



Karta przedmiotu

| | | | | | | | |
|--|---|---|---|------------------------|---|---|-------|
| Nazwa i kod przedmiotu | Bezpieczeństwo danych w systemach radiokomunikacyjnych, PG_00048364 | | | | | | |
| Kierunek studiów | Elektronika i telekomunikacja | | | | | | |
| Data rozpoczęcia studiów | luty 2025 r. | Rok akademicki realizacji przedmiotu | | | 2025/2026 | | |
| Poziom kształcenia | II stopnia | Grupa zajęć | | | Grupa zajęć fakultatywnych Grupa zajęć specjalnościowych Grupa zajęć powiązanych z prowadzonymi badaniami naukowymi w dziedzinie nauki związanej z kierunkiem - profil ogólnoakademicki | | |
| Forma studiów | stacjonarne | Sposób realizacji | | | na uczelni | | |
| Rok studiów | 1 | Język wykładowy | | | polski | | |
| Semestr studiów | 2 | Liczba punktów ECTS | | | 2.0 | | |
| Profil kształcenia | ogólnoakademicki | Forma zaliczenia | | | zaliczenie | | |
| Jednostka prowadząca | Wydział Elektroniki, Telekomunikacji i Informatyki -> Katedra Systemów i Sieci Radiokomunikacyjnych | | | | | | |
| Imię i nazwisko wykładowcy (wykładowców) | Odpowiedzialny za przedmiot | | dr inż. Andrzej Marczak | | | | |
| | Prowadzący zajęcia z przedmiotu | | dr inż. Andrzej Marczak | | | | |
| Formy zajęć i metody nauczania | Forma zajęć | Wykład | Ćwiczenia | Laboratorium | Projekt | Seminarium | RAZEM |
| | Liczba godzin zajęć | 15.0 | 0.0 | 15.0 | 0.0 | 0.0 | 30 |
| | W tym liczba godzin zajęć na odległość: 0.0 | | | | | | |
| Aktywność studenta i liczba godzin pracy | Aktywność studenta | Udział w zajęciach dydaktycznych, objętych planem studiów | | Udział w konsultacjach | | Praca własna studenta | RAZEM |
| | Liczba godzin pracy studenta | 30 | | 4.0 | | 16.0 | 50 |
| Cel przedmiotu | Celem przedmiotu jest zapoznanie studentów z metodami zabezpieczeń kryptograficznych w systemach radiokomunikacyjnych. | | | | | | |
| Efekty uczenia się przedmiotu | Efekt kierunkowy | | Efekt z przedmiotu | | | Sposób weryfikacji i oceny efektu | |
| | [K7_U07] potrafi wykorzystać zaawansowane metody wspomagania procesów i funkcji, specyficzne dla kierunków studiów | | Student potrafi wykorzystać zdobytą wiedzę dotyczącą metod kryptograficznego zabezpieczania danych do zrozumienia metod zabezpieczania danych stosowanych w systemach radiokomunikacyjnych. | | | [SU1] Ocena realizacji zadania | |
| | [K7_W03] zna i rozumie w pogłębionym stopniu budowę i zasady działania komponentów i systemów związanych z kierunkiem studiów, w tym teorii, metody i złożone zależności między nimi oraz wybrane zagadnienia szczegółowe – właściwe dla programu kształcenia | | Student zna i rozumie jaką rolę odgrywają poszczególne bloki na schematach przedstawiających metody zabezpieczenia danych w systemach radiokomunikacyjnych. | | | [SW1] Ocena wiedzy faktograficznej | |
| | [K7_K02] jest gotów do krytycznej oceny odbieranych treści, uznawania znaczenia wiedzy w rozwiązywaniu problemów poznawczych i praktycznych | | Student potrafi wybierać właściwe metody zabezpieczenia danych do odpowiednich zastosowań. | | | [SK5] Ocena umiejętności rozwiązywania problemów występujących w praktyce | |

| | | | |
|---|--|---|-------------------------|
| Treści przedmiotu | <ol style="list-style-type: none"> 1. Podstawowe pojęcia i cele ochrony danych. 2. Szyfry blokowe. 3. Szyfry strumieniowe, generowanie kluczy szyfrów strumieniowych. 4. Szyfry asymetryczne. 5. Kody uwierzytelniania wiadomości (MAC). 6. Zagrożenia bezpieczeństwa transmisji w systemach radiokomunikacyjnych. 7. Uwierzytelnianie i szyfrowanie w systemach radiokomunikacyjnych. 8. Bezpieczeństwo transmisji w systemie trunkingowym TETRA. 9. Bezpieczeństwo transmisji w sieciach standardu CDMA2000. 10. Bezpieczeństwo transmisji w systemie komórkowym GSM. 11. Bezpieczeństwo transmisji w systemie komórkowym UMTS. 12. Bezpieczeństwo transmisji w systemie IEEE 802.11. 13. Mechanizmy bezpieczeństwa w systemie IEEE 802.15 Bluetooth. 14. Mechanizmy bezpieczeństwa w systemie WIMAX. 15. Radio rekonfigurowane programowo (SDR) - aspekty bezpieczeństwa danych. | | |
| Wymagania wstępne i dodatkowe | | | |
| Sposoby i kryteria oceniania osiągniętych efektów uczenia się | Sposób oceniania (składowe) | Próg zaliczeniowy | Składowa oceny końcowej |
| | Ćwiczenia praktyczne | 50.0% | 10.0% |
| | Egzamin pisemny | 51.0% | 90.0% |
| Zalecana lista lektur | Podstawowa lista lektur | V.Niemi, K.Nyberg: UMTS Security, John Wiley & Sons Inc. B. Preneel "Mobile and Wireless Communications Security" In NATO ASI on Aspects of Network and Information Security, IOS Press P. Chandra "Bulletproof Wireless Security GSM, UMTS, 802.11 and Ad Hoc Security", Elsevier Inc 2005 | |
| | Uzupełniająca lista lektur | Roger J. Sutton: Bezpieczeństwo telekomunikacji. Praktyka i zarządzanie, Wydawnictwa Komunikacji i Łączności, Warszawa | |
| | Adresy eZasobów | Adresy na platformie eNauczanie: | |
| Przykładowe zagadnienia/ przykładowe pytania/ realizowane zadania | | | |
| Praktyki zawodowe w ramach przedmiotu | Nie dotyczy | | |

Dokument wygenerowany elektronicznie. Nie wymaga pieczęci ani podpisu.