С Т А Н О В И Щ Е

за дисертационен труд за присъждане на **ОНС „ДОКТОР“**
по професионално направление **5.13. „Общо инженерство”**,
научна специалност **„Компютърни технологии в инженерната дейност”**

Автор на дисертационния труд: маг. инж. Иван Любомиров Дрънков

Тема на дисертационния труд: „Анализ на изтекли критични данни с цел разпознаване на потенциални заплахи за информационната сигурност“

Член на научното жури: проф. д-р инж. Даниела Велева Минковска
професор в кат. Програмиране и компютърни технологии, Факултет Компютърни системи и технологии, Технически Университет – София

1. Актуалност на разработвания в дисертационния труд проблем в научно и научно-приложно отношение

Бързото развитие на информационно-комуникационните технологии и масовото преминаване на дигиталните и бизнес процеси в облачни структури, поставя въпросите за информационната сигурност пред предизвикателството да се търсят и прилагат подходящи методи и средства за киберсигурността на всяка организация. Успоредно с технологичния напредък, кибератаките стават все по-сложни, по целенасочени и по разрушителни. Сред най-опасните последствия от тези инциденти са тези, свързани с изтичане на данни (data breaches). Те засягат конфиденциална информация, интелектуална собственост, лични данни и стратегически корпоративни тайни. Традиционните подходи за киберзащита, фокусирани предимно върху периметърната сигурност (защитни стени, антивирусен софтуер и системи за откриване на проникванията), вече не са достатъчни. Съвременните заплахи често успяват да заобиколят тези бариери. Веднъж изтекли извън защитения периметър, критичните данни могат да се появят в нерегламентирани пространства, като тъмната мрежа (Dark Web), хакерски форуми или публични платформи за споделяне на код.

Налице е научно-практическо противоречие: от една страна, съществуват огромни масиви от изтекла критична информация, която съдържа индикатори за компрометиране и ценни разузнавателни данни за заплахи, а от друга страна, липсват систематизирани подходи и инструменти за техния дълбочинен анализ с цел разпознаване на бъдещи вектори на атака. Това води до силна необходимост от преодоляването на тази празнота. Разработването на методи за анализ на изтекли критични данни позволява не просто да се констатират минали щети, но и да се извлекат закономерности за тактиките, техниките и процедурите на кибер престъпниците.

Това прави темата на дисертационния труд, и поставените и решени проблеми в него, изключително актуална, със силно изразена научно-теоретична и практико-приложна значимост за съвременната информационна сигурност. Предвид развитието на съвременните тенденции в тази област, актуалността на представения дисертационен труд е безспорна, което се доказва и от множеството научни форуми посветени на тази тема..

2. Степен на познаване състоянието на проблема и творческа имплементация на литературния материал

В дисертационния труд авторът показва много добро познаване на тематиката и адекватна интерпретация на литературния материал. Представеният за рецензиране дисертационен труд е с обем от 123 страници, които включват увод, четири глави, заключение, приноси, списък с публикациите, свързани с дисертационния труд, и списък с използвана литература, включващ 56 литературни източника. Към дисертацията има и речник на използваните съкращения. В дисертацията са използвани 78 фигури и 10 таблици.

3. Съответствие на избраната методика на изследване и поставената цел и задачи на дисертационния труд с постигнатите приноси

Комплексната цел на дисертационния труд е да се разработи и приложи методологичен подход за автоматизирана обработка, унифициране и анализ на големи по обем хетерогенни данни от изтекли или компрометирани източници, с цел тяхното профилиране, категоризация и извличане на потенциални заплахи.

Научното изследване се основава на хипотезата, че прилагането на цялостно решение за изследване и анализиране на изтекли данни, реализирано с подходяща Активна Система и Анализатор на Изтекли Данни (АСАИД), ще доведе до повишена ефективност при ранното откриване на рискове, и до изграждане на механизми за превенция на информационната сигурност. За тестването на тази хипотеза е използвана методика, съчетаваща концептуално моделиране, базирано на множество клъстери от бази данни, и реализирана като облачна услуга от тип Software as a Service. Използвани са и адаптивни алгоритми, анализ на данните и експериментална оценка с помощта на разработена система Pyformat. Приложените методи на изследване са подходящи и достатъчни за постигане на поставените цели и обосноваване на приносите на дисертационния труд.

В ***увода*** са представени целта, основните задачи за изпълнение, аргументацията и актуалността на темата на дисертационния труд. Допълнително се очертава мотивацията за изследването, предвид съвременното развитие в управлението на критичните данни и киберсигурността.

В ***първа глава*** е направен обширен преглед на литературата за текущото състояние на системите за анализ на критични данни. Въведени са ключови понятия и дефиниции, анализирани са основните компоненти и функционалности на съществуващи системи. След сравнението е направен извод, че няма такава система, която да прави подробен анализ на данните и да дава отчет за

потенциалните заплахи. По този начин са идентифицирани пропуски в настоящите системи и практики, които тази дисертация има за цел да адресира.

Във ***втора глава*** се разглежда процесът на формулиране и моделиране на предложената система за анализ на изтекли критични данни (АСАИД). Установени са теоретичните основи на концептуалния модел, описани са основните компоненти за обработка на информацията, и е представена цялостната трислойна клиент-сървър архитектура на системата. Тази глава ефективно превежда информационните цели във формална системна спецификация, определяща структурата и поведението на концептуалния модел.

В ***трета глава*** са описани основните етапи, свързани с управлението на събраните данни. Описани са методи за валидиране, верифициране и филтриране на данните, спрямо тяхната критичност. Предложени са основни алгоритми за анализ на данните, с цел, извличане на смислови зависимости.

В ***четвърта глава*** е представено внедряването и автоматизацията на системата. Направено е подробно описание на техническите аспекти на разработения прототип, включително схема на базата данни, скриптове за автоматизация, бизнес логика и интеграция на компоненти, базирани на разработен модул на АСАИД – Pyformat. Описана е емпиричната част на изследването, включително експерименталния дизайн и неговите резултати. Получените резултати са анализирани и интерпретирани с помощта на таблици и фигури, което позволява систематична оценка на предложения подход за анализ на критични данни..

В ***заключението*** е направено обобщение на изпълнените цели и задачи на дисертационния труд, като се обосновава и приложението на модела за анализ на изтекли критични данни, с цел, увеличаване на информационната сигурност.

4. Научни и/или научно-приложни приноси на дисертационния труд

Основните приноси представени от автора в дисертационния труд могат да се обобщят като приноси с научно-приложен характер, и приноси с приложен характер, По мое мнение, те би трябвало да се преквалифицират за да бъдат добре формулирани и достатъчни, по следния начин:

Научно-приложни приноси:

1. Предложен е концептуален модел на система за анализ и известяване на изтекли критични данни, базиран на парадигмата за управлениие на данните и киберсигурност.
2. Формулирани и анализирани са основните етапи, свързани с обработката на големи масиви изтекли данни, Този процес е реализиран чрез алгоритми, подлежащи на измерима оптимизация и емпирична проверка.
3. Проведени и съпоставени са основни емпирични анализи, които могат да се приложат при изтекли данни, както и принципът им на работа, с осигурена надеждност и валидност на измерванията.

Приложни приноси:

1. Разработен е софтуерен продукт Pyformat за обработка на големи масиви данни от тип „изтекли данни“, включващ формати за инструкции и филтри за качество.
2. Създаден е проект на активна система и анализатор на изтекли данни, включваща и активна система за известие на изтекли данни (АСАИД), който е частично реализиран.

5. Преценка на публикациите по дисертационния труд: брой, характер на изданията, в които са отпечатани

Във връзка с разработването на дисертационния труд, докторантът е представил 3 научни труда, от които 2 в съавторство и един самостоятелен труд, всички на английски език. И трите публикации са издадени в Годишника на МГУ „Св. Ив. Рилски”, София. Няма данни за публикации на докторанта в индексирани международни бази от данни SCOPUS или Web of Science. Няма данни за цитирания на публикации на докторанта.

6. Мнения, препоръки и бележки

Като цяло, мнението ми за представения дисертационен труд е, че той е разработен последователно и има високо ниво на научни изследвания.

Могат да се посочат следните редакционни забележки:

- в съдържанието на целия труд липсват цитирания – т.е. имаме некоректно оформление на позоваванията в текста, на фигурите и таблиците, което е формално нарушение на академичния стил на цитиране.
- формализираната част на концептуалния модел би могла да бъде допълнително задълбочена чрез по-строги математически представяния на адаптивната логика.
- не е необходимо на две места в дисертационния труд да бъде описана структурата на дисертацията по глави (стр. 9 и стр. 125).
- наличие на множество грешки от форматиращ характер, като: заглавията на главите са с по-малък шрифт от подточките, различна големина на шрифта на еквивалентни подточки (напр. 1.6.1 и 1.6.2), неизравнен текст (стр. 46, 47, 117, 123), и други малки грешки от синтактичен и форматиращ характер.
- Формулите в дисертацията следва да се номерират и да се цитира източник, ако е необходимо.
- на много места в текста, няма позоваване на фигурите, които са представени, както и някои фигури са с много дребен шрифт и малък контраст (напр. фиг. 4.3)

Въпреки направените забележки, считам, че докторантът показва добро познаване на предметната област. Бих препоръчала на докторанта да продължи и разшири изследванията си в областта на информационната сигурност, като усили

своята публикационна дейност предимно в престижни научни български и международни конференции и индексирани издания.

7. **<u>Заключение с ясна положителна или отрицателна оценка на дисертационния труд</u>**

Крайната ми оценка за дисертационният труд на маг. инж. Иван Любомиров Дрънков е ***положителна***. Извършена е значителна по обем и съдържание изследователска работа. Дисертационният труд напълно отговаря на изискванията на Закона за развитие на академичния състав на Република България, на Правилника за неговото приложение и на Правилника за условията и реда за придобиване на научни степени в МГУ „Св. Ив. Рилски”, София.

Това ми дава основание да оценя положително дисертационния труд и да препоръчам на научното жури **да присъди на маг. инж. Иван Любомиров Дрънков образователната и научна степен „доктор“** по направление 5.13. „Общо инженерство”, научна специалност „Компютърни технологии в инженерната дейност”.

София, 04.08.2026 г. ЧЛЕН НА НАУЧНОТО ЖУРИ:

/проф. д-р Даниела Минковска/

O P I N I O N

on dissertation for obtaining the educational and scientific degree "**Doctor**"
Higher education field: 5.**"Technical sciences"**,
Professional field: 5.13. **"General engineering"**,
Scientific specialty **"Computer Technologies in Engineering"**.

Author of the dissertation: M, Eng. Ivan Lyubomirov Drankov

Dissertation title: „Analysis of Leaked Critical Data for the Identification of Potential Information Security Threats"

Member of the scientific jury: Prof. Dr. Eng. Daniela Veleva Minkovska
Full professor, Department of Programming and Computer Technologies, Faculty of Computer Systems and Technologies, Technical University of Sofia

1. Relevance of the problem developed in the dissertation in scientific and applied terms

The vast development of the informatics-communicative technology and mass transition of the digital and business process towards cloud infrastructures raises questions on the security of information in the face of the search and application of the necessary cybersecurity methods and tools of every organization. Alongside the technological advance, the cyberattacks grow in complexity, with narrower targeting and greater destructivity. Among the most dangerous consequences are those related to data leakage, or data breaches. They impact confidential information, intellectual possession, private data, as well as strategic confidential corporate secrets. The traditional approaches of cybersecurity, focused mainly on the perimeter security (firewalls, antivirus software, and tools for locating penetrations) are no longer sustainable enough. Modern threats often get through these barriers, and quickly at that. Once leaked outside the security perimeter, the critical data can emerge on any non-reglamented place, be it the dark web, hacker forums, public platforms for code sharing, etc.

A scientific-practical contradiction occurs: on one end, there are massive arrays of leaked critical data, which contains indicators of compromise and valuable threat intelligence, while on the other end, there is a lack of systematized approaches and tools for their in-depth analysis aimed at identifying future attack vectors. This leads to a great need for the overcoming of this hole. The establishment of methods for leaked data analysis allows not merely to document past damage, but also to derive patterns regarding the tactics, techniques, and procedure of cybercriminals.

This makes the subject of this dissertation, including the raised and solved problems in it, incredibly topical, with well-set scientific-theoretical and practical-applied significance for modern information security.

Considering the development of the current tendencies in this field, the relevance of the presented dissertation is indisputable, as evidenced by the numerous scientific forums dedicated to this topic.

2. **Degree of knowledge of the issue and creative interpretation of the reference material**

The author shows in-depth knowledge of the themes and competent interpretation of the literary material within the dissertation. The presented for evaluation dissertation rounds at 123 pages, which include an introduction, four chapters, a conclusion, contributions, a list of publications related to the dissertation, and a list of references comprising 56 sources. Towards it, there is also a vocabulary of the abbreviations that occur. The dissertations consist of 78 figures and 10 tables.

3. **Conespondence of the chosen research methodology and the set goal and tasks of the PhD dissertation with the contributions achieved**

The complex goal of the dissertation is to develop and apply a methodological approach of automated processing, standardization, and analysis of large volumes of heterogeneous data from leaked or compromised sources, the purpose of profiling and categorizing them and identifying potential threats.

This scientific research is based on the theory that the application of a comprehensive solution for investigating and analyzing leaked data, realized through the appropriate Active Data Leak Detection and Analysis System (ADLDAS) will lead to an increased efficiency in the early detection of risks and establishing of mechanisms for information security prevention. To test this hypothesis, a methodology was employed that combines conceptual modeling based on multiple database clusters and is implemented as a Software-as-a-Service (SaaS) cloud service. Adaptive algorithms, data analysis, and experimental evaluation using the developed Pyformat system were also utilized. The applied research methods fit and successfully achieve the set objectives and substantiating the contributions of the dissertation.

The ***introduction*** sets the research question, as well as main objectives, the argumentation, and the relevance of the dissertation topic. Additionally, the motivation for the study is outlined in light of contemporary developments in critical data management and cybersecurity.

The ***first chapter*** provides an extensive literature review on the current state of critical data analysis systems. The key concepts and definitions have been introduced, so are the key components and functionalities of existing systems analyzed. The comparison is followed by a conclusion of the non-existence of a system that conducts a detailed analysis of the data and reports on potential threats. Through that, gaps in current systems and practices have been identified, which this dissertation aims to address.

The ***second chapter*** looks at the process of formulation and modelling of the offered Active Data Leak Detection and Analysis System (ADLDAS). The theoretical base of the conceptual model has been set, the main components of information processing

described, and the system's overall three-tier client-server architecture—introduced. This chapter effectively translates the information objectives into a formal system specification defining the structure and behavior of the conceptual model.

The ***third chapter*** describes the main stages of managing the collected data. It describes the methods of data validation, verification, and filtering based on criticality. It aloes offers basic data algorithms aiming to extract meaningful dependencies.

The ***fourth chapter*** showcases the implementation and automation of the system offered; a thorough explanation of the technological aspects or the prototype, including the database schema, automation scripts, business logic, and component integration based on the developed USAID module – Pyformat. The chapter also includes a description of the empirical part of the study, both with the experimental design and its results. The results have been analyzed and interpreted with the help of tables and figures, which allows for a systematic evaluation of the proposed approach for critical data analysis.

The ***conclusion*** holds the summary of the accomplished tasks and objectives of the dissertation, and substantiates the application of the model for analyzing leaked critical data with the aim of enhancing information security.

4. Scientific and/or applied research contributions of the PhD dissertation

The main contributions of the author in this dissertation can be summarized as contributions of a scientific-applied nature and contributions of an applied nature. In my expertise, they should be reformulated—so as to be well-worded and sufficient—in the following way:

Scientific-applied contributions

1. A conceptual model of a system for analyzing and alerting on leaked critical data is proposed, based on the data management and cybersecurity paradigm..
2. The key stages involved in processing large datasets of leaked data have been formulated and analyzed. This process is implemented using algorithms subject to measurable optimization and empirical verification.
3. Key empirical analyses applicable to leaked data, along with their operating principles, have been conducted and compared, ensuring the reliability and validity of the measurements.

Applied contributions:

1. A software product named Pyformat has been developed for processing large datasets of the "leaked data" type, incorporating instruction formats and quality filters..
2. A design for an active system and a leaked data analyzer has been created, including an Active Data Leak Detection and Analysis System (ADLDAS), who is partially implemented.

5. **Assessment of PhD dissertation publications: number and type of journals where they have been published**

In relation to the development of the dissertation, the doctoral candidate has presented 3 scientific works, 2 of which in co-authorship and one individual, all three in English. All three publications have been published in the Yearbook of the University of Mining and Geology "St. Ivan Rilski", Sofia. No additional publications by the doctoral candidate have been indexed in international databases such as Scopus or Web of Science. There is no information on citing of the mentioned publications.

6. **Opinions, recommendations and notes**

Overall, my evaluation of the presented dissertation material is that is has been developed systematically, characterized by a high level of scientific research.
The following edits can be applied:

- The entire work lacks citations; incorrect format of mentions within the text (inline citations), of the figures and tables, which counts as a formal violation of the set academic style of citing.
- The formalized part of the conceptual model could be further developed through stricter mathematical representations of adaptive logic.
- There is no need for two places to provide walk-through the dissertation (p. 9 and p. 125).
- There are many mistakes in terms of fomratting, like: the titles of the chapters use smaller font than the subpoints, different font size for equivalent sub-points (eg. 1.6.1 and 1.6.2), uneven text body (p. 46, 47, 117, 123), and other minor mistakes of syntactic and formatting character.
- The formulas follow to be numbered and with a cited source, if needed.
- Many places in the text lack referencing of the figures discussed or have figures with too small of a font and low contrast (ed. fig. 4.3)

Despite the remarks provided, I find that the doctorate candidate demonstrates a good understanding of the subject area, and I would suggest them to further research and deepen their work in the cybersecurity field. It would be especially beneficial if they were to broaden their publication activity in prestigious Bulgarian and international scientific conferences and indexed publications.

7. **Conclusion with a clear positive or negative evaluation of the PhD dissertation**

My final grade for the dissertation work of Eng. Ivan Lyubomirov Drankov is ***positive***. The conducted work of research is considerable both in size and content. The dissertation fully meets the requirements of the Law on the Development of the Academic Staff in the Republic of Bulgaria, of the Regulations for its implementation and the Regulations on the conditions and procedure for acquiring academic degrees at the University of Mining and Geology "St. Ivan Rilski", Sofia.

All this gives me grounds to evaluate this dissertation positively and to recommend that the scientific jury **award MSc Eng. Ivan Lyubomirov Drankov the educational and scientific degree of "Doctor"** in field 5.13. "General Engineering", scientific specialization "Computer Technologies in Engineering”.

Sofia, 04.08.2026 MEMBER OF THE SCIENTIFIC JURY:

/Prof. Dr. Daniela Minkovska/