International Journal of Religion
2024
Volume: 5| Number 9 | pp. 760 – 771
ISSN: 2633-352X (Print) | ISSN: 2633-3538 (Online)
ijor.co.uk
DOI: https://doi.org/10.61707/p60brq41

Scientific and Methodological Approach to Strengthening Intellectual Security and Human-Centricity through Optimizing the Use of Artificial Intelligence

Svitlana Kryshtanovych[1], Tetiana Tatarnikova[2], Svitlana Rybkina[3], Olena Kopanchuk[4] and Vladimir Motorny[5]

Abstract

The main goal of the article is to form a new modern approach to ensuring intellectual security by optimizing the use of artificial intelligence. The object of the research is the intellectual security system and modern technologies based on artificial intelligence. The research methodology involves the use of the modern IDEF0 method, which facilitates the process of optimizing the use of artificial intelligence, as well as the method of expert analysis and the Delphi method. As a result of using the above methods, decompositions of models for ensuring intellectual security were built. The innovativeness of the results obtained is revealed through careful information support for the detailing of the proposed IDEF0 model, which consists of a detailed presentation of the first and second level models, which provide information for strengthening human-centricity, and the 3rd level model, which provides information on the optimization of artificial intelligence.

Keywords: *Intellectual Security, Modeling, Information Technology, Human-Centricity, Artificial Intelligence*

INTRODUCTION

In the era of relentless technological progress, artificial intelligence (AI) occupies a special place, which becomes not only a tool for development and innovation, but also a potential threat to the intellectual security of society. The use of AI opens up new prospects for improving human activity, but also requires a thorough analysis of the risks and challenges that may arise as a result of its uncontrolled spread. Thus, the importance of a scientific and methodological approach to strengthening intellectual security and ensuring human-centricity through optimizing the use of AI becomes obvious.

It should be noted that in today's development conditions, the issue of human-centricity and how to effectively manage one's own human resources has reached a new level due to significant changes in the external environment. Consequently, the problem that has arisen is revealed due to the rapid development of digital technologies, which have brought a new vision of how one can rethink one’s own processes and activities. This became possible due to the use of artificial intelligence technologies. Its sudden appearance in the mass market has created a boom that has become a primary threat to intellectual security and the definition of man's place in it. There have been many controversial issues and debates about how to apply artificial intelligence in a way that preserves human-centricity as such. Optimizing the use of artificial intelligence at different levels of human activity. It is still ongoing, and therefore, in our opinion, this issue should continue to be investigated.

Strengthening intellectual security through optimizing the use of AI requires a comprehensive approach that brings together scientists, technologists, human rights activists and policymakers. Only through joint efforts can we develop effective control and regulatory mechanisms that will not only prevent possible threats, but will also contribute to the positive development of AI technologies, taking into account the interests and needs of humans.

[1] Department of Pedagogy and Psychology, State University of Physical Culture named after Ivan Bobersky, Lviv, 59013, Ukraine E-mail: svitlana.kryshtanovych@gmail.com

[2] Security Service of Ukraine The Ukrainian scientific and research Institute of special equipment and forensic expertise, Kyiv, 03113, Ukraine

[3] Department of public management and law, Communal Institution of Higher Education “Dnipro Academy of Continuing Education” of Dnipropetrovsk Regional Council, Dnipro, 39000, Ukraine

[4] Education center of the national university of civil protection of Ukraine, Kharkiv, 49000, Ukraine

[5] Department of units daily activities management, Odesa Military Academy, Odesa, 51000, Ukraine

Thus, a scientific and methodological approach to strengthening intellectual security and human-centricity through optimizing the use of AI is not only an important, but also a necessary step towards creating a harmonious and safe digital future, where technologies serve for the benefit of people without compromising their fundamental rights and freedom.

The main goal of the article is to form a new modern approach to ensuring intellectual security by optimizing the use of artificial intelligence. The object of the research is the intellectual security system and modern technologies based on artificial intelligence.

The structure of the article includes a detailed review of the literature, a description of the methodology, a review of relevant literature, a presentation of the results and their discussion and comparison. At the end of the study, conclusions were presented.

LITERATURE REVIEW

The study of existing sources and literature occupies a key place in the scientific research process, since it allows project participants to better understand the scope of artificial intelligence and intellectual security, identify existing knowledge gaps and identify directions for further research. A preliminary literature review contributes to the development of a sound theoretical framework necessary for the development of valid and effective models. Studying and analyzing existing publications, studies and theories not only helps to provide a proper scientific foundation for one's work, but also provides a link between new results and what is already known in the field. This creates the conditions for more effective contributions to the scientific community, allowing not only to present new discoveries, but also to adequately fit them into the context of existing knowledge.

Thus, in a study by Fan, et al. (2020) focuses on the importance of the relationship between brain science and the development of artificial intelligence, emphasizing the importance of an interdisciplinary approach to improving AI. In the context of our research, this connection can serve as a basis for the development of new methods for optimizing the use of AI within the framework of intelligent security, taking into account human aspects and behavioral patterns.

At the same time, a study by Schukajlow, et al. (2018) emphasizes mathematical modeling and emphasizes the value of empirical research in understanding and improving adaptation processes of new technologies. Today, these modeling methods are very effective in developing methodological approaches to training enterprise personnel in methods of optimizing the use of AI to improve intellectual safety.

Haenlein and Kaplan (2019) offer an overview of the development of artificial intelligence and its impact on society, which is useful for understanding current trends and challenges in the application of AI. In the context of our study, the historical context helps to identify security issues that have arisen in the past and take them into account when developing modern AI optimization methods. The Hirschheim (2012) study appears to provide an in-depth historical analysis of the development of information systems, which can serve as a basis for understanding how information technology and AI have influenced and can influence the intellectual security of organizations.

Van Engelenburg, et al. (2019) focus on the importance of context-aware systems that can automatically adapt to changes in their environment. Such systems have significant potential for intelligent security because they can more accurately identify and respond to potential threats in real time. In the context of our study, the development of AI-based context-aware systems can significantly enhance the protection of enterprise information assets.

The article by Roztocki, et al. (2019) explores the impact of information and communication technologies on socio-economic development, which provides a broader context for understanding the importance of AI not only as a security tool, but also as a means of increasing the efficiency and competitiveness of enterprises. From a research perspective, these insights can be used to develop strategies to optimize the use of AI that will contribute to intellectual security and overall enterprise growth.

A study by Rudra, et al. (2018) reveal the importance of information and communications technology (ICT) infrastructure for economic growth using data from different countries. In the context of our study, the link between ICT infrastructure and economic development can serve as a basis for arguing the importance of optimizing the use of AI in business as a key element for strengthening intellectual security and increasing competitiveness.

Vial (2019) article explores the essence of digital transformation and identifies directions for further research in this area. In the context of our work, an overview of the aspects of digital transformation and its impact on the strategic positioning of companies can help to better understand how the integration of AI in business models contributes to innovative development and strengthening intellectual security.

A study by Alvarez, et al. (2016) analyzes how crisis situations affect assimilation and differences in technological development. This source can provide insights on how businesses can adapt the use of AI to strengthen their intellectual security in the face of uncertainty and economic challenges. Similar research by Baesu, Bejinaru (2020) highlighting knowledge management strategies for leadership in a digital business environment. This source highlights the importance of knowledge management as part of the process of optimizing the use of AI, which can lead to better intelligence and improved organizational performance.

Abbass paper (2014) explores the integration of artificial intelligence into social systems, focusing on function, automation, and interaction between humans and autonomous systems. In the context of our research, this work provides valuable insights on the importance of developing AI systems that promote human-centeredness and provide a high level of intellectual safety, taking into account trust and ethical aspects of the interaction between people and technology.

Amershi et al. (2014) research focuses on the role of humans in the interactive learning process of machines, emphasizing the importance of human contributions to the development and improvement of AI algorithms. This approach resonates with our research because it highlights the need for human-centric models for optimizing the use of AI, where human knowledge and expertise serve as the basis for ensuring the safety and efficiency of intelligent systems.

Despite the large number of existing literature sources and scientific developments in the field of ensuring intellectual security and the use of artificial intelligence, our analysis found that this topic still contains scientific gaps that require further in-depth study (Table. 1).

Table 1. Main scientific gaps in the existing literature on the topic under study

Scientific gap	Essence
Integrating a Human-Centric Approach into the Development and Implementation of AI in Enterprises	There is a significant dearth of research that examines in detail methods and strategies for integrating human-centric principles into the development, implementation, and use of AI in business operations. This means a deeper understanding of how AI technologies can respect and protect the rights and interests of workers and customers, and help improve the quality of the work environment and service, is required.
Development of methods for assessing intellectual security risks when using AI	The need to develop comprehensive methods that make it possible to effectively assess the risks of intellectual security associated with the implementation and use of artificial intelligence in enterprise activities. Such methodologies should include analysis of the potential impact of AI on data privacy, intellectual property protection, and preventing the leakage of corporate information.
Creating models for optimizing the use of AI to improve enterprise competitiveness while ensuring intellectual security	A gap has been identified in research on models that demonstrate how optimizing the use of AI can simultaneously strengthen intellectual security and improve the competitiveness of companies. Models need to be developed to enable enterprises to leverage the benefits of artificial intelligence to innovate, optimize processes and improve productivity without compromising the security of their intellectual assets and data

Despite significant advances in this field, there is a need for more research to develop more effective methods and models to enable enterprises to effectively manage their competitiveness and intellectual security using artificial intelligence technologies. This need underscores the importance of our research to develop and implement innovative approaches that can fill existing gaps in knowledge and practice. Thus, the scientific objective of the article is to present the author's vision of ensuring intellectual security through optimizing the use of artificial intelligence technologies.

METHODOLOGY

Our research methodology is a comprehensive approach that integrates various analysis methods to optimize the use of artificial intelligence to strengthen intelligent security. This approach combines the IDEF0 method for modeling business processes, the expert analysis method for expert opinion, and the Delphi method for achieving consensus among experts. This multifaceted methodology allows for in-depth analysis and determination of the most effective ways to apply AI in enterprises to maximize the benefits of intelligent security.

The IDEF0 method is based on the idea of creating structured models that reflect the relationships between different functions in the system. Designed as a tool for modeling business processes, IDEF0 allows you to analyze and optimize enterprise operations in detail in the context of the use of artificial intelligence. Its application in the study helps identify key areas that require improvement to improve intelligent safety, including the development of clear guidelines for the implementation and operation of AI.

The expert analysis method used in the study allows us to attract the experience and knowledge of specialists in the field of artificial intelligence and intellectual security. This method ensures that a wide range of opinions and ideas are collected, which contributes to a deeper understanding of the potential risks and opportunities associated with the use of AI in enterprises. Analysis of expert opinions helps to identify key areas for further research and development of recommendations.

As part of the expert research methodology, 30 experts were involved, each of whom has significant experience and high qualifications in the field of ensuring intellectual security and the use of artificial intelligence in enterprise management systems and increasing its competitiveness. The selection of experts is based on their professional experience, academic achievements and contributions to the development of relevant research areas. The peer review process was conducted in full compliance with ethical standards and principles of peer review, ensuring confidentiality, objectivity of assessments and respect for the professional views of participants. All participants are properly informed of the aims and objectives of the study and how their responses and analysis will be used. This approach not only facilitates the collection of high-quality and valid data, but also ensures a high level of trust and openness between researchers and experts, which is key to the successful conduct of expert research.

To objectify our research and the possibility of practical implications, we chose a specific enterprise that uses elements of artificial intelligence in its activities and requires optimization of intellectual security - the NovaPost enterprise.

The Delphi method, in turn, is used to achieve consensus among experts on issues that caused disagreement during expert analysis. This method provides an iterative process of discussion in which experts revise their preliminary assessments based on an anonymous exchange of views, allowing for greater agreement on complex issues. The use of the Delphi method in the study is aimed at forming a consensus expert opinion on the most effective strategies for optimizing the use of artificial intelligence to strengthen intellectual security. This method makes an important contribution to the process of guideline validation, ensuring high reliability and acceptability for a wide range of specialists.

The combination of these methods creates a powerful methodological basis for research, allowing not only to analyze existing processes and identify potential risks, but to develop innovative solutions to improve intellectual safety. This approach provides a deep understanding of the challenges facing enterprises in the context of artificial intelligence and helps develop effective strategies to overcome them.

Each of the methods used has its own advantages and disadvantages. The IDEF0 method provides high visualization and structuring of processes, but can be labor-intensive to implement and requires deep knowledge in the field of modeling. The expert analysis method allows you to collect a wide range of opinions, but may encounter subjectivity in assessments. The Delphi method helps to achieve consensus, but its effectiveness lies in the ability to correctly organize the process of discussion and analysis of expert opinions. Using these methods in combination minimizes their disadvantages and enhances their advantages, providing an integrated and multifaceted approach to research.

RESULTS AND DISCUSSIONS

Before starting the simulation, we set ourselves the goal of "Achieving intellectual security at NovaPost". For this purpose, the key blocks/processes that will allow it to be achieved were singled out (through expert analysis, their list was summarized to the 4 most important ones). For the modeling process, let's set the mathematical notation of the key target as S0. At the same time, to achieve it, equality (1) must be fulfilled:

$$S0=\{S1;S2;S3.....Sn\} \tag{1}$$

Thus, we will highlight the 4 most significant blocks of achieving S0:

S1. Ensuring the protection of intellectual potential at the enterprise. This block focuses on safeguarding NovaPost's intellectual assets, which include patents, trade secrets, and proprietary knowledge. Implementing robust cybersecurity measures, securing intellectual property rights, and fostering a culture of confidentiality among employees are essential steps. The goal is to prevent unauthorized access, theft, or leakage of critical information that could compromise the company's competitive edge and innovation capabilities.

S2. Preservation of people-centeredness at the enterprise. At the heart of NovaPost's success is its commitment to maintaining a people-centered approach. This strategy emphasizes the importance of valuing and investing in the workforce as the key drivers of innovation and productivity. By fostering an inclusive, supportive, and engaging work environment, NovaPost aims to attract and retain top talent, encourage creativity, and ensure employee well-being, which in turn, contributes to the overall intellectual security and resilience of the organization.

S3. Formation of an artificial intelligence management system. Recognizing the transformative power of artificial intelligence (AI), this block involves the creation of a sophisticated AI management system to streamline operations, enhance decision-making, and unlock new avenues for innovation. By integrating AI into its core processes, NovaPost seeks to optimize efficiency, improve predictive analytics, and foster a culture of continuous learning and adaptation, ensuring that the enterprise stays at the forefront of technological advancements.

S4. Building a digital development strategy at the enterprise. This final block revolves around devising a forward-looking digital development strategy that aligns with NovaPost's long-term goals. It encompasses investing in cutting-edge technologies, digital upskilling of the workforce, and embracing digital transformation initiatives. The aim is to create a resilient and agile digital infrastructure that can support the company's growth, enhance customer experiences, and navigate the challenges and opportunities of the digital age effectively.

Through Graph Theory, we will present and construct the network of reaching S0 (Fig. 1).

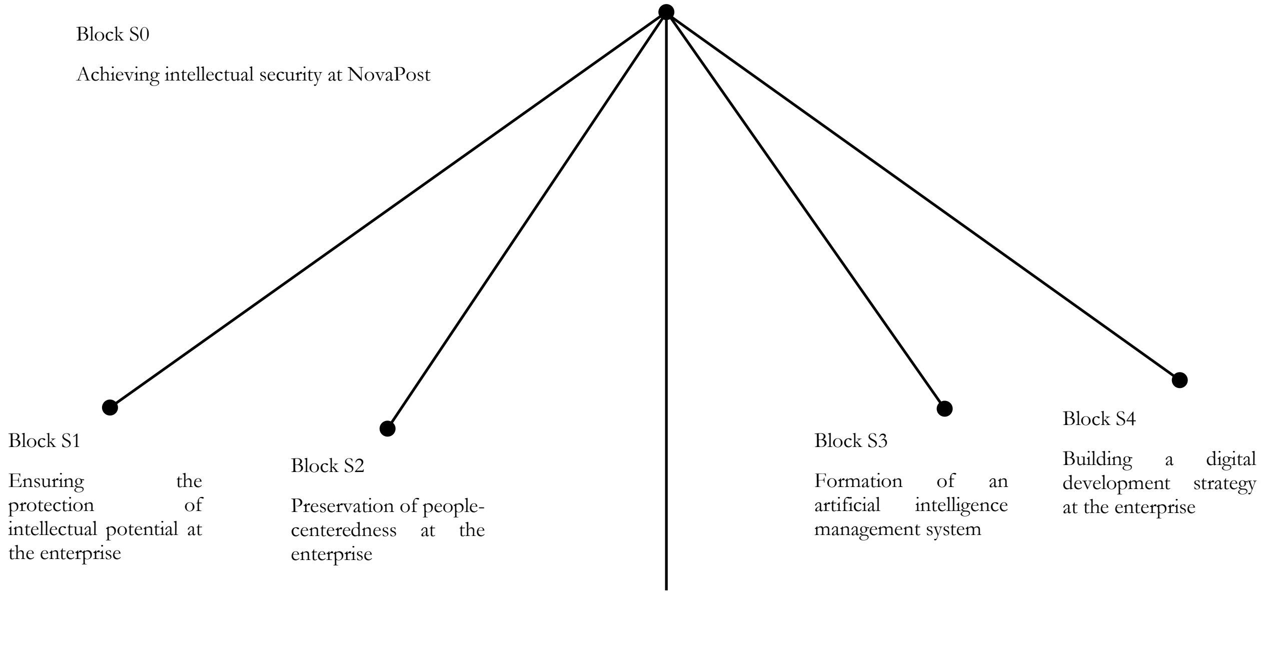
Block S0
Achieving intellectual security at NovaPost
Block S1
Ensuring the protection of intellectual potential at the enterprise
Block S2
Preservation of people-centeredness at the enterprise
Block S3
Formation of an artificial intelligence management system
Block S4
Building a digital development strategy at the enterprise

Figure 1. The construct the network of reaching S0

At the same time, modeling involves auxiliary elements that can be visualized in a more detailed form through the black box (Fig. 2).

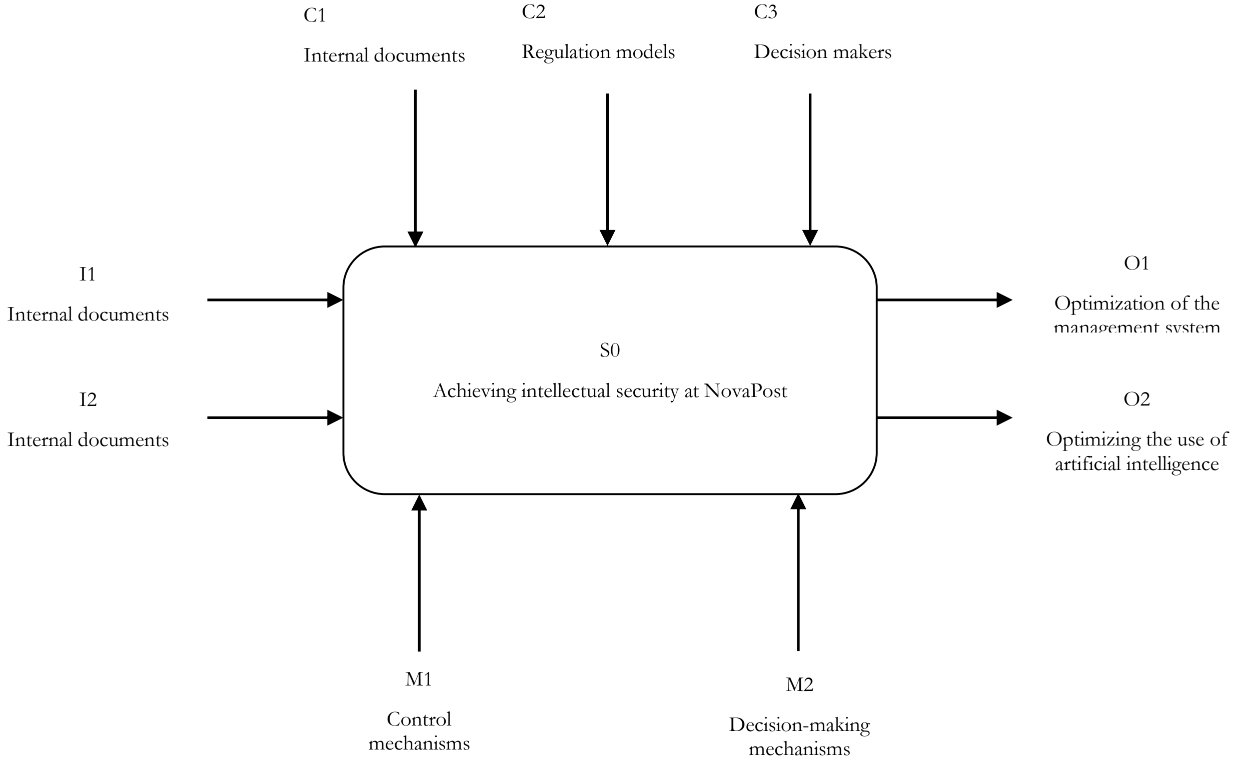
C1
Internal documents
C2
Regulation models
C3
Decision makers
I1
Internal documents
I2
Internal documents
S0
Achieving intellectual security at NovaPost
O1
Optimization of the management system
O2
Optimizing the use of artificial intelligence
M1
Control mechanisms
M2
Decision-making mechanisms

Figure 2. The black box of reaching S0

First, you should build a decomposition of the first level of modeling for ensuring intellectual security through the appropriate software and IDEF0 technologies (Fig. 3).

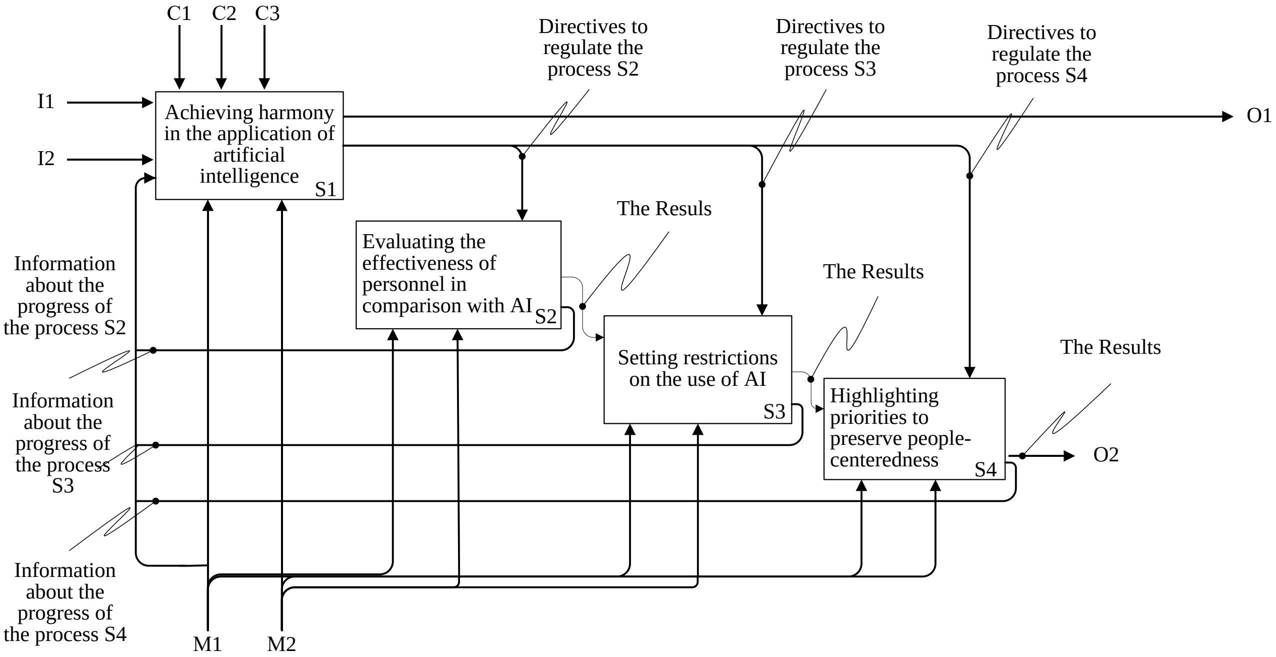
C1
C2
C3
I1
I2
Achieving harmony in the application of artificial intelligence
S1
Directives to regulate the process S2
Directives to regulate the process S3
Directives to regulate the process S4
O1
Evaluating the effectiveness of personnel in comparison with AI
S2
The Resuls
The Results
Setting restrictions on the use of AI
S3
The Results
Highlighting priorities to preserve people-centeredness
S4
O2
Information about the progress of the process S2
Information about the progress of the process S3
Information about the progress of the process S4
M1
M2

Figure 3. The decomposition of the first level of modeling for ensuring intellectual security through the appropriate software and IDEF0 technologies

However, this is only the first level, it is necessary to carry out deeper modeling and detail the most important block, namely S2, for which the following equality will be fulfilled (2):

$$S2=\{S21;S22;S23.....S2n\} \qquad (2)$$

S21. Achieving harmony in the application of artificial intelligence. This sub-block emphasizes the need for a synergistic relationship between AI and human employees at NovaPost. It involves deploying AI in ways that complement human skills and enhance decision-making processes without replacing the human touch. The aim is to leverage AI for routine, repetitive tasks and data analysis, thereby freeing up human employees to focus on more creative, strategic, and interpersonal activities that require emotional intelligence, critical thinking, and personal judgment. Achieving harmony means ensuring that AI supports employees, fostering a collaborative environment where technology and human talent coexist in a mutually beneficial ecosystem.

S22. Evaluating the effectiveness of personnel in comparison with AI. Here, the focus is on establishing metrics and benchmarks to assess the contributions of human employees versus AI systems. This evaluation should not aim to pit humans against machines but rather to identify areas where each can contribute most effectively to the enterprise's goals. Understanding the unique strengths and limitations of both human employees and AI can help NovaPost optimize task allocation, enhance productivity, and ensure a dynamic workforce that is both technologically advanced and deeply human-centric.

S23. Setting restrictions on the use of AI. To preserve the human element within the workplace, it is crucial to define clear boundaries for AI deployment. This sub-block involves developing ethical guidelines and regulatory frameworks that govern how AI is implemented within the enterprise. Such restrictions are intended to prevent overreliance on automation in areas where human judgement is paramount, safeguard against potential biases in AI algorithms, and ensure that AI tools are used responsibly and transparently. By setting these boundaries, NovaPost can protect its core values and ensure that technological advancements enhance rather than undermine the human aspects of work.

S24. Highlighting priorities to preserve people-centeredness. Lastly, this sub-block calls for a clear articulation of the priorities that underpin NovaPost's commitment to a people-centered approach. It involves identifying key principles such as diversity, equity, inclusion, employee well-being, and professional development as non-negotiable aspects of the company's culture. These priorities should guide the deployment of AI and digital strategies, ensuring that technological progress serves to enrich the work environment, foster a sense of belonging and purpose among employees, and ultimately, contribute to a more humane and productive enterprise (Fig.4).

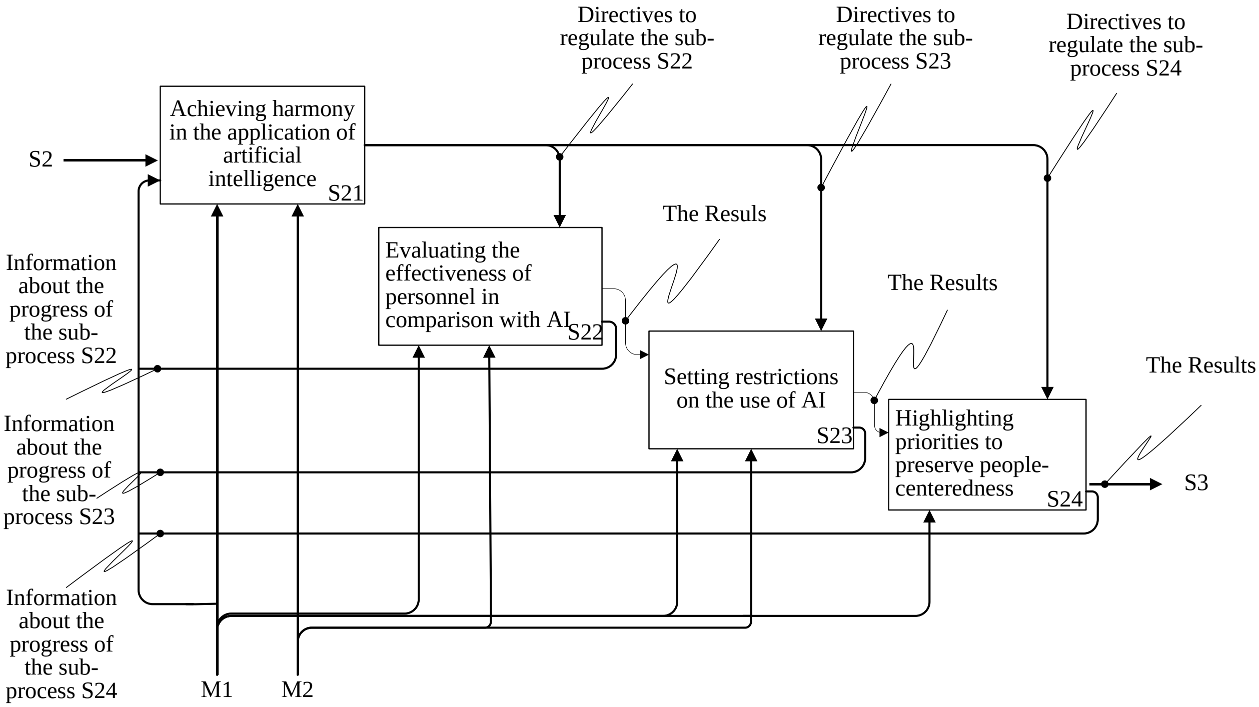
Directives to regulate the sub-process S22
Directives to regulate the sub-process S23
Directives to regulate the sub-process S24
S2
Achieving harmony in the application of artificial intelligence
S21
The Resuls
Evaluating the effectiveness of personnel in comparison with AI
S22
The Results
Information about the progress of the sub-process S22
Setting restrictions on the use of AI
S23
The Results
Information about the progress of the sub-process S23
Highlighting priorities to preserve people-centeredness
S24
S3
Information about the progress of the sub-process S24
M1
M2

Figure 4. The decomposition of the second level (S2) of modeling for ensuring intellectual security through the appropriate software and IDEF0 technologies

Of course, the proposed modeling method allows for even deeper detailing. Therefore, consider S22 (3):

$$S22=\{S22\text{-}1;S22\text{-}2;S22\text{-}3.....S22n\} \qquad (3)$$

S22-1. Setting AI evaluation indicators. Artificial intelligence technologies are different and require correspondingly different approaches to assessment. How they should be assessed depends on many variables. For some, quality is important, not quantity; for others, it’s the opposite. Quantitative and qualitative indicators should reflect the main purpose of the assessment.The goal is to create a standardized set of criteria that can quantify the benefits and limitations of AI in various operational contexts, ensuring that these technologies are being utilized to their fullest potential and in alignment with NovaPost's strategic objectives.

S22-2. Establishing personnel evaluation indicators. Parallel to AI evaluation, it's essential to define clear and fair metrics for assessing human employees' contributions. These indicators should go beyond traditional productivity measures to encompass aspects such as creativity, problem-solving ability, teamwork and collaboration, leadership and initiative, and emotional intelligence.

S22-3. Performance comparison. With both AI and human evaluation indicators in place, the next step is to conduct a comparative analysis of performance. This comparison should be context-specific, recognizing that AI and humans may excel in different areas. For instance, AI might outperform humans in data processing speed, while humans might excel in tasks requiring empathy or complex decision-making. The comparison should aim to identify complementary strengths rather than create a competitive or adversarial dynamic, facilitating strategic decisions about task allocation and team composition to leverage both AI and human capabilities effectively.

S22-4. Processing of results. The final phase involves analyzing the comparative data to derive actionable insights. This might include identifying opportunities for further AI integration where it can significantly boost efficiency, as well as recognizing areas where human involvement is crucial for innovation, customer service, or ethical considerations. The processing of results should also inform training and development programs, ensuring that employees are equipped to work effectively alongside AI and that AI systems are continually refined to support human workers better (Fig.5).

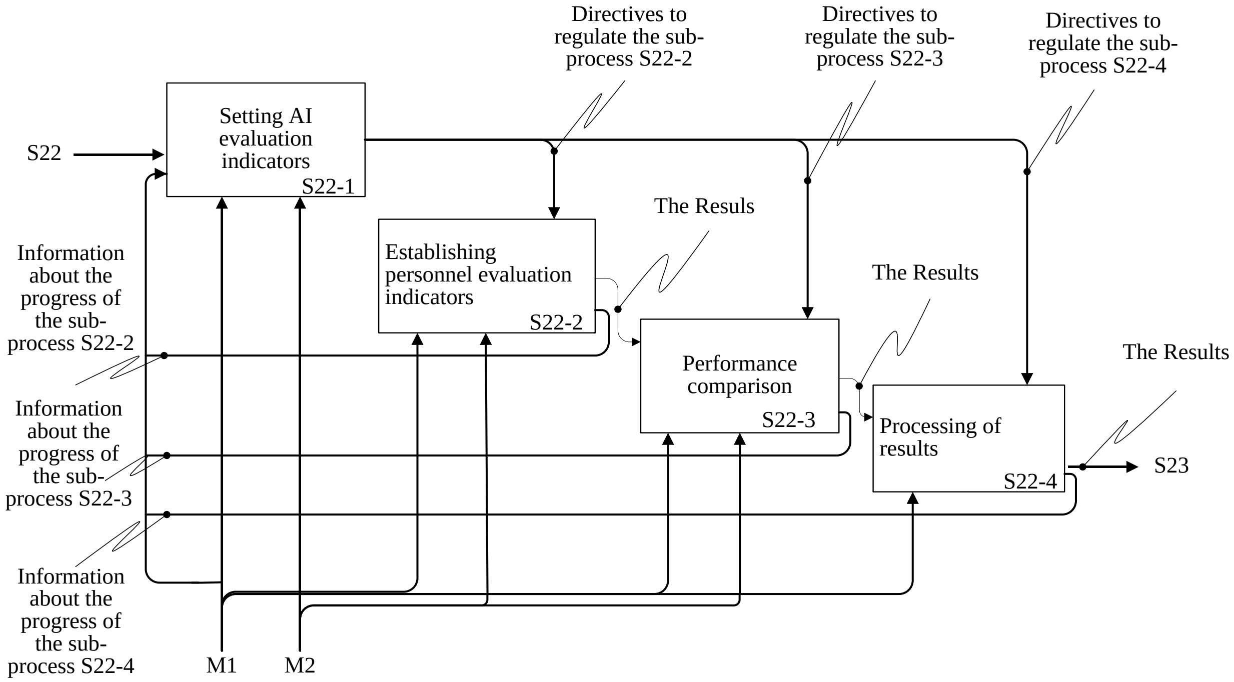
Directives to regulate the sub-process S22-2
Directives to regulate the sub-process S22-3
Directives to regulate the sub-process S22-4
S22
Setting AI evaluation indicators
S22-1
The Resuls
Establishing personnel evaluation indicators
S22-2
The Results
Information about the progress of the sub-process S22-2
Performance comparison
S22-3
The Results
Processing of results
S22-4
S23
Information about the progress of the sub-process S22-3
Information about the progress of the sub-process S22-4
M1
M2

Figure 5. The decomposition of the third level (S22) of modeling for ensuring intellectual security through the appropriate software and IDEF0 technologies

It is also necessary to present the time frame of how the proposed blocks should be performed to achieve S0 (Table 2).

Table 2. The time frame of how the proposed blocks should be performed to achieve S0

S0	1-2 months		3-4 months		5-6 months	
S1	+					
S2		+				
S3			+			
S4				+		

Establishing a clear time frame for the implementation of the IDEF0 model is essential for several reasons, primarily due to its role in ensuring project focus, resource allocation efficiency, and the timely achievement of objectives. IDEF0, a method designed to model the decisions, actions, and activities of an organization or system, is intricate and requires systematic execution. A defined time frame helps in setting realistic deadlines and milestones, which in turn fosters a disciplined approach to project management by enabling the precise tracking of progress against planned objectives. This temporal structure aids in identifying potential delays or bottlenecks early, allowing for timely adjustments.

It is necessary to carefully imagine what place our results occupy among other similar studies. To do this, it is necessary to conduct a thorough comparative analysis. Of course, this is very difficult to do in a comprehensive manner, but a number of landmark scientific works should be used for comparison. Yes, in the study by Araujo et al. (2020) public trust in automated decisions using AI is analyzed. It is important for understanding public perception of AI and its impact on decision making. Our research differs from this source by providing practical methodologies and models for optimizing AI to enhance intelligent security, which not only increases trust in AI, but provides concrete solutions to ensure it.

Auernhammer work (2020) explores the importance of human-centric design in the development of AI. While both this and our study highlight the importance of considering human needs and values, our study extends this approach by offering specific scientific and methodological tools for integrating these principles into intelligent security through AI, making it unique in this context.

At that time, Awad et al. (2020) propose a methodology for combining ethical principles with public opinion in the formation of public policy. In the context of our study, this approach is important for developing AI optimization strategies that take into account the ethical and social aspects of intellectual safety.

A study by Barredo Arrieta et al. (2020) is dedicated to explaining AI, its concepts, and the challenges on the path to responsible AI. Your research complements this work by suggesting ways to use XAI principles to optimize AI systems to improve intelligent safety, pointing to the practical application of theoretical XAI concepts in a safety context.

Bayern article (2017) analyzes how modern corporate law influences the regulation of autonomous systems, including AI. In contrast to this analysis, our research focuses on the use of artificial intelligence to improve intellectual security in business processes, which provides specific methodologies for practical implementation and consideration of legal aspects in this process.

Interesting in the context of our study is the work of Bodenschatz, et al. (18) which examines people's attitudes toward the use of autonomous systems in morally controversial situations. Our research extends this debate by highlighting the importance of optimizing AI to ensure systems behave ethically and meet intelligent safety standards, thereby offering solutions to such dilemmas.

The article by Althar, et al. (2023) focuses on developing an AI-based knowledge processing system to optimize software security. Our research is distinguished by its application of similar principles to a broader range of intelligent security in organizations, expanding the use of AI to protect enterprise data.

Research by Dolezel, et al. (2012) proposes a method for optimizing a network security system based on AI. Our research adds to this by offering a comprehensive approach to using AI not only to protect the network, but also to improve overall enterprise intelligence, including human-centricity and ethics.

Having compared our research with other works in this area, we come to the conclusion about the relevance and novelty of our work. An analysis of existing research confirms that, despite significant interest in the topic of optimizing the use of artificial intelligence in the context of ensuring intellectual security and human-centricity, many aspects remain insufficiently developed. Table 3 summarizes the key advantages and innovations of the study compared to others.

Table 3. The key advantages and innovations of the study compared to others

Advantages and innovations	Essence
Integrated Modeling Approach	Our research uses the IDEF0 method to create detailed decompositions of intelligent security models that not only identify key processes and interactions in the system, but also enable deep AI integration. This approach differs from most other studies, which often focus on general concepts without proposing specific methods for implementing technological solutions.
Advanced Peer Research	Using peer review and the Delphi method to engage 30 experts in the areas of intelligence security and enterprise AI adds significant depth and validity to your findings. Providing this level of expert input is rare and highly valuable as it allows for an objective assessment of the current state of the industry and identifies the real needs and challenges facing organizations.
Focus on Human-Centricity	Our research particularly stands out for its emphasis on the human-centric aspect of AI technology adoption, which is critical for modern business. An approach that balances technological innovation with moral considerations while ensuring the protection of personal data and intellectual property places our research at the forefront of developing

	practical and ethically responsible models for the use of AI.

Our research makes a significant contribution to filling existing gaps by proposing new methodological approaches and models that promote more effective use of AI, taking into account the requirements of intellectual safety and human-centricity. Thus, our study confirms not only the relevance of the chosen topic, but also makes a significant contribution to the development of scientific knowledge, opening new horizons for further research and practical applications in this area.

CONCLUSIONS

In conclusion, our study focuses on the significance of a new approach to ensuring intellectual security through optimizing the use of artificial intelligence, especially in the context of enterprise activities. The author's vision, based on the use of modern modeling methods, in particular IDEF0, expert analysis and the Delphi method, made it possible to build effective decomposition models to ensure intellectual security. These models serve as the foundation for creating more resilient and adaptive intelligent security systems in enterprises, which not only improves overall safety, but also strengthens the human-centric approach to management.

Using a detailed IDEF0 model that includes layers of varying granularity, the study identified ways to optimize the use of artificial intelligence in enterprises. This opens up new prospects for ensuring not only the efficiency of the enterprise, but also strengthening intellectual security in the long term.

The results of the study also indicate a limitation in the number of decomposition models, which may affect the detail and depth of analysis of the proposed approach. This emphasizes the need for further development of the methodology and the use of additional modeling methods to enrich the information base, which will increase the accuracy and efficiency of ensuring intellectual security in enterprises.

Through software and a clear model functional structure, we present how any process can be effectively optimized. Moreover, we present not only the optimization blocks/processes, but also a deep detail of each of them. Such schemes are one of the results of our research. A key success factor is the integration of a human-centric approach into an intelligent security strategy, which involves involving employees in the process of developing and implementing intelligent security systems. This will not only ensure a high level of adoption of these systems within the organization, but will also contribute to the creation of an adaptive and flexible security system that can effectively respond to rapid changes in security requirements and the technology environment.

Prospects for further research in this area open the way for the development of new modeling methods and analytical tools aimed at improving the processes of identifying, analyzing and managing risks associated with intellectual security in enterprises. Particular attention in the future may be given to the development of complex integrated systems that take into account not only the technical aspects of safety, but also social, moral and organizational dimensions.

Thus, the study findings emphasize the importance of further development and optimization of intelligent security systems in enterprises using artificial intelligence. This will not only improve the efficiency of the enterprise, but will also help create a safer and more stable business environment.

REFERENCES

Abbass, H. (2019). "Social integration of artificial intelligence: Functions, automation allocation logic and human-autonomy trust," Cognitive Computation, vol.11, no.2, pp. 159–171. https://doi.org/10.1007/s12559-018-9619-0

Althar, R., Samanta, D., Purushotham, D., et al. (2023). "Design and Development of Artificial Intelligence Knowledge Processing System for Optimizing Security of Software System," SN COMPUT. SCI, vol.4, pp. 297-331. https://doi.org/10.1007/s42979-023-01785-2

Alvarez, I., Di Caprio, D., Santos-Arteaga, F. Javier (2016). "Technological assimilation and divergence in time of crisis," Technological and Economic Development of Economy, vol. 22, no.2, 254–273. https://doi.org/10.3846/20294913.2015.1033663

Amershi, S., Cakmak, M., Knox, W., Kulesza, T. (2014). "Power to the people: The role of humans in interactive machine learning," AI Magazine, vol. 35, no.4, pp. 105–120. https://doi.org/10.1609/aimag.v35i4.2513

Araujo, T., Helberger, N., Kruikemeier, S., De Vreese, C. (2020). "In AI we trust? Perceptions about automated decision-making by artificial intelligence," AI & Society, vol.35, no.3, pp.611–623. https://doi.org/10.1007/s00146-019-00931-w

Auernhammer, J. (2020). "Human-centered AI: The role of human-centered design research in the development of AI. In S. Boess, M. Cheung, and R. Cain (Eds.)," Synergy – DRS International Conference 2020. https://doi.org/10.21606/drs.2020.282

Awad, E., Anderson, M., Anderson, S., Liao, B. (2020). "An approach for combining ethical principles with public opinion to guide public policy," Artificial Intelligence, vol.28, no.7, 103349. https://doi.org/10.1016/j.artint.2020.103349

Baesu, C., Bejinaru, R. (2020). "Knowledge management strategies for leadership in the digital business environment," Proceedings of the International Conference on Business Excellence, vol. 14, pp. 646-656. https://doi.org/10.2478/picbe-2020-0061

Barredo Arrieta, A., Díaz-Rodríguez, N., Del Ser, J., Bennetot, A., Tabik, S., Barbado, A., Garcia, S., Gil-Lopez, S., Molina, D., Benjamins, R., Chatila, R., Herrera, F. (2020). "Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI," Information Fusion, vol. 58, pp. 82–115. https://doi.org/10.48550/arXiv.1910.10045

Bayern, S. (2017). "The implications of modern business–entity law for the regulation of autonomous systems," European Journal of Risk Regulation, vol. 7, no.2, pp. 297–309. https://doi.org/10.1017/S1867299X00005729

Bodenschatz, A., Uhl, M., Walkowitz, G. (2021). "Autonomous systems in ethical dilemmas: Attitudes toward randomization," Computers in Human Behavior Reports, vol. 4, 100145. https://doi.org/10.1016/j.chbr.2021.100145

Dolezel, P., Holik, F., Merta, J., Stursa, D. (2012). "Optimization of a Depiction Procedure for an Artificial Intelligence-Based Network Protection System Using a Genetic Algorithm" Applied Sciences vol.11, no. 5. https://doi.org/10.3390/app11052012

Fan, J., Fang, L., Wu, J., Guo, Y., Dai, Q. (2020). "From Brain Science to Artificial Intelligence. Engineering", vol. 6, no. 3, pp. 248–252. https://doi.org/0.1016/j.eng.2019.11.012

Haenlein, M., Kaplan, A. (2019). "A Brief History of Artificial Intelligence: On the Past, Present, and Future of Artificial Intelligence," California Management Review, vol. 61, no. 4, pp. 5–14. https://doi.org/10.1177/0008125619864925

Hirschheim, R., Klein, H. (2012). "A Glorious and Not-So-Short History of the Information Systems Field," Journal of the Association for Information Systems, vol.13, no. 4, pp.188–235. https://doi.org/10.17705/1jais.00294

Roztocki, N., Soja, P., Weistroffer, R. (2019). "The role of information and communication technologies in socioeconomic development: towards a multi-dimensional framework," Information Technology for Development, vol.25, no.2, pp. 171-183. https://doi.org/10.1080/02681102.2019.1596654

Rudra, P., Girijasankar, M., Bagchi, T. (2018). "Information communication technology (ICT) infrastructure and economic growth: A causality evinced by cross-country panel dana," IIMB Management Review, vol.30, pp. 91–103. https://doi.org/10.1016/j.iimb.2018.01.001

Schukajlow, S., Kaiser, G., Stillman, G. (2018). "Empirical research on teaching and learning of mathematical modelling: A survey on the current state-of-the-art," ZDM Mathematics Education, vol. 50, no. 1, pp. 5-18. https://doi.org/10.1007/s11858-018-0933-5

Van Engelenburg, S., Janssen, M., Klievink, B. (2019). "Designing context-aware systems: A method for understanding and analysing context in practice," Journal of Logical and Algebraic Methods in Programming, vol. 103, pp. 79–104. https://doi.org/10.1016/j.jlamp.2018.11.003

Vial, H. (2019). "Understanding digital transformation: A review and a research agenda," Journal of Strategic Information Systems, vol. 28, no. 2, 118–144. https://doi.org/10.1016/j.jsis.2019.01.003