УНИВЕРСИТЕТ ЗА НАЦИОНАЛНО И СВЕТОВНО СТОПАНСТВО

С Т А Н О В И Щ Е

От: **доц. д-р Веселин Димитров Попов**
Стопанска академия „Д. А. Ценов“ – Свищов
Научна специалност „Приложение на изчислителната техника в икономиката“

Относно: дисертационен труд за присъждане на образователна и научна степен **„доктор“** по *05.02.08 „Приложение на изчислителната техника в икономиката“* 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 г. на Ректора на УНСС.

1. Информация за дисертанта

Дисертантът се е обучавал по докторска програма към катедра „Информационни технологии и комуникации“ на УНСС по научна специалност „Приложение на изчислителната техника в икономиката“ съгласно Заповед на Ректора на УНСС № 966/30.04.2020 г. Обучението е осъществено в редовна форма през периода от 27.04.2020 г. до 27.04.2023 г.

2. Обща характеристика на представения дисертационен труд

Представеният дисертационен труд е в обем от 169 страници и се състои от: въведение; три глави; заключение, включващо научни и научно-приложни приноси, списък с публикации по темата на дисертационния труд, бъдеща работа и използвана литература; списък на фигурите; списък на таблиците; използвани съкращения. Научният

проблем е представен на 147 страници, илюстриран е с 43 фигури, а данните са систематизирани в 1 таблица. Библиографската справка включва 119 литературни източници. Дисертационният труд е представен във вид и обем, съответстващи на изискванията и критериите за такъв тип разработки.

Използването на големи данни и свързаната с тях сигурност са актуален научен проблем. Тази актуалност е добре обоснована от автора във въведението на дисертационния труд.

Обектът, предметът на изследването и изследователският проблем са добре дефинирани. С тях са свързани формулираната цел и поставените задачи. Въпреки големия брой поставени задачи (девет) може да се отчете, че те са изпълнени успешно.

Изследователска теза не е дефинирана, а е представена чрез три хипотези, който са доказани в изложението. За постигане на целта и решаване на изследователските задачи на научното изследване са използвани разнообразни подходи и методи като, системен анализ и синтез, сравнителен анализ, аналогия, систематизация, прототипиране и др. Изложението има добра логическа последователност.

Използваните литературни източници са коректно цитирани. Проверката за плагиатство на дисертационния труд с програмата StrikePlgiarizm.com, извършена на 5.9.2023 г. показва изключително ниска повторяемост при сравнението с документи от базата данни.

3. Оценка на получените научни и научно-приложни резултати

Докторантката предлага метод за проектиране на оперативен център за информационна сигурност (ОЦИС), който включва три нива на управление и прилага принципи и методи типични за информационната сигурност и киберсигурността, както и контроли от ISO 27001. Първото ниво включва адаптивна сигурност и интелигентна обработка, второто осигурява вътрешна сигурност в средата Hadoop и се фокусира върху сигурността на софтуерния бизнес, а третото ниво използва SIEM система за наблюдение и анализ на събития за сигурност в реално време. С това тя постига целта на дисертационния труд – да бъдат предложени принципи и методи за проектиране и изграждане на оперативен център, който да управлява информационната сигурност, за системи, опериращи с големи данни.

Реализиран е прототип, изграден с технологиите на предложената архитектура. 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.

4. Оценка на научните и научно-приложни приноси

Приемам всички посочени от автора научни и приложни приноси. Като най-значими от тях, може да се посочат следните:

- 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.
- 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.

Направените приноси имат значение за теорията и практиката на управлението на информационната сигурност в системи с големи данни.

5. Оценка на публикациите по дисертацията

Авторът е представил четири публикации, свързани с темата на дисертационния труд – една статия и три доклада на научни конференции. Три от тях са на английски език. Единият от докладите е изнесен на конференция в чужбина.

6. Оценка на автореферата

Авторефератът отговаря на изискванията и точно отразява съдържанието на дисертационния труд.

7. Критични бележки, препоръки и въпроси

Въпреки безспорните качества на дисертационния труд, мога да направя следните препоръки:

- Авторефератът превишава препоръчителния обем. Той може по синтезирано и по-накратко да представи дисертационния труд;
- Реализираният прототип, изграден с технологиите на предложената архитектура следва да бъде по-подробно описан в глава 2. „Сигурност в средата на големите данни и оперативен център за сигурност“. В дисертационния труд реализираният прототип само е споменат в принос № 6.

Към автора на дисертационния труд имам два въпроса.

1. На фиг. 13 са представени използваните технологии при различните нива на ОЦИС. Както посочва автора, на ОЦИС е важно да се постигне интеграция на усъвършенствани инструменти за управление на сигурността, като решения за SIEM, QRadar и MicroFocus IDOL. Как се решава интеграцията на тези инструменти и възможно ли е да възникнат рискове в тази насока за функционирането на ОЦИС?

2. Възможни ли са проблеми с мащабирането и производителността на оперативния център за сигурност, когато платформата обработва големи обеми от данни, предвид обстоятелството, че обработката на големи данни и използването на изкуствен интелект за тази цел са ресурсоемки дейности?

8. Заключение

На база гореизложеното, считам че дисертационният труд на Ивона Пламенова Велкова представлява самостоятелно изследване по актуален и значим проблем, както за теорията, така и за практика на информационните технологии. Трудът съдържа необходимите научни и научно-приложни приноси и отговаря на всички изисквания и критерии за присъждане на образователната и научна степен „Доктор".

Всичко това ми дава основание да дам положителна оценка „Да" за присъждане на образователната и научна степен „доктор" по научна специалност „Приложение на изчислителната техника в икономиката" на Ивона Пламенова Велкова.

18.05.2023 г. Подпис: ……

Свищов

UNIVERSITY OF NATIONAL AND WORLD ECONOMY

O P I N I O N

By: **Assoc. prof. Veselin Dimitrov Popov, PhD,**
Department of Business Informatics; D. A. Tsenov Academy of Economics – Svishtov,
professional field 05.02.08 „Application of Computing in Economics“

About: dissertation for awarding the educational and scientific degree **„doctor“** in a professional field 05.02.08 „Application of Computing in Economics“ at UNWE.

Author of the dissertation: **Ivona Plamenova Velkova**
Topic of the dissertation: *“Principles and methods for designing an operational centre for managing information security for big data systems“ ”*

Grounds for writing the opinion: participation in the scientific jury for the defence of the dissertation according to Order No. 973/06.04.2023 г. of the Deputy Rector for Research and Development of the UNWE.

1. Information about the PhD student

The PhD student was trained in a doctoral program at the Department of "Information Technologies and Communications" of the UNWE, professional direction 3.8 Economics, doctoral program "Application of computing technology in the economy", according to Order of the Rector of the UNWE No. 966/30.04.2020 г. The training was carried out in regular form during the period from 27.04.2020 to 27.04.2023.

2. General description of the presented dissertation

The presented dissertation is 169 pages long and consists of: introduction; three heads; conclusion, including scientific and scientific-applied contributions, a list of publications on the topic of the dissertation work, future work and literature used; list of figures; list of tables; abbreviations used. The scientific problem is presented on 147 pages, illustrated with 43 figures, and the data is systematized in 1 table. The bibliographic reference includes 119 literary

sources. The dissertation is presented in a form and volume corresponding to the requirements and criteria for this type of development.

The use of big data and the security associated with it is a current scientific problem. This relevance is well justified by the author in the introduction of the dissertation.

The object, the subject of the study and the research problem are well defined. The formulated goal and set tasks are related to them. Despite the large number of defined tasks (nine), it can be said that they were successfully completed.

A research thesis is not defined, but is presented through three hypotheses, which are proven in the exposition. To achieve the goal and solve the research tasks of the scientific study, various approaches and methods were used, such as, system analysis and synthesis, comparative analysis, analogy, systematization, prototyping, etc. The exposition has a good logical sequence.

The used literary sources are correctly cited. Dissertation plagiarism check with StrikePlgiarizm.com program performed on 5.9.2023 shows extremely low repeatability when compared to database documents.

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

The PhD student proposes a method for designing an information security operations centre (OCIS) that includes three levels of management and applies principles and methods typical of information security and cyber security, as well as controls from ISO 27001. The first level includes adaptive security and intelligent processing, the second provides internal security in the Hadoop environment and focuses on software business security, and the third level uses a SIEM system to monitor and analyse real-time security events. With this, the author achieves the goal of the dissertation - to propose principles and methods for designing and building an operations centre to manage information security for systems operating with big data.

A prototype built with the technologies of the proposed architecture has been implemented. The prototype combines NiFi, Micro Focus IDOL and Apache Hadoop technologies and has been tested with social media data, video stream, website data and log files.

4. Evaluation of obtained scientific and scientific-applied contributions

I accept all scientific and applied contributions indicated by the author. As the most significant of them, the following can be mentioned:

- 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.

- A prototype was implemented, built with the technologies of the proposed architecture in order to cover all the necessary functionalities. The prototype combines NiFi, Micro Focus IDOL and Apache Hadoop technologies and has been tested with social media data, video stream, website data and log files.

These contributions have implications for the theory and practice of information security management in big data systems.

5. Evaluation of the publications concerning the dissertation

The author has presented four publications related to the topic of the dissertation - one article and three reports at scientific conferences. Three of them are in English. One of the reports was presented at a conference abroad.

6. Evaluation of the abstract of the dissertation

The abstract meets the requirements and accurately reflects the content of the dissertation.

7. Critical remarks, recommendations, and questions

Despite the undoubted qualities of the dissertation work, I can make the following recommendations::

- The abstract exceeds the recommended volume. He can present the thesis in a synthesized and more concise way;
- The realized prototype built with the technologies of the proposed architecture should be described in more detail in Chapter 2. "Security in the Big Data Environment and Security Operations Center". In the dissertation, the realized prototype is only mentioned in contribution No. 6.

I have two questions for the author of the dissertation.

1. In fig. 13 presents the technologies used at the different levels of OCIS. As the author points out, achieving integration of advanced security management tools such as SIEM solutions, QRadar, and MicroFocus IDOL is important to OCIS. How is the integration of these tools decided and is it possible for risks to arise in this direction for the functioning of the OCIS?
2. Are security operations centre scaling and performance issues possible when the platform processes large volumes of data, given

that processing big data and using artificial intelligence for this purpose are resource-intensive activities?

8. Conclusion

Based on the above, I believe that the dissertation work of Ivona Plamenova Velkova represents an independent study on a current and significant problem, both for the theory and practice of information technologies. The work contains scientific and scientific-applied contributions and meets all the requirements and criteria for awarding the educational and scientific degree "Doctor".

All this gives me the reason to give a positive rating "**Yes**" for awarding the educational and scientific degree "**doctor**" in the scientific specialty "Application of Computing in Economics" to **Ivona Plamenova Velkova**.

18.05.2023 г. Signature: ……

Svishtov