**MOLDOVA STATE UNIVERSITY**
**DOCTORAL SCHOOL OF PHYSICAL, MATHEMATICAL, INFORMATION AND ENGINEERING SCIENCES**

Presented as manuscript
C.Z.U.: 004.056(043.2)=111

**BUZDUGAN AURELIAN**

# DECISION SUPPORT SYSTEMS FOR MINIMIZING CYBERSECURITY RISKS IN CRITICAL INFRASTRUCTURES

**121.03 Computer Programming**

Abstract

Author: **Buzdugan, Aurelian**
Scientific supervisor: **Căpățână, Gheorghe,** Doctor in Technical Sciences, Univ. Professor
Members of the Steering Committee: **Beldiga Maria**, Assoc. Professor, Dr. in Informatics
**Cerbu Olga**, Assoc. Professor., Dr. in Physical and Mathematical Sciences
**Ciobu Victor**, Assoc. Professor., Dr. in Physical Sciences

**CHIȘINĂU, 2022**

The thesis has been developed within the Doctoral School of Physical Sciences, Mathematics, Information and Engineering, State University of Moldova.

Doctoral Committee:

1. **ARNAUT Vsevolod**, Doctor in Physical and Mathematical Sciences, University Lecturer, State University of Moldova, President;

2. **CĂPĂȚÂNĂ Gheorghe**, Doctor in Technical Sciences, University Professor, State University of Moldova, PhD Supervisor;

3. **FILIP Florin Gheorghe**, Doctor of Engineering, University Professor, Academician, Romanian Academy, Member;

4. **COSTAȘ Ilie**, Doctor in Informatics, University Professor, Academy of Economic Studies of Moldova, Member;

5. **BELDIGA Maria**, Doctor in Informatics, University Lecturer, State University of Moldova, Member;

6. **NOVAC Ludmila**, Doctor in Physics and Mathematics, Associate Professor, State University of Moldova, Scientific Secretary.

The defense of the thesis will be held on **November 30, 2022, at 15:00**.

The doctoral dissertation and the abstract can be consulted at the library of the State University of Moldova and on the website of the National Agency for Quality Assurance in Education and Research (www.cnaa.md).

Author Buzdugan Aurelian

Scientific secretary Novac Ludmila

**Table of contents**

# CONCEPTUAL HIGHLIGHTS OF THE THESIS

**Actuality and importance of the selected topic**

The impressive evolution of information technologies (IT) and communications has transformed the world into an interdependent one with enormous advantages, but also with disadvantages through the increasing dependence on IT systems including critical infrastructures (CI). CI cyber security is a priority at national [1], European [2, 3] and global [4, 5] level. Cyber-attacks can affect systems with operational technologies (OTs) in all CI domains from medical [6], nuclear and radiological. As eloquent examples, the Austrian Ministry of Foreign Affairs or the Thyssen-Krupp factory, considered CI, were victims of cyber attacks [7]. That is why effective, including intelligent, mechanisms for identifying and managing cyber risks in CI are particularly relevant.

**The aim of the doctoral thesis** is the development of an intelligent decision support system (DSS) concept for the minimization and management of cyber risks in CI with the research objectives:

1. Researching general aspects of DSS and cyber risk management in CI.
2. Identification of DSS-specific elements and factors.
3. Assessing the impact of the human dimension in this field.
4. Development of a model, formal intelligent metric system, of a cyber security maturity assessment application within CI and DSS to identify key priorities.

**Research methodology**

Systematic analysis and selective literature analysis were applied in the thesis. These analysis methodologies enable the identification, analysis and interpretation of existing and available studies on the use of DSS in cyber risk analysis. The study design reduces the likelihood of bias and creates a comprehensive overview of the desired topic. The analysis was both qualitative and quantitative based on the purpose of the evaluation. Given the nature and scope of our research, most findings were presented in narrative form following qualitative analysis. The logical method was used to summarize the research in the use of DSS for the intended purpose, and the comparative method - to develop the DSS concept and the cyber security assessment model for CI in any field.

**Scientific novelty and originality**

The original, comprehensive and multi-lateral outputs include a DSS concept, a cybersecurity maturity assessment model, a knowledge base, and a formal intelligent metric

system with prototype application. The prototype enables the application of the cyber security assessment model.

**Scientific problem solved**

An innovative solution for ensuring CI cyber security via an original DSS has been developed, aimed at identifying, classifying and managing cyber risks in CI. For the first time, an intelligent formal metric system and a software prototype were developed to implement the assessment process and compare the level of maturity with best practices or other CIs. The maturity levels are based on technological and human dimension criteria which are universal for the CI field and contribute to increasing the level of cybersecurity maturity and minimizing risks. The DSS and the proposed model can be used separately or complementary and adapted for any type of CI depending on the context and requirements. The results are a contribution to achieving the objectives of Strategic Direction 2(g) of strategic priority V "Economic Competitiveness and Innovative Technologies" of the National Research and Innovation Program for the years 2020-2023 of the Republic of Moldova.

**Theoretical significance**

A DSS concept for cybersecurity maturity assessment and an applicable model for self-assessments and external assessments of CI cybersecurity were developed. An intelligent metric formal system and a software prototype implementing the evaluation processes were developed.

**Applicative value of the results**

The proposed CI cybersecurity assessment model includes identifying the level of maturity based on four criteria: administrative and management, education and assessment, work environment and cyber risk management. Additionally, a formal intelligent metric system and software prototype was developed in Python that facilitates use and future integrations into general risk management methodologies. The model ensures the subsequent taking of measures in the administrative management correlated with the operational processes in the CI.

The applicative value is a contribution to the implementation of the action "Evaluation and reporting on the state and level of security of critical infrastructure objectives from the perspective of information security" from Objective no. 5 "Increasing the protection capacities of national critical infrastructures", Pillar III "Consolidation of operational capacities", Chapter IV of the Information Security Strategy of the Republic of Moldova for the years 2019-2024 and the Action Plan for its implementation. The practical value of the model was validated by the Slovenian Nuclear Safety Authority, the National Metrology Institute of Moldova and the National Nuclear Safety Support Center from UTM (reflected in the Nuclear and Radiological Safety curriculum).

**Scientific results submitted for evaluation**

- Research in the field of cyber risk management in CI led to the definition of the architecture and operating principle of DSS, the theoretical concepts of implementation and adaptation of information systems in CI: human factor, target audience, resilience, modeling and simulation, complexity and interdependence, factors work environment.
- Evaluation and analysis of the impact of human factor elements on the proposed DSS in the field of CI contributed to the identification of trends and best practices in the design, development and use of IT systems. Improving DSS efficiency is achieved by:
  - using a DSS as a module to facilitate its interoperability and integration into existing risk management frameworks;
  - using standards for user interface development and coding to reduce costs and improve platform usability;
  - using modern technologies to assess the physical condition during critical decision-making.
- The CI cyber security maturity assessment model.
- Formal intelligent smart metric system "Cyber Security in Critical Infrastructures", knowledge base and application prototype developed for the first time.
- The evaluation of cyber security in the CI domains of the Republic of Moldova contributed to the validation of the cyber security maturity assessment model, confirmed the retroactive applicability in a certain domain of the CI or individual entity and to the development of recommendations for improving the maturity of national cyber security.

**Approval of the results of the thesis and scientific publications**

The scientific results were presented and discussed at 24 national conferences, including with international participation, and international conferences that took place in the Republic of Moldova (10), Austria (5), Romania (4), Ukraine (1), China (1), Japan (1) and Northern Macedonia (1).

In total, 22 articles as main author and 6 articles as co-author were elaborated and published, out of which: 8 single-author articles and 3 single-author abstracts; 3 articles were published in specialized scientific journals, of which 2 abroad and 1 in the Republic of Moldova (B+); 2 articles indexed by Web of Science and 7 articles indexed in Scopus; 7 articles published by Springer and 2 articles accepted for publication in Springer at the time of submitting the thesis; 25 articles, including abstracts, published in the conference proceedings (in 19 articles as the main author).

# CONTENTS OF THE THESIS

The thesis consists of an introduction, three chapters, conclusions and recommendations, a bibliography and 7 annexes. The main content contains 131 pages, 17 figures and 4 tables.

In the **Introduction** is presented the topicality and importance of this topic. The purpose of the doctoral thesis is described together with the research objectives, research methodologies, the scientific novelties obtained from the research and their practical value that has been identified.

**Chapter I** presents the current state of knowledge and research in the field of cyber threats on CI, as well as the basics of risk management and the opportunity to use DSSs in CI. The analysis contributed to a better understanding of the topic as well as to the identification of subsequent research areas. Initially, the research addresses the definition of goals and issues that were analyzed during the thesis. In this chapter cyber security risks are defined, their components and their impact on CI. Subsequently, the existing theory is used to deepen knowledge in this field. Certain risk mitigation and identification models are identified and applied based on previously obtained data.

Cyber security risks in CI are a common issue due to recent incidents, as well as the critical role of IT components in CI. A presentation of the functions of computers in CI is given in Figure 1. Global cyber threats are becoming increasingly acute due to the continuous development of attack methods and techniques, but also the ability to cause physical damage through information systems. Attacks by state actors create even greater risks, as they may have a high and sophisticated level of expertise and knowledge, as well as sufficient access and resources to achieve their goals. Moreover, the rapid development of artificial intelligence systems and internet-of-things, not only contributes to CI security but also opens up a new landscape of much more complex and intelligent threats or operational safety, which is not fully considered in security systems today. These systems often expand the areas of attack, so risk management becomes even more complex.

The discussion on CI protection is now focused on the cyber dimension, because all infrastructures include IT components, mainly for operational functions. CI protection is a subject that goes far beyond the technical field, being a major challenge related to strategies and policies. Thus, this topic requires an interdisciplinary approach, given the impact and level of integration of IT in CI. Moreover, the interconnection of CI at the national or international level can inadvertently lead to an increase in the attack area, which stimulates the diversification of attack methods. According to Verizon, in 2021 the rate of ransomware incidents, which can lead to sabotage operations in an organization, was 10%, which shows a double increase compared to 2020. Also, the rate of incidents that affected CI is about 10% of the total number of incidents [8]. Comparing the response time, over 90% of incidents occurred within minutes, of which 70% were

detected after a few months. Thus, the time required to launch an attack is short compared to efforts to secure and monitor these digital components within the CI [9].

In addition, the latest report of the UN group of governmental experts on promoting responsible state behavior in cyberspace in the context of international security identified as a priority cyber risks against CI and proposed rules to stop any attacks on CIs in other countries, ensuring adequate protection of their CIs, as well as cooperation with other states to exchange knowledge, expertise and good practices in this field [4].

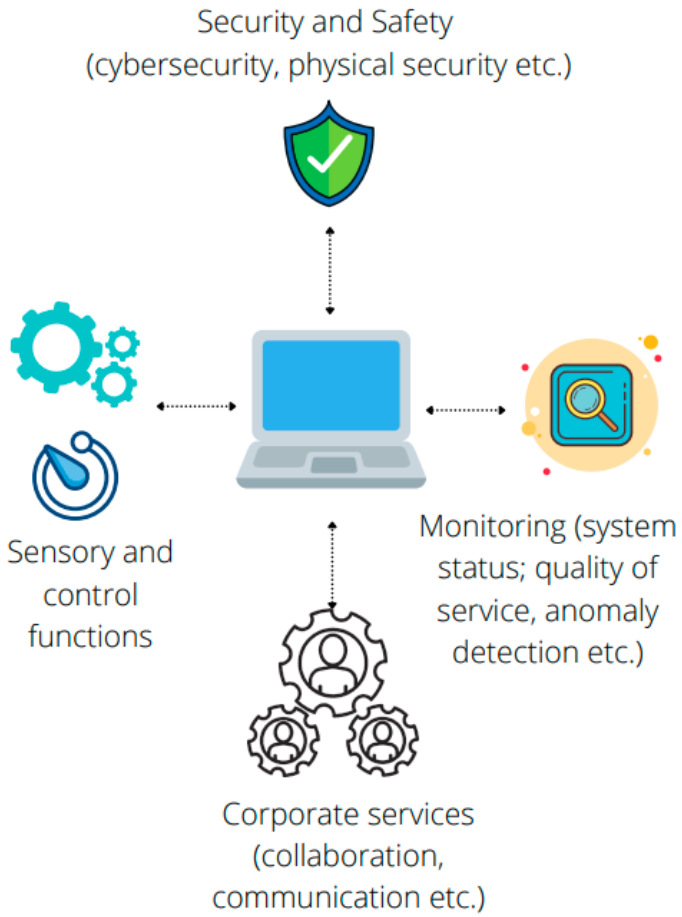


**Fig. 1. The role of computers in CI**

The need to streamline the management of cyber risks to prevent attacks on CI is also based on the activity of the guest lecturer (2015-2017) of the Department of Nuclear Safety and Security of the International Atomic Energy Agency. During this period, several cybersecurity modules were taught as part of the training offered in Kazakhstan, Slovenia and Moldova. The main purpose of the courses at that time was to raise awareness of the role of cybersecurity in CI systems used by nuclear and radiological operators.

Another personal interest is the use of emerging technologies, such as artificial intelligence or machine learning, which provide opportunities for organizations and individuals to detect

anomalies that may reveal security incidents. Cybersecurity often becomes a race against the clock to ensure the timeliness and effectiveness of these security checks. The synergy between artificial intelligence and cybersecurity can provide new capabilities and resources in ensuring the security of a system or device. At the same time, the same synergy can compromise the security of a system at a much higher level. However, many of the cyber security risks that currently exist in CI could be minimized by implementing good security practices that can be taken over and adapted from traditional IT.

Cyber risk management depends to a large extent on the processing of a large volume of risk data and a complex process of analysis, prioritization and decision-making. The interconnection, interdependence and digitization of CI significantly increase the amount of data needed to be assessed for risk management. Knowledge of cybersecurity is necessary to be able to reflect the risks of an IT system in CI, but also knowledge of the context of CI and operating systems. Data processing in the decision-making process goes beyond human limits and computer systems should be used to support this process.

This thesis explores also the specific factors of cyber risk management in this field, as well as the challenges it poses to operators and decision-makers. One of the key questions assessed is whether the existing risk management process adequately addresses cyber risks. Areas, where further research is needed, have been identified, and a DSS concept was proposed that will improve cyber risk management in CI. To evaluate the efficiency and applicability of a DSS concept, a formal intelligent metric system and prototype in Python were developed, that implements the evaluation process of the proposed model, as well as incorporates elements from the findings and results obtained in this research.

The human dimension is another element that has a critical role to play in the development and use of decision support systems. The implications of the human dimension in a DSS for cyber risk management in CI were evaluated. The impact of the human factor on DSSs was analyzed and solutions were proposed to overcome the limitations caused by the human dimension. It was also discussed how the proposed solutions and recommendations can increase the efficiency of DSSs used in areas with stringent security requirements, such as CI.

Given the number of risk management methodologies in CI, it can be considered that management should be holistic and include scenarios and functions that also cover cyber risks. This finding defined potential further research in defining a DSS to identify, prioritize, and possibly propose controls that would effectively manage cyber risks in CI.

As a solution to the problem, it was proposed to carry out the risk management process through a DSS. The elements identified as necessary and critical for this system are knowledge of

the CI system and its digital components, methodologies and tools of cyber attack, resilience, interconnection, dependence and human-readable results. Because these elements could involve large amounts of specialized data, DSSs would be the optimal solution by integrating various methodologies and information systems to identify risks and select or recommend the best solutions. Such a system that also uses modern technologies is an appropriate solution in terms of efficiency and cost and would help solve the identified problem.

Several areas that do not have extensive coverage have been identified, as well as future research topics. Understanding the cyber risks and all the implications for a CI, in combination with DSSs, would allow operators and decision-makers to make informed and informed decisions about the risks identified. A DSS that explicitly focuses on cyber risks would complement and support existing research and is needed to support long-term goals in managing emerging risks. While physical events and damage in CI have been major risks for years, it is now clear that risk management in this area does not comprehensively cover the new nature of the risks posed by cyberspace. A DSS explicitly focused on cyber risks and developed in a way that is seen as a component would increase the likelihood that it would be adopted by risk managers and used in real-case scenarios. Such a modular system would improve risk management processes in CI fields [10].

These results provide valuable insights into the possibility of using DSSs for cyber risk management in CI. The data of the analysis helps validate and confirm the topicality of the selected research issue and provided valuable information for understanding the current situation in this field. The knowledge gained allowed us to confirm the research objectives and the need to explore the factors necessary for the concept of DSS.

**Chapter II** describes the process of validating the potential of DSSs in the management of cyber risks in the field of CI and the proposed concept of DSSs. To ensure the quality of the analysis, the latest developments and results in this field were analyzed, selecting specialized studies from journals or conference papers. Based on these results, a DSS concept for cyber risk management in CI was proposed. The chapter begins with a description of the research methods used and, mainly, a systematic analysis of the literature. This method requires the identification of existing work on this topic that prevents duplication and duplication of research and helps to identify potential research directions and areas that have not been sufficiently analyzed.

Based on the results of the review, no DSS takes into account all types of cybersecurity risks, but only a subset of them. It is also found that existing methods that combine risk identification, prioritization and mitigation are insufficiently explored. This direction was selected based on the proposed DSS concept, which would improve the risk assessment and management

process. The risk management process is also becoming increasingly complex and often requires adaptation to the requirements and context of each type of CI. The analysis shows that cyber risks are generally included in the risk management process, but these risks would be better identified and managed when there is more expertise. Very few methodologies exclusively assess the impact that IT and cybersecurity have on CI, as a separate mode or process. For the effective management of cyber risks in CI, it is necessary to improve the accuracy and decision-making capacity.

Another identified need is the design and development of a modular DSS that is easy to integrate into other DSSs or risk management entities or frameworks. There is a reduced number of papers on this topic, which indicates that the development of a common DSS for all types of risks can consume too many resources. Thus, a DSS developed as a module for easier interconnection and sharing of data would allow easy integration and adaptation for various domains and systems. There is also an emphasis on the importance of the interface of a DSS that can be correlated with the efficiency in use by operators or decision-makers, as well as the level of IT knowledge required.

Subsequently, the concept of DSS for cyber risk management in the field of CI was presented, as well as the factors that are directly correlated with the efficiency, performance and implementation rate of a DSS. The following key elements have to be considered when developing a DSS for the CI domain: human factor, end user, resilience, modeling and simulation, complexity and interdependence (Figure 2). This represents one of the original results of the thesis.

The language system is one of the first elements to consider when identifying the types of data needed and potential sources. Given that the DSS is to be adapted for CI, useful and necessary data sources have been selected. While certain approaches can be adapted from the IT field when it comes to cyber risks, the CI field contains specific systems, such as industrial control systems, that need to be considered. The elements proposed for the language system should be used from the design phase. Each type of data can be classified according to one or more proposed categories. Such an approach will be useful when developing modules and systems that will recommend or identify decisions. As complex systems for specific domains are addressed the categories could be used to reduce the costs and resources required for further processing of this data.

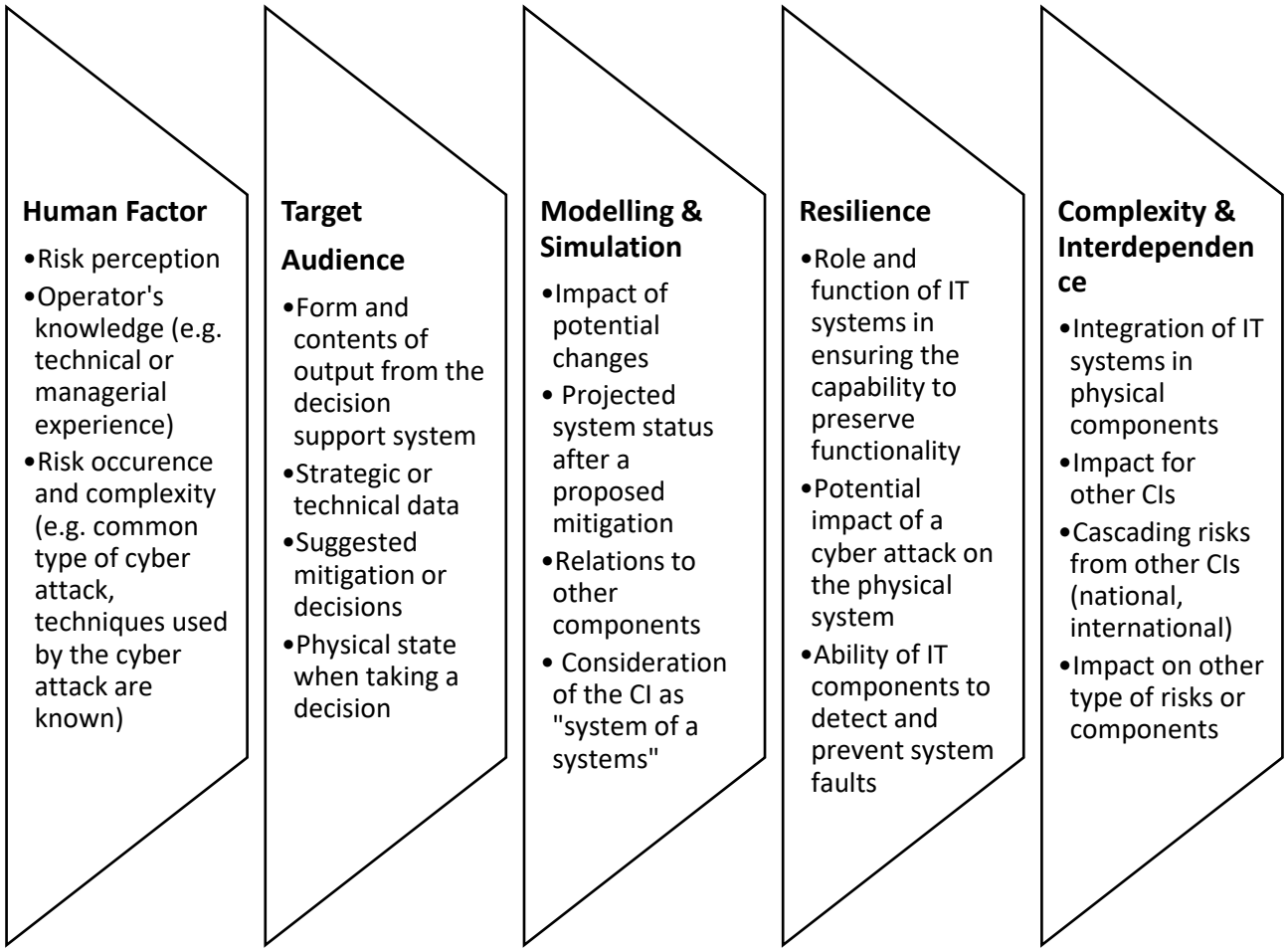


**Fig. 2. Elements to be considered for a decision support system in risk management**

The proposed entries for the language system are presented in Figure 3. The general architecture of a DSS was also evaluated and adaptations for presentation and language systems were proposed, taking into account the specific field of CI. In addition, recommendations were included on how to evaluate and include the elements of the human factor in the design phase of the DSS.

The presentation system, or user interface, has one of the most important roles in ensuring the efficiency and adoption of the system. An IT product that is difficult to use is less likely to succeed both in the marketplace and in fulfilling its purpose. Therefore, the context and elements of the human factor are among the main requirements in the design of the user interface. The human factor has an even more important role because the perceived efficiency of the DSS can be directly related to this factor. The human factor must be taken into account from the process of identifying and assessing a cyber risk to the decision-making process.

In addition, if the DSS is analyzed as an application, then the adaptability would provide a reduced time and cost to solve a problem, and also improve the quality of the software application [11]. Having a system that can learn the type of input data, and validate and classify automatically,

will streamline the process of design, development and use of the system through minimal manual interventions. This will ensure that the proposed DSS will correspond to the proposed modular design so that it can be adapted to different types of CIs, as well as to specific requirements in terms of cyber risk management.

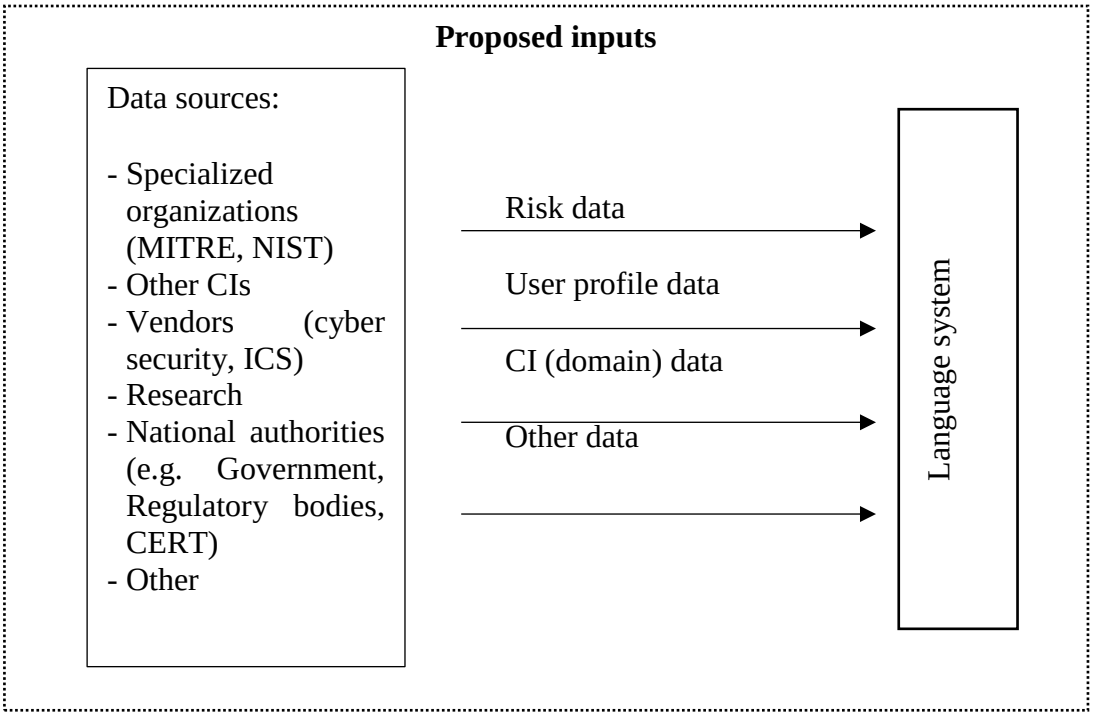


**Fig. 3. Potential inputs in the DSS's language system**

Another important condition that must be taken into account when designing the DSS architecture is context. Given that the proposed DSS has a very specific role and purpose, criteria that would ensure that the DSS is fit for purpose for any of the areas of CI must also be considered. The context often imposes requirements for IT systems, from the hardware and software used, and network connectivity to the types of data that can be consumed within the system.

The human dimension also plays a critical role in the context of a DSS in CI, due to the characteristics of the field. As the DSS is a socio-technical system, it must be designed and adapted to the needs of users, their roles in the organization, as well as the context. Elements of the human factor, such as perception, skills, and ability to make the right decisions in situations of pressure or professional culture play a critical role in the proposed DSS. A multidimensional and accurate overview of the impact of the human dimension on information systems would facilitate the appropriate approach to known risks or problems, as well as the identification of solutions.

The dependence and impact of the human factor on information systems are very wide. On the one hand, they can negatively influence and reduce the efficiency of decisions recommended or made by DSSs. On the other hand, taking into account all known constraints or risks from the design phase, the perceived efficiency of such a system can be improved and maximized.

Common constraints such as costs, delivery time, and organizational culture can influence the quality of the final DSS. It is also recommended to use existing standards, such as ISO 9241 or ISO 27001, as these represent a proven solution to reduce the cost and time of delivery/implementation of the product, given that most functional requirements can be covered by current standards. By following good practices, certain known problems or constraints imposed by the elements of the human factor can be avoided. Moreover, modern computer technologies, such as those that read biometric parameters, represent an opportunity to recognize and minimize the risks presented by humans. Furthermore, DSS can also support organizational activities, such as employee evaluations or training, as well as practical exercises. These would help increase the culture of cybersecurity, and also the professional skills of end users, which would have a positive impact on the perceived efficiency and use of DSSs.

Another possible solution to reduce certain human risks or errors in the decision-making process is automation. This has many benefits in terms of reducing costs as well as improving efficiency. However, by definition, a CI does not meet the requirements for the use of decision automation by a DSS in the cyber risk management process. Certain actions can be identified for automation thus anticipating the occurrence of problems. The activities of evaluation and supervision of operators become critical for safe automation, improving the quality of automation, reducing known errors or human limitations, and reducing final costs. It is also worth mentioning that DSS is considered a sustainable solution [12], which means that the effort to develop such systems would pay off and help coordinate efforts in solving emerging issues and risks.

The identified items apply to a DSS that is used in the CI domain. However, these results can be applied to any other type of IT system in this field.

**Chapter III** describes the model [13], formal intelligent metric system and related prototype application for assessing the maturity of cyber security of CI. It also describes the case studies of the integration of computer security in the field of medicine, nuclear and radiology in the Republic of Moldova. These areas are currently considered CI and are among the top targets for cybercriminals. To achieve the case study objective, the planned activity included a comparative analysis between the legislative framework, technical controls and good practices, standards and international guidelines.

The results of the analysis of the legislative framework in the field of nuclear and radiological safety in the Republic of Moldova are presented in chronological order. These findings were correlated with the evolution of international recommendations and best practices in this field by the IAEA. It also investigated how national cybersecurity legislation has affected the field of CI, including nuclear and radiological. In general, the level of security in the

government sector is assessed as being in a developing state and currently with a low maturity [14]. This helped build an objective picture of the cyber security for this CI area.

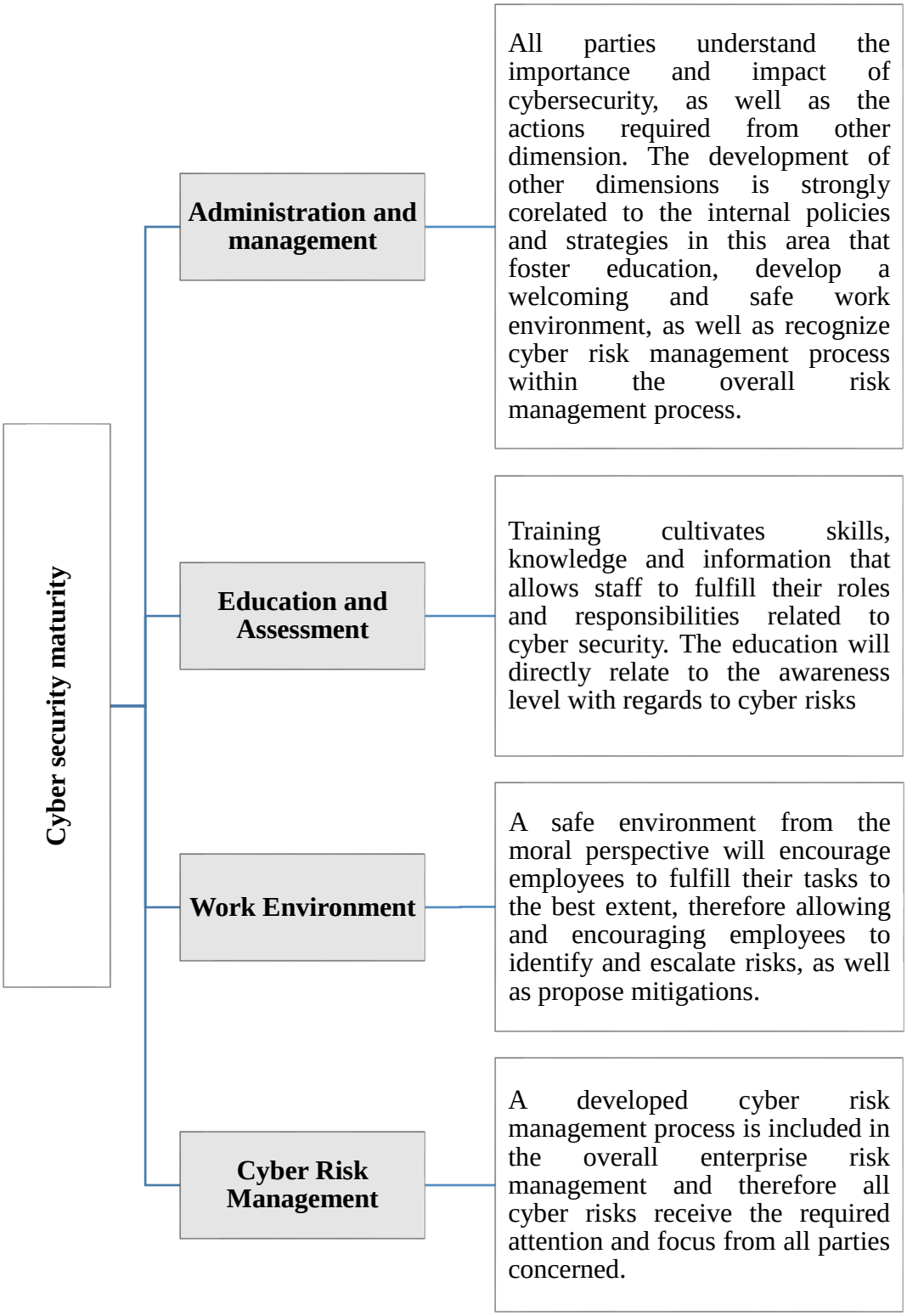


**Fig. 4. Interdependence of cyber security dimensions**

These results were matching with similar analyses performed at the national level of the entire IT landscape [15]. Developments have been critically analyzed and recommendations have

been proposed on improving the legal framework, the impact of vertical cooperation, the exchange of expertise and good practice at the horizontal level, as well as the overall cyber security program. The findings are aligned with the proposed model and confirm its applicability and authenticity. Subsequently, the model for assessing the maturity level of cybersecurity for CI organizations was developed and presented (Figure 4). This model is complementary to the DSS concept proposed in Chapter II and incorporates the identified critical elements and aspects. The model combines four key dimensions that describe the maturity of cybersecurity, is easy to read and understand and can be adapted to the needs and requirements of each organization in the field of CI. Simplicity and clarity would increase the adoption rate while keeping costs and effort low. This model can support a better decision-making process regarding cyber risk management, as it can show areas that need attention to increase their level of maturity. The model is multidimensional and can be used both to evaluate the efficiency of the proposed DSS from a technological point of view and the human dimension, but also to serve as a basis for the features or algorithms developed within the troubleshooting system in a DSS.

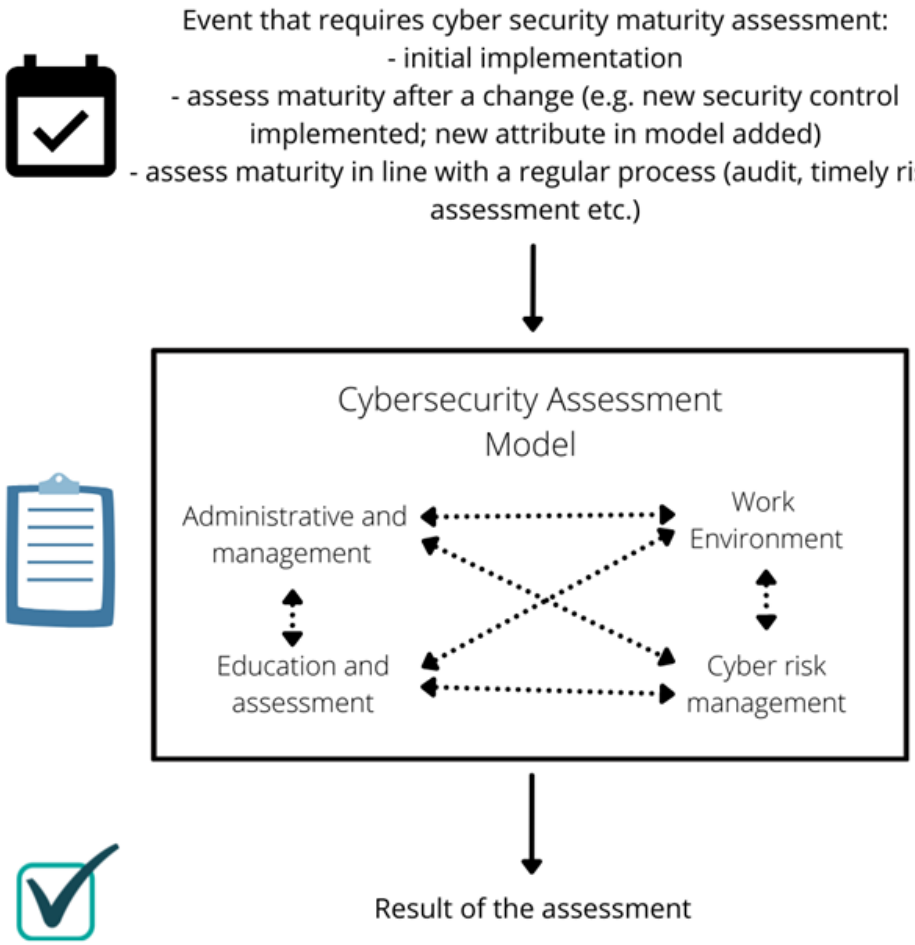


**Fig. 5. The process and triggers to assess cyber security maturity**

The evaluation process can support the implementation of DSSs and review organizational aspects related to cyber risks to ensure that DSSs are efficient and meet expectations, as well as used during various processes or needs in the organization (Figure 5). This chapter also includes the presentation of the “Cyber Security in Critical Infrastructure” knowledge base and the intelligent formal metric system “Cyber Security in Critical Infrastructure” that was developed for the first time. This formal system uses and applies the elements of the proposed model to create a cyber security assessment process. Additionally, a copyright has been registered with AGEPI on the formal intelligent metric system "Cybersecurity in critical infrastructures” (Series 0, No. 7305 of 04.08.2022).

The prototype of the application "Cyber security in critical infrastructures" was also developed and presented. The program highlights the versatility and options for integrating the model into any IT risk management system. Additionally, the program denotes the potential of the model to be translated into a simple application, which can be used by decision-makers during the evaluation process. The interface format and programming language used by this program (classes, libraries and functions) have been carefully selected to facilitate the adoption and adaptation of the model.

Below is a snippet of the Main Menu of the application:

*The organizations found in the database are as follows*

*1. Air_Trafic_Control*

*2. Institutie_Medicala*

*3. Operator_Energy*

*4. Nuclear_Operator*

*Choose organization: > 2*

*MAIN MENU*

*1. General information*

*2. Evaluation: Policies and administration*

*3. Evaluation: Training and Education*

*4. Evaluation: Work environment*

*5. Assessment: Cyber risk management*

*6. Print the latest results*

*7. Change the organization*

*8. Compare maturity*

*9. Exit*

During the development, new possibilities for improving the model were identified and implemented, such as enriching the evaluation results with recommendations, such as warnings when maturity is below a minimum threshold. An example of this functionality is given below:

****** General information about cyber security maturity level ******

*Last assessment performed on: 2021-05-19*

*Latest average score: 2.9*

**** WARNING ****

*Overall cyber security maturity is below average. Actions are required to improve the security stance. To view the results by dimension, select PRINT LATEST RESULTS*

The program can be used in evaluating multiple organizations as well as selecting the dimensions of cybersecurity in an organization that needs attention or improvement. In addition, the application can be combined with the DSS originally proposed for cyber risk management. This experimental activity helped to develop new perspectives on DSS architecture, its performance, as well as the impact and integration of such a system in an organization.

Subsequently, the results of the retroactive application of the model to nuclear and radiological developments were presented. The results confirmed the applicability and effectiveness of the model from another standpoint, as well as inputs on the evolution steps regarding the development of the cyber security program at the national level. It was proven that policies and management, as well as cyber risk awareness, are among the initial factors leading to the development of an advanced security program. Next, it highlights how other dimensions are developing, such as user training and cyber risk management based on organizational or national laws, regulations and requirements.

The **Conclusions** highlight the main results of this doctoral thesis. The DSS concept can be used to identify and manage cyber risks, as well as to respond to incidents, and can be integrated into other risk management frameworks, to minimize costs. This concept focuses on all the roles within a CI, and is based on the analysis of the impact of the elements of the human factor on the information systems. The model, formal system and cyber security assessment application have been developed starting from the conditions necessary for the development of an effective cyber security program, taking into account the role of technologies and human factors in the field of CI.

The results are an original solution to the current challenges of cyber risk management in the field of CI. The results are comprehensive and multilateral and include a DSS concept, a cybersecurity maturity assessment model, a formal intelligent metric system and a prototype application. The results are universal for the CI field and represent a modern and innovative solution to increase the level of cyber security and minimize the associated risks. The concept,

model, formal system or application can be used separately or complementary and can be adapted to any type of CI, depending on requirements. The solutions are practical and easy to use for assessing cyber security and contributing operatively and directly to ensuring the cyber security of critical infrastructures. This is important for ensuring the safe development of IT in the field of CI. The results do not contain software products or codes that can easily become obsolete, while the concept and formal system can be easily used and adapted for each CI. All results obtained, developed, prototypes and concepts have been published in peer-reviewed journals, papers at conferences or scientific seminars.

# FINAL CONCLUSIONS AND RECOMMENDATIONS

Cyber risk management in CI represents a current research topic due to the risks posed by cyber threats in all fields. The number of attributes and amount of data that must be analyzed within the cyber risk management process often exceeds human abilities. Computer-aided decision-making is a modern solution to this question and can help improve the efficiency and resources spent on this process. Following the research carried out, the following four general conclusions can be made:

1. **DSSs represent a viable solution for cyber risk management in CI**. Based on the research conducted through a systematic literature review, it can be stated that although risk management processes are of research interest, there has been no DSS that addresses the entire cyber risk management process in the field of CI, starting with risk identification to classification, mitigation and assessment. It is recommended to include key elements during the development of the proposed DSS concept, namely: human factor, target audience, resilience, modeling and simulation, complexity and interdependence. The development of DSS as a module is also proposed to increase cost efficiency and deployment rate. It has been identified as a critical need to evaluate the human factor during the design, development and use of DSS.
2. **A DSS concept was developed for cyber risk management in the field of CI,** which is one of the original results of this thesis. To avoid the cybersecurity problems created by DSS as a program, the DSS has been described at a conceptual level, to avoid situations where an application becomes outdated and contains known vulnerabilities in a very short period. One of the requirements of the DSS concept is to enable and empower the end user, decision maker or operator to effectively and quickly make an informed decision on how to address identified cyber risks. This result is supported by recommending some technical aspects and methodologies regarding the construction of DSS, such as following the standards for designing a friendly and usable interface, evaluating the elements of the human factor and using automation where the type of tasks allows it and the risk is reduced. From an architecture standpoint, the language and presentation system were described and data types were proposed for use by these systems, which are correlated with the DSS context and scope. These systems are at the heart of the DSS and are directly responsible for the efficiency and perceived performance of the DSS. Furthermore, were proposed as requirements the assessment of the CI context and risk management process during system design, to ensure that these are addressed from the initial stages. This would ensure that the DSS is fit for purpose. The impact of the human dimension, both positive and negative, on DSS to be used in safety domains was analyzed. Recommendations are presented on how to reduce

the negative impact of human factor elements on the proposed DSS, and mainly: the use of a modular DSS, use of standards for user interface development and coding to reduce costs and improve platform usability and use of modern technologies, such as biometrics, to assess an operator's physical condition when making critical decisions. As a solution to overcome known limitations caused by human factor elements such as perception, skills, and ability to make correct decisions under pressure or professional culture, as well as to reduce costs and improve efficiency, the use of autonomous decision-making is proposed. Benefits, criteria, and strategies were identified to automate certain types of tasks, reduce user fatigue, and improve overall DSS efficiency.

3. **A cybersecurity maturity assessment model was developed** and confirmed to be applicable and effective for different types of CI. The model was developed to estimate the efficiency of DSS used in the CI field. An original result achieved through this model is the ability to offer solutions on several dimensions, the model being able to identify the area that requires investment – technologies or user training. The model can be used to facilitate periodic information security audits, being aligned with ISO 27001. The model has been reviewed by multiple external organizations, which have confirmed its originality, applicability of innovative aspects in the field of CI as well as efficiency. The attributes of the model were also included in the master's program seminars for the Nuclear and Radiological Security course at the Technical University of Moldova. For the first time, the knowledge base "Cybersecurity in critical infrastructures" was developed, based on which the intelligent formal metric system "Cybersecurity in critical infrastructures" was developed. Additionally, a copyright has been registered with AGEPI regarding the formal intelligent metric system. The prototype of the "Cyber Security in Critical Infrastructures" application has also been developed. The prototype amplifies the results of the assessment process by adding situation-dependent recommendations. The development of the cyber security program in CI domains from the Republic of Moldova was analyzed and presented. The retroactive application of the model to the given CI domains validated its use in such scenarios and, in addition, helped to define recommendations regarding the improvement of cyber security maturity at the national level.

4. **The trends and steps in establishing a cyber security program in CI fields were identified**, through the retroactive analysis of cyber security development in the Republic of Moldova. Thus, recommendations are proposed on how to improve and simplify this process. An in-depth research into the development of the nuclear and radiological legislative framework in the Republic of Moldova was carried out, as a result of which the increasing role of cyber security of critical targets and the necessary emphasis on cyber security elements in the assessment of the

physical security was stressed out. A chronological analysis of the role and attention of cyber security in the nuclear and radiological legislative framework was also performed. Cyber security in medicine has been assessed from a high-level perspective, and as a result, common vulnerabilities against systems in medicine, as well as limitations related to human factors elements, have been identified. Recommendations were proposed from the perspective of technical controls to be implemented, as well as on the policy and management side to improve horizontal cooperation both nationally and internationally. The trends that organizations follow in the process of increasing the level of cyber security maturity were also presented.

**Recommendations for future research**

Although the research focused on the use of DSS in CI, it was observed that this issue can be analyzed from different points of view. Based on this research, the following recommendations are made:

- Evaluation from other perspectives of the impact of the human dimension on DSS to be used in CI;
- Identification of standards or interoperability frameworks that improve risk management in CI domains;
- Improving the legislative framework of cyber security in the field of medicine and reviewing the effectiveness of the proposed model for selected countries or regions;
- Feasibility and implementation of integrated security controls.

## REFERENCES


1. Legea nr. 257 din 22.11.2018 *privind aprobarea Strategiei de securitate a informațiilor a Republicii Moldova pentru anii 2019-2024*, MO al RM nr.13-21 din 18.01.2019
2. European Commission 2020, Joint communication to the European Parliament and the Council - The EU's Cybersecurity Strategy for the Digital Decade, [Online] la adresa: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=JOIN:2020:18:FIN. accesat la 3 august 2021
3. European Commission 2020, Proposal for a directive of the European Parliament and of the Council on the resilience of critical entities, COM(2020) 829, [Online] la adresa: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:829:FIN, accesat la 3 august 2021
4. United Nations 2021, Report of the Group of Governmental Experts on Advancing responsible State behavior in cyberspace in the context of international security (A/76/135), accesat la 20 iulie 2021
5. World Economic Forum 2020. The Global Risks Report 2020. [Online] la adresa: http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf accesat la 20 martie 2020
6. European Medicine Agency 2018, Data anonymization - a key enabler for clinical data sharing, [Workshop report], 2018, [Online] la adresa: https://www.ema.europa.eu/en/documents/report/report-data-anonymisation-key-enabler-clinical-data-sharing_en.pdf pp 14-15, accesat la 3 august 2021
7. ENISA 2020, ENISA Threat Landscape 2020, [Online] la adresa, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-main-incidents/at_download/fullReport, accesat la 3 august 2021
8. VERIZON - 2021 Data Breach Investigations Report, 2021
9. VERIZON - 2019 Verizon Incident Preparedness and Response Report. 2019
10. **BUZDUGAN, A**. Integration of Cyber Security in Healthcare Equipment. In: Tiginyanu I., Sontea V., Railean S. (eds) 4th International Conference on Nanotechnologies and Biomedical Engineering. ICNBME 2019, IFMBE Proceedings, vol 77, pp 681-684, Springer Nature Switzerland AG (2020), DOI:10.1007/978-3-030-31866-6_120
11. CĂPĂŢÂNĂ, Gh., CIOBU, V., PALADI, F.: Adaptive Application for Complex Systems Modeling. In: Conference of Mathematical Society of the Republic of Moldova. 4, Chişinău. Chişinău: Centrul Editorial-Poligrafic al USM, pp. 487-490. ISBN 978-9975-71-915-5. (2017)
12. FILIP, F.G. (2020). *DSS - A Class of Evolving Information Systems*. In: Dzemyda G., Bernatavičienė J., Kacprzyk J. (eds) Data Science: New Issues, Challenges and Applications. Studies in Computational Intelligence, vol 869. Springer, Cham. DOI:10.1007%2F978-3-030-39250-5_14
13. **BUZDUGAN, A.,** CĂPĂȚÂNĂ, Gh. (2022) Cyber Security Maturity Model for Critical Infrastructures. In: Ciurea, C., Boja, C., Pocatilu, P., Doinea, M. (eds) Education, Research and Business Technologies. Smart Innovation, Systems and Technologies, vol 276. Springer, Singapore. The 20th International Conference on Informatics in Economy, Bucharest University of Economic Studies, https://doi.org/10.1007/978-981-16-8866-9_19
14. CERNEI, V., Models and methods for governmental cyber risk management. In: The Collection. Economic security in the context of sustainable development. Ediția 6, 10 dec 2021, Universitatea de Stat „Alecu Russo" din Bălți, pp. 258-261. ISBN 978-9975-155-01-4.
15. BOLUN, I., CIORBA, D., ZGUREANU, A., BULAI, R., CALIN, R., BODOGA, C.: Informatics security assessment in the Republic of Moldova. In: Journal of Engineering Sciences. vol. XXVII, no. 4 (2020), pp. 103-119. ISSN 2587-3474. DOI:10.5281/zenodo.4288297

# ANNOTATION

**The thesis „Decision Support Systems for Identification and Minimizing Cyber Security Risks in Critical Infrastructures" is written in Romanian by Mr. Aurelian BUZDUGAN for fulfilling the requirements for PhD in informatics, speciality 121.03 - Computer Programming. The thesis has been elaborated at the Moldova State University, Chisinau, 2022.**

**The structure of the thesis**: The thesis consists of an Introduction, three chapters. Conclusions and Recommendations, Bibliography of 191 titles. The main text amounts to 131 pages, including 17 figures, 4 tables and 7 annexes. The obtained results were published in 28 scientific papers with a volume of over 7 sheets of author.

**Keywords:** decision support systems, critical infrastructures, cyber risk management, language system, presentation system, human dimension, a model for cyber security maturity assessment, knowledge base, intelligent formal metric system, application architecture.

**Research purpose:** develop, evaluate and validate the use of a decision support system (DSS) in managing cyber risks in critical infrastructures (CI).

**Research objectives:** review the use of DSS in risk management in the context of CIs; identify the elements and peculiar requirements when developing the concept of using a DSS in a context and environment where safety requirement is critical; evaluate the factors and their impact upon perceived efficiency of information systems; develop and validate a model, metric intelligent formal system and application to evaluate cyber security maturity in CI; evaluate and propose recommendations on the cyber security legal framework in CI in the Republic of Moldova.

**The scientific novelty and originality:** an innovative DSS concept, an evaluation model of cybersecurity maturity and DSS efficiency, a knowledge base, a metric intelligent formal system, and a software prototype implementing this system. The prototype also enables the application of the cybersecurity assessment model and presents the results through an easy-to-use interface and easy-to-understand metrics.

**The main scientific problem solved:** ensuring CI cyber security through an innovative solution based on an DSS concept developed as a module and intended to identify, classify and manage cyber risks in CI.

**The theoretical significance:** a developed concept of DSS for cybersecurity maturity assessment. The concept is supplemented by an applicable model for external assessment or self-assessment of CI cybersecurity. Additionally, a metric intelligent formal system and a software prototype implementing the selected evaluation process were developed.

**The applicative value:** a model for DSS efficiency evaluation, a metric intelligent formal system and a software prototype.

**The implementation of results: t**he DSS model has been awarded the Bronze Medal at CadetINOVA 2021 - Innovation and Scientific Research Exhibition, Bronze medal at the International Exhibition of Inventions and Innovations „Traian Vuia" 2022, has been positively evaluated and assessed as applicable for the CI domain by the Slovenian Nuclear Security Administration, National Institute of Metrology from Moldova, Technical University of Moldova, as well as included in the master's degree curriculum in „Nuclear and Radiological Safety" within Technical University of Moldova. The copyright on the intelligent formal metric system has been registered with AGEPI.

# ADNOTARE

**Teza „Sisteme de suport decizional pentru identificarea și diminuarea riscurilor cibernetice în infrastructuri critice” este scrisă în limba română de dl Aurelian BUZDUGAN pentru îndeplinirea cerințelor pentru doctorat în informatică, specialitatea 121.03 – Programarea calculatoarelor. Teza a fost elaborată la Universitatea de Stat din Moldova, Chișinău, 2022.**

**Structura tezei**: Teza constă din Introducere, trei capitole, concluzii și recomandări. Bibliografia cuprinde 191 de titluri. Lucrarea conține 131 de pagini de text de bază, 17 figuri, 4 tabele și 7 anexe. Rezultatele obținute au fost publicate în 28 de lucrări științifice cu un volum de peste 7 coli autor.

**Cuvinte cheie:** sisteme suport decizionale, infrastructuri critice, managementul riscurilor cibernetice, sistem limbaj, sistem de prezentare, dimensiune umană, model pentru evaluarea maturității securității cibernetice, baza de cunoștințe, sistem formal metric inteligent, arhitectura aplicației.

**Scopul:** dezvoltarea, evaluarea și validarea potențialului și a utilizării SSD în gestionarea riscurilor cibernetice în IC.

**Obiective de cercetare:** evaluarea utilizării SSD în gestionarea riscurilor în contextul IC; identificarea elementelor și a cerințelor specifice pentru dezvoltarea conceptului de SSD în corelare cu contextul dictat de cerințele de siguranță și securitate în IC; evaluarea factorilor și impactul acestora asupra eficienței percepute a sistemelor informaționale; dezvoltarea și validarea unui model, sistem formal metric inteligent și aplicație pentru evaluarea maturității securității cibernetice în IC; evaluarea și propunerea recomandărilor privind cadrul legal de securitate cibernetică a IC în Republica Moldova.

**Noutatea și originalitatea științifică:** un concept SSD, un model de evaluare a maturității securității cibernetice și a eficienței SSD, o bază de cunoștințe, un sistem formal metric inteligent și un prototip software ce implementează acest sistem. Prototipul permite totodată aplicarea modelului de evaluare a securității cibernetice și prezintă rezultatele printr-o interfață ușor de utilizat și metrici ușor de înțeles.

**Principala problemă științifică rezolvată:** asigurarea securității cibernetice IC printr-o soluție inovativă bazată pe un concept de SSD dezvoltat ca modul și destinat identificării, clasificării și managementului riscurilor cibernetice în IC.

**Semnificația teoretică:** A fost dezvoltat un concept de SSD pentru evaluarea maturității securității cibernetice. Conceptul este suplimentat de un model aplicabil pentru evaluare externă sau autoevaluare a securității cibernetice IC. Adițional, a fost dezvoltat un sistem formal metric inteligent și un prototip software care implementează procesul de evaluare selectat.

**Valoarea aplicativă:** un model pentru evaluarea eficienței SSD, un sistem formal metric inteligent și un prototip software.

**Implementarea rezultatelor științifice:** Modelul SSD a fost premiat cu Medalia de bronz la Salonul Internațional al Inovării și Cercetării Științifice CadetINOVA 2021, Medalia de bronz la Salonul Internațional de Invenții și Inovații „Traian Vuia” 2022, avizat pozitiv de Administrația Slovenă pentru Securitate Nucleară, Institutul Național de Metrologie din Moldova, Universitatea Tehnică a Moldovei, precum și inclus în curriculumul de master al disciplinei „Securitate nucleară și radiologică” din cadrul UTM. Dreptul de autor privind sistemul formal metric inteligent a fost înregistrat la AGEPI.

# АННОТАЦИЯ

**Диссертация «Системы поддержки принятия решений для идентификации и минимизации киберрисков в критических инфраструктурах» написана на румынском языке г-ном Аурелиан БУЗДУГАН в соответствии с требованиями докторской программы в информатике, специальность 121.03 - компьютерное программирование. Диссертация разработана в Государственном Университете Молдовы, Кишинев, 2022 г.**

**Структура диссертации**: Диссертация состоит из введения, трех глав, выводов и рекомендаций, библиографии из 191 названий. Работа содержит 131 страницы основного текста, 17 рисунков, 4 таблиц и 7 приложений. Полученные результаты опубликованы в 28 научных работах объемом более 7 авторских листов.

**Ключевые слова:** системы поддержки принятия решений (СППР), критические инфраструктуры (КИ), управление киберрисками, языковая система, система представления, человеческое измерение, модель оценки зрелости кибербезопасности, база знаний, интеллектуальная формальная метрическая система, архитектура приложения.

**Цель исследования**: разработка, оценка и апробация потенциала и использования СППР в управлении киберрисками в КИ.

**Задачи исследования**: оценка использования СППР в управлении рисками в контексте КИ; определение специфических элементов и требований для разработки концепции СППР в соответствии с контекстом, продиктованным требованиями безопасности в КИ; оценка факторов и их влияние на воспринимаемую эффективность информационных систем; разработка и валидация модели, формальной системы и приложения для оценки зрелости кибербезопасности в КИ; оценка и предложение рекомендаций по нормативно-правовой базе кибербезопасности в КИ в Республике Молдова.

**Научная новизна и оригинальность:** оригинальная концепция СППР, модель оценки зрелости кибербезопасности и эффективности СППР, база знаний, интеллектуальная формальная система и программный прототип, реализующий эту систему. Прототип также позволяет применять модель оценки кибербезопасности и представляет результаты с помощью простого интерфейса и простых показателей для понимания.

**Главная решенная научная проблема:** обеспечение кибербезопасности КИ за счет инновационного решения, основанного на концепции СППР, разработанного в виде модуля и предназначенного для выявления, классификации и управления киберрисками в КИ.

**Теоретическая значимость.** Концепция СППР была разработана для оценки зрелости кибербезопасности. Концепция дополняется применимой моделью внешней оценки или самооценки кибербезопасности КИ. Кроме того, были разработаны интеллектуальная формальная система и прототип программного обеспечения, реализующие выбранный процесс оценки.

**Практическая ценность работы**: модель оценки эффективности СППР, формальная система и прототип программного обеспечения.

**Внедрение научных результатов:** Модель СППР была награждена Бронзовой медалью на международном конкурсе инноваций и исследований CadetINOVA 2021, Бронзовой медалью на Международной выставке изобретений и инноваций „Traian Vuia” 2022, положительно оценена Управлением Ядерной Безопасности Словении, Национальным Институтом Метрологии Молдовы, включена в учебную программу мастерата ТУМ по дисциплине «Ядерная и Радиационная Безопасность». Авторское право на интеллектуальную формальную метрическую систему было зарегистрировано AGEPI.

**UNIVERSITATEA DE STAT DIN MOLDOVA**

Cu titlu de manuscris
C.Z.U.: 004.056(043.2)=111

**BUZDUGAN AURELIAN**

# SISTEME DE SUPORT DECIZIONAL PENTRU IDENTIFICAREA ȘI DIMINUAREA RISCURILOR CIBERNETICE ÎN INFRASTRUCTURI CRITICE

**121.03 Programarea calculatoarelor**

Rezumatul tezei de doctor în informatică

**CHIȘINĂU, 2022**

**BUZDUGAN AURELIAN**

# SISTEME DE SUPORT DECIZIONAL PENTRU IDENTIFICAREA ȘI DIMINUAREA RISCURILOR CIBERNETICE IN INFRASTRUCTURI CRITICE

**121.03 Programarea calculatoarelor**

Rezumatul tezei de doctor în informatică

Aprobat spre tipar: 25.10.2022
Hârtie ofset. Tipar ofset.
Coli de tipar.: 1,8

Formatul hârtiei 60x84 1/16
Tiraj 10 ex
Comanda nr. 170

Centrul Editorial-Poligrafic al USM
Str. Al.Mateevici, 60, Chisinau, MD-2009
Email: cep1usm@mail.ru, usmcep@mail.ru