СТАНОВИЩЕ

за дисертационен труд на
Красимир Стайков Коев
на тема

"Повишаване на кибернетичната сигурност и отбрана на комуникационните и информационни структури на МО и БА"

представен за придобиване на образователна и научна степен "доктор" в
Област на висшето образование 9. „Сигурност и отбрана“
Професионално направление 9.1. „Национална сигурност“
Докторска програма „Киберсигурност“

от полк. доц. д-р Николай Тодоров Стоянов
Институт по отбрана "Професор Цветан Лазаров"
бул. Професор Цветан Лазаров 2, гр. София,
тел. +359 2 9221801, GSM: +359 882110016,
e-mail: n.stoianov@di.mod.bg

1. Характеристика на дисертационния труд

Представеният за рецензиране дисертационен труд е разработен на 189 страници включващ увод, три глави, изводи и получени резултати и използвани литературни източници. Основният текст на дисертационния труд е разработен на 179 страници в това число 28 фигури и 3 таблици.

1.1. Актуалност на разработвания проблем

Киберсигурността е един от основните фактори оказващи влияние върху националните интереси в нашето съвремие. На лице е развитието на различни кибероперации от различни действащи лица. Като се започне с основните (елементарните) опити за сканиране за уязвимости на определени мрежи, премине се през различите типове атаки като фишинг, социален инженеринг и др. и се стигне т.нар. Advanced Persistent Threats.

Към днешна дата няма държавна структура или частна организация която да няма присъствие в интернет пространството. Това присъствие е застрашено от възможността за провеждане на кибератаки срещу ресурсите или услугите на съответната организация.

Безспорно киберсигурността и киберотбраната са ключови елементи на съвременната сигурност, но така също и представляват възможности за информационно превъзходство – основен елемент в съвременните бойни действия.

Актуалността на предложения дисертационен труд се определя от необходимостта от изследване на съществуващата система за киберсигурност на МО и БА, определяне на насоките за развитие и начините за подобряване на тази сигурност.

Считам, че темата на дисертационното изследване е актуална както от научна, така и от приложна гледна точка. Докторантът е фокусирал своите изследвания върху анализ на системите за

киберсигурност на редица държави ги е съпоставил със системата за киберсигурност на МО и БА.

1.2 Цели и задачи

Целта на изследването дефинирана в работата е „въз основата на анализ и синтез на системите на водещи държави, съюзи и организации да се синтезира усъвършенстван модел на национална система за кибер сигурност съгласно новите тенденции за киберпространството“ . Произтичащите от тази цел задачи са формулирани точно и ясно, именно:

- Изследване на модели за специализирани структури за противодействие на киберзаплахи с анализ и оценка на общите и специфичните елементи, необходими при архитектурата за киберсигурност в отбраната на страната и водещи модели в света (САЩ, Германия, ЕС, НАТО)
- Анализиране на състоянието, основните и специфичните характеристики, организационните архитектури и функционалните способности на съвременните модели на киберзащита.
- При отчитане на националните особености и възможности, да се създаде архитектурен модел на високо ниво, за киберзащита на страната, заедно със съответните функционални, технологични и управленски функции на отделните му елементи и взаимодействието им със съответните международни киберорганизации и киберсистеми по линия на НАТО и ЕС.

Така дефинираните цели са целесъобразни и реализуеми.

1.3. Структура на дисертационния труд

В Увода авторът описва общата концепция на научното изследване и формулира целта, задачите, обекта и предмета на изследване, научно-изследователските задачи, методите

излолзвани в изследването, ограничения, полезност и предизвикателства и инструментариумът използван в изследването.

В глава първа от дисертационния труд авторът прави анализ на системите за киберсигурност на САЩ, Германия и Русия. Проследен е пътя на еволюция на националните киберинтереси на САЩ и са идентифицирани трите стратегически цели: (1) предотвратяване на кибератаките срещу националните критични инфраструктури; (2) намаляване на националната уязвимост към кибератаки; и (3) свеждане до минимум на щетите и времето за възстановяване от кибератаките. Представена е структурната схема на американското киберкомандване към 2015 г. и 2017 г., а така също и мястото на кибер командването и киберелементите в департамента за вътрешна сигурност на САЩ. Представени са архитектурата и функционалната схема на системата за киберсигурност на САЩ.

В извършения анализ на киберстратегията на Германия авторът е идентифицирал основните стратегически цели, а именно: (1) Защита на критичната информационна единна инфраструктура е основен приоритет; (2) Създаване на сигурни ИТ системи; (3) Повишаване на информационната сигурност в публичната администрация; (4) Създаване на Национален център за реакция при киберзаплахи; (5) Създаване на Национален съвет по киберсигурност; (6) Ефективен контрол на киберпрестъпността; (7) Координиране на действията с ЕС и НАТО за осигуряване на достатъчно безопасно киберпространство; (8) Използване на надеждни информационни технологии; (9) Развитие на човешките ресурси; (10) Разработване на инструментариум (организационен и технически) за отговор на кибератаки. Представена и анализирана е структурата на киберкомандването на Германия както и е изследвана системата й за киберсигурност.

Извършен е анлаиз на системата за киберсигурност на Русия и са предложени следните изводи: (1) Руската система за киберсигурност е изградена като строго йерархична структура; (2) Липсват методология и правила за привличане на публични-частни отношения и бизнес организации; (3) Липсва функционална гъвкавост в мирно и военно време; (4) Липсват комуникации с други организации и съюзи; (5) Кибероперациите са на ниво водене на

военни операции и защита на националните (федерални) военни органи и структури. Разгледана е и е анализирана ролята на кибермента във военната система на Руската Федерация.

Във втора глава от дисертационното изследване, авторът е анализирал системите за киберсигурност на НАТО и ЕС. Разгледал е организационните структури и възгледите на НАТО за киберсигурността и е обособил приоритетите на НАТО в областта на киберсигурността. Авторът е анализирал проблемите за киберсигурността на ниво ЕС като е идентифицирал основните стратегически приоритети: (1) постигане на устойчивост на киберпространството; (2) драстично намаляване на престъпленията в кибернетичното пространство; (3) разработване на политика за киберотбрана и изграждане на капацитет във връзка с Общата политика за сигурност и отбрана (ОПСО); (4) развитие на индустриални и технологични ресурси за киберсигурност; (5) създаване на последователна международна политика на Европейския съюз за киберпространството и насърчаване на основните ценности на ЕС.

Глава три от дисертационния труд е посветена на въпроса за повишаване на способностите на системата за киберсигурност на национално ниво и на МО и БА. Представени иса анализирани основните завена имащи иотношение към киберсигурноста в Република България, разгледани са основните регламентиращи документи и изградените на тази основа взаимовръзки, направен е анализ на състоянието на системата за киберсигурност, предложена е архитектура на национална система за киберсигурност, идентифицирани са слабостите и възможните направления за развитие. На основата на така дефинираните системи и елементи е извършен сравнителен анализ между разглежданите системи за киберсигурност. Предложена е струура и функционално характеристики на Военен център за киберотбрана.

В частта "Заключение" са систематизирани и обобщени резултатите получени в дисертационното изследване.

1.4. Използвани литературни източници

Докторантът е проучил и използвал 128 литературни източници на български и английски език. Цялостното изложение на

дисертационното изследване показва, че докторантът има широк поглед върху състоянието на проблема и говори добре за неговата висока теоретична и практическа осведоменост.

2. Аналитична характеристика на дисертационния труд

Дисертационния труд има теоретико-приложен характер. Теоретичността се определя от подходите и начините използвани от докторанта за формулиране, формализиране и търсене на решение за повишаване на киберсигурността и отбраната на КИС в МО и БА. Приложния характер на дисертацията е определен от задачите, свързани с изпълнението на целта на изследването, подхода за тяхното решаване, както и от получените приложни резултати.

3. Приноси в дисертационния труд

Дисертационният труд притежава приноси с научно-приложен и приложен характер. Научно-приложните приноси могат да се обобщят като доразвиване на знанието в областта на подходите за анализ и оценка на системите за киберсигурност и начините за структуриране на архитектурни и функционални модели на системи за кибер сигурност. Получените резултати в изследването показват приложимостта и съдържателността им за решаване на практически задачи, свързани с моделиране, анализ и подход за повишаване на киберсигурността и отбраната на КИС в МО и БА.

4. Публикации и цитирания

Представени са три публикации като и във трите дисертантът е самостоятелен автор. Едня от публикациите е представена в списание CIO, а другите две са представени в научни конференции.

5. Авторство на получените резултати

От представените публикации може да се направи извода, че дисертационният труд и получените в него резултати са лично дело на докторанта.

6. Автореферат и авторска справка

Авторефератът вярно и точно отразява дисертационния труд, а именно: заглавието, целта, поставените задачи, приносите на автора, получените фактически данни, изводите и списъка на публикациите на автора по темата на дисертацията.

7. Бележки по дисертационния труд

Нямам забележки и препоръки, които да поставят под съмнение получените резултати и приноси. Въпросите на които не мога да получа отговор от съдържанието на дисертационния труд са:

- До каква степен предложените в дисертационното изследване структури за киберсигурност са в синхрон със закона за киберсигурност и съществуващите киберструктури в МО и БА?

Препоръките, които си позволявам да отправя към докторанта са:

- В дисертационният труд няма общоприет термин за използване на понятието киберсигурност и неговите производни. На много места се използва понятието кибернетична сигурност и др. С цел по-голяма терминологична чистота е желателно да се съобразим с наложените понятия в закона за киберсигурност и те да бъдат използвани в цялото изследване.
- В бъдещата си работа авторът да положи усилия за публикуване на съществуващите и бъдещи резултати в реномирани научни издания у нас и в чужбина, а така също и видимост на работата в екип.

Цялостната ми оценка за дисертационния труд е положителна. Дисертантът демонстрира познаване на предметната област и подход и практически знания и умения за реализирането в практиката на предложените от него решения.

Заключение

Като обобщение на гореизложеното, считам, че са изпълнени всички условия и изисквания на Закона за развитие на академичния състав в Република България и правилника към него за присъждане на образователна и научна степен "доктор" и давам с убеждение **положителна оценка** на кандидата **Красимир Стайков Коев** като предлагам на уважаемото научно жури да присъди **образователната и научната степен „доктор”** в **област на висшето образование 9. „Сигурност и отбрана “, професионално направление 9.1. „Национална сигурност “, докторска програма „Киберсигурност“.**

21.02.2019 г. Рецензент:

гр. София полк. доц. д-р Николай Стоянов