STUDIJŲ DALYKO (MODULIO) APRAŠAS

Dalyko (modulio) pavadinimas	Kodas
Informacinės saugos pagrindai	

Dėstytojas (-ai)	Padalinys (-iai)
Koordinuojantis: doc. dr. Igoris Belovas **Kitas (-i):**	Vilniaus universiteto Matematikos ir informatikos institutas Akademijos g. 4 LT-08663 Vilnius

Studijų pakopa	Dalyko (modulio) tipas
Pirmoji	Privalomas

Įgyvendinimo forma	Vykdymo laikotarpis	Vykdymo kalba (-os)
Auditorinė	7 semestras	Lietuvių

Reikalavimai studijuojančiajam	
Išankstiniai reikalavimai:	**Gretutiniai reikalavimai (jei yra):**
Programavimo pagrindai, Algoritmų teorija, Duomenų mokslo elementai	Algebra, Matematinė statistika

Dalyko (modulio) apimtis kreditais	Visas studento darbo krūvis	Kontaktinio darbo valandos	Savarankiško darbo valandos
5	133	55	78

Dalyko (modulio) tikslas: studijų programos ugdomos kompetencijos		
Dalyko tikslas – siekiama, kad studentai susipažintų su informacinių sistemų saugos problemomis bei metodais, skirtais apsaugoti informacines sistemas bei duomenis, ugdytų praktinius gebėjimus taikyti informacijos apsaugos technologijas.		
Dalyko (modulio) studijų siekiniai	**Studijų metodai**	**Vertinimo metodai**
Gebės spręsti problemas, organizuoti ir planuoti darbus vertinant informacinio saugumo grėsmes ir užtikrinant organizacijos saugumo politiką.	Probleminis dėstymas, kompiuteriniai praktiniai darbai, savarankiškas darbas, aktyvaus mokymosi metodai (grupės diskusija; situacijų analizė).	Individualus darbas, praktiniai darbai.
Gebės atlikti organizacijos saugumo grėsmių analizę, taikyti žinias informacinių sistemų saugumui stebėti ir apsaugos patikimumui įvertinti.	Kompiuteriniai praktiniai darbai, savarankiškas darbas.	Individualus darbas, praktiniai darbai
Gebės paaiškinti esmines informacinės saugos sąvokas, išmanys kriptografijos bei elektroninio parašo taikymo sritis.	Probleminis dėstymas, kompiuteriniai praktiniai darbai, savarankiškas darbas, aktyvaus mokymosi metodai (grupės diskusija; situacijų analizė).	Egzaminas, praktiniai darbai
Gebės pritaikyti reikiamas duomenų saugos priemones, siekiant užtikrinti organizacijos duomenų saugumą, atsižvelgiant į poreikį jas tobulinti.	Probleminis dėstymas, kompiuteriniai praktiniai darbai, savarankiškas darbas,	Praktiniai darbai
Gebės parinkti ir pritaikyti informacinę saugą užtikrinančius sistemų integravimo sprendimus, taikyti saugos standartus organizacijos veikloje.	Probleminis dėstymas, kompiuteriniai praktiniai darbai, savarankiškas darbas, aktyvaus mokymosi metodai (grupės diskusija; situacijų analizė).	Egzaminas, praktiniai darbai

Temos	Kontaktinio darbo valandos							Savarankiškų studijų laikas ir užduotys	
	Paskaitos	Konsultacijos	Seminarai	Pratybos	Laboratoriniai darbai	Praktika	**Visas kontaktinis darbas**	**Savarankiškas darbas**	**Užduotys**
1. Informacijos ir informacinių sistemų saugos sąvokos ir principai. Informacijos saugos problemos, objektai ir subjektai	2						**2**	**4**	Literatūros analizė
2. Informacijos saugos grėsmės. Grėsmių ir atakų klasifikacija. Informacijos saugos realizavimo principai ir mechanizmai.	2						**2**	**4**	Literatūros analizė.
3. Pagrindinės kriptografijos sąvokos. Kriptosistemų klasifikacija. Klasikinės kriptosistemos.	2				6		**8**	**10**	Literatūros analizė. Praktinės užduotys.
4. Blokiniai šifrai. AES kriptosistema. Elektroninės kodų knygos, šifro blokų grandinių, šifro atgalinio ryšio, srauto atgalinio ryšio ir skaitliuko režimai.	4				7		**11**	**12**	Literatūros analizė. Praktinės užduotys.
5. Srautiniai šifrai. Vernamo sistema. Golombo pseudoatsitiktinės sekos. Statistiniai testai. Tiesinių registrų sistemos.	4				6		**10**	**10**	Literatūros analizė. Praktinės užduotys.
6. Viešojo rakto kriptosistemos. RSA. RSA saugumas ir kriptoanalizė. Skaitmeniniai parašai.	3				7		**10**	**12**	Literatūros analizė. Praktinės užduotys.
7. Diskretieji logaritmai. Difi-Helmano raktų derinimo algoritmas. Difi-Helmano sistemos kriptoanalizė. Maišos funkcijos. Parašas su	3				7		**10**	**12**	Literatūros analizė. Praktinės užduotys.

maišos funkcija.									
8. Organizacinės apsaugos priemonės. Informacinių sistemų saugumo stebėjimas ir patikimumo vertinimas.	2						**2**	**4**	Literatūros analizė.
9. Egzaminas								**10**	Literatūros kartojimas, pasiruošimas egzaminui
Iš viso	**22**				**33**		**55**	**78**	

Vertinimo strategija	**Svoris proc.**	**Atsiskaitymo laikas**	**Vertinimo kriterijai**
Praktinių / laboratorinių / individualių darbų gynimai	50	Po kiekvieno praktinio darbo (semestro metu)	Vertinama 1–10 pažymių vertinimo skalėje: **10–9:** Puikios žinios ir gebėjimai. Vertinimo lygmuo. 90–100 % teisingų atsakymų. **8–7:** Geros žinios ir gebėjimai, gali būti neesminių klaidų. Sintezės lygmuo. 70-89 % teisingų atsakymų. **6–5:** Vidutinės žinios ir gebėjimai, yra klaidų. Analizės lygmuo. 50–69 % teisingų atsakymų. **4–3:** Žinios ir gebėjimai nesiekia vidutinių, yra (esminių) klaidų. Žinių taikymo lygmuo. 20–49 % teisingų atsakymų. **2–1:** Netenkinami minimalūs reikalavimai. 0–19 % teisingų atsakymų.
Egzaminas	50	Egzaminų sesijos metu	Vertinama 1–10 pažymių vertinimo skalėje: **10–9:** Puikios žinios ir gebėjimai. Vertinimo lygmuo. 90–100 % teisingų atsakymų. **8–7:** Geros žinios ir gebėjimai, gali būti neesminių klaidų. Sintezės lygmuo. 70–89 % teisingų atsakymų. **6–5:** Vidutinės žinios ir gebėjimai, yra klaidų. Analizės lygmuo. 50–69 % teisingų atsakymų. **4–3:** Žinios ir gebėjimai nesiekia vidutinių, yra (esminių) klaidų. Žinių taikymo lygmuo. 20–49 % teisingų atsakymų. **2–1:** Netenkinami minimalūs reikalavimai. 0–19 % teisingų atsakymų.

Autorius	**Leidimo metai**	**Pavadinimas**	**Leidimas**	**Leidimo vieta ir leidykla ar internetinė nuoroda**
Privaloma literatūra				
A. Mikalauskienė, Z. Brazaitis	2010	Informacinių sistemų sauga		Vilnius: Vilniaus universiteto leidykla
G. Skersys	2011	Informacijos sauga		Vilnius: TEV
W. W. Stallings	2017	Cryptography and Network Security: Principles and Practice	6th ed.	Boston, MA: Pearson Education
Papildoma literatūra				
E. Kazanavičius [ir kt.]	2008	Informacijos saugos vadyba		Kaunas: Vitae litera
E. Sakalauskas [ir kt.]	2008	Elektroninių dokumentų ir duomenų sauga		Kaunas: Vitae litera
E. Sakalauskas [ir kt.]	2008	Kriptografijos sistemos		Kaunas: Vitae litera
E. Sakalauskas [ir kt.]	2008	Kriptografijos teorija		Kaunas: Vitae litera
V. Stakėnas	2007	Kodai ir šifrai. Informacijos kodavimo ir kriptografijos pagrindai		Vilnius: Vaistų žinios
R. Šleževičienė	2005	Kriptografijos įvadas		Šiauliai: Šiaulių universiteto leidykla
O. Vasilecas [ir kt.]	2008	Informacinių sistemų sauga		Vilnius: Technika
A. Venčkauskas, E. Kazanavičius	2011	Informacinių technologijų saugos metodai		Vilnius: TEV
A. Venčkauskas, J. Toldinas	2008	Kompiuterių ir operacinių sistemų sauga		Kaunas: Vitae Litera
S. Azad, A. K. Pathan (eds.)	2019	Practical Cryptography: Algorithms and Implementations using C++		CRC Press/Taylor & Francis Group
M. E. Whitman, H. J. Mattford	2017	Principles of Information Security	6th ed.	Boston, MA : Cengage Learning