

PROGRAMME OF POSTGRADUATE STUDIES

POSTGRADUATE MBA STUDIES CYBER SECURITY MANAGEMENT (name of the studies)

**Adopted by the Resolution by the Senate of MUT No. 59/WAT/2021
of June 24, 2021**

Applicable from October 1, 2021

Warsaw

2021

PROGRAMME OF POSTGRADUATE MBA STUDIES

assessed by the Council for the Education at the Cybernetics Faculty and the Council for the Scientific Discipline "Technical Information Technologies and Telecommunication" and adopted by the Senate of MUT

The Resolution by the Senate of MUT No. .../WAT/2021 of June 24, 2021

the name of Postgraduate Studies:

POSTGRADUATE MBA STUDIES "CYBER SECURITY MANAGEMENT"

conducted at:	Faculty of Cybernetics
applicable from:	the academic year October 1, 2021
The form of the studies:	part-time (non-residential) studies
Duration:	2 semesters
Total number of hours:	232
Quantity of ECTS credits:	35
Language of the studies:	English
Code of the studies:	WCYIXCNP21E
Qualification requirements:	Graduate Level Diploma (Master's and Professional Degree)
Form of completion of studies:	final examination
Level of the Polish Qualifications Framework granted after completion of studies:	partial, level 7
Information on incorporating the qualification into the Integrated Qualification System (IQS)	
- date of incorporation of the qualification into IQS¹: <i>not applicable</i>	
- qualification code in IQS:	

¹ If applicable

SHORT CHARACTERISTICS OF THE QUALIFICATION AWARDED

Postgraduate MBA Studies “Cyber security management” are aimed at those wishing to improve skills related to cyber security in its broadest sense. The studies are intended for people with higher education and specific experience in managerial positions, who are professionally involved with aspects of cyber security. The studies will be conducted in English in cooperation with University of Genova (Italy) and NATO Communications and Information Agency.

Postgraduate studies provide knowledge, skills and competences, in the field of, among other things:

- cyber security systems,
- contemporary digital threats,
- legal aspects of cyber security and cybercrime,
- risk management in cyber security,
- crisis management in cyber security,
- IT service and project management,
- managerial decisions,
- the “information warfare” theory,
- national cyber security system,
- NATO cyber security policy.

EXPECTED LEARNING OUTCOMES

The MBA post-graduate education programme shall cover courses in the form of lectures, exercises, laboratory classes and seminars, and the final examination.

Based on the organisational and programme assumptions, an alumnus of post-graduate MBA cyber security studies should achieve the following learning outcomes as a result of the study programme.

Symbol and the number of the outcome	The description of the expected learning outcomes	Code of the description component	
		of a field nature	of an occupational nature
	KNOWLEDGE Alumnus:		
P_W01	has an in-depth knowledge in the field of the management of information resources and databases	P7S_WG	P7Z WO
P_W02	knows and understands the economic, organisational, social and military determinants of an organisation's crisis caused by a breach of its cyber security	P7S_WG	P7Z WT
P_W03	knows and understands the theories of "information warfare" as a modern form to conduct actions	P7S_WG	P7Z WT
P_W04	knows and understands the aspects and regulations of cyber security and cyber crime	P7S_WG	P7Z WT
P_W05	knows and understands the basic cyber security threats and methods to counteract them	P7S_WG	P7Z WT
P_W06	knows basic challenges and trends in the field of cyber security	P7S_WK	P7Z WT
P_W07	has in-depth knowledge of modelling decision-making problems and of methods and computer tools for solving these problems in the field of management	P7S_WG	P7Z WT
P_W08	has a comprehensive knowledge in the field of methods of modelling cyber security threats	P7S_WG	P7Z WZ
P_W09	has knowledge in the field of cyber security policies, strategies and systems used by NATO	P7S_WG	P7Z WT
P_W10	knows and understands economic, social and military determinants of threats in the field of cyber security	P7S_WK	P7Z WT
P_W11	knows the basic principles and methods of project and IT service management	P7S_WK	P7Z WT

SKILLS Alumnus:			
P_U01	can practically apply solutions in the field of management of information resources to protect databases	P7S_UW	P7Z UO
P_U02	can effectively lead teams, including crisis teams, in ensuring cyber security	P7S_UW	P7Z UO
P_U03	can identify and effectively counteract cases of "information warfare"	P7S_UW	P7Z UO
P_U04	can apply the applicable legal regulations to cyber security processes	P7S_UW	P7Z UI
P_U05	can assess risks and apply appropriate methods and techniques to deal with basic cyber security threats	P7S_UW	P7Z UO
P_U06	can use basic technologies and tools to ensure cyber security in practice	P7S_UW	P7Z UO
P_U07	can practically use technologies, techniques, and security tools in IT networks	P7S_UW	P7Z UO
P_U08	can use knowledge in the field of cyber security policies, strategies and systems used by NATO to improve national cyber security systems	P7S_UW	P7Z UN
P_U09	can make effective managerial decisions using appropriate methods and computer-aided decision-making tools	P7S_UW	P7Z UI
P_U10	can assess economic, social and military threats in the field of cyber security	P7S_UW	P7Z UI
P_U11	can independently plan and implement his/her own learning and carry out his/her own learning in the field of cyber security	P7S_UO	P7Z UO
P_U12	can apply in practice the basic principles and methods of project and IT service management	P7S_UU	P7Z UN
SOCIAL COMPETENCES Alumnus:			
P_K01	is ready to recognise the importance of knowledge in solving cyber security problems	P7S_KK	P7Z KO
P_K02	appreciates the need for practical implementation of an effective cyber security policy	P7S_KO	P7Z KP
P_K03	is ready to think and act in an entrepreneurial manner in the field of cyber security	P7S_KO	P7Z KP P7Z KW

*) P_W - learning outcomes - knowledge category
P_U - learning outcomes - skills category
P_K - learning outcomes - category of social competences

LIST OF THE COURSES

The information sheets of the courses shall be appended to the curriculum / degree programme.

Code of the course	Name of the course	Quantity of ECTS credits:
WCYIXCNP-CSSE	Cyber security systems	3
WCYIXCNP-CYBE	Cybercrime	1
WCYIXCNP-ZRCE	Risk management in cyber security	2
WCYIXCNP-ZKCE	Crisis management in cyber security	3
WCYIXCNP-DMEE	Managerial decisions	3
WCYIXCNP-ZPIE	Project management and systems engineering in cyber security	1
WCYIXCNP-OBDE	Protection of transactional and statistical databases	2
WCYIXCNP-ZUIE	IT service management	2
WCYIXCNP-TWIE	"Information warfare" theory	3
WCYIXCNP-KSCE	National Cyber Security System	2
WCYIXCNP-PNCE	NATO policy on cyber security	3
WCYIXCNP-EKE	Final exam	10
In total:		35

THE MEANS OF VERIFICATION AND ASSESSMENT OF THE STUDENT'S ACHIEVEMENT OF THE EXPECTED LEARNING OUTCOMES

Implementation of the concept of conducting classes based on learning outcomes translates into various forms and evaluation criteria. An important aspect of the verification is the unambiguous definition of evaluation criteria for individual learning outcomes. During the first classes as part of particular courses, the tutors shall inform students of postgraduate studies about the expected learning outcomes for each subject and about the forms and methods to verify the outcomes.

The verification of the expected learning outcomes, especially in the field of knowledge verification, shall be carried out in the form of tests and examinations. The specific nature of the courses being taught renders this verification in written or oral form, as necessary. The results of this verification shall be documented in the written works and in reports of the tests and examinations.

At the same time, learning outcomes in the field of knowledge, skills and social competences are verified during practical meetings at exercises, laboratory classes, seminars, and workshops. The basic forms of verification of the assumed learning

outcomes are *case studies*, laboratory tasks, take-home assignments, multimedia presentations, essays, reviews, and elaborations. The results of this verification shall be documented in the form of handwritten elaborations prepared by the students, in the form of printouts of prepared elaborations or in electronic form.

The final form of verification of knowledge, skills and social competences is, in accordance with § 23 sec. 3 of the MUT Postgraduate Study Regulations, a final examination conducted at the end of studies by a committee designated by a decision of the dean.

PROGRAMME OF PART-TIME (NON-RESIDENTIAL) POSTGRADUATE STUDIES

FACULTY OF CYBERNETICS

NAME OF THE STUDIES: POSTGRADUATE MBA STUDIES "CYBER SECURITY MANAGEMENT"

The Courses		the hours / credits in total ECTS		of which hours:			the hours / credits' rigor ECTS in a semester				Organisational Unit in charge of the course		
		teaching hours	ECTS	lectures	exercises	laboratory/project/ seminar/ classes	I		II				
							hours	ECTS	hour	ECTS			
1	Cyber security systems	24	3	12		12	24	x	3			Foreign Partner	
2	Cybercrime	16	1	8	8		16	+	1			National Partner/UKSW	
3	Risk management in cyber security	20	2	10	4	6	20	+	2			Faculty of Cybernetics	
4	Crisis management in cyber security	24	3	12		12	24	+	3			National Partner	
5	Managerial decisions	24	3	16		8	24	x	3			Faculty of Cybernetics	
6	Project management and systems engineering in cyber security	16	1	8		8	16	+	1			Faculty of Cybernetics	
7	Protection of transactional and statistical databases	20	2	12		8				20	+	2	Faculty of Cybernetics
8	IT service management	20	2	14	6					20	+	2	Faculty of Cybernetics
9	"Information warfare" theory	24	3	12		12				24	x	3	Faculty of Cybernetics
10	National Cyber Security System	20	2	10	10					20	+	2	NASK
11	NATO policy on cyber security	24	3	12		12				24	+	3	Foreign Partner
12	Final exam	8	10							8	x	10	Examination committee
The hours / credits in total ECTS		240	35	126	28	78	124	13	116	22			
Types and number of rigours in the semester:						exam - x	2		2				
						test - +	4		4				

THE FORM TO COMPLETE THE STUDIES

At the Military University of Technology, the conditions to complete postgraduate studies are laid down in the MUT Postgraduate Study Regulations.

Pursuant to § 21 (1) of the MUT Postgraduate Study Regulations, the studies are completed by a final examination conducted by an examination committee set up by a decision by the Dean of the Faculty.

CONDITIONS TO OBTAIN A CERTIFICATE OF COMPLETION OF THE STUDIES

A final examination shall be required in order to obtain the certificate. The certificate of completion of studies shall include the result of studies, determined in accordance with § 25 of the MUT Postgraduate Study Regulations.

The document formalising and giving legal effect to the obtained certificate of completion of postgraduate studies shall be the Rector's decision.

“APPROVED BY”

Dean of Faculty of
Cybernetics

Zbigniew TARAPATA,
PhD, Eng. Professor
at MUT

INFORMATION SHEET OF THE COURSE

Name of the course:	Cyber security systems	Systemy cyberbezpieczeństwa
Code of the course:	WCYXCNP-CSSE	
Language of lectures:	English	
Applicable from:	2021/2022	
Form of classes number of hours/rigour, hours in total	<i>Lect. – 12/x, Lab – 12; in total: 24 hours – 3 credits ECTS</i>	
Author:	<i>Prof. Alessandro ARMANDO</i>	
Organisational Unit in charge of the course	<i>Foreign Partner</i>	
Short description of the course:	The course will introduce the student of the post-graduate studies to the technical aspects of Cybersecurity.	
Full description of the course (program content):	<p>Lectures will introduce students to some selected topics of Cybersecurity and will engage them in hands-on activities on some simple, yet significant practical problems.</p> <p>Lecture topics:</p> <ol style="list-style-type: none">1. Cybersecurity and Cyber-risk - (2 hrs.)2. Black-box view of cryptography (both symmetric and public-key encryption) – (1 hrs.)3. The key distribution problem – (1 hr.)4. Digital Signatures – (1hr.)5. Secure Elements (Smartcards and Hardware Security Modules) – (1 hr.)6. Digital Certificates and the Public Key Infrastructure – (1hr.)7. Security Protocols – (2hrs.)8. Secure e-mail (PGP, Certified Mail) – (1hr.)9. Web Security – (2hrs.) <p>The laboratory classes shall be conducted in the form of case studies and project tasks. The work on case analyses and project is partially carried out in a team form. The results of team work/conclusions/proposals for problem-solving solutions are presented and discussed within the training group.</p> <p>Topics of laboratory classes:</p> <ol style="list-style-type: none">1. Security protocols – (8hrs.)2. GPG – (4hrs.)	
The reference books and papers:	<p>The basic reference books and papers:</p> <ul style="list-style-type: none">• C. Pfleeger and S. Pfleeger. <i>Security in Computing</i>. Pearson Ed., 2015.• W. Stallings and L. Brown. <i>Computer Security: Principles and Practice</i>. Pearson, 2014.	
Learning outcomes:	W1. Knows and understands the main cyber security threats and methods to	

	<p>counter them / P_W05.</p> <p>W2. Has in-depth knowledge of and methods for modelling cyber security threats / P_W08.</p> <p>W3. Knows and understands the economic, social and military determinants of cyber security risk / P_W10.</p> <p>U1. Is able to apply appropriate methods and techniques to deal with basic cyber security threats / P_U05.</p> <p>U2. Is able to assess economic, social and military threats to cyber security / P_U10.</p>
<p>Methods and criteria for assessing the students (the method to verify the achievement of the expected learning outcomes):</p>	<ul style="list-style-type: none"> ● The education module shall be credited on the basis of a written examination. ● The positive grade obtained at the laboratory classes is required for the student to be admitted to the mid-term/final/end-term course test. ● Achievement of W1, W2, W3 and U1, U2 effects is verified during the laboratory classes and final course test.
<p>ECTS balance sheet (student workload)</p>	<p>Activity / workload of the student in hours.</p> <ol style="list-style-type: none"> 1. Participation in lectures / 12 hours 2. Participation in laboratory classes / 12 hours 3. Unassisted studying topics of lectures / 20 hours 4. Unassisted preparation for laboratory classes / 20 hours 5. Participation in consultations / 2 hours 6. Preparation for course test / 20 hours 7. Participation in course test / 2 hours <p>Total workload of the student: 88 hours – 3 credits ECTS</p>

“APPROVED BY”

Dean of Faculty of
Cybernetics

Zbigniew TARAPATA,
PhD, Eng. Professor
at MUT

INFORMATION SHEET OF THE COURSE

Nazwa przedmiotu:	<i>Cybercrime</i>	<i>Cyberprzestępczość</i>
Code of the course:	WCYIXCNP-CYBE	
Language of lectures:	English	
Applicable from:	2021/2022	
Form of classes number of hours/rigour, hours in total	<i>Lect. – 8+, Ex – 8; in total: 16 hours – 1 pkt. ECTS</i>	
Author:	<i>Agnieszka GRYSZCZYŃSKA, PhD, DSc, Eng.</i>	
Organisational Unit in charge of the course	National Partner/UKSW	
Short description of the course:	The aim of the course is to prepare students for the criminal law analysis of the most common security incidents - i.e. determining which incidents constitute crimes and performing a criminal law analysis of the elements of a prohibited act. Moreover, the goal of the classes is to prepare students to independently determine what evidence should be collected depending on the act that is the subject of the proceedings.	
Full description of the course (program content):	<p>Classes are conducted in a manner that activates listeners, in the form of lectures with elements of workshops and group discussions, case studies, group mini-projects, and the use of multimedia techniques.</p> <p>Lecture topics:</p> <ul style="list-style-type: none">• Concept of cyber security and incidents (0,5hr.)• The concepts of crime, cybercrime, and computer crime (0,5hr.)• Legal bases of liability for selected acts violating availability, confidentiality or integrity of data or information systems (1hr.)• Incidents that violate the availability of resources using DoS, DDoS, and ransomware attacks as examples. (1hr.)<ul style="list-style-type: none">○ Analysis of legal basis of liability for an attack• Incidents violating the confidentiality of resources (1hr.)<ul style="list-style-type: none">○ Criminal liability for hacking○ Violations of personal data protection○ Identity theft○ Analysis of the basis of liability for an attack• Fraud, computer fraud, theft of funds from bank accounts (1hr.)<ul style="list-style-type: none">○ Analysis of legal grounds for criminal liability• Laundering the proceeds of crime (0,5hr.)• Concept of electronic evidence (0,5hr.)• Procedural aspects of securing evidence in cybercrime cases (1hr.)• Filing of notices of suspected criminal offences, victim and notifier in criminal proceedings (1 hr.) <p>Workshops (8hrs.) are conducted in the form of case study analyses and small project tasks, some of which are carried out in a team format. Team</p>	

	work results/conclusions/proposals of solutions to problem situations are presented and discussed in the training group.
The reference books and papers:	<p>The basic reference books and papers:</p> <ul style="list-style-type: none"> • Agnieszka Gryszczyńska, Pozyskiwanie i analiza danych dotyczących incydentów cyberbezpieczeństwa [w:] Internet. Analityka danych, red. G. Szpor, Warszawa 2019, s. 296-313, ISBN 978-83-8198-138-5 • Agnieszka Gryszczyńska, Prowadzenie postępowań karnych w sprawach z zakresu dystrybucji ransomware, [w:] Rocznik Bezpieczeństwa Morskiego Nr 1/S/2019, Przestępczość Teleinformatyczna 2018, red. J. Kosiński, Gdynia 2019, s.193-218, ISSN 1898-3189 • Internet. Cyberpandemia, red. Grażyna Szpor, Agnieszka Gryszczyńska; C.H. Beck; 2021 • Internet. Analityka danych, red. Kamil Czaplicki, Grażyna Szpor, CH. Beck, Warszawa 2019 • Internet. Strategie bezpieczeństwa, red. Grażyna Szpor, Agnieszka Gryszczyńska; C.H. Beck; 2017 <p>The supplementary books:</p> <ul style="list-style-type: none"> • B. Kunicka-Michalska, Przestępstwa przeciwko ochronie informacji i wymiarowi sprawiedliwości. Rozdział XXX i XXXIII Kodeksu karnego. Komentarz, Warszawa 2000
Learning outcomes:	<p>W1. Graduate knows criminal law elements of prohibited acts / P_W04. W2. Graduate knows and understands the phenomena connected with threats in cyberspace, methods of their identification / P_W05 U1. The graduate is able to define issues connected with cybercrime in legal and extra-legal context / P_U04 U2. Graduate is able to make a criminal law analysis of a cyber security incident / P_U04 K1. The graduate is ready to undertake actions connected with counteracting threats in cyberspace / P_K03</p>
Methods and criteria for assessing the students (the method to verify the achievement of the expected learning outcomes):	<ul style="list-style-type: none"> • The course shall be completed on the basis of a pass in an oral form. • Achievement of W1, W2 and U1, U2 effects is verified during the workshop and final course test.
ECTS balance sheet (student workload)	<p>Student's activity / workload in hours:</p> <ol style="list-style-type: none"> 1. Participation in lectures / 8 hrs. 2. Participation in exercise classes / 8 hrs. 3. Independent study of the lectures subject / 8 hrs. 4. Preparing for the credit / 8 hrs. 5. Participation in consultations / 2 hrs. <p>The total student's workload: 34 hours / 1 credit ECTS</p>

“APPROVED BY”

Dean of Faculty of
Cybernetics

Zbigniew TARAPATA,
PhD, Eng. Professor
at MUT

INFORMATION SHEET OF THE COURSE

Module name:	<i>Risk management in cyber security</i>	<i>Zarządzanie ryzykiem w cyberbezpieczeństwie</i>
Code of the course:	WCYIXCNP-ZRCE	
Language of lectures:	English	
Applicable from:	2021/2022	
Form of classes number of hours/rigour, hours in total	Lect. – 10/+, Ex – 4, Lab – 6; in total: 24 hours - 2 credit ECTS	
Author:	<i>Jerzy STANIK, PhD, Eng.</i>	
Organisational Unit in charge of the course	<i>Faculty of Cybernetics / Institute of IT Systems</i>	
Short description of the course:	<p>The subject allows to provide the student of postgraduate studies with the basics of knowledge about the problems related to the security of various objects / entities operating in cyberspace and their management in terms of cyber threats. Students learn to identify and understand the problems of information cybersecurity, construct models and methodologies for measuring the level of cyberthreats in relation to various types of systems / objects functioning in cyberspace. Students learn how to effectively and efficiently use the available technical and organizational security measures as well as instruments and mechanisms to protect sensitive cyberspace resources. Moreover, students acquire skills in the area of cybersecurity risk analysis and estimation as well as the effects of cyber threats in cyberspace. They acquire skills related to:</p> <ul style="list-style-type: none">• Managing the level of cybersecurity in cyberspace systems,• basic measures to protect them against cyber attacks• monitoring the cybersecurity of facilities, entities or information systems functioning in cyberspace.• skills in using methodologies and risk analysis tools and assessing the effectiveness of technical and organizational security measures,• skills and good practices of developing cybersecurity documentation, eg normative documentation; operational documentation, procedures for reacting and documenting incidents in cyberspace.	
Full description of the course (programme content):	<p>Lectures are conducted in a conventional way that activates the audience, using a multimedia presentation.</p> <p>Lecture topics:</p> <ol style="list-style-type: none">1. Basic concepts of cybersecurity (cyberspace, cybersecurity, the concept of an information resource, information pyramid, basic security attributes of a sensitive object, PDCA model, security in cyberspace from the position of international law) – Lect. 1 hour.2. Basic elements of security in cyberspace (criteria for classification of sensitive cyberspace resources and their security attributes; valuation of sensitive resources in terms of cybersecurity; vulnerabilities; cyberthreats and protection of sensitive resources)	

<p>The reference books and papers:</p>	<p align="center">– Lect. 1 h; Ex 1 h</p> <ol style="list-style-type: none"> 3. Models of measuring the level of security in cyberspace. (Generalized risk model - model of cyber threats; Model for the protection of personal data in the light of the GDPR; Model of the Ministry of Digitization from 2015, Model based on the risk function; Security model oriented to changes in the value of security attributes, Safety measurement model based on the potentials of the threat system and ; Security measurement model based on the criteria for assessing the quality of the system functioning in cyberspace; Model based on components in relation to the identified cyberspace risk areas) – Lect. 2 hours;. Ex 2 hours 4. Methodology of measuring the level of risk in cybersecurity (the concept of risk, the process of dealing with cybersecurity risk and its stages / activities, risk assessment, risk management, acceptable risk, residual risk, risk monitoring and review, methods for assessing the effectiveness of information security security) – Lect. 2 h; Lab 3 h 5. Methodology of designing and implementing a security system in relation to a selected subject of operation in cyberspace. (Stages of design and implementation of a security system according to ISO / IEC 27003: 2014; life cycle of a security system for a selected cyberspace object, security technologies, methods of measuring security effectiveness, security system improvement techniques) – Lect. 2 h; Lab 3 h 6. Documentation of the cybersecurity management system (Types of cybersecurity documentation, normative documentation; operational documentation) – Lect. 2 h; Ex 1 h <p>Exercise and laboratory activities are conducted in the form of guided discussions and case study analyzes. Working in groups / solving tasks.</p> <p>The basic reference books and papers:</p> <ul style="list-style-type: none"> • Dębowski T., Cyberbezpieczeństwo wyzwaniem XXI wieku, RCHAEGRAPH, Wydawnictwo Naukowe, Łódź – Wrocław 2018, • Zagrożenia i wyzwania bezpieczeństwa współczesnego świata. Wymiar ekonomiczno- społeczny, pod red. Izabeli Oleksiewicz i Kingi Stępień, Wydawnictwo Rambler, 2016, • Tekielska P., Czekaj Ł., Działania służb w Unii Europejskiej realizujących zadania na rzecz bezpieczeństwa cybernetycznego, w: Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku, M. Górka (red.), Warszawa 2014, Difin. <p>The supplementary reference books and papers:</p> <ul style="list-style-type: none"> • Dominika Lisiak-Felicka, Maciej Szmit, Cyberbezpieczeństwo administracji publicznej w Polsce wybrane zagadnienia, European association for security Kraków 2016 • Banyś T., Łuczak J., Ochrona danych osobowych w praktyce. Jak uniknąć błędów i ich konsekwencji prawnych, wyd. PRESSCOM, Wrocław 2017, Wyd. III, stron 408, ISBN 978-83-65611-30-7 • Dorothy E. Denning, Wojna informacyjna i bezpieczeństwo informacji, WNT 2002 r. • PN ISO/IEC 27001: 2017, Systemy zarządzania bezpieczeństwem informacji – Specyfikacja i wytyczne do stosowania. • PN ISO/IEC 27002:2017, Technika informatyczna Praktyczne zasady zarządzania bezpieczeństwem informacji. • PN ISO/IEC 27005, Technika informatyczna - Techniki bezpieczeństwa - Zarządzanie Bezpieczeństwem Informacji ryzyka. • Dokumentacja przetwarzania danych osobowych zgodnie z RODO.
--	--

<p>Learning outcomes:</p>	<p>W1. Knows and understands basic cyber security threats and methods to counter them / P_W05.</p> <p>W2. Knows the basic challenges and development trends in cyber security /P_W06.</p> <p>U1. Can assess risk and apply appropriate methods and techniques to counter basic cyber security threats /P_U05.</p> <p>U2. Is able to use basic cyber security technologies and tools in practice / P_U07.</p> <p>U3. Is able to plan and realize own learning independently in the field of cyber security / P_U11.</p> <p>K1. Understands the necessity of practical implementation of an effective policy to ensure cyber security of information systems / P_K02.</p> <p>K2. Is ready to think and act in an entrepreneurial way in the field of cyber security assurance / P_K03.</p>
<p>Methods and criteria for assessing the students (the method to verify the achievement of the expected learning outcomes):</p>	<ul style="list-style-type: none"> • The module is passed on the basis of a credit. • Passing of classes and laboratories is a prerequisite for obtaining credit and laboratories. • The achievement of effects W1, W2 is checked during the classes and during the pass mark credit. The achievement of U1, U2, U3 is checked during the presentation of the results of the case studies and guided discussions during classes and laboratories.
<p>ECTS balance sheet (student workload)</p>	<p>Student's activity / workload in hours</p> <ol style="list-style-type: none"> 1. Participation in lectures / 10 hrs. 2. Participation in classes / 4 hrs. 3. Participation in laboratories / 6 hrs. 4. individual studying of the lectures subjects / 15 hrs. 5. individual preparation to exercises / 15 hrs. 6. The participation in consultations / 2 hrs. 7. Preparation for the course test / 20 hrs. 8. The participation in the assessment / 1 hour. <p>The total student's workload: 73 hrs / 2 credits ECTS</p>

“APPROVED BY”

Dean of Faculty of
Cybernetics

Zbigniew TARAPATA, PhD,
Eng. Professor at MUT

INFORMATION SHEET OF THE COURSE

Name of the course:	<i>Cyber security crisis management</i>	<i>Zarządzanie kryzysowe w cyberbezpieczeństwie</i>
Code of the course:	WCYIXCNP-ZKCE	
Language of lectures:	English	
Applicable from:	2021/2022	
Form of classes number of hours/rigour, hours in total	<i>Lect. – 12/4, Lab – 12; in total: 24 hours – 3 credits ECTS</i>	
Author:	<i>Bogusław HAJDASZ, PhD</i>	
Organisational Unit in charge of the course	<i>National Partner</i>	
Short description of the course:	The course will enable the postgraduate student to learn the basic principles and practical methods of crisis management in an organization affected by a cyberattack and its renewal after a crisis.	
Full description of the course (programme content):	<p>Classes are conducted in a way that activates students: in the form of lectures with elements of workshops and group discussions, case studies, mini-group projects, surveys, and tests, as well as using multimedia techniques. Before the class, students prepare an introductory task - 6 slides of the PP presentation "How we dealt with the crisis in my previous company/institution"</p> <p>Lecture topics:</p> <ol style="list-style-type: none">1. Cybersecurity crisis of the organization and its evolution (1hr.)2. Managing the risk of cybersecurity incidents in the organization (1hr.)3. Efficient crisis management - possible scenarios, main challenges, and existing strategic options (1hr.)4. Goals, stages, and strategies for dealing with the cybersecurity crisis (2hrs.)5. The leader of the organization and his crisis management teams: CMT, BCT, CSIRT (1,5hr.)6. Critical success factors in dealing with the crisis of the organization (1hr.)7. Tests and surveys - self-assessment of the manager's ability to manage a company crisis and assessing the preparedness and ability of the organization to survive a cybersecurity crisis (for a student's own use only) (2hrs.)8. Practical activities increasing the chances of surviving the cybersecurity crisis of the organization (1,5hr.)9. Case study: assessment of the efficiency of crisis management (1hr.)10. Strategic renewal - changing the model of the organization after the cybersecurity crisis and building a crisis-resilient organization (2hrs.)	

	<p>11. Discussion of selected introductory tasks presentations – The ways of dealing with a crisis caused by a cybersecurity incident in a given company/institution (3hrs.)</p> <p>12. Conclusions and summary (0.5hr.)</p> <p>Workshops are conducted in the form of case study analyzes and small project tasks partly carried out in a team form. The results of the team's work- conclusions and proposed solutions to crisis situations are presented and discussed by the whole group.</p>
The reference books and papers:	<p>The basic reference books and papers:</p> <ul style="list-style-type: none"> • Crandall W.R., Parnell, J.A. Spillan J.E. Crisis Management in the New Strategy Landscape. SAGE Publications 2010 • Jnaneswar K., Gayathri Ranjit. Exploring the Cyber Threat Landscape and Cyber Crisis Management Model. International Journal of Science and Research (IJSR) Volume 5 Issue 8, 2016 • Holger Kaschner. Cyber Crisis Management: Das Praxishandbuch zu Krisenmanagement und Krisenkommunikation (German Edition), Springer Verlag 2020 • Belz G., Cyfert Sz. Strategiczna i organizacyjna odnowa przedsiębiorstw. Wydawnictwo UE we Wrocławiu 2017 <p>Supplementary literature:</p> <ul style="list-style-type: none"> • Hajdasz B. Wybory strategiczne podczas odnowy przedsiębiorstwa (Strategic decisions during company renewal) HP 2017
Learning outcomes:	<p>W1. Knows and understands the economic, organizational, social and military determinants of an organization's crisis caused by a breach of its cyber security / P_W02.</p> <p>U1. Can effectively lead crisis teams in providing cyber security / P_U02.</p> <p>U2. Can independently plan and implement own learning in the field of cyber security / P_U11.</p>
Methods and criteria for assessing the students (the method to verify the achievement of the expected learning outcomes):	<ul style="list-style-type: none"> • The module shall be completed on the basis of an oral assessment. • A positive mark for credit is obtained from laboratory classes. • The achievement of W1 effect is verified during the laboratory classes and the final course test. • The achievement of effect U1, U2 is checked during the presentation of the results of the case studies and guided discussions during laboratory and workshops.
ECTS balance sheet (student workload)	<p>Activity / workload of the student in hours.</p> <ol style="list-style-type: none"> 1. Participation in lectures / 12 hours 2. Participation in laboratory classes / 12 hours 3. Unassisted studying topics of lectures / 20 hours 4. Unassisted preparation for laboratory classes / 20 hours 5. Participation in consultations / 2 hours 6. Preparation for course test / 20 hours 7. Participation in course test / 2 hours <p>Total workload of the student: 88 hours – 3 credits ECTS</p>

“APPROVED BY”

Dean of Faculty of
Cybernetics

Zbigniew TARAPATA,
PhD, Eng. Professor
at MUT

INFORMATION SHEET OF THE COURSE

Name of the course:	<i>Managerial decisions</i>	<i>Decyzje menedżerskie</i>
Code of the course:	WCYIXCNP-DMEE	
Language of lectures:	English	
Applicable from:	2021/2022	
Form of classes number of hours/rigour, hours in total	<i>Lect. – 16/x, Lab – 8; in total: 24 hours – 3 pkt. ECTS</i>	
Author:	<i>Zbigniew TARAPATA, PhD, DSc, Eng.</i>	
Organisational Unit in charge of the course	<i>Faculty of Cybernetics / Institute of IT Systems</i>	
Short description of the course:	<p>The course provides postgraduate students with knowledge in the field of managerial decision-making. Students will be introduced to both models, methods and computer tools used to solve decision-making problems. Students learn about the principles of modelling decision-making problems, types of decision-making models, examples of models of typical decision-making problems in the field of management and command, and their applications. They are introduced to the problem of decision making in deterministic and random (risk) conditions, with multiple criteria (multi-criteria optimization), in conflict situations (elements of game theory). In addition, they learn about the analysis of complex projects (CPM, PERT, CPM-cost), forecasting methods and optimization of investment decisions.</p>	
Full description of the course (programme content):	<p>Lecture topics (16 hours):</p> <ol style="list-style-type: none">1. Decisions versus operations research. Modelling of decision-making problems, types of decision-making models (continuous, discrete, mixed, linear, non-linear), examples of models of typical decision-making problems from the field of management and command (4 hrs).2. Decision making under risk: risk vs uncertainty, measures of decision risk, decision trees, elements of utility theory. Examples of formulating and solving practical decision-making problems under risk conditions (2 hrs).3. Multi-criteria decision making. Dominated and non-dominated solutions, Hasse diagram. Methods of solving multi-criteria problems (metacriteria, compromise solution methods, criteria function prioritization, ranking methods, etc.). Examples of formulating and solving practical problems as tasks with multiple criteria (3 hrs).4. Decision-making in conflict situations. Two-person games, coalition and non-coalition games, games with nature, games and multi-criteria problems. Examples of using decision game theory in management and command (2 hrs).5. Network models of complex undertakings: CPM, PERT, CPM-Cost (2 hrs).6. forecasting methods: exponential smoothing models, trend models, econometric models. Examples of using forecasts in management (2 hrs).7.	

	<p>7. investment decisions optimisation (1 hour).</p> <p>Topics for practical classes (8 hours):</p> <ol style="list-style-type: none"> 1. Modelling of decision problems and tools for solving formulated problems (Solver, OpenSolver, WinQSB, GAMS), 4 hrs; 2. Decision making with multiple criteria. Methods of solving multi-criteria tasks (metacriteria, compromise solution methods, criteria function hierarchy, ranking methods, etc.), 2 hrs; 3. Forecasting methods: exponential smoothing models, trend models, econometric models, 2 hrs.
<p>The reference books and papers:</p>	<p>The basic reference books:</p> <ul style="list-style-type: none"> • Taha H: Operations Research: An Introduction, Pearson, 2016. • Watson J.: Strategy: An Introduction to Game Theory, 2nd Edition, W. W. Norton & Company, 2013. <p>The additional reference books:</p> <ul style="list-style-type: none"> • Kukuła K. (red.): Badania operacyjne w przykładach i zadaniach. PWN, Warszawa, 2015. • Szapiro T. (red.): Decyzje menedżerskie z Excelem, PWE, Warszawa, 2000. • Manikowski A., Tarapata Z.: Prognozowanie i symulacja rozwoju przedsiębiorstw, WSE, Warszawa, 2000. • Manikowski A., Tarapata Z.: Ocena projektów gospodarczych, Cz.1, Modele i metody, Difin, Warszawa, 2001. • Manikowski A., Tarapata Z.: Ocena projektów gospodarczych, Cz.2, Przykłady i zadania, Difin, Warszawa, 2001.
<p>Learning outcomes:</p> <p>Methods and criteria for assessing the students (the method to verify the achievement of the expected learning outcomes):</p>	<p>W1. Has in-depth knowledge of modelling decision-making problems and methods and computer tools for solving these problems in the field of management / P_W07.</p> <p>W2. Has in-depth knowledge in the field of knowledge and methods of modelling cyber security threats / P_W08.</p> <p>U1. Can effectively make managerial decisions using appropriate methods and computer tools supporting these decisions / P_U09.</p> <p>U2. Can independently plan and realize own learning in the field of cyber security / P_U11.</p> <ul style="list-style-type: none"> • The module is passed on the basis of an examination conducted in an oral form. • A positive mark is required for passing the credit from laboratories. • Achievement of W1 and W2 effects is verified during the laboratory and credit. • The achievement of effects U1, U2 is checked during the presentation of the results of the case studies and guided discussions during laboratory classes.
<p>ECTS balance sheet (student workload)</p>	<p>Student's activity / workload in hours</p> <ol style="list-style-type: none"> 1. Participation in lectures / 16 hrs. 2. Participation in laboratories / 8 hrs. 3. Learning the topics of lectures / 32 hrs. 4. individual preparation to laboratories / 12 hrs. 5. participation in consultations / 2 hrs. 6. preparation to the assessment credit / 16 hrs. 7. participation in assessment / 2 hrs. <p>The total student's workload: 88 hrs / 3 pts. ECTS</p>

“APPROVED BY”

Dean of Faculty of
Cybernetics

Zbigniew TARAPATA,
PhD, Eng. Professor
at MUT

INFORMATION SHEET OF THE COURSE

Nazwa przedmiotu:	<i>Project management and systems engineering in cyber security</i>	<i>Zarządzanie projektami i inżynieria systemów w cyberbezpieczeństwie</i>
Code of the course:	WCYIXCNP-ZPIE	
Language of lectures:	English	
Applicable from:	2021/2022	
Form of classes number of hours/rigour, hours in total	<i>Lect. – 8/4, Lab – 8; in total: 16 hours – 1 credit ECTS</i>	
Author:	<i>Mariusz CHMIELEWSKI, PhD, Eng.</i>	
Organisational Unit in charge of the course	<i>Faculty of Cybernetics / Institute of IT Systems</i>	
Short description of the course:	<p>The module presents issues of building information and communication systems, paying attention to the key aspects of managing IT projects and including cyber security issues.</p> <p>The module discusses practical aspects of applying project management methodologies with particular emphasis on requirements engineering, software complexity estimation, cost estimation, project scheduling and implementation of supervision techniques.</p> <p>Practical examples of development and R&D projects taking into account various implementation conditions and support tools will illustrate all the issues. Toolkits will be presented together with methods for assessing the quality of IT projects in terms of quality supervision of the production and exploitation process. The subject will also cover tools used in analysis and design of IT services and systems - tools for system architecture modeling, cost estimation and project realization supervision.</p> <p>The subject will also describe techniques for managing the effective implementation of projects using agile methodologies, e.g. Scrum supported by techniques and tools for assessing the quality of teamwork, e.g. Health Check Model and soft techniques for effective management of production teams.</p> <p>Enterprise Architecture Modeling is a modern method of managing companies focused on understanding business processes and their representation in the organization but also on building, implementing services and running systems on the infrastructure.</p> <p>An important element of the presented content will be innovative technologies in the field of decision support and knowledge management systems, mobile and eHealth systems, and especially cyber security issues related to their construction and maintenance. The discussed security issues will refer to the use of mobile and wearable devices as well as indicate the dangers of processing sensory data and making inferences (artificial intelligence methods) on their basis.</p>	
Full description of the course	Lecture classes are based on the presentation of theoretical issues with concrete practical illustration (supported by tools and practical cases of	

<p>(programme content):</p>	<p>projects implementation). Issues of cyber security of mobile and wearable technologies will be illustrated by projects and experiences from their design, development and implementation. Classes will be conducted in a manner activating students, in the form of lectures with elements of workshops (practical demonstrations) and group discussions, case studies, mini-projects. Developed examples will be made available by the groups and the instructor for review and discussion, providing a basis for quality assessment of the work performed.</p> <p>Lecture topics:</p> <ol style="list-style-type: none"> 1. Terminology of software engineering and IT project management (0,5 hr.) 2. Project management methodologies Prince2, PMBok key concepts, processes, roles and artifacts - issues of risk management, change, configuration (1hr.) 3. Specificity of agile methodologies - Scrum, Nexus and applied management principles focused on teams (0,5hr.) 4. Tools to support the implementation of IT projects - disciplines and support tools (1 hr.) 5. Requirements engineering - key techniques for business and system analysis and requirements modelling for IT system (1hr.) 6. Software complexity estimation and cost estimation using Use Case Points method (0,5hr.) 7. Enterprise architecture elements - enterprise intellectual capital model - architectural perspectives, methods and notations, analytical processes and enterprise value (1hr.) 8. Elements of information systems architecture - modeling and aspects of performance evaluation (1 hr.) 9. Continuous Integration and Deployment Environments (CI&CD) - benefits of their implementation (0,5hr.) 10. Cyber security of cloud and mobile systems construction and data processing security issues (1 hr.) <p>Topics of workshops and practical implementations:</p> <ol style="list-style-type: none"> 1. Workshop: Requirements engineering and complexity assessment of the described system using selected implementation technologies (2hrs.) 2. Workshop: project execution planning according to the selected methodology and allocation of resources required for the project execution (2hrs.) 3. Workshop: developing recommendations for the IT project implementation environment supporting the selected innovative technologies and cyber security aspects. (2hrs.) 4. Workshop: qualitative assessment and review of IT project implementation and delivery environment ensuring the selected cyber security aspects. (2hrs.) <p>Workshops are conducted in the form of analyses of case studies and project tasks, some of which are carried out in a team format. Team work results/conclusions/proposals of solutions to problem situations are presented and discussed in the training group. The course assessment will consist of the development of components required in the management of IT projects, taking into account aspects of cybersecurity and correct design of continuous integration and deployment (CI&CD) environments</p>
<p>The reference books and papers:</p>	<p>Literatura podstawowa:</p> <ul style="list-style-type: none"> • U K Stationery Office, An Introduction to Prince2: Managing and Directing Successful Projects – 1.07.2009, Stationery Office Books, ISBN-13 : 978-0113311880,

	<ul style="list-style-type: none"> • Manifest programowania zwinnego, agilemanifesto.org [dostęp 2021-03-04] • Sutherland, Jeff, and J. J. Sutherland. <i>Scrum: the art of doing twice the work in half the time</i>. Currency, 2014. • Ian Sommerville, Inżynieria oprogramowania, ISBN: 9788301212599 • Sam Newman, Design, Build, Ship: Faster, Safer Software Delivery, O'Reilly Media; 1st edition (June 4, 2021), ISBN-10 : 1491984872 • Lankhorst, Enterprise Architecture at Work, ISBN-10: 3662539322 <p>Literatura uzupełniająca:</p> <ul style="list-style-type: none"> • Kruchten, Philippe. <i>The rational unified process: an introduction</i>. Addison-Wesley Professional, 2004. • Philbin, Simon P., and Donald A. Kennedy. "Diagnostic framework and health check tool for engineering and technology projects." <i>Journal of Industrial Engineering and Management (JIEM)</i> 7.5 (2014): 1145-1166. • Clemmons, Roy K. "Project estimation with use case points." <i>The Journal of Defense Software Engineering</i> 19.2 (2006): 18-22. • Lientz, Bennet, and Lee Larssen. <i>Risk management for IT projects</i>. Routledge, 2006. • Studer, Rudi, V. Richard Benjamins, and Dieter Fensel. "Knowledge engineering: Principles and methods." <i>Data & knowledge engineering</i> 25.1-2 (1998): 161-197. • Poli, Roberto, Michael Healy, and Achilles Kameas, eds. <i>Theory and applications of ontology: Computer applications</i>. New York: Springer, 2010. • David Robertson, Peter Weill, Ross W. Jeanne, David C Robertson, Architektura korporacyjna jako strategia, 2010,
<p>Learning outcomes:</p> <p>Methods and criteria for assessing the students (the method to verify the achievement of the expected learning outcomes):</p>	<p>W1. He knows basic principles and methods of IT project management / P_W11</p> <p>U1. Can apply in practice the basic principles and methods of IT project and service management / P_U12</p> <p>U2. Can independently plan and realize own learning in the field of cyber security / P_U11</p> <ul style="list-style-type: none"> • The module is passed on the basis of a credit. • A prerequisite for passing the module is obtaining a positive mark from the workshop • Achievement of W1 and U1, U2 effects is verified during the workshop and during the pass mark credit.
<p>ECTS balance sheet (student workload)</p>	<p>Student's activity / workload in hours:</p> <ol style="list-style-type: none"> 1. Participation in lectures /8 hrs. 2. Participation in workshops /8 hrs. 3. Individual studying of the lectures subjects / 8 hrs. 4. individual preparation to the laboratories / 8 hrs. 5. participation in consultations / 2 hrs. 6. preparation of credit material / 12 hrs. 7. participation in assessment credit / 2 hrs. <p>The total student's workload: 48 hours / 1 credit ECTS</p>

“APPROVED BY”

Dean of Faculty of
Cybernetics

Zbigniew TARAPATA,
PhD, Eng. Professor
at MUT

INFORMATION SHEET OF THE COURSE

Nazwa przedmiotu:	Protection of transactional and statistical databases	Ochrona transakcyjnych i statystycznych baz danych
Code of the course:	WCYIXCNP-OBDE	
Language of lectures:	English	
Applicable from:	2021/2022	
Form of classes number of hours/rigour, hours in total	Lect. – 12/4, Ex – 8; in total: 20 hours – 2 credit ECTS	
Author:	<i>Bolesław SZAFRAŃSKI, PhD, DSc, Eng.</i>	
Organisational Unit in charge of the course	<i>Faculty of Cybernetics / Institute of IT Systems</i>	
Short description of the course:	The subject allows the student to learn about the main threats and methods of data protection in databases considered against the background of architecture and contemporary applications of database technology. In particular, attention will be paid to the fundamental differences between the rules for the protection of transactional and statistical databases. Processes and mechanisms of confidentiality protection, mechanisms of data integrity protection (statistical and dynamic) and the issue of ensuring the continuity of the database system will be discussed. The importance of management decisions and the role of the database system administrator team in these processes will be emphasized. Due to the rapid increase in the importance of data analysis using the concept of "Big Data", the lectures also included the issues of security of information processes that use often incomplete, inconsistent Internet distributed network resources.	
Full description of the course (programme content):	Topics of the lectures <ul style="list-style-type: none">• Basic concepts in the field of databases, (1hr.)• Architecture and design of databases from the point of view of the security of database systems, (1hr.)• Classification of database applications: transactional and statistical databases, differences in the protection rules for transactional and statistical databases, (1hr.)• Models and mechanisms for the protection of confidentiality, integrity and availability of data in transactional databases (3hrs.)• Models and mechanisms for the protection of confidentiality, integrity and availability of data in statistical databases, (3hrs.)• Tasks of the database administrator team in ensuring database security, (2hrs.)• Directions of development of database protection methods - security of information processes using network information resources (in the Big Data environment). (1hr.) Exercise topics <ul style="list-style-type: none">• Security of databases against the background of information security, (2hrs.)• Discussion (case study) of management and practical aspects of the	

<p>The reference books and papers:</p>	<p>advantages and disadvantages of database protection methods, (2 hrs.)</p> <ul style="list-style-type: none"> • Discussion (case study) of management, organizational and technological security problems against the background of the database design process, (2hrs.) • Case study of information process security issues in the Big Data environment. (2 hrs.) <p>The basic reference books:</p> <ul style="list-style-type: none"> • Banasiński C. (red.): „Cyberbezpieczeństwo. Zarys wykładu”, Wolters Cluwer, Warszawa, 2018. • Garcia-Molina H., Ullman J. D., Widom J.: „Systemy baz danych. Kompletny podręcznik”, Helion, Gliwice, 2011, • Sullivan D.: „NoSQL – Przyjazny przewodnik”, Helion, Gliwice, 2017, • Dygaszewicz J., Szafrąński B.: „Informatyczne wsparcie produkcji statystycznej”, Wojskowa Akademia Techniczna, Warszawa, 2021, • Szafrąński B., „Bezpieczeństwo procesów decyzyjnych w środowisku niepewnych i niekompletnych danych”, C. H. Beck, Internet. Przetwarzanie danych osobowych, Warszawa, 2019. <p>The additional reference books:</p> <ul style="list-style-type: none"> • Denning D.: „Kryptografia i ochrona danych”, WN-T, Warszawa, • Szafrąński B., „Analiza danych w warunkach niepewności źródeł danych”, C. H. Beck. Internet. Analityka danych, Warszawa, 2019, • Szpor G., Gryszczyńska A., Czaplicki K.: (red.): „Ustawa o Krajowym Systemie Cyberbezpieczeństwa. Komentarz”, Wolters Kluwer, Warszawa, 2019.
<p>Learning outcomes:</p>	<p>W1. Has in-depth knowledge of the protection of transactional databases / P_W01</p> <p>W2. Knows and understands basic threats of cyber security of databases and methods to counter them / P_W05.</p> <p>W3. Knows and understands the economic, social and military determinants of threats to database cyber security / P_W10</p> <p>U1. Can practically apply solutions in the field of database security / P_U01</p> <p>U2. Can apply appropriate methods and techniques to counter basic threats to transactional databases / P_U05</p> <p>U3. Can use in practice basic technologies and tools to ensure cyber security / P_U06</p> <p>K1. Is ready to acknowledge knowledge in solving cyber security problems / P_K01.</p>
<p>Methods and criteria for assessing the students (the method to verify the achievement of the expected learning outcomes):</p>	<ul style="list-style-type: none"> • The module is passed on the basis of a credit. • Passing of the laboratory classes is a prerequisite for obtaining credit. • Achievement of the effects W1, W2, W3 is verified during the laboratories and during the pass mark credit. Effects U1, U2, U3 are verified during laboratories.
<p>ECTS balance sheet (student workload)</p>	<p>Student's activity / workload in hours:</p> <ol style="list-style-type: none"> 1. participation in lectures / 12 hrs. 2. participation in laboratories / 8 hrs. 3. individual studying of the lectures subjects / 20 hrs. 4. individual preparation to the laboratories / 20 hrs. 5. participation in consultations / 2 hrs. 6. the preparations to the examination test / 10 hrs. 7. participation in the examination / 2 hrs. <p>The total student's workload: 74 hrs / 2 credit ECTS</p>

“APPROVED BY”

Dean of Faculty of
Cybernetics

Zbigniew TARAPATA,
PhD, Eng. Professor at
MUT

INFORMATION SHEET OF THE COURSE

Name of the course:	<i>IT services management</i>	<i>Zarządzanie usługami IT</i>
Code of the course:	WCYIXCNP-ZUIE	
Language of lectures:	English	
Applicable from:	2021/2022	
Form of classes number of hours/rigour, hours in total	<i>Lect. – 14/4, Sem – 6; in total: 20 hours – 2 credits ECTS</i>	
Author:	<i>Wiesław BARCIKOWSKI, PhD, Eng.</i>	
Organisational Unit in charge of the course	<i>Faculty of Cybernetics / Institute of IT Systems</i>	
Short description of the course:	The course will introduce the student of the post-graduate studies to the basic principles and practical methods of IT service management.	
Full description of the course (programme content):	<p>Classes are conducted in a way that activates the audience, in the form of lectures and seminars..</p> <p>Lecture topics (14 hrs):</p> <ol style="list-style-type: none">1. Busines –IT relations – problems of joint functioning (1h)2. Basics of IT service management (1h)3. Standards in the field of IT service management– the ITIL Library (2h)4. Service strategy and design – principles and main processes (3 h)5. Service transition and operation – principles and main processes(3h)6. Tools supporting the management of IT services (2h)7. Implementation of IT service management systems(2h) <p>Lecture topics (6 hrs):</p> <ol style="list-style-type: none">1. SLA agreements between Busines and IT relations (3h)2. Organization of IT service management (3h) <p>The seminars are conducted in the form of discussions and small project tasks carried out in a team form.</p>	
The reference books and papers:	<p>The basic reference books and papers:</p> <ul style="list-style-type: none">• An Introductory Overview of ITIL v3, itSMF, 2007• ITIL WhitePaper. Zarządzanie usługami IT, CT Partners, 2016• Orzechowski Remigiusz, Tarasiewicz A., Kreowanie wartości poprzez efektywne zarządzanie usługami IT, e-Mentor, nr 4, Szkoła Główna Handlowa, 2008. <p>The supplementary literature:</p> <ul style="list-style-type: none">• Aligning CobiT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit, IT Governance Institute, USA, OGC, UK, 2008• Barcikowski Wiesław, Zarządzanie usługami informatycznymi – wprowadzenie, Biuletyn Wojskowej Akademii Technicznej, nr 1, 2016• PN-ISO/IEC20000: 2007 Technika informatyczna – Zarządzanie usługami. Part 1: Specifications, Part 2: Rules of conduct	

	<ul style="list-style-type: none"> • Żebrowski Artur, ISO 20000 - zarządzanie usługami IT zgodnie z zasadami sztuki, Wydawnictwo Wiedza i praktyka, 2015
Learning outcomes:	<p>W1. has a thorough knowledge of information resources management / P_W01</p> <p>W2. knows basic principles and methods of IT services management / P_W11</p> <p>U1. can practically apply solutions in the field of information resources management / P_U01</p> <p>U2. can practically apply basic principles and methods of project and IT services management / P_U12</p> <p>U3. Can independently plan and realize own learning in the field of cyber security / P_U11</p>
Methods and criteria for assessing the students (the method to verify the achievement of the expected learning outcomes):	<ul style="list-style-type: none"> • The education module shall be credited on the basis of the form of a test • The positive grade obtained at the seminar classes is required for the student to be admitted to the final course test.
ECTS balance sheet (student workload)	<p>Student's activity / workload in hours:</p> <ol style="list-style-type: none"> 1. Participation in lectures / 14 hrs. 2. Participation in workshops / 6 hrs. 3. Learning the topics of lectures / 20 hrs. 4. Individual preparation to workshops / 15 hrs. 5. Participation in consultations / 2 hrs. 6. The preparation for the assessment credit / 5 hrs. 7. Participation in the assessment test / 2 hrs. <p>The total student's workload: 64 hrs. / 2 credit. ECTS</p>

“APPROVED BY”

Dean of Faculty of
Cybernetics

Zbigniew TARAPATA,
PhD, Eng. Professor at
MUT

INFORMATION SHEET OF THE COURSE

Name of the course:	<i>The information warfare theory</i>	<i>Teoria wojny informacyjnej</i>
Code of the course:	WCYIXCNP-TWIE	
Language of lectures:	English	
Applicable from:	2021/2022	
Form of classes number of hours/rigour, hours in total	<i>Lect. – 12/x, Lab – 12; in total: 24 hours – 3 credits ECTS</i>	
Author:	<i>Col. Rafał KASPRZYK, PhD, Eng.</i>	
Organisational Unit in charge of the course	<i>Faculty of Cybernetics / Institute of IT Systems</i>	
Short description of the course:	The course allows to provide the student of postgraduate studies with the basics of knowledge about the problems related to the so-called information warfare. Students will learn: forms of activities and models of combat in cyberspace; models, methods and tools for identifying, recognizing and assessing the possibilities of information impact; models, methods and tools to counteract the information impact; the issues of manipulating people with the use of artificial intelligence; hacking artificial intelligence; OSINT basics.	
Full description of the course (programme content):	Lecture topics: <ul style="list-style-type: none">• Cyberspace, Internet, information environment, energy wars, information wars, wars of the future. (1hr)• Forms of activities in cyberspace: CYBEROPS, INFOOPS, PSYOPS. (1hr)• TTP (ang. <i>Tactics, Techniques & Procedures</i>) used to wage war in cyberspace. (1hrs)• Models of combat (operations) in cyberspace. (1hr)• Modeling and analysis of network systems. (2hrs)<ul style="list-style-type: none">○ Models, methods and tools for the identification, recognition and assessment of the information impact.○ Models, methods and tools for counteracting the information impact.○ Simulation of the propagation of information disturbances (pathologies) in the network environment (the influence of the network structure on the dynamics of propagation).• Artificial intelligence, the use of artificial intelligence in military operations, manipulating people with the use of artificial intelligence, hacking artificial intelligence. (2hrs)	

	<ul style="list-style-type: none"> • Game theory as a classic language of description of conflict and cooperation versus information warfare. (2hrs) • Concept, process and tools of Open Source Intelligence. (1hr) • Capabilities to conduct operations in cyberspace. (1hr) <p>Laboratory classes:</p> <ul style="list-style-type: none"> • The laboratories are conducted in the form of case study analyzes and small project assignments, partly carried out in a team form. The results of the team's work / conclusions / proposed solutions to problem situations are presented and discussed in the forum of the training group. (12 hrs.): <ul style="list-style-type: none"> ○ Models of combat (operations) in cyberspace (4 hrs.); ○ Modeling and analysis of network systems (4 hrs.); ○ Concept, process and tools of Open Source Intelligence (4 hrs.).
The reference books and papers:	<p>The basic reference books and papers:</p> <ul style="list-style-type: none"> • R. Brzeski, Wojna informacyjna – wojna nowej generacji, wyd. ANTYK, Warszawa 2014 r. • D. Denning, Wojna informacyjna i bezpieczeństwo informacji, Wydawnictwo Naukowo-Techniczne, 2002 r. • D. Chotikul, The Soviet Theory of Reflexive Control in Historical and Psychocultural Perspective: A Preliminary Study, Monterey, California, 1986 r. • T. Thomas, Russia's Reflexive Control Theory and the Military, Journal of Slavic Military Studies, 2004. <p>The complementary reference books and papers:</p> <ul style="list-style-type: none"> • R. Ratajczak, Nowoczesne wojny informacyjne, DIFIN, Warszawa 2016 r. • L. Sykulski, Rosyjska geopolityka a wojna informacyjna, PWN, Warszawa 2019 r. • A. Langer, Wojna hybrydowa, WarBook, 2018 r.
Learning outcomes:	<p>W1. Knows the concept of information warfare as an increasingly important form of influence on the enemy / P_W03.</p> <p>W2. Knows methods, models and tools of identifying, recognizing and assessing possibilities of information influence as well as methods, models and tools of counteracting information influence of an adversary / P_W08.</p> <p>W3. Knows basic challenges and trends related to the development of artificial intelligence in the context of information warfare / P_W06.</p> <p>U1. Can identify, recognize and analyse cases of information operations in / P_U03.</p> <p>U2. Can effectively counter (minimize the effects of) hostile information operations / P_U03.</p> <p>U3. Is able to use solutions based on artificial intelligence in information operations and countering hostile information operations / P_U03.</p>
Methods and criteria for assessing the students (the method to verify the achievement of the expected learning outcomes):	<ul style="list-style-type: none"> • The module shall be completed on the basis of a pass mark credit, conducted orally. • Successful completion of laboratory classes is a prerequisite for obtaining credit. • The achievement of the effects W1, W2 and W3 is checked during the laboratories and the pass mark credit. • The achievement of effects U1, U2, U3 is checked during the presentation of the results of the case studies and guided discussions during laboratory classes.
ECTS balance sheet	Activity / workload of the student in hours.

(student workload)	<ol style="list-style-type: none">1. Participation in lectures / 12 hours2. Participation in laboratory classes / 12 hours3. Unassisted studying topics of lectures / 20 hours4. Unassisted preparation for laboratory classes / 20 hours5. Participation in consultations / 2 hours6. Preparation for course examination / 20 hours7. Participation in course test / 2 hours <p>Total workload of the student: 88 hours – 3 credits ECTS</p>
--------------------	---

“APPROVED BY”

Dean of Faculty of
Cybernetics

Zbigniew TARAPATA,
PhD, Eng. Professor
at MUT

INFORMATION SHEET OF THE COURSE

Name of the course:	<i>National cyber security system</i>	<i>Krajowy system cyberbezpieczeństwa</i>
Code of the course:	WCYIXCNP-KSCE	
Language of lectures:	English	
Applicable from:	2021/2022	
Form of classes number of hours/rigour, hours in total	<i>Lect. – 10/4, Ex – 10; in total: 20 hours – 2 credits ECTS</i>	
Author:	<i>Krzysztof SILICKI</i>	
Organisational Unit in charge of the course	<i>National Partner / NASK</i>	
Short description of the course:	The course will introduce to the student of the post-graduate studies the architecture of the national cybersecurity system in Poland and practical aspects of cybersecurity on the national and sectorial level.	
Full description of the course (programme content):	<p>Lectures will introduce to students some selected topics of national cybersecurity system in Poland and will engage them in hands-on activities on some simple practical case studies.</p> <p>Lecture topics (10 hours):</p> <ol style="list-style-type: none">1. Structure and functioning of national cybersecurity system (KSC) – practical aspects (1 hr)2. Current cybersecurity threat landscape- especially in the context of risk for proper functioning of important services for state and economy as well as for citizens (1 hr)3. Incident notification, management and coordination on national level and EU level (1hr)4. Roles and duties of national and sectorial CSIRTs, competent authorities for cybersecurity, operators of essential services, digital service providers and other stakeholders of KSC (2 hrs)5. Strategic level of coordination: role of governmental plenipotentiary for cybersecurity, national council for cybersecurity and national cybersecurity strategy (1 hr)6. S46 - ICT system supporting functioning of the KSC (1 hr)7. National cybersecurity system in the context of strategic documents and regulations of European Union (1 hr)8. Selected topics of development of EU and national cybersecurity certification system (1 hr)9. Cybersecurity of next generation telecom networks (5G) – national and EU perspective (1 hr) <p>The hands-on exercises shall be conducted in the form of selected topics in depth analysis and case studies. Students will be divided into small 3-4 pers. groups to perform task. The results of team work/conclusions/proposals for problem-solving solutions are presented and discussed within the training group.</p>	

	<p>Topics of laboratory classes:</p> <ol style="list-style-type: none"> 1. Coordination of incidents on the national and EU level (1 hr) 2. Cybersecurity management – compliance with the law duties (1 hr) 3. Realisation of cybersecurity requirements in the organisations of different size – ENISA best practices (2 hrs) 4. Large scale incidents and crises - coordination in the EU approach (1 hr) 5. Different cases of cybersecurity incident notification and incident handling (2 hr) 6. Cooperation among stakeholders of national cybersecurity system (including cooperation with law enforcement) (1 hr) 7. Main elements of EU and national cybersecurity certification system (1 hr) 8. Threats, risks and mitigation measures in 5G networks – national and EU approach (1 hr)
The reference books and papers:	<p>The basic reference books and papers:</p> <ul style="list-style-type: none"> • The Act on national cybersecurity system from 5.07.2018 with amendments • A bill on Electronic Communication Law Prawo • Banasiński C. (red.): „Cyberbezpieczeństwo. Zarys wykładu”, Wolters Cluwer, Warszawa, 2018, • Szpor G., Gryszczyńska A., Czaplicki K.: (red.): „Ustawa o Krajowym Systemie Cyberbezpieczeństwa. Komentarz”, Wolters Kluwer, Warszawa, 2019. • ENISA Threat Landscape • ENISA: How to setup CSIRT and SOC
Learning outcomes:	<p>W1. Knows and understands basic cyber security threats and methods to counter them / P_W05.</p> <p>W2. Knows the basic challenges and development trends in cyber security / P_W06.</p> <p>U1. Can apply basic methods and techniques of risk management in cyber security /P_U05.</p> <p>U2. Is able to use in practice basic technologies and tools for ensuring cyber security / P_U07.</p> <p>U3. Is able to plan and realize own learning independently in the field of cyber security / P_U11.</p>
Methods and criteria for assessing the students (the method to verify the achievement of the expected learning outcomes):	<ul style="list-style-type: none"> • The module is passed on the basis of credit. • Passing of the laboratory classes is a prerequisite for passing the module. • The achievement of effects W1, W2 is checked during the classes and during the pass mark credit. Achievement of U1, U2, U3 effect is verified during the presentation of the results of case studies and guided discussions during classes.
ECTS balance sheet (student workload)	<p>Activity / workload of the student in hours.</p> <ol style="list-style-type: none"> 1. Participation in the lectures / 10 hours 2. Participation in exercise classes / 10 hours 3. Unassisted studying topics of lectures / 10 hours 4. Unassisted preparation for laboratory classes / 10 hours 5. Participation in consultations / 2 hours 6. Preparation for course test / 10 hours 7. Participation in course test / 1 hour <p>Total workload of the student: 53 hours – 2 credits ECTS</p>

“APPROVED BY”

Dean of Faculty of
Cybernetics

Zbigniew TARAPATA,
PhD, Eng. Professor
at MUT

INFORMATION SHEET OF THE COURSE

Name of the course:	<i>NATO policy on cyber security</i>	<i>Polityka NATO w zakresie cyberbezpieczeństwa</i>
Code of the course:	WCYIXCNP-PNCE	
Language of lectures:	English	
Applicable from:	2021/2022	
Form of classes number of hours/rigour, hours in total	<i>Lect. – 12/4, Proj – 12; in total: 24 hours – 3 credits ECTS</i>	
Author:	<i>Konrad WRONA, Dr.-Ing.</i>	
Organisational Unit in charge of the course	<i>Foreign Partner/NCIA</i>	
Short description of the course:	The course will introduce the student of the post-graduate studies to the evolution of NATO approach to cyber security, influence of changing security environment on NATO cyber security policy, and NATO initiatives concerning cyberspace.	
Full description of the course (programme content):	<p>Lectures will be organized in a hybrid form of in-person and virtual meetings, engaging students into discussions and analytical activities.</p> <p>Lecture topics:</p> <ul style="list-style-type: none">• Importance of cyberspace as the fifth domain of military operations; (2hrs)• Cyber security aspects in policy, doctrine and strategy documents of NATO; (4hrs)• Influence of evolving security environment on NATO cyber security policy; (3hrs)• NATO initiatives focused on strengthening cyber defence and cyber resilience capabilities of the Alliance. (3hrs) <p>Scope of project activities:</p> <p>Analysis of use cases and challenges related to international cyber security collaboration in context of the NATO strategy.</p>	
The reference books and papers:	<ul style="list-style-type: none">• Joanna Świątkowska (Ed.), NATO Road to Cybersecurity, The Kościuszko Institute, 2016.• Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 2nd Edition, Cambridge University Press, 2017.• Cybersecurity and Cyberdefense Exercises, Center for Security Studies (CSS), ETH Zürich, 2018.• Zestaw aktualizowanych jawnych dokumentów NATO, artykułów naukowych i analiz przypadków dostępny na platformie MS Teams WATW. Stallings and L. Brown. <i>Computer Security: Principles and Practice</i>. Pearson, 2014.	
Learning outcomes:	W1. Has knowledge of the policies, strategies and systems for ensuring cyber security in NATO / P_W09.	

	<p>W2. Knows and understands basic cyber threat intelligence models and principles of their use in cyber security threat analysis / P_W09.</p> <p>U1. Can apply knowledge of NATO cyber security policy, strategy and assurance systems for the improvement of national cyber security systems / P_U08.</p> <p>U2. Can independently plan and implement own learning in the field of cyber security / P_U11.</p>
<p>Methods and criteria for assessing the students (the method to verify the achievement of the expected learning outcomes):</p>	<p>The module is passed on the basis of the project and the examination, conducted in an oral form.</p> <ul style="list-style-type: none"> • In order to be admitted to the examination, a positive mark must be obtained from the group project. • The achievement of effects W1 and W2 is checked during the project and exam. • The achievement of effects U1, U2 is checked during the presentation of the results of the case studies and guided discussions during project classes.
<p>ECTS balance sheet (student workload)</p>	<p>Activity / workload of the student in hours.</p> <ol style="list-style-type: none"> 1. Participation in lectures / 12 hours 2. Participation in laboratory classes / 12 hours 3. Unassisted studying topics of lectures / 25 hours 4. Unassisted preparation for laboratory classes / 25 hours 5. Participation in consultations / 2 hours 6. Preparation for course test / 20 hours 7. Participation in course test / 2 hours <p>Total workload of the student: 98 hours – 3 credits ECTS</p>



Wojskowa
Akademia
Techniczna

**Uchwała
Rady Dyscypliny Naukowej
Informatyka Techniczna i Telekomunikacja
Wojskowej Akademii Technicznej
im. Jarosława Dąbrowskiego**

nr 44/RDN ITiT/2021 z dnia 16 czerwca 2021 r.

**w sprawie zaopiniowania programów podyplomowych studiów MBA
przydzielonych do dyscypliny
Informatyka Techniczna i Telekomunikacja**

Na podstawie § 25 ust. 1 pkt 13 Statutu WAT, stanowiącego załącznik do uchwały Senatu WAT nr 16/WAT/2019 z dnia 25 kwietnia 2019 r. w sprawie uchwalenia Statutu Wojskowej Akademii Technicznej im. Jarosława Dąbrowskiego (t.j. obwieszczenie Rektora WAT nr 2/WAT/2019 z dnia 9 października 2019 r.) uchwała się, co następuje:

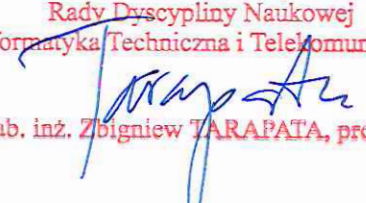
§ 1

Pozytywnie opiniuje się niżej wymienione programy studiów podyplomowych MBA obowiązujące od roku akademickiego 2021/2022:

- 1) Program studiów podyplomowych MBA *Zarządzanie Cyberbezpieczeństwem* – stanowiący załącznik nr 1 do uchwały,
- 2) Programme of postgraduate MBA studies *Cyber Security Management* – stanowiący załącznik nr 2 do uchwały.

§ 2

Uchwała wchodzi w życie z dniem podjęcia.

PRZEWODNICZĄCY
Rady Dyscypliny Naukowej
"Informatyka Techniczna i Telekomunikacja"

dr hab. inż. Zbigniew TARAPATA, prof. WAT



Wojskowa
Akademia
Techniczna

Wydział
Cybernetyki



**Opinia
Wydziałowej Rady ds. Kształcenia
Wydziału Cybernetyki Wojskowej Akademii Technicznej**

nr 31/WRdsK/2021 z dnia 15 czerwca 2021 r.

w sprawie programów podyplomowych studiów MBA

Na podstawie § 92 ust. 1 pkt. 2 *Statutu WAT, stanowiącego załącznik do uchwały Senatu WAT nr 16/WAT/2019 z dnia 25 kwietnia 2019 r. w sprawie uchwalenia Statutu Wojskowej Akademii Technicznej im. Jarosława Dąbrowskiego* (t.j. obwieszczenie Rektora WAT nr 2/WAT/2019 z dnia 9 października 2019 r.) oraz § 17 ust. 1 pkt. 2 *Regulaminu Wydziałowej Rady do spraw Kształcenia Wydziału Cybernetyki Wojskowej Akademii Technicznej im. Jarosława Dąbrowskiego* postanawia się, co następuje:

§ 1

Pozytywnie opiniuje się niżej wymienione programy studiów podyplomowych MBA obowiązujące od roku akademickiego 2021/2022:

- 1) Program studiów podyplomowych MBA *Zarządzanie Cyberbezpieczeństwem*
– stanowiący załącznik nr 1 do opinii,
- 2) Programme of postgraduate MBA studies *Cyber Security Management*
– stanowiący załącznik nr 2 do opinii.

**Zastępca przewodniczącego
Wydziałowej Rady ds. Kształcenia WCY**

dr Joanna PIASECKA