COURSE DESCRIPTION CARD - SYLLABUS

Course name
Management of IT Systems Security [S1IZarz1>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
Polish

Form of study
full-time

Requirements
elective

Number of hours

Lecture
15

Laboratory classes
0

Other
0

Tutorials
30

Projects/seminars
0

Number of credit points

2,00

Coordinators

dr inż. Maciej Siemieniak
maciej.siemieniak@put.poznan.pl

Lecturers

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: Multimedia presentation for students on information security, standards, security policy in the organization, model of the information security system, risk, security of IT systems, risk management and risk reduction strategies, security selection strategy.
Classes: Instructor: Explaining the essence of the tools used and how to perform the tasks assigned to students. Presentation of tasks by students.

Course topics

Lectures: Multimedia presentation for students on the following topics: 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. security of information systems (concepts, definitions, reference to information security, security attributes, risk management and risk reduction strategies, three-level reference model, resource hierarchy model, security selection strategy, implementation and post-implementation activities).
Exercise classes: Instructor: Explanation of the essence of the tools used and how to perform tasks for the following topics: mind map, Ishikawa diagram, error and event tree, flow diagram, mini lecture on maxi issues, lecture on the subject; Task topics related to information and IT systems security.
Students prepare: 1. mind map for the concept of "information" - multimedia or graphic presentation (poster) with discussion; 2. Ishikawa diagram for the problem of "unauthorized access to data or information in the enterprise" (any type of data/information: financial, personnel, technological, production, research and development, sales strategy, etc.) - multimedia or graphic presentation (poster) with discussion; 3. error and event tree for the event "laptop stolen from the president's car" - multimedia presentation with discussion; 4. flow diagram - based on the text describing the process of entering data into the IT system (algorithm, decision-making processes, actions, performers) - multimedia presentation with discussion; 5. mini lecture on maxi issues - multimedia presentation in the form of a lecture/lecture on a selected topic (cryptology, computer crime, cyberterrorism, spam, chain mail, hacker, cracker, malware - prevention and security, threats on the Internet - protection, prevention, the most popular social networking sites - negative phenomena, how to use them safely, safe online shopping, safe login, safe passwords); 6. IT systems security management - multimedia presentation in the form of a lecture/reading (outline of the problem, most important issues, based on the 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. Białas A. (2023), Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie. Wydawnictwo Naukowe PWN, WNT
2. Jason A., (2021), Podstawy bezpieczeństwa informacji. Praktyczne wprowadzenie. Wydawnictwo Helion
3. Kowalewski J., Kowalewski M., (2021), Zarządzanie ryzykiem w bezpieczeństwie informacji organizacji. Oficyna Wydawnicza Politechniki Warszawskiej
4. Jacek Łuczak, Marcin Tyburski, Systemowe zarządzanie bezpieczeństwem informacji. Wydawnictwo Uniwersytetu Ekonomicznego we Wrocławiu, Poznań 2010.

Additional:
1. Molendowska M., Miernik R., (2021), Bezpieczeństwo w cyberprzestrzeni. Wybrane zagadnienia. Wydawnictwo Adam Marszałek
2. Andrzej Borucki, Gospodarka elektroniczna. Wydawnictwo Politechniki Poznańskiej, 2013.
3. Andrzej Borucki, E-biznes. Wydawnictwo Politechniki Poznańskiej, 2012.
4. Stokłosa J. i innni, Ochrona danych i zabezpieczenia w systemach teleinformatycznych, Wydawnictwo Politechniki Poznańskiej 2003
5. 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