РЕЦЕНЗИЯ

от проф. д.н. Николай Маринов Николов, професор ПУ „Паисий Хилендарски“, за присъждане на образователната и научна степен „доктор“ по: област на висше образование - 9.0 „Сигурност и отбрана“, професионално направление- 9.1.“Национална сигурност“, докторска програма “Национална сигурност“

Автор на дисертационно изследване: Костадин Рангелов Баков

Тема: „Кибербиосигурността като елемент от системата за национална сигурност“

Научен ръководител: доц. д-р Иван Димитров Станчев, проф. д-р Илия Николов Илиев

1. Общо описание на представените материали

Със заповед № РД-22-1702 от 18.07.2025 г. на Ректора на Пловдивския университет „Паисий Хилендарски“ (ПУ) съм определен за член на научното жури по процедура за защита на дисертационен труд на тема: **„Кибербиосигурността като елемент от системата за национална сигурност“**, за придобиване на образователната и научна степен „доктор“ в област на висше образование **- 9.0 „Сигурност и отбрана“** , професионално направление - **9.1.“Национална сигурност“**, докторска програма - **„Национална сигурност“**

Автор на дисертационния труд е **Костадин Рангелов Баков** – докторант на самостоятелна подготовка към катедра **„Политически науки и национална сигурност“ ,** с научни ръководители- **доц. д-р Иван Димитров Станчев и проф. д-р Илия Николов Илиев**. от ПУ “Паисий Хилендарски“

Представеният от кандидата **Костадин Рангелов Баков** комплект материали на хартиен и електронен носител **е** в съответствие с Чл.36 (1) от Правилника за развитие на академичния състав на ПУ, като включва следните документи: молба до Ректора на ПУ за разкриване на процедурата за защита на дисертационен труд; автобиография в европейски формат; протокол от Катедрения съвет, за докладване на готовността за откриване на процедурата и с предварително обсъждане на дисертационния труд; дисертационен труд; автореферат (BG, EN); списък на научните публикации по темата на дисертацията; копия на публикациите по темата на дисертацията; декларация за оригиналност и достоверност на приложените документи.

Кандидатът е приложил 3 (три) броя статии, 2 (две) от които в съавторство, 2 в реферирани издания и 1 в нереферирано издание. Всички публикации се приемат за рецензиране. Справката за съответствие с минималните изисквания за ОНС „доктор“ показва 50 събрани точки по група от показатели А и 70 събрани точки по група от показатели Г.

2. Кратки биографични данни за кандидата

Кандидатът-асистент Костадин Баков е с кариера в националната сигурност с работа в криминална полиция, икономическа полиция, противодействие на контрабандата, трафика на хора, на оръжие и пролиферациите. Професионалният му път преминава през различни ръководни позиции, като зам.- директор I степен „Полиция” ОД на МВР – гр. Пловдив, директор Териториална дирекция на КОНПИ – Пловдив и Търговски директор – Трафик СОТ

ЕООД –Пловдив. От май 2021 година е асистент - ПУ "Паисий Хилендарски", ФИСН, катедра ПННС.

Образованието му включва магистърска степен по финанси и банково дело, с диплома от Стопанска академия „Д. А. Ценов" в Свищов. Завършил е Средно-специално образование в СМУ „Ф.Е. Дзержински"- Пазарджик. Това допълване на практическо и академично обучение е основата за успешната му кариера в сектора за сигурност.

3. Актуалност на тематиката и целесъобразност на поставените цели и задачи

Обект на дисертационното изследване е кибербиосигурността като елемент на системата за национална сигурност. **Предмет на изследването** са правните и техническите аспекти на кибербиосигурността, като съчетание на познания в три различни области – национална сигурност, информационни технологии и молекулярни биотехнологии, които се съгласуват с охранителни и оперативно-издирвателни аспекти.

Целта на дисертационен труд е **да се създаде концепция за защита на кибербиосигурността в Р България**.

За постигането на поставената цел в процеса на изследване са определени за решаване следните **научноизследователски задачи**: да се анализира съвременното състояние на кибербиосигурността и нейното място в системата на националната сигурност; да се изследват биологичните оръжия и извърши тяхната класификация през призмата на научните постижения в областта на молекулярните биотехнологии; да се идентифицират опасностите и заплахите и се определи степента на риска при кибербиоатаки; да се систематизират получените резултати и се предложи модел на концепция за кибербиосигурност; да се определят насоките за развитие и усъвършенстване на дейността за противодействие на кибербиоатаки; да се анализира ефективността при прилагане на бързи методи за диагностика на заболявания като рисков фактор за биосигурността.

Изследователска хипотеза:

На базата на констатирано отсъствие на концепция, доктрина и програми за кибер-биосигурност в България и предвид нарастващата взаимосвързаност на информационните системи с биомедицинските и биотехнологични данни, се формулира хипотезата, **че разработването и внедряването на интегриран модел за кибербиосигурност, обхващащ правни, технически и организационни аспекти, значително ще повиши устойчивостта на националната сигурност на Р България срещу кибербиоатаки и ще минимизира рисковете, произтичащи от споделянето на чувствителни бази данни в контекста на членството в Европейския съюз. Този модел следва да включва стратегия за противодействие на биологични оръжия, систематизиране на заплахите и рисковете, както и насоки за развитие и усъвършенстване на дейностите по превенция и реагиране при кибербиоатаки.**

Теоретико-методологическа основа на изследването

За теоретична и методологическа база на изследването са използвани системния подход; теорията на управлението, конфликтологията; теорията и практиката на създаване на биосензори, теоретичните основи на молекулярните биотехнологии. В дисертационното

изследване са използвани национални институционални и образователни нормативни документи, енциклопедична и справочна литература, други учебно-методически материали.

Методология и методика на изследването

В хода на изследването за решаването на изследователските задачи е използван комплекс от:

– **теоретични методи**: анализ и синтез на общите характеристики на кибербиосигурността, изискваща интердисциплинарен подход на планираните изследвания.

– **емпирични методи**: наблюдение на средата за откриване рисковете при защита и пренос на чувствителни биологични данни, анкета на различни групи от населението за отчитане индивидуалния и обществен риск при пренос и съхранение на чувствителни биологични бази данни, експертна оценка за приложимостта на биосензори и техники за бърза диагностика на потенциални причинители на биологична заплаха на населението.

– **статистически методи**: за обработка, обобщаване и анализ на резултатите се използват различни методи за обработка и анализ на чувствителните биологични бази данни.

За целенасоченост, конкретност и задълбоченост на изследването се приемат следните **ограничения**:

1. Детайлно се разглеждат източниците, които изследват модели на биосензори и диагностични тестове за откриване на потенциални биологични заплахи.

2. Дейностите на други участници в противодействието като част от системата за национална сигурност не са предмет на настоящото изследване.

3. Времевият обхват на изследването е 2022 г. – 2025 г. Пространственият (териториален) обхват включва територията на Р България по отношение на анкетните проучвания и международна среда при съпоставката и анализа на данни, проведени в международна среда.

4. Нормативна база е актуална към 01.01.2025г.

Дисертационният труд на кандидата асистент Костадин Баков изследва кибербиосигурността като съществен елемент от националната сигурност. Актуалността на разработвания проблем е важна, както в научно, така и в научно-приложно отношение, защото в съвременния свят кибербиосигурността става критично важна за защитата на биологичните данни и системи.

4. Познаване на проблема

Кандидатът Костадин Баков, познава състоянието и правилно оценява изследваният проблема, а именно важността на задачата да се разработят стратегии, принципи, правила, алгоритми и методологии, които да положат основите на концепция за кибербиосигурността на територията на България, като член на ЕС.

Към настоящия момент на национално ниво отсъстват доктрина, концепция и програми за кибербиосигурност. По предложената тема на дисертационния труд не са известни научни публикации и разработки от други български автори, разглеждащи детайлно аспектите на кибербиосигурността в условията на споделяне на чувствителни бази от данни.

5. Методика на изследването

Избраната методика на изследване позволява постигане на поставената цел и получаване на адекватен отговор на задачите, поставени за решаване в дисертационния труд.

През **първия (подготвителен) етап на изследването** (2020-2022 г.) се анализира изследваният проблем от гледна точка на техническото и технологичното ниво в двете основни области – информационни технологии и молекулярни биотехнологии (биосензори). Разкриват се ключовите характеристики на двете динамично развиващи се области в една интердисциплинарна област. Определят се обектът и предметът, целите и задачите на изследването, както и се формулира работната хипотеза.

През **втория (основен) етап** (2023-2024г.) се разработват концептуалните основи на платформа за изграждане на система за кибербиосигурност. Едновременно се внасят корекции в методиката за изследване, формулират се стратегии за научно изследване на нови биосензори, както и прилагането съществуваща апаратура и биосензори за провеждане на биомониторинг.

През **третия (заключителен) етап** (2025г.) се обобщават резултатите, формулират се основните изводи и препоръки, представени в дисертационния труд.

6. Характеристика и оценка на дисертационния труд

Формулиран е научноизследователският проблем - в системата за сигурност липсва орган, отговорен за биосигурността и кибербиосигурността. Също така, липсва структура, функционално отговорна за защита на биосигурността и кибербиосигурността, както и концепция за нейното осигуряване. Основните изводи от изследването подчертават необходимостта от интегриран подход към кибербиосигурността, включващ технически и организационни мерки.

Проведената анкета сред специалисти работещи в различни области като сигурност, киберсигурност и клинични лаборатории също показват тревожни резултати. Те сочат за ниска степен на готовност за опазване на чувствителни биомедицински данни и липса на подготвеност за реакция при биотерористични заплахи. Това извежда необходимостта от незабавни действия за подобряване на капацитета и подготовката в защитата на тези ключови сектори. Изследването е актуално, тъй като в контекста на дигитализацията и глобализацията, заплахите към биосигурността стават все по-големи.

7. Приноси и значимост на разработката за науката и практиката

Достоверността и обосноваността на резултатите от дисертационния труд е осигурена: от логиката на изследването и от приложената концептуална и теоретико-методологическа основа.

Значимост на резултатите

Научната новост на изследването се състои в разкриване на взаимовръзките между биосигурността, киберсигурността и средата за сигурност, в конструирането на модел за кибербиосигурност като елемент на системата за националната сигурност.

Теоретичната значимост на изследването се състои в решаването на научната задача – формулиране на концепция за кибербиосигурност. Изследването предлага нови концепции

и модели за интегриране на кибербиосигурността с биосигурността и физическата сигурност, което е недостатъчно проучено и изследвано досега.

Практическата значимост на изследването се състои в предлагането на система от апарати и биосензори, които да се използват за провеждане на бърз анализ на агентите на потенциална биотерористична атака. Предлагат се практически решения и стратегии за защита на чувствителни данни, което предоставя широк спектър от приложения в държавната и частната сфера.

Дисертационният труд представя значителни научни и научно-приложни постижения, свързани с кибербиосигурността като важен компонент от националната сигурност:

1. Модел за интеграция на сигурността. Разработен е модел, който съчетава физическата сигурност с киберсигурността и биосигурността. Той е ключов за осъществяването на перманентен контрол върху организации и фирми, работещи с чувствителни данни.
2. Концепция за кибербиосигурност. Представена е концепция, която обединява правните и техническите аспекти на кибербиосигурността. Тя има потенциал да служи като основа за разработване на стратегии за защита на чувствителни лични данни.
3. Интердисциплинарен подход при надграждане на дейностите за осигуряване на кибербиосигурност. Този подход включва методологии за обработка на големи масиви от данни, свързани с личната информация на гражданите.
4. Биосензори и бърз анализ. Предложени са системи от апарати и биосензори, които да провеждат бърз анализ на потенциални биотерористични агенти. Това като практическо приложение може да подобри готовността за справяне с биологични атаки.
5. Проверка на информираност. Проведени са емпирични изследвания, които анализират нивото на информираност на специалисти и органи относно кибербиологичните рискове. Резултатите потвърждават необходимостта от обучение и повишаване на осведомеността.
6. Разработка на протоколи: Създадени са конкретни изисквания към методологията за взаимодействие между физическите и киберсигурността. Това е важен аспект за защита на чувствителни лични данни и реакцията при инциденти.

На базата на анализа и констатациите от изследването са предложени и конкретни мерки за подобряване на кибербиосигурността:

1.Разработване и приемане на нови правни регулации, които да обхващат специфичните нужди на кибербиосигурността. Тези нормативни актове трябва да включват изисквания за защита на биомедицинските данни и процедури за реагиране при инциденти. Особено внимание трябва да се обърне на регламента МИС 2, който въвежда задължителни стандарти за сигурност и поверителност на медицинската информация.

2. Провеждане на редовни обучения и семинари за служителите в здравните институции и лаборатории относно добрите практики за киберсигурност кибербиосигурност.

3. Инвестиране в модерни технологии за киберсигурност, включително системи за откриване на проникванията (IDS), за предотвратяване на проникванията (IPS) и инструменти за мониторинг на мрежовия трафик. Те трябва да бъдат внедрени в критичните инфраструктури и постоянно обновявани.

4. Участие в международни форуми и инициативи за обмен на информация и добри практики в областта на кибербиосигурността. Създаване на партньорства с държави и организации за съвместни проекти и изследвания.

5. Организиране на регулярни симулации и упражнения за реакция при кибератаки и биотерористични заплахи. Тези упражнения ще помогнат на институциите да идентифицират слабостите в системите и да разработят ефективни планове за действие.

6. Публично-частни партньорства: Насърчаване на публично-частни партньорства между правителствени агенции, академични институции и частния сектор за разработване на иновативни решения и технологии за кибербиосигурност.

7. Въвеждане на редовен мониторинг и одит на системите за киберсигурност в здравните институции и лаборатории. Това ще помогне за ранното откриване на уязвимости и своевременното им отстраняване.

8. Специално внимание на изследователските центрове, работещи с генетично модифицирани организми (ГМО). Тези центрове трябва да бъдат оборудвани със специфични мерки за защита на техните бази данни и експериментални резултати, тъй като потенциалните последствия от компрометиране на тази информация могат да бъдат особено сериозни.

На основата на разработения дисертационен труд се извеждат следните научни и научно-приложни приноси:

1. Предложен е модел за съчетаване на физическата сигурност с киберсигурност и биосигурност при осъществяване на контрол на институции, организации и фирми, работещи с чувствителни данни.

2. Разработен е модел за интердисциплинарен подход при надграждане на дейностите по осигуряване на кибербиосигурност при вектора чувствителни персонални данни – обработване на големи масиви от данни с чувствителна информация – регламент за съхранение и достъп до чувствителни големи бази данни.

3. Предложена е концепция за интердисциплинарен подход за разработване на протокол от мероприятия, които да осигурят кибербиосигурността при работа с чувствителни данни на хората, касаещи здравния им статус.

Дисертационният труд на Костадин Баков представлява принос в областта на кибербиосигурността. Научните и научно-приложните постижения подчертават необходимостта от интегрирани и проактивни подходи при защита на чувствителни данни и биологични системи. Първо, разработването на интегриран модел за кибербиосигурност, който синхронизира физическата сигурност с биосигурността, е от критично значение за защитата на чувствителни данни и биологични системи в условия на нарастващи заплахи. Второ, проведените емпирични изследвания за нивото на информираност на младите специалисти и специалисти в различни области подчертават необходимостта от обучение и изготвяне на протоколи за действия при кибератаки и биотероризъм. Трето, концепцията за необходимостта от нова дисциплина кибербиосигурност, основа за бъдещи изследвания, с особено значение за националната сигурност.

7. Преценка на публикациите по дисертационния труд

Общо описание на публикациите

1. Bakov, K. The New Realities In Synchronizing Physical Security And Cybersecurity In Digitalsocieties“, научно списание „Сигурност и отбрана“ – НВУ „Васил Левски“ , Година III Брой 1, 2024г.

Докладът „New Realities in Security and Defense“ разглежда променящите се динамики в сферата на сигурността и отбраната, особено в условията на съвременни хибридни заплахи, които обединяват кибер и физическа сигурност. Основният акцент е върху необходимостта от интегрирани стратегии и подходи, които да съчетават различни аспекти на сигурността, включително технологични иновации и междуинституционално сътрудничество. Подчертава се важността на адаптивността и проактивността в политиките за сигурност, за да се справят с новите предизвикателства, пред които е изправено обществото.

2. Mollova-Doshkova, D., Bakov, K., Iliev, I. The Art of Asking and Analyzing Sensitive Questions in Breast Milk Microbiome Research, Acta Microbiol. Bulg., приета за публикуване в издание 40(2) за 2024г.

Основното съдържание на изследването „The Art of Asking and Analyzing Sensitive Questions in Breast Milk Microbiome Research“ подчертава важността на човешкото мляко като основен източник на микробна колонизация при новородените, което играе критична роля в развитието на техния чревен микробиом. Проучването акцентира на предизвикателствата при проектирането на анкети за събиране на информация относно нагласите на майките към кърменето и значението на микробиомата на кърмата. Резултатите показват, че значителен процент от майките са готови да участват в научни изследвания, свързани с микробиома на кърмата, което подчертава необходимостта от информираност за ползите от кърменето.

3. Bakova, D., Yaneva, A., Harizanova, S., Shopova, D., Mihaylova, A., Kasnakova, P., Bakov, K., ... & Iliev, I. (2025). Monitoring Health Risks Associated with Body Modifications (Tattoos and Permanent Makeup): A Systematic Review. *Cosmetics*, *12*(1), 8

Изследването „Monitoring Health Risks Associated with Body Modifications (Tattoos and Permanent Makeup): A Systematic Review“ разглежда потенциалните здравословни рискове, свързани с татуировки и перманентен грим, в контекста на тяхното разпространение и последващи здравословни проблеми. Основните идентифицирани рискове включват нарушения на кожния микробиом, възпалителни процеси и инфекции, алергични реакции, токсичност на татуировъчните мастила и недостатъчна хигиена Статията се фокусира върху физическите и здравословни рискове от телесни модификации.

Статиите на Костадин Баков са изследвания в свързани области. Първата статия относно здравните рискове от телесни модификации предоставя важни данни за мигновените

и дългосрочни последици от практики, свързани с физическата сигурност, които обогатяват концепцията за кибербиосигурността. Втората статия за микробиома на кърмата изтъква нуждата от иновации в здравната система, от съществено значение в контекста на защита на биологичните данни и микробиомни изследвания. Третата статия относно новите реалности в сигурността и отбраната предлага стратегически подходи за интеграция на физическата и киберсигурността. Те допълват теоретичната основа на дисертацията с практически примери и данни.

Публикациите могат да бъдат класифицирани по вид (статии – 3 броя), по значимост (статии в издания с импакт-фактор – 3 броя), по място на публикуване (статии в реферирани международни списания – 2 броя; 1 брой в нереферирано) по език, на който са написани (на английски език – 3 броя), по брой на съавторите (самостоятелни – 1 брой; с двама съавтори – 1 брой; с трима и повече съавтори – 1 брой).

9. Лично участие на докторанта

Костадин Баков е показва лична ангажираност и активна роля в проведеното дисертационно изследване. Това включва не само формулирането на основната тема и структура на изследването, но и извършването на задълбочени анализи на кибербиосигурността, физическата сигурност и биосигурността.. Кандидатът е формулирал концепция за управление на кибербиосигурността, което е оригинален принос в научната област. Проведените емпирични изследвания доказват личния му ангажимент, като той е проучил нивата на информираност сред специалистите и е анализирал получения материал.

Кандидатът Костадин Баков участва в научни конференции, където представя резултатите от изследването си. Там той кандидатът способността си да интегрира знания от националната сигурност, информационните технологии и молекулярните биотехнологии.

10. Автореферат

Авторефератът е разработен според изискванията и отразява основните резултати, постигнати в дисертацията.

11. Критични забележки и препоръки

За да се повиши обобщимостта на резултатите, е необходимо разширяване на географския обхват, за идентификация и верификация на ключовите показатели в кибербиосигурността. За целта препоръчвам в бъдещите научни изследвания на кандидата да се проведат проучвания в различни региони на България и в международен контекст, за да се определи как културните и социални фактори влияят на нагласите и мерките за защита в областта на кибербиосигурността.

12. Лични впечатления

С кандидата ас. Костадин Баков работим в екип по основни бакалавърски дисциплини с практико-приложна насоченост – „Основи на оперативно-издирвателната дейност“,

„Оперативно-издирвателна дейност за разкриване на престъпленията“, „Разузнавателна дейност и анализ“, същият разработва и провежда ролеви игри, симулативни занятия и практически задачи и казуси, на високо ниво на теоретична и практическа подготовка.

13. Препоръки за бъдещо използване на дисертационните приноси и резултати

Препоръчвам да се разработят програми за обучение, фокусирани върху подготовката на млади специалисти в областите на кибербиосигурността.

ЗАКЛЮЧЕНИЕ

Дисертационният труд *съдържа* ***научни, научно-приложни и приложни резултати, които представляват оригинален принос в науката*** и **отговарят на всички** изисквания на Закона за развитие на академичния състав в Република България (ЗРАСРБ), Правилника за прилагане на ЗРАСРБ и съответния Правилник на ПУ „Паисий Хилендарски“.

Кандидатът **е** представил **достатъчен** брой научни трудове. В работите му има оригинални научни и приложни приноси. Теоретичните му разработки имат и практическа приложимост, като част от тях са пряко ориентирани и внедрени от него в учебната и в преподавателската му работа. Научната и преподавателската квалификация, опит и стаж на кандидата ас. Костадин Рангелов Баков **е несъмнена** и с високо качество на своето съдържание.

Дисертационният труд показва, че кандидатът Костадин Рангелов Баков **притежава** задълбочени теоретични знания и професионални умения по научна специалност „Национална сигурност“ като **демонстрира** качества и умения за самостоятелно провеждане на научно изследване. Поради гореизложеното, убедено давам своята ***положителна оценка*** за проведеното изследване, представено от рецензираните по-горе - дисертационен труд, автореферат, постигнати резултати и приноси, и ***предлагам на почитаемото научно жури да присъди образователната и научна степен „доктор“*** на **Костадин Рангелов Баков** в област на висше образование: **9.0.“Сигурност и отбрана“,** професионално направление **9.1.“Национална сигурност“** докторска програма „**Национална сигурност“**

11.08.2025 г. **Рецензент: проф. д.н. Николай Маринов Николов**

.....