Name: **Safety Technology of Information Systems**		NEPTUN-code: *NBXIB1EMNE*	Number of periods/week: full-time: 2 lec + 0 sem + 2 lab
Credit: 4 *Requirement:* exam		*Prerequisite:* -	
Responsible: Valéria PÓSER, Ph.D.	*Position:* associate professor	*Faculty and Institute name:* John von Neumann Faculty of Informatics Institute of Biomatics	

Way of assessment:
- requirement of signature: mid-term exam
- Oral exam. Final mark is calculated as the average of the mid-term and the exam.

Competences

Course description:
Students will learn about the vulnaribilites of the elements of information systems, their security issues, protection methods, tools and their practical application. Major topics that are covered: The elements of informatics systems, its sensibility. Fundamental concepts of encryption. Symmetric and asymmetric encryption methods. Hash functions. Block cipher modes of operation. Authentication of message. Internet security protocols, SSL, TLS, IPsec. Security services of operation systems. Encryption, authentication, practical realization of digital signatures. Safe correspondence and data storage (PGP), key management, the authentication of keys, encryption of letters, digital signature, disassembling. Certification problems, password-based partner authentication. Users' identification, authentication, authorization, access control. User management. Secure remote operations. Public key infrastructure, its elements and function. Firewalls, penetration detecting, protection against viruses, data loss prevention, rescue and archiving.

Literature
Levente Buttyán, István Vajda: Cryptography and their Applications, Typotex, 2012 (in Hungarian) Tibor Szentgyörgyi –Csaba Filkor – Balázs Borbély: Construction of a Modern Work Environment, Windows Server 2012 and Windows 8 and Office 365 bases, Jedlik Oktatási Stúdió Budapest, 2012 (in Hungarian, electronic notes) Gregg Kreizman: An Introduction to Information Security Architecture, Gartner The Future of IT Conference, 2011 (electronic notes) Heys, Howard M. "A tutorial on linear and differential cryptanalysis." Cryptologia 26.3, 189-221. 2002 (electronic notes) John McCabe with the Windows Server team: Introducing Windows Server 2016, Microsoft Press, 2016