COURSE DESCRIPTION

Introduction to cybersecurity

Academic year 2026-2027

1. Programme-related data

1.1. Higher Education Institution	Babeș-Bolyai University
1.2. Faculty	History and Philosophy
1.3. Department	Department of International Studies and Contemporary History
1.4. Field	Security Studies
1.5. Level of study	Bachelor's degree
1.6. Degree programme / Qualification	Security studies in English
1.7. Form of education	Full-time

2. Course-related data

2.1. Course title	**Introduction to Cybersecurity**			Course code	**HLE3318**
2.2. Course coordinator	Iulian-Florentin Popa				
2.3. Seminar coordinator					
2.4. Year of study	2	2.5. Semester	3	2.6. Type of assessment	Exam
2.7. Course status	Optional			2.8. Course type	Specialisation subject

3. Total estimated time (hours per semester of teaching activities)

3.1. Number of hours per week	**4**	of which: 3.2. course	**2**	3.3. seminar/ laboratory/ project	**2**
3.4. Total of hours in the curriculum	**56**	of which: 3.5. course	**28**	3.6. seminar/ laboratory	**28**

Time allocation for individual study (IS) and self-taught activities (ST)	**hours**
Learning from textbooks, course materials, bibliography, and notes (IS)	25
Additional research in the library, on subject-specific electronic platforms, and on-site	20
Preparing seminars/ laboratories/ projects, assignments, reports, portfolios, and essays	15
Tutoring (professional guidance)	1
Examinations	4
Other activities	4
3.7. Total hours of individual study (IS) and self-taught activities (ST)	**69**
3.8. Total hours per semester	**125**
3.9. Number of credits	**5**

4. Prerequisites (where applicable)

4.1. curriculum-related	Not applicable
4.2 skills-related	Basic skills in operating ICT tools and equipment are required.

5. Specific conditions (where applicable)

5.1. course-related	Not applicable
5.2. seminar/laboratory-related	Smart board or projector, workstations (e.g. PC, laptop)

6.1. Competencies resulting from the completion of the degree programme *(as referred to in the curriculum)*[1]

[1] The professional and/or transversal skills targeted by the subject for which the course description is prepared will be copied from the curriculum of the degree programme. For each competency, the complete entry, including the competency code, will be copied with the exact wording that appears in the curriculum, without any changes.

Professional competencies	
Competency code	**Competency**
PC1	Analysis of the national and international security environment
PC3	Security risk and vulnerability assessment
PC11	Strategic security advisory and policy recommendations
Transversal competencies	
Competency code	**Competency**
TC4	Professional ethics and accountability
TC5	Autonomous decision-making and responsibility management

6.2. Learning outcomes relevant to the degree programme (as referred to in the curriculum)[2]

Learning outcomes targeted by the subject		
Competency code	**Knowledge and comprehension**	**Specific academic skills**
PC1	1. C11:The student/graduate explains key concepts in strategic studies and international security (hybrid threats, deterrence, human security) relevant to security assessments.	1. A8: The student/graduate produces security assessments and forward-looking scenarios based on geopolitical indicators and risk analysis.
PC3	2. C12: The student/graduate describes risk management frameworks (identify–analyse–evaluate–treat–monitor) applicable to physical and organisational security.	2. A9: The student/graduate applies vulnerability assessment tools and proposes context-specific risk mitigation measures.
PC11	3. The student/graduate describes the methods of strategic analysis, risk assessment, and decision-making support used in the field of security.	3. A13: The student/graduate formulates security recommendations and action plans for clients/organisations using data and analytical assessments.
TC4	The student/graduate explains the principles of professional ethics, academic integrity, and social responsibility in professional and institutional activities.	A3: The student/graduate applies fundamental ethical principles and legislation in scientific research, including research integrity aspects. They conduct, review or report research while avoiding misconduct such as fabrication, falsification and plagiarism. A5: The student/graduate develops and demonstrates in-depth knowledge and complex understanding of a specific research field, including responsible research, ethical and scientific integrity principles, respect for privacy and GDPR requirements related to research activities in a given discipline.
TC5	The student/graduate describes methods and tools for organizing activities, time management, and task prioritization in academic and organizational contexts.	The student/graduate autonomously manages academic activities and individual tasks, respecting deadlines, ethical standards, and the specific requirements of the university environment.

7. Subject-specific learning outcomes

If no competency is copied from either of the two categories, the row corresponding to that category is deleted from the table.

[2] The learning outcomes relevant for the degree programme and targeted by the subject for which the course description is prepared will be listed. The entries, copied without any changes from the Curriculum by subject type (Core Subject/Specialisation Subject/Complementary Subject), are listed under the corresponding competency.

Knowledge and comprehension
1. The student/graduate explains the fundamental principles of cybersecurity, the typologies of cyber threats (malware, phishing, ransomware, APT attacks), and their impact on organizational and national security.
2. The student/graduate describes the protection mechanisms of cyber infrastructures and endpoints, including access control, identity management, data encryption, network security, and cybersecurity incident management.
3. The student/graduate understands the role of cybersecurity technologies and tools in the detection, analysis, and prevention of cyber threats in institutional and international contexts.
4. The student/graduate describes the stages of cyber incident response and digital crisis management, including incident identification, impact analysis, crisis communication, and operational recovery measures.
Specific academic skills
1. The student/graduate applies the methodology for analysing cyber risks and vulnerabilities in order to assess the impact of threats on information systems and critical infrastructures.
2. The student/graduate describes and uses concepts and theories specific to cybersecurity for the analysis of phenomena within the field of cybersecurity.
3. The student/graduate carries out academic research and interdisciplinary analysis activities using scientific sources, databases, and digital resources relevant to the field of cybersecurity.

8. Contents

8.1. Course	Teaching and learning methods	Remarks[3]
Fundamentals of Cybersecurity. The Cyber Dimension of Security	Lecture, debate	
Specialized Terminology. Cybersecurity Risks, Threats, and Vulnerabilities	Lecture, debate	
The CIA Triad and the Cybersecurity Cube	Lecture, debate, case study	
Organizational Cybersecurity. Minimum Cybersecurity Requirements for Organizations	Lecture, debate	
Mobile Device Cybersecurity	Lecture, debate	
Physical Security of Endpoints and Cyber Infrastructures	Lecture, debate	
Human Resource Cybersecurity. Security Requirements	Lecture, debate	
Cybersecurity Incident Response	Lecture, debate, case study	
Organization of Cybersecurity Incident Response	Lecture, debate, case study	
Cybersecurity Standards	Lecture, debate, case study	
Mobile Devices (MD) Cybersecurity	Lecture, debate, case study	
IoT Cybersecurity	Lecture, debate, case study	
Generative AI and Large Language Models (LLMs) in Cybersecurity	Lecture, debate, case study	
Romania's Cybersecurity Strategy	Lecture, debate, case study	

Ozkaya, Erdal, *Cybersecurity: The Beginner's Guide. A Comprehensive Guide to Getting Started in Cybersecurity*, Birmingham, Packt Publishing, 2019.

McDonough, Bart, *Cyber Smart: Five Habits to Protect Your Family, Money, and Identity from Cyber Criminals*, Indianapolis, Wiley, 2019.

Blau, Alex et al., *Cybersecurity*, Boston, Massachusetts, Harvard Business Review Press, 2019.

[3] For example, organisational aspects, recommendations for students, specific aspects relating to the course/seminar, such as inviting experts in the field, etc.

Brooks, Charles J., Craig, Philip, Short, Donald, Somerset, Christopher, *Cybersecurity Essentials*, Hoboken, New Jersey, John Wiley & Sons, 2018.

Sanger, David E., *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age*, New York, Crown Publishing Group, 2018.

Directoratul Naţional pentru Securitate Cibernetică (DNSC), *Ghid de securitate cibernetică*, Bucureşti, 2021, disponibil la: Ghid de securitate cibernetică 2021.

Serviciul Român de Informaţii (SRI), *Ghid de bune practici de securitate cibernetică*, Bucureşti, 2020, disponibil la: Ghid de bune practici de securitate cibernetică.

Fortinet, *AI In Cybersecurity: Key Benefits, Defense Strategies, & Future Trends,* disponibil la: fortinet.com.

H O T Ă R Â R E privind aprobarea Strategiei de securitate cibernetică a României, pentru perioada 2022—2027, precum şi a Planului de acţiune pentru implementarea Strategiei de securitate cibernetică a României, pentru perioada 2022—2027, disponibil la https://securitatea-cibernetica.ro/documente/Strategia-de-securitate-cibernetica-a-Romaniei.pdf.

CIS Critical Security Controls v 8.1, disponibil la https://learn.cisecurity.org/cis-controls-download

8.2. Seminar/ laboratory	**Teaching and learning methods**	**Remarks**
Fundamentals of Cybersecurity. The Cyber Dimension of Security	Lecture, debate	
Specialized Terminology. Cybersecurity Risks, Threats, and Vulnerabilities	Lecture, debate	
The CIA Triad and the Cybersecurity Cube	Lecture, debate, case study	
Organizational Cybersecurity. Minimum Cybersecurity Requirements for Organizations	Lecture, debate	
Mobile Device Cybersecurity	Lecture, debate	
Physical Security of Endpoints and Cyber Infrastructures	Lecture, debate	
Human Resource Cybersecurity. Security Requirements	Lecture, debate	
Cybersecurity Incident Response	Lecture, debate, case study	
Organization of Cybersecurity Incident Response	Lecture, debate, case study	
Cybersecurity Standards	Lecture, debate, case study	
Mobile Devices (MD) Cybersecurity	Lecture, debate, case study	
IoT Cybersecurity	Lecture, debate, case study	
Generative AI and Large Language Models (LLMs) in Cybersecurity	Lecture, debate, case study	
Romania's Cybersecurity Strategy	Lecture, debate, case study	

Ozkaya, Erdal, *Cybersecurity: The Beginner's Guide. A Comprehensive Guide to Getting Started in Cybersecurity*, Birmingham, Packt Publishing, 2019.

McDonough, Bart, *Cyber Smart: Five Habits to Protect Your Family, Money, and Identity from Cyber Criminals*, Indianapolis, Wiley, 2019.

Blau, Alex et al., *Cybersecurity*, Boston, Massachusetts, Harvard Business Review Press, 2019.

Brooks, Charles J., Craig, Philip, Short, Donald, Somerset, Christopher, *Cybersecurity Essentials*, Hoboken, New Jersey, John Wiley & Sons, 2018.

Sanger, David E., *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age*, New York, Crown Publishing Group, 2018.

Directoratul Național pentru Securitate Cibernetică (DNSC), *Ghid de securitate cibernetică*, București, 2021, disponibil la: Ghid de securitate cibernetică 2021.

Serviciul Român de Informații (SRI), *Ghid de bune practici de securitate cibernetică*, București, 2020, disponibil la: Ghid de bune practici de securitate cibernetică.

Fortinet, *AI In Cybersecurity: Key Benefits, Defense Strategies, & Future Trends,* disponibil la: fortinet.com.

H O T Ă R Â R E privind aprobarea Strategiei de securitate cibernetică a României, pentru perioada 2022—2027, precum și a Planului de acțiune pentru implementarea Strategiei de securitate cibernetică a României, pentru perioada 2022—2027, disponibil la https://securitatea-cibernetica.ro/documente/Strategia-de-securitate-cibernetica-a-Romaniei.pdf.

CIS Critical Security Controls v 8.1, disponibil la https://learn.cisecurity.org/cis-controls-download

9. Evaluation

Type of activity	9.1 Evaluation criteria[4]	9.2 Evaluation methods[5]	9.3 Percentage in the final grade
9.4. Course	Degree of understanding of the fundamental concepts of cybersecurity; ability to analyse and interpret cyber threats and vulnerabilities; correct use of specialized terminology	EXAM	50%
9.5. Seminar/ laboratory	Ability to apply theoretical concepts within cybersecurity platforms and exercises; understanding of protection mechanisms and incident response	CISCO Test	25%
	Capacity for critical analysis and resolution of cybersecurity scenarios; argumentation of proposed solutions and use of relevant academic and technical sources	Theoretical-applied exercise	25%
9.6 Minimum standard for passing			
The student must obtain at least 5 (five). The student must demonstrate basic knowledge of the fundamental concepts of cybersecurity, threat typologies, cybersecurity principles, and the responsible use of digital technologies.			

10. SDG labels (Sustainable Development Goals)[6]

	○	Sustainable Development Generic Label

[4] The evaluation criteria must directly reflect the learning outcomes targeted at the level of the degree programme respectively at the level of the subject. More specifically, the learning outcomes set out in the expected learning outcomes are assessed.

[5] Both final evaluation methods and ongoing evaluation strategies should be established.

[6] Select a single label which, according to the *Implementation of SDG labels in the academic process*, best matches the subject. If the subject addresses sustainable development in a generic manner (i.e. by presenting/introducing the general framework of sustainable development, etc.), then the Sustainable Development generic label may be applied. If none of the labels describe the subject, select the last option: *"No label applies."*

								No label applies

Date of entry:
...

Signature of course coordinator

.....

Signature of seminar coordinator

.....

Date of approval in the department:
...

Signature of the head of department

.....