KONSTANTIN
PRESLAVSKY
UNIVERSITY
SHUMEN

ШУМЕНСКИ УНИВЕРСИТЕТ
“ЕПИСКОП КОНСТАНТИН ПРЕСЛАВСКИ”
ЗАЕДНО ПИШЕМ ИСТОРИЯТА

REVIEW

By Prof. Krasimir Mitkov Kordov, PhD
Konstantin Preslavsky University of Shumen

of the dissertation of Iliyan Magdalenov Barzev, entitled
„Research and analysis of the possibilities for detection of malware through machine learning”
presented for obtaining the educational and scientific degree „Doctor”, in the professional field 4.6 „Informatics and Computer Sciences”.

Shumen
2026

By order of the Director of IICT-BAS and by the decision of the first session of the Scientific Jury, I have been appointed as a reviewer for this procedure. This review is prepared in accordance with the Development of the Academic Staff in the Republic of Bulgaria Act, the Regulations for its implementation, and the Regulations of IICT-BAS. No signals of plagiarism or violations have been submitted regarding this procedure.

1. Documents

As a reviewer, the following documents are presented to me:

1.1. Application for opening the procedure;

1.2. Dissertation thesis entitled: „Research and analysis of the possibilities for detection of malware through machine learning”;

1.3. Declaration of originality of results;

1.4. Abstract in Bulgarian;

1.5. Abstract in English;

1.6. Order for dismissal (graduation with the right to defense);

1.7. List of publications related to the dissertation and the publications themselves;

1.8. Report on the fulfillment of the minimum requirements of IICT;

1.9. Preliminary opinion on the dissertation;

1.10. Report for registration in NACID;

1.11. Full similarity report (plagiarism check).

2. Brief assessment of the submitted documentation

The documentation is complete and formatted according to regulatory requirements. It provides a clear overview of the doctoral student's qualifications and the credibility of the results. The similarity report shows no unauthorized use of foreign text.

3. Relevance of the dissertation

The topic is highly relevant due to the critical need for data and infrastructure protection from rapidly evolving malware. Since traditional signature-based methods are insufficient, the use of intelligent machine learning approaches is necessary. The goal of developing hybrid models and adaptive frameworks addresses modern cybersecurity challenges.

4. Description of the dissertation

The dissertation has a total volume of 143 pages and consists of an introduction, 3 chapters, conclusion, bibliography from 155 sources. The content includes 43 figures, 20 tables, contributions, a list of publications and noted citations.

The introduction provides an introduction to the subject matter and clarifies the actuality of the topic due to the continuous increase in cyberattacks globally.

The first chapter is introductory and presents an analysis and classification of machine learning algorithms for the detection of malicious software, with a comparative analysis and an analysis of the performance of the considered algorithms being made. Based on the review conducted, the purpose and tasks of the dissertation thesis are defined.

The second chapter presents a model for selecting a virtual machine for conducting experiments for malware detection through the routing of requests between different models based on the level of confidence.

In the Third chapter, numerical experiments and the practical realization of the application „Shipka Guard" are described, which integrates a mechanism for feedback and explainability of decisions.

From the presented 155 literature sources it is clear that an extensive and in-depth literature review of the problem has been made.

5. Contributions

The following scientific and scientific-applied contributions are indicated in the dissertation:

1. Two mathematical models are proposed, through which a selection of software for a suitable virtual machine can be made for the purposes of experimental testing for malware detection.
2. An improved static analysis approach for malware detection is proposed by optimizing feature extraction by combining different machine learning algorithms. Tests conducted with the proposed hybrid algorithms show better performance.
3. A framework for static malware classification is proposed, which uses feature optimization and ensemble learning. The results show that the false positive analysis for the ensemble is significantly lower than that of individual models.
4. Self-aware malware classification is proposed by routing models based on a trust system for feature selection and explainability. The routing logic increases the power of the ensemble with trust-based decisions and provides

a flexible mechanism useful for both historical and contemporary malware characteristics.

5. A trust-aware adaptive framework for malware classification with feedback corrections is proposed. This framework is both adaptive and robust, as it includes a self-aware model classifier that uses adaptive logic to automatically choose between traditional and contemporary model layers by measuring the reliability of the prediction. The integration of explainability contributes to the confidence in the decisions, which is increased by more information about the features from a local and global perspective.

I accept the first two as scientific, and the rest as scientific-applied contributions, and I consider that they fully reflect the results achieved in the dissertation.

6. Abstract

The abstract of the dissertation is 45 pages in volume (43 pages in English version) and adequately reflects the structure and content of the dissertation manuscript and the results presented in it. All necessary structural elements of the dissertation are included.

7. Publications

Based on the dissertation, 4 publications in English have been published indexed in SCOPUS, as 3 of them have an SJR (impact rank). The citation rate of the publications reflects their significance within the scientific community.

From the presented publications, it becomes clear that the doctoral student exceeds the minimum national requirements for obtaining the educational and scientific degree „Doctor”, in scientific area 4. „Natural sciences, Mathematics and Informatics”, in professional field 4.6 „Informatics and Computer Sciences”.

8. Critical assessments, remarks and recommendations

- Conclusions are missing in Chapter 2.
- Some of the contributions are very descriptive and could be shorter and clearer.
- In the numbering of Table 2.1. and in the citation of Table 3.2, technical errors have been made.
- Some spelling and stylistic errors are noticed in the text.
- I recommend publishing separate publications.

9. Conclusion

In conclusion of my review, considering the presented dissertation, I note the relevance of the topic, the in-depth study of the subject area and the obtained contributions. The remarks and the recommendations do not diminish the achieved results. I consider that the presented work is completely sufficient in volume and quality and meets the requirements of the Act for the Development of the Academic Staff in the Republic of Bulgaria, the Regulations for its implementation and the Regulations of IICT-BAS. I give a positive assessment of the presented work on „Research and analysis of the possibilities for detection of malware through machine learning“, and I propose to the esteemed Scientific Jury to award Iliyan Magdalenov

Barzev the educational and scientific degree „Doctor” in scientific area 4. „Natural sciences, Mathematics and Informatics”, in professional field 4.6 „Informatics and Computer Sciences”.

Date: 06.03.2026

НА ОСНОВАНИЕ

ЗЗЛД