CYBERSECURITY

Str. Dr. Ion Rațiu, Nr. 5-7
550012, Sibiu, România
stiinte.ulbsibiu.ro

Tel.: +40 269 21.66.42
Fax: +40 269 21.66.17
E-mail: stiinte@ulbsibiu.ro

1. Mission of the study program

The fundamental mission of the *Cybersecurity* master's degree program is to train specialists capable of protecting information and systems owned by organizations and governments against cyber threats in an increasingly digitally interconnected world. This program aims to prepare students to become experts in protecting information systems and networks against cyber threats by providing students with a solid foundation in cybersecurity technologies and policies, as well as practical skills to manage and mitigate security risks.

In order to fulfill its mission, the *Cybersecurity* Master's program ensures the development and training of professional and transversal competences, useful for the qualifications obtained (described by the learning outcomes: knowledge, skills, responsibility and autonomy), in line with national and international standards.

2. Objectives of the study program

- Understanding the fundamental concepts and principles of cyber security. Students will learn about cyber threats, vulnerabilities of information systems and how to protect systems from cyber attacks;
- Developing proficiency in risk analysis. Students will learn how to identify and assess cyber risks and develop appropriate security strategies to mitigate these risks;
- Protecting data and information. Students will learn how to implement security systems to protect data and information. This may include encryption, authentication and access control;
- Detecting and preventing cyber threats. Students will learn how to detect and prevent cyber threats, such as virus or phishing attacks, using advanced security tools;
- Developing analytical skills. Students will learn how to perform security analysis and identify system vulnerabilities so that appropriate security solutions can be developed;
- Security incident communication and management. Students will learn how to successfully communicate security issues and develop action plans to manage security incidents;
- Understanding cyber threats and vulnerabilities. Students will learn about different types of cyber threats such as hacking, phishing, malware, DDOS attacks and more;
- Develop the technical skills needed to protect information and computer systems from cyber attacks. These include, among others, security data analysis, cryptography, network security, application security, and developing cybersecurity solutions;
- Developing management and leadership skills. These include developing cybersecurity policies, managing cybersecurity risks, developing cybersecurity strategies, and coordinating cybersecurity efforts in the organization:
- Understanding cybersecurity regulations and standards. Students will be familiarized with various cybersecurity regulations and standards such as GDPR, NIST and ISO/IEC 27001;
- Developing the ability to work in teams. Students will have the opportunity to work in teams and develop communication and collaboration skills with peers;
- Developing ethical and legal skills. This objective includes learning about applicable ethical and legal norms and standards in the field of cybersecurity, as well as the social and legal impact of cyber-attacks;
- Developing management and leadership skills. Students will learn how to lead cybersecurity teams and make strategic decisions to protect organizations against cyber threats.

- Create the prerequisites to be able to provide teams capable of improving cybersecurity locally and nationally in line with international realities;
- Developing innovative security solutions. The final objective of the master's program is to prepare students to innovate and develop new security solutions to address the increasingly complex challenges of cybersecurity.

3. Study program premises and deliverables

The *Cybersecurity* master's degree program of the Informatics master's field of university studies, is part of the professional master's degree programs, being mainly oriented towards the training of graduates interested in concepts and solutions for the improvement and practical application of specific elements of cybersecurity. The study program ensures the formation of cognitive, professional (instrumental) and attitudinal (interpersonal) skills in accordance with national and international standards.

The competences developed by the graduates of this study program qualify them for the following occupations, according to the diploma supplement and RNCIS registration - expert in computer forensics; 2529.6 - ICT security administrator; 2529.7 - ICT systems security consultant; 2529.8 - ICT systems security manager; 2529.9 - semantic technologies engineer.

4. Teaching activity

Courses	364 hours
Seminars	-
Laboratories	392 hours
Projects	-
Practical work	75 hours

5. Student assessment

	Number of assessments/years of study			
Evaluation type	**Year 1**	**Year 2**	**TOTAL**	**%**
Exams	8	8	16	84.21
Colloquiums	1	2	3	15.79
Other forms	-	-	-	-

6. How to apply (access conditions). Conditions for enrolment in the following year of study. Conditions for passing one year of study.

Admission to the *Cybersecurity* master's degree program is based exclusively on the candidate's academic skills and no discriminatory criteria are applied. Enrolment in the admission competition is based solely on the bachelor's degree or other equivalent academic qualifications. Admission is based on an oral test assessed pass/fail, a language proficiency test assessed pass/fail and the classification of candidates admitted to the oral test is based entirely on the mark obtained in the bachelor's degree examination. The admission regulations present the admission criteria as well as the criteria for the admission of candidates with the same mark in the bachelor's degree examination.

Enrolment for the following year is conditional on meeting the promotion conditions set out in the Regulation on the professional activity of students.

7. Equal opportunities

The recruitment, admission, transfer and mobility of students to the *Cybersecurity* program are carried out transparently in accordance with the legislation in force and the procedures approved by

the ULBS Senate. Admission is based exclusively on the candidate's academic skills and does not apply any discriminatory criteria.

8. Program sustainability

From the perspective of environmental sustainability, the *Cybersecurity* study program promotes efficient use of resources through the following measures: configuring the study groups to minimize energy consumption related to the conduct of teaching activities but ensuring efficient professional training; encouraging the use of electronic format for homework, reports or projects; using electronic support materials.

Also, the waste resulting from applied activities is managed according to the rules in force and the waste collection system adopted by ULBS.

There is a great need for computer specialists today. With the rapid technological advancement and increasing dependence on technology in various fields, the demand for computer professionals has increased significantly.

Professional training through the *Cybersecurity* master's program responds to the needs of society by conferring sustainability to social and economic development.

9. Making training flexible. Conditions.

The flexibility of the study program is ensured through optional and elective courses.

There are 6 optional courses, grouped in pairs into 3 packages, from which students will choose at least one. The optional courses are offered starting from the second semester. The large number of optional courses adds flexibility to the study program and allows students to acquire competences for various professional pathways.

10. Methodology for assessing competences at the end of studies

The conditions for taking the graduation examination are set out in the applicable Methodology for the Completion of Studies, approved by the University Senate. According to this methodology, the presentation to the graduation examination is conditional to the passing of all the subjects foreseen in the curriculum.

GRADUATION EXAM

1 *Dissertation writing period: semesters 3-4;*
2 *Registration period for the graduation exam - during June.*
3 *Period for taking the dissertation examination: week 40 of year II*
4 *Number of credits for the dissertation examination: 10 credits.*

11. Preparation for a teaching post by admission exam

In order to fill a teaching position (secondary, high school or higher education in the undergraduate field), the graduate must have a Certificate of Graduation from a study program for psycho-pedagogical training (which allows the exercise of the teaching profession) coordinated by the Department for the Preparation of Teachers at ULBS (or at another university).

The psycho-pedagogical training for obtaining the Graduation Certificate is done following the completion of two modules:

(1) Module I (30 credits) - which is carried out additionally, in parallel with the undergraduate studies or as a postgraduate program, at the end of which the Graduation Certificate (Module I) is obtained.
(2) Module II (30 credits) - to be taken after the bachelor's degree, in parallel with the master's degree or postgraduate studies. It is finalized with a Certificate of Completion (in-depth level).