COURSE DESCRIPTION CARD - SYLLABUS

Course name
Security policy of a telecom operator [S2EiT1-ESPiO>PBOT]

Course

Field of study
Electronics and Telecommunications

Year/Semester
2/3

Area of study (specialization)
Programmable Electronic Systems and Optotelecommunications

Profile of study
general academic

Level of study
second-cycle

Course offered in
Polish

Form of study
full-time

Requirements
elective

Number of hours

Lecture
30

Laboratory classes
0

Other (e.g. online)
0

Tutorials
0

Projects/seminars
15

Number of credit points

4,00

Coordinators

dr hab. inż. Mieczysław Jessa prof. PP
mieczyslaw.jessa@put.poznan.pl

Lecturers

Prerequisites

Students know the principles, with necessary mathematical background, theory of communication necessary to understand, analyze and evaluate the operation of analogue and digital transmission systems. Is able to extract information from Polish or English language literature, databases and other sources.

Course objective

The presentation of data protection methods in communication systems with the description of the special role of security policy document prepared with the use of international and national standards.

Course-related learning outcomes

Knowledge:
1. He has knowledge on methods and systems used to ensure security of information sent in communication systems.

Skills:

1. Is able to apply and/or to design professional monitoring and security systems for different networks or communication systems.
2. Knows limitations of his/her knowledge, understands the necessity of further self-studying.

Social competences:
1. Is aware of responsibility for designed systems (electronic and communication) and knows physical and social threats that can appear as the result of irresponsible usage of communication systems.
2. Is aware of the necessity to approach solving technical problems with responsibility and professionalism.

Methods for verifying learning outcomes and assessment criteria

Learning outcomes presented above are verified as follows:

Learning outcomes presented above are verified as follows:
Learning outcomes are verified with a written exam. Exam consists of 5 open questions. Answers are scored equally. Minimum number of scores to pass the exam is equal to 50%. Questions are chosen individually and randomly from a set of questions prepared by the lecturer. The set of predefined subjects is sent to students by email.
Knowledge and skills gathered during the Project are assessed by written project and oral presentation of the results of this project. The final mark is the average of two marks. The assessment levels are the following: under 3 - mark 2.0, from 3 to 3.25 - mark 3.0; from 3.26 to 3.75 - mark 3.5; from 3.76 to 4.25 - mark 4.0; from 4.26 to 4.75 - mark 4.5; above 4.75 - mark 5.0.

Programme content

During the course students learn about basic methods of information protection. They are discussed the following subjects: vulnerability, threat, security incident, classification of threats, categories of threats, examples of threats in wired and wireless networks, in computer networks, possible relations during identification of threats, failures statistics, vulnerability analysis, protection analysis, standards concerning information security (de-jure and de-facto), international, regional and national, definition of risk, risk assessment methods (deduction and induction methods, qualitative methods), methods of risk reduction, risk management according BS, ISO/IEC and NIST standards, Polish norm PN, security management methods according BS, ISO/IEC, NIST, the structure of the policy document proposed by international and national standards, basic security instructions and procedures, examples of security policy documents, technical resources necessary to introduce security policy into a practice of a telecom operator, methods of security quality assessment with the use of international and national standards, the evaluation of information security policy, audit of security policy, the role of document UE 206/679 known as General Data Protection Regulation, known in Poland as RODO, for security policy of a telecom operator.
The goal of the Project is to prepare and implement in software/hardware a chosen security component of a communication system. Student can choose a component suggested by the teacher or can propose his own component, after earlier acceptance of the teacher. Among existing propositions we have risk assessment of an exemplary event (e.g. the loss of PIN, password, a credit card, e-mail server failure etc.) with one of methods described during the lecture; an implementation a chosen method of authentication in an FPGA; hardware or software protection of confidentiality of emails exchanged in a public network; preparation of en exemplary policy document for a small company; preparation of an exemplary set of control points for local computer network audit.

Course topics

none

Teaching methods

Lecture: Multimedia presentation.
Tutorials: A combination of exercise and project method.

Bibliography

Basic
1. K. Liderman, Bezpieczeństwo informacyjne, nowe wyzwania, PWN, 2017.
2. A. Białas, Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie, WNT, Warszawa, 2007.
Additional
1. J. Stokłosa, T. Bilski, T. Pankowski, Bezpieczeństwo danych w systemach informacyjnych, PWN, 2001.
2. K. Liderman, Analiza ryzyka i ochrona informacji w systemach komputerowych, PWN, Warszawa, 2008.

Breakdown of average student's workload

	Hours	ECTS
Total workload	100	4,00
Classes requiring direct contact with the teacher	58	2,00
Student's own work (literature studies, preparation for laboratory classes/ tutorials, preparation for tests/exam, project preparation)	42	2,00