



KARTA PRZEDMIOTU

Kod przedmiotu	studia stacjonarne:	E-ID2C-03-s2, E-ID2C-03-s3
	studia niestacjonarne:	E-2IZ2C-1007-s3
Nazwa przedmiotu	Bezpieczeństwo komunikacji bezprzewodowej	
Nazwa przedmiotu w języku angielskim	Security of Wireless Communication	
Obowiązuje od roku akademickiego	2022/2023	

USYTUOWANIE PRZEDMIOTU W SYSTEMIE STUDIÓW

Kierunek studiów	Informatyka
Poziom kształcenia	II stopień
Profil studiów	Ogólnoakademicki
Forma i tryb prowadzenia studiów	Studia stacjonarne i niestacjonarne
Zakres	Cyberbezpieczeństwo
Jednostka prowadząca przedmiot	Katedra Systemów Informatycznych
Koordynator przedmiotu	Mgr inż. Michał Młodawski
Zatwierdził	Dziekan Wydziału Elektrotechniki, Automatyki i Informatyki dr hab. inż. Roman Deniziak, prof. PŚk

OGÓLNA CHARAKTERYSTYKA PRZEDMIOTU

Przynależność do grupy/bloku przedmiotów		Przedmiot specjalnościowy
Status przedmiotu		Wybieralny
Język prowadzenia zajęć		Polski
Usytuowanie w planie studiów - semestr	studia stacjonarne	Semestr II lub Semestr III
	studia niestacjonarne	Semestr II lub Semestr III
Wymagania wstępne		Wprowadzenie do cyberbezpieczeństwa
Egzamin (TAK/NIE)		NIE
Liczba punktów ECTS		3

Forma prowadzenia zajęć		wykład	ćwiczenia	laboratorium	projekt	inne
Liczba godzin w semestrze	studia stacjonarne:	30		15	15	
	studia niestacjonarne:	18		9	9	

EFEKTY UCZENIA SIĘ

Kategoria	Symbol efektu	Efekty kształcenia	Odniesienie do efektów kierunkowych
Wiedza	W01	Student zna i rozumie podstawowe zagrożenia wynikające z komunikacji bezprzewodowej	INF2_W02
	W02	Student zna i rozumie działanie wybranych protokołów komunikacji	INF2_W06
	W03	Student zna i rozumie schematy inżynierii wstecznej wybranych protokołów komunikacji	INF2_W02
Umiejętności	U01	Student potrafi używać metod do symulacji wybranych protokołów komunikacji i radzenia sobie z typowymi atakami na nie	INF2_U01, INF2_U02, INF2_U05, INF2_U07, INF2_U11
	U02	Student potrafi tworzyć oprogramowanie wykorzystujące wybrane, odpowiednio zabezpieczone, protokoły komunikacji	INF2_U01, INF2_U02, INF2_U05, INF2_U09
	U03	Student potrafi zaprojektować system zgodny ze standardami oraz odporny na wybrane rodzaje ataków.	INF2_U01, INF2_U02, INF2_U05, INF2_U07, INF2_U09, INF2_U11
Kompetencje społeczne	K01	Student rozumie potrzebę ciągłego podnoszenia kompetencji w zakresie cyberbezpieczeństwa szczególnie w kwestii bezpieczeństwa komunikacji bezprzewodowej.	INF2_K03, INF2_K04
	K02	Student jest gotów do obiektywnej oceny swojej roli w projekcie informatycznym.	IN_K02

TREŚCI PROGRAMOWE

Forma zajęć	Treści programowe
wykład	Wprowadzenie do komunikacji bezprzewodowej (poznanie podstawowych pojęć związanych z komunikacją bezprzewodową, obliczenie budżetu linku danych, zapoznanie ze zjawiskiem propagacji fal radiowych) Wprowadzenie do bezpieczeństwa komunikacji bezprzewodowej (wprowadzenie do wybranych ataków takich jak: Packet Sniffing, Jamming, Man in the Middle, Rogue Access Point, omówienie wybranych metod szyfrowania danych i korekcji błędów) Poznanie warstwy fizycznej i założeń matematycznych wybranych modulacji sygnału radiowego (obszar zagadnień związanych ze sprzętową modulacją sygnałów. Zapoznanie z wybranymi modulacjami sygnału i ich wpływu na możliwość dokonania inżynierii wstecznej sygnału radiowego z uwzględnieniem stopnia trudności) Analiza oraz zabezpieczenie wybranych protokołów komunikacji bezprzewodowej (omówienie wybranych aspektów bezpieczeństwa protokołów: Bluetooth, ZigBee, Wi-Fi, LoRa, 5G, GPS i innych) Sprzętowe i programowe wsparcie w procesie analizy oraz symulacji protokołów komunikacji (omówienie procesu analizy oraz symulacji wybranych protokołów komunikacyjnych przy użyciu specjalistycznego oprogramowania)

laboratorium	1. Analiza wybranych rodzajów ataków i reagowanie na nie 2. Analiza propagacji fal radiowych (wykorzystaniem standardowego modelu propagacji fal radiowych oraz z wykorzystaniem śledzenia promieni) 3. Symulacja referencyjnego sygnału radiowego (zbadanie wpływu modulacji sygnału radiowego i korekcji błędów na stopień odbioru wiadomości oraz ich poufności) 4. Pełna symulacja wybranych protokołów komunikacji, następnie dokonywanie próby ataku i reagowania na nie.
projekt	Zadania realizowane w ramach zajęć polegają na zaprojektowaniu, stworzeniu i udokumentowaniu określonej aplikacji/symulacji. Tematyka problemu rozwiązywanego przez program jest zgodna z zagadnieniami realizowanymi podczas zajęć laboratoryjnych. Projekty są realizowane w grupach. Studenci powinni wykazać się samodzielną realizacją zadań projektowych, a ponadto zaproponować sposób sprawdzenia poprawności przyjętych rozwiązań.

METODY WERYFIKACJI EFEKTÓW UCZENIA SIĘ

Symbol efektu	Metody sprawdzania efektów kształcenia					
	Egzamin ustny	Egzamin pisemny	Kolokwium	Projekt	Sprawozdanie	Inne
W01			X	X		X
W02			X	X	X	X
W03			X	X		X
U01				X		X
U02			X	X	X	X
U03				X	X	X
K01			X	X	X	X
K02			X	X	X	X

FORMA I WARUNKI ZALICZENIA

Forma zajęć	Forma zaliczenia	Warunki zaliczenia
wykład	zaliczenie z oceną	Uzyskanie co najmniej 50% punktów z kolokwium końcowego w formie pisemnej lub ustnej.
laboratorium	zaliczenie z oceną	Uzyskanie co najmniej 50% punktów za zadania laboratoryjne, a także kolokwia lub kolokwium końcowe.
projekt	zaliczenie z oceną	Uzyskanie oceny 3 poprzez kompletne wykonanie pierwszych trzech etapów projektu. Poprawne wykonanie następnych etapów umożliwia uzyskanie wyższej oceny. Projekty będą realizowane w zespołach 2-4 osobowych.

NAKŁAD PRACY STUDENTA

Bilans punktów ECTS												
Lp.	Rodzaj aktywności	Obciążenie studenta										Jednos tka
		studia stacjonarne					studia niestacjonarne					
1.	Udział w zajęciach zgodnie z planem studiów	W	C	L	P	S	W	C	L	P	S	h
		30		15	15		18		9	9		
2.	Inne (konsultacje, egzamin)	2		2	2		2		1	1		h
3.	Razem przy bezpośrednim udziale nauczyciela akademickiego	66					40					h

4.	Liczba punktów ECTS, którą student uzyskuje przy bezpośrednim udziale nauczyciela akademickiego	2.64	1.60	ECTS
5.	Liczba godzin samodzielnej pracy studenta	9	35	h
6.	Liczba punktów ECTS, którą student uzyskuje w ramach samodzielnej pracy	0.36	1.40	ECTS
7.	Nakład pracy związany z zajęciami o charakterze praktycznym	30	18	h
8.	Liczba punktów ECTS, którą student uzyskuje w ramach zajęć o charakterze praktycznym	1.20	0.72	ECTS
9.	Sumaryczne obciążenie pracą studenta	75	75	h
10.	Punkty ECTS za moduł <i>1 punkt ECTS=25 godzin obciążenia studenta</i>	3		ECTS

LITERATURA

1. Szóstka Jarosław; Fale i Anteny; Wydawnictwa Komunikacji i Łączności ISBN: 83-206-1626-3, 978-83-206-1626-2; Warszawa 2019
2. Sutton Roger J.; Bezpieczeństwo telekomunikacji. Praktyka i zarządzanie; Wydawnictwa Komunikacji i Łączności; ISBN: 83-206-1517-8; Warszawa 2004
3. John Padgett, John Bahr, Guide to Bluetooth Security, NIST Special Publication 800-121 Rev. 2 (update 1)
4. 3GPP TS 33.401, "Technical Specification Group Services and System Aspects: 3GPP System Architecture Evolution (SAE) Security architecture".
5. 3GPP TS 33.501, "Security architecture and procedures for 5G system".
6. P. Calhoun, Ed., Control and Provisioning of Wireless Access Points (CAPWAP) Protocol Binding for IEEE 802.11