POZNAN UNIVERSITY OF TECHNOLOGY

EUROPEAN CREDIT TRANSFER AND ACCUMULATION SYSTEM (ECTS)

COURSE DESCRIPTION CARD - SYLLABUS

Course name
Basics of cyberspace security [N1IBiJ1>PBwC]

Course

Field of study
Safety and Quality Engineering

Area of study (specialization)
–

Level of study
first-cycle

Form of study
part-time

Year/Semester
3/6

Profile of study
general academic

Course offered in
Polish

Requirements
compulsory

Number of hours

Lecture
0

Tutorials
0

Laboratory classes
9

Projects/seminars
9

Other
0

Number of credit points

2,00

Coordinators

dr inż. Sebastian Kubasiński
sebastian.kubasinski@put.poznan.pl

Lecturers

Prerequisites

The student has knowledge of the basics of management and information technologies studied at the Bachelor's level. The student is familiar with the connection between the risk of threats in cyberspace and their effects on the functioning of an organisation. Moreover, the student should have the ability to use the already acquired knowledge in practice and is ready to work in team structures.

Course objective

The interest of Security Engineering students in cyber security issues and the types of threats and their techniques of prevention, in solving both technological and decision-making problems of this discipline of knowledge.

Course-related learning outcomes

Knowledge:
1. The student knows the fundamental dilemmas of modern civilization and development trends and best practices in security engineering, concerning cyber security in organizations. [K1_W10]
2. The student has advanced knowledge of methods, techniques, tools and materials used in preparation for conducting scientific research and solving simple engineering tasks with the use of

information technology, information protection and computer support, in relation to cybersecurity. [K1_W11]
3. The student knows in-depth the terms and principles of copyright protection, information security and intellectual property protection in market economy, in the context of organisation's functioning in cyberspace. [K1_W12]

Skills:
1. The student is able to appropriately select sources and information from them, evaluate, critically analyse and synthesise such information. [K1_U01]
2. The student is able to apply various techniques to communicate in professional and other environments. [K1_U02]
3. The student is able to use analytical, simulation and experimental methods to formulate and solve engineering tasks, also using ICT methods and tools, in the context of ensuring security in cyberspace. [K1_U04]
4. The student is able to identify changes in requirements, standards, regulations and technical progress and the reality of the labour market, in the context of ensuring security in cyberspace, and on their basis identify the need to supplement knowledge. [K1_U12]

Social competences:
1. The student is aware of the recognition of the importance of knowledge in solving safety and quality engineering problems and continuous improvement. [K1_K02]
2. The student is aware of the understanding of non-technical aspects and effects of engineering activities, including their impact on the environment and the related responsibility for making decisions, in the context of functioning of an organisation in cyberspace. [K1_K03]

Methods for verifying learning outcomes and assessment criteria

Learning outcomes presented above are verified as follows:

Formative assessment:
Laboratory: current assessment of the tasks performed on a scale of 2- 5; the pass mark for the first and second attempt - 50% + 1%;
Project: ongoing assessment of the individual parts of the project on a scale of 2- 5; threshold for passing the first and second attempt - 50% + 1%;
Summative assessment:
Laboratory: average of partial marks for individual tasks; the pass mark for the first and second attempt - 50% + 1%,
Project: average of partial marks for the completion of the individual phases of the project + mark for the editing level of the project and progress during the course; threshold for passing the first and second attempt - 50% + 1%.

Programme content

Information security; major threats to businesses: Phishing, Man-in-the-Middle attacks, Denial of Service (DOS) attack; cyber security in remote work; cyber attack; principles of protection against external threats.

Course topics

Laboratory:
1 Introduction to cyber security. Cyber security requirements and standards. 2. Identification of cyber security problems and risks. 3. Practical actions to mitigate cyber security risks. 4. Incident and business continuity management of an organisation in cyberspace.
Project: Students design an instruction on how to represent an organisation safely in cyberspace, for a selected workstation indicated by the instructor.

Teaching methods

Laboratory:
- expository methods (multimedia presentation, video, demonstration), panel discussion, case study, brainstorming, practical exercises.
Project:
- multimedia presentation, case study

Bibliography

Basic:
1. ISO/IEC 27032 - Technologia informacyjna - Techniki bezpieczeństwa - Wytyczne dotyczące bezpieczeństwa cybernetycznego.
2. Normy ISO rodziny 27000, PKN 2014 lub późniejsze.
3. Karpiński M., Bezpieczeństwo Informacji: praca zbiorowa, Wydawnictwo PAK, 2012.
4. Brdulak J. J., Sobczak P., Wybrane problemy zarządzania bezpieczeństwem informacji, OW SGH, 2014.
5. Gałach A., Zarządzanie Bezpieczeństwem Informacji w Sektorze Publicznym, Wydawnictwo C.H. Beck, 2009.
6. Campbell T., Practical Information Security Management, A Complete Guide to Planning and Implementation, Springer 2016.

Additional:
1. Shuttonm R. J., Bezpieczeństwo w telekomunikacji, WKŁ, Warszawa, 2004.
2. Bilski T., Pankowski T., Stokłosa J., Bezpieczeństwo danych w systemach informatycznych, Wydawnictwo Naukowe PWN, 2001.
3. Stallings W., Cryptography and Network Security: Principles and Practice, Pearson Education, 2011.

Breakdown of average student's workload

	Hours	ECTS
Total workload	50	2,00
Classes requiring direct contact with the teacher	18	0,50
Student's own work (literature studies, preparation for laboratory classes/ tutorials, preparation for tests/exam, project preparation)	32	1,50