УНИВЕРСИТЕТ ЗА НАЦИОНАЛНО И СВЕТОВНО СТОПАНСТВО

Р Е Ц Е Н З И Я

От: *доц. д-р Дорина Петрова Кабакчиева;*
Университет за национално и световно стопанство (УНСС);
Научна специалност: Професионално направление 3.8: Икономика, научна специалност „Приложение на изчислителната техника в икономиката“

Относно: дисертационен труд за присъждане на образователна и научна степен **„доктор“** по *Професионално направление 3.8: Икономика, докторска програма „Приложение на изчислителната техника в икономиката,* в УНСС.

Основание за представяне на рецензията: участие в състава на научното жури по защита на дисертационния труд съгласно Заповед № 973/06.04.2023г. на Ректора на УНСС.

Автор на дисертационния труд: *Ивона Пламенова Велкова*
Тема на дисертационния труд: *„Принципи и методи за проектиране на оперативен център за управление на информационна сигурност за системи с големи данни“*

1. Информация за дисертанта

Дисертантът се е обучавал по докторска програма към *катедра „Информационни технологии и комуникации“, факултет „Приложна информатика и статистика“* на УНСС, по *професионално направление 3.8: Икономика, докторска програма „Приложение на изчислителната техника в икономиката,* съгласно Заповед на Зам.-ректора по НИД на УНСС № 966/30.04.2020г. Обучението е осъществено в *редовна* форма през периода 27.04.2020г. – 27.04.2023г.

- *Кратка биографична справка*

Придобита образователно-квалификационна степен „Бакалавър“ по специалност “Бизнес информатика и комуникации“ в УНСС през периода 2014-2018г..

Придобита образователно-квалификационна степен „Магистър“ по специалност „Бизнес информатика“ в УНСС през периода 2018-2019г..

- *Заемани академични и други длъжности до момента (вкл. длъжности извън ВУ или научна организация).*

От март 2018г. работи в УНСС, като се занимава с разработка на софтуер и поддръжка на университетски системи към дирекция „Информационни технологии“, и с обучение на студенти по дисциплини, включени в учебни програми на катедра „Информационни технологии и комуникации“.

- *Кратка информация за изпълнението на индивидуалния план*

В индивидуалния план на докторанта Ивона Велкова са били предвидени общо 6 изпита - по три изпита през първата и втората година от обучението – всички изкарани успешно.

Предвидено е разработването на научни публикации в рамките на 30 кредита, през втората и третата година на обучението. За изпълнението по този показател са получени 35 кредита за публикувани три доклада на конференции и една статия в научно списание.

Всички дейности от индивидуалния учебен план са изпълнени и е получена положителна оценка от обучаващата катедра.

2. Обща характеристика на представения дисертационен труд

- *Структура, обем*

Представеният ми за рецензиране дисертационен труд на тема „Принципи и методи за проектиране на оперативен център за управление на информационна сигурност за системи с големи данни ” е в общ обем от 170 страници и включва въведение, три глави, заключение, използвана литература, списъци на фигурите и таблиците, използвани термини и съкращения. Обемът и структурата на дисертацията отговарят на изискванията за подобен вид научни разработки.

Във Въведението е обоснована актуалността на изследователския проблем, правилно са определени обектът и предметът на изследването, дефинирана е основната цел на дисертационния труд - да се предложат принципи и методи за проектиране и изграждане на оперативен център за управление на информационната сигурност (ОЦИС) за системи с големи данни, формулирани са задачите, които се изпълняват за постигане на целта, и са представени работните хипотези.

Първа глава е обзорна и акцентира върху същността на големите данни и управлението на информационната сигурност. Направен е анализ на спецификата при работа с различни видове големи данни, представени са функционалните възможности на съществуващи системи за обработка на големи данни и са сравнени по подходящо избрани критерии, като са направени изводи относно технологичните решения, които могат да бъдат

използвани и комбинирани за постигане на крайния резултат на дисертационния труд. Разгледани са приложения на ИИ за повишаване на информационната сигурност при големи данни, за да се придобие представа относно съществуващите възможности за откриване на уязвимости и пробиви в системата, и да се вземе решение кои системи да бъдат използвани в проектирания оперативен център. Тъй като основен фокус на дисертационния труд е информационната сигурност при големи данни, са разгледани основните принципи и подходи при управление на информационната сигурност, и съществуващи системи за сигурност в среда за големи данни. Изследователският проблем на дисертационния труд е съвместяването на технологии и предоставяне на различни нива на сигурност при изграждането на оперативен център в системи за големи данни, затова в последната част на главата са дискутирани ключови характеристики и функции на оперативните центрове за сигурност, както и предизвикателствата, свързани с големия обем и сложността на големите данни. В резултат на направения анализ и реализираното обобщение на възможностите на средите за големи данни, съобразени с нуждите на дисертационния труд, в края на втора глава са посочени избраните софтуерните средства, които са използвани при проектирането на ОЦИС.

Втора глава е насочена към проектирането на архитектура на ОЦИС. Представени са основните принципи за проектиране на подобни центрове и някои методи, които са подходящи за проектирането и внедряването на оперативен център за сигурност при системи за големи данни. Разгледано е еволюционното развитие на архитектурите на оперативните центрове за информационна сигурност, като са посочени основните предизвикателства при проектиране и изграждане на оперативен център за сигурност от ново пето поколение. На базата на извършения анализ са предложени актуални принципи, които да улеснят проектирането на ОЦИС и да доведат до създаването на метод за изграждане на нов тип оперативен център за системи с големи данни, който да гарантира, че чувствителните данни са защитени, инцидентите със сигурността се откриват и се реагира навреме, и се извършва адаптация към променящите се технологии и бизнес. Международният стандартът ISO 27001 е използван като референтна рамка за изграждане и управление на ОЦИС, посочени са избрани подходящи контроли, които са интегрирани в методологичната рамка за проектиране на нов тип ОЦИС.

Предложен е метод, който включва гореспоменатите контроли и се базира на изложените принципи за създаване на функционална архитектура, която ще позволи изграждането на актуално поколение

ОЦИС, който да работи с полу-структурирани и неструктурирани данни, като използва системи и решения за обработка на големи данни и извличане на знания от тях. Предложената архитектура е с три нива на управление на сигурността, включващи сигурност при извличането и съхранението на данни, вътрешно-базирана Hadoop сигурност и анализ на резултатите. Първото ниво е базирано на концепцията за адаптивна сигурност на Gartner, подход за киберсигурност, който постоянно анализира поведението и събитията в мрежата, и има готовност да се адаптира към заплахи, като ги проучва и анализира преди да се случат. Включва интелигентно управление на сигурността чрез прилагане на алгоритми за машинно обучение и ИИ, като се обработват данни от видео потоци, социални медии и други хетерогенни източници, което води до подобрение на ефективността на цялата системата, като й позволява да се адаптира към променящите се обстоятелства и да реагира на възникващи заплахи в реално време. Второто ниво на предложената функционална архитектура е съсредоточена върху вътрешната сигурност на системи за големи данни (в самата инфраструктура), която в конкретния случай се отнася до вътрешно-базираната Hadoop сигурност, и софтуерната бизнес сигурност, включваща мерки за сигурност на ниво приложение. Най-високото трето ниво в предложената функционална архитектура представлява анализ и визуализация на получените резултати, за да могат по-лесно да бъдат идентифицирани настъпилите събития и при наличието на нарушение да се генерират известия. На всяко едно от нивата са предложени технологични решения, които е подходящо да се приложат в работещ модел на ОЦИС.

Специално внимание е отделено на компонентите на адаптивна сигурност за система за големи данни, като е предложена концептуална архитектура със съответни възможни технологични решения. Представени са и конкретни приложения за интелигентна обработка на данни от различни източници - социални медии, видео потоци от камери и уеб-сайтове, за разпознаване на лица, автомобилни номера, преброяване на хора, които да са с контекст към определяне на по-високо ниво на сигурност.

В трета глава е описано приложението на предложения метод за проектиране и изграждане на оперативен център за сигурност, като са представени функционалностите с конкретни софтуерни решения. Представен е и примерен случай за работата на оперативния център за информационна сигурност, чрез който се верифицира изпълнението на поставените пред него цели.

В Заключението са обобщени получените резултати, представени са

постигнатите научни и научно-приложни приноси, изброени са публикациите по темата на дисертационния труд и са дадени насоки за бъдеща работа.

- *Оценка за: актуалност на темата; целта; задачите; обекта; предмета; основната теза на дисертационния труд*

Разглежданата в дисертационния труд проблематика отговаря на ключовата роля на информационните технологии в съвременното общество. Информационната сигурност е от съществено значение за защитата на данните и информацията при съхранението, обработката и анализа на големи данни. Тъй като ефективното управление на информационната сигурност изисква интегриран подход, включващ прилагането на политики, стандарти, процедури и технически контрол за защита срещу потенциални заплахи, идеята за изграждането на оперативен център за управление на информационната сигурност, с цел осигуряване на защита на дигиталната информация и подходящо ниво на сигурност за бизнеса, е актуален и важен научноизследователски проблем.

В дисертационния труд е предложен подход, с който се осигурява сигурност на различните нива на данните, на процесите и на комуникациите в системи за големи данни, като данните са извлечени от хетерогенни източници, част от които са видео потоци от камери, данни от уеб сайтове, социални медии и др. Като се имат предвид подобни предложения от водещи ИТ компании (Kaspersky), прилагането на Адаптивната стратегия за сигурност и използването на елементи на ИИ при работа с големи данни, това направление е много актуално, и иновативно.

- *Използвана научна литература (оценка на осведомеността на дисертанта по проблематиката, разглеждана в дисертационния труд).*

Използваните литературни източници са 119 на брой, публикувани през последните няколко години (след 2019г.) и включват научни публикации и актуална информация, публикувана на специализирани интернет страници.

3. Оценка на получените научни и научно-приложни резултати

Цялостното впечатление от дисертационния труд е, че той е резултат от задълбочена и добросъвестно извършена изследователска дейност. Материалът е отлично структуриран, изложението е ясно и

последователно. Авторът ясно определя своето отношение по всеки въпрос, а направените изводи и избраните подходи са подходящо мотивирани.

Предложен е метод за проектиране на ОЦИС за системи с големи данни, който се базира на най-съвременни методи, технологии и услуги за защита на сигурността, и при който се прилага Адаптивна стратегия за сигурност.

Разработената функционална архитектура предлага многостепенен подход към управлението на сигурност и има за цел да осигурява цялостна защита за системи с големи данни, като интегрира конкретни софтуерни технологии, които да постигнат поставените цели.

Представените резултати са получени чрез задълбочен анализ на съществуващи и доказано ефективни подходи, стандарти и иновативни технологии за осигуряване на информационна сигурност и работа с големи данни. Предложената функционална архитектура е описана с конкретни софтуерни решения като е реализиран прототип, свързващ технологиите NiFi, Micro Focus IDOL и Apache Hadoop. Прототипът е тестван с неструктурирани данни от социални медии, видео поток, данни от уебсайтове и лог файлове, като чрез този примерен случай за работата на ОЦИС е верифицирано изпълнението на поставените пред него цели.

Всичко това ми дава основание да твърдя, че докторантът е постигнал поставената научна цел в дисертацията като е получил необходимите научни резултати.

4. Оценка на научните и научно-приложни приноси

Оценявам приносите на автора като научни, в областта на обогатяване на съществуващи знания, и научно-приложни.

Научните приноси в дисертационния труд включват:

- На базата на направен задълбочен анализ на съществуващи съвременни подходи, принципи и технологии, са изведени:
    - Определение и необходими елементи на „оперативен център за сигурност“, съответстващо на съвременните условия за функциониране на такъв център в среда на големи данни;
    - Подходящи критерии за сравнение на технологии за обработка на големи данни с фокус върху събирането, организацията и съхранението на неструктурирани данни, с възможности за прилагане на средства за изкуствен интелект;

- Принципи и методи за управление на ОЦИС, необходими за обхващане на спецификата на управление на сигурността на системите, работещи в среда на големи данни.

- Дефиниран метод за проектиране и създаване на функционална архитектура на ОЦИС, включваща три нива на управление на сигурност, обхващащи мрежово ниво на сигурност, процес по извличане и обработка на данни, удостоверяване на вътрешно-базирана сигурност в среда за големи данни и анализ на получените резултати.

Научно-приложните приноси в дисертационния труд включват:

- Реализиран прототип, изграден с технологиите на предложената архитектура, свързващ технологиите NiFi, Micro Focus IDOL и Apache Hadoop, и тестван с данни от социални медии, видео поток, данни от уебсайтове и лог файлове.

5. Оценка на публикациите по дисертацията

Представените публикации по дисертационния труд са общо 4 на брой – 3 от тях са доклади на конференции и 1 е статия в научно списание. Два от докладите са самостоятелни разработки на международни конференции, проведени в България, един е в съавторство – на международна конференция в чужбина. Статията е публикувана в реномирано списание, индексирано в известни международни научни бази данни . Всички четири публикации са на английски език.

На рецензента не е известно представените публикации да са получили цитирания до момента.

6. Оценка на автореферата

Авторефератът отговаря напълно на съдържанието на дисертационния труд и коректно обобщава направените научни изследвания и постигнатите резултати.

7. Критични бележки, препоръки и въпроси

Предложенията и бележките, направени в рецензията за вътрешно катедрената защита са взети предвид и са коректно отразени.

Препоръките ми към докторанта са основно насочени към бъдещо публикуване на получените оригинални научни и научно-приложни резултати в специализирани списания и конференции с висок рейтинг, за да се повиши тяхната видимост в научните среди и да се увеличи вероятността за получаване на цитирания.

8. Заключение

По моя преценка Ивона Велкова е завършен изследовател, който притежава необходимите умения самостоятелно да формулира и решава научни задачи. Смятам, че представеният дисертационен труд отговаря на изискванията, установени от „Закона за развитието на академичния състав в Република България“, както и на правилника на УНСС за получаване на исканата образователна и научната степен ”Доктор”.

Всичко това ми дава основание да предложа на уважаемото научно жури да бъде присъдена научната и образователна степен „доктор“ на Ивона Велкова по научна специалност „Приложение на изчислителната техника в икономиката“.

25.05.2023г. Подпис: ……

UNIVERSITY OF NATIONAL AND WORLD ECONOMY

REVIEW

From: *Assoc. Prof. Dr. Dorina Petrova Kabakchieva;*
University of National and World Economy (UNWE);
Professional field 3.8: Economics, scientific specialty "Application of Computing in Economics"
Referring: PhD Thesis for awarding educational and scientific degree "Doctor" (PhD) in *Professional field 3.8:* Economics, *PhD program "Application of Computing in Economics,* at the UNWE.

Reasoning for presenting the review: Participation in the scientific jury for the defense of the PhD Thesis, under Order No 973 / 06.04.2023 of the Rector of UNWE.

Author of the dissertation: *Ivona Plamenova Velkova*
Dissertation topic: "*Principles and Methods for Design of an Information Security Management Operational Center for Big Data Systems"*

1. Information about the candidate

The candidate has been trained on a Doctoral Programme at the Department of Information Technologies and Communication, Faculty of Applied Informatics and Statistics, UNWE, in the professional *field 3.8: Economics, PhD Programme on the Application of Computing in Economics,* in accordance with the Order of the Vice-Rector on Scientific Research of UNWE No 966/30.04.2020. The training was carried out in *full-time* form during the period 27.04.2020 – 27.04.2023.

- *Brief biographical reference*

Acquired educational and qualification degree Bachelor in Business Informatics and Communications at the UNWE during the period 2014-2018.

Acquired Educational and Qualification Degree of Master in Business Informatics at the UNWE during the Period 2018-2019.

- *Academic and other positions held so far (incl. positions outside HEIs or scientific organization).*

As of March 2018, the candidate works at the UNWE, dealing with software development and maintenance of university systems at the Information Technologies Directorate, also teaching students in disciplines included in the educational programmes of the Department of Information Technologies and Communication.

- *Brief information on the implementation of the individual plan*

A total of 6 exams were included in the individual plan of the candidate Ivona Velkova - three exams for the first and second year of training - all successfully completed.

The development of scientific publications within 30 credits was envisaged in the second and third years of study. For the performance under this indicator, 35 credits were obtained for published three papers at conferences and one article in a scientific journal.

All the activities included in the individual plan have been implemented and a positive assessment has been received from the training department.

2. General xActivities of the Dissertation Presented

- *Structure, volume*

The PhD Thesis presented for review and titled "Principles and Methods for Design of an Information Security Management Operational Center for Big Data Systems" is with a total volume of 170 pages, including an ntroduction, three chapters, conclusion, references, lists of figures and tables, terms and abbreviations used. The volume and structure of the PhD thesis meet the requirements for such kind of scientific papers.

In the Introduction section, the actuality of the research problem is justified, the subject of the study and the main purpose of the PhD thesis are defined - to propose principles and methods for the design and development of an operational center for information security management (OCISM) for big data systems, the tasks that are performed to achieve the goal are formulated and the working hypotheses are presented.

The first chapter provides an overview and focuses on the essence of big data and information security management. An analysis of the specifics of working with different types of big data is performed, the functional capabilities of existing big data processing systems are presented and compared according to appropriately selected criteria, and conclusions are drawn about the technological solutions that can be used and combined to achieve the final result of the PhD thesis. Applications of AI to enhance information security in big data are discussed, in order to gain insight into the existing capabilities for

detecting vulnerabilities and system breaches, and to decide which systems to use in the designed operational center. Since the main focus of the dissertation is information security in big data systems, the basic principles and approaches for information security management and the existing security systems in big data environments are discussed. The research problem of the PhD thesis is the integration of technologies and the provision of different levels of security in the construction of an operational center in big data systems. Therefore, the last part of the chapter discusses key features and functions of operational security centers, as well as challenges related to the large volume and complexity of big data. As a result of the analysis, the software tools that are suitable to be used for the design of the OCISM are selected.

The second chapter is aimed at the design of an OCISM architecture. The basic principles for the design of such centers and some methods that are suitable for the design and implementation of an operational security center for big data systems are presented. The evolution of the architectures of operational information security centers is discussed, indicating the main challenges in designing and building a new fifth generation security operational center. Based on the analysis, updated principles to facilitate the design of OCISM are proposed, leading to the creation of a method for designing a new type of operational center for big data systems, ensuring that sensitive data is protected, security incidents are detected and responded to in time, and adaptation to changing technologies and businesses is achieved. The international standard ISO 27001 is used as a reference framework for the design of OCISM, and appropriate controls are selected and integrated into the methodological framework for the design of a new type of OCISM.

A method is proposed, incorporating the aforementioned controls and based on the defined principles, for creating a functional architecture that will allow the development of an up-to-date generation of OCISM that works with semi-structured and unstructured data using systems and solutions to process big data and extract knowledge from them. The proposed architecture has three levels of security management, including data retrieval and storage security, in-house based Hadoop security, and result analysis. The first level is based on Gartner's concept of adaptive security, a cybersecurity approach that constantly analyzes network behavior and events, and is ready to adapt to threats by researching and analyzing them before they happen, by processing data from video streams, social media and other heterogeneous sources, resulting in an improvement in the efficiency of the entire system, allowing it to adapt to changing circumstances and responding to emerging threats in real time. The second level of the proposed functional architecture focuses on the internal security of big data systems (within the infrastructure itself), which in this case

refers to internal-based Hadoop security, and software business security, including application-level security measures. The highest third level in the proposed functional architecture is an analysis and visualization of the results obtained, so that the events that have occurred can be more easily identified and notifications can be generated in the presence of a violation. At each of the levels, appropriate technological solutions are proposed to be implemented in a working model of OCISM.

Special attention is paid to adaptive security features for big data systems, and a conceptual architecture with relevant technological solutions is proposed. Specific applications for intelligent processing of data from different sources - social media, video streams from cameras and websites, for face and car plates recognition, counting people who have a context to determine a higher level of security, are also considered.

The third chapter describes the application of the proposed method for the design and development of an operational security center, presenting the functionalities with specific software solutions. An example of concrete implementation of the Operational Center for Information Security is also presented, through which the achievement of objectives is verified.

The Conclusion summarizes the results obtained, presents the achieved scientific and applied scientific contributions, lists the publications on the topic of the PhD thesis and provides guidelines for future work.

- *Assessment of the topic; the purpose; tasks; object; subject; main thesis of the dissertation*

The issues discussed in the PhD thesis correspond to the key role of information technologies in modern society. Information security is essential for the protection of data and information when storing, processing and analyzing big data. Since effective information security management requires an integrated approach, including the implementation of policies, standards, procedures and technical controls to protect against potential threats, the idea of building an operational center for information security management in order to ensure the protection of digital information and an appropriate level of security for business is an important research problem.

An approach for providing security at different levels of data, for processes and communications in big data systems, is proposed in the PhD thesis, relevant for data extracted from heterogeneous sources, e.g. video streams from cameras, data from websites, social media, etc. Having in mind similar offerings from leading IT companies (Kaspersky), the implementation of the Adaptive Security Strategy and the use of AI technologies for ensuring

information security when working with big data, is very up-to-date and innovative topic.

- *Used scientific literature (assessment of the awareness of the candidate on the issues discussed in the dissertation).*

The total number of literary sources used is 119, published in the last few years (after 2019), and including scientific publications and up-to-date information published on specialized websites.

3. Evaluation of scientific and applied research results achieved

The overall impression is that the PhD thesis is the result of a thorough and conscientious research activity. The document is very well structured, the exposition is clear and consistent. The author clearly defines her attitude on each issue, and the conclusions drawn and the approaches chosen are appropriately motivated.

A method for designing OCISM for big data systems is proposed, which is based on state-of-the-art methods, technologies and services for security protection, and in which an Adaptive Security Strategy is applied.

The developed architecture offers a multi-level approach to security management and aims to provide comprehensive protection for big data systems by integrating specific software technologies to achieve the set goals.

The presented results are obtained through an in-depth analysis of existing and proven effective approaches, standards and innovative technologies, for ensuring information security and processing big data. The proposed functional architecture is described with specific software solutions and a prototype is developed, integrating NiFi, Micro Focus IDOL and Apache Hadoop technologies. The prototype has been tested with unstructured social media data, video stream, website data and log files, and through this example case the implementation of the OCISM has been verified.

All of the above mentioned gives me the reason to conclude that the PhD student has achieved the scientific goal defined in the PhD thesis by obtaining the necessary scientific results.

4. Evaluation of scientific and applied research contributions

The author's contributions are appreciated as scientific contributions, in the field of enrichment of existing knowledge, and applied research contributions.

The *scientific contributions* of the PhD thesis include:

- Based on an in-depth analysis of modern approaches, principles and technologies, the following are outlined:
  - Definition and identified necessary elements of an "operational security center" for big data environments;
  - Appropriate criteria for comparison of big data processing technologies with a focus on collecting, organizing and storing unstructured data, with opportunities for the application of artificial intelligence tools;
  - Principles and methods for the development of OCISM, capturing the specifics of security management for big data systems.
- A proposed method for designing and creating a functional architecture of OCISM, including three levels of security management and covering network level of security, data extraction and processing, authentication of internal-based security in a big data environment, and analysis of the results obtained.

The *applied research contributions* of the PhD thesis include:

- A realized prototype, based on the technologies of the proposed architecture, using NiFi, Micro Focus IDOL and Apache Hadoop technologies, and tested with social media data, video stream, website data and log files.

5. Evaluation of dissertation publications

The total number of presented publications on the PhD thesis are 4 – 3 of them are conference papers and 1 is an article in a scientific journal. Two of the papers are authored by the candidate and are accepted at international conferences held in Bulgaria, one is co-authored – at an international conference abroad. The article is published in a reputable journal, indexed in well-known international scientific databases. All four publications are in English.

The reviewer is not aware that the submitted publications have received citations so far.

6. Evaluation of the autoref

The autoreferate fully corresponds to the content of the PhD thesis and correctly summarizes the scientific research performed and the results achieved.

7. Critical remarks, recommendations and questions

The comments and remarks made in the review of the internal department defense are taken into account and are correctly reflected.

The recommendations to the PhD student are mainly aimed at future publication of original scientific and applied research results in specialized journals and conferences with a high rating, in order to increase their visibility among the members of the scientific community and to increase the likelihood of obtaining citations.

8. Conclusion

In my opinion, Ivona Velkova is an accomplished researcher who has the necessary skills to formulate and solve scientific tasks independently. I believe that the presented PhD thesis meets the requirements established by the Law on the Development of Academic Staff in the Republic of Bulgaria, as well as the UNWE Rules for obtaining the requested educational and scientific degree of Doctor (PhD).

All of the above mentioned gives me grounds to propose to the honorable scientific jury to award the scientific and educational degree "Doctor" (PhD) to Ivona Velkova in the scientific specialty "Application of Computing in Economics".

25 May 2023 Signature:.....
Sofia