Subject card

Subject name and code	Secure Network Systems and Services, PG_00049302
Field of study	Biomedical Engineering

Date of commencement of studies	October 2023	Academic year of realisation of subject	2026/2027
Education level	first-cycle studies	Subject group	Optional subject group Subject group related to scientific research in the field of study
Mode of study	Full-time studies	Mode of delivery	at the university
Year of study	4	Language of instruction	Polish
Semester of study	7	ECTS credits	3.0
Learning profile	general academic profile	Assessment form	exam

Conducting unit	Faculty of Electronics, Telecommunications and Informatics
Name and surname of lecturer (lecturers)	Subject supervisor — dr inż. Adam Bujnowski
	Teachers — dr inż. Adam Bujnowski

Lesson types and methods of instruction	Lesson type	Lecture	Tutorial	Laboratory	Project	Seminar	SUM
	Number of study hours	15.0	0.0	15.0	0.0	0.0	30
	E-learning hours included: 0.0						

Learning activity and number of study hours	Learning activity	Participation in didactic classes included in study plan	Participation in consultation hours	Self-study	SUM
	Number of study hours	30	3.0	42.0	75

Subject objectives	The goal of the subject is to familiarize students with typical problems related to the security of information systems. There will be expresses issues related to the security - sources of the problems, techniques of detection and analysis of the problem.

Learning outcomes	Course outcome	Subject outcome	Method of verification
	[K6_U07] can apply methods of process and function support, specific to the field of study	Student is able to create acces policy for selected information service and apply it	[SU4] Assessment of ability to use methods and tools
	[K6_W08] Knows and understands the fundamental dilemmas of modern civilisation and basic economic, legal and other conditions of various types of activities related to the field of study, including the basic concepts and principles in the field of industrial property and copyright protection.	Student is able to estimate cost of applied securiity policy	[SU2] Assessment of ability to analyse information
	[K6_U04] can apply knowledge of programming methods and techniques as well as select and apply appropriate programming methods and tools in computer software development or programming devices or controllers using microprocessors or programmable elements or systems specific to the field of study	Student is able to automate system log analysis	[SU4] Assessment of ability to use methods and tools
	[K6_U09] can carry out a critical analysis of the functioning of existing technical solutions and assess these solutions, as well as apply experience related to the maintenance of technical systems, devices and facilities typical for the field of studies, gained in the professional engineering environment	Student knows basic sources of information about actual security issues and knows how to use them	[SU2] Assessment of ability to analyse information
	[K6_U02] can perform tasks related to the field of study in an innovative way as well as solve complex and nontypical problems, applying knowledge of physics, in changing and not fully predictable conditions	Student analyses protection level of the given system	[SU1] Assessment of task fulfilment

Subject contents	Principal terms, safe system definition, measures of the server availability, redundance, scalability etc..
	Physical protection of the computer system
	Server room infrastructure and security
	Basic of the cryptology
	Principla cryptographic technologies used in the information systems
	Protection of the operating system
	Management of the computer pharms
	Analysis of the system security, Syste logs
	Computer virusses - principles of functioning and protection against virusses
	Network traffic controll, Firewalls
	Database security
	WWW security
	Fileservers security
	Overview of the typical hackers techniques
	Summary - System cybersecurity list

Prerequisites and co-requisites	

Assessment methods and criteria	Subject passing criteria	Passing threshold	Percentage of the final grade
	final writting	50.0%	50.0%
	laboratory achievements	50.0%	50.0%

Recommended reading	Basic literature	Praca zbiorowa, Vademecum teleinformatyka T1 , 2 i ch , IDG
		Wainwright , Apache 2.0 dla zaawansowanych, Helion/Wrox 2003/06
		Polaczek, Audyt bezpieczeństwa w praktyce, Helion 2006
		Kifner, Polityka bezpieczeństwa i ochrony informacji, Helion
	Supplementary literature	Greg Hoglund, Jamie Butler, Rootkity . sabotowanie jądra systemu Windows, Helion 2006
	eResources addresses	Adresy na platformie eNauczanie:

Example issues/ example questions/ tasks being completed	

Work placement	Not applicable