REVIEW

by Prof. D.Sc. Nikolai Marinov Nikolov, Professor at Plovdiv University "Paisii Hilendarski," regarding the awarding of the educational and scientific degree "Doctor" in the field of higher education - 9.0 "Security and Defense," professional field - 9.1 "National Security," doctoral program "National Security."

Author of the dissertation research: Kostadin Rangellov Bakov

Topic: "Cyberbiosecurity as an Element of the National Security System"

Scientific supervisors: Assoc. Prof. Dr. Ivan Dimitrov Stanchev, Prof. Dr. Iliya Nikolov Iliev

1. General Description of the Presented Materials

By order No. РД-22-1702 from July 18, 2025, of the Rector of Plovdiv University "Paisii Hilendarski" (PU), I have been appointed as a member of the scientific jury for the defense procedure of the dissertation work on the topic: "Cyberbiosecurity as an Element of the National Security System," for acquiring the educational and scientific degree "Doctor" in the field of higher education - 9.0 "Security and Defense," professional direction - 9.1 "National Security," doctoral program - "National Security." The author of the dissertation is Kostadin Rangellov Bakov – a doctoral student under independent preparation at the Department of Political Sciences and National Security, with scientific supervisors – Assoc. Prof. Dr. Ivan Dimitrov Stanchev and Prof. Dr. Iliya Nikolov Iliev from PU "Paisii Hilendarski."

The set of materials presented by the candidate Kostadin Rangellov Bakov in both paper and electronic formats complies with Article 36 (1) of the Regulations for the Development of the Academic Staff at PU, including the following documents: a request to the Rector of PU for opening the procedure for defending the dissertation; a curriculum vitae in European format; a protocol from the Department Council reporting the readiness to start the procedure with a preliminary discussion of the dissertation; dissertation; summary (BG, EN); a list of scientific publications on the dissertation topic; copies of publications on the dissertation topic; a declaration of originality and authenticity of the attached documents.

The candidate has submitted 3 (three) articles, 2 (two) of which are co-authored, 2 in referred publications and 1 in a non-reviewed publication. All publications are accepted for review. The report on compliance with the minimum requirements for the educational and scientific degree "Doctor" shows 50 points collected from group A indicators and 70 points collected from group G indicators.

2. Short Biographical Data for the Candidate

The candidate-assistant Kostadin Bakov has a career in national security, working in criminal police, economic police, countering smuggling, human trafficking, arms trafficking, and proliferations. His career path includes various leadership positions, such as Deputy Director I degree "Police" at the Plovdiv Regional Directorate of the Ministry of Interior, Director of the Territorial Directorate of the Commission for Combating Corruption and Forfeiture of Unlawfully Acquired Property – Plovdiv, and Commercial Director at Traffic SOT

EOOD – Plovdiv. Since May 2021, he has been an assistant at PU "Paisii Hilendarski", Faculty of Security Studies, Department of Political Sciences and National Security.

His education includes a master's degree in finance and banking from the D. A. Tsenov Academy of Economics in Svishtov. He graduated from Secondary Specialized Education at the Musical School "F. E. Dzerzhinski" in Pazardzhik. This combination of practical and academic training is the foundation for his successful career in the security sector.

3. Relevance of the Topic and Justification of Goals and Objectives

The **object** of the dissertation research is cyberbiosecurity as an element of the national security system. The **subject** of the study is the legal and technical aspects of cyberbiosecurity, combining knowledge in three different fields – national security, information technology, and molecular biotechnology, which align with security and operational-investigative aspects.

The **aim** of the dissertation is to create a concept for protecting cyberbiosecurity in the Republic of Bulgaria.

To achieve the stated aim, the following research **tasks** have been defined: to analyze the current state of cyberbiosecurity and its place within the national security system; to examine biological weapons and classify them through the lens of scientific achievements in molecular biotechnology; to identify dangers and threats and determine the degree of risk from cyberbioattacks; to systematize the obtained results and propose a model for a cyberbiosecurity concept; to define directions for development and improvement of activities to counter cyberbioattacks; to analyze the effectiveness of rapid diagnostic methods for diseases as a risk factor for biosafety.

Research Hypothesis:

Based on the observed absence of a concept, doctrine, and programs for cyberbiosecurity in Bulgaria and the increasing interconnection of information systems with biomedical and biotechnological data, the hypothesis is formulated that the development and implementation of an integrated model for cyberbiosecurity, encompassing legal, technical, and organizational aspects, will significantly enhance the resilience of the national security of the Republic of Bulgaria against cyberbioattacks and minimize the risks arising from sharing sensitive databases in the context of EU membership. This model should include a strategy for countering biological weapons, systematizing threats and risks, as well as guidelines for developing and improving preventive and responsive activities concerning cyberbioattacks.

Theoretical and Methodological Basis of the Research

The theoretical and methodological basis of the research employs a systems approach; theories of management and conflictology; theories and practices of creating biosensors; and the theoretical foundations of molecular biotechnology. The dissertation research utilizes national institutional and educational regulatory documents, encyclopedic and reference literature, and other educational-methodological materials.

Methodology and Methods of Research

In the course of the research, a complex of methods has been used:

- Theoretical methods: analysis and synthesis of the general characteristics of cyberbiosecurity, requiring an interdisciplinary approach to the planned studies.
- Empirical methods: observation of the environment to identify risks in protecting and transferring sensitive biological data, surveys of different population groups to assess individual and community risks in the transfer and storage of sensitive biological databases, expert evaluation of the applicability of biosensors and rapid diagnostic techniques for potential biological threat agents.
- Statistical methods: various methods are employed for processing, summarizing, and analyzing the results of sensitive biological databases.

To ensure proper focus, specificity, and depth of the research, the following limitations are accepted:

1. Detailed examination of sources investigating models of biosensors and diagnostic tests for detecting potential biological threats.
2. Activities of other participants in counteractions as part of the national security system are not subject to this research.
3. The time frame of the research is 2022 - 2025. The spatial (territorial) scope includes the territory of the Republic of Bulgaria concerning survey studies and an international environment for comparing and analyzing data conducted in an international context.
4. The regulatory framework is current as of January 1, 2025.

The dissertation work of the candidate assistant Kostadin Bakov investigates cyberbiosecurity as an essential element of national security. The relevance of the developed problem is significant both from a scientific and practically applicable perspective because, in the modern world, cyberbiosecurity is becoming critically important for protecting biological data and systems.

4. Understanding the Problem

The candidate Kostadin Bakov is familiar with the current state and appropriately assesses the researched problem, emphasizing the importance of developing strategies, principles, rules, algorithms, and methodologies that will lay the foundations for a cyberbiosecurity concept in Bulgaria, as a member of the EU.

Currently, at the national level, there is an absence of doctrine, concept, and programs for cyberbiosecurity. There are no known scientific publications and developments by other Bulgarian authors addressing the aspects of cyberbiosecurity concerning the sharing of sensitive data.

5. Methodology of Research

The chosen research methodology allows for achieving the stated goals and obtaining adequate answers to the tasks set for resolution in the dissertation. In the **first (preparatory)** phase of the research (2020-2022), the researched problem is analyzed from the technical and

technological perspective in two main fields – information technology and molecular biotechnology (biosensors). Key characteristics of both dynamically developing fields in an interdisciplinary domain are revealed. The subject and object are defined, along with the objectives and tasks of the research, and the working hypothesis is formulated.

In the **second (main) phase** (2023-2024), the conceptual foundations of a platform for building a cyberbiosecurity system are developed. Simultaneously, adjustments are made in the research methodology, and strategies for scientific research of new biosensors are formulated, as well as the application of existing equipment and biosensors for conducting biomonitoring.

In **the third (final) phase** (2025), the results are summarized, and principal conclusions and recommendations presented in the dissertation are formulated.

6. Characteristics and Evaluation of the Dissertation Work

The research problem is scientifically formulated – the national security system lacks an organ responsible for biosafety and cyberbiosecurity. Furthermore, there is a lack of a structure functionally responsible for protecting biosafety and cyberbiostability, as well as a concept for ensuring it. The main findings from the research emphasize the necessity of an integrated approach to cyberbiosecurity, including technical and organizational measures.

The survey conducted among specialists working in various fields such as security, cybersecurity, and clinical laboratories also shows alarming results. They indicate a low level of preparedness for protecting sensitive biomedical data and a lack of preparedness for response to bioterrorist threats. This underscores the need for immediate actions to improve capacity and preparedness in protecting these key sectors. The research remains relevant, as, in the context of digitization and globalization, the threats to biosafety are growing.

7. Contributions and Significance of the Development for Science and Practice

The **validity** and **justification** of the results of the dissertation are ensured by the logical flow of the investigation and the applied conceptual and theoretical-methodological basis.

The scientific novelty of the research consists of revealing the interconnections between biosafety, cybersecurity, and the security environment, in constructing a model for cybersecurity as an element of the national security system.

The theoretical significance of the research lies in solving the scientific task – the formulation of a concept for cyberbiosecurity. The research offers new concepts and models for integrating cybersecurity with biosafety and physical security, which had previously not been sufficiently explored.

The practical significance of the research lies in presenting a system of devices and biosensors that can be used for rapid analysis of potential bioterrorist agents. Practical solutions and strategies for the protection of sensitive data are proposed, providing a wide range of applications in the public and private sectors.

The dissertation presents significant scientific and applied achievements related to cyberbiosecurity as an important component of national security:

8. Model for Security Integration: A model has been developed that combines physical security with cybersecurity and biosafety. This is key to achieving permanent control over organizations and companies working with sensitive data.
9. Cyberbiodefense Concept: A concept has been presented that unites the legal and technical aspects of cyberbiodefense. It has the potential to serve as a basis for developing strategies to protect sensitive personal data.
10. Interdisciplinary Approach to Cybersecurity Activities: This approach includes methodologies for processing large datasets related to citizens' personal information.
11. Biosensors and Rapid Analysis: Systems of devices and biosensors have been proposed to conduct rapid analysis of potential bioterrorism agents. This practical application could improve readiness to respond to biological attacks.
12. Awareness Assessment: Empirical studies have been conducted that analyze awareness levels among specialists and authorities regarding cyberbiological risks. The results confirm the need for training and raising awareness.
13. Protocol Development: Specific requirements have been established for the methodology regarding interaction between physical security and cybersecurity. This is an important aspect for the protection of sensitive personal data and response to incidents.

Based on the analysis and findings from the research, specific measures have been proposed to improve cyberbiodefense:

1. Development and Adoption of New Legal Regulations: Regulations should cover the specific needs of cyberbiodefense. These legal acts should include requirements for the protection of biomedical data and procedures for responding to incidents. Special attention should be paid to Regulation MIS 2, which introduces mandatory security and privacy standards for medical information.
2. Regular Training and Seminars for Health Institution Employees: Conducting regular training and seminars for health institution employees regarding good cybersecurity practices.
3. Investment in Modern Cybersecurity Technologies: Including intrusion detection systems (IDS), to prevent intrusions, and tools for monitoring network traffic. These should be implemented in critical infrastructures and continuously updated.
4. Participation in International Forums and Initiatives: For the exchange of information and best practices in the field of cybersecurity. Establishing partnerships with countries and organizations for joint projects and research.
5. Organizing Regular Simulations and Exercises: For response to cyberattacks and bioterrorist threats. These exercises will help institutions identify weaknesses in systems and develop effective action plans.

6. Public-Private Partnerships: Promoting public-private partnerships between government agencies, academic institutions, and the private sector to develop innovative solutions and technologies for cybersecurity.
7. Regular Monitoring and Auditing: Of the cybersecurity systems in health institutions and laboratories. This will help in the early detection of vulnerabilities and timely remediation.
8. Special Attention to Research Centers Working with Genetically Modified Organisms (GMOs): These centers should be equipped with specific protective measures for their databases and experimental results, as the potential consequences of compromising this information can be particularly serious.

Based on the developed dissertation work, the following scientific and applied contributions are delineated:

1. A model is proposed for combining physical security with cybersecurity and biosafety in the oversight of institutions, organizations, and firms working with sensitive data.
2. A model for an interdisciplinary approach has been developed to enhance activities for ensuring cybersecurity concerning sensitive personal data – processing large volumes of sensitive information – regulations for storage and access to sensitive large databases.
3. A concept for an interdisciplinary approach is proposed to develop protocols for activities to ensure cybersecurity when dealing with sensitive data concerning individuals' health status.

The dissertation work by Kostadin Bakov represents a significant contribution to the field of cyberbiodefense. The scientific and applied achievements emphasize the necessity for integrated and proactive approaches to the protection of sensitive data and biological systems. First, developing an integrated model for cybersecurity that synchronizes physical security with biosafety is of critical importance for protecting sensitive data and biological systems in the face of increasing threats. Second, the empirical studies conducted regarding awareness levels among young specialists and professionals underscore the need for training and the development of action protocols in response to cyberattacks and bioterrorism. Third, the concept of a new discipline in cyberbiodefense, foundational for future studies, is of particular significance for national security.

8. Assessment of Publications Related to the Dissertation Work

General Description of the Publications

1. Bakov, K. New Realities in Security and Defense, scientific journal "Security and Defense" – National Military University "Vasil Levski," Year III Issue 1, 2024.

The report "New Realities in Security and Defense" examines the changing dynamics in the field of security and defense, especially in the context of modern hybrid threats that merge cyber and physical security. The primary focus is on the need for integrated strategies and approaches that combine various security aspects, including technological innovations and

inter-institutional cooperation. The importance of adaptability and proactivity in security policies is emphasized to address the new challenges faced by society.

2. Mollova-Doshkova, D., Bakov, K., Iliev, I. The Art of Asking and Analyzing Sensitive Questions in Breast Milk Microbiome Research, Acta Microbiol. Bulg., accepted for publication in issue 40(2) for 2024.

The main content of the study "What Art of Asking and Analyzing Sensitive Questions in Breast Milk Research" highlights the significance of human milk as a primary source of microbial colonization in newborns, playing a critical role in their gut microbiome development. The study emphasizes the challenges in designing surveys to gather information regarding mothers' attitudes towards breastfeeding and the importance of breast milk microbiota. The results indicate that a significant percentage of mothers are willing to participate in scientific research related to breast milk microbiota, underlining the necessity of awareness about the benefits of breastfeeding.

3. Bakov, D., Yanev, D., Nizivanov, S., Shuliev, D., Uihilov, D., Kasnikov, P., Bakov, K., ... & Riliev, R. (2025). Uniting Health Risks Associated with Body Modifications (Tattooing and Permanent Makeup): A Systematic Review. Cosmetics, 12(1), 8.

The study "Uniting Health Risks Associated with Body Modifications (Tattooing and Permanent Makeup): A Systematic Review" examines the potential health risks associated with tattoos and permanent makeup in the context of their prevalence and subsequent health issues. The main identified risks include disruptions to the skin microbiome, inflammatory processes, infections, allergic reactions, tattoo ink toxicity, and insufficient hygiene. The article focuses on the physical and health risks associated with body modifications.

Kostadin Bakov's articles are studies in related fields. The first article regarding health risks associated with body modifications provides critical data about the immediate and long-term consequences of practices related to physical security that enrich the concept of cyberbiodefense. The second article on the microbiome of breast milk highlights the need for innovations in the health system, crucial in the context of protecting biological data and microbiome research. The third article regarding new realities in security and defense offers strategic approaches for integrating physical security with cybersecurity. They supplement the theoretical foundation of the dissertation with practical examples and data.

The publications can be classified by type (articles - 3), significance (articles in impact-factor publications - 3), publication venue (articles in referred international journals - 2; 1 in non-refereed), language (in English - 3), and number of co-authors (single-authored - 1; with two co-authors - 1; with three or more co-authors - 1).

9. Personal Involvement of the Doctoral Candidate

Kostadin Bakov demonstrates personal commitment and an active role in the conducted dissertation research. This includes not only formulating the main topic and structure of the study but also conducting in-depth analyses of cybersecurity, physical security, and biosafety. The candidate has formulated a cybersecurity management concept, which is an original contribution to the scientific field. The conducted empirical research proves his personal

commitment, as he has studied awareness levels among specialists and analyzed the collected material. Candidate Kostadin Bakov participates in scientific conferences, where he presents the results of his research. There, he showcases his ability to integrate knowledge from national security, information technology, and molecular biotechnology.

10. Summary of the Abstract

The abstract has been developed according to the requirements and reflects the main results achieved in the dissertation.

11. Critical Remarks and Recommendations

To enhance the generalizability of the results, it is necessary to expand the geographical scope for the identification and verification of key indicators in cybersecurity. To this end, I recommend that the candidate's future scientific research include studies in different regions of Bulgaria and within an international context to determine how cultural and social factors influence attitudes and protective measures in the field of cybersecurity.

12. Personal Impressions

I work as part of a team with the candidate Assoc. Kostadin Bakov on fundamental bachelor's disciplines with a practical orientation – "Fundamentals of Operational Investigation Activities," "Operational Investigative Activities for Detecting Crimes," "Intelligence and Analysis," where he develops and conducts role plays, simulation exercises, and practical tasks at a high level of theoretical and practical training.

13. Recommendations for Future Use of Dissertation Contributions and Results

I recommend developing training programs focused on the preparation of young specialists in the fields of cybersecurity.

CONCLUSION

The dissertation contains scientific, applied, and practical results, which represent an original contribution to science and comply with all requirements of the Law for Development of the Academic Staff in the Republic of Bulgaria (LDAS), the Regulation for Implementation of LDAS, and the relevant Regulations of PU "Paisii Hilendarski."

The candidate has presented a sufficient number of scientific works. There are original scientific and applied contributions in his work. His theoretical developments also have practical applicability, with some directly oriented and implemented by him in his teaching and educational work. The scientific and pedagogical qualifications, experience, and service of the candidate Assoc. Kostadin Rangellov Bakov are unquestionable and of high quality in their content.

The dissertation demonstrates that candidate Kostadin Rangellov Bakov possesses in-depth theoretical knowledge and professional skills in the scientific specialty “National Security,” showcasing qualities and capabilities for conducting independent scientific research. For the above reasons, I confidently give my positive evaluation for the conducted research presented in the reviewed dissertation work, abstract, achieved results, and contributions, and I

propose to the honorable scientific jury to grant the educational and scientific degree “Doctor” to Kostadin Rangellov Bakov in the field of higher education: 9.0 "Security and Defense," professional direction 9.1 "National Security," doctoral program "National Security."

11.08.2025 **Reviewer: Prof. D.Sc. Nikolai Marinov Nikolov**

……..