УНИВЕРСИТЕТ ЗА НАЦИОНАЛНО И СВЕТОВНО СТОПАНСТВО

С Т А Н О В И Щ Е

От: *Проф. д-р Камелия Георгиева Стефанова;*
УНСС;
Приложение на изчислителната техника в икономиката

Относно: дисертационен труд за присъждане на образователна и научна степен **„доктор“** по научна специалност *„Приложение на изчислителната техника в икономиката“* в УНСС.

Автор на дисертационния труд: *Ивона Пламенова Велкова - докторант към катедра „Информационни технологии и комуникации”*

Тема на дисертационния труд:
„Принципи и методи за проектиране на оперативен център за управление на информационна сигурност за системи с големи данни”

Основание за представяне на становището: участие в състава на научното жури по защита на дисертационния труд съгласно Заповед № 973/06.04.2023г. на Зам.-ректора по НИД и МС на УНСС.

1. Информация за дисертанта

Дисертантът е обучаван по докторска програма към *катедра „Информационни технологии и комуникации”* на УНСС по *научна специалност „Приложение на изчислителната техника в икономиката“* съгласно Заповед на Зам.-ректора по НИД на УНСС № 966/29.04.2020г. Обучението е осъществено в *редовна* форма през периода 2020-2023 год.

2. Обща характеристика на представения дисертационен труд

Представеният за рецензиране дисертационен труд е посветен на изключително актуална проблематика, която обхваща множество нови насоки и важни решения за развитието на информационните системи днес. Превръщането на големите данни в критичен ресурс за управление на информационните среди поставя много въпроси пред технологичната общност за развитие на различни аспекти от функционирането на

системите.

Докторантката много амбициозно и задълбочено подхожда към изследователската тема и насочва своята разработка към интегриран подход на проучване на основните проблеми на сигурността, изкуствения интелект, големите данни, съответните необходими технологии, за да предложи нови принципи и методи при проектирането на центрове за информационна сигурност за съвременните системи в среда на големи данни.

Дисертационният труд е в общ обем от 170 страници. Структурно съдържа: въведение, три глави, заключение и използвана литература. За задълбочената изследователска работа свидетелстват използваните източници, които са 119 и по-голяма част от тях са от последните 2-3 години.

Първата глава е въведението в дисертационния труд, което подходящо е насочено към актуалността на изследователския проблем в контекста на значимостта на изграждането на единен център за оперативна сигурност, за какъвто няма известни решения за обединяване на различни системи за големи данни, които извличат и обработват неструктурирани данни с ИИ от разнородни източници, и е постигната когнитивна и адаптивна сигурност.

Дисертантът обосновава коректно своята разработка, като формулира съответно обект, предмет и цел на изследването.

Обектът на изследването обхваща принципи и методи за проектиране на оперативен център за управление на сигурността в системи за големи данни.

Предметът на изследването е насочен към изграждането на нов тип оперативен център за управление на сигурността, базиран на обработка с ИИ на неструктурирани данни, системи с големи данни и Управление на информацията за сигурността и събитията, интегрирани в обща архитектура.

Целта на дисертационния труд ясно е дефинирана: да бъдат предложени принципи и методи за проектиране и изграждане на оперативен център, който да управлява информационната сигурност, за системи, опериращи с големи данни.

3. Оценка на получените научни и научно-приложни резултати

Втора глава е посветена, много пространно, на теоретичните аспекти на изследваните проблеми. Представени и дефинирани са основни понятия и техните характеристики. Описани са различните видове данни и делът им на генериране в света. Обърнато е специално внимание на същността на

големите данни и особеностите на системите за обработката им – Apache – Hadoop, Spark, Hive и MicroFocus IDOL. Тук са предложени критерии за сравнение и са съпоставени различни софтуери. Извършеното сравнение помага за взимане на решение кои продукти да бъдат използвани при изграждането на бъдещата архитектура.

Следващата точка е посветена на ПРИЛОЖЕНИЕ НА ИЗКУСТВЕН ИНТЕЛЕКТ ЗА СИГУРНОСТ ПРИ ГОЛЕМИ ДАННИ и разглежда важни аспекти от ролята на ИИ за управление на сигурността.

Обособено място в главата е отделено на ПРИНЦИПИ И ПОДХОДИ ЗА УПРАВЛЕНИЕ НА ИНФОРМАЦИОННАТА СИГУРНОСТ. Ясно са описани различни видове сигурност, видове хакерски атаки, различни функции на системите за сигурност в среда на големи данни, инструменти за сигурност.

Следващата точка представя проучване в областта на ОПЕРАТИВНИ ЦЕНТРОВЕ ЗА ИНФОРМАЦИОННА СИГУРНОСТ. Изведена е дефиниция за ОЦИС и са разгледани различните функции, които изпълнява. Представени са съществуващи решения за управление на информационната сигурност в системи с големи данни.

Трета глава, логично е насочена към същността и методологията на изследователския проблем. Проучени и описани са основните, утвърдили се в практиката, принципи и методи на проектиране на Оперативен Център за Сигурност. Представени са накратко особеностите на различните видове поколения на ОЦИС, характерни за различните етапи от тяхното развитие, както и предизвикателствата пред които са изправени. Обобщена е разработката на пето поколение ОЦИС и са дефинирани принципи, които да помогнат да изграждането на нов ОЦИС. Използвани са контроли за сигурност от стандарта ISO 27001, които имат отношение към предмета на дисертационния труд. Същностната част и основното лично, творческо постижение в предложената разработка е проектирането на функционална архитектура от ново поколение за ОЦИС и обособяването и дефинирането на три нива за постигане на по-високо ниво на защита с използване на ИИ при събирането на разнородни типове данни от различни източници. Следва подробното описание на функционалностите и инструментите последователно за всяко ниво от архитектурата на ОЦИС за системи с големи данни. Демонстрирано е познаването на много различни технологии, техните функционалности и насоки за свързаност, за целите на създаване на ОЦИС за системи с големи данни.

Подробно са описани ролите на всеки инструмент, който се прилага на всяко от трите нива на предложената архитектура.

Четвърта глава е посветена на приложните аспекти на дисертационния труд. Показани са конкретни резултати от тестването на компонентите на архитектурата. Описани са процесите на технологично изграждане на архитектурата и е постигната ефективната съвместимост между отделните продукти. Изложението последователно доказва адекватността на избраните технологии за всяко едно от нивата на оперативния център за информационна сигурност и постигането на целевите функционалности. Архитектурата е тествана с реални данни, които са извлечени от социални среди – Twitter.

Логично в заключението се посочват аспектите, в които може да продължи изследването и да бъдат подобрени на предложените подходи.

4. Оценка на научните и научно-приложни приноси

Определено, представеният дисертационен труд има своите изследователски и научно-приложни приноси.

Приемам списъка с предложените приноси, като резултат от задълбочената научно-изследователска и приложна работа по дисертационния труд.

5. Оценка на публикациите по дисертацията

Публикациите по дисертационния труд обхващат една статия и три доклада, от които два доклада и статията са самостоятелни, а останалите са в съавторство.

Под печат е доклад на тема Approaches to higher security level for Hadoop environment.

6. Оценка на автореферата

Считам, че авторефератът коректно отразява същността, обхвата и приносните аспекти на разработения дисертационен труд. Авторефератът е в обем от 135 страници, като основното му съдържание е в размер на 65 страници. Той съдържа основните моменти на дисертационния труд, както и справка за постигнатите научно-приложни приноси.

7. Критични бележки, препоръки и въпроси

Към докторантката имам следните въпроси:

1. Какво налага проектирането на ново поколение ОЦИС и с какво основно повишава функционалността на съществуващите?

2. Как се стига до предложението за тази компонентна структура на ОЦИС?

8. Заключение

По моя преценка, представеният дисертационен труд на тема „ПРИНЦИПИ И МЕТОДИ ЗА ПРОЕКТИРАНЕ НА ОПЕРАТИВЕН ЦЕНТЪР ЗА УПРАВЛЕНИЕ НА ИНФОРМАЦИОННА СИГУРНОСТ ЗА СИСТЕМИ С ГОЛЕМИ ДАННИ“, за придобиване на образователна и научна степен „доктор”, с автор Ивона Велкова, притежава необходимите качества на задълбочено, самостоятелно проведено и завършено научно изследване.

Считам, че е представен значим резултат от постигане на забележителен обем нови знания, от запознаване с нови технологии, от предлагане на нови решения и от разработване на конкретни приложни решения.

Предлагам на уважаемите членове на НЖ да приемем постигнатите резултати от изследователската дейност на Ивона Велкова като основателни и да вземем решение за присъждане на ОНС „доктор“ по професионално направление 3.8. Икономика, научна специалност „Приложение на изчислителната техника в икономиката“.

27.05.2023г. Подпис: ……

Проф. д-р Камелия Стефанова

UNIVERSITY OF NATIONAL AND WORLD ECONOMY

R E V I E W

From: Prof. Dr. Kamelia Georgieva Stefanova;

UNWE;

Application of computing in economics

Regarding: Dissertation on awarding educational and scientific degree "Doctor" in scientific specialty "Application of Computing in Economics" at the UNWE.

Dissertation Author: Ivona Plamenova Velkova; PhD student at the Information Technologies and Communications Department

Thesis topic:

“Principles and methods for designing an operational center for managing information security for big data systems“

Reason for writing the review: participation in the composition of the scientific jury for the defense of the dissertation work according to Order No. 973/06.04.2023 by the Vice-Rector for Research and International Affairs at the University of National and World Economy (UNWE).

1. Information about the dissertant

The doctoral student has been trained under the doctoral program at the Department of Information Technology and Communications at the University of National and World Economy (UNWE), specializing in "Application of Computer Science in Economics," according to the Order of the Vice-Rector for Research and International Affairs at UNWE No. 966/29.04.2020. The training has been conducted in a full-time form during the period 2020-2023.

2. Overview of the dissertation

The dissertation presented for review is dedicated to extremely topical issues that cover many new directions and important solutions for the development of information systems today. Big data becomes a critical resource for managing information environments that raises many questions for the technology community to develop various aspects of systems functionalities.

The PhD student very ambitiously and thoroughly approaches the research topic and directs her development towards an integrated approach of exploring the main problems of security, artificial intelligence, big data, the relevant necessary technologies to propose new principles and methods in the design of information security centers for modern systems in a big data environment.

The total volume of the dissertation is 170 pages. The structure contains: introduction, three chapters, conclusion, and list of references. For the benefit of research work were used 119 relevant materials and most of them are from the last 2-3 years.

The first chapter of the dissertation appropriately addresses the relevance of the research problem in the context of the importance of building an operational security information center. There are not currently known solutions for integrating various big data systems that extract and process unstructured data using AI from heterogeneous sources, while achieving cognitive and adaptive security.

The doctoral student appropriately justifies her research by formulating the object, subject, and goal of the study.

The object of the research encompasses principles and methods for designing an operational security information center in big data systems.

The subject of the research is focused on building a new type of operational

security information center, based on AI processing of unstructured data, big data systems, and Security Information and Event Management, integrated into a common architecture.

The goal of the dissertation is clearly defined: to propose principles and methods for designing and building an operational center that manages information security for systems operating with big data.

3. Evaluation of scientific and applied research results obtained

The second chapter extensively addresses the theoretical aspects of the researched problems. It presents and defines fundamental concepts and their characteristics. Special attention is given to the substance of big data and the features of their processing systems, such as Apache Hadoop, Spark, Hive, and MicroFocus IDOL. Criteria for comparison are proposed, and various software solutions are compared. This comparison aids at making decisions about which products to be used in the construction of the future architecture.

The next section focuses on the APPLICATION OF ARTIFICIAL INTELLIGENCE FOR SECURITY IN BIG DATA and examines important aspects of the role of AI in security management.

A significant part of the chapter is devoted to PRINCIPLES AND APPROACHES TO INFORMATION SECURITY MANAGEMENT. Different types of security, types of hacking attacks, various functions of security systems in the context of big data environments, and security tools are clearly described.

The following point presents a study in the field of OPERATIONAL SECURITY INFORMATION CENTERS. A definition of OSIC is provided, and different functions it performs are discussed. Existing solutions for managing information security in big data systems are presented.

Overall, the second chapter successfully evaluates and discusses the

theoretical and conceptual aspects related to the research problems. It provides a comprehensive understanding of the key concepts, technologies, and approaches relevant to the dissertation topic.

The third chapter logically focuses on the substance and methodology of the research problem. The main principles and methods for designing an Operational Security Information Center (OSIC), which have been established in practice, are investigated, and described. The characteristics of different generations of OSICs, typical of various stages of their development, as well as the challenges they face, are briefly presented. The development of the fifth generation OSIC is summarized, and principles are defined to propose the construction of a new OSIC. Security controls from the ISO 27001 standard, relevant to the subject of the dissertation, are utilized. The core and main creative achievement of the proposed development lie in the design of a next-generation functional architecture for the OSIC and the introduction and definition of three levels to achieve a higher level of protection by utilizing AI in gathering diverse types of data from various sources. A detailed description of the functionalities and tools for each level of the OSIC architecture for big data systems follows. Proficiency in multiple technologies, their functionalities, and connectivity guidelines is demonstrated for the purpose of creating an OSIC for big data systems. The roles of each tool applied at each level of the proposed architecture are thoroughly described.

The fourth chapter is dedicated to the practical aspects of the dissertation work. Concrete results from testing the components of the architecture are presented. The processes of technological construction of the architecture are described, and effective compatibility between individual products are achieved. The description systematically demonstrates the adequacy of the chosen technologies for each level of the OSIC and the achievement of target

functionalities. The architecture is tested with real data extracted from social media environments, specifically Twitter.

Logically, in conclusion, the aspects in which further research can be conducted and the proposed approaches can be improved are indicated.

4. Evaluation of scientific and applied contributions

Certainly, the presented dissertation work has its research and applied contributions.

I accept the list of proposed contributions because of the well demonstrated in-depth scientific research and applied work on the dissertation.

5. Evaluation of dissertation publications

The publications on the dissertation consist of one article and three papers, of which two papers and the article are individual and the rest are co-authored.

A paper on “Approaches to higher security level for Hadoop environment” is in print.

6. Evaluation of the authorship

The authorship correctly reflects on the substance, scope, and contribution aspects of the developed dissertation. The authorship has a volume of 135 pages, its main content is 65 pages. It contains the main points of the dissertation, as well as a reference to the achieved scientific and applied contributions.

7. Critical remarks, recommendations and questions

I have the following questions to the PhD student:

1. What does the design of a new generation OSIC entail and how does it primarily enhance the functionality of the existing systems?

2. How have you decided to configure the suggested architectural structure of the proposed OSIC?

8. Conclusion

In my opinion, the presented doctoral thesis on the topic „Principles and methods for designing an operational center for managing information security for big data systems“ by Ivona Velkova possesses the necessary qualities of in-depth, independently conducted, and successfully completed scientific research.

I believe that significant results have been achieved through the acquisition of a remarkable volume of new knowledge, the exploration of new technologies, the proposal of innovative solutions, and the development of concrete practical applications.

I recommend that the esteemed members of the honorable members of the Scientific Jury acknowledge the attained research outcomes by considering them substantial and decide to award Ivona Velkova the educational and scientific degree "Doctor" in professional field 3.8. Economics, scientific specialty "Application of computing in economics".

27 May 2023

With respect: .....

Prof. Dr. Kamelia Stefanova