УНИВЕРСИТЕТ ЗА НАЦИОНАЛНО И СВЕТОВНО СТОПАНСТВО

С Т А Н О В И Щ Е

От: *Доцент доктор Недко Георгиев Тагарев;*
Университет за национално и световно стопанство;
научна специалност 3.8. Икономика

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

Автор на дисертационния труд: *Ивайло Христосков Илиев*
Тема на дисертационния труд: *ПОДОБРЯВАНЕ НА КИБЕРСИГУРНОСТТА В МАЛКИЯ И СРЕДЕН БИЗНЕС В БЪЛГАРИЯ*

Основание за представяне на становището: участие в състава на научното жури по защита на дисертационния труд съгласно Заповед №3011/02.10.2025 на Ректора на УНСС.

1. Информация за дисертанта

Дисертантът се е обучавал по докторска програма към *Катедра „Национална и регионална сигурност“/факултет „Икономика на инфраструктурата“* на УНСС по *научна специалност 3.8. Икономика* съгласно Заповед на Зам.-ректора по НИД на УНСС №486/15.03.2019 Обучението е осъществено в *свободна* форма през периода 26.02.2019 – 26.02.2025

2. Обща характеристика на представения дисертационен труд

Структура, обем. Кратка оценка за: актуалност на темата; цел; задачи; обект; предмет; основна теза; използвана научна литература.

Структура и обем на дисертационния труд

Дисертационният труд се състои от три основни глави, предшествани от увод и последвани от заключение, библиография и приложения. Обемът е значителен и обхваща 221 стр.

Уводът представя актуалността, обекта, предмета, целите и задачите на

изследването. Първа глава разглежда теоретичните аспекти на киберсигурността, факторите за нейното значение в България, както и мястото на МСП в икономиката. Втора глава предлага методика за повишаване на киберсигурността в МСП, включително управление на риска, законодателни и институционални мерки. Трета глава представя емпирично изследване на нагласите на потребители и бизнеси, както и анализ на резултатите. Заключението обобщава изводите и препоръките. Библиография и приложения включват използваните източници(199 бр.) и допълнителни материали.

Актуалност на темата

Темата е изключително актуална и значима в контекста на нарастващата дигитализация и киберзаплахи в България и глобално. МСП са особено уязвими поради липса на ресурси и експертиза, което ги прави честа мишена на кибератаки. Пандемията от COVID-19 само засили тази необходимост от фокус върху киберсигурността.

Цел

Основната цел на дисертацията е да се анализират проблемите на киберсигурността в българските МСП, да се идентифицират взаимовръзките с институции и потребители, и да се предложат конкретни мерки за подобряване на ситуацията.

Задачи

- Изграждане на теоретичен контекст за МСП и киберсигурността.
- Анализ на факторите за развитие на киберпрестъпността.
- Разглеждане на механизмите за противодействие на национално и европейско ниво.
- Проучване на нагласите на потребители и бизнеси.
- Даване на препоръки за подобряване на бизнес климата и сигурността.

Обект

Конкретните проблеми на киберсигурността, с които се сблъскват малките и средни предприятия в България.

Предмет

Повишаването на киберсигурността и превенцията в МСП чрез методики, законодателни и институционални мерки, както и чрез повишаване на осведомеността.

Основна теза

В България киберсигурността на МСП изисква незабавни и координирани действия от страна на държавни институции, бизнеси и потребители. Липсата на такива действия влошава бизнес климата и

доверието между компании и клиенти.

Използвана научна литература

Авторът използва богата и разнообразна литература на български и английски език, включително:

- Специализирани трудове по киберсигурност и икономика;
- Доклади на международни организации (ЕС, Световна банка, ОИСР);
- Национални статистически данни (НСИ, Евростат);
- Академични статии и проучвания;
- Правни и нормативни източници.

Това гарантира солидна теоретична и емпирична основа на изследването.

3. Оценка на получените научни и научно-приложни резултати

Акцентира се върху: постигнатите основни научни и/или научно-приложни резултати; използваната методология; изпълнението на поставените цел и задачи.

Дисертационният труд на Ивайло Илиев постига серия от значими научни и научно-приложни резултати, които допринасят както за теорията, така и за практиката в областта на киберсигурността за малки и средни предприятия (МСП) в България.

На първо място - теоретично обогатяване на понятието „киберсигурност“. Авторът предлага комплексна, интердисциплинарна дефиниция на киберсигурността, която надхвърля чисто техническия подход. Тя се разглежда като организация на ресурси, процеси и структури за защита на киберпространството от събития, които не съвпадат с правата на собственост. Този подход интегрира правни, икономически, социални и технически аспекти, което го прави ценен теоретичен принос.

На второ място се дентифицират специфичните рискове и уязвимости на българските МСП. Чрез анализа са систематизирани и категоризирани ключовите заплахи за МСП (напр. ransomware, фишинг, злонамерен софтуер), като е акцентирано върху факторите, които ги правят особено уязвими - ограничени финансови и човешки ресурси, ниска дигитална култура и липса на специализиран персонал.

На трето място разработване на цялостна четириетапна методика за повишаване на киберсигурността. Това е основен научно-приложен резултат. Методиката обхваща:

Етап 1: Идентифициране и оценка на риска (финансов, пазарен, сигурностен).

Етап 2: Законодателни инициативи на национално и ЕС ниво.

Етап 3: Институционални реакции и механизми за реагиране при инциденти.

Етап 4: Конкретни действия за всички заинтересовани страни (МСП, банки, институции, клиенти).

Тази структурирана рамка предлага ясен и приложим път за предприемаче на действия.

Проведено е оригинално емпирично изследване, което сравнява нагласите и разбиранията на два ключови сегмента. На първо място потребителите на услуги на МСП и на втора собственици/мениджъри на МСП. Резултатите показват нивото на осведоменост, предразсъдъци и очаквания от двете страни, което е ценна информация за разработването на целеви политики и кампании.

Направени са конкретни препоръки за всички заинтересовани страни. На базата на целия анализ дисертацията предлага много конкретни, практико-ориентирани препоръки, адресирани към:

- МСП, чрез въвеждане на многофакторно удостоверяване, обучение на персонала, криптиране на данни, разработване на планове за реагиране.
- Държавни институции, чрез хармонизиране на законодателството, подобряване на институционалното сътрудничество, насърчаване на публични кампании за повишаване на осведомеността.
- Банки и финансови институции, чрез подобряване на сигурността на транзакциите и комуникацията с клиенти.
- Потребители, чрез поведенчески модели за по-безопасно онлайн пазаруване.

По отноиение на използнваната методология авторът прилага комплексен и многостранен методологичен подход, което гарантира задълбоченост и достоверност на изследването. На първо място теоретичен и дескриптивен анализ. Той се използва за изграждането на понятийния апарат в Глава 1. Включва анализ на научна литература, правни рамки (национални и в ЕС), официални доклади и статистически данни от източници като НСИ, Евростат, ENISA и др.

Сравнителен анализ, който е приложен при съпоставянето на дефинициите за МСП в различни контексти (ЕС, Световна банка, САЩ), както и при анализа на нивото на дигитализация на България в сравнение с други държави-членки на ЕС (например чрез индекса DESI).

Качествен анализ на риска, който се прилага във Втора глава за идентифициране и категоризиране на финансови, пазарни и сигурностни рискове, свързани с дигитализацията и киберзаплахите за МСП.

В Трета глава е проведено качествено и/или количествено проучване

(от характера на въпросите в анкетата се предполага наличието на количествен компонент) сред две фокусни групи - потребители и собственици/мениджъри на МСП. Това позволява проверка на теоретичните хипотези и получаване на актуална информация за нагласите на практиците.

Приложен е и казусен анализ, като се анализират българските МСП като цяло и в частност на стопанската структура на София служи за детайлен казусен анализ, илюстриращ общите тенденции и проблеми.

Комбинацията от тези методи позволява, както широта на обхвата, така и дълбочина на анализа.

По отношение на изпълнението на поставените цели и задачи, дисертационният труд успешно изпълнява поставените в увода цели и задачи.

Целта – да се очертаят проблемите на киберсигурността на МСП и да се дадат препоръки – е напълно постигната. Направен е всестранен анализ и накрая са формулирани ясни, практически насоки за действие.

Задача 1 (Изграждане на теоретичен контекст) е изпълнена изчерпателно в Глава 1 и Глава 3, където е представена подробна характеристика на МСП в България и тяхната роля в икономиката.

Задача 2 (Очертаване на факторите за киберпрестъпност) е изпълнена в подглавия 2.1, 2.2 и 2.3, където се анализират дигитализацията, финансовите проблеми и човешкият фактор като предпоставки за растеж на киберпрестъпленията.

Задача 3 (Разглеждане на механизмите за противодействие) е напълно покрита във Втора глава, целият фокус на която е именно върху методиките, законодателните и институционалните механизми за борба с киберпрестъпността.

Задача 4 (Очертаване на възможни решения и добри практики) е реализирана в заключителната част на Втора глава (конкретни действия) и в Глава 4 (възможни пътища за подобрение и добри практики).

Задача 5 (Изследване на нагласите) е успешно изпълнена в Трета глава посредством емпиричното проучване.

Задача 6 (Даване на препоръки за бизнес климата) е изпълнена в заключението и в различни части на труда, където препоръките са насочени именно към подобряване на общата бизнес среда чрез повишаване на киберсигурността.

Дисертационният труд представлява сериозно, добре структурирано и аргументирано изследване. Той не само констатира проблемите на киберсигурността в българските МСП, но и предлага цялостна, многостепенна и практична методика за тяхното решаване, което го прави ценен принос както за академичната общност, така и за бизнес-практиците и законодателите.

4. Оценка на научните и научно-приложни приноси

- *Кратка оценка за приносите, посочени от дисертанта*
- *Акцентира се върху основните научни и/или научно-приложни приноси в дисертационния труд.*

Приносите на дисертационния труд са ясно формулирани и демонстрират както теоретична, така и практическа стойност:

- Теоретичен принос – Разширяване на понятието „киберсигурност“ чрез интердисциплинарна дефиниция, която интегрира правни, икономически, социални и технически аспекти. Това надхвърля традиционния технически подход и спомага за по-цялостно разбиране на проблема.
- Идентифициране на рискове – Систематизиране на ключовите заплахи за българските МСП (напр. ransomware, фишинг) и факторите, които ги правят уязвими – ограничени ресурси, ниска дигитална култура, липса на експертиза.
- Методика за повишаване на киберсигурността – Разработената четириетапна рамка (оценка на риска, законодателни инициативи, институционални реакции и превантивни мерки) предлага ясен и приложим път за действие.
- Емпирично изследване – Сравнителният анализ на нагласите на потребители и бизнеси предоставя ценни данни за осведомеността и очакванията на двете групи, което може да се използва за целеви политики.
- Практически препоръки – Конкретни насоки за МСП, институции, банки и потребители, които са директно приложими и могат да допринесат за повишаване на киберсигурността в България.

Приносите са добре обосновани и отразяват задълбочен анализ на проблема, което ги прави ценни както за академичната общност, така и за бизнес-практиците и регулаторните органи.

5. Оценка на публикациите по дисертацията

Представените четири научни публикации на докторант Ивайло Илиев демонстрират впечатляваща широта на научните интереси и сериозен подход към изследването на критични аспекти на съвременната национална сигурност. Публикациите не само отразяват резултатите от дисертационния труд, но и залагат здрава основа за неговата защита, показвайки способността на автора да се ангажира със сложни и актуални проблеми в областта.

Публикациите имат висока научна стойност, която се проявява в няколко направления. На първо място, те покриват ключови аспекти от съвременната концепция за национална сигурност – от киберсигурност и информационна война през устойчиво развитие до организационното усъвършенстване на специалните служби. Това демонстрира способност за

комплексно мислене и разбиране на взаимовръзките между различни измерения на сигурността. Във всяка от публикациите се усеща дълбоко разбиране на спецификите на българския контекст, съчетан с ясно осъзнаване на европейските и международните измерения на разглежданите проблеми.

От методологична гледна точка публикациите показват развита способност за работа с разнородни източници и методи на изследване. Авторът умело комбинира правен анализ в публикацията за киберсигурността със статистически методи и анализ на публични политики в текста за устойчивото развитие. Особено впечатляващ е критичният анализ на организационните проблеми в системата на специалните служби, който разкрива дълбоко разбиране на оперативните и управленски аспекти на сигурността.

Всички публикации засягат изключително актуални теми, които са в центъра на вниманието както на академичните среди, така и на практиците в областта на сигурността. Анализът на последиците от пандемията COVID-19 върху европейската сигурност, както и разглеждането на информационната война като съвременно предизвикателство, показват добра ориентация в текущите тенденции и способност за своевременни научни отговори на възникващи предизвикателства.

Публикациите не просто допълват дисертационния труд, а по същество представляват неговите основни стълбове. Те демонстрират развитието на последователна и логична изследователска програма, в която различни аспекти на националната сигурност се разглеждат системно и взаимосвързано. Способността на автора да се движи уверено между теоретичния анализ и практическите препоръки е доказателство за зрелостта на изследването.

Въпреки впечатляващите качества, има възможности за допълнително усъвършенстване. В някои от публикациите може да се открие известна неравномерност в дълбочината на анализа, като отделни раздели са по-повърхностни в сравнение с други. Също така, по-широкото включване на сравнителен анализ с опита на други държави от ЕС и НАТО би обогатило значително изводите и препоръките.

Като цяло, научните публикации на докторант Ивайло Илиев представляват солиден научен принос в изследването на националната сигурност на България в съвременния контекст. Те свидетелстват за неговата способност да провежда самостоятелно научно изследване, да анализира комплексни проблеми и да формулира адекватни решения. Публикациите напълно отговарят на изискванията за дисертационен труд и предоставят достатъчно доказателства за научната и професионална компетентност на автора.

6. Оценка на автореферата

Авторефератът на дисертационния труд на г-н Ивайло Илиев на тема „Подобряване на киберсигурността в малкия и среден бизнес в България“ представлява всеобхватно, добре структурирано и академично строго изложение на изследване с висока научна и приложна стойност. Документът напълно отговаря на изискванията за този вид публикации и убедително демонстрира необходимостта от проучването, неговата методологична обосновка и очакваните приноси.

Избраната тема е изключително актуална и от стратегическо значение за България. Авторът умело подчертава критичната роля на МСП за българската икономика (над 95% от всички предприятия) и парадокса между тяхната жизненоважност и техната уязвимост в киберпространството. Контекстът на ускорената дигитализация, подсилена от пандемията от COVID-19, и недостатъчната институционална и потребителска култура в България са представени като ключови предпоставки за изследването. Темата не е само локално значима, но се вписва и в по-широките европейски и глобални дискусии за киберсигурността на малкия бизнес.

Авторефератът следва класическа и ясна структура: увод, обща характеристика, цели и задачи, методология, очаквани приноси. Логиката на изследването е последователна: от теоретично осмисляне на понятието „киберсигурност“ и идентифициране на проблемите в българския контекст, през разработване на методика за решение, до нейната апробация чрез емпирично изследване и формулиране на препоръки. Този подход гарантира цялостност и покритие на всички аспекти на изследователския проблем.

Използваната методология е комплексна и включва както качествени (анализ на литературата, сравнителен и казусен анализ), така и количествени (емпирично проучване) методи. Комбинацията от теоретично изследване и практическо проучване на нагласите на бизнеси и потребители допринася за по-дълбоко и нюансирано разбиране на проблема. Емпиричната част, макар и с ограничен обем извадка, предоставя ценни качествени инсайти за различията и приликите в представите на двете ключови групи.

Авторефератът предлага изчерпателно резюме на дисертацията. Той навлязва в достатъчни детайли, за да информира читателя за основните аргументи и заключения, без да става прекалено технически или тромав. Езикът е научно строг, но достъпен. Единствена забележка би била, че в някои раздели, особено в теоретичната част, има известна повтаряемост и претоварваност с детайли, които могат да бъдат допълнително компресирани за още по-голяма яснота.

Като цяло, авторефератът е отлично изготвен документ, който убедително представя значимостта, подхода и приносите на дисертационния

труд. Той не само информира, но и генерира интерес към пълния текст на изследването. Демонстрира сериозен научен принос и ясна насоченост към решаване на реален и належащ социално-икономически проблем.

7. Критични бележки, препоръки и въпроси

Критични бележки

- Не е изработен визуално методически модел.

Препоръки

- Добре е да се използват бовече визуални и организационни елементи – таблици, графики и фигури в теоретичната и методическата част, които ще подпомогнат възприемането на информацията.

Въпроси

1) На какво основание смятате, че законодателните инициативи (Етап 2) са ефективен елемент от вашата методика в конкретния български контекст и не би било по-реалистично този етап да бъде заменен или значително модифициран, за да се фокусира върху налагане и прилагане на съществуващите закони, вместо върху създаването на нови?

2) Как именно вашата интердисциплинарна дефиниция се отразява пряко в предложените от Вас практически стъпки? Можете ли да посочите конкретни препоръки от дисертацията, които са пряко вдъхновени от социалните, икономически или правните измерения на вашата дефиниция и които не биха възникнали при строго технически подход?

8. Заключение

Независимо от отправините критични бележки и препоръки по дисертационния труд, давам положителна оценка ЗА присъждане на научно-образователна степен „доктор“ по научна специалност 3.8. Икономика в УНСС, на Ивайло Христосков Илиев.

27.10.2025/София/УНСС Подпис: ……

O P I N I O N

From: Associate Professor Nedko Georgiev Tagarev, PhD;
University of National and World Economy;
Scientific Specialty 3.8. Economics
Regarding: a dissertation for the award of the educational and scientific degree "Doctor" in scientific specialty 3.8. Economics at UNWE.
Author of the dissertation: Ivaylo Hristoskov Iliev
Dissertation Title: IMPROVING CYBERSECURITY IN SMALL AND MEDIUM-SIZED BUSINESSES IN BULGARIA
Reason for submitting this opinion: Participation in the composition of the Scientific Jury for the dissertation defense according to Order №3011/02.10.2025 of the Rector of UNWE.

1. Information about the doctoral candidate

The doctoral candidate was enrolled in a doctoral program at the Department of National and Regional Security / Faculty of Infrastructure Economics at UNWE in the scientific specialty 3.8. Economics, pursuant to Order №486/15.03.2019 of the Vice-Rector for Research and Development at UNWE. The education was conducted independently from 26.02.2019 to 26.02.2025.

2. General characteristics of the submitted dissertation

Structure, Volume. Brief assessment of: topic relevance; aim; tasks; object; subject; main thesis; scientific literature used.

Structure and Volume of the Dissertation

The dissertation consists of three main chapters, preceded by an introduction and followed by a conclusion, bibliography, and appendices. The volume is substantial, comprising 221 pages.

Structure and Content of the Dissertation

The introduction presents the relevance, object, subject, aim, and tasks of the research. The first chapter examines the theoretical aspects of cybersecurity, the factors contributing to its importance in Bulgaria, and the role of SMEs in the economy. The second chapter proposes a methodology for enhancing cybersecurity in SMEs, including risk management, legislative, and institutional measures. The third chapter presents empirical research on the attitudes of consumers and businesses, along with an analysis of the results. The conclusion summarizes the findings and recommendations. The bibliography and appendices include the sources used (199 entries) and supplementary materials.

Relevance of the Topic

The topic is highly relevant and significant in the context of increasing digitalization and cyber threats in Bulgaria and globally. SMEs are particularly vulnerable due to a lack of resources and expertise, making them frequent targets of cyberattacks. The COVID-19 pandemic further underscored the need for a heightened focus on cybersecurity.

Aim

The primary objective of this dissertation is to examine the cybersecurity challenges faced by Bulgarian SMEs, to identify the interrelationships between these entities and their stakeholders, and to propose targeted measures for enhancing the situation.

Tasks

- Building a theoretical context for SMEs and cybersecurity.
- Analysis of the factors for the development of cybercrime.
- Examination of counteraction mechanisms at the national and European level.
- Investigation of the attitudes of consumers and businesses.

- Providing recommendations for improving the business climate and security.

Object

The specific cybersecurity problems faced by small and medium-sized enterprises in Bulgaria.

Subject

The enhancement of cybersecurity and prevention in SMEs through methodologies, legislative and institutional measures, as well as through raising awareness.

Main Thesis

In Bulgaria, the cybersecurity of SMEs requires immediate and coordinated actions from state institutions, businesses, and consumers. The lack of such actions worsens the business climate and the trust between companies and clients.

Scientific Literature Used

The author utilizes a rich and diverse body of literature in both Bulgarian and English, including:

- Specialized works on cybersecurity and economics;
- Reports from international organizations (EU, World Bank, OECD);
- National statistical data (NSI, Eurostat);
- Academic articles and studies;
- Legal and regulatory sources.
- This ensures a solid theoretical and empirical foundation for the research.

3. Assessment of the Obtained Scientific and Applied Results

The focus is on the main scientific and/or applied results achieved, the methodology used, and the fulfillment of the set aims and tasks.

The dissertation of Ivaylo Iliev achieves a series of significant scientific and applied results, contributing to both the theory and practice in the field of cybersecurity for small and medium-sized enterprises (SMEs) in Bulgaria.

Firstly, there is a theoretical enrichment of the concept of "cybersecurity". The author proposes a comprehensive, interdisciplinary definition of cybersecurity that goes beyond a purely technical approach. It is considered an organization of resources, processes, and structures for protecting cyberspace from events that are inconsistent with property rights. This approach integrates legal, economic, social, and technical aspects, making it a valuable theoretical contribution.

Secondly, the specific risks and vulnerabilities of Bulgarian SMEs are identified. Through analysis, the key threats to SMEs (e.g., ransomware, phishing, malware) have been systematized and categorized, emphasizing the factors that make them particularly vulnerable, including limited financial and human resources, a low digital culture, and a lack of specialized personnel.

Thirdly, the development of a comprehensive four-stage methodology for enhancing cybersecurity. This is a primary applied-scientific result. The methodology encompasses:

Stage 1: Identification and assessment of risk (financial, market, security).

Stage 2: Legislative initiatives at the national and EU level.

Stage 3: Institutional responses and incident response mechanisms.

Stage 4: Specific actions for all stakeholders (SMEs, banks, institutions, customers).

This structured framework provides a clear and actionable path for stakeholders to follow.

An original empirical study was conducted to compare the attitudes and understandings of two key segments: firstly, users of SME services, and secondly, owners/managers of SMEs. The results reveal the level of awareness, preconceptions, and expectations from both sides, which is valuable information for developing targeted policies and campaigns.

Specific recommendations have been made for all stakeholders. Based on the comprehensive analysis, the dissertation offers very concrete, practice-oriented recommendations addressed to:

- SMEs, through the implement of multi-factor authentication, staff training, data encryption, and the development of response plans.
- State institutions can achieve this by harmonizing legislation, improving institutional cooperation, and promoting public awareness campaigns.
- Banks and financial institutions can enhance the security of transactions and communication with customers.
- Consumers, through behavioral models for safer online shopping.

Regarding the methodology used, the author applied a complex and multifaceted methodological approach, ensuring the depth and reliability of the research.

Firstly, theoretical and descriptive analysis. This is used for building the conceptual framework in Chapter 1. It involves the analysis of scientific literature, legal frameworks (national and EU), official reports, and statistical data from sources such as NSI, Eurostat, ENISA, etc.

A comparative analysis was applied when juxtaposing definitions of SMEs in different contexts (EU, World Bank, USA), as well as when analyzing Bulgaria's level of digitalization compared to other EU member states (for example, using the DESI index).

Qualitative risk analysis, applied in the Second Chapter, to identify and categorize the financial, market, and security risks associated with digitalization and cyber threats for SMEs.

In Chapter Three, a qualitative and/or quantitative survey (the nature of the questionnaire questions suggests the presence of a quantitative component) was conducted among two focus groups - consumers and owners/managers of SMEs. This enables the testing of theoretical hypotheses and the collection of up-to-date information on the attitudes of practitioners.

Case study analysis was also applied, analysing Bulgarian SMEs as a whole, and in particular, the economic structure of Sofia served as a detailed case study, illustrating the general trends and problems.

The combination of these methods allows for both breadth of scope and depth of analysis.

Regarding the fulfillment of the set aims and tasks, the dissertation successfully achieves the objectives outlined in the introduction.

The aim – to outline the cybersecurity problems faced by SMEs and provide recommendations – has been fully achieved. A comprehensive analysis has been made, and clear, practical guidelines for action have been formulated at the end.

Task 1 (Building a Theoretical Context) is thoroughly addressed in Chapters 1 and 3, where a detailed characterization of SMEs in Bulgaria and their role in the economy is presented.

Task 2 (Outlining the factors for cybercrime) is fulfilled in subchapters 2.1, 2.2, and 2.3, which analyse digitalization, financial problems, and the human factor as prerequisites for the growth of cybercrime.

Task 3 (Examining Counteraction Mechanisms) is fully covered in the Second Chapter, the entire focus of which is precisely on the methodologies, legislative, and institutional mechanisms for combating cybercrime.

Task 4 (Outlining possible solutions and good practices) is realized in the final part of the Second Chapter (specific actions) and in Chapter 4 (possible paths for improvement and good practices).

Task 5 (Investigating attitudes) was successfully accomplished in Chapter Three through the empirical research.

Task 6 (Providing recommendations for the business climate) is fulfilled in the conclusion and throughout various sections of the work, where the recommendations are specifically aimed at enhancing the overall business environment by improving cybersecurity.
The dissertation represents a serious, well-structured, and well-argued study. It not only identifies the cybersecurity problems of Bulgarian SMEs but also proposes a comprehensive, multi-level, and practical methodology for their resolution, making it a valuable contribution to both the academic community and business practitioners and legislators.

4. Assessment of the Scientific and Applied Contributions

Brief assessment of the contributions stated by the doctoral candidate
Focus on the main scientific and/or applied contributions in the dissertation.
The contributions of the dissertation are clearly formulated and demonstrate both theoretical and practical value:

- Theoretical Contribution – Expansion of the concept of "cybersecurity" through an interdisciplinary definition that integrates legal, economic, social, and technical aspects. This approach transcends the traditional technical perspective, contributing to a more comprehensive understanding of the problem.
- Risk Identification – Systematization of the key threats to Bulgarian SMEs (e.g., ransomware, phishing) and the factors that make them vulnerable, including limited resources, low digital culture, and a lack of expertise.
- Methodology for Enhancing Cybersecurity – The developed four-stage framework (risk assessment, legislative initiatives, institutional responses, and preventive measures) offers a clear and actionable path.
- Empirical Research – The comparative analysis of consumer and business attitudes provides valuable insights into the awareness and expectations of both groups, informing targeted policies.
- Practical Recommendations – Specific guidelines for SMEs, institutions, banks, and consumers that are directly applicable and can contribute to enhancing cybersecurity in Bulgaria.

The contributions are well-substantiated and reflect an in-depth analysis of the problem, making them valuable for the academic community, business practitioners, and regulatory bodies alike.

5. Assessment of the Publications Related to the Dissertation

The four scientific publications by doctoral candidate Ivaylo Iliev demonstrate an impressive breadth of scientific interests and a serious approach to researching critical aspects of modern national security. The publications not only reflect the results of the dissertation work but also lay a solid foundation for its defense, showing the author's ability to engage with complex and current problems in the field.
The publications possess high scientific value, as evidenced in several areas. Primarily, they cover key aspects of the modern concept of national security – from cybersecurity and information warfare, through sustainable development, to the organizational improvement of the special services. This demonstrates a capacity for complex thinking and an understanding of the interconnections between different dimensions of security. In each publication, a deep understanding of the specific Bulgarian context is evident, combined with a clear awareness of the European and international dimensions of the problems examined.
From a methodological standpoint, the publications show a developed ability to work with diverse sources and research methods. The author skillfully combines legal analysis in the publication on cybersecurity with statistical methods and public policy analysis in the text on

sustainable development. Particularly impressive is the critical analysis of the organizational problems within the special services system, which reveals a deep understanding of the operational and managerial aspects of security.

All publications address highly topical themes that are at the forefront of attention for both academic circles and security practitioners. The analysis of the consequences of the COVID-19 pandemic on European security, as well as the examination of information warfare as a contemporary challenge, shows a good orientation towards current trends and an ability to provide timely scientific responses to emerging challenges.

The publications do not merely supplement the dissertation; they essentially constitute its main pillars. They demonstrate the development of a consistent and logical research program, in which different aspects of national security are examined systematically and in relation to one another. The author's ability to move confidently between theoretical analysis and practical recommendations is a testament to the maturity of the research.

Despite the impressive qualities, there is room for further improvement. In some publications, a certain unevenness in the depth of analysis can be observed, with some sections being more superficial than others. Furthermore, a broader inclusion of comparative analysis with the experience of other EU and NATO countries would significantly enrich the conclusions and recommendations.

Overall, the scientific publications of doctoral candidate Ivaylo Iliev represent a solid scientific contribution to the study of Bulgaria's national security in the contemporary context. They testify to his ability to conduct independent scientific research, analyse complex problems, and formulate adequate solutions. The publications fully meet the requirements for a doctoral dissertation and provide sufficient evidence of the author's scientific and professional competence.

6. Assessment of the Abstract (Autoreferat)

The abstract (autoreferat) of the dissertation by Mr. Ivaylo Iliev, titled "Improving Cybersecurity in Small and Medium-Sized Businesses in Bulgaria," represents a comprehensive, well-structured, and academically rigorous summary of a study with high scientific and applied value. The document fully meets the requirements for this type of publication and convincingly demonstrates the necessity of the research, its methodological foundation, and the expected contributions.

The chosen topic is extremely current and of strategic importance for Bulgaria. The author skillfully highlights the critical role of SMEs in the Bulgarian economy (accounting for over 95% of all enterprises) and the paradox between their vital importance and vulnerability in cyberspace. The context of accelerated digitalization, intensified by the COVID-19 pandemic, and the insufficient institutional and consumer culture in Bulgaria are presented as key prerequisites for the study. The topic is not only locally significant but also aligns with broader European and global discussions on cybersecurity for small businesses.

The abstract follows a classic and clear structure: introduction, general characteristics, aims and tasks, methodology, and expected contributions. The research logic is sequential: from a theoretical conceptualization of the term "cybersecurity" and identification of problems in the Bulgarian context, through the development of a solution methodology, to its testing via empirical research and the formulation of recommendations. This approach ensures comprehensiveness and coverage of all aspects of the research problem.

The methodology employed is complex and encompasses both qualitative (literature analysis, comparative analysis, and case study analysis) and quantitative (empirical survey) methods. The

combination of theoretical investigation and practical surveys of business and consumer attitudes contributes to a deeper and more nuanced understanding of the problem. The empirical part, although based on a limited sample size, provides valuable qualitative insights into the differences and similarities in the perceptions of the two key groups.
The abstract provides an exhaustive summary of the dissertation. It goes into sufficient detail to inform the reader about the main arguments and conclusions without becoming overly technical or cumbersome. The language is scientifically rigorous yet accessible. One minor remark would be that in some sections, particularly the theoretical part, there is a degree of repetition and an overload of details that could be further compressed for even greater clarity.
Overall, the abstract is an excellently prepared document that convincingly presents the significance, approach, and contributions of the dissertation. It not only informs but also generates interest in the full text of the study. It demonstrates a serious scientific contribution and a clear focus on solving a real and pressing socio-economic problem.

7. Critical Remarks, Recommendations, and Questions

Critical Remarks

- A visual methodological model was not developed.

Recommendations

- It would be beneficial to incorporate more visual and organizational elements, such as tables, graphs, and figures, in the theoretical and methodological sections, which would aid in the comprehension of the information.

Questions

1. On what basis do you consider legislative initiatives (Stage 2) to be an effective element of your methodology in the specific Bulgarian context, and would it not be more realistic for this stage to be replaced or significantly modified to focus on the enforcement and implementation of existing laws, rather than on creating new ones?
2. How exactly is your interdisciplinary definition directly reflected in the practical steps you have proposed? Can you point to specific recommendations from the dissertation that are directly inspired by the social, economic, or legal dimensions of your definition and which would not have emerged from a strictly technical approach?

8. Conclusion

Notwithstanding the critical remarks and recommendations directed at the dissertation, I give a positive assessment FOR the award of the educational and scientific degree "Doctor" in the scientific specialty 3.8. Economics at UNWE to Ivaylo Hristoskov Iliev.

27.10.2025 / Sofia / UNWE Signature: _____