COURSE DESCRIPTION CARD - SYLLABUS

Course name

Management of IT Systems Security

Course

Field of study

Engineering Management

Year/Semester

3/6

Area of study (specialization)

Profile of study

general academic

Level of study

First-cycle studies

Course offered in

polish

Form of study

full-time

Requirements

elective

Number of hours

Lecture

15

Laboratory classes

Other (e.g. online)

Tutorials

15

Projects/seminars

Number of credit points

2

Lecturers

Responsible for the course/lecturer:

Maciej Siemieniak, Ph.D., Eng.

email: maciej.siemieniak@put.poznan.pl

tel. 61 665 33 89

Faculty of Engineering Management

ul. J. Rychlewskiego 2, 60-965 Poznan

Responsible for the course/lecturer:

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, 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. has expanded and in-depth knowledge of the sciences necessary to understand and describe the issues of information security and information systems management in organizations.

2. has basic knowledge of the life cycle of information and socio-technical systems.

3. has basic knowledge regarding the organization and management of information and IT security in the organization, regarding quality management and business operations.

Skills

1. is able to plan and conduct experiments, including computer measurements and simulations regarding information security, interpret obtained results and draw conclusions about the level of IT systems security.

2. is able to use analytical, simulation and experimental methods to formulate and solve engineering tasks.

3. can, when formulating and solving engineering tasks, notice their systemic, socio-technical, organizational, economic and non-technical aspects.

Social competences

1. is aware that creating activities that meet the needs of information and IT systems security in an organization requires a systematic approach taking into account technical, economic, marketing, legal, organizational and financial issues.

2. is aware of the importance and understands the non-technical aspects and effects of engineering activities, including its impact on the environment, and the associated responsibility for the decisions taken.

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. For each of the seven tasks students receive grades (7 grades). The final grade is the average of these 7 marks. 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;

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, 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. Andrzej Borucki, Gospodarka elektroniczna. Wydawnictwo Politechniki Poznańskiej, 2013.

2. Andrzej Borucki, E-biznes. Wydawnictwo Politechniki Poznańskiej, 2012.

Breakdown of average student's workload

	Hours	ECTS
Total workload	60	2,0
Classes requiring direct contact with the teacher	30	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