STUDIJŲ DALYKO (MODULIO) APRAŠAS

Dalyko (modulio) pavadinimas	Kodas
Kibernetinė sauga	

Dėstytojas (-ai)	Padalinys (-iai)
Koordinuojantis: doc. F. Kuliešius **Kitas (-i):**	Fizikos fakultetas

Studijų pakopa	Dalyko (modulio) tipas
Pirmoji (bakalauro) studijų pakopa	privalomas

Įgyvendinimo forma	Vykdymo laikotarpis	Vykdymo kalba (-os)
Nuolatinė	8 (pavasaris) semestras	Lietuvių

Reikalavimai studijuojančiajam	
Išankstiniai reikalavimai: Kompiuterinis raštingumas, programavimo pagrindai	**Gretutiniai reikalavimai (jei yra):**

Dalyko (modulio) apimtis kreditais	Visas studento darbo krūvis	Kontaktinio darbo valandos	Savarankiško darbo valandos
5	140	64	76

Dalyko (modulio) tikslas: studijų programos ugdomos kompetencijos		
• Supažindinti studentus su kibernetinėmis grėsmėmis, rizikos vertinimu ir pagrindiniais saugos elementais ir standartais; • suteikti žinių apie kriptografijos pagrindus, informacinių infrastruktūrų apsaugą bei informacijos saugos užtikrinimo būdus; • įgytas žinias įtvirtinti praktinių užsiėmimų metu, suteikiant būtinas kompetencijas efektyvioms savarankiškoms gilesnėms dalyko studijoms ir darbui;		
Dalyko (modulio) studijų siekiniai	**Studijų metodai**	**Vertinimo metodai**
Žinos kibernetinės saugos taksonomiją. Žinos pagrindinius duomenų saugą reglamentuojančius dokumentus ir standartus. Žinos dažniausiai naudojamus kriptografijos metodus ir jų taikymus. Mokės įvertinti kibernetines grėsmes ir riziką. Gebės reaguoti į galimas kibernetines atakas.	Paskaitos, diskusijos, pratybos	Egzaminas raštu,

Temos	Kontaktinio darbo valandos							Savarankiškų studijų laikas ir užduotys	
	Paskaitos	Konsultacijos	Seminarai	Pratybos	Laboratoriniai darbai	Praktika	**Visas kontaktinis darbas**	**Savarankiškas darbas**	**Užduotys**
Kibernetinė sauga Pagrindiniai taksonomijos elementai, galimos grėsmės, pažeidžiamumai ir KS principai	2			2			**4**	**6**	MS OS slaptažodžio atkūrimas

Pagrindiniai kompiuterinių ir informacinių sistemų pažeidžiamumai ir saugos būdai. Interneto serverių apsauga nuo atakų. Pažeidžiamumo testavimo (pen testing) pagrindai.	4			6			**10**	**8**	Pažintis su pagrindiniais pen testerio įrankiais, jų diegimas ir naudojimas Nutolusio kompiuterio užvaldymas, „blue screen“, svetimų procesų stabdymas
Informacijos saugos taisyklės ir saugos valdymo standartai (ISO/IEC 17799/2700x...)..	2						**2**	**4**	ISO saugos standartų diegimo planavimas
Rizikos vertinimas ir valdymas. Sprendimai netikėtose situacijose bei veiksmai po saugumo incidentų.	2			4			**6**	**6**	Rizikos vertinimo ir valdymo projektinis darbas Konfidencialumo, integralumo ir pasiekiamumo balanso užduotis
Saugos analizė ir kūrimas įvairiuose objektuose (fiziniai resursai, vartotojai, duomenys, duomenų perdavimas, užkardos, IDS/IPS, DLP... **Autentifikacijos autorizacijos, bei prieigos kontrolės** strategijos planavimas, konfigūravimas ir valdymas. **Saugių kompiuteriniu tinklų planavimas ir kūrimas**, grėsmių radimas tinkluose. Intervencijos aptikimo/prevencijos (IDS/IPS) bei turinio analizės/valdymo sistemos. Saugos valdymas, tinklo perimetro saugos užtikrinimas. Saugos problemos bevieliuose tinkluose. **KS diegimo pavyzdžiai.** Geros praktikos KS metodikos ir patvirtinti modeliai (validated design).	6			4			**10**	**10**	Saugos politikos planavimas ir diegimas
Kriptografijos teorija. Simetrinis ir asimetrinis šifravimas bei pagrindiniai algoritmai. Maišos funkcijos. Rakto perdavimo protokolai. Išvestinių raktų (KDF) funkcijos	8			8			**16**	**20**	Šifravimas dešifravimas naudojant Rail Fence, Vigenere ir kt. perstatų algoritmus. Sumažintas RC4 šifro variantas. Šifravimo naudojant DES algoritmą analizė. Merkle-Hellman kriptosistema. RSA šifravimo sistema Diffie-Hellman-Merkle algoritmas
Kriptografijos naudojimas. Kriptografijos, viešųjų/privačių raktų bei sertifikatų naudojimas informacijos saugai užtikrinti. **Parašai ir sertifikatai**. Elektroninis parašas. Skaitmeniniai sertifikatai. Sertifikatų diegimas. Viešųjų raktų infrastruktūra. Teisinės duomenų saugos problemos.	2			2			**4**	**4**	Elektroninio parašo naudojimas.
Virtualūs privatūs tinklai (VPN). IPSec, SSL/TLS ir kt. tuneliai.	4			4			**8**	**12**	VPN kanalų konfigūravimas ir administravimas
Blokų grandinės. BG principai ir technologijos. BG taikymas dokumentų ir fizinių objektų bei jų generuotų duomenų saugai užtikrinti	2			2			**4**	**6**	Saugios paskirstytos decentralizuotos sistemos kūrimas
Iš viso	**32**			**32**			**64**	**76**	

Vertinimo strategija	Svoris proc.*	Atsiskaitymo laikas	Vertinimo kriterijai
Savarankiškų praktinių darbų įvertinimas Privaloma atlikti ir laiku atsiskaityti visus praktinius darbus.	30	Viso semestro metu	Pasirengimas atsakyti į klausimus, klaidų kiekis, darbo rezultatų aprašymo kokybė, gebėjimas paaiškinti gautus rezultatus.
Veiklos pratybų metu vertinimas Privaloma atlikti ir laiku atsiskaityti visus praktinius darbus.	20	Viso semestro metu	Gebėjimas savarankiškai atlikti užduotis pratybų kompiuterių klasėje metu.
Egzaminas (raštu)	50	Egzaminų sesijos metu	Klausimo suvokimas ir paaiškinimas

* Vertinama 10-ies balų sistemoje, kaupiamasis balas gaunamas padauginus iš svorio koeficiento.

Autorius	Leidimo metai	Pavadinimas	Periodinio leidinio Nr. ar leidinio tomas	Leidimo vieta ir leidykla ar internetinė nuoroda
Privaloma literatūra				
D. Gollman	2013	Computer Security,		Wiley, ISBN : 978-1-118-51708
R. Panko	2010	Corporate Computer and Network Security, 2/Ed,		Prentice Hall, ISBN-0131854755
A. Čenys, J. Juknius,	2011	Saugumo patikros ir etiško įsilaužimo technologijos,		TEV
E. Sakalauskas, N. Listopadskis, GS. Dosinas	2008	Kriptografijos teorija		Vitae Litera
Papildoma literatūra				
M. Lučinskij, P. Poderskis, P. Tumėnas,	2007	Duomenų saugos pradmenys		Smaltija
R. Anderson	2008	Security Engineering 2Ed,.		Wiley, ISBN: 978-0-470-06852-6
Th. R. Peltier, J. Peltier, J. Blackley,.	2005	Information security fundamentals		Auerbach Publications