СТАНОВИЩЕ

от

полковник доцент доктор инж. Галин Райнов ИВАНОВ

началник на катедра „Мениджмънт на сигурността и отбраната“

при Военна академия “Георги Стойков Раковски”

Област на висшето образование: 9. „Сигурност и отбрана”

Професионално направление: 9.1. „Национална сигурност”

България, София, п.к. 1504,
Бул. „Евлоги и Христо Георгиеви“ № 82,
Тел.: +395 02 92 26670, Факс: +359 02 92 26539,
E-mail: iwanow_off@abv.bg

на дисертационния труд

на *д-р Дмитро Игорович ПРОКОПОВИЧ-ТКАЧЕНКО*

на тема*: „Организационно-управленски механизми за информационна и киберсигурност на държавата в условията на хибридни заплахи“*

представен за процедура по придобиване на научна степен „доктор на науките”, област на висшето образование 9. „Сигурност и отбрана“, професионално направление 9.1. „Национална сигурност“.

Основание за изготвяне на становището:

Заповед на Ректора на АНИС № 004/03.09.2026 г.

София, 2026 г.

1. Актуалност и значимост на разработвания научен проблем

Дисертационното изследване обвързва проблематиката на информационната и киберсигурността с политиката за национална сигурност на държавата и разглежда усъвършенстването на единната национална политика за киберсигурност като ключово направление за повишаване на устойчивостта на държавата.

Представеният за защита труд доказва актуалността и значимостта на научния проблем както в структурно отношение, така и чрез получените резултати. Дисертационният труд е разработен в сфера, в която има налични изследвания и приложения в практиката, така и ред все още нерешени въпроси, част от които са съществено научно-изследователско предизвикателство. В това отношение ***д-р Дмитро Игорович ПРОКОПОВИЧ-ТКАЧЕНКО*** е поставил една доста амбициозна и не толкова лесна за реализиране изследователска цел, а именно: *„……е теоретико-методологическо обосноваване, разработване и валидиране на организационно-управленските механизми на информационната и киберсигурността на държавата чрез формиране на интегрирана държавна киберустойчивост (модел ИДКУ) и определяне на тази основа на перспективите за повишаване на ефективността на единната национална политика за киберсигурност на Република България като секторна политика на националната сигурност в условията на хибридни заплахи“.*

Настоящото изследване е извършено във връзка с налаганото в съвременния свят мислене и се фокусира върху анализа на теоретичните и практическите аспекти на проблематиката за националната сигурност, информационната сигурност, киберсигурността, киберустойчивостта, хибридните заплахи и защитата на критичните комуникационно-информационни системи и се формира като интердисциплинарно научно направление, което съчетава науката за сигурността, публичното управление, военните науки, теорията на информационната сигурност, кибернетиката, телекомуникациите, правото, стратегическите комуникации и управлението на риска. В съвременната наука доминира подходът, при който националната сигурност се тълкува като сложна многоравнинна система, в която

военно-политическото, информационното, кибернетичното, икономическото, енергийното, социалното, технологичното и хуманитарното измерение образуват единен контур на държавната устойчивост, а политиката за киберсигурност се проявява като негова секторна съставка.

Изследването е фокусирано върху представянето на същността на системното управление на киберсигурността в стремежа към повишаване на ефективността на процеса и неговото непрекъснато усъвършенстване, във връзка с формализирани и стандартизирани процедури и цялостен анализ на факторите, които ги определят.

Ценността на изследването се отнася до научната и практическата актуалност на темата, което произтича от необходимостта от разработване на интегрирана организационно-управленска рамка, способна да преодолее фрагментирания подход към информационната и киберсигурността и да повиши ефективността на единната национална политика за киберсигурност на държавата. Такава рамка трябва да съчетава стратегическо планиране, институционална координация, управление на риска, защита на критичните комуникационно-информационни системи и мрежи, управление на киберкризи, развитие на човешкия потенциал, технологична оперативна готовност, стратегически комуникации и международно сътрудничество. Именно в този контекст дисертационното изследване разработва и валидира концептуалния модел „Интегрирана държавна киберустойчивост“ (ИДКУ), насочен към усъвършенстване на организационно-управленските механизми на информационната и киберсигурността на държавата и към повишаване на ефективността на единната национална политика за киберсигурност в условията на хибридни заплахи.

Този дисертационен труд предоставя синтезирано и допълнено знание, което може да допринесе за създаването на безопасна среда и насърчаването на специфична култура на безопасност, свързана с новите киберзаплахи. Основната цел на това изследване е анализът на многоизмерните детерминанти на процеса на управление на безопасността в рамките на държавата и представянето на примерни решения в тази област.

В този смисъл темата на дисертационния труд ***„Организационно-управленски механизми за информационна и киберсигурност на държавата в условията на хибридни заплахи“*** е особено актуална. Тя има не само подчертана теоретична, но и определена практико-приложна значимост.

Основното съдържание на научната разработка на ***д-р Дмитро Игорович ПРОКОПОВИЧ-ТКАЧЕНКО*** напълно съответства на темата на дисертационния му труд ***„Организационно-управленски механизми за информационна и киберсигурност на държавата в условията на хибридни заплахи“***. Предложеният за становище дисертационен труд касае научни въпроси в предметна област сигурност и отбрана, които са категорично дисертабилни.

Резултатите от подобно научно изследване са безусловно необходими и определено биха способствали за усъвършенстване на стратегическите и оперативни планове на национално ниво. Като се има предвид, че изследвания с подобно съдържание са все още рядкост у нас, настоящият дисертационен труд ще запълни един вакуум в системата за национална сигурност, свързана с киберустойчивостта на страната и може да се изведе като предпоставка за успех при изграждането на високо равнище на сигурност в национален и наднационален характер.

2. Оценка на научните резултати и приносите на дисертационния труд

Получените научни резултати в дисертационния труд ми дават твърди основания да подкрепя посочените от кандидата за присъждане на образователна и научна степен „доктор на науките“ в автореферата претенции за приноси, които определям в две основни направления като научни и научно-приложни приноси и ги свързвам със следните постигнати резултати:

2.1. Приноси с научно значение:

2.1.1. Обоснована е интегрираната държавна киберустойчивост като седемслойна организационно-управленска архитектура и практически инструмент за развитие на единната национална политика за киберсигурност.

2.1.2. Киберустойчивостта на критичните комуникационно-информационни системи и мрежи е обоснована като самостоятелна управленска категория на националната сигурност.

2.1.3. Разработена е операционна матрица на хибридните заплахи и механизъм за междуведомствена координация чрез RACI, IoC обмен, ситуационна осведоменост, кризисни протоколи и взаимодействие CSIRT/SOC.

2.2. Приноси с научно-приложно значение:

2.2.1. Обоснован е КРИЦ като институционално координационно-аналитично ядро и е предложен национален MISP-базиран механизъм за обмен на индикатори за компрометация.

2.2.2. Формирана е многокомпонентна методология за оценяване и валидиране на ИДКУ чрез AHP, Delphi, сценарен и GAP-анализ, експертно и социологическо оценяване и цифрови инструменти.

2.2.3. Разработена е пътна карта за 2026–2030 г. с нормативно-правни, институционални, оперативно-технически, образователно-кадрови и международни мерки.

Анализът и интерпретацията на данните съдържат необходимите теоретични обобщения в търсенето на ново решение на актуален проблем от областта на управлението на сигурността, като с това представляват оригинален принос в съвременната наука.

В научно отношение предложеният дисертационен труд може да се използва в учебния процес на широк кръг читатели – за докторанти, студенти и специализанти от АНИС - гр. Пловдив, а също така да бъде предназначен за използване при обучение по сродни специалности в професионално направление „Национална сигурност“ в други висши учебни заведения и научно-изследователски институти, работещи в сферата на сигурността и отбраната в страната и в чужбина.

В практическо отношение, приложимостта на разработката се очаква да е по-значима, тъй като осигурява добра платформа за системното разбиране и

натрупване на познание от страна на държавните институции в управлението на киберсигурността, която от своя страна е елемент на националната сигурност.

3. Становище относно наличието или липсата на плагиатство

Към днешна дата не ми е известно да са постъпили сигнали относно публикациите на кандидата за плагиатство от анонимен или неанонимен характер. Нямам данни представяния научен труд или част от него да са плагиатствани.

Считам, че дисертационният труд е лично дело на ***д-р Дмитро Игорович ПРОКОПОВИЧ-ТКАЧЕНКО.***

4. Критични бележки и препоръки

В представения дисертационен труд и автореферата към него съществуват технически и редакционни грешки, неточности и повторения при оформянето му от автора, които не намаляват научната му стойност.

Основната ми препоръка е, че резултатите от изследването, освен чрез автореферата и с публикациите по темата, следва да получат необходимата публичност чрез издаването на учебник или учебно пособие по темата.

Посочените недостатъци не се отразяват негативно върху значимостта на приносите в дисертационния труд. Дисертацията е задълбочен и самостоятелен научен труд по актуален проблем и с постигнатите научни и научно-приложни приноси доказва способността на докторанта самостоятелно да разработва въпроси в областта на национална сигурност.

5. Заключение

Предложеният дисертационен труд от ***д-р Дмитро Игорович ПРОКОПОВИЧ-ТКАЧЕНКО*** на тема: ***„Организационно-управленски механизми за информационна и киберсигурност на държавата в условията на хибридни заплахи“*** е напълно завършен научен труд, който съответства на заглавието и основното съдържание на разработката.

Считам, че дисертационният труд на докторанта ***д-р Дмитро Игорович ПРОКОПОВИЧ-ТКАЧЕНКО*** отговаря на изискванията на чл. 6 (3) от Закона за

развитие на академичния състав в Република България и на чл. 27 от Правилника за прилагането му и се явява необходимата основа за присъждане на научна степен „доктор на науките“ в област на висшето образование: 9. „Сигурност и отбрана”, професионално направление 9.1 „Национална сигурност.

6. Оценка на дисертационния труд

Представеният дисертационен труд на ***д-р Дмитро Игорович ПРОКОПОВИЧ-ТКАЧЕНКО*** отговаря на изискванията на Закона за развитието на академичния състав в Република България и Правилника за прилагане на закона за развитието на академичния състав в Република България.

Давам **положителна оценка** на дисертационния труд на тема: ***„Организационно-управленски механизми за информационна и киберсигурност на държавата в условията на хибридни заплахи“*** *с автор* ***д-р Дмитро Игорович ПРОКОПОВИЧ-ТКАЧЕНКО.***

ЧЛЕН НА НАУЧНОТО ЖУРИ:
ПОЛКОВНИК ДОЦ. Д-Р ИНЖ. ГАЛИН ИВАНОВ

10.10.2026 г.