovation potential of the region in the system of ensuring national security
Source: developed by authors.

Table 2. Process Regulation Directives and Progress Information A1—A3

A	Regulatory guidelines	Progress information
A1	◆ Mandatory approval of indicators and calculation methods; ◆ Approval of weighting factors and procedures for their revision; uniform data and metadata formats; ◆ Rules for integrating sources; ◆ Policy for protecting personal data and commercial secrets; ◆ Protocol for resolving indicator conflicts	◆ Coverage of the source register (%), date of last update; ◆ List and status of approved boundaries (territory/period/sectors); ◆ Report on compliance with formats and metadata (proportion of records that comply with the standard)
A2	◆ Mandatory piloting in at least three typologically different regions; ◆ Feedback-based calibration protocol for thresholds and weights; ◆ Standardized testing scenarios for panels and reports	◆ Values of the integral index and sub-indexes (with confidence intervals/sensitivity to weights); ◆ Map of competencies and dependencies (version, date); ◆ Matrix of risks and readiness (list of critical risks, responsible parties, response times); ◆ List and status of identified “bottlenecks”
A3	◆ Approved regulations of roles and responsibilities; ◆ Schedule for updating data, weights and methodologies; ◆ Standards for public reporting and open data; ◆ Information protection, backup and recovery policies	◆ Ranked list of projects with justification of points and funding sources; ◆ Status of roadmaps (percentage of milestones completed, overdue tasks); ◆ KPI performance indicators (actual vs. plan, warning signals); ◆ Minutes of coordination meetings and decisions made

Source: developed by authors.

Our approach fundamentally shifts the focus from technological or legal subsystems to a guided process of assessing the region's innovation potential in direct relation to national security goals, formalized in IDEF0 with the ICOM introductory model and clear stages A1—A3. Unlike works that are dominated more by the description of architectures or algorithms without process decomposition, we introduce transparent interfaces of “inputs,” “controls,” “outputs” and “mechanisms,” data standards, weighting factors and prioritization rules, which makes the results reproducible between regions and suitable for institutionalization. As emphasized by O. Ilyash et al. [16], the predictive model of the impact of technological growth components on economic security provides valuable quantitative optics, but does not set a procedural framework for data collection and validation and does not establish a regulation of institutional interaction; in our case, these issues are resolved by stages A1 (standardization) and A3 (regulation, monitoring). As demonstrated by the results of A. J. Saleh et al. [17], ensuring proper legal governance of cryptoassets is an important element of national security. In our case, the results of the study integrate the legal dimension as “governance” into ICOM, while combining it with data, mechanisms, and outputs at the regional level.

At the level of implementing regional methodologies, O. Raevneva [18] systematizes existing approaches to the economic security of regions and assessment technologies. However, the results of the study are limited to individual indicators. Our study is somewhat expanded, since it includes a process superstructure that combines indicators with roadmaps and procedures for portfolio selection of dual-functional solutions. The results of the study by D. Stadelmann et. [19] prove that the human resources potential of politicians and representatives of the military sphere has a direct impact on security policy. We believe that this factor is important, but not contextual, since it does not neutralize the role of a transparent da-

ta and process architecture. Our study also takes this factor into account, but as an element of “mechanisms” and “management,” without changing the procedural logic. Ultimately, according to Y. Bekh et al. [20], the factor of creative leadership is also important in the context of change management. However, in our opinion, without establishing and maintaining a standardized process and metrics, even the most advanced creative leadership can be ineffective. In this context, our approach also includes this element, but as part of the operational cycle.

Summarizing the results of our research, we note that we managed to substantiate that the assessment of the innovation potential of the region is an integral element of the system of ensuring national security, since it directly affects the protection of sovereignty, territorial integrity, democratic constitutional order and other national interests. The functional model IDEF0 proposed by us with the introductory model ICOM provides a controlled decomposition of the process from defining boundaries, criteria and data standards to the formation of portfolios of dual-functional solutions, roadmaps and regulations of interaction between all subjects of ensuring national security. Thus, the phased logic A1—A3 creates a reproducible circuit that connects indicators of innovation with specific management actions. As a result, we obtain an effective methodological approach that eliminates key gaps at the junction of institutional, organizational and technological aspects, moves the discussion from the level of general declarations to operationally managed practices and provides a basis for comparability of regions and accountability of decisions.

However, not everything was achieved within the framework of this article. Therefore, the prospects for further research will be to study the impact of the growth of corruption, leadership and motivation systems on the speed of scaling innovations, in particular through comparative case studies of regions of different types.

REFERENCES

1. Prav, R. (2021). Ways to improve the efficiency of mechanisms for ensuring the national security of Ukraine in the context of European experience. *Scientific Perspectives*, 9(15), 197—206. [https://doi.org/10.52058/2708-7530-2021-9\(15\)-197-206](https://doi.org/10.52058/2708-7530-2021-9(15)-197-206)
2. Rushchyshyn, N., Medynska, T., Nikonenko, U., Kostak, Z., Ivanova, R. (2021). Regulatory and legal component in ensuring state's financial security. *Business: Theory and Practice*, 22(2), 232—240. <https://doi.org/10.3846/btp.2021.13580>
3. Kryshtanovych, M., Panfilova, T., Khomenko, A., Dziubenko, O., Lukashuk, L. (2023). Optimization of state regulation in the field of safety and security of business: a local approach. *Business: Theory and Practice*, 24(2), 613—621. <https://doi.org/10.3846/btp.2023.19563>
4. Avdeev, V., Avdeeva, O., Rozenko, S., Kiselev, E., Kuleshov, I., Morozov, A. (2021). Current directions of legal ensuring national security. *Cuestiones Políticas*, 39(69), 373—385. <https://doi.org/10.46398/cuestpol.3969.23>
5. Kryshtanovych, M., Antonova, L., Filippova, V., Dombrovska, S., Pidlisna, T. (2022). Influence of COVID-19 on the functional device of state governance of economic growth of countries in the context of ensuring security. *International Journal of Safety and Security Engineering*, 12(2), 193—199. <https://doi.org/10.18280/ijssse.120207>
6. Beglytsia, V., Antonova, L., Kozlova, L., Datsii, O., Datsii, N. (2021). System of concepts communications of state institutions and society as the basis of national security and socio-economic stability. *Financial and Credit Activity: Problems of Theory and Practice*, 3(38), 549—556. <https://doi.org/10.18371/fcaptp.v3i38.237487>
7. Kruk, S. (2019). *Institutional development of public administration in the field of ensuring national security of Ukraine*: Doctor of Science in Public Administration: 25.00.05 “Public administration in the field of state security and public order.” NUCSU. Kharkiv. URL: <https://nuczu.edu.ua/images/topmenu/science/spetsializovani-vcheni-rady/diskruk.pdf> (Last accessed: 20.12.2025).
8. Sytnyk, G. (2011). Institutional and civilizational paradigm of research of problems and public administration aspects of national security. *Bulletin of the National Academy for Public Administration under the President of Ukraine*, 2, 25—34. URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe? (Last accessed: 03.02.2026).
9. Dumchykov, M., Utkina, M., Bondarenko, O. (2022). Cybercrime as a threat to the national security of the Baltic States and Ukraine: The comparative analysis. *International Journal of Safety and Security Engineering*, 12(4), 481—490. <https://doi.org/10.18280/ijssse.120409>
10. Polishchuk, O., Bobrova, Y., Bobrov, Y. (2021). The formation of a safety ecosystem in the context of ensuring the national homeland security. *International Journal of Safety and Security Engineering*, 11(6), 683—689. <https://doi.org/10.18280/ijssse.110608>
11. Melnychuk, L., Andriichuk, Y., Chaltseva, O., Shtyrov, O., Yevtushenko, I. (2023). Countering threats to effective management of personnel potential in the public administration system. *Financial and Credit Activity Problems of Theory and Practice*, 2(49), 426—434. <https://doi.org/10.55643/fcaptp.2.49.2023.4009>
12. Yemanov, V., Belay, S., Sporyshev, K. (2022). Information-analytical method of improving the efficiency of technical intelligence of the technical support units of the National Guard of Ukraine. *Collection of scientific papers of the National Academy of the National Guard of Ukraine*, 1(39), 104—110. <https://doi.org/10.33405/2409-7470/2022/1/39/263376>
13. Verbivska, L., Lagodiienko, V., Filyppova, S., Papaika, O., Malin, O., Neustroiev, Y. (2022). Regulatory policy of the entrepreneurship development as a dominant of economic security of the national economy. *International Journal of Safety and Security Engineering*, 12(5), 543—552. <https://doi.org/10.18280/ijssse.120501>
14. Bielai, S., Antonova, L., Hololobov, S., Yevtushenko, I., Sporyshev, K. (2024). The impact of a practice-oriented paradigm on public administration and national security. *International Journal of Sustainable Development and Planning*, 19(1), 277—288. <https://doi.org/10.18280/ijssdp.190126>
15. Bobrova, Y., Bobrov, Y., Vavreniuk, S., Bondarenko, O. (2024). Algorithmic framework for an information system ensuring sustainable development and national security. *Ingénierie des Systèmes d'Information*, 29(1), 153—159. <https://doi.org/10.18280/isi.290117>

16. Ilyash, O., Lupak, R., Kravchenko, M., Trofymenko, O., Duliaba, N., Dzhadan, I. (2022). A forecasting model for assessing the influence of the components of technological growth on economic security. *Business: Theory and Practice*, 23(1), 175—186. <https://doi.org/10.3846/btp.2022.15298>
17. Saleh, A. J., Alazzam, F. A. F., Rabbo Aldrou, K. K. A., Zavalna, Z. (2020). Legal aspects of the management of cryptocurrency assets in the national security system. *Journal of Security & Sustainability Issues*, 10(1), 235—247. [https://doi.org/10.9770/jssi.2020.10.1\(17\)](https://doi.org/10.9770/jssi.2020.10.1(17))
18. Rayevnyeva, O. (2019). *Economic security of the regions: Comparative analysis of approaches and construction of the technology of assessment*. In: Theoretical and Methodological Approaches to the Formation of a Modern System of Enterprises, Organizations and Institutions' Development: Collective Scientific Monograph (1st edition). Dallas, USA. <https://doi.org/10.36074/tmfmseoid.ed-1.16>
19. Stadelmann, D., Portmann, M., Eichenberger, R. (2015). Military careers of politicians matter for national security policy. *Journal of Economic Behavior & Organization*, 116, 142—156. <https://doi.org/10.1016/j.jebo.2015.04.001>
20. Kryshchanovych, M., Bekh, Y., Zhyzhko, T., Povstyn, O., Molnar, O. (2025). The role of creative leadership in change management. *Creativity Studies*, 18(2), 506—522. <https://doi.org/10.3846/cs.2025.22189>
21. OECD. (2011). *Regions and Innovation Policy*. OECD Publishing. <https://doi.org/10.1787/9789264097803-en>
22. OECD. (2024). *Innovation diffusion: A practical handbook for implementing policies in regions*. OECD Publishing. URL: https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/12/innovation-diffusion_55ddc906/959acfec-en.pdf (Last accessed: 03.02.2026).
23. European Commission, Directorate-General for Research and Innovation. (2024). *European Innovation Scoreboard 2024*. URL: https://research-and-innovation.ec.europa.eu/knowledge-publications-tools-and-data/publications/all-publications/european-innovation-scoreboard-2024_en (Last accessed: 04.01.2026).
24. Paulk, M. C., Curtis, B., Chrissis, M. B., Weber, C. V. (1993). *Capability Maturity Model for Software, Version 1.1*. Software Engineering Institute, Carnegie Mellon University, CMU/SEI-93-TR-24.
25. Cinelli, M., Kadziński, M., Miebs, G., Gonzalez, M. (2020). How to support the application of multiple criteria decision analysis? Let us start with a comprehensive taxonomy. *Omega*, 96, 102261. <https://doi.org/10.1016/j.omega.2020.102261>
26. Costa, J., Silva, M. (2024). Multicriteria Decision-Making in Public Security: A Systematic Review. *Mathematics*, 12(11), 1754. <https://doi.org/10.3390/math12111754>

Received 25.09.2025

Revised 25.03.2026

Accepted 10.04.2026

М.Ф. Криштанович¹ (<https://orcid.org/0000-0003-1750-6385>),
В.М. Пасічник¹ (<https://orcid.org/0000-0002-2447-2374>),
Л.П. Бондаренко¹ (<https://orcid.org/0000-0002-3313-3569>),
Л.І. Данчак¹ (<https://orcid.org/0000-0001-8768-7543>),
Л.М. Щеховська² (<https://orcid.org/0000-0002-6119-166X>)

¹ Національний університет «Львівська політехніка»,
вул. С. Бандери, 1, 79000, Львів, Україна
+380 32 258 2282, coffice@lpnu.ua

² Державний університет «Київський авіаційний інститут»,
просп. Любомира Гузара, 1, 03058, Київ, Україна,
+380 44 406 7901, post@kai.edu.ua

КОНЦЕПТУАЛЬНЕ ФУНКЦІОНАЛЬНЕ МОДЕЛЮВАННЯ ОЦІНКИ РЕГІОНАЛЬНОГО ІННОВАЦІЙНОГО ПОТЕНЦІАЛУ В СИСТЕМІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Вступ. Інновації є критичною умовою стійкості та відновлення регіонів України навіть попри пандемію COVID-19 і повномасштабне збройне вторгнення російської федерації, адже безпосередньо зміцнюють захищеність суверенітету, територіальної цілісності та демократичного конституційного ладу. Кожна область має власний інноваційний і безпековий потенціал, який слід розкривати через системне оцінювання як відправну точку для пріоритизації інвестицій та узгодження з цілями національної безпеки.

Проблематика. Відсутній узагальнений, простий у використанні та відтворюваний методичний підхід, що комплексно відображає сам процес оцінювання інноваційного потенціалу саме в контексті забезпечення національної безпеки, через що виникають розпорошення ресурсів, дублювання зусиль і повільне впровадження рішень. Необхідною є розробка функціональної моделі оцінювання на основі IDEF0 (*Integration Definition for Function Modeling*), яка структурує входи, виходи, керування і механізми, забезпечуючи узгоджені управлінські рішення та прозорі критерії відбору проєктів.

Мета. Обґрунтувати і побудувати на основі функціонального моделювання IDEF0 декомпозицію поетапного процесу оцінювання інноваційного потенціалу регіону в системі забезпечення національної безпеки для прийняття узгоджених та максимально ефективних управлінських рішень.

Матеріали й методи. Застосовано функціональне моделювання IDEF0 із побудовою контекстної діаграми та ієрархічної декомпозиції функцій, спираючись на принципи програми ICAM.

Результати. Запропоновано методичний підхід на основі IDEF0 з моделлю ICOM і етапами A1—A3, що формує стандартизовані дані, узгоджені метрики, профіль спроможностей, ранжований портфель рішень і дорожні карти їх реалізації.

Висновки. Оцінювання інноваційного потенціалу регіону є необхідною умовою зміцнення національної безпеки, бо напряму переводить стратегічні цілі у керовані, перевірені дії.

Ключові слова: національна безпека, модель IDEF0, інновації, інноваційний потенціал, регіони.