ЮГОЗАПАДЕН УНИВЕРСИТЕТ
·НЕОФИТ РИЛСКИ·
БЛАГОЕВГРАД

СТАНОВИЩЕ

От: доц. д-р Елена В. Ставрова, „ЮЗУ „Н. Рилски“-Благоевград, Научна специалност „Финанси, парично обръщение, кредит и застраховка“, професионално направлеие 3.8. Икономика,

Относно: Дисертационен труд на тема: „***„Финансовите разходи за кибер риск в бизнеса и публичния сектор в Гърция“***

Основание за представяне на становището: участие в състава на научното жури по защита на дисертационния труд, съгласно Заповед No 1267 /10.06. 2025 г. на проф. д-р Николай Марин, Ректор на ЮЗУ „Н. Рилски“-Благоевград.

Автор на дисертационния труд: Мария Стефанос Куцари

I. Общо представяне на дисертационния труд

Дисертационният труд на Мария Стефанос Куцари за присъждане на образователната и научна степен „**Доктор**“ се състои от увод, три глави, заключение и използвана литература. Той включва 153 страници текст, 22 таблици, 30 фигури и и справка за използваната литература, съдържаща 111 заглавия..

Темата на дисертацията е изключително актуална и значима както в международен, така и в национален контекст. В условията на дигитализация на публичния и частния сектор, изследването на финансовите измерения на киберриска в Гърция допринася за по-дълбоко разбиране на икономическите последствия от нарастващите киберзаплахи не само в национален, но и в международен контекст. Изследването попълва съществена празнина в литературата, особено като се има предвид оскъдната достъпна емпирична информация за региона. В същото време тя е много комплексна и сложна, и за разработването ѝ са необходими добра теоретична подготовка, високи аналитични способности и опит в извършването на научни изследвания.

Обектът на изследване в дисертацията е **финансовото въздействие на киберриска върху ключови индустрии в частния и публичния сектор на Гърция**. Това включва реални икономически сектори, които са особено уязвими към киберзаплахи поради високата си степен на дигитализация и критично значение за националната икономика, като : Енергетика; Комуникации; Здравеопазване; Ритейл (търговия на дребно); Банки и финанси; Дигитална инфраструктура; Правителствени услуги. Заслужава да се отбележи , че този избор е напълно основателен и е свързан с голямата им икономическа тежест в БВП на Гърция, различната им степен на подготвеност и уязвимост към кибератаки, както и критичното им значение за функционирането на държавата като субект.

Предметът на изследването е **количественото измерване и анализ на финансовите разходи, причинени от киберинциденти** – включително преките (напр. глоби, възстановителни дейности), непреките (загуба на репутация, доверие на клиентите) и пропуснатите ползи. Разработеният инструментариум с цел финансиализация на проблема с кибератаките е подчинен на целта – оценяване на ефектите и възможности за управление и прогнозиране на щетите с включването в базата данни за изследване на : **честота на инциденти** в отделните сектори, **разходи за инцидентит**е, връзката между инциденти и **системен риск**, ефектите на инцидентите върху **устойчивостта и конкурентоспособността на икономиката.**

Спазено е утвърденото изискване за дисертационен труд: точно и ясно е определена изследователската **теза.**

Прецизно са представени основните изследователски подходи и **методи**, включващи теоретично обобщаване, сравнителен анализ, дескриптивен анализ и оригинални иконометрични методи като изчисляване на процента на инцидентите, логаритмичен регресионен анализ за изследване на връзките между финансовите разходи и специфичните за индустрията фактори, системен анализ на риска (използвайки съотношението дълг/приходи) и двувариатен анализ (тестове за корелация на тау на Пиърсън и Кендъл).

Структурата на дисертацията е логически изградена и е подчинена на цялостното разработване на изследователския проблем, на постигането на седем изследователски **задачи и цели**. Текстът е обогатен и сполучливо онагледен с таблици и фигури, които способстват за лесното му възприемане и вникване в същността на изследването.

II. Преценка на формата и съдържанието на дисертационния труд

В **Първа глава** на дисертацията се въвежда и дефинира концепцията за кибер риск в контекста на нарастващото развитие на информационните технологии и повсеместното разпространение на Интернет и поставя акценти върху произхода и еволюцията на Интернет и киберпространството, значението на киберпространството и ИКТ, нарастващия брой кибер заплахи, управлението на кибер риска, ролята на отделните индивиди в условията на угроза от кибератаки, Подобаващо място и внимание е отделено на Национална стратегия на Гърция, структурирана около 5 основни оси, 15 цели и над 50 действия. Направено е обобщение на основните роли и действия на частния и публичния сектор в управлението на киберсигурността, включително техническа сигурност, политики, повишаване на осведомеността, одити, планове за кризи, научноизследователска и развойна дейност и подкрепа за гражданите и МСП. Оригинален принос на докторанта е въвеждането концепцията за управление на риска и споделената отговорност в борбата срещу кибер заплахите.

Втора глава описва развитието и текущото състояние на стратегиите за киберсигурност в Гърция, със специален фокус върху цифровите финансови услуги. В нея дисертантът е анализирал актуалното състояние на и**нституционалната рамка за киберсигурност, представена от** ключови институции и законодателни мерки, създадени в Гърция за борба с киберзаплахите. Подчертава се ролята на тези органи в предотвратяването, разследването и подобряването на цифровата трансформация на публичния сектор. Анализирани са н**ационалните и международни инициативи в тази област.** Подчертан е значителният напредък на Гърция в областта на киберсигурността, като страната заема 7-мо място в Националния индекс за киберсигурност (NCSI) за периода 2016-2023 г., което я поставя сред челните позиции в световен мащаб. Това постижение се дължи на координираните усилия на различни гръцки органи. Втора глава предоставя подробен преглед на всеобхватните стратегии и институционални мерки за киберсигурност в Гърция. Тя демонстрира ангажимента на страната за защита на критичната инфраструктура и гражданите, като същевременно набляга на адаптацията на бизнеса и финансовия сектор към новите заплахи и включването на напредничави технологии като AI в националната стратегия за сигурност.

Трета глава се фокусира върху количественото определяне на финансовите разходи, свързани с кибер риска в Гърция, изследвайки тяхното въздействие върху системния риск и предоставяйки емпирични доказателства за вземащите решения. Главата си поставя за цел да оцени средните разходи за киберинциденти, използвайки

надеждни финансови отчети, и да тества хипотезата, че кибер рисковете представляват измерима финансова опасност, но не са основен фактор за увеличаване на системния риск, въпреки значителната вероятност от големи щети при отделни събития. В тази глава са установени разпространението на типовете атаки, динамиката на нарушенията на данните и нарушенията на поверителността, секторното разпределение на инцидентите, установени са средните разходи по тип инцидент, потенциала за големи щети за големи корпорации, установени са средните разходи по сектор.

Глава 3 предоставя задълбочен емпиричен анализ на финансовите последици от кибер риска в Гърция. Тя подчертава сложността на измерването на тези разходи, идентифицира най-уязвимите сектори и типове атаки, и изследва взаимовръзката между кибер инцидентите, системния риск и икономическия растеж, като предоставя ценни данни за вземане на решения в областта на киберсигурността.

По отношение на **представителността на данните**, изложени в труда може да се отбележи, че са с необходимата представителност и актуалност. Цитирането и позоваването на първичните литературни и справочни източници е коректно.

В **техническо отношение** дисертацията е отлично оформена. Балансирана е като обем в трите си глави. Качествата на таблиците и фигурите е на много високо ниво. Документационният материал е коректно изведен и изчерпателен. Стилът и езикът на изложение са на нужното равнище за дисертационен труд.

Оценка на автореферата

В резултат на задълбоченото ми запознаване с автореферата и със съдържанието на дисертационния труд достигнах до заключението, че:

1. Авторефератът е разработен в съответствие с изискванията.
2. В съдържателно и структурно отношение авторефератът напълно съответства на дисертационния труд. Той коректно отразява основните моменти в дисертацията и дава ясна представа за постигнатото от Мария Куцари.

IV. Въпроси и препоръки по дисертационния труд

Внимателното ми запознаване с дисертационния труд ми дава основание да обобщя, че в него няма допуснати съществени пропуски, неточности или противоречия. Същевременно имам няколко **препоръки и уточняващи въпроси**, които могат да бъдат отправни точки за бъдеща работа на докторанта.

- Необходимо и важно е да бъде разгледана ролята на човешкия фактор чрез включването на поведенчески аспекти и анализ на „вътрешни заплахи“, което ще допринесе за по-пълно разбиране на рисковата среда, особено в публичния сектор.
- Допълнителен научен принос към разработката би била оценката на възвръщаемостта от инвестиции в киберсигурност (ROI): Добавянето на анализ на рентабилността на мерките за сигурност би помогнало на организациите да обосноват бъдещи ИТ бюджети.
- Интеграция на съвременни прогностични технологии: Препоръчвам да бъдат приложени алгоритми от машинното обучение (ML) за подобряване на точността на прогностичен модел.

С цел доуточняване формулирам следните **въпроси към дисертанта:**

1. Как оценява Мария Куцари надеждността и изчерпателността на източниците за киберинциденти, при условие че много често с цел съхраняване на корпоративен имидж липсва публичност по темата?
2. Какви конкретни нормативни или регулаторни препоръки би предложила на гръцкото правителство въз основа на резултатите от научното изследване?
3. Кои според Мария Куцари ще бъдат трите най-уязвими сектора в Гърция през следващите пет години и какви превантивни мерки бихте препоръчали за тях?

V. Обобщена оценка на дисертационния труд и заключение

Представеният дисертационният труд е цялостно и добросъвестно научно изследване на значим и актуален научен проблем. Изследователските задачи успешно са изпълнени, а поставените изследователски цели - реализирани. Постигнати са научно-приложни приноси, които обогатяват научното знание и подпомагат практиката. Дисертационният труд заслужава положителна оценка и отговаря на изискванията за присъждане на исканата научна степен.

Всичко това ми дава основание с пълна убеденост да препоръчам на уважаемите членове на Научното жури да присъдят на **Мария Стефанос Куцари** образователната и научната степен **“Доктор”** в професионално направление 3.8. Икономика, научна специалност „Финанси, парично обръщение, кредит и застраховка“.

Дата: 30.07.2025

Благоевград

Изготвил становището:

Доц. д-р Елена Велкова Ставрова

ЮГОЗАПАДЕН УНИВЕРСИТЕТ
·НЕОФИТ РИЛСКИ·
БЛАГОЕВГРАД

OPINION

From: Assoc. Prof. Dr. Elena V. Stavrova, South-West University "Neofit Rilski" - Blagoevgrad, Scientific Speciality "Finance, Money Circulation, Credit and Insurance", Professional Field 3.8. Economics.

Regarding: Dissertation Thesis on the topic: "The Financial Costs of Cyber Risk in the Business and Public Sector in Greece"

Grounds for submitting the opinion: Participation in the scientific jury for the defense of the dissertation thesis, in accordance with Order No. 1267 /10.06.2025 of Prof. Dr. Nikolay Marin, Rector of South-West University "Neofit Rilski" - Blagoevgrad.

Author of the Dissertation Thesis: Maria Stefanos Koutsari

I. General Presentation of the Dissertation Thesis

The dissertation thesis by Maria Stefanos Koutsari for the award of the educational and scientific degree "Doctor" consists of an introduction, three chapters, a conclusion, and a bibliography. It includes 153 pages of text, 22 tables, 30 figures, and a list of references containing 111 titles.

The topic of the dissertation is exceptionally relevant and significant in both international and national contexts. In the conditions of digitalization of the public and private sectors, the study of the financial dimensions of cyber risk in Greece contributes to a deeper understanding of the economic consequences of increasing cyber threats not only in a national but also in an international context. The research fills a significant gap in the literature, especially considering the scarce available empirical information for the region. At the same time, it is very complex and intricate, and its development requires good theoretical preparation, high analytical abilities, and experience in conducting scientific research.

The object of research in the dissertation is the financial impact of cyber risk on key industries in the private and public sectors of Greece. This includes real economic sectors that are particularly vulnerable to cyber threats due to their high degree of digitalization and critical importance for the national economy, such as: Energy; Communications; Healthcare; Retail; Banking and Finance; Digital Infrastructure; Government Services. It is worth noting that this choice is fully justified and is related to their significant economic weight in Greece's GDP, their varying degrees of preparedness and vulnerability to cyberattacks, and their critical importance for the functioning of the state as an entity.

The subject of the research is the quantitative measurement and analysis of financial costs caused by cyber incidents – including direct (e.g., fines, recovery activities), indirect (loss of reputation, customer trust), and lost profits. The developed toolkit for the financialization of the cyberattack problem is subordinated to the goal – evaluating the effects and possibilities for managing and forecasting damages by including in the research database: incident frequency in individual sectors, incident costs, the relationship between incidents and systemic risk, and the effects of incidents on the resilience and competitiveness of the economy.

The established requirement for a dissertation thesis has been met: the research thesis is precisely and clearly defined.

The main research approaches and methods are precisely presented, including theoretical generalization, comparative analysis, descriptive analysis, and original econometric methods such as incident rate calculation, logarithmic regression analysis to examine the relationships between financial costs and industry-specific factors, systemic risk analysis (using the debt-to-revenue ratio), and bivariate analysis (Pearson and Kendall's tau correlation tests).

The structure of the dissertation is logically constructed and subordinated to the comprehensive development of the research problem, to the achievement of seven research tasks and objectives. The text is enriched and successfully illustrated with tables and figures, which facilitate its easy comprehension and understanding of the essence of the research.

II. Assessment of the Form and Content of the Dissertation Thesis

The **First Chapter** of the dissertation introduces and defines the concept of cyber risk in the context of the growing development of information technologies and the widespread adoption of the Internet, emphasizing the origin and evolution of the Internet and cyberspace, the importance of cyberspace and ICT, the increasing number of cyber threats, cyber risk management, and the role of individuals in the face of cyberattack threats. Due attention is paid to Greece's National Strategy, structured around 5 main axes, 15 objectives, and over 50 actions. A summary of the main roles and actions of the private and public sectors in cybersecurity

governance is provided, including technical security, policies, awareness raising, audits, crisis plans, research and development, and support for citizens and SMEs. An original contribution of the doctoral student is the introduction of the concept of risk management and shared responsibility in the fight against cyber threats.

The **Second Chapter** describes the development and current state of cybersecurity strategies in Greece, with a special focus on digital financial services. In it, the doctoral student has analyzed the current state of the institutional framework for cybersecurity, presented by key institutions and legislative measures established in Greece to combat cyber threats. The role of these bodies in preventing, investigating, and improving the digital transformation of the public sector is highlighted. National and international initiatives in this area are analyzed. The significant progress of Greece in the field of cybersecurity is emphasized, with the country ranking 7th in the National Cybersecurity Index (NCSI) for the period 2016-2023, placing it among the leading positions globally. This achievement is due to the coordinated efforts of various Greek authorities. The Second Chapter provides a detailed overview of the comprehensive strategies and institutional measures for cybersecurity in Greece. It demonstrates the country's commitment to protecting critical infrastructure and citizens, while emphasizing the adaptation of the business and financial sectors to new threats and the inclusion of advanced technologies such as AI in the national security strategy.

The **Third Chapter** focuses on the quantitative determination of financial costs associated with cyber risk in Greece, examining their impact on systemic risk and providing empirical evidence for decision-makers. The chapter aims to estimate the average costs of cyber incidents using reliable financial reports and to test the hypothesis that cyber risks represent a measurable financial danger, but are not a primary factor in increasing systemic risk, despite the significant probability of large damages in individual events. In this chapter, the distribution of attack types, the dynamics of data breaches and privacy violations, the sectoral distribution of incidents, the average costs per incident type, the potential for large damages for large corporations, and the average costs per sector are established.

Chapter 3 provides an in-depth empirical analysis of the financial consequences of cyber risk in Greece. It highlights the complexity of measuring these costs, identifies the most vulnerable sectors and attack types, and examines the interrelationship between cyber incidents, systemic risk, and economic growth, providing valuable data for decision-making in the field of cybersecurity.

Regarding the representativeness of the data presented in the work, it can be noted that they possess the necessary representativeness and timeliness. The citation and referencing of primary literary and reference sources are correct.

In technical terms, the dissertation is excellently formatted. It is well-balanced in volume across its three chapters. The quality of the tables and figures is very high. The documentary material is correctly presented and comprehensive. The style and language of presentation are at the required level for a dissertation thesis.

III. Assessment of the Abstract

As a result of my thorough review of the abstract and the content of the dissertation thesis, I have concluded that:

1. The abstract has been prepared in accordance with the requirements.
2. In terms of content and structure, the abstract fully corresponds to the dissertation thesis. It correctly reflects the main points of the dissertation and provides a clear overview of Maria Koutsari's achievements.

IV. Questions and Recommendations for the Dissertation Thesis

My careful review of the dissertation thesis gives me reason to conclude that it contains no significant omissions, inaccuracies, or contradictions. At the same time, I have a few recommendations and clarifying questions that can serve as starting points for the doctoral student's future work.

- It is necessary and important to examine the role of the human factor by including behavioral aspects and an analysis of "insider threats," which will contribute to a more complete understanding of the risk environment, especially in the public sector.
- An additional scientific contribution to the work would be an assessment of the return on investment in cybersecurity (ROI): Adding an analysis of the profitability of security measures would help organizations justify future IT budgets.
- Integration of modern predictive technologies: I recommend applying machine learning (ML) algorithms to improve the accuracy of the predictive model.

For clarification, I formulate the following questions for the doctoral student:

1. How does Maria Koutsari assess the reliability and comprehensiveness of cyber incident sources, given that public disclosure on the topic is often lacking to preserve corporate image?
2. What specific legislative or regulatory recommendations would Maria Koutsari propose to the Greek government based on the results of the scientific research?

3. Which, according to Maria Koutsari, will be the three most vulnerable sectors in Greece over the next five years, and what preventive measures would you recommend for them?

V. Overall Assessment of the Dissertation Thesis and Conclusion

The presented dissertation thesis is a comprehensive and conscientious scientific study of a significant and current scientific problem. The research tasks have been successfully completed, and the set research objectives have been realized. Scientific and applied contributions have been achieved, which enrich scientific knowledge and support practice. The dissertation thesis deserves a positive evaluation and meets the requirements for the award of the requested scientific degree.

All of this gives me full confidence to recommend to the esteemed members of the Scientific Jury to award Maria Stefanos Koutsari the educational and scientific degree "Doctor" in professional field 3.8. Economics, scientific specialty "Finance, Money Circulation, Credit and Insurance."

Date: 30.07.2025 **Blagoevgrad**

Prepared the opinion: Assoc. Prof. Dr. Elena Velkova Stavrova