Р Е Ц Е Н З И Я

на дисертационен труд за придобиване на образователна 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 на дисертационния труд: маг. инж. Ивайло Данчов Николов

Тема на дисертационния труд: „Управление на информационната сигурност в компютърни мрежи"

Рецензент: проф. дн Михаил Петков Илиев, катедра „Телекомуникации" на Русенския университет „Ангел Кънчев"

1. ТЕМА И АКТУАЛНОСТ НА ДИСЕРТАЦИОННИЯ ТРУД

Предмет на изследванията на дисертационния труд са възможностите за управление сигурността на компютърни мрежи, осигуряващи подобрената им защита от заплахи на информационните им ресурси при атаки от типа „отказ на обслужване". Обществения интерес за повишаване на информационната сигурност прави тематиката по изследване, разработване и внедряване на съвременни методи и средства за повишена сигурност изключително актуална.

Съществени особености на проблема с информационната сигурност са присъщите й динамика и многоаспектност, изискващи изследвания в областта на технологии, архитектури, управление на услугите и данните. Паралелно с това е необходимо и разработване и внедряване на съвременни методи и средства за информационна сигурност, както и създаване на нормативна уредба, свързана с тематиката.

Заличено обстоятелство, на основание чл.2 от ЗЗЛД

2. ОБЗОР НА ЦИТИРАНАТА ЛИТЕРАТУРА

Представеният ми за рецензиране дисертационен труд на тема „Управление на информационната сигурност в компютърни мрежи" е в обем 162 стр., формат А4 текст, 97 фигури, 7 таблици и 11 приложения. Дисертационният труд е структуриран в 4 глави и заключение. В края на всяка глава са формулирани изводи, обобщаващи съдържанието на главата. При разработването на дисертационния труд авторът е ползвал 174 информационни източника, от които 57 на български език, 106 на английски език и 11 интернет сайта.

В дисертационния труд е направен обзор, включващ материали, публикувани през последните години. Считам, че докторантът е навлязъл в същността на проблематиката по темата на дисертационния труд и чрез интерпретация на информацията от обзора е успял да формулира целта и основните задачи, които водят до постигане на целта.

3. МЕТОДИКА НА ИЗСЛЕДВАНЕ

При разработване на дисертационния труд в отделните глави авторът е използвал в различна степен аналитични, симулационни и експериментални методи на изследване. Във втора глава е направено математическо описание на обслужването на заявки като съвкупност за формиране на информационните потоци. Използвано е аналитично моделиране в контекста на „задръствания" при масово обслужване на заявки. Изследвани са входния поток, неговото разпределение и времето на обслужване на заявките.

Въз основа на теоретичен и експериментален подход е синтезиран графичен модел, чрез който в трета глава е реализирана експериментална постановка в мрежова среда и са симулирани различни атаки върху някои от използваните комуникационни протоколи.

В четвърта глава е разработен алгоритъм, свързан с идентификация на инциденти, чрез прилагане на поведенчески модел вследствие анализ и декодиране на телетрафика.

Прилагането на различни методи на изследване е позволило на автора да получи резултати, позволяващи да се формулират конкретни изводи по задачите на научното изследване.

4. ПРИНОСИ НА ДИСЕРТАЦИОННИЯ ТРУД

Получените резултати от изследването на инж. Ивайло Данчов Николов ми дават основание да класифицирам приносите му в дисертационния труд като научно-приложни и приложени, свързани с обогатяване на съществуващи знания и технически системи, създаване на нови класификации, методи и алгоритми, получаване и доказване на потвърдителни факти.

Обобщавам основните приноси на докторанта както следва:

1. Синтезиран е графичен модел за управление на информационната сигурност въз основа на съществуващата теория и практика. В експериментални условия са реализирани атаки от типа „отказ на обслужване" в съответствие с описания модел за информационна сигурност.
2. Създадена е методика за наблюдение на атаки от типа „отказ на обслужване" в резултат на направените изследвания в контекста на дисертационния труд.
3. Предложен е алгоритъм за откриване на инциденти, свързани със сигурността на информацията, като са дадени насоки за неговото реализиране.
4. Предложено е описание на механизма на представените атаки от тип „отказ на обслужване", което може да бъде основа за бъдещо изследване в посока минимизиране на рисковете за сигурността на информацията.
5. Реализирана е мрежова архитектура в среда GNS3 чрез използване на виртуални машини. В експерименталния модел са реализирани множество атаки от тип „отказ на обслужване", включително от маскирани IP адреси в използвания мрежови сегмент.
6. Доказан е принципът за привеждане на различни по предназначение IP базирани системи в състояние „отказ на обслужване", като

проведените експерименти се отнасят до udp flood атаки при поточно предаване на медийни данни.

7. Представени са конкретни решения за минимизиране на последиците от атаки от типа „отказ на обслужване“.

5. ПУБЛИКАЦИИ ПО ДИСЕРТАЦИОННИЯ ТРУД

Основните резултати, получени в дисертационния труд, са представени в 10 публикации на български език, представени на научни конференции. Три от публикациите са под печат. Седем от публикациите са самостоятелни, три са в съавторство с научните ръководители. Една от публикациите е представена на студентска научна сесия. В публикациите са изложени основните изводи от дисертационния труд. Публикациите са предимно в национални и университетски конференции като някои са с международно участие. Освен тях в периода на обучение докторантът има още 5 публикации.

Въпреки че липсват публикации в научни форуми в чужбина, представеният брои публикации е по-голям от изискванията и считам, че научната общност у нас е запозната с изследванията на докторанта.

Нямам информация за известни цитирания на публикациите на дисертанта.

6. АВТОРСТВО НА ПОЛУЧЕНИТЕ РЕЗУЛТАТИ

Като цяло описанието е коректно и задълбочено. Специфичният стил и начин на изложение на дисертационния труд и публикациите по него ми дават основание да смятам, че те са дело на автора инж. Ивайло Данчов Николов.

7. АВТОРЕФЕРАТ И АВТОРСКА СПРАВКА

Представеният автореферат на дисертационния труд е в обем от 54 страници, структурирани в 4 глави и заключение. Авторефератът е подготвен съгласно изискванията, представя в синтезиран вид същността на дисертационния труд и отразява основните приноси на кандидата и публикациите по дисертационния труд.

8. ПРЕПОРЪКИ И ЗАБЕЛЕЖКИ

Част от препоръките, които бяха направени от мен при предварителното обсъждане на дисертационния труд, са взети предвид при окончателното редактиране на работата. По-съществените забележки и препоръки към представения ми за рецензиране дисертационен труд са:

1. Глава 1 е силно „размита". От нея не следват аргументирано целта и задачите, които са заложени в дисертационния труд;
2. Излишно подробно е развита глава 2. Дадени са основни положения от теорията на масовото обслужване, които са подходящи по-скоро за учебник или учебно помагало;
3. Някои изводи, дадени в края на главите, са априорно известни;
4. Не се цитират всички информационни източници, дадени в края на дисертационния труд;
5. Препоръчвам дисертантът да представи резултатите от работата си и в по-значими издания и научни прояви у нас и в чужбина.

9. ЗАКЛЮЧЕНИЕ

Темата на дисертационния труд е актуална и интересна. Работата има достатъчен обем и дълбочина на изследването. Получените резултати са достатъчно значими за образователна и научна степен „доктор". Публичността на работата е достатъчна. По дисертационния труд от автора са направени 10 публикации.

Докторантът е провел изследвания, получил е, представил е и е анализирал резултати от симулации и реални измервания. Направил е и съответните изводи, което ми дава основание да преценя, че дисертационният труд има необходимите научно-приложни и приложни приноси.

Посочените в т. 8 по-горе препоръки и забележки по представения ми за рецензиране дисертационен труд не омаловажават резултатите от направеното изследване.

Заличено обстоятелство,
на основание чл.2 от ЗЗЛД

Спазени са законовите изисквания от гледна точка на процедурите по докторантурата. Дадена е възможност на научната общност да се запознае с проведените изследвания и получените резултати.

Имайки предвид изложеното считам, че са удовлетворени изискванията за разработване на дисертационен труд за образователна и научна степен „доктор" и давам положителна комплексна оценка на дисертационния труд.

Препоръчвам на уважаемите членове на научното жури да присъдят образователна и научна степен „доктор" по научна специалност „Комуникационни мрежи и системи" на Ивайло Данчов Николов.

гр. Русе
03.04. 2018 г.

Рецензент:

Заличено обстоятелство, на основание чл.2 от ЗЗЛД

/Проф. дн инж. М. Илиев/