УНИВЕРСИТЕТ ЗА НАЦИОНАЛНО И СВЕТОВНО СТОПАНСТВО

С Т А Н О В И Щ Е

От: проф. д-р Евгения Петрова Ковачева*;*
Университет по библиотекознание и информационни технологии;
4.6. Информатика и компютърни науки

Относно: дисертационен труд за присъждане на образователна и научна степен **„доктор“** по ПН 3.8 Икономика в 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

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

1. Информация за дисертанта

Дисертантът се е обучавал по докторска програма към Информационни технологии и комуникации/ Факултет Приложна информатика и статистика на УНСС по ПН 3.8 *Икономика*, докторантска програма *Приложение на изчислителната техника в икономиката* съгласно Заповед на Зам.-ректора по НИД на УНСС № 966/30.04.2020. Обучението е осъществено в редовна форма през периода 27.04.2020 - 27.04.2023.

2. Обща характеристика на представения дисертационен труд

Темата на дисертационния труд е актуална. В момента създаването на оперативни центрове за управление на информационната сигурност за големи данни е важен процес, защото ние генерираме все повече данни и е важно те да бъдат защитени. Проектирането на системи трябва да бъде сигурно по дизайн.

Представеният дисертационен труд е разположен на 153 страници, разделена в 3 глави: Сигурност в среда на големи данни и оперативен

център за сигурност, Проектиране на архитектура на оперативен център за информационна сигурност, Прилагане на метода за оперативен център за сигурност с архитектурни решения.

Посочените три глави покриват амбициозните 9 задачи на докторантката за постигане на основната цел. Всяка глава завършва с изводи.

Разгледани са 119 източника. Не може да се отчете колко от използваните източници са от последните пет години, защото на голяма част от изброената литература липсва година на издаване. За съжаление на навсякъде фигурира автор на публикацията. На някои места е сложен публикуващия [4, 15], но на други места го няма [1,5,8, 16, 21-24 и т.н.]. Липсват и годините на издаване на част от материалите, има и връзки, които не водят към представения материал, например [14]. Например при отваряне на [39] ясно се вижда автора и годината на публикуване, но те липсват в текста *By Yustyna Velykholova, March 30, 2017*.

3. Оценка на получените научни и научно-приложни резултати

Прави добро впечатление познаването на терминологичния език и коректното разделение на сигурността физическа, информационна, кибер и т.н.

Представените основни елементи и функционалности на Оперативните центрове за информационна сигурност в 2.4 са извлечени от насоките на Европейската комисия и други източници от [73-88]. Преди да се изгради и приложи *Метода за оперативен център за сигурност с архитектурни решения* глава 4 е добре да се представят вече създадени такива центрове. Детайлната информация със сигурност е конфиденциална, но като примери биха обогатили работата. Прилагането на различни типове решения и спецификата на приложимостта на адаптивна сигурност, на решения за интелигентна обработка на данни, на второ ниво от функционалната архитектура показват разбирането и дълбокото проучване на докторантката.

Илона Велкова поставя трите си работни хипотези в началото на дисертационния труд и накрая обръща внимание, че те са доказани успешно.

Дисертационният труд е илюстриран с 43 изображения. При Проектиране на архитектура на оперативен център за информационна сигурност би било добре да има повече разработки на докторантката тук ясно е отличена фигура 15, но създаването на повече визуално представят подобрява разбирането на материята.

Единствената приложена таблица за *Сравнение между технологичните среди за големи данни* може да бъде мултиплицирана при сравнение на технологиите и други фактори, които докторантката представя в работата си. Табличното представяне систематизира и дава по-бързо и по-ясна картина.

4. Оценка на научните и научно-приложни приноси

Докторантката е представила 6 научно и научно-приложни приноса.

1. Изследвана е същността и компонентната структура на „оперативен център за сигурност“ и е дефинирано актуално определение и необходими елементи, спрямо съвременните условия за функциониране на такъв център в среда на големи данни.
2. Предложени са критерии за сравнение на технологии за обработка на големи данни, във връзка с целите на разработката по отношение на събирането, организацията и съхранението на неструктурирани данни, с възможности за прилагане на средства за изкуствен интелект.
3. Изведени са основни принципи и методи за управление на оперативен център за информационна сигурност, обхващащи процеса, функционалностите и нивата на сигурност.
4. За проектирането и изграждането на ОЦИС са предложени актуални принципи, необходими за обхващане на спецификата на управление на сигурността на системите, работещи в среда на големи данни.
5. Дефиниран е метод за проектиране и създаване на функционална архитектура на ОЦИС. Предложената архитектура е с 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.
6. Реализиран е прототип, изграден с технологиите на предложената архитектура с цел обхващане на всички необходими функционалности. Прототипът свързва технологиите NiFi, Micro Focus IDOL и Apache Hadoop и е тестван с данни от социални медии, видео поток, данни от уебсайтове и лог файлове

Според мен основният й научно-приложен принос е 2, който е специфичен за обработката на големи данни. Приносите 4 и 6 бих ги окачествила като приложни.

5. Оценка на публикациите по дисертацията

Представените четири публикации, представят разработката на Илона Велкова главно по глава 2. Добре би било да публикува и извлечените от нея особености на проектирането на оперативните центрове.

6. Оценка на автореферата

Авторефератът би трябвало да бъде съкратена версия на дисертационния труд. Това, което ми бе предоставено бе 135 страници, а дисертационният труд 170. Може би има неточно подаден файл.

7. Критични бележки, препоръки и въпроси

Както споменах в началото препоръчвам на Ивона Велкова по-стриктно да цитира използваната литература в бъдеще както в списъка със заглавията така и за изображенията. Важно е да уважаваме труда на другите, от които черпим информация.

Докторантката има смесен изказ трето лице единствено число и първо лице множествено. Това се наблюдава главно в изводите на всяка глава, но е добре да се придържа към един и да подчертава заслугите си с *виждането на докторанта или докторантът …..*

Нямам лични впечатления от Илона Велкова, но в дисертационния й труд виждам изграден учен, който се стреми да проучи в детайли поставените задачи.

8. Заключение

Независимо от направените критични бележки, въз основа на гореизложеното положително становище, препоръчвам на научното жури да предложи на компетентния орган по избора на Факултет Приложна информатика и статистика на УНСС да присъди на Ивона Пламенова Велкова образователната и научна степен „доктор“ в ПН 3.8 Икономика, докторантска програма Приложение на изчислителната техника в икономиката

Дата / място Подпис: ……

UNIVERSITY OF NATIONAL AND WORLD ECONOMY

O P I N I O N

By: Prof.Eugenia Petrova Kovatcheva, PhD;
University of Library Studies and Information Technologies;
4.6. Informatics and Computer Science

Subject: dissertation work for awarding the educational and scientific degree PhD in 3.8 Economics at UNWE.

Author of the PhD thesis: Ivona Plamenova Velkova

PhD Topic: Principles and Methods for Designing an Information Security Management Operations Center for Big Data Systems

Reason for presenting the opinion: participation in the composition of the scientific jury for the defense of the dissertation according to Order No. 973/06.04.2023 of the Rector of the UNWE.

1. Information about the PhD student

The PhD student was trained in a doctoral program at Information Technologies and Communications/ Faculty of Applied Informatics and Statistics of UNWE under 3.8 Economics, a doctoral program Application of computing technology in the economy according to the Order of the Deputy Rector for Research and Development of UNSS No. 966/30.04.2020 . The training was carried out in regular form during the period 27.04.2020 - 27.04.2023.

2. General characteristics of the presented PhD Thesis

The topic of the PhD thesis is a hot topic. Currently, the creation of security operations centers for big data is an important process because we are generating more and more data and it is important they are secure. It has to be secure by design.

The presented dissertation is spread over 153 pages, divided into 3 chapters: Security in a Big Data Environment and Security Operations Center, Designing an Information Security Operations Center Architecture, Applying the Security Operations Center Method with Architectural Solutions.

The mentioned three chapters cover the ambitious 9 tasks of the doctoral student to achieve the main goal. Each chapter ends with conclusions.

119 sources were reviewed. It is not possible to count how many of the sources used are from the last five years because much of the literature listed is missing a year of publication. Unfortunately, the author of the post appears everywhere. In some places the publisher is included [4, 15], but in other places it is not [1,5,8, 16, 21-24, etc.]. The years of publication of some of the materials are also missing, there are also links that do not lead to the presented material, for example [14]. For example, when opening [39] the author and the year of publication are clearly visible, but they are missing in the text By Yustyna Velykholova, March 30, 2017.

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

Knowledge of terminology and the correct division of security into physical, informational, cyber, etc. makes a good impression.

The main elements and functionalities of Information Security Operations Centers presented in 2.4 are derived from European Commission guidelines and other sources from [73-88]. Before building and implementing the Security Operations Center Method with Architectural Solutions Chapter 4, it is good to present already established such centers. Detailed information is certainly confidential, but examples would enrich the work. The implementation of different types of solutions and the specifics of the applicability of adaptive security, intelligent data processing solutions, at the second level of the functional architecture show the understanding and deep research of the PhD student.

Ilona Velkova puts her three working hypotheses at the beginning of the dissertation and finally points out that they have been successfully proven.

The dissertation is illustrated with 43 images. In Designing an Information Security Operations Center Architecture, it would be nice to have more own work here, Figure 15 is clearly highlighted, but creating more visual representations improves understanding of the subject matter.

The single attached table for Comparison of Big Data Technology Environments can be multiplied when comparing the technologies and other factors that the PhD student presents in her work. Tabular presentation systematizes and gives a faster and clearer picture.

4. Evaluation of scientific and scientific-applied contributions

The PhD student presented 6 scientific and scientific-applied contributions.

1. The essence and component structure of a "security operations center" has been studied and an up-to-date definition and necessary elements

have been defined, in relation to the modern conditions for the operation of such a center in a big data environment.

2. Criteria are proposed for the comparison of technologies for processing big data, in relation to the development goals regarding the collection, organization and storage of unstructured data, with possibilities of applying means of artificial intelligence.
3. Basic principles and methods for managing an information security operations center covering the process, functionalities and levels of security are outlined.
4. Up-to-date principles are proposed for the design and construction of OCIS, necessary to cover the specifics of security management of systems operating in a big data environment.
5. A method for designing and creating a functional architecture of the OCIS is defined. The proposed architecture has three levels of security management, covering network level security, data extraction and processing process, authentication of internal-based security in big data environment and analysis of the obtained results.
6. A prototype was implemented, built with the technologies of the proposed architecture in order to cover all the necessary functionalities. The prototype connects NiFi, Micro Focus IDOL and Apache Hadoop technologies and has been tested with social media data, video stream, website data and log files

In my opinion, her main scientific and applied contribution is 2, which is specific to big data processing. I would classify contributions 4 and 6 as applied.

5. Evaluation of dissertation publications

The presented four publications present the development of Ilona Velkova mainly in chapter 2. It would be good if she also published the features of the design of the Security Operational Centers derived from her.

6. Evaluation of the autoref

The abstract should be a shortened version of the dissertation. What I was received was 135 pages and the thesis was 170. Maybe there is an incorrect file submitted.

7. Critical notes, recommendations and questions

As I mentioned at the beginning, I recommend that Ivona Velkova more strictly cite the literature used in the future both in the list of titles and for the

images. It is important to respect the work of others from whom we draw information.

The PhD student has a mixed singular and plural statements. This is mainly seen in the conclusions of each chapter, would be good to keep consistency.

I have no personal impressions of Ilona Velkova and in her PhD thesis I see a scientist who strives to study the tasks set in detail.

8. Conclusion

Regardless of the critical comments I made and based on my above mentioned positive opinion, I recommend the scientific jury to propose to the competent authority for the selection of the Faculty of Applied Informatics and Statistics of the UNSS to award Ivona Plamenova Velkova the educational and scientific degree Doctorate of Philosophy in 3.8 Economics, doctoral program Application of computer technology in economics

Date / place Signature: ……