COURSE DESCRIPTION CARD - SYLLABUS

Course name
Information security

Course

Field of study	Year/Semester
Engineering Security	2/4
Area of study (specialization)	Profile of study
	general academic
Level of study	Course offered in
First-cycle studies	Polish
Form of study	Requirements
part-time	compulsory

Number of hours

Lecture	Laboratory classes	Other (e.g. online)
10	10	
Tutorials	Projects/seminars	

Number of credit points

2

Lecturers

Responsible for the course/lecturer:	Responsible for the course/lecturer:
Ph.D., Eng. Krzysztof Hankiewicz,	Ph.D., Eng. Maciej Siemieniak,
Mail to: krzysztof.hankiewicz@put.poznan.pl	Mail to: maciej.siemieniak@put.poznan.pl
Phone: 61 665 34 08	Phone: 61 665 33 89
Faculty of Engineering Management	Faculty of Engineering Management
ul. J. Rychlewskiego 2, 60-965 Poznan	ul. J. Rychlewskiego 2, 60-965 Poznan

Prerequisites

The student starting this subject should have a basic knowledge of information and information 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 as well as the selection of security measures and information protection, 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

1. Knows contemporary trends and best practices in information and IT techniques, as well as supporting the risk modeling process.[P6S_WK_03]

2. Knows contemporary trends and best practices used to ensure information security. [P6S_WK_03]

3. Knows the basic techniques and tools used to solve simple engineering tasks with the use of information technology, information protection and computer support.[P6S_WK_04]

4. Knows and understands the basic concepts and principles of information security.[P6S_WK_05]

Skills

1. Can acquire, integrate, interpret information from literature, databases and other properly selected sources in the field of information security, as well as draw conclusions and formulate and justify opinions. [P6S_UW_01]

2. Can use various techniques in order to communicate in a professional environment and in other environments. [P6S_UW_02]

3. Can use information protection techniques.[P6S_UW_04]

4. Can use information and communication techniques to carry out tasks typical for engineering activities.[P6S_UU_01]

Social competences

1. understands the need and knows the possibilities of continuous training, improving professional, personal and social competences; can argue the need for lifelong learning. [P6S_KK_02]

2. Is aware that creating activities that meet the needs of information security and IT systems in an organization requires a systemic approach, taking into account technical, economic, marketing, legal, organizational and financial issues. [P6S_KK_02]

3. Is aware of the importance and understands the non-technical aspects and effects of engineering activities, including its impact on the environment and the related responsibility for decisions made. [P6S_KK_03].

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 the laboratory classes, students work individually and in small groups on assigned 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:

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:

Explanation of the essence of the tools used and how to perform the 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;

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);

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, reading.

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.

Additional

1. Liderman K., Bezpieczeństwo informacyjne, Wydawnictwo Naukowe PWN, 2017

2. Stokłosa J. i innni, Ochrona danych i zabezpieczenia w systemach teleinformatycznych, Wydawnictwo

Politechniki Poznańskiej 2003

3. Anderson R., Inżynieria zabezpieczeń, Wydawnictwo Naukowo - Techniczne 2005.

Breakdown of average student's workload

	Hours	ECTS
Total workload	50	2,0
Classes requiring direct contact with the teacher	20	1,0
Student's own work (literature studies, preparation for tutorials, preparation for tests) [1]	30	1,0

[1] delete or add other activities as appropriate