

HODNOTENIE HABILITAČNEJ PRÁCE

POSUDOK OPONENTA PRÁCE

Názov práce: **Vybrané metódy detekcie prienikov s využitím lákadiel**

Autor: **Ing. Eva Chovancová, PhD.**

Odbor habilitačného konania **Informatika**

Akad. rok: **2019/2020**

a inauguračného konania:

Oponent: **prof. Ing. Pavel Čičák, PhD.**

Pracovisko opONENTA: **FIII STU v Bratislave**

KOMENTÁR OPONENTA HABILITAČNEJ PRÁCE

AKTUÁLNOSŤ ZVOLENEJ TÉMY HABILITAČNEJ PRÁCE:

Problematika informačno-komunikačných technológií prerástla v súčasnosti do novej dimenzie. Všetko začalo prepájaním počítačov. Zatiaľ čo v nedávnej minulosti pribudlo prepájanie vecí (IoT), v súčasnosti je predmetom prepájania „všetko“ (IoE). Vhľadom na prudký rozvoj tejto disciplíny prichádzajú aj neustále nové hrozby a kybernetické útoky, ktoré môžu ovplyvniť resp. až znefunkčniť fungovanie systémov v rôznych smeroch, znegodnotiť údaje, alebo získať dôležité informácie. Predložená habilitačná práca Ing. Evy Chovancovej, PhD. sa zameriava na bezpečnosť komunikácie prostredníctvom detekcie prienikov s využitím lákadiel. Zvolená téma je aktuálna a neustále sa dynamicky rozvíja. Vzhľadom na súčasný stav problematiky v tejto oblasti hodnotím zvolenú tému ako vysoko aktuálnu s predpokladom ďalšieho výskumu.

METÓDY SPRACOVANIA HABILITAČNEJ PRÁCE:

Metodika, systematickosť a spôsob spracovania témy v práci svedčí o vysokej pedagogickej a odbornej erudovanosti habilitantky v sledovanej problematike.

Práca je koncipovaná ako komentovaný súbor vybraných publikácií autorky a kolektívu tematicky orientovaných na oblasť metód detekcie prienikov. Je formálne rozdelená do troch hlavných kapitol a devätnástich podkapitol. Ďalej obsahuje úvod, vybrané príspevky autorky k uvedenej téme doplnené sprievodným komentárom, zoznam publikácií, výskumno-pedagogických projektov ako aj pedagogickej činnosti autorky. Predložená práca obsahuje celkovo 167 strán textu a autorka použila 111 literárnych prameňov. Prvá kapitola pozostáva zo štruktúrovaného úvodu do zvolenej problematiky v oblasti informačnej bezpečnosti. Druhá kapitola sa zameriava na bezpečnostný nástroj lákadlo, pričom opisuje jeho princíp fungovania a prínos v oblasti bezpečnosti informačno-komunikačných technológií a zároveň rovnako poskytuje prehľad výskumu a súčasný stav vo zvolenej problematike. Uvedené kapitoly tvoria 29 strán predkladanej habilitačnej práce a hodnotím ich pozitívne. Hlavná časť práce je prezentovaná v tretej kapitole, ktorá pozostáva z výberu deviatich publikovaných prác vo zvolenej problematike habilitačnej práce, ktoré sú chronologicky usporiadané a opisujú postupný výskum v danej oblasti. Na základe nadväznosti jednotlivých publikácií je možné poukázať na systematickú prácu počas celého výskumu, ktorý je opísaný v predkladanej habilitačnej práci.

Samotný výskum je logicky rozdelený do dvoch oblastí:

- detekcia prienikov s využitím lákadiel,
- vývoj v oblasti zberu a agregácie údajov v sieťovom prostredí.

Záverová časť práce pozostáva z publikačných výstupov autorky a zoznamu účasti na projektoch základného a aplikovaného výskumu, čo preukazuje autorkine kontinuálne vedecko-výskumné pôsobenie počas pôsobenia na Technickej univerzite v Košiciach.

DOSIAHNUTÉ VÝSLEDKY HABILITAČNEJ PRÁCE A NOVÉ POZNATKY:

Hlavné výsledky habilitačnej práce sú prezentované v tretej, najrozsiahlejšej kapitole, pričom predstavujú vybrané vedecko-výskumné výstupy doplnené komentárom. Vybraných 9 publikácií má formu konferenčných a časopiseckých publikácií publikovaných doma i v zahraničí.

Výskum autorky je možné vnímať v dvoch rovinách a to:

1. Detekcia prienikov s využitím lákadiel. V tejto rovine sa autorka zameriava na postupný návrh a implementáciu klastrového lákadla s využitím lákadiel s rôznou interakciou v rámci systémov detekcie prienikov, pričom sa zameriava aj na efektivitu z hľadiska spravovania lákadiel.
2. Druhá rovina sa venuje výskumu v oblasti optimalizácie monitorovania a zberu dát v sieťovej prevádzke, pričom sa zameriava na zefektívnenie metód vzorkovania sieťového toku.

Medzi významné publikácie autorky, ktoré prezentujú výskum v danej oblasti patria karentované výstupy v podkapitolách 3.5 a 3.6 publikované v rokoch 2017 a 2018. Uvedené karentované publikácie obsahujú významné výsledky v oblasti detekcie prienikov s použitím lákadiel a optimalizácie zberu údajov s využitím adaptívnej agregácie sieťového toku, pričom tieto témy sú hlavným ťažiskom predkladanej habilitačnej práce.

Predkladaná práca poskytuje prehľad výskumu autorky v rokoch 2009 až 2020, pričom z predkladanej habilitačnej práce a uvedených publikačných výstupov je možné poukázať na profiláciu autora v oblasti detekcie prienikov s využitím lákadiel.

PRÍNOS PRE ĎALŠÍ ROZVOJ VEDY A TECHNIKY (UMENIA):

Predloženú habilitačnú prácu je možné vnímať tiež v dvoch rovinách.

Jedna časť je vlastne monografická resp. monotematická, ktorá preukazuje vysokú erudovanosť habilitantky nielen po odbornej, ale najmä pedagogickej

stránke. Opisuje a uvádza analýzu a vlastné pohľady na oblasť vedy, ktorej sa dlhodobo venuje. Jedná sa o bezpečnostné aspekty, formy, metódy a teoretické prístupy k detekcii prienikov s využitím lákadiel v prostredí sieťovej komunikácie vo všeobecnosti.

Druhá časť práce uvádza doteraz skúmané oblasti vrátane konkrétnych výstupov a to:

- o Detekcia prienikov s využitím lákadiel.
- o Optimalizácia monitorovania a zberu dát v sieťovej prevádzke

Za dôležité považujem, že habilitantka uvádza aj ďalšie smery možného výskumu.

PRIPOMIENKY A POZNÁMKY K HABILITAČNEJ PRÁCI:

Zásadné pripomienky k habilitačnej práci nemám. Práca je po formálnej stránke spracovaná na veľmi dobrej úrovni. Každá kapitola je dopĺňaná veľkým počtom grafických znázornení a obrázkov. Práca je písaná jasne a zrozumiteľne, je systematicky spracovaná a na úrovni zodpovedajúcej kritériám pre priznanie vedecko-pedagogického titulu docent.

OTÁZKY K RIEŠENEJ PROBLEMATIKE:

K práci mám nasledujúce otázky:

1. V oblasti vzorkovania dátového toku autorka uvádza metódu adaptívneho vzorkovania, v ktorých komponentoch systémov IDS je tento návrh využiteľný? Čo viedlo autorku k aplikácii týchto prístupov v oblasti IDS ?
2. V prípade technológie detekcie prienikov na princípe lákadiel, môže autorka bližšie opísať výhody prístupu voči tradičným IDS?

SPLNENIE SLEDOVANÝCH CIEĽOV HABILITAČNEJ PRÁCE:

Pri posudzovaní plnenia Kritérií na habilitácie docentov FEI TU konštatujem, že habilitantka plní platné kritériá, prejavila schopnosť jasného a zrozumiteľného interpretovania problematiky a vhodne využila matematický aparát pre opis skúmaných javov. Vo vedeckej činnosti sa habilitantka dlhodobo venuje oblasti detekcie prienikov v komunikačnom prostredí ako aj viacerým aplikačným doménam do ktorých poznatky prenáša. Nezanedbateľná je účasť habilitantky na riešení viacerých grantových projektov. Z habilitačnej práce a priložených dokladov vyplýva, že Ing. Eva Chovancová, PhD. je pedagogicky a vedecky skúsenou osobnosťou so schopnosťami prenášať najnovšie teoretické poznatky a praktické skúsenosti do pedagogickej a vedeckovýskumnej činnosti.

CELKOVÉ ZHODNOTENIE HABILITAČNEJ PRÁCE A ZÁVER:

Na základe celkového zhodnotenia habilitačnej práce a posúdením faktov a stanovísk z priložených dokladov (Profesijný životopis, Prehľad pedagogickej činnosti a výsledkov dosiahnutých vo výchovno-vzdelávacej činnosti, Prehľad vedecko-výskumnej činnosti a výsledkov dosiahnutých v tejto oblasti, Zoznam pôvodných publikovaných vedeckých a odborných prác, učebníc, učebných textov, Plnenie kritérií FEI TU v Košiciach pre habilitačné konanie)

konštatujem,

že habilitačná práca, ako aj vedecká spôsobilosť Ing. Evy Chovancovej, PhD. zodpovedajú požiadavkám habilitácie a

odporúčam,

aby v prípade úspešnej habilitácie bola

Ing. Eva Chovancová, PhD.

vymenovaná za docentku v odbore habilitačného konania
Informatika

V Bratislave 17. 08.2020

Predloženú habilitačnú prácu na základe predchádzajúceho hodnotenia

ODPORÚČAM prijať k obhajobe

a po jej obhájení navrhujem udeliť vedecko-pedagogický titul "docent (doc.) v odbore "

Podpisom na tomto posudku zároveň súhlasím s licenčnými podmienkami obsiahnutými v licenčnej zmluve na použitie posudku záverečnej práce, ktorá je súčasťou tohto posudku.

Dátum: 22.08.2020
podpis autora posudku

