Załącznik nr 9
do Zarządzenia Rektora Nr 35/19
z dnia 12 czerwca 2019 r.

IV. Opis programu studiów

3. KARTA PRZEDMIOTU

Kod przedmiotu	**E-TD-01-s4**
Nazwa przedmiotu	Algorytmy kryptograficzne
Nazwa przedmiotu w języku angielskim	**Cryptographic algorithms**
Obowiązuje od roku akademickiego	**2020/21**

USYTUOWANIE MODUŁU W SYSTEMIE STUDIÓW

Kierunek studiów	**Teleinformatyka**
Poziom kształcenia	**I stopień**
Profil studiów	**Praktyczny**
Forma i tryb prowadzenia studiów	**Studia stacjonarne**
Zakres	
Jednostka prowadząca przedmiot	**Katedra Elektrotechniki Przemysłowej i Automatyki**
Koordynator przedmiotu	**dr inż. Andrzej Stobiecki**
Zatwierdził	**Dziekan Wydziału Elektrotechniki Automatyki i Informatyki Dr hab. inż. Antoni Różowicz, prof. PŚk**

OGÓLNA CHARAKTERYSTYKA PRZEDMIOTU

Przynależność do grupy/bloku przedmiotów*	**Przedmiot wspólny dla kierunku**
Status przedmiotu*	**Obowiązkowy**
Język prowadzenia zajęć	**Polski**
Usytuowanie modułu w planie studiów - semestr	**Semestr IV**
Wymagania wstępne	**Algebra, Probabilistyka i statystyka**
Egzamin (TAK/NIE)	**Nie**
Liczba punktów ECTS	**2**

**pozostawić właściwe*

Forma prowadzenia zajęć	**wykład**	**ćwiczenia**	**laboratorium**	**projekt**	**Inne**
Liczba godzin w semestrze	**15**	**15**	**0**	**0**	**0**

EFEKTY UCZENIA SIĘ

Kategoria	Symbol efektu	Efekty kształcenia	Odniesienie do efektów kierunkowych
Wiedza	W01	Student poznaje metody oceny bezpieczeństwa stosowanych systemów szyfrowania.	TI1_W04
	W02	Ma poszerzoną i pogłębioną wiedzę z matematyki (teoria liczb, algebra, teoria prawdopodobieństwa) umożliwiającą projektowanie bezpiecznych systemów elektronicznych.	TI1_W01
Umiejętności	U01	Student poznaje metody oceny bezpieczeństwa stosowanych systemów szyfrowania.	TI1_U01 TI1_U18
	U02	Potrafi wykorzystać metody analityczne i symulacyjne do konstrukcji bezpiecznych systemów kryptograficznych	TI1_U13 TI1_U20
Kompetencje społeczne	K01	Ma świadomość roli społecznej absolwenta dobrej uczelni technicznej	TI1_K01 TI1_K02

TREŚCI PROGRAMOWE

Forma zajęć*	Treści programowe
Wykład	1. Wprowadzenie do kryptografii, podstawowe procedury szyfrowania danych, możliwości kryptografii. 2. Symetryczne algorytmy, współczesne algorytmy szyfrujące. 3. Problemy wykorzystywane w kryptografii asymetrycznej, algorytmy faktoryzacji i logarytmowania dyskretnego. 4. Kryptografia asymetryczna – szyfrowanie i schematy podpisów cyfrowych, wymagania, zagrożenia i metody ataków. 5. Zaawansowane schematy podpisów cyfrowych. 6. Schematy identyfikacji i uwierzytelniania – hasła jednorazowe, protokoły wyzwanie-odpowiedź, protokoły z wiedzą zerową. 7. Protokoły wymiany i uzgadniania kluczy szyfrujących.
Ćwiczenia	1. Cele kryptologii. 2. Szyfry symetryczne i asymetryczne (w tym algorytmy wymiany klucza). 3. Kryptograficzne funkcje skrótu, kody uwierzytelnienia wiadomości oraz bezpieczne przechowywanie haseł. 4. Podpis cyfrowy i karty kryptograficzne. 5. Kryptografia klucza publicznego. 6. Wirtualna prywatna sieć.

*) zostawić tylko realizowane formy zajęć

METODY WERYFIKACJI EFEKTÓW UCZENIA SIĘ

Symbol efektu	Metody sprawdzania efektów uczenia się					
	Egzamin ustny	Egzamin pisemny	Kolokwium	Projekt	Sprawozdanie	Inne
W01			+			
W02			+			
U01			+			
U02			+			
K01			+			

FORMA I WARUNKI ZALICZENIA

Forma zajęć*	Forma zaliczenia*	Warunki zaliczenia
Wykład	Zaliczenie z oceną	Uzyskanie min. 50% punktów z kolokwium końcowego
Ćwiczenia	Zaliczenie z oceną	Uzyskanie min. 50% punktów z kolokwiów cząstkowych

*) zostawić tylko realizowane formy zajęć oraz wybrać formę zaliczenia

NAKŁAD PRACY STUDENTA

Bilans punktów ECTS								
Lp.	**Rodzaj aktywności**	**Obciążenie studenta**					**Jed-nostka**
1.	Udział w zajęciach zgodnie z planem studiów	W	C	L	P	S	h
		15	15	0	0	0	
3.	Inne (konsultacje, egzamin)*	2	2	0	0	0	h
4.	**Razem przy bezpośrednim udziale nauczyciela akademickiego**	**34**					h
5.	**Liczba punktów ECTS, którą student uzyskuje przy bezpośrednim udziale nauczyciela akademickiego**	**1,36**					ECTS
6.	**Liczba godzin samodzielnej pracy studenta**	**16**					h
7.	**Liczba punktów ECTS, którą student uzyskuje w ramach samodzielnej pracy**	**0,64**					ECTS
8.	**Nakład pracy związany z zajęciami o charakterze praktycznym**	**15**					h
9.	**Liczba punktów ECTS, którą student uzyskuje w ramach zajęć o charakterze praktycznym**	**0,60**					ECTS
10.	**Sumaryczne godzinowe obciążenie pracą studenta**	**50**					h
11.	**Punkty ECTS za moduł** *1 punkt ECTS=25 godzin obciążenia studenta*	**2**					

** wszelkie formy weryfikacji efektów, w tym egzaminy oraz nie więcej niż 2 godziny konsultacji dla każdej formy zajęć*

LITERATURA

1. Menezes A., P.van Oorschot, Vanstone S., Kryptografia stosowana, WNT, Warszawa, 2005.
2. Stinson D. R., Kryptografia w teorii i praktyce, WNT, Warszawa, 2005.
3. Mochnacki W., Kody korekcyjne i kryptografia, Oficyna Wydawnicza Politechniki Wrocławskiej, Wrocław, 2000.
4. Kutyłowski M., Strothmann W., Kryptografia. Teoria i praktyka zabezpieczania systemów komputerowych, Oficyna Wydawnicza Read Me, Warszawa, 1999.
5. Koblitz N., Wykład z teorii liczb i kryptografii, WNT, Warszawa, 2009.
6. Welschenbach M., Kryptografia w C i C++, Wydawnictwo Mikom, Warszawa, 2002.
7. Stoklosa J., Bilski T., Pankowski T., Bezpieczeństwo danych w systemach informatycz-nych, PWN, Warszawa, 2001.
8. Wrona M., Niebezpieczeństwo komputerowe, RM, Warszawa, 2000.