СТАНОВИЩЕ

от д-р, инж. Тодор Стоянов Джамийков, професор в Технически Университет – София на дисертационен труд за присъждане на образователната и научна степен **„доктор“** по: област на висше образование 5. Технически науки;
професионално направление 5.3 Комуникационна и компютърна техника.
докторска програма „Автоматизация на области от нематериалната сфера (медицина, просвета, наука администрация и др.)

Автор: *Ивайло Детелинов Узунов*

Тема: *Модел за симулация и крайни решения на системите за сигурност*

Научен ръководител: *проф. д-р инж Слави Ясенов Любомиров*

1. Общо представяне на процедурата и докторанта

Със заповед № РД-22-534/25.02.2025г. на Ректора на Пловдивския университет „Паисий Хилендарски“ (ПУ) съм определен(а) за член на научното жури за осигуряване на процедура за защита на дисертационен труд на тема „Модел за симулация и крайни решения на системите за сигурност“ 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 “Автоматизация на области от нематериалната сфера (медицина, просвета, наука, административна дейност и др.)”. Автор на дисертационния труд е маг. инж. Ивайло Детелинов Узунов.

Представеният от маг. инж. Ивайло Детелинов Узунов комплект материали на хартиен носител е в съответствие с Чл.36 (1) от Правилника за развитие на академичния състав на ПУ, включва следните документи: молба до Ректора на ПУ за разкриване на процедурата за защита на дисертационен труд; автобиография в европейски формат; протокол от предварително обсъждане в катедрата; автореферат; декларация за оригиналност и достоверност на приложените документи; справка за съответствие с минималните национални изисквания; списък на публикациите; дисертационен труд; копия от публикациите по дисертационният труд;

Ивайло Детелинов Узунов завършва средното си образование през 2000 - 2005 г. в Професионална Гимназия по Строителство и Архитектура в гр. Смолян. След това, през 2016 година, завършва Технически колеж гр. Смолян. Дипломира се като професионален бакалавър по компютърни и комуникационни системи. През 2019 година се дипломира като магистър инженер по „Телематика“, в Пловдивски университет „Паисий Хилендарски“. От 2021г. до 2024г. е редовен докторант към катедра ЕИКИТ на Пловдивски университет „Паисий Хилендарски“.

Трудовия си стаж маг. инж. Ивайло Узунов започва през 2016г. като техник в сервиз за мобилни телефони. През 2020г. – 2021г. е асистент в Пловдивски университет "Паисий Хилендарски", Физико-технологичен факултет. От 2022 г работи като техник компютърни системи във фирма IT System.

2. Актуалност на тематиката

Дисертационния труд е посветен на модели за симулация и крайни решения в системите за сигурност. Разглеждат се широк спектър от теми: анализ на криптографски алгоритми като AES и RSA, различни видове киберзаплахи като фишинг, SQL инжекции, DoS атаки и зловреден софтуер, както и методи за тяхното предотвратяване. В зна-

чителна част от трудът се описват симулации, проведени в среда MATLAB, за илюстриране на принципите на атаките и ефективността на защитните механизми. Направен и обширен обзор на съществуваща литература в областта на информационната сигурност и симулационни модели за обучение и анализ на мрежови системи. Приложенията съдържат подробен код на симулации на различни видове кибер атаки в MATLAB.

Основната цел на дисертационния труд е да се изследват възможностите за прилагане на модел за симулация и крайни решения на системите за сигурност. Тази цел е постигната чрез допълнително поставени задачи, които включват извеждане на иновативни тълкувания на резултатите от научни изследвания, преглед и анализ на алгоритмите за определяне на видовете заплахи в компютърните мрежи, и предлагане за обсъждане на верифициран алгоритъм при отчитане на основните видове заплахи, критерии и фактори на въздействие. Друга поставена задача е свързана с обзора на проблемите в мрежовата сигурност и защитата на ценни информационни ресурси, както и гарантирането на целостта на информацията.

3. Познаване на проблема

В първа глава на дисертационния труд е направен анализ и са разгледани основни аспекти на информационната сигурност, като поверителност, цялостност и наличност на информацията. Описват се различни механизми за защита, включително управление на достъпа, шифриране и класификация на информацията. Представен е концепцията за защита в дълбочина.

В обзора са включени и различни видове компютърни заплахи, като зловреден софтуер, фишинг, MITM атаки и социално инженерство. Разглеждат се и методи за удостоверяване, като използване на пароли и хешове.

Прегледани са и интерпретирани по подходящ начин, чрез критичен анализ съществуващите източници по проблема. Литературната справка обхваща 143 източника, на английски език, включително и електронни. Всички те са актуални в настоящия момент научни публикации и са от реномирани списания, издания от международни конференции. Те са от водещи, изтъкнати в настоящия момент автори, чужди и наши учени и специалисти в областта.

4. Методика на изследването

Избраната методика в дисертационният труд съответства на поставената цел, като включва следните аспекти.

- Разгледани са и анализцирана спецификата на основните видове заплахи;
- Изследване и симулационен анализ на криптографски модели, включително симетрични (AES) и хеширащи (SHA, MD5) алгоритми;
- Изследване на мрежово сканиране с инструменти като Nmap и Discover за идентифициране на уязвимости;
- Анализ на уязвимости на уеб приложения, като SQL инжекции и XSS атаки;
- Провеждане на симулации на различни видове кибератаки в среда MATLAB, включително DoS, MITM и Replay/Delay атаки;
- Моделиране на защитни механизми като защитни стени чрез симулации;
- Използване на методи за симулация като Монте Карло и Agent-Based модели за оценка на рискове и анализ на динамиката на атаките;

Тези аспекти демонстрират комплексен подход, който съчетава теоретичен анализ с практически симулации и експериментални изследвания, което е в съответствие с целта на дисертацията.

5. Характеристика и оценка на дисертационния труд и приносите

Дисертационният труд изследва информационната сигурност чрез анализи, симулации и експерименти за идентифициране и преодоляване на уязвимости.

Глава I представя литературен обзор на кибератаки, информационна и компютърна сигурност, процедури за сигурност и цели на дисертацията.

Глава II анализира и изследва криптографски модели, включително симетрични (AES) и асиметрични алгоритми, хеширащи функции (SHA, MD5) и електронни подписи, като представя симулационни резултати от MATLAB.

Глава III разглежда сигурността на мрежови информационни системи, анализирайки уязвимости чрез мрежово сканиране с Nmap и Discover, фишинг атаки (SEToolkit) и уеб уязвимости като SQL инжекция и XSS.

Глава IV представя експериментални изследвания и симулационни модели в MATLAB на AES криптиране, MITM, Replay и Delay атаки, DoS атаки, вероятност за успешни атаки (Монте Карло) и Agent-Based модели за анализ на мрежова сигурност.

Авторът е представил в дисертационният труд 3 научно-приложни и 5 приложни приноса. Приемам, че обосновано и аргументирано са предложени на база, извършената и описаната в дисертацията работа.

6. Преценка на публикациите и личния принос на докторанта

Дисертационният труд на Ивайло Узунов е подкрепен от пет публикации. Четири от публикациите са в съавторство с научния ръководител, а една е самостоятелна.

Прегледа на публикациите показва, че те обхващат тематиката на дисертационния труд и представят пред научната общност постигнатите резултати. Броят им е достатъчен и съответства на приетите изисквания.

Предложените научно приложни и приложни приноси фигурират в достатъчен по обем и съдържание публикации на докторанта. Те са представени в реномирани и утвърдени в областта научни форуми, което означава, че резултатите са придобили съответната популярност и признание в научните среди. Считам, че личното участие на докторанта се проявява и е безспорно потвърдено от самостоятелната публикация и съавторството в другите с научния му ръководител.

Всички теоретични и практически постановки са аргументирани, правилно и в подходяща в методично отношение последователност. Независимо от това, могат да се посочат незначителни редакционни неточности и пропуски, някои от които са:

В увода се заявява, че дисертацията представя "модел за симулация и крайни решения на системите за сигурност на видовете заплахи в компютърните системи". Въпреки това, в първите две глави, включително литературния обзор и главата за симулационен анализ, не се предоставя достатъчно детайлна информация относно същността, структурата и характеристиките на този предложен модел. Не е ясно как литературният обзор води пряко до дефинирането на конкретния симулационен модел, който ще бъде използван и изследван в следващите глави.

Дисертацията обхваща широк спектър от теми, на кибер-заплахи и криптографски модели до експериментални изследвания с инструменти за сканиране и симулации в MATLAB. Възможно е да има липса на конкретно, детайлно фокусиране и дълбочина в изследването на конкретни аспекти. Разглеждане и изследване в такива подробности, би позволило да се направят по-изчерпателни заключения и по-силни научно-приложни приноси.

7. Автореферат

Внимателният преглед на автореферата към дисертационният труд показва наличие на пълно съответствие с изискванията за изготвянето му. Адекватно отразява основните положения и приносите в дисертационният труд. Съответства напълно на дефинираните научно приложни и приложни приноси, съдържащи се в пълния текст на дисертационният труд.

В заключение, авторефератът в съответства на дисертационния труд по отношение на структура, тематична насоченост, методология и приноси.

8. Препоръки за бъдещо използване на дисертационните приноси и резултати

Направените изследвания и предложени научно-приложни приноси са пряко използваеми в практиката. Могат да бъдат внедряване в обучителни програми за киберсигурност: Разработените MATLAB симулации на криптографски алгоритми (като AES), модели на различни атаки (DoS, Replay, Delay, MITM) и агентно-базирани модели могат да бъдат интегрирани в учебни планове и курсове за обучение на специалисти по киберсигурност.

Представените методи за анализ на уязвимости чрез сканиращи инструменти (като Nmap и Discover), техники за защита срещу инжекционни атаки (SQL Injection, PHP Code Injection, OS Command Injection) и модели за симулация на мрежови атаки и защитни стени могат да бъдат адаптирани и приложени в реални корпоративни и институционални среди.

Заключение

Дисертационният труд ***съдържа научно-приложни и приложни резултати, които представляват оригинален принос в науката*** и **отговарят на всички** изисквания на Закона за развитие на академичния състав в Република България (ЗРАСРБ), Правилника за прилагане на ЗРАСРБ и съответния Правилник на ПУ „Паисий Хилендарски".

Дисертационният труд показва, че докторантът маг. инж. Ивайло Детелинов Узунов **притежава** задълбочени теоретични знания и професионални умения по научна специалност 5. Технически науки, професионално направление 5.3. Комуникационна и компютърна техника, като демонстрира качества и умения за самостоятелно провеждане на научно изследване.

Поради гореизложеното, убедено давам своята ***положителна оценка*** за проведеното изследване, представено от рецензираните по-горе дисертационен труд, автореферат, постигнати резултати и приноси, и ***предлагам на почитаемото научно жури да присъди образователната и научна степен „доктор"*** на маг. инж. Ивайло Детелинов Узунов в област на висше образование: 5. Технически науки, професионално направление 5.3. Комуникационна и компютърна техника, докторска програма "Автоматизация на области от нематериалната сфера (медицина, просвета, наука, административна дейност и др.)".

24.04. 2025 г. **Изготвил становището**:.....

(проф. д-р Тодор Джамийков)