# KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu
Bezpieczeństwo systemów bezprzewodowych [S1Cybez1>BSB]

## Przedmiot

Kierunek studiów
Cyberbezpieczeństwo

Rok/Semestr
3/6

Studia w zakresie (specjalność)
–

Profil studiów
ogólnoakademicki

Poziom studiów
pierwszego stopnia

Język oferowanego przedmiotu
polski

Forma studiów
stacjonarne

Wymagalność
obieralny

## Liczba godzin

Wykład
24

Laboratorium
24

Inne
0

Ćwiczenia
0

Projekty/seminaria
0

## Liczba punktów ECTS

3,00

## Koordynatorzy

prof. dr hab. inż. Hanna Bogucka
hanna.bogucka@put.poznan.pl

## Wykładowcy

## Wymagania wstępne

Student rozpoczynając ten kurs powinien posiadać podstawową wiedzę z zakresu bezpieczeństwa systemów informatycznych. Ponadto powinien posiadać podstawową znajomość podstaw sieci komputerowych i technologii bezprzewodowych. Podstawy kryptografii i protokołów bezpieczeństwa.

## Cel przedmiotu

Celem przedmiotu jest zapoznanie studentów z zagrożeniami związanymi z bezpieczeństwem systemów bezprzewodowych. Omówienie technologii 5G/6G oraz systemów otwatych (np. OpenWiFi, OpenRAN, Open5GS) z perspektywy zabezpieczeń w tym stosowania do poprawy bezpieczeństwa sztucznej inteligencji. Praktyczne podejście do analizy podatności w sieciach bezprzewodowych w systemach komórkowych, systemach WLAN, TETRA, WiMAX. Zrozumienie zasad projektowania i implementacji bezpiecznych systemów bezprzewodowych.

## Przedmiotowe efekty uczenia się

Wiedza:
Student sna kluczowe technologie bezprzewodowe (Wi-Fi, LTE, 5G, 6G, TETRA) i ich architektury, z uwzględnieniem specyfiki zagrożeń bezpieczeństwa. Zna standardy i protokoły bezpieczeństwa

stosowane w systemach bezprzewodowych, w tym WPA3, IPsec, TLS, DTLS oraz mechanizmy ochrony prywatności. Posiada wiedzę na temat ataków na systemy bezprzewodowe, takie jak sniffing, spoofing, man-in-the-middle (MITM), denial-of-service (DoS) oraz metody ich wykrywania i przeciwdziałania. Jest zorientowany co do zasad projektowania i implementacji bezpiecznych systemów komunikacji bezprzewodowej, w tym wirtualnych segmentach sieci 5G (network slicing). Zna najnowsze trendy w bezpieczeństwie sieci bezprzewodowych, takie jak edge computing, sztuczna inteligencja w detekcji zagrożeń, oraz wyzwania związane z 5G/6G.[K1_W07][K1_W10][K1_W14]

Umiejętności:
Student potrafi analizować zagrożenia i identyfikować podatności w sieciach bezprzewodowych, w tym w systemach 5G/6G. Umie konfigurować i testować mechanizmy bezpieczeństwa w systemach Wi-Fi i sieciach komórkowych, takich jak np. WPA3. Umie wykorzystywać narzędzia do analizy i monitorowania ruchu w sieciach bezprzewodowych, takie jak Wireshark czy Aircrack-ng, w celu wykrywania i eliminowania zagrożeń. Potrafi projektować i implementować podstawowe systemy ochrony w sieciach bezprzewodowych oraz wirtualnych infrastrukturach sieci 5G. Umie wdrażać procedury zarządzania ryzykiem oraz analizować skuteczność stosowanych zabezpieczeń w systemach bezprzewodowych. [K1_U02][K1_U03][K1_U04][K1_U06]

Kompetencje społeczne:
Student jest zdolny do krytycznej analizy i oceny bezpieczeństwa systemów bezprzewodowych w zmieniających się warunkach technologicznych i zagrożeniowych. Jest przygotowany do podejmowania odpowiedzialnych decyzji dotyczących projektowania, wdrażania i zarządzania systemami bezprzewodowymi, z uwzględnieniem aspektów etycznych i ochrony prywatności. Potrafi współpracować w zespole interdyscyplinarnym przy realizacji projektów związanych z bezpieczeństwem sieci bezprzewodowych. Dąży do ciągłego aktualizowania wiedzy w obszarze technologii bezprzewodowych i ich bezpieczeństwa, w kontekście dynamicznego rozwoju technologii 5G/6G. [K1_K01][K1_K02][K1_K05]

## Metody weryfikacji efektów uczenia się i kryteria oceny

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:
Wykład: wiedza jest weryfikowana poprzez egzamin przeprowadznony w postaci pisemnej lub ustnej, lub też w postaci testu. Ocena zaliczeniowa wynosi 51% punktów, a podczas egzaminu nie wolno używać żadnych materiałów pomocniczych.
Laboratorium: wiedza i umiejętności są weryfikowane na podstawie oceny bieżącego postępu w realizacji zadań; sprawdzenie zakładanych efektów uczenia się odbywa się poprzez ewaluację. Pisemne raporty dotyczące poszczególnych tematów laboratoryjnych oraz, ewentualnie przeprowadzonego testu z umiejętności projektowania, konfigurowania i zastosowania zasad bezpieczeństwa w systemach bezprzewodowych w tym komórkowych.
W każdej formie zaliczenia przedmiotu ocena zależy od liczby zdobytych przez studenta punktów w stosunku do maksymalnej liczby punktów obowiązkowych. Warunkiem pozytywnego zaliczenia jest otrzymanie co najmniej 51% punktów możliwych do zdobycia. Zależność oceny od liczby punktów definiuje Regulamin Studiów. Dodatkowo zasady zaliczania przedmiotu i dokładne progi zaliczeniowe zostaną przekazane studentom na początku semestru z wykorzystaniem uczelnianych systemów elektronicznych oraz na pierwszych zajęciach (w każdej formie zajęć).

## Treści programowe

Treści programowe obejmują omówienie kluczowych technologi bezprzewodowych, takich jak Wi-Fi, LTE, 5G/6G, TETRA standardów otwartych np. OpenWiFi i OpenRAN z naciskiem na ich architekturę bezpieczeństwa oraz zagrożenia z nimi związanymi. Szczególną uwagę poświęca się wykorzystaniu sztucznej inteligencji i uczenia maszynowego do analizy ruchu sieciowego, wykrywania anomalii oraz przeciwdziałania zaawansowanym zagrożeniom, takim jak sniffing czy ataki DDoS w sieciach komórkowych i systemach WLAN. Studenci poznają mechanizmy ochrony, w tym systemy detekcji i zapobiegania włamaniom, które wykorzystują rozwiązania AI. Program obejmuje również projektowanie i implementację bezpiecznych systemów bezprzewodowych z uwzględnieniem wyzwań związanych z wirtualizacją sieci (Network Slicing) i przetwarzaniem brzegowym. Praktyczna część kursu kładzie nacisk na rozwijanie umiejętności identyfikacji ryzyk, konfiguracji zabezpieczeń oraz wdrażania strategii ochrony z wykorzystaniem technologii AI w systemach otwartych i nowoczesnych sieciach 5G/6G.

## Tematyka zajęć

Wykład:
1. Wprowadzenie do bezpieczeństwa systemów bezprzewodowych.
Przegląd podstaw bezpieczeństwa systemów bezprzewodowych 802.11.
Zasady bezpieczeństwa w systemie TETRA.
2. Wprowadzenie do bezpieczeństwa w systemach komórkowych.
Przegląd podstaw architektury bezpieczeństwa systemów GSM, UMTS, LTE, 5G/6G. Realizacja zasad integralności, poufności i uwierzytelnienia.
3. Systemy otwarte w sieciach bezprzewodowych.
Charakterystyka systemów otwartych: otwarte interfejsy, standardy i platformy. Projekty open-source w sieciach bezprzewodowych: OpenWiFi, OpenRAN, OpenAirInterface. Wady i zalety systemów otwartych: interoperacyjność, elastyczność vs podatność na ataki. Zarządzanie bezpieczeństwem w systemach otwartych.
4. Specyfika zagrożeń w sieciach bezprzewodowych.
Podstawowe ataki na sieć dostępową i szkieletową systemów bezprzewodowych. Ataki na aplikacje systemów bezprzewodowych.
5. Standardy bezpieczeństwa 802.11i oraz WPA3.
Realizacja poufności w systemach bezprzewodowych, bezpieczeństwa end to end.
6. Bezpieczeństwo systemów Wi-Fi.
Otwarte sieci Wi-Fi: zagrożenia i techniki ochrony. Narzędzia do analizy bezpieczeństwa w sieciach WLAN, np., Wireshark, Aircrack-ng, Zasady konfiguracji bezpiecznych sieci Wi-Fi.
7. Bezpieczeństwo w sieciach 5G.
Architektura bezpieczeństwa 5G/6G: warstwa RAN (Radio Access Network), Core Network i Network Slicing. Zagrożenia w sieciach 5G: ataki na wirtualizację, Edge Computing, API.
8. Mechanizmy bezpieczeństwa w sieciach 6G.
Wyzwania i potencjalne zagrożenia związane z wykorzystaniem do realizacji bezpieczeństwa sztucznej inteligencji i technologi kwantowych. Mechanizmy bezpieczeństwa SEPP (Security Edge Protection Proxy), Network Function Virtualization (NFV).
9. Przykłady użycia i projekty praktyczne.
Analiza rzeczywistych incydentów bezpieczeństwa w systemach Wi-Fi, 5G. Projektowanie i konfiguracja bezpiecznej sieci Wi-Fi w środowisku otwartym. Wdrażanie systemu Network Slicing w 5G z uwzględnieniem mechanizmów bezpieczeństwa. Ocena podatności i wdrażanie zabezpieczeń w systemach otwartych (np. OpenWiFi, OpenRAN).
10. Sztuczna inteligencja w detekcji zagrożeń w sieciach komórkowych 5G/6G i systemach WLAN.
Wykorzystanie algorytmów uczenia maszynowego do wykrywania anomalii. Ataki na tego typu rozwiązania i przeciwdziałania im.
11. Zarządzanie ryzykiem w systemach bezprzewodowych.
Metodyka analizy ryzyka (np. NIST, ISO/IEC 27005). Tworzenie polityk bezpieczeństwa dla systemów bezprzewodowych. Procedury reagowania na incydenty bezpieczeństwa. Audyty bezpieczeństwa i testy penetracyjne systemów bezprzewodowych.
12. Przyszłość bezpieczeństwa w sieciach bezpieczeństwa.
Sieci kwantowe. Nowe technologie zabezpieczeń.
Laboratorium:
1. Wprowadzenie i omówienie poszczególnych ćwiczeń laboratoryjnych oraz zasad oceniania, wykorzystanie narzędzia Cryptool.
2. Analiza struktury ramek standardu IEEE 802.11 przy użyciu oprogramowania Wireshark.
3. Analiza i łamanie zabezpieczeń wykorzystujących mechanizmy WEP, WPA/WPA2 i WPS. Zastosowanie tablic tęczowych.
4. Tworzenie i konfiguracja wirtualnych sieci WLAN.
5. Analiza działania standardu IEEE 802.1X oraz protokołów RADIUS i EAP.
6. Analiza różnych typów ataków na sieci IEEE 802.11. Wykorzytanie np. narzędzi Aircrack-ng, Kismet.
7. Systemy otwarte: bezpieczeństwo OpenWiFi. Instalacja i konfiguracja OpenWiFi. Analiza ryzyk wynikających z otwartych standardów i ich eliminacja.
8. Wykorzystanie algorytmów uczenia maszynowego do analizy anomalii w ruchu sieciowym. Klasyfikacja normalnego i podejrzanego ruchu z wykorzystaniem bibliotek Python (np. Scikit-learn).
9. Wykrywanie zagrożeń w sieciach 5G. Analiza protokołów 5G: SEPP, NAS, i NGAP. Wykorzystanie AI do predykcji potencjalnych zagrożeń w środowiskach 5G.
10. Zastosowanie AI w systemach detekcji włamań (IDS). Tworzenie prostego systemu IDS na bazie uczenia maszynowego. Analiza skuteczności wykrywania zagrożeń w sieciach Wi-Fi i 5G.

11. Testy penetracyjne w sieciach bezprzewodowych. Wprowadzenie do narzędzi testów penetracyjnych (Aircrack-ng, Metasploit). Symulacja ataków na otwarte systemy (np. OpenRAN). Przykłady projektów open-source (np. oprogramowanie kontrolerów RAN) OpenAirInterface, srsRAN.
12. Zajęcia podsumowujące. Kolokwium zaliczeniowe.

## Metody dydaktyczne

1. Wykład: prezentacja multimedialna ilustrowana przykładami.
2. Ćwiczenia laboratoryjne: wykonywanie zadań zleconych przez prowadzącego - ćwiczenia praktyczne, praca zespołowa, korzystanie z urządzeń sieciowych i środowisk symulacyjnych.

## Literatura

Podstawowa:
1. William Stallings, Wireless Communications & Networks, Pearson, 2021.
2. Mazin Alshamrani, Security and Privacy in 5G and Beyond Networks: Challenges and Solutions, Wiley, 2021.
3. Matthew S. Gast, 802.11 Wireless Networks: The Definitive Guide, O'Reilly Media, 2022.
4. Geert Leus, Danilo Mandic (red.), Machine Learning for Wireless Communications, Academic Press, 2022.
5. Literatura z uznanych czasopism naukowych, dokumenty normalizacyjne.

Uzupełniająca:
Uzupełniająca
1. Haipeng Yao, Mugen Peng, AI for 5G: Core Technologies and Applications, Springer, 2021.
2. Jie Gao, Artificial Intelligence for Wireless Communication and Networking, Wiley-IEEE Press, 2021.
3. nwar Al-Dulaimi, Syed Rizvi, Qiang Ni (red.), 5G Networks: Fundamentals, Techniques, and Applications, Wiley, 2020.

## Bilans nakładu pracy przeciętnego studenta

| | Godzin | ECTS |
|---|---|---|
| Łączny nakład pracy | 78 | 3,00 |
| Zajęcia wymagające bezpośredniego kontaktu z nauczycielem | 48 | 2,00 |
| Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych/ćwiczeń, przygotowanie do kolokwiów/egzaminu, wykonanie projektu) | 30 | 1,00 |