УНИВЕРСИТЕТ ЗА НАЦИОНАЛНО И СВЕТОВНО СТОПАНСТВО

Р Е Ц Е Н З И Я

От: проф. д-р Силвия Стоянова Парушева
Икономически университет - Варна
Научна специалност: 4.6. Информатика и компютърни науки

Относно: дисертационен труд за присъждане на образователна и научна степен „доктор“ по научна специалност „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 № 973/06.04.2023 г. 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

Докторант Ивона Велкова се е обучавала 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 № 966/30.04.2020 г. Обучението е осъществено в редовна форма през периода от 27.04.2020 до 27.04.2023 г. с научен ръководител на докторанта проф. д-р Любен Боянов. Процедурата по защита на дисертационния труд е разкрита с решение на катедра „Информационни

технологии и комуникации” (Протокол №9/30.03.2023) и решение на Факултетен съвет на факултет „Приложна информатика и статистика“ (Протокол №2 /03.04.2023 г.).

Ивона Велкова е родена в гр. Враца. Завършила е бакалавърска и магистърска степен в Университета за национално и световно стопанство съответно през 2018 и 2019 г. След завършването си е работила в счетоводна фирма „Роуз Вери“ ЕООД като оперативен счетоводител, а понастоящем заема позицията „дизайнер на софтуер“ в УНСС и се занимава с разработка на софтуер и конкретно със създаването на уеб приложения, поддръжка на университетските системи и обучение на кадри.

Като редовен докторант Ивона Велкова е изпълнила успешно задачите от индивидуалния си план. През първата година е положила общо пет изпита - три от изпитите за професионално направление и два за научната специалност, както и един в началото на третата година. През втората и третата година е работила с добро темпо по научно-изследователската работа, свързана с подготовка на дисертационния труд и публикации, свързани с него: четири доклада (три публикувани и един, който се очаква да бъде публикуван) и една статия. Отлично впечатление прави, че докторант Велкова е успяла да се вмести в сроковете на докторантурата, като в края на месец март 2023 г. или 1 месец преди края на срока й катедреният съвет на катедра „Информационни технологии и комуникации” е разкрил процедура по защитата й.

2. Обща характеристика на представения дисертационен труд

Дисертационният труд на Ивона Велкова е в общ обем от 170 стр. и обхваща въведение (обозначено като точка 1), три глави (съответно точки 2., 3. и 4.) , заключение (точка 5.), списък с научни и научно-приложни приноси, списък на публикациите по темата на труда, насоки за бъдеща работа, списък на литературните източници, списък на фигурите и таблиците и списък с използваните термини и съкращения. Представеният труд и неговата структура съответстват на изискванията за този род публикации.

Считам, че темата на дисертационния труд е изключително актуална поради факта, че съчетава в себе си две топ тенденции в развитието на информационните технологии през последните години - въпросите, свързани със значително увеличения обем на данните, генерирани от различни източници, и информационната сигурност и заплахите за данните.

Като обект на изследване в дисертацията са посочени принципите и методите за проектирането на оперативен център за управление на сигурността в системи за големи данни, а като негов предмет е посочено извеждането на „метод за изграждане на нов тип оперативен център за управление на сигурността, базиран на обработка с изкуствен интелект (ИИ) на неструктурирани данни, системи с големи данни и Управление на информацията за сигурността и събитията (Security information and event management - SIEM), интегрирани в обща архитектура“. Целта на дисертационния труд е да се предложат принципи и методи за проектиране и изграждане на оперативен център за управление на информационната сигурност за системи, опериращи с големи данни. За изпълнение на целта са заложени доста на брой задачи - общо девет, някои от които считам, че би било подходящо да се обединят.

В труда не е формулирана основна теза, но са изведени три основните работни хипотези, свързани със: създаване на модел за проектиране на оперативен център за управление на различни нива на информационната сигурност за системи с големи данни и извличането на данни от хетерогенни източници; ефективна интеграция на различни технологии и системи за работа с големи данни; многослойна архитектура с различни подходи за предоставяне на сигурност.

Списъкът с литературата обхваща 119 източника, като сред тях присъстват 67 интернет адреса, което показва, че докторантката се е позовавала предимно на актуални източници в онлайн среда.

3. Оценка на получените научни и научно-приложни резултати

Към постигнатите резултати в дисертационния труд могат да бъдат отнесени следните:

В първа глава (обозначена като точка 2) е представено научното изследване на предметната област. Авторът разглежда видовете данни, същността на големите данни, системите и подходите за обработка на големи данни. На база на система от 6 критерия е направено сравнение между четирите среди за големи данни. В изложението на главата на следващ етап се разглеждат приложенията на изкуствения интелект (ИИ) в областта на сигурността, като са изведени принципи и методи, приложими за осигуряване по-високо ниво на сигурност в организациите. Представени са принципите и подходите за управление на информационната сигурност с акцент върху системите за сигурност в средата на големи данни. С оглед обхващане на различните аспекти на сигурността и гарантиране на защитата на системата на различни нива са представени възможностите на оперативен център за информационна сигурност (ОЦИС).

Втора глава, обозначена като точка 3, е посветена на проектирането на принципи и методи за проектиране на архитектура на оперативен център за информационна сигурност. Първо са разгледани принципите и методите за проектиране на ОЦИС, след това е направен обзор на поколенията архитектури за оперативни центрове, посочени са предизвикателствата пред тях и проектирането на пето поколение центрове като възможност за преодоляването им. Изложени са актуалните принципи за изграждане на центрове и някои от контролите на стандарта ISO 27001, подходящи за внедряване в тези центрове. На следващ етап в главата се предлага метод за проектиране на архитектура на центрове за сигурност с *три нива на нейното управление*. Първото ниво се базира на адаптивна сигурност и интелигентна обработка, второто акцентира върху осигуряване на вътрешна сигурност в Hadoop среда и разглежда софтуерната бизнес сигурност, фокусирана върху сигурността на разработката и внедряването на софтуер. Третото ниво използва Security information and event management система, която осигурява мониторинг и

анализ в реално време на събития, свързани със сигурността. Намирам за много полезна предложената архитектура за адаптивна сигурност с нейните компоненти, подходяща за приложение в система с големи данни.

В трета глава (или точка 4.) се предприема потвърждаване на предложения метод чрез неговата верификация. В този процес се ползват редица от предложените инструменти за постигане на по-високо ниво на сигурност.

Прави много добро впечатление, че в края на всяка глава (втора, трета и четвърта точка) присъстват изводи, които обобщават постигнатото в главата.

Като обобщение на достиженията в дисертационния труд мога да посоча, че той е следвал поставените задачи и съответно успешно постига заложената цел на научното изследване.

4. Оценка на научните и научно-приложни приноси

В справката с научните и научно-приложни приноси на докторант Ивона Велкова присъстват шест приноса, които като цяло покриват постигнатите теоретични и практически резултати в дисертационния труд. Приемам ги за реално постигнати. Прави впечатление, че в последния принос се твърди, че е реализиран „прототип“ с прилагане на технологиите NiFi, Micro Focus IDOL и Apache Hadoop. Това се разминава с прилаганата терминология в четвърта точка, където не се говори за прототип, а се използва терминът „верифициране“. Би могло това да се унифицира.

Като цяло давам положителна оценка на постигнатите приноси. Считам, че те са достатъчно значими за предметната област на дисертацията. Прави добро впечатление, че в края на труда са дадени насоки за бъдеща работа по труда и неговото доразработване, с което докторант Велкова отговаря на потенциални въпроси за нейните бъдещи изследователски планове като научен работник.

5. Оценка на публикациите по дисертацията

В списъка с представените публикации по темата на дисертационния труд участват четири публикации – една самостоятелна статия на български език, 3 доклада на английски език от международни конференции, два от които са самостоятелни. Един труд е под печат. Посочените публикации са посветени на важни аспекти от дисертационния труд. Като количество и качество те отговарят на изискванията за придобиване на ОНС „доктор“.

6. Оценка на автореферата

Авторефератът отразява коректно структурата и съдържанието на дисертационния труд. Размерът му от 71 страници обаче надвишава стандартния обем за автореферат, който трябва по-синтезирано да представя дисертационното изследване.

7. Критични бележки, препоръки и въпроси

Предложената дисертация притежава нужните положителни страни като самостоятелен научен труд. Тя доказва способностите на докторанта да извърши научно изследване, свързано със сигурността в средата с големи данни и проектирането на оперативен център за управление на информационната сигурност за системи с големи данни. По отношение на труда могат да бъдат отправени и някои бележки, които не намаляват неговите достойнства. Посочените във въведението три хипотези би следвало да представляват част от единна научна теза на труда, развита според вижданията на докторанта в 3 основни направления.

Бих препоръчала също вместо „Създаване на *метод за проектиране* на функционална архитектура на оперативен център за сигурност“ и след това прилагането на този метод, да се използва „Разработване на *подход* за *проектиране* на …“ и впоследствие прилагане на този подход, т.е. считам, че е по-подходящо да се използва термина „подход“, който по-точно отговаря на постигнатото.

По отношение на списъка с източниците прави впечатление наличието на голяма количество онлайн източници. Смятам, че

подходящо да присъстват повече научни публикации - статии, доклади, студии и т.н., вкл. от наукометричните бази от данни като Scopus и WoS. Освен това описанието на някои източници е непълно, липсват важни задължителни атрибути. Като пример могат да се посочат източници [3], [20] и др.

Бих препоръчала докторантът да инициира съвместни публикации заедно със своя научен ръководител проф. д-р Любен Боянов.

Въпроси

В труда се използват понятията „информационна сигурност“ и „киберсигурност“. В разбиранията на автора има ли разлики между тях или те могат да се използват като взаимозаменяеми?

8. Заключение

Дисертационният труд на Ивона Велкова представлява самостоятелно научно изследване, което демонстрира нейната задълбочена теоретична подготовка в пресечната област на големите данни и сигурността. Същевременно той притежава и съществени научно-практически приноси. Дисертацията отговаря на изискванията на Закона за развитие на академичния състав в България, Правилника за неговото прилагане и Правилника на УНСС за прилагането му.

Посоченото ми дава основание да направя предложение на уважаваното научно жури да присъди образователната и научна степен „доктор“ по научна специалност „Приложение на изчислителната техника в икономиката“ на докторант Ивона Велкова.

26.05.2023 г. Подпис: …….....…

гр. Варна (проф. д-р Силвия Парушева)

UNIVERSITY OF NATIONAL AND WORLD ECONOMY

REVIEW

by Prof. Silvia Parusheva, PhD
University of Economics – Varna,
Professor in professional field 4.6 „Informatics and computer science”, validated in the register of academic composition of the National Academy of Sciences „Habilited persons with science indicators”; scientific specialty „Informatics and computer science”

Author of the dissertation work: Ivona PlamenovaVelkova

Theme of the dissertation work: Principles and methods for designing an operational center for managing information security for big data systems

PHD Thesis supervisor: Prof. Lyuben Boyanov, PhD

Primary Unit That Discovered the Procedure for the Thesis Defense: Department of “Information Technologies and Communications”, UNWE

Reason for writing the review: Order No 973/06.04.2023 of the Rector of University of National and World Economy for the opening of a procedure for the defense of the composition of a scientific jury; held the first meeting of the scientific jury on 25.04.2023.

1. Information about the PHD student

PHD student Ivona Velkova was trained in a doctoral program at the Department of “Information Technologies and Communications” of the UNWE in the scientific specialty “Application of computing technology in the economy” according to the Order of the Vice Rector for Research of the UNWE No. 966/30.04.2020. The training was carried out in regular form during the period from 27.04.2020 to 27.04.2023 with the scientific supervisor of the doctoral student Prof. Dr. Lyuben Boyanov. The procedure for the defense of

the dissertation was disclosed by the decision of the Department of Information Technologies and Communications (Protocol No. 9/30.03.2023) and the decision of the Faculty Council of the Faculty of Applied Informatics and Statistics (Protocol No. 2 /03.04.2023).

Ivona Velkova was born in Vratsa. She completed her bachelor's and master's degrees at the University of National and World Economy in 2018 and 2019, respectively. After her graduation, she worked at the “Rose Veri” EOOD accounting firm as an operational accountant, and currently holds the position of “software designer” at UNWE and deals with software development and specifically with the creation of web applications, support of university systems and staff training.

As a full-time PHD student, Ivona Velkova has successfully completed the tasks of her individual plan. In the first year, she passed a total of five exams - three of the exams for the professional direction and two for the scientific specialty, as well as one at the beginning of the third year. During the second and third years, she worked at a good pace on the research work related to the preparation of the dissertation and publications related to it: four reports (three published and one expected to be published) and one article. It makes an excellent impression that PHD student Velkova managed to fit in the terms of the doctoral studies, as at the end of March or 1 month before the end of her term, the departmental council of the “Information Technologies and Communications” department revealed a procedure for her defense.

2. General characteristics of the presented dissertation work

Ivona Velkova's dissertation has a total volume of 170 pages and includes an introduction (marked as section 1), three chapters (respectively sections 2., 3. and 4.), a conclusion (section 5.), a list of scientific and applied contributions, list of publications on the topic of the work, directions for future work, list of literature sources, list of figures and tables, and list of used terms and abbreviations. The presented work and its structure correspond to the requirements for this kind of publication.

In my opinion, the topic of the dissertation is extremely relevant because it combines two top trends in the development of information technologies in

recent years - the issues related to the significantly increased volume of data generated from various sources and information security and data threats.

As the object of research in the dissertation, the principles, and methods for the design of an operation center for security management in big data systems are specified, and as its subject, the derivation of “a method for building a new type of operation center for security management based on artificial intelligence (AI) processing of unstructured data, big data systems and Security information and event management (SIEM) integrated into a common architecture”. The purpose of the dissertation is to propose principles and methods for the design and construction of an information security management operations center for systems operating with big data. To fulfill the goal, quite several tasks are set - nine in total, some of which I believe would be appropriate to combine.

The dissertation does not formulate a main thesis, but three main working hypotheses related to: creating a model for designing an operational center for managing different levels of information security for big data systems and the extraction of data from heterogeneous sources; effective integration of various technologies and systems for working with big data; a multi-layered architecture with different approaches to providing security.

The bibliography includes 119 sources, including 67 Internet addresses, which shows that the doctoral student referred mainly to up-to-date sources in the online environment.

3. Evaluation of the obtained scientific and scientific-applied results

The following can be attributed to the achieved results in the dissertation work:

In the first chapter (marked as section 2) the scientific research of the subject area is presented. The author examines the types of data, the nature of big data, systems, and approaches for processing big data. Based on a system of 6 criteria, a comparison is made between the four big data environments. The presentation of the next stage of the chapter examines the applications of artificial intelligence (AI) in the field of security, and the principles and methods applicable to ensure a higher level of security in organizations are

derived. Information security management principles and approaches are presented with an emphasis on security systems in big data environments. With a view to covering the various aspects of security and guaranteeing the protection of the system at various levels, the capabilities of an operational information security center (OISC) are presented.

A second chapter, designated as section 3, is devoted to the design principles and methods of designing an information security operations center architecture. First, the principles and methods for the design of OISC are examined, then an overview of the generations of operating center architectures is made, the challenges facing them and the design of fifth generation centers as an opportunity to overcome them are indicated. Current principles for building centers and some of the controls of the ISO 27001 standard suitable for implementation in these centers are presented. At the next stage, the chapter proposes a method for designing a security center architecture with three levels of its management. The first level is based on adaptive security and intelligent processing, the second focuses on providing internal security in a Hadoop environment and considers software business security, focused on the security of software development and deployment. The third level uses a Security information and event management system that provides real-time monitoring and analysis of security-related events. I find very useful the proposed adaptive security architecture with its components suitable for application in a big data system.

In the third chapter (or section 4.), confirmation of the proposed method is undertaken through its verification. In this process, a number of the proposed tools are used to achieve a higher level of security.

It makes a very good impression that at the end of each chapter (second, third and fourth sections) there are conclusions that summarize what has been achieved in the chapter.

As a summary of the achievements in the dissertation work, I can point out that it followed the set tasks and accordingly successfully achieved the set goal of the scientific research.

4. Evaluation of scientific and scientific-applied contributions

In the list of scientific and scientific-applied contributions of doctoral student Ivona Velkova, there are six contributions, which generally cover the theoretical and practical results achieved in the dissertation work. I accept them as actually achieved. Notably, the latest contribution claims to have implemented a „prototype“ using NiFi, Micro Focus IDOL and Apache Hadoop technologies. This diverges from the terminology used in the fourth point, which does not speak of a prototype, but uses the term "verification". This could be unified.

In general, I give a positive assessment of the contributions achieved. I believe that they are sufficiently relevant to the subject area of the dissertation. It makes a good impression that at the end of the paper, guidelines are given for future work on the paper and its further development, with which doctoral student Velkova answers potential questions about her future research plans as a researcher.

5. Evaluation of dissertation publications

The list of presented publications on the topic of the dissertation includes four publications - one independent article in Bulgarian, 3 reports in English from international conferences, two of which are independent. A paper is in print. The mentioned publications are devoted to important aspects of the dissertation work. In terms of quantity and quality, they meet the requirements for obtaining the educational and scientific degree „Doctor“.

6. Evaluation of the abstract

The abstract correctly reflects the structure and content of the dissertation work. However, its size of 71 pages exceeds the standard volume for an abstract, which should present the dissertation research in a more synthesized way.

7. Critical notes, recommendations, and questions

The proposed dissertation has the necessary positive aspects as an independent scientific work. It demonstrates the doctoral student's abilities to

conduct scientific research related to security in a big data environment and the design of an information security management operations center for big data systems. Regarding the work, some remarks can be made that do not detract from its merits. The three hypotheses mentioned in the introduction should represent part of a single scientific thesis of the work, developed according to the views of the doctoral student in 3 main directions.

I would also recommend that instead of “Establish a method to design a functional security operations center architecture” and then implement that method, use “Develop an approach to design ...” and then implement that approach, i.e. I believe it is more appropriate to use the term “approach” which more accurately corresponds to what has been achieved.

Regarding the list of sources, the presence of many online sources is striking. I think it is appropriate to present more scientific publications - articles, reports, studies, etc., incl. from scientometric databases such as Scopus and Web of Science. In addition, the description of some sources is incomplete, missing important mandatory attributes. As an example, sources [3], [20], etc. can be mentioned.

I would recommend that the doctoral student initiates joint publications together with his supervisor Prof. Dr. Lyuben Boyanov.

Questions

The dissertation uses the terms “information security” and “cyber security”. In the author's understanding, are there differences between them, or can they be used interchangeably?

8. Conclusion

Ivona Velkova's dissertation is an independent scientific study that demonstrates her in-depth theoretical training in the intersection of big data and security. At the same time, he also has significant scientific and practical contributions. It meets the requirements of the Law on the Development of the Academic Staff in Bulgaria, the Regulations for its Implementation and the UNWE Regulations for its Implementation.

The above gives me the reason to make a proposal to the respected scientific jury to award the educational and scientific degree “Doctor” in the scientific specialty “Application of computing technology in the economy” to doctoral student Ivona Velkova.

26.05.2023 Signature: …….....…

Varna (Prof. Dr. Silvia Parusheva)