

Program studiów podyplomowych

Cyberbezpieczeństwo

(od r.a. 2023/2024)

Rok I Semestr zimowy (I)

Nazwa zajęć	punkty ECTS	Forma zajęć	Liczba godzin	Forma zaliczenia
Państwo i społeczeństwo ryzyka	1	Wykład	8	Z + PP
Polityka cyberbezpieczeństwa w organizacji - ochrona danych osobowych i informacji niejawnych	2	Konwersatorium Ćwiczenia	8 4	Z + inne
Analiza, ocena i zarządzanie ryzykiem występowania cyberzagrożeń	2	Konwersatorium Ćwiczenia	4 6	Z + A
Bezpieczeństwo zasobów cyfrowych	1	Konwersatorium Ćwiczenia	4 4	Z + A
Bezpieczeństwo wewnętrzne i cyberbezpieczeństwo RP	2	Wykład	10	Z/O + PP
Infrastruktura krytyczna i bezpieczeństwo przemysłowe	2	Konwersatorium Ćwiczenia	8 4	Z + inne
Technologie budowy i zabezpieczeń serwisów internetowych	1	Ćwiczenia	8	Z + A
OSINT 2.0 – praktyczne wprowadzenie do technik białego wywiadu w Internecie	2	Konwersatorium	6 4	Z + A
Kryminalistyka cyfrowa	2	Konwersatorium Ćwiczenia	4 8	Z/O + PP
Normy bezpieczeństwa i ciągłości działania	1	Konwersatorium Ćwiczenia	4 4	Z/O + T + A

Rok I Semestr letni (II)

Polityka cyberbezpieczeństwa UE	1	Wykład	8	Z + PP
Ochrona danych i prywatności w Internecie, bezpieczeństwo systemów bazodanowych i pracy w chmurze	2	Konwersatorium Ćwiczenia	2 6	Z + A

Przetwarzanie języka naturalnego i sztuczna inteligencja	2	Ćwiczenia	12	Z + inne
Wprowadzenie do bezpieczeństwa IoT	1	Wykład	8	Z + PP
Symulacje cyberataków	3	Konwersatorium Ćwiczenia	4 8	Z/O + T + A
Analiza Big Data w bezpieczeństwie i gospodarce	3	Konwersatorium Ćwiczenia	4 8	Z/O + PP
Psychomanipulacja w cyberprzestrzeni	1	Konwersatorium Ćwiczenia	4 4	Z + A
Audyt i kontrola w cyberbezpieczeństwie	1	Ćwiczenia	8	Z + A

A - aktywna obecność na zajęciach

O - ocena

T - test

Z - zaliczenie

PP - praca pisemna