

OPINION

Subject: Dissertation by Ivan Lyubomirov Drankov,
on the topic: “Analysis of Leaked Data to Identify Potential Threats to Information Security,”
submitted for the acquisition of the educational and scientific degree of “Doctor”
in the professional field: 5.13. “General Engineering,”
doctoral program “Computer Technologies in Engineering.”
by Associate Professor Dr. Stanislav Dimitrov, IICT-BAS, member of the scientific jury,

Information on the Procedure

According Order No. RD – 13-33 / June 24, 2026, of the Rector of St. Ivan Rilski,” I was selected as a member of the academic jury, and at the first meeting of the academic jury, held on June 30, 2026, I was assigned to prepare an opinion on the procedure, for which I received all the relevant documents.

1. Relevance of the Problem Addressed in the Dissertation from a Scientific and Applied Scientific Perspective

Digital transformation is a process of organizational change driven by the increasingly widespread use of information and communication technologies in the public and private sectors. As a result of this transformation, vast amounts of data containing sensitive, confidential, and critical information are generated, processed, and stored.

At the same time, the development of internet services, cloud platforms, social media, and e-commerce creates conditions for the accumulation of significant data sets. These represent a valuable strategic resource for organizations because they support process analysis, decision-making, and the creation of new services. At the same time, this data has become a primary target for various types of cyberattacks.

Malicious actions by hackers, vulnerabilities in information systems, shortcomings in modern technologies, and low digital literacy among users create conditions conducive to large-scale data breaches. These datasets are characterized by large volume, rapid and intensive accumulation, a variety of formats, and varying degrees of reliability.

These characteristics necessitate the development and implementation of new methodological and technological approaches for the automated processing, analysis, and interpretation of data, which will enable the effective detection of anomalies, the identification of potential cyber threats, and the timely improvement of information security management processes.

Knowledge of the Research Problem

The doctoral candidate demonstrates in-depth knowledge of the field in which he is working and is exceptionally well-versed in the nature of the research problem. This is evidenced by the literature review, which contains a total of 56 sources—primarily in English—and the published results.

2. Analytical Characteristic

The dissertation consists of a total of 131 pages, 82 figures, 9 tables, and 56 references. It is structured as follows: a list of abbreviations and terms, an introduction, 4 chapters, a conclusion, the contributions of the dissertation, and references.

Chapter 1 chronologically traces the impact of information on society and the use of technologies for its dissemination, as well as the need for data protection. It describes in detail the negative phenomenon associated with digital information—data leaks. Methods for classifying the types of leaked information and the legal requirements for handling them are presented. A comprehensive overview of the characteristics and features of existing systems for processing and analyzing leaked data is provided.

Chapter 2 presents a methodology for creating the Active System and Leaked Data Analyzer (ASLDA), outlining the stages of its development, the implementation model, and the possibilities for building, expanding, and maintaining high efficiency.

Chapter 3 presents a study of issues related to data formatting, validation, and verification, as well as data filtering and retrieval based on specific criteria. An analysis of data distribution and the classification of data into various categories has been prepared. An intermediate format for converting standardized and non-standardized data is implemented. Functions for storing raw data and various data compensation techniques are utilized. The various types of analyses implemented in the developed system are described, and scenarios regarding the effectiveness of ASLDA's implementation are examined.

Chapter 4 describes the technological tools, hardware resources, and modules created for the implementation of ASLDA. The implementation of the system as a cloud-based solution and its shortcomings are examined. The process of data collection and initial processing using the pyformat module created by the doctoral candidate is presented, and it is compared with MS Excel in terms of data processing time. All analyses that can be performed and the generation of reports from them are presented in detail. A comparative analysis is presented, demonstrating the advantages of the developed system over existing ones.

The conclusion summarizes the results obtained from the complex task of designing a comprehensive solution for the investigation and analysis of leaked data. The results of this research serve as a means of enhancing information security.

3. Scope and Alignment of the Selected Research Methodology with the Aims and Objectives of the Dissertation and with the Contributions Achieved

The scope of the research is the process of automated processing, standardization, and analysis of large volumes of heterogeneous data from leaked or compromised sources.

The focus of the research is the profiling, categorization, and extraction of potential threats from leaked and compromised data.

The objectives of the research are aimed at identifying patterns and relationships in the processed data that will support the early detection of risks and the development of mechanisms for preventing cyber threats.

The methodology chosen for this study is based on the presentation of ASLDA as an information system composed of multiple functionally interconnected subsystems. The main subsystems include a database, a database management system, a data analyzer, a notification system, and a storage system.

The architecture of the information system is a modular, three-tier client-server structure, featuring a clustered server, a shared-nothing database, and additional computing modules. The three-tier architecture separates the presentation, application logic, and data management layers, allowing for the separation of functionalities and the independent development of individual components.

The use of a cluster architecture and a non-shared database enables the distribution of data processing and storage across individual computing resources. Additional computing modules support the automated processing and analysis of large volumes of heterogeneous data.

In this way, the developed ASID architecture creates a unified environment for receiving, standardizing, storing, processing, and analyzing data from leaked or compromised sources. The implemented functional subsystems lay the groundwork for automated data profiling and categorization, the detection of patterns and dependencies, and the identification of potential risks and cyber threats.

4. Evaluation of the Abstract and the Author's Publications Related to the Dissertation

The abstracts submitted in Bulgarian and English accurately reflect the content of the dissertation and comply with the requirements of the Law on Scientific Research and the Regulations for the Implementation of the Law on Scientific Research. Based on the submitted declaration of originality and the description of the results, it can be determined that they are the doctoral candidate's own work.

The doctoral candidate has two published articles and one accepted for publication. One article is authored solely by the candidate, while the other two are co-authored, with Ivan Drankov listed as the first author. No citations of publications have been reported to date.

The publications on the dissertation topic presented above fully meet the specific requirements of St. Ivan Rilski University of Mining and Geology for the award of the academic and scientific degree of "Doctor," since the doctoral candidate has earned 40 points out of the required 30.

The results of the plagiarism check conducted on the StrikePlagiarism.com website show the following: Similarity Coefficient 1: 1.63% and Similarity Coefficient 2: 0.65%

5. Contributions of the Doctoral Candidate

I fully accept the doctoral candidate's contributions as formulated.

6. Opinions, Critical Comments, and Recommendations

I have no critical comments regarding the doctoral candidate's work, only editorial ones. Following the recommendations I made during the expanded department council meeting of the Department of Mathematics and Computer Science at the St. Ivan Rilski University of Mining and Geology "St. Ivan Rilski" on June 10, 2026, regarding the internal defense of Ivan Drankov's dissertation, I confirm that he has addressed them and incorporated them into the final version of his dissertation.

7. Final Comprehensive Evaluation

The results obtained on the topic of the dissertation convincingly demonstrate that Ivan Lyubomirov Drankov possesses the necessary theoretical knowledge and practical skills in the field of informatics and computer science. The submitted dissertation fully complies with the requirements of the Law on the Development of Academic Staff in the Republic of Bulgaria, the Regulations for its Implementation, as well as the Regulations for its Application and the Rules and Procedures for the Admission and Training of Doctoral Students and the Awarding of the Academic Degrees of "Doctor"

and “Doctor of Science” at the St. Ivan Rilski University of Mining and Geology, Sofia. **The results obtained in the dissertation give me grounds to give a categorically positive evaluation of the presented work, and I propose that the esteemed Scientific Jury award Mr. Eng. Ivan Lyubomirov Drankov the academic and scientific degree of “Doctor” under the doctoral program “Computer Technologies in Engineering,” professional field 5.13. “General Engineering.”**

August 11, 2026

Jury Member:

/Assoc. Prof. Dr. Eng. Stanislav Dimitrov/