Informatyka - Studia stacjonarne II stopnia

Specjalność: Cyberbezpieczeństwo (Cybersecurity)

Program studiów zgodny z: PRK (poziom 7) oraz body of knowledge zdefiniowanym w standardach: ACM / IEEE Computer Science Curricula 2013 (CS 2013) i ACM / IEEE Computer Engineering Curricula 2016
Dziedzina: nauki inżynieryjno - techniczne
Dyscyplina: Informatyka techniczna i telekomunikacja - profil ogólnoakademicki
Nadawany tytuł zawodowy: magister inżynier

Rekrutacja:

Wymagania wynikające z rekrutacji: kandydat na te studia musi posiadac kompetencje inżynierskie (tytuł zawodowy inżyniera) oraz kwalifikacje, tj. wiedzę, umiejętności i kompetencje zdefiniowane w Uchwale Senatu PP w sprawie zatwierdzenia kierunkowych efektów uczenia się dla studiów prowadzonych na Politechnice Poznańskiej nr 42 z dnia 24 kwietnia 2017 roku dotyczące studiów I stopnia na kierunku Informatyka podane obok, które są weryfikowane w procedurze rekrutacyjnej.

Semestr 1:

Lp.	Moduł kształcenia - przedmiot	Egz	W	C	L	P		ECTS	Ob.	Podst.	Prakt.	Bad.
1	Wprowadzenie do cyberbezpieczeństwa (Introduction to Cybersecurity)	E	30		30			5	obi		Prakt.	
2	Kryptografia i podstawy kryptoanalizy (Cryptography and Basics of Cryptanalysis)	E	30	15	30			6	obi		Prakt.	Bad.
3	Innowacyjność i kreatywne myślenie (Innovation and Creative Thinking) (nauki społeczne)		30	15				3	obi		Prakt.	
4	Zaawansowane bezpieczeństwo systemów komputerowych (Advanced System Security)		15		45			6	obi		Prakt.	
5	Bezpieczeństwo funkcjonalne (Functional Safety)		30		15			4	obi		Prakt.	Bad.
6	Bezpieczeństwo sieci bezprzewodowych (Wireless Communication Security)		30		15			4	obi		Prakt.	
7	Komunikacja w języku angielskim (Communication in English) / Język polski (Polish)			30				2	obi	Podst.		

8	Podstawowe szkolenie z zakresu BHP (Basic health and safety training)		4					0		Podst.		
			169	60	135	0		30				
		Razem godz.:	364									

Semestr 2:

Lp.	Moduł kształcenia - przedmiot	Egz	W	C	L	P		ECTS	Ob.	Podst.	Prakt.	Bad.
1	Bezpieczeństwo aplikacji (Application Security)	E	15		45			5	obi		Prakt.	Bad.
2	Bezpieczeństwo sieci (Network Security)		15		45			5	obi		Prakt.	Bad.
3	Bezpieczeństwo systemów IoT (IoT Security)	E	30		30	15		6	obi		Prakt.	Bad.
4	Przedmiot obieralny 1: Bezpieczeństwo sieci definiowanych programowo (Security of Software-Defined Networks) / Ataki typu Side-channel (Side-channel Attacks)		15		15			3	obi		Prakt.	
5	Przedmiot obieralny 2: Bezpieczeństwo analizy Big Data (Security of Big Data Analytics) / Mechanizmy naruszeń i zapewnienia bezpieczeństwa w Chmurze i Centrach Danych (Mechanisms of Violations and Ensuring Security in Cloud and DC) / Bezpieczeństwo w systemach przechowywania danych (Security in Data Storage Systems)		15		30			4	obi		Prakt.	
6	Metodologia projektów badawczych (Methodology of research projects)			30				2	obi			Bad.
7	Przedmiot obieralny 3: Bezpieczeństwo przemysłowego Internetu Rzeczy (Security of Industrial IoT) / Technologia Blockchain i kryptowaluty (Blockchain Technology and Cryptocurrency)		15		15			2	obi		Prakt.	Bad.
8	Przedmiot obieralny 4: Informatyka Śledcza (Digital Forensics) / Wojna cybernetyczna (Cyber Warfare)		15					1	obi		Prakt.	
9	Pisanie prac naukowo-technicznych (Scientific & Technical Writing)			30				2		Podst.		Bad.
			120	60	180	15		30				
		Razem godz.:	375			Cały rok:		60				

Semestr 3:

Lp.	Moduł kształcenia - przedmiot	Egz	W	C	L	P		ECTS	Ob.	Podst.	Prakt.	Bad.
1	Seminarium dyplomowe (Diploma Seminar)					30		2				Bad.
2	Projekt badawczo-wdrożeniowy (Research and Implementation Project)		15			15		2	obi		Prakt.	Bad.
3	Zarządzanie bezpieczeństwem systemów IT oraz testy penetracyjne (Information Systems Security Management and Penetration Testing)		30		30	30		6	obi		Prakt.	
4	Przygotowanie pracy magisterskiej (Master's Thesis Preparation)					60		15	obi			Bad.
5	Analiza złośliwego oprogramowania (Malicious Software Analysis)		15		30			3	obi		Prakt.	
6	Przedmiot obieralny: (nauki humanistyczne): Komunikacja interpersonalna (Interpersonal Communication) / Komunikacja międzykulturowa (Intercultural Communication)		10	20				2	obi		Prakt.	
			70	20	60	135		30				
		Razem godz.:	285									
Podsumowanie wszystkich semestrów			359	140	375	150		90				
		Razem godz.:	1024									

Podsumowanie Programu Kształcenia

Liczba godzin - Podsumowanie wszystkich semestrów:	1 024
Konsultacje, egzaminy	102
Wszystkie godziny kontaktu z prowadzącym	1 126
Liczba punktów ECTS:	90
Punkty ECTS modułów obieralnych:	86
Wymagana liczba punktów ECTS modułów obieralnych 30% z 90	27

Łączny wymiar zajęć ćwiczeniowych, laboratoryjnych i projektowych	665
Liczba punktów ECTS z zajęć o charakterze praktycznym związanych ze zdobywaniem przez studentów umiejętności praktycznych właściwych dla zakresu działalności zawodowej informatyka	67
Suma punktów ECTS zajęć służących zdobywaniu pogłębionej wiedzy, umiejętności prowadzenia badań naukowych oraz kompetencji społecznych niezbędnych w działalności badawczej	51
% punktów ECTS zajęć służących zdobywaniu pogłębionej wiedzy, umiejętności prowadzenia badań naukowych oraz kompetencji społecznych niezbędnych w działalności badawczej	56,67
Liczba punktów ECTS z zajęć z zakresu nauk podstawowych dla kierunku Informatyka	4

Stosowane metody weryfikacji efektów uczenia się - szczegółowy opis metod weryfikacji (sposobów sprawdzenia czy zamierzone efekty uczenia się zostały osiągnięte) dla poszczególnych przedmiotów znajduje się na kartach ECTS - do zaliczenia danego przedmiotu, konieczne jest osiągnięcie wszystkich zakładanych efektów uczenia się.

Ocena formująca (inaczej, formatywna), tj .ocena wspomagajaca proces uczenia się:

a) w zakresie wykładów:

• na podstawie odpowiedzi na pytania dotyczące materiału omówionego na poprzednich wykładach,

b) w zakresie laboratoriów / ćwiczeń:

• na podstawie oceny bieżącego postępu realizacji zadań,

Ocena podsumowująca (inaczej sumatywna), tj. ocens podsumowująca stopień osiągania przez studenta zakładanych efektów kształcenia:

a) w zakresie wykładów weryfikowanie założonych efektów uczenia się realizowane jest przez:

• ocenę wiedzy i umiejętności wykazanych na egzaminie pisemnym o charakterze problemowym (w przypadku niektórych przedmiotów student może ko
wyboru,

• omówienie wyników egzaminu,

b) w zakresie laboratoriów / ćwiczeń weryfikowanie założonych efektów uczenia się realizowane jest przez:

• ocenę przygotowania studenta do poszczególnych sesji zajęć laboratoryjnych (sprawdzian „wejściowy") oraz ocenę umiejętności związanych z realiza

• ocenianie ciągłe, na każdych zajęciach (odpowiedzi ustne) – premiowanie przyrostu umiejętności posługiwania się poznanymi zasadami i metodami,

• ocenę sprawozdania przygotowywanego częściowo w trakcie zajęć, a częściowo po ich zakończeniu; ocena ta obejmuje także umiejętność pracy w ze

• ocenę wiedzy i umiejętności związanych z realizacją zadań projektowych / laboratoryjnych poprzez 2 kolokwia w semestrze,

• ocenę i „obronę" przez studenta sprawozdania z realizacji projektu,

Uzyskiwanie punktów dodatkowych za aktywność podczas zajęć, a szczególnie za:

• omówienia dodatkowych aspektów zagadnienia,

• efektywność zastosowania zdobytej wiedzy podczas rozwiązywania zadanego problemu,

• umiejętność współpracy w ramach zespołu praktycznie realizującego zadanie szczegółowe w laboratorium,

• uwagi związane z udoskonaleniem materiałów dydaktycznych,

• wskazywanie trudności percepcyjnych studentów umożliwiające bieżące doskonalenia procesu dydaktycznego.

i innych wzorcach międzynarodowych

Polska Rama Kwalifikacji		
Wiedza (efekty z I stopnia studiów)	**Umiejętnosci (efekty z I stopnia studiów)**	**Kompetencje (efekty z I stopnia studiów)**
K1st_W1 - 8	K1st_U2 - 14	

Polska Rama Kwalifikacji		
Wiedza	**Umiejętnosci**	**Kompetencje**
K2st_W2, K2st_W3, K2st_W4, K2st_W5, K2st_W9	K2st_U1, K2st_U3, K2st_U6, K2st_U8, K2st_U15, K2st_U16	K2st_K1, K2st_K2, K2st_K4
K2st_W2, K2st_W3, K2st_W4, K2st_W6	K2st_U1, K2st_U3, K2st_U4, K2st_U5, K2st_U7, K2st_U11, K2st_U16	K2st_K1, K2st_K2, K2st_K3
K2st_W8, K2st_W9	K2st_U5, K2st_U16	K2st_K3
K2st_W1, K2st_W3, K2st_W4, K2st_W5, K2st_W6	K2st_U1, K2st_U4, K2st_U5, K2st_U6 , K2st_U8, K2st_U9, K2st_U10, K2st_U15	K2st_K1, K2st_K2
K2st_W2, K2st_W3, K2st_W5, K2st_W6	K2st_U1, K2st_U3, K2st_U4, K2st_U8, K2st_U15, K2st_U16	K2st_K1, K2st_K2, K2st_K4
K2st_W2, K2st_W3, K2st_W5, K2st_W6	K2st_U1, K2st_U3, K2st_U4, K2st_U8, K2st_U15, K2st_U16	K2st_K1, K2st_K2,
K2st_W3	K2st_U1, K2st_U12, K2st_U13, K2st_U14	K2st_K3

	K2st_U5	

Polska Rama Kwalifikacji		
Wiedza	**Umiejętnosci**	**Kompetencje**
K2st_W1, K2st_W2, K2st_W3, K2st_W4, K2st_W5	K2st_U1, K2st_U2, K2st_U3, K2st_U4, K2st_U5, K2st_U6	K2st_K1, K2st_K2, K2st_K4
K2st_W3, K2st_W4, K2st_W6	K2st_U1, U2st_U3, K2st_U8, K2st_U9, K2st_U11, K2st_U15, K2st_U16	K2st_K1, K2st_K2, K2st_K4
	K2st_U7	
K2st_W1, K2st_W3, K2st_W4, K2st_W5	K2st_U1, K2st_U3, K2st_U5, K2st_U8, K2st_U12, K2st_U15, K2st_U16	K2st_K1, K2st_K2
K2st_W1 K2st_W3, K2st_W4	K2st_U1, U2st_U2, U2st_U3, K2st_U5, K2st_U9, K2st_U11, K2st_U15, K2st_U16	K2st_K1, K2st_K2, K2st_K4
K2st_W2, K2st_W4, K2st_W6, K2st_W7	K2st_U1, K2st_U3, K2st_U4, K2st_U6, K2st_U10, K2st_12, K2st_13, K2st_U16	K2st_K1, K2st_K2, K2st_K3, K2st_K4
K2st_W1, K2st_W4, K2st_W6	K2st_U1, K2st_U6, k2st_U8, k2st_U12	K2st_K1, K2st_K2, K2st_K4
K2st_W1, K2st_W2, K2st_W3, K2st_W4, K2st_W6	K2st_U1, U2st_U6, K2st_U8, K2st_U9, K2st_U12, K2st_U16	K2st_K1, K2st_K2, K2st_K3, K2st_K4
	K2st_U1, K2st_U12, K2st_U13, K2st_U14	K2st_K3

Polska Rama Kwalifikacji		
Wiedza	**Umiejętnosci**	**Kompetencje**
K2st_W4, K2st_W6, K2st_W7	K2st_U1, K2st_U2, K2st_U12, K2st_U13, K2st_U16	K2st_K1, K2st_K2, K2st_K3, K2st_K4
K2st_W1, K2st_W4, K2st_W6, K2st_W8, K2st_W9	K2st_U2, K2st_U4, K2st_U5, K2st_U6, K2st_U8, K2st_U9, K2st_U10, K2st_U11, K2st_U12, K2st_U13, K2st_U15	K2st_K2, K2st_K3, K2st_K4
K2st_W1, K2st_W2, K2st_W4, K2st_W8, K2st_W9	K2st_U5, K2st_U6, K2st_U8, K2st_U9, K2st_U10, K2st_U11, K2st_U13, K2st_U15, K2st_U16	K2st_K1, K2st_K2, K2st_K3, K2st_K4
K2st_W1, K2st_W2, K2st_W3, K2st_W4, K2st_W5, K2st_W6	K2st_U1, K2st_U2, K2st_U3, K2st_U4, K2st_U5, K2st_U6, K2st_U8, K2st_U9, K2st_U10, K2st_U11, K2st_U13, K2st_U16	K2st_K1, K2st_K2, K2st_K3, K2st_K4
K2st_W1 K2st_W4, K2st_W5	K2st_U1, K2st_U3, K2st_U5, K2st_U6	K2st_K1, K2st_K2, K2st_K4
	K2st_U2, K2st_U15	K2st_K4

rzystać z dowolnych materiałów dydaktycznych) / w formie testu wielokrotnego

cją ćwiczeń laboratoryjnych,

spole,

Odniesienie do kierunkowych efektów uczenia się dla programu studiów - Informatyka

Efekt uczenia się :	K2st_W1	K2st_W2	K2st_W3	K2st_W4	K2st_W5	K2st_W6	K2st_W7	K2st_W8	K2st_W9
Semestr 1:									
Moduł kształcenia - przedmiot									
Wprowadzenie do cyberbezpieczeństwa (Introduction to Cybersecurity)	-	+	+	+	+	-	-	-	+
Kryptografia i podstawy kryptoanalizy (Cryptography and Basics of Cryptanalysis)	-	+	+	+	-	+	-	-	-
Innowacyjność i kreatywne myślenie (Innovation and Creative Thinking) (nauki społeczne)	-	-	-	-	-	-	-	+	+
Zaawansowane bezpieczeństwo systemów komputerowych (Advanced System Security)	+	-	+	+	+	+	-	-	-
Bezpieczeństwo funkcjonalne (Functional Safety)	-	+	+	-	+	+	-	-	-
Bezpieczeństwo sieci bezprzewodowych (Wireless Communication Security)	-	+	+	-	+	+	-	-	-
Komunikacja w języku angielskim (Communication in English) / Język polski (Polish)	-	+	+	-	+	+	-	-	-
Podstawowe szkolenie z zakresu BHP (Basic health and safety training)	-	-	-	-	-	-	-	-	-
Semestr 2:									
Moduł kształcenia - przedmiot									
Bezpieczeństwo aplikacji (Application Security)	+	+	+	+	+	-	-	-	-
Bezpieczeństwo sieci (Network Security)	-	-	+	+	-	+	-	-	-
Bezpieczeństwo systemów IoT (IoT Security)	-	-	-	-	-	-	-	-	-
Przedmiot obieralny 1: Bezpieczeństwo sieci definiowanych programowo (Security of Software-Defined Networks) / Ataki typu Side-channel (Side-channel Attacks)	+	-	+	+	+	-	-	-	-
Przedmiot obieralny 2: Bezpieczeństwo analizy Big Data (Security of Big Data Analytics) / Mechanizmy naruszeń i zapewnienia bezpieczeństwa w Chmurze i Centrach Danych (Mechanisms of Violations and Ensuring Security in Cloud and DC) / Bezpieczeństwo w systemach przechowywania danych (Security in Data Storage Systems)	+	-	+	+	-	-	-	-	-
Metodologia projektów badawczych (Methodology of research projects)	-	+	-	+	-	+	+	-	-
Przedmiot obieralny 3: Bezpieczeństwo przemysłowego Internetu Rzeczy (Security of Industrial IoT) / Technologia Blockchain i kryptowaluty (Blockchain Technology and Cryptocurrency)	+	-	-	+	-	+	-	-	-
Przedmiot obieralny 4: Informatyka Śledcza (Digital Forensics) / Wojna cybernetyczna (Cyber Warfare)	+	+	+	+	-	+	-	-	-
Pisanie prac naukowo-technicznych (Scientific & Technical Writing)	-	-	-	-	-	-	-	-	-
Semestr 3:									
Moduł kształcenia - przedmiot									
Seminarium dyplomowe (Diploma Seminar)	-	-	-	+	-	+	+	-	-
Projekt badawczo-wdrożeniowy (Research and Implementation Project)	+	-	-	+	-	+	-	+	+
Zarządzanie bezpieczeństwem systemów IT oraz testy penetracyjne (Information Systems Security Management and Penetration Testing)	+	+	-	+	-	-	-	+	+
Przygotowanie pracy magisterskiej (Master's Thesis Preparation)	+	+	+	+	+	+	-	-	-
Analiza złośliwego oprogramowania (Malicious Software Analysis)	+	-	-	+	+	-	-	-	-
Przedmiot obieralny: (nauki humanistyczne): Komunikacja interpersonalna (Interpersonal Communication) / Komunikacja międzykulturowa (Intercultural Communication)	-	-	-	-	-	-	-	-	-
	10	10	12	15	9	12	2	3	4

Efekt uczenia się :	K2st_U1	K2st_U2	K2st_U3	K2st_U4	K2st_U5	K2st_U6	K2st_U7	K2st_U8	K2st_U9	K2st_U10	K2st_U11	K2st_U12	K2st_U13	K2st_U14	K2st_U15	K2st_U16
Semestr 1:																
Moduł kształcenia - przedmiot																
Wprowadzenie do cyberbezpieczeństwa (Introduction to Cybersecurity)	+	-	+	-	-	+	-	+	-	-	-	-	-	-	+	+
Kryptografia i podstawy kryptoanalizy (Cryptography and Basics of Cryptanalysis)	+	-	+	+	+	-	+	-	-	-	+	-	-	-	-	+
Innowacyjność i kreatywne myślenie (Innovation and Creative Thinking) (nauki społeczne)	-	-	-	-	+	-	-	-	-	-	-	-	-	-	-	+
Zaawansowane bezpieczeństwo systemów komputerowych (Advanced System Security)	+	-	-	+	+	+	-	+	+	+	-	-	-	-	+	-
Bezpieczeństwo funkcjonalne (Functional Safety)	+	-	+	+	-	-	-	+	-	-	-	-	-	-	+	+
Bezpieczeństwo sieci bezprzewodowych (Wireless Communication Security)	+	-	+	+	-	-	-	+	-	-	-	-	-	-	+	+
Komunikacja w języku angielskim (Communication in English) / Język polski (Polish)	+	-	-	-	-	-	-	-	-	-	-	+	+	+	-	-
Podstawowe szkolenie z zakresu BHP (Basic health and safety training)	-	-	-	-	+	-	-	-	-	-	-	-	-	-	-	-
Semestr 2:																
Moduł kształcenia - przedmiot																
Bezpieczeństwo aplikacji (Application Security)	+	+	+	+	+	+	-	-	-	-	-	-	-	-	-	-
Bezpieczeństwo sieci (Network Security)	+	-	-	-	-	-	-	+	+	-	+	-	-	-	+	+
Bezpieczeństwo systemów IoT (IoT Security)	-	-	-	-	-	-	+	-	-	-	-	-	-	-	-	-
Przedmiot obieralny 1: Bezpieczeństwo sieci definiowanych programowo (Security of Software-Defined Networks) / Ataki typu Side-channel (Side-channel Attacks)	+	-	+	-	+	-	-	+	-	-	-	+	-	-	+	+
Przedmiot obieralny 2: Bezpieczeństwo analizy Big Data (Security of Big Data Analytics) / Mechanizmy naruszeń i zapewnienia bezpieczeństwa w Chmurze i Centrach Danych (Mechanisms of Violations and Ensuring Security in Cloud and DC) / Bezpieczeństwo w systemach przechowywania danych (Security in Data Storage Systems)	+	-	-	-	+	-	-	-	+	-	+	-	-	-	+	+
Metodologia projektów badawczych (Methodology of research projects)	+	-	+	+	-	+	-	-	-	+	-	-	-	-	-	+
Przedmiot obieralny 3: Bezpieczeństwo przemysłowego Internetu Rzeczy (Security of Industrial IoT) / Technologia Blockchain i kryptowaluty (Blockchain Technology and Cryptocurrency)	+	-	-	-	-	+	-	-	-	-	-	-	-	-	-	-
Przedmiot obieralny 4: Informatyka Śledcza (Digital Forensics) / Wojna cybernetyczna (Cyber Warfare)	+	-	-	-	-	-	-	+	+	-	-	+	-	-	-	+
Pisanie prac naukowo-technicznych (Scientific & Technical Writing)	+	-	-	-	-	-	-	-	-	-	-	+	+	+	-	-
Semestr 3:																
Moduł kształcenia - przedmiot																
Seminarium dyplomowe (Diploma Seminar)	+	+	-	-	-	-	-	-	-	-	-	+	+	-	-	+
Projekt badawczo-wdrożeniowy (Research and Implementation Project)	-	+	-	+	+	+	-	+	+	+	+	+	+	-	+	-
Zarządzanie bezpieczeństwem systemów IT oraz testy penetracyjne (Information Systems Security Management and Penetration Testing)	-	-	-	-	+	+	-	+	+	+	+	-	+	-	+	+
Przygotowanie pracy magisterskiej (Master's Thesis Preparation)	+	+	+	+	+	+	-	+	+	+	+	-	+	-	-	+
Analiza złośliwego oprogramowania (Malicious Software Analysis)	+	-	+	-	+	+	-	-	-	-	-	-	-	-	-	-
Przedmiot obieralny: (nauki humanistyczne): Komunikacja interpersonalna (Interpersonal Communication) / Komunikacja międzykulturowa (Intercultural Communication)	-	+	-	-	-	-	-	-	-	-	-	-	-	-	+	-
	17	5	9	8	11	9	2	10	7	5	6	6	6	2	10	13

Efekt uczenia się :	K2st_K1	K2st_K2	K2st_K3	K2st_K4
Semestr 1:				
Moduł kształcenia - przedmiot				
Wprowadzenie do cyberbezpieczeństwa (Introduction to Cybersecurity)	+	+	-	+
Kryptografia i podstawy kryptoanalizy (Cryptography and Basics of Cryptanalysis)	+	+	+	-
Innowacyjność i kreatywne myślenie (Innovation and Creative Thinking) (nauki społeczne)	-	-	+	-
Zaawansowane bezpieczeństwo systemów komputerowych (Advanced System Security)	+	+	-	-
Bezpieczeństwo funkcjonalne (Functional Safety)	+	+	-	+
Bezpieczeństwo sieci bezprzewodowych (Wireless Communication Security)	+	+	-	-
Komunikacja w języku angielskim (Communication in English) / Język polski (Polish)	-	-	+	-
Podstawowe szkolenie z zakresu BHP (Basic health and safety training)	-	-	-	-
Semestr 2:				
Moduł kształcenia - przedmiot				
Bezpieczeństwo aplikacji (Application Security)	+	+	-	+
Bezpieczeństwo sieci (Network Security)	+	+	-	+
Bezpieczeństwo systemów IoT (IoT Security)	-	-	-	-
Przedmiot obieralny 1: Bezpieczeństwo sieci definiowanych programowo (Security of Software-Defined Networks) / Ataki typu Side-channel (Side-channel Attacks)	+	+	-	-
Przedmiot obieralny 2: Bezpieczeństwo analizy Big Data (Security of Big Data Analytics) / Mechanizmy naruszeń i zapewnienia bezpieczeństwa w Chmurze i Centrach Danych (Mechanisms of Violations and Ensuring Security in Cloud and DC) / Bezpieczeństwo w systemach przechowywania danych (Security in Data Storage Systems)	+	+	-	+
Metodologia projektów badawczych (Methodology of research projects)	+	+	+	+
Przedmiot obieralny 3: Bezpieczeństwo przemysłowego Internetu Rzeczy (Security of Industrial IoT) / Technologia Blockchain i kryptowaluty (Blockchain Technology and Cryptocurrency)	+	+	-	+
Przedmiot obieralny 4: Informatyka Śledcza (Digital Forensics) / Wojna cybernetyczna (Cyber Warfare)	+	+	+	+
Pisanie prac naukowo-technicznych (Scientific & Technical Writing)	-	-	+	-
Semestr 3:				
Moduł kształcenia - przedmiot				
Seminarium dyplomowe (Diploma Seminar)	+	+	+	+
Projekt badawczo-wdrożeniowy (Research and Implementation Project)	-	+	+	+
Zarządzanie bezpieczeństwem systemów IT oraz testy penetracyjne (Information Systems Security Management and Penetration Testing)	+	+	+	+
Przygotowanie pracy magisterskiej (Master's Thesis Preparation)	+	+	+	+
Analiza złośliwego oprogramowania (Malicious Software Analysis)	+	+	-	+
Przedmiot obieralny: (nauki humanistyczne): Komunikacja interpersonalna (Interpersonal Communication) / Komunikacja międzykulturowa (Intercultural Communication)	-	-	-	+
	16	17	10	14

Wiedza		
Sym.	**Kierunkowe efekty uczenia się z zakresu wiedzy prowadzące do uzyskania kompetencji poziomu 7 PRK**	
K2st_W1	ma **zaawansowaną i pogłębioną wiedzę** z zakresu szeroko rozumianych systemów informatycznych, podstaw teoretycznych ich budowania oraz metod, narzędzi i środowisk programistycznych wykorzystywanych do ich implementacji	B
K2st_W2	ma **uporządkowaną i podbudowaną teoretycznie wiedzę ogólną** związaną z kluczowymi zagadnieniami z zakresu informatyki	B
K2st_W3	ma **zaawansowaną wiedzę szczegółową** dotyczącą wybranych zagadnień z zakresu informatyki	B
K2st_W4	ma wiedzę o trendach rozwojowych i najistotniejszych nowych osiągnięciach informatyki i innych, wybranych, pokrewnych dyscyplin naukowych	B
K2st_W5	ma **zaawansowaną i szczegółową** wiedzę o procesach zachodzących w cyklu życia systemów informatycznych sprzętowych lub programowych	B
K2st_W6	zna zaawansowane metody, techniki i narzędzia stosowane przy rozwiązywaniu złożonych zadań inżynierskich i prowadzeniu prac badawczych w wybranym obszarze informatyki	B
K2st_W7	ma wiedzę nt. kodeksów etycznych związanych z pracą naukowo-badawczą prowadzoną w zakresie informatyki	B
K2st_W8	zna ekonomiczne, prawne i inne uwarunkowania działalności firm IT	
K2st_W9	ma podstawową wiedzę dotyczącą zarządzania / prowadzenia działalności gospodarczej oraz indywidualnej przedsiębiorczości	

Legenda:

Żółtawe tło w skrajnej prawej kolumnie (H) z literą "B": Wiedza o charakterze pogłębionym, która może być wykorzystywane w prowadzeniu badań naukowych z zakresu informatyki

English version
has **advanced and in-depth knowledge** of widely understood information systems, theoretical foundations of their construction and methods, tools and programming environments used to implement them
has a **structured and theoretically founded general knowledge** related to key issues in the field of computer science
has **advanced detailed knowledge** regarding selected IT issues
has knowledge about development trends and the most important cutting edge achievements in computer science and other selected and related scientific disciplines
has **advanced and detailed** knowledge of the processes occurring in the life cycle of hardware or software information systems
knows advanced methods, techniques and tools used to solve complex engineering tasks and conduct research in a selected area of computer science
has knowledge about ethical codes related to scientific research conducted in the field of computer science
knows the economic, legal and other determinants of the activities of IT companies
has basic knowledge of management / running a business and individual entrepreneurship

Umiejętności	
Sym.	**Kierunkowe efekty uczenia się z zakresu umiejętności prowadzące do uzyskania kompetencji poziomu 7 PRK**
K2st_U1	potrafi pozyskiwać informacje z literatury, baz danych oraz innych źródeł (w języku polskim i angielskim), integrować je, dokonywać ich interpretacji i krytycznej oceny, wyciągać wnioski oraz formułować i wyczerpująco uzasadniać opinie
K2st_U2	potrafi posługiwać się technikami informacyjno-komunikacyjnymi wykorzystywanymi przy realizacji przedsięwzięć informatycznych
K2st_U3	potrafi planować i przeprowadzać eksperymenty, w tym pomiary i symulacje komputerowe, interpretować uzyskane wyniki i wyciągać wnioski oraz formułować i weryfikować hipotezy związane ze złożonymi problemami inzynierskimi i prostymi problemami badawczymi
K2st_U4	potrafi wykorzystać do formułowania i rozwiązywania zadań inżynierskich i prostych problemów badawczych metody analityczne, symulacyjne oraz eksperymentalne
K2st_U5	potrafi — przy formułowaniu i rozwiązywaniu zadań inżynierskich — integrować wiedzę z różnych obszarów informatyki (a w razie potrzeby także wiedzę z innych dyscyplin naukowych) oraz zastosować podejście systemowe, uwzględniające także aspekty pozatechniczne
K2st_U6	potrafi ocenić przydatność i możliwość wykorzystania nowych osiągnięć (metod i narzędzi) oraz nowych produktów informatycznych
K2st_U7	potrafi poprawnie użyć wybraną metodę szacowania pracochłonności wytwarzania oprogramowania
K2st_U8	potrafi dokonać krytycznej analizy istniejących rozwiązań technicznych oraz zaproponować ich ulepszenia (usprawnienia)
K2st_U9	potrafi ocenić przydatność metod i narzędzi służących do rozwiązania zadania inżynierskiego, polegającego na budowie lub ocenie systemu informatycznego lub jego składowych, w tym dostrzec ograniczenia tych metod i narzędzi;
K2st_U10	potrafi - stosując m.in. koncepcyjnie nowe metody - rozwiązywać złożone zadania informatyczne, w tym zadania nietypowe oraz zadania zawierające komponent badawczy
K2st_U11	potrafi — zgodnie z zadaną specyfikacją, uwzględniającą aspekty pozatechniczne — zaprojektować złożone urządzenie, system informatyczny lub proces oraz zrealizować ten projekt — co najmniej w części — używając właściwych metod, technik i narzędzi, w tym przystosowując do tego celu istniejące lub opracowując nowe narzędzia
K2st_U12	potrafi porozumiewać się w języku polskim i angielskim przy użyciu różnych technik w środowisku zawodowym oraz w innych środowiskach, także z wykorzystaniem narzędzi informatycznych
K2st_U13	potrafi przygotować i przedstawić opracowanie naukowe w języku polskim i angielskim, przedstawiające wyniki badań naukowych lub przentację ustną dotyczącą szczegółowych zagadnień z zakresu informatyki
K2st_U14	ma umiejętności językowe w zakresie języka angielskiego, zgodne z wymaganiami określonymi dla poziomu B2+ Europejskiego Systemu Opisu Kształcenia Językowego
K2st_U15	potrafi współdziałać w zespole, przyjmując w nim różne role
K2st_U16	potrafi określić kierunki dalszego uczenia się i zrealizować proces samokształcenia, w tym innych osób

Legenda:

Żółtawe tło w skrajnej prawej kolumnie (H) z literą "B": Umiejętności, które mogą być wykorzystywane w prowadzeniu badań naukowych z zakresu informatyki

	English version
B	is able to obtain information from literature, databases and other sources (both in Polish and English), integrate them, interpret and critically evaluate them, draw conclusions and formulate and fully justify opinions
B	is able to use information and communication techniques used in the implementation of IT projects
B	is able to plan and carry out experiments, including computer measurements and simulations, interpret the obtained results and draw conclusions and formulate and verify hypotheses related to complex engineering problems and simple research problems
B	can use analytical, simulation and experimental methods to formulate and solve engineering problems and simple research problems
B	can - when formulating and solving engineering tasks - integrate knowledge from different areas of computer science (and if necessary also knowledge from other scientific disciplines) and apply a systemic approach, also taking into account non-technical aspects
B	is able to assess the suitability and the possibility of using new achievements (methods and tools) and new IT products
	can correctly use the chosen method of estimating the labor consumption of software development
	can carry out a critical analysis of existing technical solutions and propose their improvements (streamlines)
	is able to assess the usefulness of methods and tools for solving an engineering task, consisting in the construction or evaluation of an IT system or its components, including the limitations of these methods and tools;
B	is able - using among others conceptually new methods - to solve complex IT tasks, including atypical tasks and tasks containing a research component
	is able - in accordance with a given specification, taking into account non-technical aspects - to design a complex device, IT system or process and implement this project - at least in part - using appropriate methods, techniques and tools, including adapting to this purpose existing tools or developing new ones
B	can communicate both in Polish and English using different techniques in a professional environment and in other environments, also using IT tools
B	is able to prepare and present a scientific study in Polish and English, presenting the results of scientific research or oral presentation on specific issues in the field of computer science
	has English language skills in accordance with the requirements set for the B2 level of the Common European Framework of Reference for Languages
B	is able to interact in a team, taking various roles in it
B	can determine the directions of further learning and implement the process of self-education, including other people

Kompetencje społeczne		
Sym.	Kierunkowe efekty uczenia się prowadzące do uzyskania kompetencji poziomu 7 PRK	
K2st_K1	rozumie, że w informatyce wiedza i umiejętności bardzo szybko stają się przestarzałe	B
K2st_K2	rozumie znaczenie wykorzystywania najnowszej wiedzy z zakresu informatyki w rozwiązywaniu problemów badawczych i praktycznych	B
K2st_K3	rozumie znaczenie działalności popularyzatorskiej dotyczącej najnowszych osiągnięć z zakresu informatyki	B
K2st_K4	ma świadomość potrzeby rozwijania dorobku zawodowego oraz przestrzegania zasad etyki zawodowej	B

Legenda:

Żółtawe tło w skrajnej prawej kolumnie (H) z literą "B": Kompetencje, które mogą być wykorzystywane w prowadzeniu badań naukowych z zakresu informatyki

English version
understands that in the field of IT the knowledge and skills quickly become obsolete
understands the importance of using the latest knowledge in the field of computer science in solving research and practical problems
understands the importance of popularization activities concerning the latest achievements in the field of computer science
is aware of the need to develop professional achievements and comply with the rules of professional ethics

Dojrzałość zajęć - klasy przedmiotów

	Formalnie poprawny	Obserwo-walny	Powtarzal ny	Miejsce prezentacji materiałów dydaktycznych (adres URL)	Bezpiecz ny
Semestr 1:					
Moduł kształcenia - przedmiot					
Wprowadzenie do cyberbezpieczeństwa (Introduction to Cybersecurity)	x		x		x
Kryptografia i podstawy kryptoanalizy (Cryptography and Basics of Cryptanalysis)	x		x		x
Innowacyjność i kreatywne myślenie (Innovation and Creative Thinking) (nauki społeczne)	x		x		
Zaawansowane bezpieczeństwo systemów komputerowych (Advanced System Security)	x		x		x
Bezpieczeństwo funkcjonalne (Functional Safety)	x		x		
Bezpieczeństwo sieci bezprzewodowych (Wireless Communication Security)	x		x		x
Komunikacja w języku angielskim (Communication in English) / Język polski (Polish)	x		x		x
Podstawowe szkolenie z zakresu BHP (Basic health and safety training)	x				x
Semestr 2:					
Moduł kształcenia - przedmiot					
Bezpieczeństwo aplikacji (Application Security)	x		x		x
Bezpieczeństwo sieci (Network Security)	x		x		x
Bezpieczeństwo systemów IoT (IoT Security)	x		x		x
Przedmiot obieralny 1: Bezpieczeństwo sieci definiowanych programowo (Security of Software-Defined Networks) / Ataki typu Side-channel (Side-channel Attacks)	x		x		x
Przedmiot obieralny 2: Bezpieczeństwo analizy Big Data (Security of Big Data Analytics) / Mechanizmy naruszeń i zapewnienia bezpieczeństwa w Chmurze i Centrach Danych (Mechanisms of Violations and Ensuring Security in Cloud and DC) / Bezpieczeństwo w systemach przechowywania danych (Security in Data Storage Systems)	x				x
Metodologia projektów badawczych (Methodology of research projects)	x		x		x
Przedmiot obieralny 3: Bezpieczeństwo przemysłowego Internetu Rzeczy (Security of Industrial IoT) / Technologia Blockchain i kryptowaluty (Blockchain Technology and Cryptocurrency)	x		x		x
Przedmiot obieralny 4: Informatyka Śledcza (Digital Forensics) / Wojna cybernetyczna (Cyber Warfare)	x		x		
Pisanie prac naukowo-technicznych (Scientific & Technical Writing)	x		x		x
Semestr 3:					
Moduł kształcenia - przedmiot					
Seminarium dyplomowe (Diploma Seminar)	x				x
Projekt badawczo-wdrożeniowy (Research and Implementation Project)	x				x
Zarządzanie bezpieczeństwem systemów IT oraz testy penetracyjne (Information Systems Security Management and Penetration Testing)	x		x		x
Przygotowanie pracy magisterskiej (Master's Thesis Preparation)	x		x		
Analiza złośliwego oprogramowania (Malicious Software Analysis)	x		x		
Przedmiot obieralny: (nauki humanistyczne): Komunikacja interpersonalna (Interpersonal Communication) / Komunikacja międzykulturowa (Intercultural Communication)	x		x		

Liczba przedmiotów	23
Liczba przedmiotów formalnie poprawnych	23
% przedmiotów formalnie poprawnych	100,00%
Liczba przedmiotów obserwowalnych	0
% przedmiotów obserwowalnych	0,00%
Liczba przedmiotów powtarzalnych	19
% przedmiotów powtarzalnych	82,61%
Liczba przedmiotów bezpiecznych	17
% przedmiotów bezpiecznych	73,91%

Formalnie poprawny. Moduł posiada kartę ECTS (sylabus) i spełnia wymagania nałożone przez WSZJK.

Obserwowalny. Ponad 1/3 zajęć prowadzonych w ramach modułu podlega samoocenie z wykorzystaniem ankiety.

Powtarzalny. Wszystkie formy zajęć składających się na dany moduł są prowadzone w oparciu o materiały udostępniane studentom w formie papierowej lub elektronicznej, takie jak slajdy wykładowe, zadania programistyczne, opisy ćwiczeń laboratoryjnych.

Bezpieczny. Wszystkie zajęcia prowadzone w ramach modułu mają przypisane zastępczych prowadzących, którzy w razie choroby lub innego zdarzenia losowego są w stanie poprowadzić dane zajęcia, dzięki czemu unika się przekładania lub odwoływania zajęć.

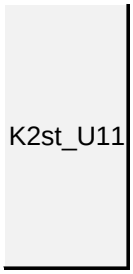
EFEKTY UCZENIA SIĘ PROWADZĄCE DO UZYSKANIA KOMPETENCJI INŻYNIERSKICH

Efekt uczenia się :	Wiedza	Umiejętnosci	Kod składnika opisu - poziom 7 PRK
Semestr 1:			
Wprowadzenie do cyberbezpieczeństwa (Introduction to Cybersecurity)	K2st_W5, K2st_W9,	K2st_U3, K2st_U6, K2st_U8,	P7S_WG, P7S_UW
Kryptografia i podstawy kryptoanalizy (Cryptography and Basics of Cryptanalysis)	K2st_W6,	K2st_U3, K2st_U4, K2st_U5, K2st_U7, ,	P7S_WG, P7S_UW
Innowacyjność i kreatywne myślenie (Innovation and Creative Thinking) (nauki społeczne)	K2st_W9,	K2st_U5,	P7S_WG, P7S_UW
Zaawansowane bezpieczeństwo systemów komputerowych (Advanced System Security)	K2st_W5, K2st_W6,	K2st_U4, K2st_U5, K2st_U6, K2st_U8, K2st_U9, K2st_U10,	P7S_WG, P7S_UW
Bezpieczeństwo funkcjonalne (Functional Safety)	K2st_W5, K2st_W6,	K2st_U3, K2st_U4, K2st_U8,	P7S_WG, P7S_UW
Bezpieczeństwo sieci bezprzewodowych (Wireless Communication Security)	K2st_W5, K2st_W6,	K2st_U3, K2st_U4, K2st_U8,	P7S_WG, P7S_UW
Komunikacja w języku angielskim (Communication in English) / Język polski (Polish)			
Podstawowe szkolenie z zakresu BHP (Basic health and safety training)		K2st_U5,	P7S_UW
Semestr 2:			
Bezpieczeństwo aplikacji (Application Security)	K2st_W5,	K2st_U3, K2st_U4, K2st_U5, K2st_U6,	P7S_WG, P7S_UW
Bezpieczeństwo sieci (Network Security)	K2st_W6,	K2st_U8, K2st_U9, ,	P7S_WG, P7S_UW
Bezpieczeństwo systemów IoT (IoT Security)		K2st_U7,	P7S_WG, P7S_UW
Przedmiot obieralny 1: Bezpieczeństwo sieci definiowanych programowo (Security of Software-Defined Networks) / Ataki typu Side-channel (Side-channel Attacks)	K2st_W5,	K2st_U3, K2st_U5, K2st_U8,	P7S_WG, P7S_UW
Przedmiot obieralny 2: Bezpieczeństwo analizy Big Data (Security of Big Data Analytics) / Mechanizmy naruszeń i zapewnienia bezpieczeństwa w Chmurze i Centrach Danych (Mechanisms of Violations and Ensuring Security in Cloud and DC) / Bezpieczeństwo w systemach przechowywania danych (Security in Data Storage Systems)		K2st_U5, K2st_U9, ,	P7S_WG, P7S_UW
Metodologia projektów badawczych (Methodology of research projects)	K2st_W6,	K2st_U3, K2st_U4, K2st_U6, K2st_U10,	P7S_WG, P7S_UW
Przedmiot obieralny 3: Bezpieczeństwo przemysłowego Internetu Rzeczy (Security of Industrial IoT) / Technologia Blockchain i kryptowaluty (Blockchain Technology and Cryptocurrency)	K2st_W6,	K2st_U6,	P7S_WG, P7S_UW
Przedmiot obieralny 4: Informatyka Śledcza (Digital Forensics) / Wojna cybernetyczna (Cyber Warfare)	K2st_W6,	K2st_U8, K2st_U9,	P7S_UW
Pisanie prac naukowo-technicznych (Scientific & Technical Writing)			
Semestr 3:			
Seminarium dyplomowe (Diploma Seminar)	K2st_W6,		P7S_WG
Projekt badawczo-wdrożeniowy (Research and Implementation Project)	K2st_W6, K2st_W9,	K2st_U4, K2st_U5, K2st_U6, K2st_U8, K2st_U9, K2st_U10, ,	P7S_WG, P7S_UW
Zarządzanie bezpieczeństwem systemów IT oraz testy penetracyjne (Information Systems Security Management and Penetration Testing)	K2st_W9,	K2st_U5, K2st_U6, K2st_U8, K2st_U9, K2st_U10, ,	P7S_WG, P7S_UW
Przygotowanie pracy magisterskiej (Master's Thesis Preparation)	K2st_W5, K2st_W6,	K2st_U3, K2st_U4, K2st_U5, K2st_U6, K2st_U8, K2st_U9, K2st_U10, ,	P7S_WG, P7S_UW
Analiza złośliwego oprogramowania (Malicious Software Analysis)	K2st_W5,	K2st_U3, K2st_U5, K2st_U6,	P7S_WG, P7S_UW
Przedmiot obieralny: (nauki humanistyczne): Komunikacja interpersonalna (Interpersonal Communication) / Komunikacja międzykulturowa (Intercultural Communication)			

INŻYNIERSKICH		
Profil ogólnoakademicki dla kwalifikacji pierwszego i drugiego stopnia		
Symb.	**MNiSW**	**WIiT PP**
	WIEDZA	
P7S_WG	absolwent zna i rozumie podstawowe procesy zachodzące w cyklu życia urządzeń, obiektów i systemów technicznych	ma **zaawansowaną i szczegółową** wiedzę o procesach zachodzących w cyklu życia systemów informatycznych sprzętowych lub programowych
		zna zaawansowane metody, techniki i narzędzia stosowane przy rozwiązywaniu złożonych zadań inżynierskich i prowadzeniu prac badawczych w wybranym obszarze informatyki
P7S_WK	absolwent zna i rozumie ogólne zasady tworzenia i rozwoju form indywidualnej przedsiębiorczości	ma podstawową wiedzę dotyczącą zarządzania / prowadzenia działalności gospodarczej oraz indywidualnej przedsiębiorczości
	UMIEJĘTNOŚCI	
P7S_UW	absolwent potrafi planować i przeprowadzać eksperymenty, w tym pomiary i symulacje komputerowe, interpretować uzyskane wyniki i wyciągać wnioski	potrafi planować i przeprowadzać eksperymenty, w tym pomiary i symulacje komputerowe, interpretować uzyskane wyniki i wyciągać wnioski oraz formułować i weryfikować hipotezy związane ze złożonymi problemami inzynierskimi i prostymi problemami badawczymi
P7S_UW	absolwent potrafi przy identyfikacji i formułowaniu specyfikacji zadań inżynierskich oraz ich rozwiązywaniu: − wykorzystać metody analityczne, symulacyjne i eksperymentalne, − dostrzegać ich aspekty systemowe i pozatechniczne, − dokonać wstępnej oceny ekonomicznej proponowanych rozwiązań i podejmowanych działań inżynierskich	potrafi wykorzystać do formułowania i rozwiązywania zadań inżynierskich i prostych problemów badawczych metody analityczne, symulacyjne oraz eksperymentalne
		potrafi — przy formułowaniu i rozwiązywaniu zadań inżynierskich — integrować wiedzę z różnych obszarów informatyki (a w razie potrzeby także wiedzę z innych dyscyplin naukowych) oraz zastosować podejście systemowe, uwzględniające także aspekty pozatechniczne
		potrafi ocenić przydatność i możliwość wykorzystania nowych osiągnięć (metod i narzędzi) oraz nowych produktów informatycznych
		potrafi poprawnie użyć wybraną metodę szacowania pracochłonności wytwarzania oprogramowania
P7S_UW	absolwent potrafi dokonać krytycznej analizy sposobu funkcjonowania istniejących rozwiązań technicznych i ocenić te rozwiązania	potrafi dokonać krytycznej analizy istniejących rozwiązań technicznych oraz zaproponować ich ulepszenia (usprawnienia)
P7S_UW	absolwent potrafi zaprojektować – zgodnie z zadaną specyfikacją – oraz wykonać typowe dla kierunku studiów proste urządzenie, obiekt, system lub zrealizować proces, używając	potrafi ocenić przydatność metod i narzędzi służących do rozwiązania zadania inżynierskiego, polegającego na budowie lub ocenie systemu informatycznego lub jego składowych, w tym dostrzec ograniczenia tych metod i narzędzi;
		potrafi - stosując m.in. koncepcyjnie nowe metody - rozwiązywać złożone zadania informatyczne, w tym zadania nietypowe oraz zadania zawierające komponent badawczy

	odpowiednio dobranych metod, technik, narzędzi i materiałów	potrafi — zgodnie z zadaną specyfikacją, uwzględniającą aspekty pozatechniczne — zaprojektować złożone urządzenie, system informatyczny lub proces oraz zrealizować ten projekt — co najmniej w części — używając właściwych metod, technik i narzędzi, w tym przystosowując do tego celu istniejące lub opracowując nowe narzędzia

Symb.
K2st_W5
K2st_W6
K2st_W9
K2st_U3
K2st_U4
K2st_U5
K2st_U6
K2st_U7
K2st_U8
K2st_U9
K2st_U10


K2st_U11

Statystyka programu kształcenia:
Łączna liczba godzin na studiach stacjonarnych II stopnia jest równa ~1024 godz.; konsultacje, egzaminy, mentoring i konferencje – ~102 godz., co daje łączną liczbę godzin zajęć wymagających bezpośredniego udziału nauczycieli akademickich i studentów = 1126 godz. (liczbę punktów, którą student musi uzyskać w trakcie zajęć = 90). Przyjęto założenie, że jeden punkt ECTS odpowiada efektom kształcenia, których uzyskanie wymaga od studenta średnio 25 godzin pracy
Łączna liczba punktów ECTS = 90 punkty ECTS modułów obieralnych = 86 (wymagana liczba punktów ECTS modułów obieralnych 30% z 90 = 27).
Łączna liczba godzin, którą student musi uzyskać w ramach zajęć o charakterze praktycznym, w tym zajęć laboratoryjnych i projektowych oraz ćwiczeń i seminariów jest równa 665 godz. (a punktów ECTS = 67).
Liczba punktów z nauk humanistycznych i społecznych jest równa 5.
Liczba punktów za zajęcia z języka obcego: Komunikacja interpersonalna (Interpersonal Communication) oraz Scientific & Technical Writing jest równa 4.
Liczba punktów zajęć związanych z badaniami naukowymi jest równa 51, a % punktów ECTS zajęć służących zdobywaniu pogłębionej wiedzy, umiejętności prowadzenia badań naukowych oraz kompetencji społecznych niezbędnych w działalności badawczej = 57%.
Liczba punktów ECTS z zajęć z zakresu nauk podstawowych = 4