Biomatics and Applied Artificial Intelligence Institute			Semester 2. of the curriculum 2025-26-2			
Name of the subject:	Code of the subject:	Credits:	Weekly hours:			
				lec	sem	lab
Cyber security - Security awareness	NBXKB1EMNF	5	full-time	2	0	1
Responsible person for the subject: Valéria PÓSER, PhD			Classification: associate professor			
Subject lecturer(s): Anikó SZARVÁK						
Prerequisites:	NBXBK1EMNF	Introduction to cybersecurity				
Way of the assessment:	mid-term grade					

Course description	
Goal:	The course gives a general overview of current challenges in cybersecurity from the primary perspective of a conscious computer user. Various aspects of personal and (small) business cyber hygiene is examined together with related technologies with the aim of achieving a common mental basis for more specialized studies in security.
Course description:	Following broad introduction of general aims and terminology of cybersecurity, students are introduced to security aspects and threats regarding common day-to-day activities, like web browsing, direct messaging, installing of applications or using social media. A broad overview and introduction to applied cryptography is followed by practical considerations regarding modern cryptosystems and their features. Various supplementary topics, like data management, contingency planning, user authentication and authorization, risk management and social engineering are also examined.

Lecture schedule	
Education week	Topic
1.	General introduction to cybersecurity – goals and requirements, basic concepts and definitions, history and trends
2.	Cyber threat landscape – threat and defense actors, targets (attack surface), major techniques and tools (attack vectors), public threat resources and services, white and dark markets, major incidents (case studies)
3.	Browsing the web – general security of web mechanisms (browsers and servers, DNS, URL, HTTP, HTML, DOM, scripting), web identity and tracking, malicious web services, common threats, case studies
4.	E-mail services and direct messaging platforms – email mechanisms (MUA, MTA, SMTP, MIME), direct messaging platforms, distribution and subscription services, common threats, case studies
5.	Zero Trust Architecture.
6.	Secure password storage and verification, password policies, password cracking, personal and collaborative password security/management. Secure use of application credentials.
7.	Social media and cloud data sharing platforms – data driven economy, right to be forgotten, user profiling and tracking, bots and trolls, cyberbullying, incidents, and case studies. OSINT
8.	Holiday
9.	Digital identity, user authentication (three factors), authorization and access control, access control models (ACL, DAC, MAC, RBAC, ABAC, Bell-LaPadula), access control of devices, accounts and sessions, auditing, and

	accountability. Major authentication/authorization technologies (Active Directory, LDAP, Radius, Kerberos, EAP, OpenID, SAML).
10.	GDPR
11.	Assets in cybersecurity – personal, corporate and public data, networked services and cloud infrastructure, people and processes, supply chains, internal requirements (policies), external requirements (laws, directives, guidelines and sectoral requirements in EU and Hungary).
12.	Critical data and service management – identification of important assets, backup and archival strategies, long time preservation, high availability, contingency planning, disaster recovery.
13.	The human factor – threats and techniques of social engineering, case studies
14.	Theoretical test Extra Theoretical test (outside the time of the lesson)

Mid-term requirements

Conditions for obtaining a mid-term grade/signature	Student participation in the lectures and labs is required. All homeworks and the classroom test are required to complete during the midterm.

Assessment schedule

Education week	Topic
14	All topics
14	Extra Theoretical test (outside the time of the lesson)

Method used to calculate the *mid-term grade* (to be filled out only for subjects with mid-term grades)

Type of the replacement

Type of the replacement of written test/mid-term grade/signature	Extra Theoretical test at week 14. Substitution of the signature: once during one of the first 10 working days of the examination period.

Type of the exam (to be filled out only for subjects with exams)

Theoretical test

Calculation of the exam mark (to be filled only for subjects with exams)

A minimum of 50% must be achieved.

Final grade calculation methods:

Achieved result	**Grade**
89%-100%	excellent (5)
76%-88<%	good (4)
63%-75<%	average (3)
51%-62<%	satisfactory (2)
0%-50<%	failed (1)

References

Obligatory:	Class materials published in Moodle.
Recommended:	• Ciampa Mark D : Security Awareness - Applying Practical Security in Your World, ISBN: 9781305500372

	• David Willson, Henry Dalziel: Cyber Security Awareness for Accountants and CPAs, Syngress Media 2015, ISBN: 9780128047224 • David Willson, Henry Dalziel: Cyber Security Awareness for Corporate Directors and Board Members, Syngress Media 2015, ISBN: 9780128047569
Other references:	-