POZNAN UNIVERSITY OF TECHNOLOGY

EUROPEAN CREDIT TRANSFER AND ACCUMULATION SYSTEM (ECTS)

COURSE DESCRIPTION CARD - SYLLABUS

Course name
Management of IT Systems Security [S1IZarz1E>ZBSI]

Course

Field of study Engineering Management	**Year/Semester** 3/6
Area of study (specialization) –	**Profile of study** general academic
Level of study first-cycle	**Course offered in** english
Form of study full-time	**Requirements** elective

Number of hours

Lecture 15	**Laboratory classes** 0	**Other (e.g. online)** 0
Tutorials 15	**Projects/seminars** 0	

Number of credit points

2,00

Coordinators	**Lecturers**
dr inż. Maciej Siemieniak maciej.siemieniak@put.poznan.pl	

Prerequisites

The student starting this subject should have a basic knowledge of information and IT systems. He should also be able to obtain information from specified sources and be willing to cooperate as part of a team.

Course objective

Providing students with basic knowledge in the field of information security and IT systems security, necessary for the proper design, management and improvement of ICT security systems. Developing students' skills to solve information security problems and information systems.

Course-related learning outcomes

Knowledge:
The student defines key concepts and principles related to information security and information systems, including the life cycle of information and security attributes [P6S_WG_01].
The student identifies and describes various stages in the life cycle of socio-technical systems, with particular emphasis on aspects of information security [P6S_WG_13].
The student explains the basic principles of quality management and their application in the context of information system security [P6S_WK_02].

Skills:
The student analyzes the results of experiments and computer simulations concerning the security of information systems and draws conclusions regarding their effectiveness and applications [P6S_UW_09].
The student applies analytical methods and simulation tools to design and implement security strategies in information systems [P6S_UW_10].
The student integrates theoretical knowledge and practical skills to solve complex problems related to the security of information systems in various organizational environments [P6S_UW_11].

Social competences:
The student develops strategies and plans for implementing information security systems, taking into account diverse technical, economic, legal, and organizational aspects [P6S_KO_02].
The student makes responsible decisions regarding the management of information system security, considering their impact on the environment and the community [P6S_KR_01].]

Methods for verifying learning outcomes and assessment criteria
Learning outcomes presented above are verified as follows:

Knowledge acquired during lectures is verified by one test that takes place during the last class. The test consists of 10 differently scored questions. Passing threshold: 50% of correct answers. Assessment issues include only material from lectures.
During exercises, students work in groups on specific topics, which they present in the form of a multimedia presentation. Students receive grades for each task. The content of the tasks is related to the subject, and the scope of tasks includes lecture issues.

Programme content

Lectures:
1. information security (meaning and definitions of information, information life cycle, the essence of information security, concepts related to information security, incidents, elements of information security, evolution of the information security management system (ISMS), ISMS standards, ISMS policy in the organization, ISMS model, risk, ISMS implementation in the organization, risk assessment methods).
2. IT systems security (concepts, definitions, reference to information security, security attributes, risk management and risk reduction strategies, three-level reference model, hierarchy of assets model, security selection strategy, implementation and post-implementation activities).
Tutorials:
Lecturer:
The essence of tools and how to perform tasks for the following topics: mind map, Ishikawa diagram, fault tree analysis, event tree analysis, flow diagram, mini lecture on maxi matters, lecture on the subject; Task topics related to the security of information and IT systems.
Students:
1. mind map for the term "information" - a multimedia or graphic (poster) presentation;
2. Ishikawa diagram for the problem of "unauthorized access to data or information in an enterprise" (any type of data / information: financial, personal, technological, production, research and development, sales strategy, etc.) - multimedia or graphic presentation (poster);
3. fault tree analysis and event tree analysis for the event "laptop from the president's car was stolen" - multimedia presentation;
4. flow diagram - based on the text describing the process of entering data into the IT system (algorithm, decision-making processes, activities, organizational units) - multimedia presentation;
5. mini lecture on maxi matters - multimedia presentation in the form of a lecture / read (cryptology, computer crime, cyberterrorism, spam, internet chain, hacker, cracker, malware - prevention and security, online threats - protection, prevention, the most popular social media/websites - negative phenomena, how to use them safely, secure online shopping, secure login, secure passwords);
6. IT system security management - multimedia presentation in the form of lecture / reading (outline of the problem, the most important issues, based on lectures);

Teaching methods

Lectures: multimedia presentation - text, drawings, diagrams, tables, explanatory examples, short conversation with students.
Exercises: lecturer - multimedia presentation, students - multimedia and graphic (poster) presentation, short lecture, discussion.

Bibliography

Basic:
1. Jacek Łuczak, Marcin Tyburski, Systemowe zarządzanie bezpieczeństwem informacji. Wydawnictwo Uniwersytetu Ekonomicznego we Wrocławiu, Poznań 2010.
2. Andrzej Białas, Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie. Wydawnictwo naukowo-techniczne, Warszawa 2006, 2007.
3. Raggad Bel G., (2010), Information Security Management. Taylor&Francis Inc.
4. Alexander David., (2021), Information Security Management Principles. BCS Learning & Development Limited

Additional:
1. Andrzej Borucki, Gospodarka elektroniczna. Wydawnictwo Politechniki Poznańskiej, 2013.
2. Andrzej Borucki, E-biznes. Wydawnictwo Politechniki Poznańskiej, 2012.
3. Stokłosa J. i innni, Ochrona danych i zabezpieczenia w systemach teleinformatycznych, Wydawnictwo Politechniki Poznańskiej 2003
4. Anderson R., Inżynieria zabezpieczeń, Wydawnictwo Naukowo - Techniczne 2005

Breakdown of average student's workload

	Hours	ECTS
Total workload	50	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)	20	1,00