Subject code	Credits
INF6017	6

Course title in Lithuanian

SAUGIOS ELEKTRONINĖS APLINKOS

Course title in English

SECURE DIGITAL ENVIRONMENTS

Short course annotation in Lithuanian (up to 500 characters)

Šiuolaikiniame pasaulyje veiklos procesams migruojant į debesų kompiuteriją, yra būtina užtikrinti informacinių sistemų apsaugą nuo kibernetinės erdvės grėsmių. Bendras supratimas (grėsmės, saugomi objektai, veiklos tęstinumo užtikrinimo reikalavimai, būtinybė saugoti asmens privatumą ir kitas pamatines vertybes) yra reikalingas optimizuojant (įvairių subjektų) veiklą ir įvertinant būtinus išteklius, skiriamus kibernetinio saugumo tikslams pasiekti. Pateikiama bendra informacija apie saugumo organizacijas (pvz. CERT) ir jų veiklą, saugumo organizavimą įmonėse, įvadas į tinklų saugumą ir informacinių sistemų saugumą.

Short course annotation in English (up to 500 characters)

In the modern world when business processes migrate to cloud computing, it is necessary to ensure the protection of information systems against cyber threats. A common understanding (risks, secured objects, requirements to business continuity ensuring, the need to protect personal privacy and other fundamental values) is required for optimization of (various subjects) activities and estimating the necessary resources for achievement of cyber security purposes. The course Provides general information about the security organizations (e.g. CERT) and its operation, the security organization in the enterprises, introduction to the networks security and information systems security.

Prerequisites for entering the course

Basic software development knowledge

Course aim

To convey the security principles applicable to telecommunication and information systems.

Content

No	Content (topics)
1.	Internet: security of open systems, their evolution.
2.	Viruses, botnets.
3.	E-identity in networks
4.	Cyber fraud, organised crime in Internet
5.	Hactivism
6.	Cyberwar
7.	National and international regulation
8.	Bid Data and privacy; information leakage; personal security in cyberspace, coding, keys.
9.	Hardware security
10.	Critical infrastructure, decentralisation
11.	Trends and future threats

Distribution of workload for students (contact and independent work hours)

Lectures	**45 hours**
Laboratory work	**15 hours**
Individual students work	**100 hours**
Total:	**160 hours**

Structure of cumulative score and value of its constituent parts

Final written exam (50%), mid-term written exam (17%), and assessments of laboratory (practical) work (33%).

Recommended reference materials

No.	Publication year	Authors of publication and title	Publishing house	Number of copies in		
				University library	*Self-study rooms*	*Other libraries*
Basic materials						
1.	2014	E. van Ommeren, M. Borrett, M. Kuivenhoven. Staying Ahead in the Cyber	Sogeti and IBM	Open access https://goo.gl/sJ6AVM		

		Security Game: What Matters Now		
2.	2012	Security Enhanced Applications for Information Systems	InTech	Open access http://goo.gl/2du0s1
3	2009	D. Farmer, W. Venema. Forensic Discovery.	Addison Wesley	Open access http://www.porcupine.org/forensics/forensic-discovery/
4	2006	NIST. An Introduction to Computer Security: The NIST Handbook	NIST	Open access http://www.freetechbooks.com/an-introduction-to-computer-security-the-nist-handbook-t725.html
Supplementary materials				
1	2014	L. Ablon, M.C. Libicki, A.A. Golay. Markets for Cybercrime Tools and Stolen Data: Hacker's Bazaar.	RAND	Open access http://www.rand.org/pubs/research_reports/RR610.html

Course programme designed by

Doc. Dr. K.Šidlauskas, Dr. R.Šablinskas