REVIEW

regarding a dissertation work for the acquisition of an
Educational and Scientific Degree „Doctor“ in

higher education area - 5. „Technical sciences”
professional field - 5.3 „Communication and Computer Engineereing”,
scientific specialty - „Communication Networks and Systems”.

Author: M.Sc. Iskren Pavlinov Yankov
Dissertation Topic: Innovation, Methodology and Design of Model for Cyberoth and Cybersecurity of Communication Networks and Systems of State Structures and Institutions
Reviewer: Assoc. Prof. Boyan Dimitrov Karapenev PhD, Technical University of Gabrovo

1. Theme and relevance of the dissertation

Accelerated digitalization in the Republic of Bulgaria in recent years has imposed the development, implementation and refinement of modern communication-information technologies, management and analysis systems of large data (BigData) and increasingly used forms of artificial intelligence, IoT, industry 4 and others. The issue of providing cybersecurity and reliable protection in corporate and company networks and systems of malicious breaches coming from the global Internet arises after the tumultuous and rapid development of digitalization in the Republic of Bulgaria since 2012 with the entry of digital television.

At present, the topic of the dissertation is very up -to -date, as each state and private organization invest considerable investments in ensuring the secure and reliable cyber protection of its systems and information massifs. Safety risks are a prerequisite for significant financial, economic, as well as moral losses and damage.

Modern requirements and regulations require organizations not to allow the expiration of personal and confidential information and data. The creation of methodologies for the organization of networks and systems protection provide effective implementation of counteraction against cyberintimidation and cyberattacks.

The object of the developed dissertation work is theoretical and experimental study of methods and means of enhancing cybersecurity in communication and information networks and systems of state structures and institutions through the implementation of organizational, educational, administrative and technical measures and new solutions leading to risk minimization, despite existing protective mechanisms. Identifying the risks to information resources is a complex and dynamic process based on continuous monitoring of computer networks and systems to detect potential threats in information security and cyber protection.

The dissertation work clearly and accurately defined the reasons, the object, the object, the purpose, the means and the tasks for the implementation and the content of the individual heads fully corresponds to them.

2. Review of cited literature

A total of 128 literary sources were attached to the literature used, of which 56 in Bulgarian, 64 in English and 8 web-adreses. About 20% of them have been issued in the last 5 years.

Not all of these literary sources are cited in the note.

3. Research methodology

On the issue of the developed topic, the dissertation has been working since 2016 and for the time to the present time it has successfully managed the challenges related to providing cybersecurity in communication networks and systems. The research methodology includes theoretically and experimental consideration of methods and tools for improving cybersecurity, offering new copyrights to reduce risk. Analysis of significant cyberattacks has been made

historically, the current regulatory framework has been evaluated and a model to reduce risks has been proposed. The dissertation combines the overview of more than 128 literary sources, mainly publications of articles and reports, analysis and development of model(s) and methodologies to achieve increased cybersecurity of communication and information networks and systems with continuous adaptation of organizational, administrative and technical measures to secure it.

Subject, purpose and tasks of scientific research

The subject of the study is the management of information security in the event of threats to information resources in state organizations viewed as local sites. The study examined methods for managing information security by simulating computer attacks such as „Denial of Service" (DoS) and „Ransomware" on local structures. The aim is to provide evidence to improve information security through effective mechanisms to detect and prevent attacks such as „Denial of Service" and „Ransomware", emphasizing the importance of timely response and adequate protection measures.

The main idea of the studies carried out is that reliable information security management can provide an acceptable level of cyber protittal and cyberotname on computer networks and systems. The construction of a hybrid model combining a cloud, the deployment of On-Prem centers to restore information services after disasters, and the creation of a single system that connects any state structure, both with the state cyberoblak in a fully protected and encrypted environment, can It guarantees the overall security of a country.

The purpose of the dissertation is to evaluate the vulnerabilities of state structures in various cyberattack scenarios by conducting simulations of attacks such as „Denial of Service" (DoS) and „Ransomware" in controlled experimental conditions. By studying the vulnerabilities that have arisen, it is aimed at justifying the need to build an integrated local and global level protection system.

To achieve the goal, the author has formulated and solved the following **tasks**:

1. Identification and analysis of the risks of using computer networks: conducting a theoretical study and analysis of existing threats to information resources. Assessment of factors contributing to the emergence of vulnerabilities in computer networks and systems of state institutions. Study of global cyberspace and disclosure of vulnerabilities: an analysis of technological and large -scale threats, with an emphasis on the factors contributing to the development of cyberattacks at the global and local levels. Assessment of the influence of these threats on the information security of state structures.

2. Development of an innovative information security model: Creation of a protection model based on existing theoretical and practical approaches in the field of information security and cyberothum. The model must integrate a variety of methods and technologies that provide effective protection at both locally and globally.

3. Simulation of computer attacks such as „Denial of Service" and „Ransomware virus" by performing experimental simulations of attacks in order to evaluate their impact on the information and communication resources of state structures, as well as their vulnerability in various cyberattack scenarios.

4. Assessment of the functionality and practical action of the innovative project to provide a high degree of protection of information resources and continuity of services in state institutions. Formation of policies and procedures for protection against cybereptacks. Developing a complex of policies, methodology and mechanisms to provide effective protection against local and global cyberluchs.

The purpose of research involves identifying and analyzing the risks to information security in computer networks and systems of state institutions, the development of an innovative model for cyber protection that integrates various technologies and approaches for local and global protection, simulation studies of attacks, such as „refusing of services" and „Cryptovirus", evaluation of vulnerabilities and preparation of a complex of policies and procedures to provide a high degree of protection and continuity of services in global network

systems and structures, research and analysis of the functionality of individual components of the proposed model.

The purpose of research involves identifying and analyzing the risks to information security in computer networks and systems of state institutions, the development of an innovative cyber -protection model that integrates various technologies and approaches for local and global protection, simulation studies of attacks, such as „refusing of services" and „Cryptovirus", assessment of vulnerabilities and preparation of a complex of policies and procedures to provide a high degree of protection and continuity of services in global network systems and structures, research and analysis of the functionality of individual components of the proposed model.

The middle of the study is laboratory uses of optical methods and systems for cyber protittal and cyberot branch, including Cisco Meraki MX, Cisco Meraki Cloud and Cisco Umbrella models. This methodology offers an innovative solution for hybrid use of local and state cloud structure for the protection of local and global systems, providing comprehensive protection in cybervet. The problem is solved by which countries are striving for global protection of their systems, but often neglect local protection. The combination of various protective systems allows adequate protection to be provided both in the case of a target attack against a separate state structure and in a large-scale global cyberwarm.

The research methods used are analytical, simulation and practical, and cover the receipt of the dependencies of the parameters and characteristics obtained from the implementation of the proposed model(s).

The research methods used - cybersecurity review and literary study; Analysis and evaluation of cybersecurity systems of various state and private institutions, analysis of different cyberattacks historically; the proposed design solution (hybrid model) to increase cybersecurity; Results and analysis of simulating computer attacks of different types - successfully leads to the achievement of the set goal and the accomplishment of the tasks set in the dissertation work.

4. Evaluating the exhibition in the dissertation work

The structure of the dissertation has a total volume of 121 pages and includes Introduction, Chapter 1 - Review of cyber protection and security in computer systems and networks, at the end of which are formulated tasks for implementation, Chapter 2 - Conceptual project for providing cybers and security in A computer system associated with a global trash of a country, Chapter 3 - Simulation research and analysis of the attacks of services and cryptovirus and consideration of the mechanisms of infection, Chapter 4 - Assessment of functionality and methodology of the innovative cyber defense project of state structures and institutions, Analyzes and conclusions, Reference for the main contributions, The scientific novelty and applicability of the development, a List of publications on theme and the Literature used.

5. Contributions to the dissertation

The contributions to the dissertation, according to its content and represented, completely coincide with my opinion and are reduced to:

Scientific-applied contributions

1. Cybersecurity has been carried out, the existing regulatory framework in the Republic of Bulgaria and abroad has been studied and an analysis of significant cyberattacks against state and private institutions has been made in historical terms. The impact of various malware (computer attacks) on the functionality of computer systems and networks has been analyzed and analyzed.

2. It has been developed and empirically confirmed the concept that the integration of local defense mechanisms into a single global cybersecurity system significantly increases the effectiveness of protection against modern cyberbles.

3. A new model has been proposed in which local and global defense systems work in sync in the transfer and data protection, ensuring the continuity and reliability of the processes.

4. The proposed model allows effective interaction between local and cloud infrastructures using encrypted communication tunnels, which guarantees the integrity and security of the data.

Applied contributions

1. An analysis has been made and each of the components of the proposed new model has been examined, which demonstrates the performance of the approach for cyber protection at local and global points, examining the time limits of infection of the system and detecting threats to their neutralization.

2. The proposed model has been developed an algorithm for encrypting information in the communication tunnels to ensure the reliability of the connection and the integrity of the data.

3. The possibility of defining the cyberotbrain of the systems by three approaches is identified: approach with local protection, through the systems of Cisco Meraki MX, Cisco Umbrella, Cisco Defense Orchestor, which is entirely cloudy, and cloud based seam. It grows into a state cloud structure of cyberothtrane. The third approach is through the construction of two types of disaster recovery centers.

4. Schemes and topologies with analytical sequence for the application of the model have been developed, as well as the stages and methodology of actions are described to provide starting data for the creation of a cyber and cyber protection system adaptive to each infrastructure.

6. Publications and cited publications on the dissertation

On the subject of the dissertation work, 5 independent publications were made and presented - 1 Report of the International Scientific Conference ICTACSE 2018 (Istanbul) - in English, 1 Report of the International Symposium of the SAI „John Atanasov" 2022 (Sofia) and 3 reports of the National Scientific Scientific Conference with international participation „TechCo" 2023 and 2024. The number of publications made (papers) complies with the Rules for the development of the academic staff of TU-Gabrovo. No information has been presented on known cited by other authors of the attached publications to the dissertation work. There is no list with other publications of the dissertation, if any.

I believe that the doctoral studies presented in the dissertation contain the main contributions for which he claims.

7. Authorship of the results obtained

The publications made, as well as the structure and content of the dissertation, give me reason to believe that the applicant is undoubtedly its author. He has gained a lot of professional experience in the field of information systems and cybersecurity.

8. Autoreferate and author reference

The autoreraf is represented in a volume of 53 pages and correctly reflects the structure, content of the dissertation, contributions and publications made of the applicant.

9. Opinions, recommendations and notes on dissertation work

Recommendations:

- The exhibition of the dissertation is given the essence of basic concepts and definitions related to cybersecurity that increase the volume of the overview part;
- It is not clear from the exhibition in the dissertation work whether simulation and/or real studies have been carried out and results obtained for the functioning of the proposed model, or of individual components, for cyberoth and cybersecurity of communication networks and systems;
- The stroke of the place in places could be improved.

I recommend the proposed innovative and hybrid model, if possible, can be practically implemented, researched, analyzed and optimized as needed.

I also recommend that the dissertation continues and further deepen its work on the theme of the dissertation work and enriches with its publications the scientific achievements in the field of cybersecurity in modern communication and information networks and systems.

Positives:

- The topics are considered and represented in the great depth of analysis and research and summarizes and offers specialized work and development in the field of cyberoth and cybersecurity in communication networks and systems, and in particular of state structures and institutions;

- The very well generalized defined and submitted conclusions to the individual chapters, as well as the directions for the future development of the subject matter and the application of the results obtained in the dissertation, make an impression;

- A good impression is made with software products and presented figures, mostly structural and block schemes, in the exhibition.

The dissertation work, the autoreferate, the publications, analyzes and conclusions and the achieved scientific-applied and applied contributions undoubtedly show that its author mag. Iskren Pavlinov Yankov has the ability to in -depth literary and theoretical analyzes and studies based on extensive and specialized professional experience in the field of information systems and cybersecurity. This characterizes the dissertation as a narrow specialist in the field of cyberoth and cybersecurity with opportunities for future development.

The topic of the dissertation is very interesting and up -to -date. The work has sufficient volume and depth of the study. The results obtained are significant enough for the acquisition of the educational and scientific degree „Doctor". The publicity of the work is sufficient. The dissertation work has been made by 5 publications.

10. Conclusion

I believe that the submitted dissertation work **meets** the requirements of the Academic Staff Development Act in the Republic of Bulgaria. The results achieved give me reason **to suggest** the acquisition of the Doctor's educational and scientific degree to M.Sc. Iskren Pavlinov Yankov, higher education area - 5. „Technical Sciences", professional field - 5.3 „Communication and Computer Engineereing", doctoral program – „Communication Networks and Systems".

16.12.2024 Reviewer: /signature/

/Assoc. Prof. B. Karapenev, PhD/