REVIEW

by Prof. Dr. Todor Dimitrov Tagarev, Institute of Information and Communication Technologies, Bulgarian Academy of Sciences, professor in the professional area 5.2 "Electrical Engineering, Electronics, and Automatics", scientific specialization in "Application of the Principles and Methods of Cybernetics in Various Scientific Areas"

for acquiring the scientific degree of "Doctor of Philosophy" (PhD) in the doctoral programme "Computer Systems, Complexes, and Networks", professional area: „5.3. Communications and Computer Technologies", with candidate **Ivan Kostadinov Gaidarski**.

Through the order # 48 of February 24, 2022 of Prof. Doctor of Mathematical Sciences Galia Angelova, Director of the Institute of Information and Communication Technologies (IICT), Bulgarian Academy of Science, issued on the basis of article 4(2) of the Law of Developing the Academic Personnel in the Republic of Bulgaria and decision of the IICT Scientific Council, Protocol # 2 of February 23, 2022, I was appointed as member of the Scientific Jury in the procedure for acquiring the educational and scientific degree "Doctor" (PhD) in the professional area: „5.3. Communications and Computer Technologies", doctoral programme "Computer Systems, Complexes, and Networks" by the doctoral student Ivan Kostadinov Gaidarski, who has presented a dissertation under the title "**Method and Models for Development of Information Security Systems in Organizations**".

In writing this review, I took in consideration the requirements and criteria for assessing doctoral dissertations and the accomplishments of the doctoral student as described in the Law of Developing the Academic Personnel in the Republic of Bulgaria, the national regulations for its implementation, and the Regulations for Specific Conditions for Acquiring Scientific Degrees and Appointment at Academic Positions in IICT-Bulgarian Academy of Sciences in its version dated December 22, 2021. In particular, in the text of the review below I will evaluate:

- whether the dissertation includes original scientific or scientific-application contributions, demonstrates in-depth theoretical knowledge of the candidate in the respective scientific area and skills for conducting individual and scientific research and presenting their results;
- technical presentation of the dissertations and availability of a declaration for originality of the research and the achieved results;

- minimal requirements to the number of points by groups of indicators for acquiring the educational and scientific degree “doctor” (PhD) in area “5. Technical Sciences”, professional area: „5.3. Communications and Computer Technologies”, as follows:

Group of Indicators	Content	Minimal Requirements
A	Indicator 1	50
G	Sum of indicators from 5 to 11	30

The candidate has presented for the review a dissertation under the title “Method and Models for Development of Information Security Systems in Organizations” consisting of 153 pages (in Bulgarian), as well as the accompanying autoreferat (abstract), both in Bulgarian and in English.

Relevance and significance of the presented research

The cyberattacks are not anymore a rare, exotic event, but a fact of our daily life, while the spectrum of cyber threats continues to expand and the attacks become ever more sophisticated. Among the targets of such attacks are public organisations, systems supporting the functioning of critical infrastructures, other business organisations, and even individuals. Each organisation has already been or will in the foreseeable future be a target of one or more attacks against its communications and information infrastructure and attempts to steal, encrypt, destroy or manipulate information that is essential for the functioning of the organisation. All this makes the topic of the doctoral research relevant and of significant importance from both scientific and application perspective.

Goal and objectives of the research

Taking into account the current trends and anticipated developments in the cyber domain, the candidate puts the focus of his research on the protection of the organisational information from insider threats. The goal of the doctoral research is formulated accordingly as “development of a method and models for designing information security systems, guaranteeing protection from internal threats directed from inside – out of sensitive information in organisations of various nature and size.” In a feasible manner and by using a widely used model of the process of systems development (visualised in Figure 5), the author formulates the objectives of the dissertational study. This approach allows him to correctly and systematically present the utilised research methods and to structure appropriately the elaboration on the results of the study.

Methodology

In his research, the candidate demonstrates the knowledge and understanding of a broad set of the normative documents, including applicable European directives, international standards, and theoretical and practical approaches to the development of information security systems, as well as the advantages and limitations of their application. That allows him to select a suitable set of principles, and on their basis to elaborate his study. Further, the candidate demonstrates knowledge and skills to use for research purposes a broad set of methods in the scientific and application areas of information and cyber security – system design, data analysis, including the analysis of big data, machine learning and artificial intelligence, system analysis and software engineering.

Structure of the dissertation

The dissertation is structured in an introduction, four chapters, conclusion, bibliography and annexes.

Chapter One presents the theoretical grounds of system design. The author elaborates on the principles, approaches, and methods for designing information security systems, presents the selected design method, and defines the framework for describing the architecture of the information security system.

Chapter Two introduces the main terms and concepts of the subject area – the provision of information security, presents current data on vulnerabilities, threats, their sources, agents and main characteristics, as well as the main approaches and methods for guaranteeing the information security of an organisation.

The third chapter is dedicated to the design of information security systems and presents the projected, architectural and functional model of the system for information protection of a generally defined, distributed organisation.

In Chapter Four the author develops a model of an organisational information security system and simulates its performance. Detailed UML models and technical descriptions are provided in annexes to the dissertation.

Contributions

The candidate claims seven scientific and scientific-application oriented contributions as a result of his doctoral research.

Of those, I accept that of scientific nature is the suggested new classification of the approaches for managing the information security of an organisation according to the type of communications and based on the detailed description of the main concepts in the “information security” area.

My opinion is that two of the contribution are of a scientific-application nature: (1) the proposed new method for designing and developing organisational information security systems that integrates known approaches and models; and

(2) the simulation model of the information security system based on object-oriented description of the architecture and agent-based representation.

I classify the remaining claimed contributions as application-oriented: the multilayer conceptual model, the respective architectural and functional models, the comparative analysis of existing platforms for realisation of the author's method, and its actual implementation over the selected platform.

Formal requirements and originality

The dissertation and the accompanying autorefereat (abstract) are delivered in accordance of the legal requirements and the specific requirements of the Institute of Information and Communication Technologies. Of a particular value is the inclusion of a glossary of the main terms, in both English and Bulgarian, as well as a dictionary with the abbreviations used in the dissertation.

As part of the dissertation the author has submitted a declaration that the presented results are original and achieved by the author. The candidate is aware of the research of his more experienced colleagues and cites correctly their work. He explicitly acknowledges the contribution of his advisor, Associate Professor Rumen Andreev, as well as that of the Head of the "IT for Security" Department of IICT, Associate Professor Zlatogor Minchev, for the support provided in organising and conducting the simulations and the analysis of their results, as presented in section 4.6 of the dissertation.

The candidate also declares that this dissertation has not been used for acquiring a scientific degree in a school of higher education, a university, or another research institute.

Publication and Citations

In the dissertation the author lists five scientific publications, presenting results of his doctoral research, and all five are in the English language. One of the publications is in a journal published by the Bulgarian Academy of Sciences, and another one is a paper presented at a conference in Bulgaria. At least one of the publications (in a Springer volume) is indexed by Scopus. One of the publications is individual, while the other four are co-authored with the scientific advisor and other colleagues from IICT.

The candidate declares in total four citations of two of the publications from the doctoral research. No self-citations are included.

I accept the declared data, which allows to calculate the scientometric indicators. Thus, the candidate considerably exceeds the minimal requirements as established by the Law and the Regulations for Specific Conditions for Acquiring Scientific Degrees and Appointment at Academic Positions in IICT-Bulgarian Academy of Sciences.

Remarks and Recommendations

The doctoral research presented in the dissertation is comprehensive and based on a broad set of methods and models. In these conditions the author not always succeeds in precisely tracking and clarifying the linkages between various models. This is particularly valid for the link between the projected model, presented in Chapter Four, and the models underlying the consequent simulations (section 4.6). This observation, however, does not change my overall assessment of the dissertation.

CONCLUSION

Taking into account all arguments presented above, my positive assessment of the presented dissertation, and the fact that the author meets all requirements of the Law on the Development of the Academic Personnel in the Republic of Bulgaria, the national regulations for its implementation, and the Regulations on the conditions and procedure for acquiring scientific degrees in the Institute of Information and Communication Technologies of the Bulgarian Academy of Sciences, my evaluation is that Ivan Kostadinov Gaidarski can be awarded the educational-scientific degree “Doctor” in the area of higher education “Technical Sciences”, professional area 5.3 “Communications and Computer Technologies”.

Member of the Scientific Jury and

На основание
ЗЗЛД

27 March 2022