COURSE DESCRIPTION CARD – SYLLABUS

Course name

Elective module in the field: Information Technology and Communication Systems in Power Engineering – IT systems for data processing and exchange

Course

Field of study
Electric Power Engineering

Year/Semester
3/5

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
30

Laboratory classes
15

Other (e.g. online)

Tutorials

Projects/seminars

Number of credit points

3

Lecturers

Responsible for the course/lecturer:
dr inż. Andrzej Kwapisz

Faculty of Environmental Engineering and Energy

email:andrzej.kwapisz@put.poznan.pl

tel. 616652282

Responsible for the course/lecturer:

Prerequisites

Knowledge of mathematical analysis, circuit theory, basics of signal processing, programming, databases.

Knowledge of computer network infrastructure, computer aided design software.

Ability to work and cooperate in a group.

Course objective

Getting to know modern information technologies used in power engineering. Application of numerical methods for data processing in power and electrical systems. To familiarize students with the methods of collecting, transmitting and storing data from the power grid. Acquainted with the methods of encryption and data protection as well as legal regulations regarding data protection.

Course-related learning outcomes

Knowledge

1. Has knowledge of the methods of processing data from the power grid.

2. Has knowledge of the security of data transmission and processing systems.

Skills

1. Is able to use available traditional and electronic data resources to acquire knowledge

2. Is able to perform data analysis based on information available in IT systems used in the power industry. Is able to use cryptographic methods and create secure warehouses and data transmission channels.

Social competences

1. Has the skills to study independently, work in a group and acquire new knowledge, and understands the impact of IT technology on the work of an engineer.

Methods for verifying learning outcomes and assessment criteria

Learning outcomes presented above are verified as follows:

Lecture

Assessment of activity in class, assessment of homework, final test in writing at the end of the semester, colloquium includes test questions or problem tasks, written exam covering the subject of the subject assessed on a scale of 0 to 100%, the final grade lectures given by more than one lecturer based on weighted average, final grade for more than one component grade based on weighted average.

Laboratory

Verification of individual preparation for classes, including material from a single exercise or block of exercises, assessment of individual exercise reports made by the student, colloquium at the end of the semester, colloquium includes test questions or problem tasks, all grades on a scale of 0 to 100%, final grade based on the weighted average of all component ratings.

Programme content

Lecture

Control and supervision systems as a tool for monitoring the operation of the power system. Application of microprocessor technique in automation and ICT systems, processing of recorded signals. Selected issues in the field of cryptography. Methods of secure data transmission, authentication methods in IT systems. Rules for preparing engineering documentation for IT systems. Selected issues in the field of data protection rights (database protection, personal data protection). Teaching support through extensive use of public programs (open licenses). Presentation of available alternative sources that allow students to independently expand their knowledge and skills.

Laboratory

Control and use systems, the use of microprocessor technology, software configuration in the client-server architecture, creation and verification of encryption keys, data encryption in databases, creating secure port connections.

Teaching methods

Lecture

Multimedia and interactive presentation presenting important issues related to the subject, didactic discussion based on the literature on the subject, informative lecture, problem lecture, case study, work on source materials.

Laboratory

Implementation of exercises, use of publicly available information and software tools to support the didactic process, encouraging students to independently search for optimal solutions and problem solving.

Bibliography

Basic

1. Kacejko P., Inżynieria elektryczna i informatyczna w nowych technologiach elektroenergetycznych, 2010
2. Kasprzak, A., Projektowanie struktur rozległych sieci komputerowych, Oficyna Wydawnicza PWr, 2001.
3. Stallings, W., Brown, L., Bezpieczeństwo systemów informatycznych : zasady i praktyka. T. 2, Helion, 2019.
4. Aumasson, J-P., Nowoczesna kryptografia : praktyczne wprowadzenie do szyfrowania, PWN, 2018.
5. Michael Welschenbach, Kryptografia w językach C i C++, Mikom, 2002.
6. Mikołaj Karpiński et al., Bezpieczeństwo informacji : praca zbiorowa, Wydawnictwo PAK, 2012.

Additional

1. Janusz Szmidt, Michał Misztal, Wstęp do kryptologii, Oficyna Wydawnicza WIT, 2002.
2. J. Izydorczyk, W. Sułek, P. Zawadzki, Kody i szyfry, Wydawnictwo PŚl, 2017.
3. Stokłosa, J., Kryptograficzna ochrona danych w systemach komputerowych, Nakom, 1994.
4. Niels Ferguson, Bruce Schneier, Kryptografia w praktyce, Helion, 2004.

Breakdown of average student's workload

	Hours	ECTS
Total workload	94	3
Classes requiring direct contact with the teacher	55	2
Student's own work (literature studies, preparation for laboratory classes, preparation of reports, preparation for tests)	39	1