

# **OPINION**

**of a dissertation  
for awarding an educational and scientific degree of "Doctor" in**

**in the field of higher education – 5. Technical Sciences  
the professional field – 5.3 “Communication and Computer Engineering”  
doctoral program – "Communication Networks and Systems"**

**Author: M.Sc. Iskren Pavlinov Yankov**

**Topic of the dissertation: Innovation, Methodology, and Design of a Model for Cyber Defense and Cybersecurity of Communication Networks and Systems of Government Structures and Institutions**

**Member of the scientific jury: Assoc. Prof. Krasen Kirov Angelov, PhD**

## **1. Topic and relevance of the dissertation work**

The dissertation work of M.Sc. Iskren Yankov is dedicated to the processes, approaches and models for the development and implementation of adaptive systems for the prevention and protection against cyber-attacks and hybrid threats through integrated methodologies and technological solutions. Considering the importance of protection of communication networks and systems of state structures and institutions, the research in the dissertation is of an innovative nature and a categorical guarantee of the relevance of the issues and a real challenge for in-depth dissertation research.

The object of research in the dissertation is the computer networks and systems of state structures and institutions and the risks of local damage despite the existing protection mechanisms in state institutions. The main emphasis is placed on the identification of risks to information resources, based on the continuous monitoring of computer networks to detect potential threats to information security. This process includes simulations of risk situations to assess the stability of network systems, similar to stress tests used to determine the level of protection.

The structure of the dissertation includes an introduction, four chapters, analysis and conclusions, list of abbreviations used, list of main contributions, scientific novelty of the dissertation, list of publications on the topic of the dissertation, and a reference list. The dissertation, with a volume of 119 pages, is developed on the basis of an analytical review of 128 literary sources, including 57 in Bulgarian and Russian, 63 in English and 8 Internet-based sources. Not all of the listed sources are cited in the dissertation.

The introduction in the first chapter of the dissertation shows that the doctoral candidate has a good knowledge of the state and regulations regarding cyber protection and security in computer systems and networks, the main global cyber threats and those specific to Bulgaria. This knowledge has allowed the author to correctly assess the current state of the problem and formulate research objectives in the dissertation work.

## **2. Research methodology**

The dissertation work aims to develop an innovative model for cyber defense and cyber security based on modern approaches and technologies.

The research methods in the dissertation work are based on analytical models, simulation modelling in a virtual environment and experimental research in an isolated real environment. The tools used for simulation modelling in a virtual environment were databases, specialized virtualization platforms, specialized scripts, software tools for auditing, filtering, prevention, detection and protection against cyber threats, risk assessment, etc. An isolated network infrastructure is used as a tool for experimental measurements, together with specialized management, monitoring and visualization tools. The chosen research methodology is adequate.

The purpose of the research is to analyze and evaluate: the mechanisms for implementing, conducting and countering cyberattacks; the functionality of the individual plan for attacks on various structural objects; the methodology and strategies that a state should implement in its cyber defense policy in order to ensure the protection of all state institutions against cyberattacks and cyber wars.

## **3. Contributions of the dissertation work**

The contributions of the dissertation work can be classified as scientific-applied and applied, which can be generally formulated and summarized as follows:

### **A) Scientific-applied contributions:**

- An assessment of the impact of significant historical cyber-attacks on state and private institutions on the functioning of computer systems and networks has been carried out.
- A concept has been developed and empirically validated to significantly increase the effectiveness of protection against modern cyber threats by integrating local protection mechanisms into a single global cybersecurity system.
- A new model has been proposed in which local and global protection systems work synchronously to transfer and protect data, ensuring continuity and reliability of processes.
- An innovative model has been created that allows effective interaction between local and cloud infrastructures using encrypted communication tunnels, which guarantees the integrity and security of data in the field of cyber defense at the state level.

### **B) Applied contributions:**

- Each of the components of the proposed new model has been studied, which has proven the efficiency of the cyber defense approach at local and global points, and the time limits from system infection and threat detection to their neutralization have been studied.
- An algorithm for encrypting information in communication tunnels has been developed for the model created, in order to ensure the reliability of the connection and the integrity of the data.
- The possibility of defining the cyber defense of systems in three approaches has been identified: an approach with local protection, through the systems Cisco Meraki MX, Cisco Umbrella, Cisco Defense Orchestrator, which is entirely cloud-based, and in a cloud module Cloud Security Device Connector. This local protection grows into a state cloud structure of

cyber defense, and the third approach is through the construction of two types of disaster recovery centers.

– Schemes and topologies with an analytical sequence for applying the model have been developed, as well as the stages and methodology of actions have been described, in order to provide input data for the creation of a cyber defense and cyber protection system adaptable to any infrastructure.

#### **4. Publications and citations of publications on the dissertation work**

The results of the dissertation have been published in 5 publications: 4 in Bulgarian language and 1 in English language. All publications are independent. One of the presented publications was presented at the International Conference on Theoretical and Applied Computer Science and Engineering – Istanbul, Turkey, 2018 (ICTACSE 2018). The remaining 4 publications are conference proceedings presented in the National Reference List of contemporary Bulgarian scientific publications with Scientific Review: 1 of them was presented at the XXX International Symposium of Union of Automation and Informatics "John Atanasov", Sofia, 2022; the remaining 3 publications are reports from the national scientific conference TechCo – Lovech 2023 and 2024.

The publications promulgate the research carried out and present the main conclusions of the dissertation work. There is no information on known citations of dissertation publications and publications referenced and indexed in global Scopus databases.

The publication activity of the PhD student covers the minimum national requirements and the requirements of the regulations for awarding of the educational and scientific degree “Doctor”.

#### **5. Authorship of the obtained results**

From the presented publications, as well as from the dissertation work, it can be seen that a significant amount of research and experimental activity was carried out by the PhD student under the guidance of his scientific supervisor. The presented results build on the existing approaches, methods, models and architectures for cyber defense and cyber security of communication networks and systems of state structures and institutions and prove the proposed innovative model of architecture for information security and cyber defense of a given state and its structures.

I believe that the main part of the conducted research and compiled analyzes of the results are entirely the personal contribution of the PhD student.

#### **6. Comments, recommendations and remarks on the dissertation work**

The topic of the dissertation is relevant and interesting. My personal opinion is that the work has a sufficient volume and the necessary depth of research. The obtained results are significant enough for the educational and scientific degree “doctor”. The publicity of the work is ensured and proven by publications at peer-reviewed scientific conferences.

I have the following important remarks and recommendations regarding the dissertation work:

- 1) The large number of abbreviations suggests a wider list of abbreviations used.

- 2) Part of the conclusions in Chapters 1, 2 and 3 are of a consensual and generally applicable nature and should be refined with regard to the proposed innovative model for cyber defense and cyber security based on modern approaches and technologies.
- 3) Chapter 3 could be more precisely and clearly integrated into the overall development of the dissertation.
- 4) I recommend the doctoral student to publicize his research and achieved results in prestigious scientific journals and international scientific conferences indexed in the world-famous Scopus/Web of Science databases.

The presented remarks and recommendations do not detract from the results achieved by the PhD student on the scientific subject in the dissertation

## **7. Conclusion**

My personal opinion is that the submitted dissertation work **meets the requirements** of the Law on the Development of the Academic Staff in the Republic of Bulgaria. The achieved results give me reason **to propose** that the educational and scientific degree "Doctor" be acquired from M.Sc. Iskren Pavlinov Yankov in the field of higher education – 5. Technical Sciences, professional field – 5.3 “Communication and Computer Engineering”, doctoral program – “Communication Networks and Systems”.

13.12.2024

**Member of the scientific jury:**     /signature/  
/Assoc. Prof. Krasen Angelov, PhD/