STUDIJŲ DALYKO (MODULIO) APRAŠAS

Dalyko (modulio) pavadinimas	Kodas
Informacijos saugumas	

Anotacija
Pasaulio skaitmenizacijasupaprastina daugelio paslaugų prieinamumą, pasiekiamumą, paspartina procesus, tačiau tuo pačiu kelia daug iššūkių informacijos apsaugai. Šio kurso metu nagrinėjamos dažniausios su informacijos saugumu susijusios problemos, priemonės nuo jų apsisaugoti. Nagrinėjama žmogaus psichologija, dažniausiai išnaudojamos silpnybės, palengvinančios informacijos vagystę ar sugadinimą.

Dėstytojas (-ai)	Padalinys (-iai)
Koordinuojantis: lektorius dr. Mindaugas Liogys	Vilniaus universiteto Komunikacijos fakulteto Verslo informacijos vadybos bakalauro studijų programos studijų progamos komitetas, Saulėtekio al. 9, 416 kab., III rūmai, LT-10222 Vilnius

Studijų pakopa	Dalyko (modulio) tipas
Pirmoji	Pasirenkamasis

Įgyvendinimo forma	Vykdymo laikotarpis	Vykdymo kalba (-os)
Mišri, auditorinė arba nuotolinė	Rudens (V) semestras	Lietuvių

Reikalavimai studijuojančiajam	
Išankstiniai reikalavimai: Anglų kalba (B1 lygis).	**Gretutiniai reikalavimai (jei yra):**

Dalyko (modulio) apimtis kreditais	Visas studento darbo krūvis (val.)	Kontaktinio darbo valandos	Savarankiško darbo valandos
5	130	52	78

Dalyko (modulio) tikslas: studijų programos ugdomos kompetencijos
Kurso tikslas – ugdyti informacijos saugumo ir jo valdymo suvokimą informacijos srauto patikimumo, fizinio kibernetinio saugumo, asmens duomenų apsaugos prasmėmis. Siekiama ugdyti studentų gebėjimą atpažinti galimas grėsmes ir priimti teisingą sprendimą grėsmių išvengimui. ***Kurso metu ugdomos bendrosios kompetencijos:*** • Kritinis mąstymas ir atvirumas naujovėms: kurso metu studentai rinks įvairią informaciją, vertins įvairaus pavidalo (tekstas, nuotraukos, video medžiaga) informacijos autentiškumą, tikrumą. Mokysis kaip atpažinti ketinimus apgaule išvilioti asmens duomenis ar pinigus. ***Kurso metu ugdomos dalykinės kompetencijos:*** • Gebėjimas suprasti ir kurti informacinę verslo organizacijos infrastruktūrą, užtikrinti naudojamos informacijos patikimumą, teisinę apsaugą ir saugumą, optimizuoti vidinės ir išorinės organizacijos informacijos sklaidą: kurso metu studentai analizuos Lietuvos ir tarptautinius informacijos saugumą reglamentuojančius dokumentus.

Dalyko (modulio) studijų siekiniai	Studijų metodai	Vertinimo metodai
Studentas supras skirtingus saugumo aspektus ir grėsmių grupes, grėsmių poveikį.	Paskaitos, seminarai, savarankiškas mokymasis	Darbo seminarų metu vertinimas, tarpinio (kontrolinio) darbo vertinimas, egzaminas
Mokės naudotis įrankiais, leidžiančiais įvertinti gaunamą informaciją.		
Gebės aktyviai ieškoti, suprasti ir analizuoti iš įvairių šaltinių gaunamą informaciją, vertinti informacijos autentiškumą, tikrumą.		
Žinos verslo valdymo, informacinių sistemų saugumo sprendimus, gebės parinkti ir pritaikyti informacijos saugos sprendimus pagal kuriamos informacinės sistemos poreikius.		
Suvoks asmens psichologinio tvirtumo, kritinio mąstymo svarbą informacinio saugumo kontekste.		
Žinos pagrindinius informacijos saugumą reglamentuojančius įstatymus bei tarptautinius standartus. Gebės juos adaptuoti praktikoje.		

Temos	Kontaktinio darbo valandos							Savarankiškų studijų laikas ir užduotys	
	Paskaitos	Konsultacijos	Seminarai	Pratybos	Laboratoriniai darbai	Praktika	**Visas kontaktinis darbas**	**Savarankiškas darbas**	**Užduotys**
1. Įvadas. Pagrindinės sąvokos. Informacijos saugumą apibrėžiantys tarptautiniai standartai, ES ir Lietuvos įstatymai.	6		2				8	14	• ISO/IEC 27002:2022: 3, 6 ir 7 skyriai
2. Informacijos, verslo valdymo sistemų saugumas. IT infrastruktūros sluoksniai	4		2				6	10	• Fundamentals of information systems security (2018): 1 skyrius
3. Daiktų interneto saugumas	2	2					4	6	• Fundamentals of information systems security (2018): 2 skyrius
4. Grėsmių informacijos saugumui tipai, žalos lygiai, grėsmių valdymo strategijos.	4		2				6	12	• Fundamentals of

									information systems security (2018): 3 skyrius • Cybersecurity threats, malware trends, and strategies (2020): 5 skyrius
5. Informacinis karas. Priemonės vertinti informacijos tikrumą.	2		2				4	8	• TrueorFalse (2020): 19 skyrius
6. Socialinė inžinerija. Žmogaus psichologija, informacijos rinkimo būdai, būdai vykdyti organizuotą ataką.	10	2	6				18	20	• Social engineering: the science of human hacking (2018): 4 ir 9 skyriai
7. Tamsusis internetas. Galimybės ir grėsmės.	4		2				6	8	
Iš viso	**32**	**4**	**16**				**52**	**78**	

Vertinimo strategija	**Svoris proc.**	**Atsiskaitymo laikas**	**Vertinimo kriterijai**
Seminarų užduočių atlikimas	40%	Semestro eigoje	Seminarų metu bus nagrinėjami įvairūs scenarijai ir analizuojamos scenarijuose atliktos klaidos ir siūlomi sprendimai kaip klaidų buvo galima išvengti. Modeliuojamos socialinės inžinerijos atakos. Iš viso trys atsiskaitomosios užduotys, bent dvi atlikti bus privaloma.
Tarpinis (kontrolinis) atsiskaitymas	20%	Semestro viduryje	Kontrolinis darbas vykdomas raštu, darbe bus pateikta 10 uždarų klausimų ir 5 atviri klausimai. Už kiekvieną uždaro klausimo teisingą atsakymą bus skiriamas 1 taškas, o už kiekvieną atvirą klausimą – 2 taškai. Surinkti taškai proporcingai bus konvertuojami į balą.
Egzaminas	40%	Sesijos metu	Egzaminas vykdomas raštu. Egzamino metu bus pateikta 10 uždarų klausimų ir 5 atviri klausimai. Už kiekvieną uždaro klausimo teisingą atsakymą bus skiriamas 1 taškas, o už kiekvieną atvirą klausimą – 2 taškai. Surinkti taškai proporcingai bus konvertuojami į balą.

Autorius	**Leidimo metai**	**Pavadinimas**	**Periodinio leidinio Nr. ar leidinio tomas**	**Leidimo vieta ir leidykla ar internetinė nuoroda**
Privalomoji literatūra				
ISO, IEC	2022	ISO/IEC 27002:2022 Information security, cybersecurity and privacy	3 leidimas	

		protection - Information security controls		
David Kim, Michael G. Solomon	2018	Fundamentals of information systems security		Jones & Bartlett Learning
Christopher Hadnagy	2018	Social engineering: the science of human hacking		Wiley
ErdalOzkayaandRafiqulIslam	2019	Insidethe Dark Web		CRC Press
Tim Rains	2020	Cybersecurity threats, malware trends, and strategies: mitigate exploits, malware, phishing, and other social engineering attacks		Packt
Papildoma literatūra				
	2014	Lietuvos Respublikos kibernetinio saugumo įstatymas (suvestinė redakcija nuo 2021-12-01)		https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/f6958c2085dd11e495dc9901227533ee/asr
	2016	Bendrasis duomenų apsaugos reglamentas		https://www.stat.gov.lt/documents/29256/5591163/CELEX_32016R0679_LT_TXT.pdf
Cindy L. Otis	2020	True or False		