DOKTORANTŪROS STUDIJŲ DALYKO SANDAS

Dalyko pavadinimas	Mokslo kryptis, kodas	Fakultetas	Institutas, katedra
Sistemų kibernetinis saugumas	Informatika (N009)	MIF	Informatikos institutas, Kibernetinio saugumo laboratorija

Studijų būdas	Kreditų skaičius ECTS	Studijų būdas	Kreditų skaičius ECTS
paskaitos	1 (rudens)	konsultacijos	1
individualus	4	seminarai	1

Dalyko anotacija
Šis dalykas pristato pagrindines kibernetinio saugumo (KS) sąvokas, leidžiančias gilintis į sudėtingesnes temas įskaitant horizontaliuosius KS taikymus informatikoje. Dalykas apima visą skaitmeninės erdvės saugaus valdymo spektrą, sričiai aktualių skaitmeninių dvynių modeliavimą, informacijos bei tinklo komunikacijos srautų saugą ir skaitmeninius tyrimus. KS neatsiejamas nuo organizacijos brandos, gerųjų praktikų ir žmogaus, kaip skaitmeninių sistemų kūrėjo ir naudotojo, dimensijos. Taigi temos padengs nuo sistemų reikalavimų laikymosi, taikomų standartų iki žmogiškųjų veiksnių keliamų rizikų atsižvelgiant į naujausius mokslinius pasiekimus ir technologijų taikymų tendencijas. Dalyke nagrinėjamos įvairios rizikos mažinimo strategijos, skirtos pažeidžiamumo poveikiui sumažinti, grėsmėms neutralizuoti ir organizacijos duomenims bei sisteminiams ištekliams apsaugoti. Šio dalyko tikslas suteikti doktorantams kibernetinio saugumo žinių ir ugdyti gebėjimus formuluoti programinės įrangos, įskaitant doktorantūros prototipų, saugumo reikalavimus, identifikuoti kompiuterinės sistemos atakos paviršių bei vertinti grėsmes ir rizikas, naudojant tinkamus algoritminius ir technologinius sprendinius bei metodikas. Dalyko pagrindinės temos: • Holistinis požiūris į KS • Saugumo politika, standartai ir ES direktyvos • Atakos paviršiaus nustatymas, grėsmių ir rizikos vertinimas • Programinės įrangos saugumo vertinimo metodai, standartai • Pažeidžiamumų aptikimo metodai • Skaitmeninių dvynių modeliavimas • Skaitmeninių nusikaltimų tyrimų metodai • Žalingo kodo analizės aplinkos ir elgsenos tyrimai • Moderniųjų technologijų taikymai gynybai • Mokslinių tyrimų saugumas *Praktinė užduotis:* pagal savo mokslinio darbo temą pasirinkti įgyvendinti KS projektą, sumodeliuoti atakos paviršių, pasinaudoti KS eksperimentiniu poligonu, išbandant KS gynybos taktikas, atlikti

eksperimentus KS grėsmių suvaldymui ir pasirinktos taktikos vertinimui, paruošti projekto ataskaitą ir pristatyti ją pranešime.
Pagrindinė literatūra
Cornish, P. (Ed.). (2021). The Oxford Handbook of Cyber Security. Oxford University Press. https://doi.org/10.1093/oxfordhb/9780198800682.001.0001
Stevens, T. (2026). Cyber Risk. Bristol University Press. https://doi.org/10.51952/9781529256048
Velu, V. K. (2022). *Mastering Kali Linux for advanced penetration testing : become a cybersecurity ethical hacking expert using metasploit, nmap, wireshark, and burp suite* (Fourth edition.). Packt Publishing, Limited. https://doi.org/10.0000/9781801812672

Konsultuojančiųjų dėstytojų vardas, pavardė	Mokslo laipsnis	Svarbiausieji darbai mokslo kryptyje, paskelbti per pastaruosius 5 metus
Prof. Linas Bukauskas	dr.	https://elaba.mb.vu.lt/mif/?aut=Linas+Bukauskas
Doc. Agnė Brilingaitė	dr.	https://elaba.mb.vu.lt/mif/?aut=Agnė+Brilingaitė