УНИВЕРСИТЕТ ЗА НАЦИОНАЛНО И СВЕТОВНО СТОПАНСТВО

Р Е Ц Е Н З И Я

От: *доцент доктор Георги Павлов; УНСС*
Научна специалност Икономика и управления(отбрана и сигурност)

Относно: дисертационен труд за присъждане на образователна и научна степен **„доктор“** по професионално направление 3.8. Икономика**,** научна специалност Икономика и управления(отбрана и сигурност) в УНСС.

Основание за представяне на рецензията: участие в състава на научното жури по защита на дисертационния труд съгласно Заповед № 3011/02.10.2025 на Заместник ректор по научноизследователската дейност на УНСС.

Автор на дисертационния труд: *Ивайло Христосков Илиев*
Тема на дисертационния труд: „Подобряване на киберсигурността в малкия и среден бизнес в България“

1. Информация за дисертанта

Дисертантът се е обучавал по докторска програма към катедра „Национална и регионална сигурност“ от факултет „Икономика на инфраструктурата“ на УНСС в професионално направление 3.8. Икономика, по научна специалност „Икономика и управление(отбрана и сигурност)“ съгласно Заповед на Ректора на УНСС №486/15.03.2019 г. Обучението е осъществено в свободна форма през периода 15.03.2019-26.02.2025 г.

Ивайло Илиев е изпълнил успешно своя индивидуален план на обучение и е отчислен със Заповед на ректора на УНСС №529/24.02.2025г. считано от 26.02.2025г. с право на защита до 26.02.2027 г.

Кандидатът е завършил средното си образование в 57-мо СОУ 2001г със специализация по Спортен мениджмънт и бакалавърска степен „Треньор по самбо“ в НСА през 2012.

Има завършени три магистратури в: НСА -„Спортен мениджмънт“, Стопанска Академия „Д.А. ЦЕНОВ“-СВИЩОВ -„Корпоративен мениджмънт“ и УНСС - „Национална сигурност“

Трудов стаж и управленски опит:

- От 2015г – до момента управител в Ринг Гейминг ЕООД - Организиране на хазартни игри;
- От 2007г до 2015г управител във Фламинго-78 ЕООД -Хазартна дейност;
- От 08.2005 до 09.2006г Въоръжена охрана в СИС ИНДУСТРИЙС ООД;
- От 04.2005 до 07.2005г Въоръжена охрана в ГОЛД ГРУП ЕООД
- От 2003 до 2005г Лична охрана в „Национална разузнавателна служба“ и
- От 2002 до 2003г Сержант в МВР.

2. Обща характеристика на представения дисертационен труд

Дисертационният труд е с обем от 222 стандартни страници и съдържа: списък със съкращенията, списък с графиките и таблиците, увод, изложение в три глави, заключение, списък с приносите, списък с използвана литература и приложения.

Малките и средни предприятия (МСП) в България са повече от 95% от всички икономически субекти. Дигитализацията на бизнеса се считаше за сила и преди пандемията от Covid-19, но ограниченията, породени от нея пренесоха по-голямата част от живота, и личен, и служебен в онлайн-пространството.

Това, в съчетание с недостатъчната подготвеност за работа с Интернет, както на потребителите (физически и юридически лица), така и на институциите в България, води до значително увеличаване на киберпрестъпността. Профилите в социалните мрежи и корпоративният уебсайт се ползват като основни инструменти за комуникация. Всичко

това обаче изисква и целенасочени действия във връзка с ограничаването на вредните влияния на киберпрестъпленията.

Актуалността на изследванията в дисертационния труд не буди съмнение.

Изследванията в работата са съсредоточени върху повишаване на осведомеността и постигане на по висока ефективност в киберсигурността.

Добре е подбрана **основната теза**, която ще се защитава, че в България, повече отколкото в по-добре развитите западноевропейски икономики, киберсигурността на малкия и среден бизнес е проблем, който изисква незабавни координирани действия от страна на институции, предприятия и потребители.

Целта е да се очертаят ясно измеренията на проблемите на киберсигурността на малкия и среден бизнес у нас заедно с техните взаимовръзки с институциите и клиентите и да се дадат препоръки за подобряването на ситуацията за българските компании.

Правилно са формулирани 5 задачи пряко свързани с целта.

Като **обект** на изследване в труда, се определят конкретните проблеми на киберсигурността, с които се сблъскват МСП в България.

Предметът е насочен главно към превенцията, прилагаща се в МСП у нас.

Библиографията се състои от 198 литературни източника (9 от тях на кирилица), като се използва както специализирана литература по темата, така и статистически данни от НСИ, Евростат, институционална статистика и изявления, онлайн и офлайн публикации на експерти по темата.

Поставените ограничения са свързани с териториалния обхват и големината на бизнеса. Изследването е базирано и фокусирано на държавните територии на Република България и е ограничено и до МСП и специфичния български контекст.

В дисертацията са използвани следните методи: анализ на литературни и информационни източници, проучване на чуждия опит, качествен анализ на риска, сравнителен анализ, казусен анализ и емпирично изследване и проучване на нагласите и разбиранията по отношение на киберпрестъпността и киберсигурността от страна на потребителите и на собствениците и ръководителите на малък и среден

бизнес. Авторът показва добра осведоменост и разбиране при изследванията и анализите.

В **първа** глава се разглеждат в детайли проблемите на киберсигурността в България. Очертани са същността и измеренията на киберсигурността, както и взаимоотношенията между отделните заинтересовани страни. Направен е преглед на статистиката за киберпрестъпленията и тяхната разкриваемост, както на институционално ниво, така и по данните от професионалистите в областта от частния сектор. Сравнителният анализ между двете позволява да се види по-лесно реалната картина на киберпрестъпността и киберсигурността в България. Направен е и общ преглед на дигитализацията в МСП у нас.

Представен е и основният понятиен апарат на разработката, привеждат се статистически данни за измеренията на МСП. Проследява се степента, в която те са дигитализирани, какви са факторите за това да се случи и взаимовръзката им с киберпрестъпленията и киберсигурността;

Втора глава обръща внимание конкретно на методите за повишаване киберсигурността на малкия и среден бизнес. Тук са описани по-добре най-често срещаните начини за кражба на чувствителна информация, като специално внимание се обръща на фишинг-атаките, тъй като те са несъмнено един от най-големите бичове за съвременния малък и среден бизнес в България, но и причина за сериозни сблъсъци с институции, особено поради факта, че в крайна сметка при тях потърпевшият доброволно предоставя информацията, подлъган от престъпниците. В тази част от разработката се обръща внимание и на реакциите на институциите, включително и банките, и механизмите на частния и държавен сектор за подобряване на киберсигурността и ограничаване на последиците за малкия и среден бизнес тогава, когато атаката вече е факт. *Първият* етап от методиката е свързан с идентифицирането и изследването на различните видове рискове за малкия и среден бизнес в контекста на киберсигурността и пряката връзка с дигитализацията. Анализът на риска се откроява като съвкупност от управленски практики както на ниво организация, така и на ниво законодател и институции. Динамиките, свързани с гарантирането на киберсигурността в МСП са значителни и изискват внимание както от страна на държавата, така и от страна на мениджмънта и служителите в компаниите. На *втория* етап се анализира нормативната база, тъй като

нормативните актове следва да се развиват в съответствие с технологичното развитие. Това в известен смисъл е препоръка към законодателят като възможност за институционални реакции и автономни решения. *Третият* етап от методиката е за борбата с пробойните в киберсигурността на МСП. *Четвъртият*, последен етап, са конкретните действия, които различните заинтересовани страни могат да предприемат за повишаване киберсигурността на малкия и среден бизнес.

В **трета** глава е представено емпирично изследване на нагласите и разбиранията по отношение на киберпрестъпността и киберсигурността от страна на потребителите и на собствениците и ръководителите на МСП.

Изследването и коментара на резултатите от него представляват апробация на изложената във втора глава методика.

Заключението обобщава всички изводи, направени в трите глави на разработката

3. Оценка на получените научни и научно-приложни резултати

МСП, подобно на по-големите организации, боравят с чувствителни данни и са изправени пред значителни финансови и репутационни рискове в случай на нарушение на сигурността на данните. За тях е от решаващо значение да признаят значението на киберсигурността и проактивно да инвестират в защитата на своите цифрови активи.

Съществува често срещано погрешно схващане, че МСП не са доходоносни цели за кибератаки. Киберпрестъпниците обаче гледат на представителите на сегмента като на лесни мишени поради техните потенциално ограничени мерки за сигурност и ресурси. Малките бизнеси все по-често се сблъскват с целенасочени атаки, насочени към кражба на ценни данни, прекъсване на операциите или изнудване за плащане на откуп. В последните години преобладават атаките при които нападателите криптират критични данни и изискват плащане, за да възстановят достъпа.

Нарушенията на киберсигурността, засягащи МСП в мащаб, могат да имат катастрофални последици за обществото -60% от МСП, претърпели кибератака, не се възстановяват и затварят в рамките на шест месеца. Ето защо е ключово лидерите да подготвят бизнеса си да бъде по-силен в лицето на предизвикателствата, които в крайна сметка могат да бъдат избегнати. Работата предлага решения, които могат да се приложат в практиката.

Изключително полезна в тази насока е разработената методика за повишаване на киберсигурността в малкия и среден бизнес в България.

Емпиричното изследване е показателно за нагласите по отношение на киберсигурността в МСП.

4. Оценка на научните и научно-приложни приноси

Приносите съответстват на постигнатото в дисертацията. Приемам ги като дело на автора.

Освен теоретичното обогатяване на понятието „Киберсигурност“ се представя методика и план за реализация на киберсигурността в МСП.

Чрез проведеното оригинално емпирично изследване за сравняване нагласите и разбиранията на потребителите на услуги от МСП и собственици/мениджъри на МСП.

Резултатите са основата за препоръките, адресирани към: -МСП; -Държавните институции; -Банки и финансови институции и -Потребители, чрез поведенчески модели за по-безопасно онлайн пазаруване

Не е забелязано плагиатство в дисертационния труд.

5. Оценка на публикациите по дисертацията

Представени са четири авторски публикации, като три са в KNOWLEDGE – International Journal:

- Информационната война и усъвършенстване дейността на специалните служби в република България
- Предизвикателства пред киберсигурността и международното публично право
- Аспекти на устойчивостта на България като гаранция за националната сигурност.

Това списание е достъпно онлайн.

Четвъртата публикация е в списанието, издавано в УНСС от факултет „Икономика на инфраструктурата“

Това е достатъчна гаранция за разпространение на получените резултати.

6. Оценка на автореферата

Представеният автореферат е разработен съгласно изискванията и достатъчно пълно и точно отразява направените изследвания.

Структурата му отговаря на съдържанието на дисертацията.

Отразени са основните моменти и приносите от разработената дисертация.

7. Критични бележки, препоръки и въпроси

Тъй като бях рецензент и на обсъждането в катедрата, където имах доста критични бележки, сега констатирам, че те са отразени в дисертационният труд и той е завършено научно изследване с формулирана проблематика, избрани методи и средства за изследване, извършено емпирично изследване и предложена методика за използване в практиката на МСП.

Като препоръка към докторанта мога да отбележа, че е добре да се публикуват резултати в специализираните международни научни издания, с цел запознаване на общността с направените изследвания и получените резултати.

С оглед на използването на резултатите е препоръчително да се публикува и монография, която да бъде използвана в работата на МСП.

8. Заключение

Дисертационният труд отговаря на нормативните изисквания на Закона за развитие на академичния състав в Република България и Правилника за неговото прилагане, както и на Правилника за учебната дейност на Университета за национално и световно стопанство (част 3 „Доктор“).

Дисертационният труд има висока теоретико-методологична и научно-приложна стойност. Разработен е в съответствие с критериите и изискванията, отнасящи се за труд от подобен характер. Авторът е извършил успешно изследване с ясни резултати.

Давам своята положителна оценка за разработения дисертационен труд и предлагам на уважаемото научно жури да присъди на *Ивайло Христосков Илиев* образователната и научна степен „доктор” в професионално направление *3.8 Икономика, научна специалност „Икономика и управление (Отбрана и сигурност)“.*

05.11.2025 / София Подпис: ……

R E V I E W

By: Associate Professor Doctor Georgi Pavlov; UNWE
Scientific specialty Economics and Management (Defense and Security)

Regarding: dissertation for awarding the educational and scientific degree "Doctor" in professional field 3.8. Economics, scientific specialty Economics and Management (Defense and Security) at UNWE.

Reason for submitting the review: participation in the scientific jury for the defense of the dissertation work according to Order No. 3011/02.10.2025 of the Vice-Rector for Research of UNWE.

Author of the dissertation: Ivaylo Hristoskov Iliev
Topic of the dissertation: "Improving cybersecurity in small and medium-sized businesses in Bulgaria"

1. Information about the dissertation candidate

The dissertation candidate studied under the doctoral program at the Department of "National and Regional Security" of the Faculty of "Infrastructure Economics" of the UNWE in the professional field 3.8. Economics, in the scientific specialty "Economics and Management (Defense and Security)" according to the Order of the Rector of the UNWE No. 486/15.03.2019. The training was carried out in a free form during the period 15.03.2019-26.02.2025.

Ivaylo Iliev has successfully completed his individual training plan and was discharged by Order of the Rector of the UNWE No. 529/24.02.2025. as of 26.02.2025 with the right to defend until 26.02.2027

The candidate completed his secondary education at the 57th Secondary School in 2001 with a specialization in Sports Management and a bachelor's degree in "Sambo Coach" at the National Academy of Sports in 2012.

He has completed three master's degrees at: National Academy of Sports - "Sports Management", Economic Academy "D.A. Tsenov"-Svishtov - "Corporate Management" and UNWE - "National Security"

Work experience and management experience:

• From 2015 - to the present, manager at Ring Gaming EOOD - Organization of gambling games

• From 2007 to 2015, manager at Flamingo-78 EOOD - Gambling activities

• From 08.2005 to 09.2006, armed security at SIS INDUSTRIES EOOD

• From 04.2005 to 07.2005, armed security at GOLD GROUP EOOD

• From 2003 to 2005, personal security at the NATIONAL INTELLIGENCE SERVICE

• From 2002 to 2003, Sergeant at the Ministry of Internal Affairs

2. General characteristics of the presented dissertation work

The dissertation has a volume of 222 standard pages and contains: a list of abbreviations, list of graphs and tables, introduction, three-chapter exposition, conclusion, list of contributions, list of used literature and appendices.

Small and medium-sized enterprises (SMEs) in Bulgaria are more than 95% of all economic entities. The digitalization of business was considered a force even before the Covid-19 pandemic, but the restrictions it caused have transferred most of life, both personal and professional, to the online space.

This, combined with the insufficient preparedness of both users (individuals and legal entities) on the Internet and institutions in Bulgaria, leads to a significant increase in cybercrime. Profiles in social networks and the corporate website are used as the main tools for communication. However, all this also requires targeted actions in relation to limiting the harmful effects of cybercrime. The relevance of the research in the dissertation is beyond doubt. The research in the work is focused on raising awareness and achieving higher efficiency in cybersecurity.

The main thesis that will be defended is well chosen, that in Bulgaria, more than in the better developed Western European economies, the cybersecurity of small and medium-sized businesses is a problem that requires immediate coordinated action by institutions, enterprises and consumers.

The goal is to clearly outline the dimensions of the cybersecurity problems of small and medium-sized businesses in our country, along with their interrelationships with institutions and customers, and to provide recommendations for improving the situation for Bulgarian companies.

5 tasks directly related to the goal are correctly formulated.

As an object of research in the work, the specific cybersecurity problems faced by SMEs in Bulgaria are determined.

The subject is mainly focused on prevention applied in SMEs in our country.

The bibliography consists of 198 literary sources (9 of them in Cyrillic), using both specialized literature on the topic, as well as statistical data from the National Statistical Institute, Eurostat, institutional statistics and statements, online and offline publications of experts on the topic.

The limitations are related to the territorial scope and size of the business. The study is based and focused on the state territories of the Republic of Bulgaria and is also limited to SMEs and the specific Bulgarian context.

The following methods were used in the dissertation: analysis of literary and information sources, study of foreign experience, qualitative risk analysis, comparative analysis, case analysis and empirical research and study of attitudes and understandings regarding cybercrime and cybersecurity by consumers and owners and managers of small and medium-sized businesses. The author shows good awareness and understanding in the research and analysis.

The **first** chapter examines in detail the problems of cybersecurity in Bulgaria. The essence and dimensions of cybersecurity are outlined, as well as the relationships between individual stakeholders. A review of cybercrime statistics and their detection rates is made, both at the institutional level and based on data from professionals in the field from the private sector. The

comparative analysis between the two allows for a more accurate picture of cybercrime and cybersecurity in Bulgaria. A general overview of digitalization in SMEs in our country is also made.

The main conceptual framework of the development is also presented, statistical data on the dimensions of SMEs are provided. The extent to which they are digitalized is tracked, what are the factors for this to happen and their relationship with cybercrime and cybersecurity;

The **second** chapter pays specific attention to methods for increasing the cybersecurity of small and medium-sized businesses. The most common ways of stealing sensitive information are better described here, with special attention paid to phishing attacks, as they are undoubtedly one of the biggest scourges for modern small and medium-sized businesses in Bulgaria, but also a cause for serious clashes with institutions, especially due to the fact that in the end, the victim voluntarily provides the information, deceived by the criminals. This part of the study also focuses on the reactions of institutions, including banks, and the mechanisms of the private and public sectors to improve cybersecurity and limit the consequences for small and medium-sized businesses when the attack has already occurred. The *first stage* of the methodology is related to the identification and study of the various types of risks for small and medium-sized businesses in the context of cybersecurity and the direct connection with digitalization. Risk analysis stands out as a set of management practices both at the organizational level and at the level of legislators and institutions. The dynamics related to ensuring cybersecurity in SMEs are significant and require attention from both the state and the management and employees in companies. The *second stage* analyzes the regulatory framework, since regulatory acts should develop in accordance with technological development. This is, in a sense, a recommendation to the legislator as an opportunity for institutional reactions and autonomous solutions. The *third* stage of the methodology is about combating breaches in the cybersecurity of SMEs. The *fourth* and final stage is the specific actions that various stakeholders can take to improve the cybersecurity of small and medium-sized businesses.

Chapter **three** presents an empirical study of the attitudes and understandings of consumers and SME owners and managers regarding cybercrime and cybersecurity.

The study and the commentary on its results constitute an approbation of the methodology presented in chapter two.

The conclusion summarizes all the conclusions drawn in the three chapters of the study.

3. Evaluation of the obtained scientific and applied scientific results

SMEs, like larger organizations, handle sensitive data and face significant financial and reputational risks in the event of a data breach. It is crucial for them to recognize the importance of cybersecurity and proactively invest in protecting their digital assets.

There is a common misconception that SMEs are not profitable targets for cyberattacks. However, cybercriminals view the segment as easy targets due to their potentially limited security measures and resources. Small businesses are increasingly facing targeted attacks aimed at stealing valuable data, disrupting operations or extorting ransom payments. In recent years, attacks have predominated in which attackers encrypt critical data and demand payment to restore access.

Cybersecurity breaches affecting SMEs on a large scale can have catastrophic consequences for society - 60% of SMEs that have suffered a cyberattack do not recover and close within six months. That is why it is crucial for leaders to prepare their businesses to be stronger in the face of challenges that can ultimately be avoided. The work offers solutions that can be implemented in practice.

The developed methodology for increasing cybersecurity in small and medium-sized businesses in Bulgaria is extremely useful in this regard.

The empirical study is indicative of the attitudes towards cybersecurity in SMEs.

4. Assessment of scientific and applied scientific contributions

The contributions correspond to what has been achieved in the dissertation. I accept them as the work of the author.

In addition to the theoretical enrichment of the concept of "Cybersecurity", a methodology and a plan for the implementation of cybersecurity in SMEs are presented.

Through the conducted original empirical study to compare the attitudes and understandings of users of SME services and SME owners/managers.

The results are the basis for recommendations addressed to: -SMEs; -State institutions; -Banks and financial institutions and -Consumers, through behavioral models for safer online shopping

No plagiarism was noticed in the dissertation work.

5. Evaluation of the dissertation publications

Four author publications are presented, three of which are in KNOWLEDGE – International Journal:

- Information warfare and improving the activities of special services in the Republic of Bulgaria
- Challenges to cybersecurity and international public law
- Aspects of the sustainability of Bulgaria as a guarantee of national security. This journal is available online.

The fourth publication is in the journal published at the UNWE by the Faculty of Infrastructure Economics

This is a sufficient guarantee for the dissemination of the results obtained.

6. Evaluation of the abstract

The presented abstract is developed in accordance with the requirements and sufficiently fully and accurately reflects the research carried out.

Its structure corresponds to the content of the dissertation.

The main points and contributions of the developed dissertation are reflected.

7. Critical notes, recommendations and questions

Since I was also a reviewer of the discussion in the department, where I had quite a few critical remarks, I now find that they are reflected in the dissertation work and it is a completed scientific study with a formulated problem, selected methods and means of research, conducted empirical research and proposed methodology for use in the practice of SMEs.

As a recommendation to the doctoral student, I can note that it is good to publish results in specialized international scientific publications, in order to familiarize the community with the research carried out and the results obtained.

In view of the use of the results, it is advisable to publish a monograph to be used in the work of SMEs.

8. Conclusion

The dissertation meets the regulatory requirements of the Act on the Development of Academic Staff in the Republic of Bulgaria and the Regulations for its implementation, as well as the Regulations for the Educational Activity of the University of National and World Economy (Part 3 "Doctor").

The dissertation has a high theoretical-methodological and scientific-applied value. It has been developed in accordance with the criteria and requirements applicable to work of a similar nature. The author has successfully conducted research with clear results.

I give my positive assessment of the developed dissertation and propose to the esteemed scientific jury to award Ivaylo Hristoskov Iliev the educational and scientific degree "Doctor" in the professional field 3.8 Economics, scientific specialty "Economics and Management (Defense and Security)".

05.11.2025 / Sofia Signature: ……