COURSE DESCRIPTION CARD - SYLLABUS

Course name
Cyber security [S2IBiJ1-BiZK>CYB]

Course

Field of study
Safety and Quality Engineering

Year/Semester
1/2

Area of study (specialization)
Safety and Crisis Management

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
0

Laboratory classes
0

Other
0

Tutorials
30

Projects/seminars
0

Number of credit points

2,00

Coordinators

dr hab. inż. Maciej Sobieraj
maciej.sobieraj@put.poznan.pl

Lecturers

Prerequisites

The student starting this course should have a basic knowledge of the basics of programming, operating systems and computer networks. He should also have the ability to obtain information from the indicated sources and be ready to cooperate as part of the team.

Course objective

Providing students with knowledge in the field of broadly understood ICT security. To acquaint students with advanced methods, techniques and tools used in solving complex tasks in the area of designing and maintaining network systems responsible for the security of transmitted data. Developing students' skills in solving cybersecurity problems appearing in modern ICT networks.

Course-related learning outcomes

Knowledge:
1. The student knows in-depth development trends and good practices regarding safety management, in particular data security in organizations in local and global terms [K2_W04].
2. The student knows in-depth the principles of information flow, communication, data protection, legal and regulatory conditions affecting cyber security, characteristic of the area of organization safety

management [K2_W14].

Skills:
1. The student is able to use methods and tools for solving complex and unusual problems as well as advanced information and communication techniques characteristic of the professional environment related to data management and protection in organizations [K2_U02].
2. The student is able to select and apply computer-aided tools for solving problems characteristic of managing the sphere of data protection in organizations [K2_U08].

Social competences:
1. The student is critical of his knowledge, is ready to consult experts when solving cognitive and practical problems, continuous training in the IT industry, in particular related to cybersecurity in the field of safety management in organizations [K2_K01].
2. A student correctly identifies and resolves dilemmas related to broadly understood security, especially in the area of data, understands the need to make the public aware of the need to shape security in various areas of the organization's functioning [K2_K02].

Methods for verifying learning outcomes and assessment criteria

Learning outcomes presented above are verified as follows:

The skills acquired during the classes are verified on an ongoing basis. During each exercise class, the correctness of the exercises is assessed on a scale from 0 to 100% (formative assessment). The final grade is determined on the basis of the average of points obtained from individual classes, it is required to obtain 51% of points to pass (summative assessment). The grading scale is consistent with the principles described in the Study Regulations.

Programme content

Cybersecurity fundamentals.

Course topics

Overview of TCP/IP protocols. Basics of cyber security (NIST; threats, vulnerabilities, vulnerabilities; IDS, IPS). Types of attacks and vulnerabilities. Preparation of penetration tests. IoT security basics. Basics of access control (AAA, user authentication, access control lists). IPSec, virtual private networks. Layer 2 security (VLANs; threats; IEEE 802.1AE/MACsec+). Firewall technologies. Solutions and procedures used in enterprises to protect against cyberattacks.

Teaching methods

Classes: multimedia presentation, illustrated with examples given on the board, practical exercises in groups, with the use of network devices.

Bibliography

Basic:
1. Santos, O., Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide, Cisco Press, Hoboken, NJ, 2021
2. Migga Kizza, J., : Guide to Computer Network Security; Springer International Publishing, 2020, 10.1007/978-3-030-38141-7

Additional:
1. Khondoker, Rahamatullah (Ed.): SDN and NFV Security - Security Analysis of Software-Defined Networking and Network Function Virtualization; Springer International Publishing 2018.
2. Woland A., Santuka, V., Harris, M., Sanbower J.,: Integrated Security Technologies and Solutions - Volume I: Cisco Security Solutions for Advanced Threat Protection with Next Generation Firewall, Intrusion Prevention, AMP, and Content Security, May 14, 2018, Cisco Press.
3. Barker, E., Quynh Dang, Sheila Frankel, Karen Scarfone, Paul Wouters: Guide to IPsec VPNs (NIST Special Publication 800-77); National Institute of Standards and Technology; 2020; This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-77r1
4. Stewart J.M.,: Network Security, Firewalls And VPNs; Jones & Bartlett Learning Information Systems

Security & Ass, 2nd Edition, 2013.
5. Blokdyk, G.,: IPsec VPN A Complete Guide; 5STARCooks; 2019.
6. Majchrzak J., Goliński M., Matura W., The concept of the qualitology and grey system theory application in marketing information quality cognition and assessment, Central European Journal of Operations Research, 2020, Vol. 28, No. 2.
7. Głąbowski M., Sobieraj M., Simulation Studies of Link Group in Elastic Optical Networks Used in Internet of Things Solutions, Transport and Telecommunication - 2023, vol. 24, no. 3, p. 278-287.

Breakdown of average student's workload

	Hours	ECTS
Total workload	60	2,00
Classes requiring direct contact with the teacher	30	1,00
Student's own work (literature studies, preparation for laboratory classes/ tutorials, preparation for tests/exam, project preparation)	30	1,00