COURSE DESCRIPTION CARD - SYLLABUS

Course name
Pre-thesis Seminar [S1Cybez1>SEMP]

Course

Field of study
Cybersecurity

Year/Semester
3/6

Area of study (specialization)
–

Profile of study
general academic

Level of study
first-cycle

Course offered in
Polish

Form of study
full-time

Requirements
compulsory

Number of hours

Lecture
0

Laboratory classes
0

Other
0

Tutorials
0

Projects/seminars
30

Number of credit points

2,00

Coordinators

prof. dr hab. inż. Mariusz Głąbowski
mariusz.glabowski@put.poznan.pl

Lecturers

Prerequisites

Has a solid knowledge of computer science, teleinformatics, and key aspects of cybersecurity, acquired throughout their education. Can clearly and effectively present their ideas, preparing professional multimedia presentations using appropriate tools. Efficiently utilizes various sources of information and understands the dynamic nature of technological advancements, which motivates them to continuously enhance their skills in cybersecurity.

Course objective

The course aims to introduce cybersecurity students to the key principles and requirements for preparing their thesis, including conducting a systematic literature review and compiling an appropriate bibliography. The classes provide ongoing supervision and support for planning and systematically executing the project, allowing students to present their initial assumptions and conclusions derived from analyzing sources related to their chosen research area. During the seminar, participants refine their ability to clearly and convincingly present their concepts and research results using various multimedia tools. The course also fosters the development of skills in precise reasoning and logical deduction, which are essential for engineering work and future careers in cybersecurity.

Course-related learning outcomes

Knowledge:
During the seminar, the student will deepen their knowledge of complex data structures, data administration principles, and related standards. They will also expand their understanding of cybersecurity and privacy principles, which are essential for managing risks associated with the use, processing, storage, and transmission of information or data. [K1_W02]
The student will gain a deeper understanding of the lifecycle, design, and operation of software-based IT systems that are resistant to cyberattacks. [K1_W09]
They will also enhance their knowledge in designing, configuring, and maintaining IT systems. [K1_W11]
Additionally, the student will acquire knowledge in project management. [K1_W18]

Skills:
The student is capable of utilizing literary sources, integrating acquired information, evaluating and interpreting it, and drawing conclusions to solve complex and unconventional problems in the field of cybersecurity. [K1_U01]
They can apply appropriately selected methods and tools, including advanced information and communication technologies. [K1_U02]
The student is able to plan and conduct software, system, and network security tests to identify vulnerabilities and propose solutions to enhance the security of the system developed in their diploma project. [K1_U03]
They are proficient in planning and conducting computer simulations and measurements, including simulations and measurements related to ICT systems performance. Additionally, they can present the obtained results in numerical and graphical form, interpret them, and draw appropriate conclusions. [K1_U04]
The student is capable of preparing and delivering a presentation in Polish on their engineering project. [K1_U11]
They can prepare and orally present a concise report in both Polish and a foreign language, addressing current problems and achievements related to their engineering work. [K1_U12]
The student is able to plan and organize individual and team work, including developing and executing a work schedule that ensures deadlines are met. They also apply occupational health and safety regulations and can effectively collaborate in interdisciplinary and multicultural teams. [K1_U15]

Social competences:
The student understands the importance of enhancing professional, personal, and social competencies and recognizes that knowledge and skills in cybersecurity evolve rapidly. [K1_K01]
They acknowledge the significance of knowledge in solving cybersecurity-related problems and are aware of the necessity of consulting experts when tackling engineering tasks that exceed their own competencies. [K1_K02]
The student is conscious of the importance of independent work and adherence to professional ethics. They are prepared to follow teamwork principles, take responsibility for jointly executed tasks, and respect the achievements and traditions of the profession. [K1_K05]

Methods for verifying learning outcomes and assessment criteria

Learning outcomes presented above are verified as follows:

Formative Assessment:
- Based on participation in discussions related to student presentations.
Summative Assessment:
- Evaluation of three presentations prepared and delivered using any selected tool on the following topics:
- Objective and scope of the thesis, general assumptions, and implementation plan
- Plan for a systematic literature review
- Results of the conducted literature review
- Assessment of the bibliography list compiled as a result of the literature review, formatted according to the chosen citation style.
- Grading is conducted according to the University Study Regulations.Earning at least 50% of the possible points is a prerequisite for passing.

Programme content

The pre-thesis seminar supports the process of selecting an engineering thesis topic, properly planning

and executing the project, with a particular emphasis on the literature review. This module includes an overview of the thesis process, general guidelines for preparing the thesis, recommendations for creating presentations, and conducting a systematic literature review.

Course topics

1. Discussion of the applicable thesis requirements and regulations.
2. Presentation of the fundamental standards for diploma theses.
4. Explanation of the principles for structuring abstracts.
5. Introduction to using source materials and an overview of major online scientific publication sources.
6. Discussion on systematic literature review methods.
7. Overview of popular citation styles for reference lists.
8. Guidelines for preparing multimedia presentations, covering both content and methodology.
9. Student progress presentations and discussions on their proposed concepts.
10. Presentation of literature review plans and their outcomes, followed by a group discussion.

Teaching methods

Student-prepared presentations and discussions related to them.

Bibliography

Basic:
Automation of systematic literature reviews: A systematic literature review, Dinter R., Tekinerdogan B., Catal C., Information and Software Technology 136: 106589, 2021 (https://doi.org/10.1016/j.infsof.2021.106589).
How-to conduct a systematic literature review: A quick guide for computer science research, Carrera-Rivera A., Ochoa W., Larrinaga F., Lasa G., MethodsX 9: 101895, 2022 (https://doi.org/10.1016/j.mex.2022.101895).

Additional:
Dobre rady dla piszących teksty naukowe, Lindsay D., Wrocław: Politechnika Wrocławska, 1995.
Jak pisać pracę

Breakdown of average student's workload

	Hours	ECTS
Total workload	60	2,00
Classes requiring direct contact with the teacher	30	1,00
Student's own work (literature studies, preparation for laboratory classes/ tutorials, preparation for tests/exam, project preparation)	30	1,00