



DALYKO APRAŠAS

Dalyko pavadinimas	Kodas
Kibernetinio saugumo technologijos	

Dėstytojas (-ai)	Padalinys
Koordinuojantis: doc. dr Linas Bukauskas	Kibernetinio saugumo laboratorija Informatikos institutas
Kitas (-i):	Matematikos ir informatikos fakultetas Vilniaus universitetas

Studijų pakopa	Dalyko tipas
Antroji	Privalomasis

Įgyvendinimo forma	Vykdymo laikotarpis	Vykdymo kalba (-os)
Auditorinė	1 semestras	Lietuvių/Anglų

Reikalavimai studijuojančiajam
Išankstiniai reikalavimai: Bendro pobūdžio informacinių technologijų, unix žinios, bei telekomunikacijų pagrindai,.

Dalyko apimtis kreditais	Visas studento darbo krūvis	Kontaktinio darbo valandos	Savarankiško darbo valandos
5	138	64	74

Dalyko tikslas: studijų programos ugdomos kompetencijos		
<p>Bendrosios kompetencijos</p> <ul style="list-style-type: none"> • Dirbti ir mokytis savarankiškai, • Abstrakčiai kritiškai ir savikritiškai mąstyti, analizuoti, sisteminti ir vertinti informaciją • Identifikuoti ir spręsti problemas. <p>Dalykinės kompetencijos</p> <ul style="list-style-type: none"> • Modeliuoti, kurti ir specifikuoti IT paslaugas/sistemas parinkus tinkamą infrastruktūrą, • Praktiškai taikyti ir vertinti interneto saugumo technologijas, jų raidą ir kryptis, • Vertinti informacinių sistemų architektūras, • Realizuoti ir taikyti algoritmus, aktualius taikomajam uždaviniui, ir juos vertinti, • Rasti specifinę informaciją skirtinguose šaltiniuose ir ją sisteminti. 		
Dalyko studijų siekiniai	Studijų metodai	Vertinimo metodai
<p>Išskirti interneto tinklo sudėtinius komponentus ir suvokti jo veiklos principus bei tinklo protokolų funkcijas.</p> <p>Atpažinti, lyginti, analizuoti ir vertinti interneto saugumą, technologijų pažeidžiamumus ir kibernetinių atakų grėsmes.</p> <p>Suvokti alternatyvas užtikrinančias tinklų ir informacijos saugumą interneto technologijoms ir parinkti optimalią konkrečiam uždaviniui ar veiklai.</p>	<p>Įtraukiamoji paskaita, užduočių sprendimas pratybų metu ir savarankiškai, įvairių šaltinių studijavimas, pateikčių rengimas ir pristatymas, situacijų analizė, duomenų interpretavimas, projekcinė veikla, konsultavimas.</p> <p>Praktinės dirbtuvės</p> <p>Seminarai</p>	<p>Egzamino testas, projekto gynimas, uždavinių sprendimų vertinimas, savęs vertinimo testai</p>

Temos	Kontaktinio darbo valandos							Savarankiškų studijų laikas ir užduotys	
	Paskaitos	Konsultacijos	Seminarai	Pratybos	Laboratoriniai darbai	Praktika	Visas kontaktinis darbas	Savarankiškas darbas	Užduotys
1. Interneto ekosistema ir BGP protokolo apžvalga	2			0			2	2	Šaltinių studijavimas, uždavinių sprendimas
2. BGP ir interneto ryšio protokolai TCP/IP, LT interneto infrastruktūra ir IP protokolo pažeidžiamumai	2			4			6	6	Šaltinių studijavimas, projektinių užduočių analizė
3. TCP, DNS interneto ryšio protokolų saugumas, debesies paslaugos, Elektroninis parašas, PKI, RSA, ED25519 taikymai SSH paslaugose	4			4			8	8	Šaltinių studijavimas, projektinių užduočių analizė
4. Kibernetinis saugumas ir „kibernetinio karo“ technologijos, nacionalinės kibernetinio saugumo strategijos, pagrindinės koncepcijos	4			4			8	8	Šaltinių studijavimas, projektinių užduočių analizė
5. Žudymo grandinė, žvalgyba, atvirų šaltinių žvalgyba bei perimetro skenavimo metodikos, pasirengimas audi	4			4			8	8	Šaltinių studijavimas, projektinių užduočių analizė, uždavinių sprendimas
6. Juodieji šablonai (seminaras) ir socialinė inžinerija	8			8			16	16	Šaltinių studijavimas, projektinių užduočių analizė
7. Interneto paslaugų rizikos vertinimo metodikos	4			4			8	8	Šaltinių studijavimas, projektinių užduočių analizė
8. Įsilaužimų stebėseną (vidinė/išorinė) ir priemonės įsilaužimo užkardymui	4			4			8	8	Šaltinių studijavimas, uždavinių sprendimas
Pasiruošimas egzaminui								10	Šaltinių studijavimas
Iš viso	32			32			64	74	

Vertinimo strategija	Svoris proc.	Atsiskaitymo laikas	Vertinimo kriterijai
Praktinės užduotys	40	Pagal pratybų metu pateiktą grafiką	Projektai - 100 %. Teisingas teorinio/praktinio uždavinio sprendimas, gebėjimas pagrįsti sprendimą, gebėjimas atsakyti į klausimus susijusius su algoritmo internet.
Egzaminas raštu	60	Sausio mėn. sesijos metu	Raštu pateikiami atviri klausimai ar užduotys, kuriuose reikia taikyti įgytas žinias. Vertinimo kriterijai: <ul style="list-style-type: none"> • aiškus minčių dėstymas raštu; • kokybiškas atsakymo turinys; • argumentuotas sprendimas; • teisingas teorinio/praktinio uždavinio sprendimas.

Autorius	Leidimo metai	Pavadinimas	Periodinio leidinio Nr. ar leidinio tomas	Leidimo vieta ir leidykla ar internetinė nuoroda

Privalomoji literatūra				
Chris Hall, Richard Clayton, Ross Anderson, Evangelos Ouzounis,	2011	Inter-X: Resilience of the Internet Interconnection Ecosystem		European Network and Information Security Agency (ENISA)
Rytis Rainys	2011	Regionu interneto tinklo infrastruktūros patikimumo tyrimai	ISBN 978-609-457-014-8	VGTU leidykla TECHNIKA
Fernando Gont	2008	Security Assessment of the Internet Protocol		CPNI www.cpni.gov.uk
Joel Weise	2001	Public Key Infrastructure Overview	816-1279-10	Sun Microsystems
William Terrill	2008	WLAN Security Today: Wireless more Secure than Wired		Siemens Enterprise Communications
ENISA	2007	A basic collection of good practices for running a CSIRT	WP2007/2.4.9 /1 (CERT-D3.1)	ENISA
Papildoma literatūra				
Kari Saarelainen, Heikki Saarinen, Markus Saviaro	2011	Technologies with potential to improve the resilience of the Internet infrastructure	Version 1.0	European Network and Information Security Agency (ENISA)
Tom Olzak	2006	DNS Cache Poisoning: Definition and Prevention		http://adventuresinsecurity.com/Papers/DNS_Cache_Poisoning.pdf
Tzeyoung Max Wu	2009	Information Assurance Tools Report – Intrusion Detection Systems	0704-0188	Information Assurance Technology Analysis Center (IATAC)