COURSE DESCRIPTION CARD - SYLLABUS

Course name
Cybersecurity and telecommunications in the power industry [S2Eltech1E>CiTwE]

Course

Field of study
Electrical Engineering

Year/Semester
1/2

Area of study (specialization)
Microprocessor Control Systems in Electrical Engineering

Profile of study
general academic

Level of study
second-cycle

Course offered in
English

Form of study
full-time

Requirements
compulsory

Number of hours

Lecture
15

Laboratory classes
0

Other
0

Tutorials
0

Projects/seminars
0

Number of credit points

1,00

Coordinators

dr inż. Andrzej Kwapisz
andrzej.kwapisz@put.poznan.pl

Lecturers

Prerequisites

The student starting the course should have basic knowledge of computer science, including operating systems and computer networks, network devices, basic communication protocols and basic knowledge of telecommunications systems.

Course objective

The aim of the course is to familiarize students with the basic issues related to the security of ICT systems, familiarization with cybersecurity threats and counteracting threats resulting from the use of modern IT technologies.

Course-related learning outcomes

Knowledge:
1. Knows and understands problems related to cybersecurity.
2. Has ordered knowledge of the architecture and security of computer and teleinformation systems.

Skills:

1. Is able to assess cybersecurity threats to ICT systems and develop strategies to counteract these threats.

Social competences:
1. Is aware of the rapid progress in the field of IT technology and the resulting threats to the security of physical infrastructure, economic and personal security.

Methods for verifying learning outcomes and assessment criteria

Learning outcomes presented above are verified as follows:

Lecture
Assessment of class activity, written test at the end of the semester, test includes test questions or problem tasks, written exam covering the subject matter assessed on a scale from 0 to 100%, final grade for lectures conducted by more than one lecturer at weighted average, final grade for more than one component grade based on weighted average, pass 60%. The number of questions in the test is 10-20, the score depends on the difficulty of the question.

Programme content

Cybersecurity systems, classification of threats to ICT systems, methods of counteracting cybersecurity threats.

Course topics

Lecture
Introduction to cybersecurity issues, threats, security vulnerabilities, attacks in cyberspace, malware, data leakage. Types of attacks on a computer network, attacks on wireless communication systems. Data encryption and cryptography, methods of cryptography with the use of symmetric and asymmetric keys. Cyber attack analysis, network infrastructure penetration tests. Security permissions in computer systems. Prevention of cybersecurity threats, network traffic monitoring and filtering, firewalls, virtual private networks - VPN. Susceptibility to cyber attacks of telecommunications and teletransmission systems used in the power industry.

Teaching methods

Lecture
Multimedia and interactive presentation presenting important issues related to the subject, didactic discussion based on the literature on the subject, information lecture, problem lecture, case study, multimedia show, demonstration.

Bibliography

Basic:
1. Białas A., Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie, PWN, Warszawa, 2017
2. Kowalewski J., Kowalewski M., Ochrona informacji i systemów teleinformatycznych w cyberprzestrzeni, Oficyna Wydawnicza PW, Warszawa, 2017
3. Krawiec J., Cyberbezpieczeństwo: podejście systemowe, Oficyna Wydawnicza PW, Warszawa, 2019
4. Liderman K. [red] i inni, Bezpieczeństwo teleinformatyczne: problemy formalne i techniczne, Wojskowa Akademia Techniczna, Warszawa, 2006
5. PN-EN 60950, Bezpieczeństwo urządzeń techniki informatycznej, PKN, Warszawa, 2002
6. PN-ISO/IEC 14888-3, Technika informatyczna - Techniki zabezpieczeń - Podpisy cyfrowe z załącznikiem - Część 3: Mechanizmy oparte na certyfikatach, PKN, Warszawa, 2002
7. PN-ISO/IEC 2382-8, Technika informatyczna - Terminologia - Bezpieczeństwo, PKN, Warszawa, 2001
8. Stallings W., Brown L., Bezpieczeństwo systemów informatycznych: zasady i praktyka. T. 1, Helion, Gliwice, 2019
9. Stallings W., Brown L., Bezpieczeństwo systemów informatycznych: zasady i praktyka. T. 2, Helion, Gliwice, 2019

Additional:
1. Białas A. [red.] i inni, Podstawy bezpieczeństwa systemów teleinformatycznych: podręcznik do szkoleń autoryzowanych przez Departament Bezpieczeństwa Teleinformatycznego Agencji

Bezpieczeństwa Wewnętrznego: , Wydaw. Pracowni Komputerowej Jacka Skalmierskiego, Gliwice, 2002
2. Engebretson P., Hacking i testy penetracyjne: podstawy, Helion, Gliwice, 2013
3. Kennedy D. [red.] i inni, Metasploit: przewodnik po testach penetracyjnych, Helion, Gliwice, 2013
4. Kowalewski J., Kowalewski M., Zagrożenia informacji w cyberprzestrzeni, cyberterroryzm, Oficyna Wydawnicza PW, Warszawa, 2017
5. Luttgens J., Pepe M., Mandia K., Incydenty bezpieczeństwa: metody reagowania w informatyce śledczej, Helion, Gliwice, 2016
6. Parker C., Firewall nie powstrzyma prawdziwego smoka, czyli Jak zadbać o cyberbezpieczeństwo: przewodnik dla niefachowców, Helion, Gliwice, 2019
7. Scambray J., Shema M., Hakerzy - aplikacje webowe: [sekrety zabezpieczeń aplikacji webowych], Translator, 2002
8. Szychowiak. M., Bezpieczeństwo systemów informatycznych: zaawansowane ćwiczenia w systemach Windows i Linux, WPP, Poznań, 2017
9. Wołowski F., Zawiła-Niedźwiecki J., Bezpieczeństwo systemów informacyjnych: praktyczny przewodnik zgodny z normami polskimi i międzynarodowymi, edu-Libri, Kraków-Warszawa, 2012
10. Odnośnik: https://pp-hip.pfsl.poznan.pl/ipac20/ipac.jsp?session=1662630L8QA66.63770&profile=bpp&page=1&group=0&term=Sieci+komputerowe+--+%3Frodki+zabezpieczaj3Fce.&index=SUBJECT&uindex=&aspect=basic_search&menu=search&ri=6&source=~!bpptest&1662632865190, Biblioteka PP, aktualizacja: 1.10.2022

Breakdown of average student's workload

	Hours	ECTS
Total workload	30	1,00
Classes requiring direct contact with the teacher	15	0,50
Student's own work (literature studies, preparation for laboratory classes/ tutorials, preparation for tests/exam, project preparation)	15	0,50