VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS
STUDIJŲ MODULIO KORTELĖ
Informacinių sistemų katedra

A dalis

Modulio pavadinimas

Informacijos saugos technologijos

Modulio pavadinimas (anglų kalba)

Information Security Technologies

Modulio grupė	**Studijų dalyko**
Modulio blokas	**Mokslo krypties doktorantūros komiteto nustatyti dalykai**
Priklausomybė	**Katedros**

Mokslo krypties ir srities kodas		**Studijos**
T 007	**T 000**	**Doktorantūros**

Modulio kodas

Fakultetas		Katedra	B, A, M, I, D	Modulio Nr.*
F	M	I	S	D	21003

* modulio registracijos numeris katedroje

Kreditai

Iš viso:	Iš jų: KD, KS, KP
6	0

Atsiskaitymo forma

Į, E1, E2, E, BE, BD, TD, A	KD, KS, KP
E	

Studijų forma		Paskaitoms	Lab. darbams	Pratyboms	Aud. darbui	Sav. darbui	Iš viso
Nuolatinės studijos	F	64	0	0	64	96	160
Ištęstinės studijos	I						

Modulio tikslas

Suformuoti žinias informacijos saugos technologijos srityje.

Modulio tikslas (anglų kalba)

To form knowledge on information security technologies.

Suteikiamos žinios ir gebėjimai

Gebėjimas suprasti ir operuoti pagrindinėmis informacinio saugumo sąvokomis ir principais. Gebėjimas identifikuoti, aprašyti ir klasifikuoti grėsmes informacinėms sistemoms. Kriptografinių algoritmų ir protokolų veikimo principus žinios. Pagrindinės kompiuterinių tinklų ir informacinių sistemų saugumo užtikrinimo techninės žinios. Atakų prieš informacines sistemas veikimo principų žinojimas. Organizacinių apsaugos priemonių taikymo žinios.

Suteikiamos žinios ir gebėjimai (anglų kalba)

Ability to understand and operate main information security concepts and principles. Ability to identify, describe and classify threats to information technology systems. Knowledge of cryptographic algorithms/protocols mechanisms knowledge. General knowledge of computer network and information technology systems technical protection measures. Knowledge of attack mechanisms against information technology systems. Knowledge of organizational information security.

Modulio anotacija

Informacinio saugumo pagrindas (informacinio saugumo problematika, grėsmių klasifikacija ir evoliucija, identifikacija, autentifikacija, priėjimo kontrolė, saugumo strategijos, modeliai, principai, taksonomijos ir antologijos); Kriptografija (simetrinio ir viešojo rakto kriptografija, DES, AES, RSA, kriptografiniai protokolai, autentifikacija, elektroninis parašas, elektroninės esybės valdymas); Tinklų saugumas (maršrūtizavimas, ugniasienės, VPN, web saugumas, tinklo perimetro apsauga, kompiuterių apsauga, autentifikavimo technologijos); Atakos į informacinių technologijų sistemas (atakų tipai, realių pavyzdžių analizė, įsiskverbimų detektavimas, formalūs analizės metodai); Efektyvių informacijos apsaugos programų diegimas (teisiniai ir privatumo klausimai, saugumo standartai, geriausi taikomi metodai, saugumo politika).

Modulio anotacija (anglų kalba)

Information Security Fundamentals (information security problematics, classification and evolution of threats, identification, authentication, access control, security principals, strategies, models, taxonomies and ontologies); Cryptography (symmetric and public key cryptography, DES, AES, RSA. stream ciphers, cryptographic protocols, authentication, electronic signature, management of electronic identity); Network Security (routing, firewalls, VPN, web security, network perimeter protection, host-level protection, authentication technologies); Attacking Information Technology Systems (attack types, real-life case studies, intrusion detection, formal analysis techniques); Information Security Technologies (antivirus, IDS, host and perimeter protection systems, Honeypots); Implementing Effective Information Security Programs (legal, regulatory and privacy issues, security standards, security best practices, security policy).

Literatūra (autorius, leidinio pavadinimas, leidykla, metai)

1. W.Stallings. Cryptography and network security: principles and practice. 7th edition. Boston, MA : Pearson Education, 2017. ISBN 9781292158587.
2. Peltier, Thomas R. Information security fundamentals. Boca Raton, FL : CRC Press, Taylor & Francis Group, 2014. ISBN 9781439810620
3. J.Stewart, M.Chapple, D.Gibson. CISSP (ISC)2 Certified Information Systems Security Professional Official Study Guide 7th Edition. Sybex. 2015.
4. Campbell, Tony. Practical information security management : a complete guide to planning and implementation. New York, NY : Apress, 2016. ISBN 9781484216842.
2. Bhattacharyya, Dhruba K, autorius. Network anomaly detection : a machine learning perspective / Dhruba Kumar Bhattacharyya, Jugal Kumar
5. Bhattacharyya, Dhruba K, autorius. Network anomaly detection : a machine learning perspective / Dhruba Kumar Bhattacharyya, Jugal Kumar Kalita. xxv, 340 p. ISBN 9781466582088.
6. Gray hat hacking : the ethical hacker's handbook / Daniel Regalado ... [et al.]. 4th ed. xxix, 625 p. ISBN 9780071832380.
7. Noble, Steven. Building modern networks : create and manage cutting-edge networks and services / Steven Noble. vii, 305 p. ISBN 9781786466976.
8. Koehler, Thomas R. Understanding cyber risk : protecting your corporate assets. 2018. 141 p. ISBN 9781472477798

IT resursai:

Savarankiško darbo turinys

Užduoties pavadinimas	Sav. darbo apimtis vienai užduočiai					Užduočių skaičius				Iš viso valandų			
	Rėžis	Priimta											
		NL(S)	I(S)	I(T)	NL(T)	NL(S)	I(S)	I(T)	NL(T)	NL(S)	I(S)	I(T)	NL(T)
Namų darbas	4-27	24				4				96			

Savarankiško darbo grafikas

Užduoties tipas	Užduoties pateikimo(*) ir atsiskaitymo(+) savaitė																			
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Nuolatinės studijos																					
Namų darbas	*		1			2			3			4									
	+					1			2			3			4						

Įvertinimo sandara

Nuolatinės studijos: Gį= 0,6%.E+ 0,4 % ND
Galutinis įvertinimas (Gį) =60 proc. egzaminas(E) + 40 proc. namų darbai (ND)

Modulio sudarytojai (vardas, pavardė):
Antanas Čenys

Modulio egzaminuotojai (vardas, pavardė):
Antanas Čenys
Nikolaj Goranin

Katedros vedėjas (vardas, pavardė):
Dalius Mažeika

Doktorantūros komisijos nutarimas

1. Modulis **atestuojamas**
2. Modulis skirtas mokslo krypčiai: **Informatikos inžinerija**
3. Modulio atestacija galioja: nuo 2023-11-29 iki 2027-08-31

Modulį atestavo
Mokslo krypties doktorantūros komisijos pirmininkas (vardas, pavardė)
Arnas Kačeniauskas

Data 2023-11-29

VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS
STUDIJŲ MODULIO DARBO PROGRAMA
Informacinių sistemų katedra

B dalis

Modulio pavadinimas

Informacijos saugos technologijos

Modulio pavadinimas (anglų kalba)

Information Security Technologies

Modulio kodas						**Kreditai**		**Atsiskaitymo forma**	
Fakultetas		Katedra	B, A, M, I, D	Modulio Nr.*		Iš viso:	Iš jų: KD, KS, KP	Į, E1, E2, E, BE, BD, TD, A	KD, KS, KP
F	M	I	S	D	21003	6	0	E	

* modulio registracijos numeris katedroje

Studijų forma		Paskaitoms	Lab. darbams	Pratyboms	Aud. darbui	Sav. darbui	Iš viso
Nuolatinės studijos	F	64	0	0	64	96	160
Ištęstinės studijos	I						

Paskaitų temų sąrašas

List of the Course lecture topics

Temos (darbo) pavadinimas	Valandų skaičius			
	NL(S)	I(S)	I(T)	NL(T)
1. Informacijos saugos konceptai ir principai. 1. Information security concepts and principles.	2			
2. Informacijos saugos svarba ir vieta šiuolaikiniam gyvenime, istorinė raida. 2. Importance of information security in a modern life, historical perspective.	2			
3. Prieigos kontrolės metodai ir technologijos. 3. Access control methods and technologies.	2			
4. Atakų tipai ir jų aptikimo metodai. 4. Attack types and their detection methods.	4			
5. Žurnalinių įrašų analizės metodai ir technologijos. 5. Methods and technologies for log records analysis.	2			
6. Duomenų nutekinimo prevencijos metodai ir technologijos. 6. DLP methods and technologies.	2			
7. Informacijos saugos grėsmės skirtinguose OSI modelio lygiuose. 7. Security threats on different OSI model layers.	4			
8. Ugniasienių tipai ir technologijos. 8. Firewall types and technologies.	2			
9. Saugaus kompiuterio tinklo topologija. 9. Secure network topology.	2			
10. IDS ir medaus puodynių metodai ir technologijos. 10. IDS and honeypot methods and technologies.	2			
11. Saugios nutolusios prieigos užtikrinimo metodai. 11. Secure remote access insuring methods and technologies.	2			
12. Duomenų kodavimo istorija, istoriniai šifravimo algoritmai. 12. Data encryption history, historical encryption algorithms.	2			
13. Informacijos teorija. 13. Information theory.	4			
14. Šiuolaikiniai simetriniai šifravimo algoritmai 14. Modern symmetrical encryption algorithms.	4			
15. Šiuolaikiniai atviro rakto algoritmai. 15. Modern public key cryptography.	4			
16. Kvantinė kriptografija. 16. Quantum cryptography.	2			
17. Kriptoanalizės metodai. 17. Methods of cryptoanalysis.	4			
18. Kriptografiniai protokolai. 18. Cryptographic protocols.	4			
19. Informacijos saugos vieta organizacijoje. ISVS sąvoka. 19. Place of information security in a modern organization. Concept of ISMS.	2			
20. Rizikos valdymo koncepcija ir metodai. 20. Risk management concepts and methods.	2			
21. Veiklos tęstinumo užtikrinimo metodai. 21. Business continuity insurance methods.	2			

22. Informacijos saugos incidentų valdymo metodai. 22. Information security incident management methods.	2			
23. Modeliavimo ir simuliacijos metodai informacijos saugoje. 23. Simulation and modeling methods in information security.	4			
24. Operacinių sistemų sauga. 24. Operating system security.	2			
Iš viso:	**64**			

Modulio sudarytojai (vardas, pavardė):
Antanas Čenys

Modulio egzaminuotojai (vardas, pavardė):
Antanas Čenys
Nikolaj Goranin

Katedros vedėjas (vardas, pavardė):
Dalius Mažeika