

STUDENTŲ ĮTRAUKIMO Į MOKSLINĘ VEIKLĄ SKATININAMOJO KONKURSO TEMA

Temos pavadinimas: Nesankcionuotų belaidžio interneto prieigos taškų erdvinio lokalizavimo metodų tyrimas ir vertinimas.
Tikslas: Sukurti metodiką, skirtą nesankcionuotų belaidžio interneto prieigos taškų identifikavimui ir jų tikslios buvimo vietos nustatymui trimatėje erdvėje.
Trumpas temos vykdymo aprašymas (ne daugiau kaip 2000 ženklių): Šiuo metu korporatyvinių tinklų kibernetinė sauga ir belaidžio interneto signalų analizė yra informacinių technologijų bei elektronikos inžinerijos esminėje sandūroje. Nesankcionuoti belaidžio interneto prieigos taškai, atsirandantys organizacijų fizinėse erdvėse be administratoriaus žinios, keičia rizikos vertinimą tokiose srityse kaip konfidencialių duomenų apsauga, pramoninis šnipinėjimas ir kritinės infrastruktūros saugumas. Kibernetinio saugumo kontekste šie įrenginiai sukuria nekontroliuojamus vartus į izoliuotus įmonės tinklus, visiškai apeidami ugniasienes bei programines perimetro apsaugos sistemas. Tokie pažeidžiami kanalai idealiai tinka piktavalių vykdomoms atakoms, duomenų paketų perėmimui arba kenkėjiško kodo injekcijoms tiesiai į vidinę infrastruktūrą. Kadangi tradicinės programinės kibernetinio saugumo priemonės negali aptikti fizinės neautorizuoto įrenginio buvimo vietos, automatiniai erdvinio lokalizavimo metodai uždaroje pastatų erdvėje tampa kritine gynybos grandimi. Vis dėlto inžineriniame taikyme tai lieka iššūkiu dėl sudėtingo radijo bangų sklidimo, atspindžių nuo konstrukcijų ir prieinamų greito reagavimo įrankių trūkumo. Šie tyrimai leis įsigilinti ir sutelkti dėmesį į šiuos pagrindinius aspektus: 1. Bus panaudota programiškai valdoma radijo įranga arba specializuoti tinklo analizatoriai, siekiant inžineriškai ištirti belaidžio interneto signalų sklidimą ir jų parametrų koreliaciją su fizine vieta. Naudojant kompiuterinio modeliavimo įrankius, studentas įgis praktinės patirties projektuojant, derinant ir analizuojant lokalizavimo sistemas, nereikalaujant ypač brangios stacionarios laboratorinės įrangos. 2. Tikslus fizinis grėsmių identifikavimas ir esamų metodų efektyvumo vertinimas yra kritiškai svarbus naujoms kibernetinės saugos technologijoms. Pavyzdžiui, išmanieji biurai ir pramoninės IoT aplinkos reikalauja nuolatinio spektro audito, o visapusiškas saugumo valdymas remiasi gebėjimu operatyviai eliminuoti nesankcionuotą interneto įrangą iš fizinio perimetro. Šie tyrimai paruos studentus spręsti šiuos iššūkius, sujungiant radijo bangų teorijos pagrindus su pažangiausiomis saugumo valdymo technologijomis. Kad pasiekti darbo tikslą, studentas turėtų išspręsti šiuos uždavinius: 1. Atlikti literatūros analizę ir išsamiai susipažinti su belaidžio prieigos taškų aptikimo bei pozicionavimo metodais tiek dvimatėje, tiek trimatėje erdvėje, nustatyti kriterijus, pagal kuriuos bus pasirenkamas tinkamiausias lokalizavimo metodas tolimesniems tyrimams bei identifikuoti esmines problemas, su kuriomis šiuo metu susiduriama vykdant belaidžio prieigos taškų pozicionavimą; 2. Pasiūlyti belaidžio interneto prieigos taškų lokalizavimo metodiką trimatėje erdvėje; 3. Atlikti pasiūlytos belaidžio interneto prieigos taškų identifikavimo ir jų tikslios buvimo vietos nustatymo trimatėje erdvėje metodikos realizaciją; 4. Galutinės ataskaitos rengimas. Ši tyrimų sritis reikalauja specifinių žinių, įgūdžių ir tikslinga kuo ankstesnėje fazėje įtraukti studentą į mokslinių tyrimų vykdymą, kad įgytų vertingų pažangios programinės ir aukšto lygio techninės įrangos naudojimo įgūdžių. Šios temos vykdymo metu studentas ženkliai pakels kvalifikaciją, gautos žinios suteiks jam postūmį toliau gilintis šioje veikloje ir vykdyti šios srities mokslinius tyrimus. Taip pat šie tyrimai leis geriau pasiruošti tolimesnėms studijoms magistrantūroje. <i>Tema skirta pirmos pakopos Kibernetinio saugumo ir ryšių technologijų, Elektronikos inžinerijos ir Kompiuterių inžinerijos studentams.</i>
Temą siūlantis mokslininkas/dėstytojas: doc. dr. Gediminas Gražulevičius