



REVIEW

By: Assoc. Prof. Eng. Ognyan Fetfov

Higher School/University/Scientific Organization: University of Telecommunications and Post

Doctoral program: Theoretical foundations of the communication technology“

Field of higher education: 5. „Technical Sciences““

Professional direction: 3.3. „Communication and Computer Technique“

Regarding: Dissertation for conferring the ONS „Doctor“; on Professional direction: 5.3. Communication and Computer Technique, Doctoral program „Theoretical foundations of the communication technology “, Department of Telecommunications, UTP.

Author of the dissertation: Tsvyatko Dobrinov Bikov

Dissertation topic: Methodology for detecting and countering complex cyberattacks in corporate environments

Basis for presenting the review/opinion: participation in the scientific jury for the defense of a dissertation, in accordance with the Order №3-УПА-108/01.07.2025 of the Rector of UTP



1. Brief information about the PhD student

Eng. Tsvyatko Bikov graduated with a bachelor's degree from the Higher School of Telecommunications and Posts-Sofia and a master's degree in Telecommunication Networks from the University of Ruse "Angel Kanchev". He has successfully completed two CISCO courses at Sofia University "St. Kliment Ohridski", for which he holds certificates.

He has successively worked as an IT support specialist, network administrator, information security expert, security architect and cybersecurity manager in a bank and a cloud services provider. His professional experience closely corresponds to the topic of the dissertation and is a certificate of in-depth knowledge of the subject.

He has been enrolled in part-time doctoral studies in the doctoral program: "Theoretical Foundations of Communication Technology" in the Department of Telecommunications with Order No. Z-6823.04.2021. with scientific supervisors Prof. Dr. Eng. Dimitar Radev and Prof. Dr. Eng. Teodor Iliev.

Eng. Bikov has fulfilled the requirements of his individual curriculum and has been discharged with the right to defend by Order No. Z-UPA-39/04.04.2024.

Eng. Bikov has been assigned a teaching workload in the department as an assistant in disciplines related to the topic of the dissertation work from the curriculum of students in the specialty Telecommunication Technologies.

2. General characteristics of the presented dissertation

The content of the dissertation covers issues related to the implementation, maintenance and operation of security systems in the communication sector.

Solutions are proposed to optimize the processes of detecting and responding to complex cyberattacks in real time. Methods for filling gaps in the classification and processing of cyberthreats using neural networks with associative memory are defined and justified.

The work is structured in an introduction, four separate chapters, divided into paragraphs, contributions, applications, used literature and abbreviations.

Each chapter is a separate part of the work and ends with conclusions that summarize the results obtained. The connection between the chapters is provided by the logic of the presentation and allows one to obtain a comprehensive picture of the scientific research.

In Chapter 1, the author analyzes the types of cyberthreats, attack vectors and current countermeasure methods and on this basis formulates the goal and main tasks of the dissertation. Chapter 2 examines specialized architectures of network security systems and proposes a standardized architectural approach for building, protecting, and troubleshooting corporate networks. Chapter 3 examines the adequacy of mechanisms for detecting and countering cyber threats using an antivirus system with advanced malware prevention features. Chapter 4 presents the practical results, research methodology, and analytical data.

3. Degree of knowledge on the research topic by the PhD student and relevance of the dissertation

Despite the extensive scientific research and applied activity that is being developed worldwide in the field of protection from malicious access to information resources, the competition with cybercriminals is constant and ubiquitous. Therefore, the relevance of the dissertation problem is beyond doubt.

It can be unconditionally assumed that the dissertation addresses current problems related to the development and application of fundamental and applied theory for identifying modern types of cyber threats and methods for delivering

malicious content.

I accept the justification of relevance made by the doctoral student and believe that the considerations presented are correct and well-founded.

The graduation in the professional development of Eng. Bykov in the field of corporate network protection unequivocally proves that he knows the subject, builds on his knowledge and successfully implements it in practice.

4. Assessment of scientific and applied scientific contributions

The material on which the contributions of the dissertation are built is designed as a completed independent scientific study in a specific area of practice, namely - methodology and solutions for countering malicious active activities, efficiency of technologies of different generations in modern telecommunication corporate networks and adequacy of mechanisms for detecting and countering complex cyberattacks.

I accept the formulation of the contributions obtained as a result of the study and believe that the author's claims faithfully reflect the essence of the dissertation.

In my opinion, they can be characterized as justification and proof by new means of significant new aspects in a current scientific field, related to:

- definition and justification of new approaches in the implementation of security mechanisms in a corporate environment;
- definition and justification of a procedure for reducing operational resources and increasing productivity in processing security-related signals and incidents by training neural networks with associative memory

The presentation of the dissertation allows one to trace the logic and cause-and-effect relationships of the analysis and simulation experiments, leaving no doubts about the reliability of the presented scientific material.

5. Assessment of publications on the dissertation

The main results obtained during the development of the dissertation work have been published in five scientific reports, of which: two at the international conference Telecommunications Forum (TELFOR), one at the International Convention on Information and Communication Technology, Electronics and Microelectronics, MIPRO and two at annual scientific conferences of the University of Technology and the University of Information and Communication "G. Benkovski". Of the presented reports, 3 are indexed in Scopus and/or Web of Science and 2 in national databases. In all reports, Eng. Bikov is in first place among the authors.

The content of the publications gives a clear idea of the topic of the research, their mutual connection and specificity and confirms the author's style and the undeniable personal contribution of the author. According to Scopus data, the number of citations of publications with the participation of the doctoral student (including self-citations) is 69. This is an indicator that the research has become known to the international scientific community.

Compared to the minimum national requirements, the total number of points from the doctoral student's publications (60 points) exceeds the required minimum of 30 points.

6. Evaluation of the abstract

The abstract of the dissertation fully reflects the author's research and allows for a comprehensive overview of the results obtained.

7. Conclusion on absence/presence of plagiarism

At the time of writing this review, I am not aware of any evidence of plagiarism. Three of the publications in the dissertation that present the main results of the research [A1, A2 and A4] are indexed in SCOPUS and have been

checked for plagiarism. This gives me reason to believe that there are no grounds for such a conclusion.

8. Critical notes, recommendations and questions

As weaknesses of my proposed material for review, I can note the following:

- part of the material in the second chapter is more descriptive and theoretical in nature, which in my opinion has a place in the first chapter;
- the goal and objectives of the dissertation, formulated in the Introduction, differ from those formulated at the end of the First Chapter;

The final version of the dissertation takes into account the recommendations I gave at the preliminary defense for formulating the tasks and summarizing the contributions of the dissertation work.

9. Conclusion

The overall design and the scientific-applied and applied contributions achieved in the dissertation work and their practical significance logically lead to the conclusion that the dissertation work on the topic "Methodology for detecting and countering complex cyberattacks in corporate environments" with the author M. Eng. Tsvyatko Dobrinov Bikov, meets the requirements of the Act on the Development of the Academic Staff in the Republic of Bulgaria (ZRASRB) and the Regulations for the Implementation of ZRASRB.

The above notes and recommendations are of an editorial nature and in no way reduce the significance of the achieved results.

This gives me reason to propose to the Scientific Jury to award M. Eng. Tsvyatko Dobrinov Bikov the educational and scientific degree "Doctor" in the scientific specialty "Theoretical Foundations of

Communication Technology", professional direction 5.3. Communication and Computer Technology, field of higher education 5. Technical Sciences.

10.08.2025 г.

Sofia

Member of Scientific Board

