COURSE DESCRIPTION CARD - SYLLABUS

Course name
Cybersecurity [S2Inf1-SzInt>CYBER]

Course

Field of study
Computing

Year/Semester
2/3

Area of study (specialization)
Artificial Intelligence

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
16

Laboratory classes
16

Other
0

Tutorials
0

Projects/seminars
0

Number of credit points

2,00

Coordinators

dr hab. inż. Paweł Śniatała prof. PP
pawel.sniatala@put.poznan.pl

prof. dr hab. inż. Mariusz Głąbowski
mariusz.glabowski@put.poznan.pl

Lecturers

Prerequisites

A student joining this course should have a basic knowledge of computer networks and cryptographic algorithms. She/he should also have the ability to obtain information from the indicated sources and be ready to cooperate as part of a team.

Course objective

To provide students with knowledge in the field of broadly understood ICT security as well as methods and tools used to estimate and control the risk of compromising confidentiality, integrity and data availability. To acquaint students with advanced methods, techniques and tools used in solving complex engineering tasks in the area of designing and maintaining network systems responsible for the security of transmitting data.

Course-related learning outcomes

Knowledge:
a student has systematic and theoretically founded general knowledge related to key issues in the field

of ict security.
a student has advanced detailed knowledge of selected issues in the field of broadly understood ict security as well as methods and tools used to estimate and control the risk of compromising of data confidentiality, integrity and availability
a student knows the development trends and the most important new achievements in the field related to design and maintenance of it and telecommunications" network systems responsible for securing transmitted data.
a student has advanced and detailed knowledge of the processes used to estimate and control the risk of compromising data confidentiality, integrity and availability.

Skills:
a student is able to obtain information on ict security threats and techniques for their estimation and control. she/he is able to integrate the obtained information (in polish and english) and subsequently subject it to critical evaluation.
a student is able to plan and conduct tests in the field of ict security, interpret the obtained results and draw conclusions.
a student is able to use experimental methods to formulate and solve engineering tasks and simple research problems in the area of ict security.
a student is able to integrate knowledge from various areas of computer science and telecommunications when formulating and solving engineering tasks related to the design and implementation of network systems responsible for the security of transmitted data.
a student is able to assess usefulness of using new hardware and software solutions for solving engineering tasks, consisting in building secure data transmission systems.

Social competences:
a student understands that knowledge and skills in the field of ict security become obsolete very quickly.
a student understands the importance of using the latest knowledge in the field of ict security in solving research and practical problems.
a student is aware of the need for a professional approach to solving ict security problems and taking responsibility for the projects she/he proposes.

Methods for verifying learning outcomes and assessment criteria

Learning outcomes presented above are verified as follows:

Learning outcomes presented above are verified as follows:
The knowledge acquired during the lecture is verified during an oral and / or written test.
Test issues, on the basis of which questions are developed, are sent to students via e-mail using the university"s e-mail system.
An oral and / or written test consists of 3 to 5 questions for which a descriptive answer is expected. Each answer to the question is rated on a scale of 0 to 5 points. Each question is scored equally. Passing threshold: 50% of points.
In the case of the oral test, students draw questions from a set of 30 questions. In the case of a written test, questions are asked by a lecturer.
The skills acquired during the laboratory classes are verified on an ongoing basis. At each laboratory class, the correctness of the exercises is assessed on a scale from 2 to 5. The final grade is the average of the grades obtained from individual laboratory classes. The final grade is the average of the grades obtained from each laboratory session.

Programme content

- Ensuring high availability of network devices responsible for safe data transmission (device hardening).
- IPSec VPN and SSL VPN network design and maintenance.
- Virtualization of firewalls.
- Ensuring security of web applications.
- Threat detection and prevention techniques at the network layer (intrusion detection systems, intrusion prevention systems).
- Security of wireless networks.
- Security of cloud services and platforms.
- Internet of Things security.

Course topics

Lecture topics:
- Ensuring high availability of network devices responsible for safe data transmission (device hardening).
- IPSec VPN and SSL VPN network design and maintenance.
- Virtualization of firewalls.
- Ensuring security of web applications.
- Threat detection and prevention techniques at the network layer (intrusion detection systems, intrusion prevention systems).
- Security of wireless networks.
- Security of cloud services and platforms.
- Internet of Things security.

Laboratory topics:
- Basic configuration of firewalls (e.g. Cisco / Huawei / CheckPoint).
- Secure access to network devices using Radius (AAA) server.
- Design and implementation of a firewall system with high availability.
- Design and implementation of IPSec VPNs.
- Design and implementation of SSL VPNs.
- Configuration of intrusion prevention system (IPS).
- Content filtering and protection using firewalls.

Teaching methods

Lectures: multimedia presentations, illustrated with examples given on the blackboard.
Laboratory exercises: practical exercises in groups with the use of network devices.

Bibliography

Basic
1. Joseph Migga Kizza: 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. Aaron Woland, Vivek Santuka, Mason Harris, Jamie Sanbower: 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. Elaine Barker, 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. J. Michael Stewart: Network Security, Firewalls And VPNs; Jones & Bartlett Learning Information Systems Security & Ass, 2nd Edition, 2013.
5. Gerardus Blokdyk: IPsec VPN A Complete Guide; 5STARCooks; 2019.

Breakdown of average student's workload

	Hours	ECTS
Total workload	50	2,00
Classes requiring direct contact with the teacher	32	1,00
Student's own work (literature studies, preparation for laboratory classes/ tutorials, preparation for tests/exam, project preparation)	18	1,00