

РЕЦЕНЗИЯ

**на 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: 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: проф. д-р инж. Пламен Златков Захариев, Русенски Университет „Ангел Кънчев“

1. Тема и актуалност на дисертационния труд

Проектирането на ефективен модел за киберсигурност и информационна защита в комуникационните мрежи и системи на държавните структури и институции изисква цялостен подход, който включва не само прилагането на иновативни технологии, но и използването на стабилна методология за гарантиране на сигурност, както и въвеждането на многослойна отбранителна стратегия за справяне с уникалните предизвикателства, пред които тези организации са изправени.

Съвременните кибератаки стават все по сложни и са базирани на усъвършенствани средства за атака, като софтуерни средства за изнудване на потребителите чрез криптиране на техните данни (т.н. рансъмуер), атаки със заблуда на потребителите (т.н. фишинг атаки), атаки с посредници, изтичане на данни и др. За противодействие на тези атаки, много организации използват съвременни технологии, като изкуствен интелект, машинно обучение и архитектури с нулево доверие (т.н. zero-trust архитектури). Все по-сложната и разрастваща се област на киберпрестъпленията и увеличаващата се нужда от специалисти в сферата на киберсигурността превръщат гарантирането на информационната конфиденциалност, цялостност и достъпност в постоянно и много сериозно предизвикателство.

Всичко това определя киберсигурността и киберотбраната като ключови направления в информационната сигурност и прави темата на дисертационния труд изключително актуална и значима за съвременното общество.

2. Обзор на цитираната литература

При подготовката на дисертационния труд са използвани общо 128 литературни източника. Шестдесет и три (63) от източниците са на английски език, а петдесет и седем

(57) са на български език. Използвани са общо осем (8) източници от Интернет пространството. Голяма част от литературните източници са книги, включително такива на световноизвестни издателства, като Springer, O'Reilly Media, Oxford University Press, Pearson, John Wiley & Sons, Wiley, Prentice Hall и др. Част от използваните литературни източници на български език са на университетски издателства.

В дисертационния труд е направен обзор, включващ източници и материали, публикувани основно през последните 10 години. Считаю, че докторантът е навлязъл в същността на изследваната предметна област и мога да заключа, че чрез анализа на литературните източници е постигната коректна формулировка на целта на дисертационния труд и на основните задачи свързани с нейното постигане.

3. Методика на изследване

Дисертационният труд е изготвен в общ обем от 119 страници и включва 68 фигури и графики. Направена е ясна и коректна формулировка на предметната област, обекта на изследване, целта и задачите на дисертационния труд. Структурата на дисертацията включва последователност от четири глави с формулирани изводи за всяка една от тях. Направени са общи изводи по дисертационния труд и са изведени обобщени научно-приложни и приложни приноси.

В Първа глава на дисертационния труд са анализирани основните видове кибератаки, видовете зловреден софтуер и мерките за намаляване влиянието на атаките или за предпазване от тях. Извършен е фактологичен преглед и анализ на киберзаплахите, които са възникнали в България през годините. Дефинирана е целта на дисертационния труд и са формулирани конкретни задачи за нейното постигане.

Във Втора глава на дисертационния труд е представен иновативен идеен проект за създаване на многослойна система за киберзащита на държавните структури и институции, който включва етапи по изграждане на локални и облачни зони на защита, създаване на цялостна методология за киберотбрана и създаване на разпределени взаимосвързани информационни центрове.

В Трета глава от дисертационния труд са извършени аналитични изследвания на популярни съвременни кибератаки. Синтезирани са методи и средства за симулационно изследване на атаки с отказ на услуги и атаки за изнудване на потребителите чрез криптиране на техните данни. Формулирани са правила, процедури, модели и методи за предотвратяване на изследваните кибератаки и за повишаване на сигурността в комуникационните и мрежовите системи.

В Четвърта глава от дисертационния труд е предложен модел за киберотбрана на държавни структури и учреждения и е направена оценка на неговата функционалност. Представени са различни атаки срещу разпределени облачни системи и информационни

центрове. Дискутирани са международни и национални стратегии и стандарти за киберсигурност и киберотбрана.

Дисертационният труд завършва с общи изводи по проведените изследвания и с представяне на научната новост на разработките на инж. Янков.

4. Приноси на дисертационния труд

На база приложената справка за приносите на дисертационния труд, предлагам те да бъдат предефинирани, обобщени и представени като научно-приложни и приложни, както следва:

1. Формулирана и доказана е хипотезата, че интегрирането на локални защитни механизми в единна глобална система за киберсигурност значително повишава ефективността на защитата срещу съвременни киберзаплахи.
2. Представен е нов иновативен модел, при който механизмите за локална и глобална защита си взаимодействат при трансфера и защитата на данните и гарантират непрекъснатостта и надеждността на комуникационните процеси.
3. Представен е нов иновативен модел за ефективна комуникация между локалните и облачните инфраструктури на държавни институции, в който се използват криптирани тунели за свързаност с гарантиране на цялостността и сигурността на предаваните данни.
4. Анализирани са алгоритми за шифриране на информацията в комуникационните тунели, чрез които се гарантира надеждността на връзката и цялостността на данните.
5. Формулиран е трислоен модел за киберотбрана на държавни институции, който включва подход за локална защита чрез специализирани комуникационни системи, допълнителна защита на информацията чрез използването на облачни платформи, както и гарантиране на цялостна защита чрез изграждането на разпределени информационни центрове за данни.
6. Направено е проучване на всеки един от елементите на представения модел и е доказана работоспособността на подхода за киберзащита на локалните и глобалните елементи в него, като са изследвани времевите диапазони от момента на провеждането на атаките срещу системите и тяхното засичане до момента на неутрализирането им.

7. Разработени са схеми за прилагане на модела за киберотбрана на държавни институции и са описани етапите и последователностите на действията за създаване на система за киберотбрана, която може да се адаптира към нуждите на всяка една инфраструктура.

5. Публикации и цитирания на публикации по дисертационния труд

Към дисертационния труд са представени общо 5 публикации, както следва:

[A.1] I. Yankov, Research of the network infrastructure for maintenance of big data bases, Международна научна сесия ICTACSE 2018 – Winter Virtual Conference, 23-24 ноември 2018, Истанбул; Участие с доклад, получен сертификат;

[A.2] И. Янков, Осигуряване на киберзащита и сигурност в компютърна система, свързана с глобалната мрежа, Сборник доклади: XXX Международен симпозиум на САИ „Джон Атанасов“, с. 53-56, 10-11 ноември 2022 г., гр. София; Симпозиума е включен в НАЦИД;

[A.3] И. Янков, Кибер война – унищожителни действия без оръжия. Съвременна методология на Кибер отбраната, Сборник доклади: VII Национална научна конференция с международно участие ТК Ловеч „TechCo 2023“, с. 167-171, 30 юни 2023, гр. Ловеч; Конференцията е включена в НАЦИД;

[A.4] И. Янков, Осигуряване на сигурност на компютърните мрежи и механизми за тяхната защита, Сборник доклади: VII Национална научна конференция с международно участие ТК Ловеч „TechCo 2023“, с. 115-119, 30 юни 2023, гр. Ловеч; Конференцията е включена в НАЦИД;

[A.5] И. Янков, Съвременни кибератаки в сектора на здравеопазването. Практически методи за превенция и защита, Сборник доклади: VIII Национална научна конференция с международно участие ТК Ловеч „TechCo 2024“, с. 148-152, 28 юни 2024, гр. Ловеч; Конференцията е включена в НАЦИД;

Представените публикации са самостоятелни. Една от публикациите е на английски език, а останалите публикации са на български език. Представените публикации покриват минималните изисквания за получаване на образователната и научна степен „доктор“.

Към дисертацията няма представени доказателства за известни цитирания на публикациите.

6. Авторство на получените резултати

По проблемите на дисертационния труд е извършена достатъчна по обем научноизследователска работа. В тази област продължава да се работи активно, което личи от използваните информационни източници.

Представените публикации по дисертационния труд и самата записка на дисертацията ми дават основание да считам, че получените в рамките на изследванията резултати са в голяма степен заслуга на докторанта Искрен Янков.

7. Автореферат и авторска справка

Авторефератът е в обем от 53 страници и представя точно основните изследвания и разработки в дисертационния труд, като представлява синтезирано негово обобщение, което дава пълна представа за практическата приложимост на получените от докторанта резултати.

8. Мнения, препоръки и забележки по дисертационния труд

Към представената версия на дисертационния труд и автореферата нямам съществени критични забележки и коментари.

Препоръчвам на докторанта да публикува по-активно резултатите от изследванията си в национални и международни списания и да продължава с изследванията си в тази изключително интересна и актуална предметна област.

9. 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 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.

Подпис: /п/
/проф. д-р инж. Пламен Захариев/