СТАНОВИЩЕ

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

в област на висше образование – Технически науки
професионално направление – 5.3 Комуникационна и компютърна техника
специалност – Комуникационни мрежи и системи

Автор: маг. инж. Ивайло Данчов Николов
Тема: Управление на информационната сигурност в компютърни мрежи

Член на научното жури: доц. д-р инж. Пенчо Колев Пенчев

1. Тема и актуалност на дисертационния труд

Развитието на Интернет, като основен елемент от комуникационната инфраструктура в световен мащаб се оказва невъзможно без реализацията на ефективни механизми за информационна защита, включително защита от Интернет атаки и механизми за тяхното предотвратяване.

Огромният обем от информация изисква използването на адекватни методи и средства за нейното опазване. От друга страна усъвършенстването на методите за комуникация, респективно обмяната на информация, поставя нови изисквания към информационната сигурност на едно по-високо ниво, изискващо ангажиране на научната общност в решаване на проблемите, свързани с опазване на информацията.

Информационната сигурност е в основата на икономическия растеж – липсата на информация, на знания, на технологии води до намаляване на печалбите на фирмите в конкурентна среда и обратното – наличието на информация, актуална, своевременна и надеждна се явява в основата на развитието на научно-техническия прогрес.

В представения дисертационен труд са предложени методи за идентифициране на рискове за информационната сигурност и етапи при аналитичното моделиране.

2. Обзор на цитираната литература

В дисертационния труд е представен литературен обзор от 174 източника. От тях 11 са интернет сайта и електронни издания.

В първа глава са изследвани същността на информационната сигурност. Отделено е достатъчна внимание на заплахите за информационната сигурност (разгледани са основно в четири аспекта).

Разгледани са програмни средства за реализиране на експерименталната постановка, базирана на симулационен софтуер във виртуалнан среда (GNS3, WinPcap, Wireshark, Dynamips).

От гледан точка на комуникационните мрежи и системи, изследванията са ограничени до симулиране на атаки от тип „отказ на обслужване“. Разработката няма отношение към проследяване на потребителите в Интернет или други обществени мрежи, а само да се осигури ндеждно управление на информационната

сигурност в процеса на събиране, обработка, съхраняване и разпространяване на информация.

Дисертантът показва добро познание на проблемите, което му позволява да формулира целта и задачите на дисертационния труд.

3. Методика на изследване

Научните изследвания в труда са организирани в три глави, използван е емпиричният изследователски метод чрез средствата на директното и индиректното наблюдение. Методите за изследване са аналитични, симулационни и експериментални.

Изследванията във втора глава са свързани с аналитичното моделиране на заявки от типа "отказ на обслужване".

Синтезирани са основни модели на информационната сигурност (фиг. 2.5), управление на информационната сигурност (фиг. 2.6). Представени са етапите през които се преминава при разработване, внедряване и експлоатация на една такава система (фиг. 2.7). Синтезиран е модел на информационна сигурност (фиг. 2.11).

Изследванията в трета глава са свързани със създаването на симулационен модел на компютърни атаки от типа „отказ на обслужване". Представена е експерименталната постановка (фиг. 3.1), изградения симулационен модел въз основа на графичния вид на експерименталната постановка в среда GNS3 (фиг. 3.2). Симулирани са атаки чрез полето за синхронизация (ACK), полето за финализиране (FIN), полето за нулиране (RST), полето за незабавно предаване (RSH). Атаки чрез препълване на User Datagram Protocol (представен е модел на система за наблюдение – фиг. 3.43). Атаки чрез ICMP – фиг. 3.35.

В четвърта глава са представени политиките за информационна сигурност, като е предложена политика за информационна сигурност – фиг. 4.2. Предложена са система за идентифициране на инциденти – фиг. 4.3, алгоритъм за идентифициране на инциденти чрез прилагане на поведенчески модел – фиг. 4.7. Предложени са методи и средства за програмна реализация на системите за откриване на инциденти.

4. Приноси на дисертационния труд

Приемам претенциите за приносите в дисертационния труд, че имат научно-приложен характер, а самите те са обособени в четири точки:

- синтезиран е графичен модел за упрзвление на информационната сигурност и направено математическо описание на масово обслужване на заявки;
- създадена е опитна постановка и представени експериментални резултати в мрежова симулационна среда, като са реализирани различни сценарии на атаки;
- представени са конкретни решения за минимизиране на последиците от атаките;
- разработен е алгоритъм за откриване и идентифициране на инциденти чрез прилагане на поведенчески модел, като са предложени методи и средства за програмна реализация на система за откриване на инцидента.

5. Публикации и цитирания на публикации по дисертационния труд

Към дисертационния труд са приложени 10 публикации. Седем от публикациите са самостоятелни, а три – в съавторство.

6. Авторство на получените резултати

От публикациите, приложени към дисертационния труд, може да се твърди за авторство на получените резултати. Резултатите, представени в публикациите, съответстват на резултатите, представени в дисертационния труд.

7. Автореферат и авторска справка

Авторефератът на дисертацията напълно отговаря на изискванията. Той представя много точно и стегнато постиженията в дисертационния труд. Приложената справка на английски език синтезира основните приноси, представени в дисертацията.

8. Забележки по дисертационния труд

Като цяло в представения дисертационен труд и съпътстващите го публикации са използвани съвременни методи и модели. Всички претенции за приноси са основателни.

Липсват насоки за бъдещи разработки.

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 **маг. инж. Ивайло Данчов Николов**

в област на висше образование - **Технически науки**,

професионално направление – **5.3 Комуникационна и компютърна техника**,

специалност – **Комуникационни мрежи и системи**

02.04.2018 г.
Габрово

Подпис:
/д

Заличено обстоятелство,
на основание чл.2 от ЗЗЛД