РЕЦЕНЗИЯ

на дисертационен труд
за придобиване на образователната и научна степен "доктор" в

област на висше образование – 5. Техчниески науки
професионално направление – 5.3 Комуникационна и компютърна техника
докторска програма – „Комуникационни мрежи и системи“

Автор: маг. Искрен Павлинов Янков
Тема: Иновативност, методология и проектиране на модел за киберотбрана и киберсигурност на комуникационните мрежи и системи на държавни структури и учреждения
Рецензент: доц. д-р инж. Боян Димитров Карапенев, Технически университет - Габрово

1. Тема и актуалност на дисертационния труд

Ускорената дигитализация в Република България през последните години налага разработването, внедряването и усъвършенстването на съвременните комуникационно-информационни технологии, системите за управление и анализ на големи масиви от данни (BigData) и все по-широко използваните форми на изкуствен интелект, IoT, Индустрия 4 и др. След бурното и бързо развитие на дигитализацията в Р. България след 2012 г. с навлизането на цифровата телевизия възниква въпросът за осигуряването на киберсигурност и надеждна защита в държавните, корпоративните, учрежденските и фирмените мрежи и системи от злонамерени заплахи и пробиви, идващи от глобалната мрежа Интернет.

В настоящия момент тематиката на дисертационния труд е много актуална, тъй като всяка една държавна и частна организация влагат значителни капиталовложения за осигуряването на сигурна и надеждна киберзащита на своите системи и информационни масиви. Рисковете за безопасността са предпоставка за значителни финансови, икономически, а също така и морални загуби и щети.

Съвременните изисквания и регулации налагат на организациите да не допускат изтичането на лична и конфиденциална информация и данни. Създаването на методологии за организация на защитата на мрежи и системи осигуряват ефективна реализация на противодействието срещу киберзаплахи и кибератаки.

Обектът на разработения дисертационен труд е теоретично и експериментално изследване на методите и средствата за повишаване на киберсигурността в комуникационно-информационните мрежи и системи на държавни структури и учреждения чрез прилагането на организационни, образователни, административни и технически мерки и нови решения, водещи до минимизиране на риска, въпреки съществуващите защитни механизми. Идентифицирането на рисковете за информационните ресурси е сложен и динамичен процес, базиран на непрекъснат мониторинг на компютърните мрежи и системи за откриване на потенциални заплахи в информационната сигурност и киберзащита.

В дисертационния труд ясно и точно са дефинирани мотивите, обектът, предметът, целта, средствата и задачите за изпълнение и съдържанието на отделните глави напълно им съответства.

2. Обзор на цитираната литература

В справката за използваната литература са приложени общо 128 литературни източника, от които 56 на български език, 64 на английски език и 8 web-адреса. Около 20% от тях са издадени през последните 5 години.

Не всички посочени литературни източници са цитирани в записката.

3. Методика на изследване

По проблематиката на разработваната тема дисертантът работи от 2016 г. и за времето до настоящия момент той успешно се справя с предизвикателствата, свързани с осигуряването на киберсигурността в комуникационните мрежи и системи. Методологията на изследванията включва теоретично и експериментално разглеждане на методите и инструментите за подобряване на киберсигурността, предлагайки нови авторски решения за намаляване на риска. Направен е анализ на значими кибератаки в исторически план, оценена е настоящата регулаторна рамка и е предложен модел за намаляване на рисковете. Дисертационният труд комбинира обзор на повече от 128 литературни източници, основно публикации на статии и доклади, анализи и разработването на модел(и) и методологии за постигането на повишена киберсигурност на комуникационно-информационните мрежи и системи с непрекъснато адаптиране на организационните, административните и техническите мерки за нейното осигуряване.

Предмет, цел и задачи на научното изследване

Предметът на изследването е управлението на информационната сигурност при възникване на заплахи за информационните ресурси в държавните организации, разглеждани като локални обекти. В рамките на изследването са разгледани методите за управление на информационната сигурност чрез симулиране на компютърни атаки от типа „отказ на обслужване“ (DoS) и „Ransomware“ върху локални структури. Целта е да се предоставят доказателства за подобряване на информационната сигурност чрез ефективни механизми за откриване и предотвратяване на атаки от типа „отказ на обслужване“ и „Ransomware“, като се подчертава значението на навременната реакция и адекватните мерки за защита.

Основната идея на извършените изследвания е, че надеждното управление на информационната сигурност може да осигури приемливо ниво на киберзащита и киберотбрана в компютърните мрежи и системи. Изграждането на хибриден модел, съчетаващ облак, разполагането на On-Prem центрове за възстановяване на информационните услуги след бедствия и създаването на единна система, която свързва всяка държавна структура както помежду им, така и с държавния кибероблак в напълно защитена и криптирана среда, може да гарантира цялостната сигурност на една държава.

Целта на дисертационния труд е да оцени уязвимостите на държавните структури при различни сценарии на кибератаки, като се проведат симулации на атаки от типа „отказ на обслужване“ (DoS) и „Ransomware“ в контролирани експериментални условия. Чрез изследване на възникналите уязвимости, се цели да се обоснове необходимостта от изграждане на интегрирана система за защита на локално и глобално ниво.

За постигане на целта авторът е формулирал и решил следните **задачи**:

1. Идентифициране и анализ на рисковете при използване на компютърни мрежи: Провеждане на теоретично изследване и анализ на съществуващите заплахи за информационните ресурси. Оценка на факторите, допринасящи за възникването на уязвимости в компютърните мрежи и системи на държавните институции.Изследване на глобалното киберпространство и разкриване на уязвимостите: Анализ на технологичните и мащабните заплахи, с акцент върху факторите, допринасящи за развитието на кибератаките на глобално и локално ниво. Оценка на влиянието на тези заплахи върху информационната сигурност на държавните структури.

2. Разработване на иновативен модел за информационна сигурност: Създаване на модел за защита, базиран на съществуващите теоретични и практически подходи в областта на информационната сигурност и киберотбраната. Моделът трябва да интегрира разнообразни методи и технологии, които да осигуряват ефективна защита както на локално, така и на глобално ниво.

3. Симулиране на компютърни атаки от типа „отказ на обслужване“ и „Ransomware вирус“ с извършване на експериментални симулации на атаките с цел да се оцени тяхното въздействие върху информационните и комуникационните ресурси на държавните структури, както и тяхната уязвимост при различни сценарии на кибератаки.

4. Оценка на функционалността и практическото действие на иновативния проект, който да осигури висока степен на защита на информационните ресурси и непрекъснатост на услугите в държавните институции. Формиране на политики и процедури за защита срещу киберзаплахи. Разработване на комплекс от политики, методология и механизми, които да осигурят ефективна защита срещу локални и глобални киберзаплахи.

Целта на научните изследвания включва идентифициране и анализа на рисковете за информационната сигурност в компютърните мрежи и системи на държавните институции, разработването на иновативен модел за киберзащита, който интегрира различни технологии и подходи за локална и глобална защита, симулационни изследвания на атаки, като „отказ от услуги“ и „криптовирус“, оценяване на уязвимостите и изготвяне на комплекс от политики и процедури, които да осигурят висока степен на защита и непрекъснатост на услугите в глобалните мрежови системи и структури, изследване и анализ на функционалността на отделни компоненти на предложения модел.

Средата на изследване е лабораторна, в която се използват огнитивни методи и системи за киберзащита и киберотбрана, като включва модели на Cisco Meraki MX, Cisco Meraki Cloud и Cisco Umbrella. Тази методология предлага иновативно решение за хибридно използване на локална и държавна облачна структура за защита на локални и глобални системи, осигурявайки цялостна защита при кибервойни. Решава се проблемът, при който държавите се стремят към глобална защита на системите си, но често пренебрегват локалната защита. Комбинирането на различни защитни системи позволява осигуряването на адекватна защита както при целева атака срещу отделна държавна структура, така и при мащабна глобална кибервойна.

Използваните методи за изследване са аналитични, симулационни и практически, и обхващат получаване на зависимостите на параметрите и характеристиките, получени от реализацията на предложения модел(и).

Използваната методика на изследване - обзор на киберсигурността и литературно проучване; анализ и оценка на системите за киберсигурност на различни държавни и частни учреждения, анализ на различни кибератаки в исторически план; предложеното проектно решение (хибриден модел) за повишаване на киберсигурността; резултати и анализ от симулиране на компютърни атаки от различен тип - успешно води до постигане на поставената цел и изпълнение на поставените задачи в дисертационния труд.

4. Оценка на изложението в дисертационния труд

Структурата на дисертационния труд има общ обем от 121 страници и включва въведение, глава 1 - Обзор на киберзащитата и сигурността в компютърните системи и мрежи, в края на която са формулирани задачите за изпълнение, глава 2 - Идеен проект за осигуряване на киберзащита и сигурност в компютърна система, свързана с глобалната мрежа на една държава, глава 3 - Симулационно изследване и анализ на атаките „отказ от услуги” и „криптовирус” и разглеждане на механизмите на заразяване, глава 4 - Оценка на функционалността и методологията на иновативния проект за кибер отбрана на Държавни структури и учреждения, Анализи и изводи, Справка за основните приноси, Научна новост и приложимост на разработката, Списък на публикациите по тематиката и Използвана литература.

5. Приноси на дисертационния труд

Приносите в дисертационния труд, според неговото съдържание и представените, напълно съвпадат с моето мнение и се свеждат до:

Научно-приложни приноси

1. Извършен е обзор на киберсигурността, проучена е съществуващата нормативна база в Р България и в чужбина и е направен анализ на значими кибератаки срещу държавни и частни учреждения в исторически план. Изследвано и е анализирано въздействието на различен зловреден софтуер (компютърни атаки) върху функционалността на компютърните системи и мрежи.

2. Разработена е и е емпирично потвърдена концепцията, че интегрирането на локални защитни механизми в единна глобална система за киберсигурност значително повишава ефективността на защитата срещу съвременни киберзаплахи.

3. Предложен е нов модел, при който локалните и глобалните защитни системи работят синхронизирано при трансфера и защитата на данните, осигурявайки непрекъснатостта и надеждността на процесите.

4. Предложеният модел позволява ефективно взаимодействие между локални и облачни инфраструктури, използвайки криптирани комуникационни тунели, което гарантира целостта и сигурността на данните.

Приложни приноси

1. Направен е анализ и е изследван всеки един от компонентите на предложения нов модел, с което е доказана работоспособността на подхода за киберзащита на локални и глобални точки, като са изследвани времевите граници от заразяване на системата и засичането на заплахите до тяхното неутрализиране.

2. Към предложения модел е разработен алгоритъм за криптиране на информацията в комуникационните тунели, за да се гарантира надеждността на връзката и целостта на данните.

3. Идентифицирана е възможността за дефиниране на киберотбраната на системите по три подхода: подход с локална защита, чрез системите на Cisco Meraki MX, Cisco Umbrella, Cisco Defense Orchestrator, която е изцяло облачна, и подход в облачния модул Cloud Security Device Connector, чиято локална защита прераства в Държавна Облачна структура на Киберотбраната. Третият подход е чрез изграждането на два вида Центрове за възстановяване след бедствия.

4. Разработени са схеми и топологии с аналитична последователност за прилагане на модела, както и са описани етапите и методиката на действия, за да бъдат осигурени изходни данни за създаването на система за киберотбрана и киберзащита, адаптивни към всяка една инфраструктура.

6. Публикации и цитирания на публикации по дисертационния труд

По тематиката на дисертационния труд са направени и представени 5 самостоятелни публикации - 1 доклад на Международната научна конференция ICTACSE 2018 (Истанбул) - на английски език, 1 доклад на Международния симпозиум на САИ „Джон Атанасов" 2022 (София) и 3 доклада на Националната научна конференция с международно участие „TechCo" 2023 и 2024 г. Броят на направените публикации (доклади) отговаря на Правилника за развитието на академичния състав на ТУ-Габрово. Не е представена информация за известни цитирания от други автори на приложените публикации към дисертационния труд. Не е приложен списък и с други публикации на дисертанта, ако има такива.

Считам, че публикациите на докторанта, представени в дисертационния труд, съдържат основните приноси, за които претендира.

7. Авторство на получените резултати

Направените публикации, както и структурата и съдържанието на дисертационния труд ми дават основание да считам, че несъмнено кандидатът е нейн автор. Той е придобил голям професионален опит в областта на информационните системи и киберсигурността.

8. Автореферат и авторска справка

Авторефератът е представен в обем от 53 страници и правилно отразява структурата, съдържанието на дисертационния труд, приносите и направените публикации на кандидата.

9. Мнения, препоръки и забележки по дисертационния труд

Препоръки:

- В изложението на дисертационния труд е дадена същността на основни понятия и дефиниции, свързани с киберсигурността, които увеличават обема на обзорната част;

- От изложението в дисертационния труд не става ясно дали са извършени симулационни и/или реални изследвания и получени резултати за функционирането на предложения модел, или на отделни негови компоненти, за киберотбрана и киберсигурност на комуникационните мрежи и системи;

- Стилът на изложението на места би могло да бъде подобрен.

Препоръчвам предложеният иновативен и хибриден модел по възможност да бъде практически внедрен, изследван, анализиран и оптимизиран при необходимост.

Също така препоръчвам на дисертанта да продължи и още повече да задълбочи работата си по тематиката на дисертационния труд и обогати със своите публикации научните достижения в областта на киберсигурността в съвременните комуникационно-информационни мрежи и системи.

Положителни страни:

- Тематиката е разгледана и представена в голяма дълбочина на анализа и изследването и обобщава и предлага специализирана работа и разработка в областта на киберотбраната и киберсигурността в комуникационните мрежи и системи и в частност на държавни структури и учреждения;

- Впечатление правят много добре обобщените дефинирани и представени изводи към отделните глави, както и заключението и насоките за бъдещото развитие на тематиката и приложението на получените резултати в дисертационния труд;

- Добро впечатление правят изработените с програмни продукти и представени фигури, най-вече структурни и блокови схеми, в изложението.

Дисертационният труд, авторефератът, направените публикации, анализи и изводи и постигнатите научно-приложни и приложни приноси показват несъмнено, че авторът й маг. Искрен Павлинов Янков притежава способности към задълбочени литературни и теоретични анализи и изследвания, базиращи се на богат и специализиран професионален опит в областта на информационните системи и киберсигурността. Това характеризира дисертанта като тесен специалист в областта на киберотбраната и киберсигурността с възможности за бъдещо развитие.

Темата на дисертационния труд е много интересна и актуална. Работата има достатъчен обем и дълбочина на изследването. Получените резултати са достатъчно значими за придобиване на образователната и научна степен „Доктор”. Публичността на работата е достатъчна. По дисертационния труд от автора са направени 5 публикации.

10. Заключение

Считам, че представеният дисертационен труд **отговаря** на изискванията на Закона за развитие на академичния състав в Република България. Постигнатите резултати ми дават основание **да предложа** да бъде придобита образователната и научна степен „доктор” от маг. Искрен Павлинов Янков, в област на висше образование – 5. Технически науки, професионално направление – 5.3 Комуникационна и компютърна техника, докторска програма – „Комуникационни мрежи и системи“.

16.12.2024 г. **Рецензент**: /п/

/доц. д-р инж. Боян Карапенев/