

СТАНОВИЩЕ

върху дисертационен труд за придобиване на образователна и научна степен “Доктор” по научна специалност „Комуникационни мрежи и системи”

Автор на дисертационния труд: инж. Петър Красенов Боянов, асистент в катедра „Комуникационна и компютърна техника”, Факултет по Технически науки, Шуменски университет „Епископ Константин Преславски“, гр. Шумен.

Тема на дисертационния труд: “Анализ и противодействие на опити за неототоризиран достъп до ресурсите на компютърните мрежи”

Изготвил становището: доц. д-р инж. Валентин Ангелов Мутков, доцент в катедра „Електроника”, Факултет „Електротехника, Електроника и Автоматика”, Русенски университет „Ангел Кънчев”

1. АКТУАЛНОСТ НА РАЗРАБОТВАНИЯ В ДИСЕРТАЦИОННИЯ ТРУД ПРОБЛЕМ.

Актуалността на разработвания в дисертационния труд проблем произтича от следните фактори.

Първо, в момента комуникационните и информационните технологии се развиват изключително динамично, непрекъснато се разработват нови стандарти и решения, осигуряващи все по-високи скорости за предаване на данни. С внедряването на новите технологии обаче се появяват и голям брой нови уязвимости и слаби места в комуникационните и компютърните мрежи. Същевременно потребителите изискват повече удобства и високо качество на предоставяните им услуги, както и запазване на конфиденциалността на използваната от тях информация и данни.

Второ, свидетели сме на лавинообразно нарастване на количеството и разширяване на спектъра на атаките срещу компютърните бази от данни, сайтове на обществени и държавни организации, на частни лица, срещу системите за електронно банкиране и електронна търговия. При това за съжаление не винаги киберпрестъпленията получават адекватен отпор.

Трето, повишаването на устойчивостта на комуникационните и компютърните мрежи срещу различни видове кибератаки ще доведе до бързото увеличаване на броя на активните потребители и на предоставяните услуги в количествено и качествено отношение. Ще осигури необходимите следващи стъпки в развитието на комуникационните и компютърни мрежи и системи.

Независимо от интензивната научно-изследователска дейност, която се развива през последните години в света в областта на защитата на достъпа до ресурсите на компютърните мрежи, все още са налице нерешени въпроси, поради което актуалността на дисертационния проблем се откроява много ясно.

Направената от докторанта обосновка на актуалността и изложените съображения са коректни и основателни. Те са основа за поставянето на научната цел на изследването: “Да се разработят алгоритми за защита на ресурсите на компютърните мрежи и системи от съвременните сканиращи мрежови атаки”.

Дисертационният труд е разработен в обем от 254 страници и обхваща: обща характеристика на дисертационния труд, 4 глави, заключение (основни резултати, получени в дисертацията), списък на използваните съкращения, литература и 6 приложения (104 стр.). Материалът е онагледен с 68 фигури и 7 таблици.

Направените в глава 1 анализ и класификация на съвременните видове кибератаки са оформени по начин, който позволява да се добие представа за характера и съдържанието на

дисертационното изследване и служат за обосноваване на задачите, които трябва да се решат за постигане на целта на дисертационния труд.

В глава 2 са идентифицирани основните фази на кибератаките, основните типове атаки и ресурсите на компютърните системи, към които са насочени, както и видовете хакери, осъществяващи тези атаки. Реализирана е реална кибератака към компютърна мрежа във ФТН при ШУ „Еп. К. Преславски“, като са установени нейните уязвимости в хостове с инсталирани три от най-често използваните операционни системи: Microsoft Windows XP, Windows 7 Enterprise и Windows 8.

В глава 3 са синтезирани: модифицирана хибридна защитна стена с модула “iptables” и модифициран скрипт, реализиращ линеен алгоритъм за изграждане на хибридна защитна стена. Създаден е модифициран скрипт, реализиращ три подалгоритъма: за блокиране на аналитични платформи, събиращи мрежова информация за потребителя; за приемане на мрежови връзки само с ново, установено и отнесено състояние за входящата веригата и за блокиране на различни видове портови сканиращи кибератаки за входящата верига.

В глава 4 е направен избор на 11 мрежови сканиращи програми за тестване поведението на разработената в дисертационния труд хибридна защитна стена. В резултат на проведените експерименти са формулирани изводи за нейните функционални възможности и е направено сравнение между предлаганите на пазара продукти за мрежово сканиране.

В заключението, от гледна точка на автора, са формулирани основните приноси и приложения на резултатите от изследването.

За проведените в дисертационния труд изследвания е използван подходящ инструментариум – основно методите и средствата за статистически анализ и математическо моделиране с помощта на компютърни системи. Резултатите са изложени в таблична и графична форма, като е направен обстоен анализ на същите. Към всяка глава е направено обобщение и изводи на получените основни резултати.

Структурата на дисертационния труд и последователността на излагане са правилни, методично издържани и позволяват да се проследят в логически план проведените изследвания и получените резултати от тях.

2. ПОЗНАВАНЕ НА СЪСТОЯНИЕТО НА ПРОБЛЕМА.

Разработеният от инж. Петър Боянов дисертационен труд се базира на 140 литературни източника, от които 5 са на кирилица, 123 на латиница и 12 уеб-сайта. Голяма част от литературните източници са тясно специализирани научни списания и реномирани международни форуми в областта на теорията и практиката на защитата на информацията в комуникационните и компютърните мрежи като например:

- Journal of Information & Communication Technology;
- Information, Knowledge, Systems Management;
- International Journal of Computer Networks and Communications Security;
- IEEE Communications Surveys & Tutorials;
- International Journal of Research Studies in Computing;

и други.

Като цяло анализът на съвременното състояние на защитата на достъпа до ресурсите на компютърните мрежи, направен в глава 1, показва, че докторантът задълбочено познава състоянието на изследвания в дисертационния труд проблем.

3. МЕТОДИКА НА НАУЧНОТО ИЗСЛЕДВАНЕ.

В научното изследване, проведено в дисертационния труд, са използвани методите на теорията на управлението, теорията на вероятностите и математическата статистика, теорията на разработването на бази от данни, теорията на програмирането и математическото моделиране. Посочените методи са използвани логически обосновано и в пълно съответствие с целта и задачите на дисертационния труд.

От най-общи позиции, използваната от докторанта методика се заключава в анализ и класификация на методите за осъществяване на кибератаки, в резултат на което са разработени и верифицирани алгоритми и програми за контрол на достъпа и защита на ресурсите на компютърните мрежи. За проведените в дисертационния труд изследвания е използван подходящ инструментариум – основно методите и средствата за статистически анализ и математическо моделиране с помощта на компютърни системи. Резултатите са изложени в таблична и графична форма, като е направен обстоен анализ на същите. Към всяка глава е направено обобщение и изводи на получените основни резултати.

Анализът на съдържанието и на получените резултати в глави 2, 3 и 4 на дисертационния труд показва, че научните изследвания са проведени коректно, поставените задачи в дисертацията са адекватни на целта и са решени в необходимия обем и на високо научно ниво, като са използвани съвременни технически средства.

4. ПРИНОСИ НА ДИСЕРТАЦИОННИЯ ТРУД

В резултат на проведеното изследване в дисертационния труд са получени следните 8 приноси с научен, научно-приложен и приложен характер:

1. Разработен е модифициран алгоритъм на работа на хибридна защитна стена срещу различните видове съвременни мрежови сканиращи кибератаки.

2. Разработен е алгоритъм за блокиране на различни видове портови сканиращи кибератаки за входящата верига.

3. Разработен е алгоритъм за приемане на мрежови връзки само с ново, установено и отнесено състояние за входящата верига.

4. Разработен е алгоритъм, блокиращ аналитични платформи, събиращи мрежова информация за потребителя.

5. Установени са фазите и действието на съвременните видове злонамерени кибератаки.

6. Разработена е класификация на съвременните видове злонамерени кибератаки.

7. Разработен е скрипт на хибридна защитна стена в Linux базирани операционни системи, използващ команди от модула “iptables” и системата за откриване на прониквания PSAD.

8. Разработената хибридна защитна стена може да се използва за обучение на студенти от ФТН по дисциплините “Предаване на данни и компютърни комуникации“, “Компютърни мрежи” и “Администриране на мрежи“.

Считам, че практическо внедряване на приносите от дисертационния труд ще допринесе за повишаване на степента на защита на комуникационните и компютърните мрежи срещу опитите за неототоризиран достъп до техните ресурси а така също и за повишаване качеството на обучение на студентите.

Проведеното в дисертационния труд изследване е тясно свързано с цялата научно-изследователска и преподавателска дейност на докторанта. Всичко това ми дава основание да считам, че горепосочените приноси са лично дело на инж. Петър Боянов.

5. ПУБЛИКАЦИИ ПО ДИСЕРТАЦИЯТА. ВНЕДРЯВАНЕ НА РЕЗУЛТАТИТЕ

Основните резултати, получени при разработването на дисертационния труд, са публикувани в седем научни доклада и четири статии. При това пет доклада са изнесени на международната конференция „International Conference on Bionics and Prosthetics, Biomechanics and Mechanics, Mechatronics and Robotics”, която се провежда ежегодно в гр. Лиепая, Латвия и в гр. Варна и два доклада са представени на научна сесия с международно участие „Курсантите и студентите на Морско училище и науката”, ВВМУ „Н. Й. Вапцаров”, гр. Варна и на научна конференция на тема „Защитата на личните данни в контекста на информационната сигурност”, Факултет "Артилерия, ПВО и КИС" при НВУ „Васил Левски”, гр. Шумен. Научните статии са публикувани в сп. „Компютърни науки и технологии“ и „Journal Scientific and Applied Research” (Licensed in EBSCO, USA), ISSN 1314-6289.

Три доклада и една статия са подготвени от докторанта съвместно с научния му ръководител, два доклада и две статии – самостоятелно, а останалите публикации са в съавторство с други учени.

Публикациите са направени през периода 2013 г. – 2014 г. и имам напълно положително отношение към представителността на научните форуми. Докладите съдържат най-съществените моменти от изследването, проведено от инж. Петър Красенов Боянов и считам, че са дали възможност на научната общественост да се запознае с дисертационния му труд.

Считам, че практическото внедряване на приносите от дисертационния труд ще допринесе за повишаване на степента на защита на комуникационните и компютърните мрежи срещу опитите за неоторизиран достъп до техните ресурси.

6. ПРЕПОРЪКИ И ЗАБЕЛЕЖКИ. ОФОРМЯНЕ НА АВТОРЕФРАТА

Към дисертационния труд нямам по-съществени забележки, освен че са допуснати няколко стилистични грешки и неточности от редакционен характер, които не са определящи за качествата на разработката.

Препоръчвам в бъдеще инж. Петър Боянов да насочи публикационната си дейност основно към наши и чуждестранни списания.

Авторефератът е в оформен акуратно и отразява в пълен обем съдържанието, резултатите и приносите получени в дисертационния труд.

7. ЗАКЛЮЧЕНИЕ

От изложеното по-горе в становището следва изводът, че дисертационният труд има качеството на завършено научно-приложно изследване по актуален и важен проблем с публикувани резултати и отговаря на изискванията за придобиване на образователна и научна степен “Доктор” на „Закона за Развитието на Академичния Състав в Република България” (ЗРАСРБ), Правилника за приложението на ЗРАСРБ и на Правилника за развитието на академичния състав в Шуменския университет „Епископ Константин Преславски”.

Дисертационният труд е разработен в резултат на проведено обучение в редовна докторантура по научната специалност „Комуникационни мрежи и системи” в ШУ „Еп. К. Преславски” гр. Шумен в периода 2013 г. - 2015 г. Дисертацията е завършена и представена за защита в началото на месец декември 2015 г.

Темата, съдържанието на дисертационния труд, обучението в докторантура, както и получените научно-приложни и приложни приноси съответстват на научната специалност „Комуникационни мрежи и системи”.

Изложените до тук факти показват, че обучението в докторантура на инж. Боянов е проведено в пълно съответствие със „Закона за Висшето Образование”, „Закона за Развитие на Академичния Състав в Република България” и изискванията на „Националната Агенция за Оценка и Акредитация”.

Не познавам лично докторанта инж. Петър Красенов Боянов.

Предвид на изложеното по-горе в становището, предлагам на научното жури ДА ДАДЕ образователната и научна степен “Доктор” на инж. Петър Красенов Боянов по научната специалност „Комуникационни мрежи и системи”.



08.01.2016 г.
гр. Русе

Член на научното жури:.....
доц. д-р инж. Валентин Мутков