



## **ВОЕННА АКАДЕМИЯ "ГЕОРГИ СТОЙКОВ РАКОВСКИ"**

1504 София, бул. "Евлоги и Христо Георгиеви" № 82, тел. 92 26 622

E-mail: rnda@md.government.bg

### **РЕЦЕНЗИЯ**

**от професор д.н. инж. Манол Петков Млеченков**

професор в катедра „Информационна сигурност” на факултет

„Артилерия, ПВО и КИС” на НВУ „Васил Левски”

живущ в гр. София, ж.к. Христо Смирненски, бл. 16, ет. 11, ап. 50,

тел. 028715112

**на научните трудове,** представени по конкурса за заемане на академична длъжност „професор” от научна област 9 „Сигурност и отбрана”, професионално направление 9.1. „Национална сигурност”, научна специалност „Киберсигурност” по учебни дисциплини „Мениджмънт на ресурсите на КИС” и „Защита на КИС”, обявена със заповед на Министъра на отбраната на Република България № ОХ-116/12.02.2018 г. и обнародван в Държавен вестник бр. 20/06.03.2018 г.

**на кандидата:** полковник доцент доктор Камен Станев Калчев, началник на катедра „Комуникационни и информационни системи” към факултет „Командно-щабен” на Военна академия „Г. С. Раковски”

СОФИЯ

2018 г.

**1. Кои трудове от представените от кандидата се приемат за оценка от рецензента:**

Кандидатът в конкурса, полковник доц. д-р Камен Станев Калчев, е предложил за рецензиране 15 труда с общ обем от 399 страници. От тях за рецензиране се приемат 15 броя [1, 2, 3, 4, 5, 6, 7, 10, 11, 12, 13, 15, 16, 17, 18], с обем от 399 страници.

За рецензиране се приема следната научна продукция:

- монография – 1 брой – [15] с обем от 123 страници;
- учебници – 1 брой – [16] с обем от 123 страници;
- публикации – 11 броя [1, 2, 3, 4, 5, 6, 7, 10, 11, 12, 13] с обем от 53 страници;
- проекти – 2 броя [17, 18] с обем от 100 страници.

**Публикациите могат да бъдат класифицирани както следва:**

**1.1. По вид:**

- статии – 8 брой [11, 3, 4, 5, 10, 11, 12, 13] с обем от 28 страници;
- доклади – 3 броя [2, 6, 7] с обем от 25 страници.

**1.2. По място на публикуване:**

- статии в национални списания – 8 броя [1, 3, 4, 5, 10, 11, 12, 13];
- доклади в трудове на международни научни конференции в България – 1 брой [7];

- доклади в научни трудове на ВА „Г. С. Раковски” – 1 брой [2];

- доклади в научни трудове на НВУ „В. Левски” – 1 брой [6];

**1.3. По езика, на който са написани:**

- на английски език – 2 броя [12, 13];
- на български език – 9 броя [1, 2, 3, 4, 5, 6, 7, 10, 11].

**1.4. По брой на съавторите:**

- самостоятелни – 10 броя [1, 3, 4, 5, 6, 7, 10, 11, 12, 13];
- с един съавтор – 1 брой [2];

**1.5. Рецензирани преди публикуване – 12 броя [1, 2, 3, 4, 5, 7, 10, 11, 12, 13, 15 16].**

**2. Обща характеристика на научно-изследователската, научно-приложната и педагогическата дейност на кандидата.**

Приетите за рецензиране трудове на полковник доц. д-р Камен Станев Калчев могат да се характеризират по следния начин.

Монографията [15] на тема „Измерване на параметри в системите за киберсигурност“ представлява завършен научен труд, в който чрез изследване и анализ са синтезирани нови модели за оценка на риска и е определена функцията за управление на риска в системата за киберсигурност.

Изследван е проблемът за сигурността в киберпространството и е обоснована областта като среда и източник на несигурност, заплаха и агресивни действия. Определени са етапите на „мрежово-центричните“ операции и на кибератаките като част от кибероперациите. Чрез анализ на аспектите на процесите на планиране и управлението на силите са изведени нови изисквания към единната КИС, а чрез прилагане на архитектурен подход са определени основните принципи за изграждане на техническата архитектура на информационните системи (ИС).

Анализирани са познати модели за описание на системи за киберсигурност, в резултат на което е определена група от модели – графичен, логически (модел с пълно прикритие) и аналитичен като подходящи за провеждане на изследвания в областта на киберсигурността.

Дефинирани са основните етапи за проектиране на ИС и на системата за киберсигурност. Предложено е прилагането на график на Гант като средство за изобразяване на връзките между последователността и продължителността на дейностите, маршрутни карти и диаграми, и унифициран език за моделиране и матрица за съпоставка.

Извършен е анализ на осем системи за компютърно моделиране като по-детайлно са представени възможностите на системите COMNET и OPNET за моделиране на мрежата, нейните елементи и процеси. Предложени са за прилагане: съвкупен показател, тегловни коефициенти и частни показатели за измерване ефективността на системите за киберсигурност.

Синтезирани са оригинални аналитични модели за:

- количествено измерване на риска с използване на размита логика в отношенията заплаха – защита – риск.

- формулирана е функция, описваща системата за управление на риска, интегрираща процеса в спектъра – приемлив риск – зона за управление – зона на неприемливия риск.

Изследвано е влиянието от прилагането на системата за управление на знания върху киберзащитата. Като краен резултат е изведено приложението за използване на три променливи: риск, киберзаплахи и съпротивление и са формулирани четири стъпки за реализиране на методиката.

Резултатите от монографичния труд са публикувани в списание с импакт фактор на английски език [12, 13].

Учебникът [16] „Киберсигурност“ е създаден в съавторство – 80%-20%, което е потвърдено с разделителен протокол. Целта на учебника е да подпомогне изучаването на тематиката по дисциплина „Киберсигурност“ (Защита на КИС). Учебникът е организиран в 11 части като последователно е разгледана тематиката свързана с:

- ролята, мястото и задачите, решавани от системите за киберсигурност. Представени са и основни критерии за класификация на системите за киберсигурност в съответствие с „Оранжевата книга“ на NIST.

- направленията за несанкциониран достъп до КИС, основните инструменти за реализиране на такъв достъп, както и начините за защита.

- описана е структурата и функциите на системата за управление на киберсигурността в организацията.

- представени са специфичните системи SCADA и стандартът TEMPEST във връзка с изискванията за паразитни електромагнитни излъчвания от гледна точка на системата за киберсигурност.

- разгледана е в необходимата технологична и организационна дълбочина подсистемата на криптозащита. Представена е спецификата в планирането на различните крипторежи – канално криптиране, криптиране от край до край и електронен подпис.

- описани са методите за оценка на риска в системите за киберсигурност.

- представени са основните изисквания при изграждането на системи за киберсигурност в съответствие със стандарта ISO-27000.

В публикация [1] са разгледани новите концептуални схващания на програмата на US Army “Future Combat Systems” за изискванията към КИС в контекста за придобиване на нови качества на ВС. Това условие налага промяна в изискванията към КИС, която трябва да създаде средата за трансформация на ВС.

В резултат на анализа е обосновано ново изискване „адаптивност”, което позволява и управлението и КИС да се анализират нефрагментарно (по фази), а като динамичен процес, и да се приложи т.нар. динамично управление. Това е новост в теорията за КИС. Предложени са механизъм за количествена оценка и показател на това изискване – коефициент на адаптивност.

Публикация [2] е разработена в съавторство – 50% – 50 %, за което е представен разделителен протокол. В нея се разглеждат съвременните методи за организиране на един от сложните процеси при планиране на

КИС – честотният мениджмънт и използваните инструменти за автоматизация на този процес. Обоснована е потребността от придобиване на инструментално средство, подпомагащо планиращия процес в българската армия, в съответствие с нарасналите изисквания към функционирането на радио-средствата в съвременните военни конфликти.

В публикация [3] след анализ на съвременния подход – т.нар. „всеобхватен подход” - са определени неговите преимущества и недостатъци и е предложена формализация на подхода като са обосновани условията за въвеждане на ограничения при неговото прилагане.

В статия [4] е представена една реална възможност за универсално измерване на способностите на системите за сигурност и отбрана, реализиращи се в определен времеви интервал (бой, операция, нормативно заложен срок и др.). Формулирани са три принципа за оценка на ефективността на способностите на КИС.

Методиката на планиране, базирана на способности, може да намери многостранно приложение.

В статия [5] е анализирана ролята и мястото на системите за управление на знания (СУЗ) в системите за управление, обосновано е мястото им в управлението и конкретно в процеса за вземане на решение, и е направен количествен анализ на ефекта от прилагането на СУЗ върху процеса за вземане на решение. Обоснован е видът на ефекта от прилагането на СУЗ върху параметрите на управленския процес, а именно - повишаване на качеството, намаляване на времето за реализация на процеса и намаляване на разходите за същия.

В доклад [6] са представени резултати от изследване на методите за проектиране на информационни системи. Анализирани са основните стъпки и особености при проектирането им. Предложени са механизми за количествена оценка на резултатите от прилагането на системи, автоматизиращи дадени процеси.

В доклад [7] са изследвани основните фактори и проблеми, определящи киберпространството като област, генерираща заплахи в процеса на глобализация. Анализирани са частично възможностите за противодействие на тези заплахи. Обосновано е обединяване на усилията за динамично сътрудничество в сферата на сигурността на заинтересованите субекти, както международни, така и национални, при решаване на проблемите за киберсигурността.

В статия [10] са разгледани съвременните тенденции и направления за интегриране на системите за командване и управление. Представени са схващанията на специалистите в областта на кибервойната за методите за въздействие, обектите и ефектите от въздействието в киберпространството в условия на кибервойна. В резултат на анализа са определени основните направления за развитие на военната техника и организацията на бъдещите военни сили и оръжия. Обоснована е тенденцията в изграждането на способности за Въоръжените сили (ВС) в глобален аспект, свързана с постигането на капацитет за водене на кибервойна.

В статия [11] е проведен анализ на достъпни източници в областта на теорията и практиката при водене на кибервойна, провеждане на кибероперации в компютърните мрежи, тактиките на действията в киберпространството, както и част от съвременните средства, използвани за такива действия. Разгледани са възлови и определящи характеристики на основни видове оръжия, използвани в киберпространството. Формулирани са основните характеристики от военно-техническа гледна точка на бойните действия в киберпространството.

Полковник Камен Калчев е участвал в два научноизследователски, образователни и приложни проекти.

В проект [18] BG051PO001-3.1.08-0001 „Усъвършенстване на системите за управление във Военна академия „Г. С. Раковски””, финансиран по програма РЧР на Европейския съюз като ръководител.

Разработен е с един съавтор с принос 50% – 50%, за което е представен разделителен протокол.

Формата на проекта е в съответствие с изискванията на инвеститора (Министерството на образованието и науката). Проектът е уникален не само със съдържанието си, но преди всичко с подхода, приложен за постигане на неговата цел.

Описани са и са анализирани основните процеси в управлението на ВА „Раковски“, чрез съвременен инструмент за описание на процеси, което позволява да се автоматизира изследването им за време, участващи обекти и колизии между тях.

Резултатът от изследването е с практико-приложна насоченост и се използва за основа при подготовката на спецификацията за обществените поръчки, съпътстващи изпълнението, и на второ място - за промяна на основните правилници, регламентиращи дейността на Военна академия. Проектът е класиран, финансиран и от януари 2015 г. резултатите от него са въведени в експлоатация. В резултат на проекта са придобити:

- Интегрирана система за управление на висше учебно заведение „PeopleSoft“ от тип ERP (Enterprise Resource Planning);
- Система за документооборот, базирана на продукта SharePoint;
- Система за защита, базирана на защитна стена “Micro Thick”, и антивирусен софтуер.

Проект [19] е „Комуникационно-информационна система за батальонна бойна група (ББГ)“. Възложен е от фирма СТЕМО ООД и е разработен с един съавтор с принос 50% – 50%, за което е представен разделителен протокол.

Проектът включва цялостно описание на КИС (с всичките й елементи– мрежи, възли, оборудване, система за защита) на батальонна бойна група. Разчетите и описанието започват от оперативни изисквания, през системно описание, до техническа реализация. Разработен е във



форма, съответстваща на изискванията на възложителя, и включва множество схеми, таблици и разчети. Представява завършен проектантски труд, притежаващ необходимата степен на детайлизация и качествата да бъде реализиран.

### **3. Оценка на педагогическата подготовка и дейност на кандидата**

Педагогическата дейност на полковник доц. д-р Камен Станев Калчев се характеризира като съчетание от преподавателска и научно-изследователска дейност.

До 2000 г. заема различни командни и щабни длъжности в свързочни формирования на БА. В периода 1989 – 1995 г. завършва Техническия университет в гр. София по специалност „Магистър инженер по изчислителна техника“.

От 2000 г. след успешен конкурс е назначен за асистент в катедра „Комуникационни и информационни системи“ във ВА „Раковски“. В периода 2003 – 2005 г. разработва и успешно защитава докторска дисертация и последователно заема длъжност „старши асистент“ – 2003 – 2005 г. и „главен асистент“ - 2005 – 2009 г. От 2009 г. е избран за „доцент“ в катедра КИС, а от 2009 г. е избран за началник на катедрата.

Средната му аудиторна заетост, приравнена към упражнения, е над 450 часа. Провежда занятия с редовни и задочни обучаеми по дисциплините:

- „Организация и управление на комуникационно-информационните системи в оперативните и тактическите формирования”
- „Защита на комуникационните и информационните системи”
- „Мениджмънт на ресурсите на КИС”
- „Организация и управление на комуникационно-информационните системи в сигурността и отбраната”, и курсове по „Защита на информацията в КИС“ и „Киберсигурност“.

По всяка от дисциплините е разработил учебник, курс лекции и учебно-методически пособия. Същите са разработени на достъпен стил и са много добре онагледени, което е предпоставка за трайното усвояване на знания от обучаемите. Автор е на три учебни програми.

Доц. д-р Калчев провежда занятията на високо методическо ниво. Ежегодно ръководи по 4 - 5 дипломанта, завършващи обучението си във ВА „Раковски“. До момента на конкурса е бил ръководител на трима успешно защитили докторанти и в момента е ръководител на трима, на които им предстои защита.

#### **4. Основни научни резултати и приноси**

Основните научни резултати и приноси от проведените изследвания на полковник доц. д-р Камен Станев Калчев могат да се характеризират като научни, научно-приложни и приложни.

Като **научни приноси** могат да се определят:

1. Синтезиран е оригинален правдоподобен модел за количествено определяне на риска в системите за киберсигурност. (Risk assessment in cyber security systems) [12, 13, 15].

2. Дефиниран е аналитичният модел на функцията, която определя поведението на системата за управление риска в системите за киберсигурност. (Formalization of processes in the systems for risk management in cybersecurity) [12,13, 15].

3. Чрез анализ е обосновано ново изискване „адаптивност“ и показател за оценка, което позволява управлението и КИС да се анализират нефрагментарно (по фази), а като динамичен процес и да се приложи т.нар. динамично управление, което е новост в теорията за КИС [1].

Като **научно-приложни приноси** могат да се определят:

1. В резултат от проведено изследване на модела за количествено определяне на риска чрез симулацията му в диапазон от стойности на

променливите „съпротивление“ и „заплахи“ - от 0 до 100 в % е предложен универсален метод за измерване способностите на системите за сигурност. Предложен е графична форма за представяне на крайният резултат, позволяващ бърз графичен анализ.[4]

2. Концептуално е изследвана функцията на поведение на системата за управление на риска. В резултат на това изследване в интегриран графичен вид са представени областите и тяхното разположение на различните стратегии при управление – „област на приемлив риск“, „област на неприемлив риск“ и област на управляемост на риска [6].

3. Изследван е проблемът за сигурността в киберпространството и е обоснована областта като среда и източник на несигурност, заплахи и агресивни действия. На базата на изводите от анализа на „всеобхватния подход“ е предложена формализиране на подхода и е обосновано условието за въвеждане на ограничения при прилагането му. [3, 7].

4. След проведено изследване на технологичната и организационната подсистема на криптозащита са предложени универсални методи в планирането на различни криптомрежи – канално криптиране, криптиране от край до край и електронен подпис и са изведени три принципа за оценка ефективността на способностите на КИС [4].

5. Анализирани са познати модели за описание на системи за киберсигурност. В резултат на това е синтезирана група модели – графичен, логически (модел с пълно прикритие) и аналитичен като подходящи за провеждане на изследвания и проектиране на системи за киберсигурност [15].

6. След анализ на схващанията за водене на кибервойна са изведени основните направления за развитие на военната техника и организацията на бъдещите военни сили и оръжия. Обоснована е тенденцията в изграждането на способности за Въоръжените сили (ВС) в глобален аспект, свързана с постигането на капацитет за водене на кибервойна.

Формулирани са основните характеристики от военно-техническа гледна точка на бойните действия в киберпространството [10, 11].

Като **приложни приноси** могат да се определят:

1. Синтезирани са в подходяща форма знания в областта на киберсигурността, позволяваща по – удобно представяне и изучаване на същите [2, 3, 4, 5, 16].

2. Разработен е изпълним проект за изграждане на КИС (с под-система за защита на информацията) за батальонна бойна група [19].

3. Разработен е изпълним проект за усъвършенстване на система за управление на Военна академия чрез информационна система (включваща подсистема за защита на информацията). Този проект е реализиран и чрез него ВА е придобила такава система (съответно и функционираща подсистема за информационна сигурност) [18].

#### **5. Оценка на значимостта на приносите за науката и практиката**

Посочените по-горе приноси са отразени в рецензираните публикации, учебника и монография на полковник доц. д-р Камен Калчев и се прилагат в учебния процес и административната дейност на Военна академия „Г. С. Раковски“. Същите спомагат за развитие на теорията и практиката в професионално направление 9.1. „Национална сигурност“, научна специалност „Киберсигурност“.

Изведените нови изискване на КИС, методи за оценка на нейната ефективност и киберзащита, могат да се използват от екипите, разработващи документи с ведомствено и национално значение.

#### **6. Оценка в каква степен приносите са дело на кандидата**

Оценявам постигнатите приноси за лично дело и постижение на полковник доц. д-р Камен Станев Калчев и приемам, че са резултат от проведените от него изследвания.

#### **7. Критични бележки за рецензираните трудове**

По научната продукция на кандидата могат да се формулират следните критичните бележки:

1. Отделни пасажии от текста в учебника [16] се нуждаят от редактиране и текстообработка; отделни формули са с размер на шрифта, несъразмерен с този на основния текст.

2. Препоръчвам в учебното съдържание и публикациите да се включат препоръките на международните стандарти ISO/IEC 27017:2015 и ISO/IEC 27032:2012(E), които имат отношение към киберзащитата на системите.

**8. Лични впечатления и други въпроси, по които рецензентът счита, че следва да вземе отношение**

Познавам кандидата, участващ в конкурса на академична длъжност „професор” от 1997 г. до 1999 г., като обучаем във Военна академия и от 2000 г. до сега като преподавател. В периода от 2003 г. до 2005 г. му бях ръководител при разработването на докторската дисертация. Прояви изключителна упоритост и компетентност и успя да я разработи и защити предсрочно за две години.

Има изградени навици за работа и ръководене на екип, ползва се с авторитет в катедрата и сред обучаемите. Високата му професионална подготовка дава основание да бъде привлечан в работата на екипи, работещи по проблемите на комуникационните и информационните системи в операции за управление при кризи. Работи за повишаване на квалификацията си. Своевременно изучава новостите в предметната област, която преподава и насочва научно-изследователската си дейност за прилагане и развитие на постиженията в сферата на комуникационните и информационните мрежи и системи, защитата на информацията и киберзащитата. Следи новостите в прилагането на нови методи и форми на обучение и се стреми да ги прилага при обучението на слушателите и студентите във Военна академия „Г. С. Раковски”. Ежегодно през последните девет години публикува статии в списанието за IT директори

СИО, в които представя новостите в развитието на КИС и киберзащитата. Две от публикациите на доц. д-р Калчев са в списание с импакт фактор „SocioBrains – International Scientific Refereed Online Journal – 2018/02.“

В съответствие с изискваните 100 точки за участие в конкурса за „професор“ по наукометрични данни за класификация на научната продукция, дейности и постижения, доц. Калчев покрива 239,2 точки.

Като отчитам личните и професионални качества на кандидата, считам, че ако полковник доц. д-р Камен Калчев заеме академичната длъжност „професор“, ще допринесе за издигане нивото на обучението на кадри, които се обучават във Военна академия „Г. С. Раковски“.

## **9. Заключение**

Като имам предвид цялостната преподавателска и научноизследователска дейност на единствения кандидат в конкурса, оценката на неговите резултати и приноси, предлагам на научното жури да **избере полковник доц. д-р Камен Станев Калчев за „професор“** в научна област на висше образование 9, „Сигурност и отбрана“, професионално направление 9.1. „Национална сигурност“, научна специалност „Киберсигурност“ по учебни дисциплини „Мениджмънт на ресурсите на КИС“ и „Защита на КИС“.

## **10. Оценка на кандидатите**

Оценявам, че дейността и постигнатите резултати от единствения кандидат в конкурса полковник доц. д-р Камен Станев Калчев **отговарят на изискванията** на Закона за развитие на академичния състав в Република България, Правилника за неговото прилагане и на Правилника за заемане на академични длъжности във Военна академия „Георги Стойков Раковски“ и давам **положителна оценка**.

РЕЦЕНЗЕНТ .....

**професор д.н. инж. Манол Петков**