COURSE DESCRIPTION CARD - SYLLABUS

Course name
Introduction to Cybersecurity [S1Cybez1>WdC]

Course

Field of study
Cybersecurity

Year/Semester
1/1

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
30

Laboratory classes
0

Other
0

Tutorials
0

Projects/seminars
30

Number of credit points

4,00

Coordinators

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

Lecturers

Prerequisites

None

Course objective

The course aims to introduce students to the fundamentals of cybersecurity and data protection, covering topics such as information security, risk assessment, and security management. It combines theoretical knowledge with practical skills through group projects involving risk analysis, the design and implementation of data protection systems, and preparation for cybersecurity operations in an international context (e.g., EU and NATO). The course provides foundational knowledge and skills without requiring prior experience in the field.

Course-related learning outcomes

Knowledge:
- Understands key concepts and standards in cybersecurity.
- Knows methods for risk assessment and data protection in IT systems.
- Understands the functioning of SOC, CSIRT, and SIEM systems.

Skills:
- Can analyze threats and vulnerabilities and propose mitigation measures.
- Is capable of acquiring information on vulnerabilities and threats.
- Effectively collaborates in a project team.

Social competences:
- Recognizes the importance of continuous learning in a rapidly changing environment.
- Is aware of the responsibility associated with decisions in IT security projects.

Methods for verifying learning outcomes and assessment criteria

Learning outcomes presented above are verified as follows:

1. Knowledge: Verified through a written exam with open-ended questions.
2. Skills: Assessed via ongoing evaluation of group projects and the final presentation of results.
In each form of the course assessment, the grade depends on the number of points the student earns relative to the maximum number of required points. Earning at least 50% of the possible points is a prerequisite for passing. The relationship between the grade and the number of points is defined by the Study Regulations. Additionally, the course completion rules and the exact passing thresholds will be communicated to students at the beginning of the semester through the university's electronic systems and during the first class meeting (in each form of classes).

Programme content

The course "Introduction to Cybersecurity" familiarizes students with key concepts, threats, and data protection techniques essential for information security in cyberspace. It covers fundamental aspects of information security, risk assessment methods, and organizational security management. The course also addresses the international context of cybersecurity, including initiatives by the EU, NATO, and other international organizations. It develops both analytical and practical skills through group projects. This is the first cybersecurity course in the engineering curriculum and does not require prior knowledge in this field.

Course topics

I. Introduction to Cybersecurity (12x45 min)
1. Basic concepts and definitions:
- The significance of cyberspace in modern society.
- Terminology: vulnerability, threat, attack, risk.
- Security cube: key objectives, data states, and areas of defensive actions.
- Models, standards, and recommendations (e.g., NIST, ISO 27000).
- Vulnerability databases and their role (e.g., CVE).
2. Types of vulnerabilities and attacks:
- Vulnerabilities and malicious software.
- Attack classifications (e.g., DDoS, phishing, ransomware).
- Security specifics in cloud systems and IoT.
3. Basic protection strategies:
- Risk management and security policies.
- Models and mechanisms for access control (IAAA).
II. Cybersecurity in an International Context: (6x45 min)
1. International initiatives:
- EU actions: ENISA, EUROPOL, Digital Single Market.
- NATO's role and collaboration with the EU on cyber defense.
- International organizations: UN, OECD, G7, G20.
2. Incident response teams:
- Tasks and structure of response teams.
- Case studies of real incidents and response methods.
III. Cyber Hygiene and Protection Tools: (12x45 min)
1. Basics of network operation in the context of security.
2. Principles of secure usage of devices and networks:
- Password management and two-factor authentication (2FA).
- Digital certificates and public key infrastructure (PKI).

IV. Practical Aspects of Cybersecurity:
1. Case studies:
- Analysis of cyberattacks and their impact.
- Organizational responses to security incidents.
2. Group project:
- Development and implementation of a data protection system in a test environment.
- Risk analysis, security policies, and presentation of results.

Teaching methods

- Lectures online with multimedia presentations and case analyses.
- Group projects conducted in laboratory settings.

Bibliography

Basic:
1. "Cybersecurity Essentials" by Charles J. Brooks, Christopher Grow, Philip A. Craig, Jr., and Donald Short. Published by John Wiley & Sons in 2018. ISBN: 978-1-119-36239-5.
2. "Network Security Essentials: Applications and Standards" by William Stallings. Published by Pearson in 2017. ISBN: 978-0-134-52733-8.

Additional:
1. Documents from ENISA, NIST, and NATO on cybersecurity.
2. Instructor-provided materials.

Breakdown of average student's workload

	Hours	ECTS
Total workload	120	4,00
Classes requiring direct contact with the teacher	60	2,00
Student's own work (literature studies, preparation for laboratory classes/ tutorials, preparation for tests/exam, project preparation)	60	2,00