СТАНОВИЩЕ

за дисертационен труд
за придобиване на образователната и научна степен „доктор“ в

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

Автор: маг. Искрен Павлинов Янков
Тема на дисертационния труд: „Иновативност, методология и проектиране на модел за киберотбрана и киберсигурност на комуникационните мрежи и системи на държавни структури и учреждения”
Член на научното жури: доц. д-р инж. Красен Киров Ангелов

1. Тема и актуалност на дисертационния труд

Дисертационният труд на маг. Искрен Янков е посветен на процесите, подходът и моделите за разработване и внедряване на адаптивни системи за превенция и защита срещу кибератаки и хибридни заплахи чрез интегрирани методологии и технологични решения. С оглед на значимостта на защитата на комуникационните мрежи и системи на държавни структури и учреждения, изследването в дисертационния труд е с иновативен характер и категорична гаранция за актуалността на проблематиката и реално предизвикателство за задълбочено дисертационно изследване.

Обект на изследване в дисертационен труд са компютърните мрежи и системи на държавни структури и учреждения и рисковете от локални поражения, въпреки съществуващите защитни механизми в държавните институции. Поставен е основен акцент на идентифицирането на рисковете за информационните ресурси, базиран на непрекъснат мониторинг на компютърните мрежи за откриване на потенциални заплахи за информационната сигурност. Този процес обхваща симулации на рискови ситуации, които служат за оценка на устойчивостта на мрежовите системи, по аналогия със стрес-тестовете, използвани за определяне на нивото на защита.

Структурата на дисертационния труд включва увод, четири глави, анализ и изводи, списък на използваните съкращения, справка на основните приноси, научна новост в дисертацията, списък на публикациите по темата на дисертационния труд, списък на използваната литература. Дисертационният труд, с обем от 119 страници, е разработен на база аналитичен обзор на 128 литературни източника, в т.ч. 57 на български и руски език, 63 на английски език и 8 интернет-базирани източника. Не всички изброени източници са цитирани в дисертационния труд.

Изложението в първата глава на дисертацията показва добро познаване от страна на дисертанта на състоянието и регулациите по отношение на киберзащитата и сигурността в компютърните системи и мрежи, основните глобални киберзаплахи и специфичните за България такива. Тези знания са позволили на дисертанта правилно да

анализира и оцени съвременното състояние на проблема и да формулира целите на изследванията в дисертационния труд.

2. Методика на изследване

Дисертационният труд има за цел да разработи иновативен модел за киберотбрана и киберсигурност, базиран на съвременни подходи и технологии.

Методите за изследване в дисертационния труд са базирани на аналитични модели, имитационно моделиране във виртуална среда и експериментално изследване в изолирана реална среда. Като инструменти за имитационното моделиране във виртуална среда са ползвани бази данни специализирани платформи за виртуализация, специализирани скриптове, софтуерни инструменти за одит, филтрация, превенция, детектиране и защита от киберзаплахи, оценка на риска и др. Като инструменти за експерименталните измервания е използвана изолирана мрежова инфраструктура съвместно със специализирани инструменти за управление, мониторинг и визуализация. Избраната методика за изследване е адекватна.

Целта на изследването е анализ и оценка на: механизмите за осъществяване и протичане и противодействие на кибератаки; функционалността на индивидуалният план при атаки по различни структурни обекти; методологията и стратегиите, които следва да прилага една държава в своята киберотбранителна политика, с цел осигуряване на защита на всички държавни институции от кибератаки и кибервойни.

3. Приноси на дисертационния труд

Приносите в дисертационния труд може да се класифицират като научно-приложни и приложни, които най-общо могат да се формулират и обобщят по следния начин:

А) Научно-приложни приноси:

– Извършена е оценка на въздействието от значими кибератаки срещу държавни и частни учреждения в исторически план върху функционалността на компютърните системи и мрежи.

– Разработена е и емпирично е потвърдена концепция за значително повишаване ефективността на защитата срещу съвременни киберзаплахи чрез интегрирането на локални защитни механизми в единна глобална система за киберсигурност.

– Предложен е нов модел, при който локалните и глобалните защитни системи работят синхронизирано при трансфера и защитата на данни, осигурявайки непрекъснатост и надеждност на процесите.

– Създаден е новаторски модел, който позволява ефективно взаимодействие между локални и облачни инфраструктури, използвайки криптирани комуникационни тунели, което гарантира целостта и сигурността на данните в областта на киберотбраната на държавно ниво.

Б) Приложни приноси:

– Изследван е 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.

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

– Идентифицира се 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 в облачен модул Cloud Security Device Connector. Тази локална защита прераства в Държавна Облачна структура на Киберотбраната и третият подход е чрез изграждането на два вида Центрове за възстановяване след бедствия.

– 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.

4. Публикации и цитирания на публикации по дисертационния труд

Резултатите от дисертационния труд са обнародвани в 5 публикации: 4 на български език и 1 на английски език. Всички публикации са самостоятелни. Една от представените публикации е докладвана на Международна конференция по теоретични и приложни компютърни науки и инженерство – Истанбул, Турция, 2018 г.(International Conference on Theoretical and Applied Computer Science and Engineering – ICTACSE 2018). Останалите 4 публикации са доклади на конференции, отчетени в Националния референтен списък на съвременни български научни издания с научно рецензиране: 1 от тях изнесен на XXX Международен симпозиум на САИ „Джон Атанасов, София, 2022 г.; останалите 3 публикации са доклади на национална научна конференция TechCo 2023 г. и 2024 г.

В публикациите са обнародвани извършените изследвания и са изложени основните изводи от дисертационния труд. Няма информация за известни цитирания на публикациите на дисертанта, както и за публикации реферирани и индексирани в световни бази данни Scopus.

Публикационната дейност на докторанта покрива минималните национални изисквания и изискванията на правилника за придобиване на образователна и научна степен „Доктор“.

5. Авторство на получените резултати

От представените публикации, както и от изложението на дисертационния труд се вижда, че е реализиран значителен обем от научно-изследователска и експериментална дейност от докторанта под ръководството на неговия научен ръководител. Представените резултати надграждат съществуващите до момента подходи, методи, модели и архитектури за киберотбрана и киберсигурност на комуникационните мрежи и системи на държавни структури и учреждения и доказват предложеният иновативен модел на архитектурата за информационна сигурност и киберотбрана на дадена държава и нейните структури.

Смятам, че основният дял от проведените изследвания и съставени анализи на резултатите са изцяло личен принос на докторанта.

6. Мнения, препоръки и забележки по дисертационния труд

Темата на дисертационния труд е актуална и интересна. Считам, че работата има достатъчен обем и необходимата дълбочина на изследването. Получените резултати са достатъчно значими за образователна и научна степен „доктор". Публичността на работата е осигурена и доказана с публикации на доклади в реферирани научни конференции.

Към дисертационната работа имам следните по-съществени забележки и препоръки:

1) Големият обем от абревиатури предполага един по-широк списък на използваните съкращения.
2) Част от изводите в Глава 1, 2 и 3 имат констативен и общоприложен характер и следва да се прецизират по отношение на предложеният иновативен модел за киберотбрана и киберсигурност, базиран на съвременни подходи и технологии.
3) Глава 3 би могла да бъде по-прецизно и ясно интегрирана към общата разработка в дисертационния труд.
4) Препоръчвам на докторанта да обнародва извършените от него изследвания и постигнати резултати в престижни научни списания и международни научни конференции индексирани в световно известните бази от данни на Scopus/Web of Science.

Представените забележки и препоръки не омаловажават постигнатите от докторанта резултати по научната тематика в дисертационния труд.

7. 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".

13.12.2024 г. **Член на научното жури: /п/**

гр. Габрово /доц. д-р инж. Красен Ангелов/