

WSB University						
Field of study: National security						
Course: Security in communication						
Educational profile: practical						
Education level: I-cycle studies						
Number of hours per semester	1		2		3	
	I	II	III	IV	V	VI
Full -time studies (L/C/lab/pr/e)*						18c
Part-time studies (L/C/lab/pr/e)						14c
LECTURER	dr inż. Krystian Mączka					
FORM	Classes					
COURSE OBJECTIVES	To acquaint the student with the main threats of communication security breach and methods of securing communication.					
Reference to learning outcomes		Description of learning outcomes			Verification of learning outcomes	
Field-related learning outcome	PQF					
Knowledge						
BN_W06	P6U_W	Knows and understands the process of violating communication security, knows methods of increasing security in communication;			Test	
Skills						
BN_U02	P6U_U	Can choose methods of securing communication adequately to the category of secrets passed on;			Test	
Social competences						
BN_K06	P6U_K	He is ready to take professional actions in the field of selecting methods of securing communication;			Test	
Students' own workload (in didactic hours 1h=45 minutes)**						
Full- time Participation in lectures = Participation in classes = 18 Preparation to classes = 15 Preparation to lectures = Preparation to an examination = 15 Project tasks = e-learning = Credit/examination =2 others (indicate which) = 2 TOTAL: 52 ECTS points: 2 Including practical classes:				Part-time Participation in lectures = Participation in classes = 14 Preparation to classes = 17 Preparation to lectures = Preparation to an examination = 17 Project tasks = e-learning = Credit/examination =2 others (indicate which) = 2 TOTAL:52 ECTS points:2 Including practical classes:		
PREREQUISITES	n/a					

COURSE CONTENT (Division into contact hours and e-learning)	Contact hours: <ul style="list-style-type: none"> • Division and definitions of selected categories of threats • Information security management • Methods of securing communication • Classification of user authentication methods <ul style="list-style-type: none"> ◦ The specificity of methods based on the user's knowledge ◦ Authorization methods based on biometric techniques ◦ User authentication based on physical authorization attribute • Applications of cryptography • Application of a digital signature • Steganography E-learning:n/a
LITERATURE (compulsory reading)	<ul style="list-style-type: none"> • Richard E. Blahut, Cryptography and Secure Communication 1st Edition, ISBN-13: 978-1107014275, ISBN-10: 1107014271 • Bryan C. Taylor, Hamilton Bean, The Handbook of Communication and Security, 2019
OPTIONAL LITERATURE (including at least two items in English, either books or articles)	<ul style="list-style-type: none"> • ALRIKABI, Haider TH; HAZIM, Hussein Tuama. Enhanced Data Security of Communication System Using Combined Encryption and Steganography. <i>International Journal of Interactive Mobile Technologies</i>, 2021, 15.16 • Stavroulakis, Peter & Stamp, Mark. (2010). Handbook of Information and Communication Security. 10.1007/978-3-642-04117-4.
TEACHING METHODS (Division into contact hours and e-learning)	Contact hours: Interactive lecture Brainstorm Discussion E-learning:n/a
TEACHING AIDS	Multimedia projector, software supporting security solutions.
PROJECT (if implemented in the framework of a classes module)	Project goal:n/a Topic of the project: Project form:
FORM AND CONDITIONS OF ASSESSMENT (Division into contact hours and e-learning)	Test

* L-lecture, C- classes lab- laboratory, pro- project, e- e-learning