РЕЦЕНЗИЯ

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

област на висше образование – Технически науки
професионално направление – Комуникационна и компютърна техника
специалност – Комуникационни мрежи и системи

Автор: инж. Ивайло Данчов Николов
Тема: Управление на информационната сигурност в компютърни мрежи
Рецензент: проф. д.н. Иван Ганчев Гарванов, заместник-ректор по „Качеството на обучението и акредитацията“ и ръководител на катедра „Информационни системи и технологии“ в Университета по библиотекознание и информационни технологии, гр. София.

1. Тема и актуалност на дисертационния труд

Актуалността на дисертационния труд се определя от важността на разглеждания основен проблем – информационната сигурност в компютърни мрежи. Безспорната актуалност на темата на дисертационния труд произтича от масовото използване на компютърните мрежи и опасността от изтичане на информация от тях, както и възможността за загуба на информация. Сигурността на информацията в компютърните мрежи несъмнено е тема, която предизвиква голям интерес не само поради актуалността си, наложена от ежедневието ни, но и поради сериозността на последствията от тях.

Считам, че темата на дисертацията е изключително актуална и богата на предизвикателства. Докторантът Ивайло Николов е успял да обоснове тази актуалност и в резултат на направения анализ е откроил някои от нерешените проблеми. Смятам, че целта и задачите на дисертационния труд са коректно формулирани.

2. Обзор на цитираната литература

За целите на изследването докторантът е използвал общо 174 литературни източници. От тях 163 са публикации, книги и закони, а 11 са интернет страници. На български език са 68 източника, а на английски език – 106. По-голямата част от използваните източници са издадени в периода на обучение на докторанта (2014-2017 г.), което показва, че той активно е търсил най-новите изследвания по проблематиката на дисертационния труд. Част от цитираните публикации са публикувани в престижни международни списания с импакт фактор, което показва актуалността на проблема и задълбочеността на докторанта в неговите изследвания. Прави много добро впечатление цитирането на световно признати учени както от чужбина, така и от България. Цитирането на шест закона в дисертационния труд е съвсем нормално и

обяснимо от факта, че докторантът работи от дълги години в съдебната администрация и познава много добре нормативната база в страната. От всичко казано до тук става ясно, че докторантът познава много задачите, по които се работи както в страната, така и в чужбина по проблематиката на дисертационния труд. В хода на изложението на дисертацията докторантът се позовава коректно на тези литературни и виртуални източници. В резултат на всичко казано считам, че Ивайло Николов познава детайлно разработения в дисертацията проблем, използвал е широк набор от литература, въз основа на която анализира изследваната проблематика и прави коректни изводи и обобщения. Докторантът борави сполучливо с понятийния апарат по темата и притежава способност да прави логически обосновани и подплатени с научна тежест заключения.

3. Методика на изследване

Целта, задачите и методиката на изследването са формулирани точно и съответстват на темата на дисертационния труд. Формулираната цел съвпада с темата на дисертацията и е управление на информационната сигурност в компютърни мрежи чрез постигане на надеждно ниво на защита на информационните ресурси. Управлението на информационната сигурност е изследвана от гледна точка на атаките от типа „отказ на обслужване“ с цел постигане на приемливо ниво на сигурност на информационните ресурси.

За постигане на тази цел са формулирани четири задачи, които са реализирани във всяка една от главите на дисертационния труд. Те са коректно дефинирани и отговарят на заглавието и на изследователската цел.

Задача 1. Определяне на рисковете за информационната сигурност посредством провеждане на задълбочен обзор и анализ на съществуващите заплахи за информационните ресурси.

За решаването на задачата е изследвана същността на информационната сигурност въз основа на съществуващата теория и практика. Синтезирани са основните заплахи за информационната сигурност. Направен е задълбочен обзор на виртуалните мрежи като основа за последващи изследвания, като са описани и анализирани някои програмни средства за реализиране на симулационни изследвания.

Задача 2. Аналитично моделиране на заявките с оглед синтезиране на модел на информационна сигурност на база на известни методи от теорията и практиката в областта на информационната сигурност.

За решаването на поставената задача е направено теоретично изследване на трафика чрез неговия анализ при масово обслужване на заявки. Въз основа на разпределението на входящия информационен поток и възможностите за задръствания при обслужване на заявки е синтезиран аналитичен модел на системата. Компютърните атаки от типа „отказ на обслужване“ са базирани върху информационните потоци.

Задача 3. Създаване на симулационен модел на компютърни атаки от тип „отказ на обслужване" и провеждане на експериментални изпитания.

За решаването на тази задача е създаден симулационен модел за реализиране на компютърни атаки от типа „отказ на обслужване" в среда GNS3 и в реални условия.

Задача 4. Формулиране на политика за информационна сигурност на базата на получените резултати.

За решаване на задачата е формулирана примерна политика за информационна сигурност на базата на анализа на трафика в системите за идентифициране на инциденти. Представени са някои програмни решения.

Положително впечатление прави правилното използване на основните понятия и термини в областта на изследването. Материалът е онагледен с таблици, фигури и формули, които доказват или допълват тезата на автора. Дисертационното изследване е основано на резултатите, получени вследствие използването на няколко научно-изследователски подхода.

Методите за изследване са аналитични и експериментални, като докторантът умело ги прилага във виртуална среда за емулиране на различни мрежови устройства и типове трафици в мрежата, както и практическа реализация на атаки от типа „отказ на обслужване". За реализиране на изследванията са използвани следните софтуерни продукти за емулиране и наблюдение на устройствата: Graphical Network Simulator3, Wireshark, Microsoft Network Monitor ver. 3.4, Colasoft Capsa Network Analyzer, iPerf.

За установяване зависимостите при управление на информационната сигурност са генерирани някои от познатите атаки от типа „отказ на обслужване", чийто алгоритъм и начин на действие е подробно описан при реализиране на съответната атака. Избраният подход за работа позволява провеждането на обстойни анализи, повторяемост при обработката на данните и осигуряване прогнозиране на процесите при аналогични атаки от типа „отказ на обслужване". В резултат на проведените изследвания върху атаките от типа „отказ на обслужване" и възможността за проследяване на процесите са направени съответните изводи в края на всяка от главите.

4. Приноси на дисертационния труд

Приносът на автора бих го формулирал като **потвърждаване на известни факти, обогатяване на съществуващи знания с нови факти и разкриване на възможности за приложение на научните постижения в практиката.**

Приносите на дисертационния труд могат да се формулират като:

Синтезиран е графичен модел за управление на информационна сигурност и е направено математическо описание на масово обслужване на

заявки с цел елиминиране възможността за изпадане на системата в състояние „отказ на обслужване";

Създадена е опитна постановка и са получени експериментални резултати в мрежова симулационна среда. Реализирани са различни сценарии на атака върху някои от използваните комуникационни протоколи;

Доказан е експериментално принципът за провеждане на различни по предназначение IP базирани системи в състояние „отказ на обслужване", чрез "UDP flood" атаки при поточно предаване на медийни данни и са представени конкретни решения за минимизиране на последиците от атаките;

Разработен е алгоритъм за откриване и идентифициране на инциденти чрез прилагане на поведенчески модел и са предложени методи и средства на програмна реализация на система за откриване на инцидента.

Тези приноси са лично дело на докторанта и съдържат **научен и научно-приложен характер**. Поради актуалността на изследваните проблеми, свързани с информационната сигурност в компютърните мрежи, бих оценил разработките на кандидата като **приноси с приложение на научните постижения в практиката**.

5. Публикации и цитирания на публикации по дисертационния труд

Докторантът Ивайло Николов е публикувал части от дисертационния си труд в 10 научни публикации, като 3 са в съавторство с научните си ръководители и 7 са самостоятелни. За публикациите в съавторство не са приложени разделителни протоколи затова приемам приноса на авторите по равно. Наличието на публикации в съавторство показва, че той може да работи както самостоятелно, така и в колектив. Не са забелязани цитирания на тези публикации, но и по процедурите за „доктор" не се изискват такива.

6. Авторство на получените резултати

За личното участие на автора в получените резултати може да се съди по публикациите, приложени към дисертационния труд. Седем от публикациите са самостоятелни, в 3 публикации има 1 съавтор, като в 1 от тях е първи автор и в 2 е втори. Резултатите, представени в дисертацията са авторски и дело единствено на докторанта. В дисертационния труд не е забелязано плагиатство. След направена проверка за плагиатство със системата Plagiat Finder също не бяха открити дубликати. Използваните от автора текстове са коректно цитирани. Личните приноси са ясно отделени и формулирани.

7. Автореферат и авторска справка

Авторефератът към дисертационния труд вярно и точно отразява неговото съдържание, той напълно изпълнява функциите си съгласно ЗРАСРБ. В автореферата са описани основните части на дисертацията. Особено внимание е отделено на получените резултати, направените изводи и получените приноси от автора, както и списъка с неговите публикации.

Заличено обстоятелство, на основание чл.2 от ЗЗЛД

8. Забележки по дисертационния труд

Препоръчвам на автора да се опита в бъдеще да публикува в международни конференции и списания по възможност реферирани в международните бази от данни Scopus и Web of Science.

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 **инж. Ивайло Данчов Николов** в област на висше образование – Технически науки, професионално направление – Комуникационна и компютърна техника, специалност – Комуникационни мрежи и системи.

01.04.2018 г.

Заличено обстоятелство, на основание чл.2 от ЗЗЛД

Подпис:
/проф. д.н. Иван Гарванов/