REVIEW

of a dissertation
for the acquisition of the educational and scientific degree "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: 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
Reviewer Prof. Plamen Zlatkov Zahariev, PhD, University of Ruse "Angel Kanchev"

1. Topic and relevance of the dissertation work

The design of an effective model for cyber security and information protection in the communication networks and systems of the governmental structures and institutions requires a comprehensive approach, which includes not only the application of innovative technologies, but also the use of a stable methodology for ensuring security, as well as the introduction of a multi-layered defense strategy to address the unique challenges these organizations face.

The modern cyber-attacks are becoming increasingly sophisticated and are based on advanced means of attack, such as software tools to extort users by encrypting their data (ransomware), attacks for deceiving the users (phishing attacks), Man-in-the-Middle attacks, data leakage attacks, etc. To counter these attacks, many organizations use modern technologies, such as artificial intelligence, machine learning and zero-trust architectures. The increasingly complex and growing field of cybercrime and the increasing need for specialists in the field of the cybersecurity are making the processes for ensuring the information confidentiality, integrity and accessibility a constant and very serious challenge.

All this defines the cybersecurity and the cyber-defense as key directions in information security and makes the topic of the dissertation extremely relevant and significant for the modern society.

2. Review of cited literature

A total of 128 references were used in the preparation of the dissertation. Sixty-three (63) of the references are in English, and fifty-seven (57) are in Bulgarian. A total of eight (8) Internet sources were used. A large part of the references are books, including those of world-renowned publishing houses, such as Springer, O'Reilly Media, Oxford University Press, Pearson, John

Wiley & Sons, Wiley, Prentice Hall, etc. Part of the used references in Bulgarian language are from renown university publishing houses.

The dissertation contains an overview, which was made based on sources and materials published mainly in the last 10 years. I believe that the PhD student is well aware of the essence of the researched subject area. I can conclude that through the analysis of the references, the PhD student has made a correct formulation about the goal of the dissertation and that he has well defined the main tasks related to the achievement of this goal.

3. Research methodology

The dissertation is prepared and organized in 119 pages and includes 68 figures and graphics. A clear and correct formulation of the subject area, the objectives of the study, the purpose of the research and the tasks of the dissertation was made. The structure of the dissertation includes four chapters with well formulated conclusions for each of them. The general conclusions for the dissertation and the applied and scientific-applied contributions have been defined and presented.

The First chapter of the dissertation contains an analysis on the main types of cyberattacks, the types of malicious software and the measures to reduce the impact of the attacks or to protect the systems and the networks against them. A factual review with an analysis on the cyberthreats that have been identified in Bulgaria over the years has been carried out. The goal of the dissertation is well defined and the specific tasks for its achievement are also formulated.

In the Second Chapter of the dissertation, an innovative conceptual project for the creation of a multi-layer system for cyber protection of governmental structures and institutions is presented, which includes the stages for establishment of local and cloud protection zones, the development of a comprehensive methodology for cyber defence and the creation of distributed interconnected information centres.

Chapter Three of the dissertation contains analytical studies about popular modern cyberattacks. The methods and tools for simulation and evaluation of Denial-of-Service attacks and Ransomware attacks are synthesized, presented and discussed. The rules, procedures, models and methods to prevent the investigated cyber-attacks and to increase security in communication and network systems have been formulated.

In the Fourth Chapter of the dissertation, a model for cyber defence of governmental structures and institutions is proposed and its functionality is evaluated. Various attacks against distributed cloud systems and data centres are presented. International and national strategies and standards for cybersecurity and cyber-defence are presented and discussed.

The dissertation ends with general conclusions on the conducted research activities and with a presentation about the scientific novelty of the studies done by Eng. Yankov.

4. Contributions of the dissertation work

Based on the presented list of contributions of the dissertation, I propose their redefinition, summarization and presentation as the following scientific-applied and applied contributions:

1. The hypothesis that the integration of local defense mechanisms into a unified global cybersecurity system can lead to the significant increase of the effectiveness of the protection against modern cyber threats is formulated and proven.

2. A new innovative model is presented, in which the local and global protection mechanisms interact during the transfer and protection of data and guarantee the continuity and reliability of the communication processes.

3. A new innovative model for effective communication between the local and cloud infrastructures of government institutions is presented, in which encrypted tunnels are used for connectivity, guaranteeing the integrity and security of the transmitted data.

4. An algorithm for the encryption of the information in the communication tunnels is analyzed, which ensures the reliability of the connection and the integrity of the data.

5. A three-layer model for cyber defense of governmental institutions is formulated, which includes an approach for local protection through specialized communication systems, additional protection of the information through the use of cloud platforms, as well as guaranteeing comprehensive protection through the construction of distributed information data centers.

6. A study on each of the elements of the presented model is made and the workability of the approach to cyber defense of the local and global elements in it is proven by examination of the time range from the moment of the attacks against the systems and their detection to the moment of their neutralization.

7. Schemes for implementation of the model for cyber defense of governmental institutions are developed and the stages and steps for taking actions to create a cyber defense system that can be adapted to the needs of any infrastructure are described.

5. Publications and citations of publications on the dissertation work

A total of 5 publications related to the dissertation have been presented, as follows:

[A.1] I. Yankov, Research of the network infrastructure for maintenance of big data bases, International Scientific Session ICTACSE 2018 – Winter Virtual Conference, November 23-24, 2018, Istanbul; Participation with report, certificate received;

[A.2] I. Yankov, Ensuring cyber protection and security in a computer system connected to the global network, Proceedings: XXX International Symposium of SAI "John Atanasov", p. 53-56, November 10-11, 2022, city Sofia; The symposium is included in NACID;

[A.3] I. Yankov, Cyber warfare – destructive actions without weapons. Modern methodology of Cyber defense, Proceedings of the VII National scientific conference with international participation TK Lovech "TechCo 2023", p. 167-171, June 30, 2023, Lovech; The conference is included in NACID;

[A.4] I. Yankov, Ensuring security of computer networks and mechanisms for their protection, Proceedings of the VII National scientific conference with international participation TK Lovech "TechCo 2023", p. 115-119, June 30, 2023, Lovech; The conference is included in NACID;

[A.5] I. Yankov, Modern cyberattacks in the healthcare sector. Practical methods for prevention and protection, Proceedings of the VIII National scientific conference with international participation TC Lovech "TechCo 2024", p. 148-152, June 28, 2024, Lovech; The conference is included in NACID.

All of the publications are authored by the PhD candidate. One of the publications is in English language, and the other publications are in Bulgarian language. The presented publications cover the minimum requirements for the educational and scientific degree "Doctor". No evidences of known citations of the publications were submitted with the dissertation.

6. Authorship of the obtained results

A sufficient amount of scientific research work has been carried out on the problems of the dissertation. Active work continues in this subject area, which is evident from the used references.

The presented publications on the dissertation and the dissertation itself are giving me the reason to believe that the results, which were obtained within the framework of the presented studies, are to a large extent the sole contribution of the PhD student Iskren Yankov.

7. Abstract and author's reference

The Abstract has a volume of 53 pages and is accurately representing the main studies and the contents of the thesis by presenting a synthesized summary of it, which gives a complete idea of the practical applicability of the results obtained by the PhD student.

8. Comments, recommendations and remarks on the dissertation work

I have no significant critical remarks and comments regarding the presented version of the Dissertation and the Abstract. I recommend to the PhD student to publish more actively the results of his research activities in national and international journals and to continue with his studies in this extremely interesting and modern subject area.

9. Conclusion

I believe that the submitted Dissertation meets the requirements of the Law for Development of the Academic Staff of the Republic of Bulgaria. The achieved results give me the reason to propose to the members of the scientific jury to award the educational and scientific degree "Doctor" to Eng. Iskren Pavlinov Yankov, in the field of Higher Education - 5. Technical sciences, Professional field - 5.3. Communication and computer technology and Doctoral program "Communication networks and systems".

16.12.2024 **Reviewer**: **/signature/**

/Prof. Plamen Zahariev, PhD/