Załącznik Nr 1 do Uchwały Nr RWZST-3-IV/1/2025
Rady Programowej kierunku Zarządzanie
Wydziału Zarządzania Sportem i Turystyką
Akademii Wychowania Fizycznego im. Jerzego
Kukuczki w Katowicach z dnia 15 kwietnia 2025 r.

<table>
<tr><td colspan="4">KARTA ZAJĘĆ</td></tr>
<tr><td colspan="4">Akademia Wychowania Fizycznego im. Jerzego Kukuczki w Katowicach
Wydział Zarządzania Sportem i Turystyką</td></tr>
<tr><td colspan="4">Zarządzanie studia I stopnia, profil ogólnoakademicki</td></tr>
<tr><td>Nazwa zajęć / nazwa grupy zajęć</td><td colspan="3">PRAWO W OBSZARZE BEZPIECZEŃSTWA INFORMACJI I CYBERPRZESTRZENI</td></tr>
<tr><td rowspan="11">Efekty uczenia się</td><td colspan="3">Wiedza</td></tr>
<tr><td>K_W02</td><td>W1</td><td>Ma zaawansowaną i uporządkowaną wiedzę z zakresu cyberbezpieczeństwa, w tym znajomość kategorii zagrożeń w cyberprzestrzeni, systemu bezpieczeństwa RP, aspektów prawnych ochrony prywatności oraz penalizacji cyberprzestępczości.</td></tr>
<tr><td>K_W03</td><td>W2</td><td>Zna i interpretuje w stopniu zaawansowanym podstawowe zasady prawa, ze szczególnym uwzględnieniem regulacji dotyczących funkcjonowania podmiotów gospodarczych w kontekście zagrożeń cyfrowych.</td></tr>
<tr><td colspan="3">Umiejętności</td></tr>
<tr><td>K_U12</td><td>U1</td><td>Potrafi posługiwać się przepisami prawa, normami i standardami w procesach planowania, organizowania i kontroli zadań w zakresie bezpieczeństwa informacji.</td></tr>
<tr><td>K_U21</td><td>U2</td><td>Potrafi zastosować odpowiednie metody i narzędzia analityczne oraz systemy informatyczne wspomagające ocenę zagrożeń i procesy decyzyjne w obszarze cyberbezpieczeństwa.</td></tr>
<tr><td>K_U26</td><td>U3</td><td>Potrafi w sposób klarowny i precyzyjny wypowiadać się na piśmie, konstruując logiczne uzasadnienia z wykorzystaniem wiedzy z zakresu prawa i zarządzania bezpieczeństwem</td></tr>
<tr><td colspan="3">Kompetencje społeczne</td></tr>
<tr><td>K_K09</td><td>K1</td><td>Dostrzega i formułuje problemy moralne i dylematy etyczne związane z funkcjonowaniem w środowisku cyfrowym; postępuje zgodnie z zasadami etyki zawodowej.</td></tr>
<tr><td>K_K07</td><td>K2</td><td>Odpowiedzialnie przygotowuje się do wykonywania zadań, projektuje i realizuje działania z zakresu cyberbezpieczeństwa zgodnie z obowiązującymi normami.</td></tr>
<tr><td>K_K04</td><td>K3</td><td>Jest przygotowany do organizowania pracy zespołowej i współdziałania z innymi uczestnikami procesów zarządzania bezpieczeństwem informacji.</td></tr>
<tr><td>Treści zajęć</td><td colspan="3">1. Pojęcie i zakres cyberbezpieczeństwa
2. Kategorie zagrożeń w cyberprzestrzeni – klasyfikacja i przykłady incydentów.
3. System bezpieczeństwa cyberprzestrzeni RP
4. Ochrona prywatności i danych osobowych
5. Bezpieczeństwo baz danych – obowiązki administratorów danych, odpowiedzialność prawna.</td></tr>
</table>

	6. Cyberprzestępczość i cyberataki – definicje, penalizacja, orzecznictwo. 7. Rola Rady Europy i NATO w regulowaniu przestrzeni cyfrowej – prawo międzynarodowe i bezpieczeństwo zbiorowe.
Metody dydaktyczne	1. Dyskusje problemowe 2. Praca zespołowa nad scenariuszem incydentu cyfrowego 3. Test wiedzy i projekt grupowy
Kryteria oceny efektów uczenia się	I. Praktyczny/projekt Kryteria oceny efektów uczenia się: 2,0 – Student nie osiągnął wymaganych efektów uczenia się. 3,0 – Student wykazuje braki, które jednak nie dyskwalifikują dalszej edukacji i mogą zostać usunięte. Zwykle wiadomości zestawione luźno, brak połączeń i związków logicznych. Rozwiązuje problemy typowe o niewielkim stopniu trudności. 3,5 – Student wykazuje poprawne rozumienie pojęć, wyjaśnia ważniejsze zjawiska. Rozwiązuje problemy typowe, przeważnie poprawnie operuje posiadanymi informacjami. 4,0 – Zakres wiedzy studenta obejmuje podstawowe treści przedmiotu ze znajomością powiązań logicznych. Poprawnie rozumuje w kategoriach przyczynowo-skutkowych. 4,5 – Wyczerpujące opanowanie całego materiału programowego. Student sprawnie wykorzystuje wiedzę. Umiejętnie dokonuje oceny problemów, procesów i zjawisk. 5,0 – Ponad przeciętne opanowanie całego materiału programowego. II. Pisemny/test Kryteria oceny efektów uczenia się: 2,0 – student nie osiągnął wymaganych efektów uczenia się (punktacja poniżej 50%). 3,0 – student osiągnął efekty uczenia się w stopniu dostatecznym (51 do 60%). 3,5 – student osiągnął efekty uczenia się w stopniu dostatecznym plus (61 do 70%). 4,0 – student osiągnął efekty uczenia się w stopniu dobrym (71 do 80%). 4,5 – student osiągnął efekty uczenia się w stopniu dobrym plus (81 do 90%). 5,0 – student osiągnął efekty uczenia się w stopniu bardzo dobrym (91 do 100%). III. Ustny/aktywność Kryteria oceny efektów uczenia się: 2,0 – Student niezaangażowany. 3,0 – Student pracuje niesystematycznie. 3,5 – Student przejawia przeciętną aktywność. 4,0 – Student wykazuje dobre przygotowanie w sferze komunikacji i umiejętności interpersonalnych. Jest aktywny, podejmuje zadania dodatkowe. 4,5 – Student jest zainteresowany problematyką przedmiotu. Przejawia postawę racjonalną, krytyczną i kreatywną.

	5,0 – Student twórczy w odpowiedzi, nie unika krytyki, posiada własne zdanie. Umiejętnie wyciąga wnioski. Jest aktywny, chętnie stawia pytania oraz problemy do dyskusji.
Literatura	1. Wąsik K. *Międzynarodowe regulacje prawne dotyczące cyberprzestrzeni* „Cybersecurity and Law" 2023/2 .s. 133 – 155. 2. Skoczylas D., Cyberzagrożenia w cyberprzestrzeni. Cyberprzestepczośc, cyberterroryznm i incydenty sieciowe „Prawo w działaniu. Sprawy karne" 2023/53, s/ 97-113. 3. Prawne i społeczne aspekty cyberbezpieczenstwa, red. S. Gwoździewicz, K. Tomaszycki, Warszawa 2017 4. Aleksandrowicz T., Bezpieczenstwo w cyberprzestrzeni ze stanowiska prawa międzynarodowego „Przegląd Bezpieczeństwa wewnętrznego" 2016/15, s. 11 - 26
Bilans punktów ECTS	udział w wykładach = 26h udział w ćwiczeniach=13h przygotowanie do kolokwium = 10h realizacja zadań projektowych = 29h łączna liczba godzin: 78 h w bezpośrednim kontakcie z prowadzącym 50% godzin liczba punktów ECTS = 3 pkt. Minimalna ilość godzin nakładu pracy studenta 3(pkt ECTS) x 26h = 78h

Forma oceny efektów uczenia się			
Efekty uczenia się	**Forma oceny**		
	Praktyczny	Pisemny	Ustny
W1	X	X	
W2	X	X	
U1	X		X
U2	X	X	
U3			X
K1	X		X
K2			X
K3	X		X

<table>
<tr><td colspan="4">KARTA ZAJĘĆ</td></tr>
<tr><td colspan="4">Akademia Wychowania Fizycznego im. Jerzego Kukuczki w Katowicach
Wydział Zarządzania Sportem i Turystyką</td></tr>
<tr><td colspan="4">Zarządzanie studia I stopnia, profil ogólnoakademicki</td></tr>
<tr><td>Nazwa zajęć / nazwa grupy zajęć</td><td colspan="3">PRAWO W OBSZARZE BEZPIECZEŃSTWA INFORMACJI I CYBERPRZESTRZENI</td></tr>
<tr><td rowspan="11">Efekty uczenia się</td><td colspan="3">Wiedza</td></tr>
<tr><td>K_W02</td><td>W1</td><td>Ma zaawansowaną i uporządkowaną wiedzę z zakresu cyberbezpieczeństwa, w tym znajomość kategorii zagrożeń w cyberprzestrzeni, systemu bezpieczeństwa RP, aspektów prawnych ochrony prywatności oraz penalizacji cyberprzestępczości.</td></tr>
<tr><td>K_W03</td><td>W2</td><td>Zna i interpretuje w stopniu zaawansowanym podstawowe zasady prawa, ze szczególnym uwzględnieniem regulacji dotyczących funkcjonowania podmiotów gospodarczych w kontekście zagrożeń cyfrowych.</td></tr>
<tr><td colspan="3">Umiejętności</td></tr>
<tr><td>K_U12</td><td>U1</td><td>Potrafi posługiwać się przepisami prawa, normami i standardami w procesach planowania, organizowania i kontroli zadań w zakresie bezpieczeństwa informacji.</td></tr>
<tr><td>K_U21</td><td>U2</td><td>Potrafi zastosować odpowiednie metody i narzędzia analityczne oraz systemy informatyczne wspomagające ocenę zagrożeń i procesy decyzyjne w obszarze cyberbezpieczeństwa.</td></tr>
<tr><td>K_U26</td><td>U3</td><td>Potrafi w sposób klarowny i precyzyjny wypowiadać się na piśmie, konstruując logiczne uzasadnienia z wykorzystaniem wiedzy z zakresu prawa i zarządzania bezpieczeństwem</td></tr>
<tr><td colspan="3">Kompetencje społeczne</td></tr>
<tr><td>K_K09</td><td>K1</td><td>Dostrzega i formułuje problemy moralne i dylematy etyczne związane z funkcjonowaniem w środowisku cyfrowym; postępuje zgodnie z zasadami etyki zawodowej.</td></tr>
<tr><td>K_K07</td><td>K2</td><td>Odpowiedzialnie przygotowuje się do wykonywania zadań, projektuje i realizuje działania z zakresu cyberbezpieczeństwa zgodnie z obowiązującymi normami.</td></tr>
<tr><td>K_K04</td><td>K3</td><td>Jest przygotowany do organizowania pracy zespołowej i współdziałania z innymi uczestnikami procesów zarządzania bezpieczeństwem informacji.</td></tr>
<tr><td>Treści zajęć</td><td colspan="3">8. Pojęcie i zakres cyberbezpieczeństwa
9. Kategorie zagrożeń w cyberprzestrzeni – klasyfikacja i przykłady incydentów.
10. System bezpieczeństwa cyberprzestrzeni RP
11. Ochrona prywatności i danych osobowych
12. Bezpieczeństwo baz danych – obowiązki administratorów danych, odpowiedzialność prawna.
13. Cyberprzestępczość i cyberataki – definicje, penalizacja, orzecznictwo.</td></tr>
</table>

	14. Rola Rady Europy i NATO w regulowaniu przestrzeni cyfrowej – prawo międzynarodowe i bezpieczeństwo zbiorowe.
Metody dydaktyczne	4. Dyskusje problemowe 5. Praca zespołowa nad scenariuszem incydentu cyfrowego 6. Test wiedzy i projekt grupowy
Kryteria oceny efektów uczenia się	I. Praktyczny/projekt Kryteria oceny efektów uczenia się: 2,0 – Student nie osiągnął wymaganych efektów uczenia się. 3,0 – Student wykazuje braki, które jednak nie dyskwalifikują dalszej edukacji i mogą zostać usunięte. Zwykle wiadomości zestawione luźno, brak połączeń i związków logicznych. Rozwiązuje problemy typowe o niewielkim stopniu trudności. 3,5 – Student wykazuje poprawne rozumienie pojęć, wyjaśnia ważniejsze zjawiska. Rozwiązuje problemy typowe, przeważnie poprawnie operuje posiadanymi informacjami. 4,0 – Zakres wiedzy studenta obejmuje podstawowe treści przedmiotu ze znajomością powiązań logicznych. Poprawnie rozumuje w kategoriach przyczynowo-skutkowych. 4,5 – Wyczerpujące opanowanie całego materiału programowego. Student sprawnie wykorzystuje wiedzę. Umiejętnie dokonuje oceny problemów, procesów i zjawisk. 5,0 – Ponad przeciętne opanowanie całego materiału programowego. II. Pisemny/test Kryteria oceny efektów uczenia się: 2,0 – student nie osiągnął wymaganych efektów uczenia się (punktacja poniżej 50%). 3,0 – student osiągnął efekty uczenia się w stopniu dostatecznym (51 do 60%). 3,5 – student osiągnął efekty uczenia się w stopniu dostatecznym plus (61 do 70%). 4,0 – student osiągnął efekty uczenia się w stopniu dobrym (71 do 80%). 4,5 – student osiągnął efekty uczenia się w stopniu dobrym plus (81 do 90%). 5,0 – student osiągnął efekty uczenia się w stopniu bardzo dobrym (91 do 100%). III. Ustny/aktywność Kryteria oceny efektów uczenia się: 2,0 – Student niezaangażowany. 3,0 – Student pracuje niesystematycznie. 3,5 – Student przejawia przeciętną aktywność. 4,0 – Student wykazuje dobre przygotowanie w sferze komunikacji i umiejętności interpersonalnych. Jest aktywny, podejmuje zadania dodatkowe. 4,5 – Student jest zainteresowany problematyką przedmiotu. Przejawia postawę racjonalną, krytyczną i kreatywną. 5,0 – Student twórczy w odpowiedzi, nie unika krytyki, posiada własne zdanie. Umiejętnie wyciąga wnioski. Jest aktywny, chętnie stawia pytania oraz problemy do dyskusji.

Literatura	5. Wąsik K. *Międzynarodowe regulacje prawne dotyczące cyberprzestrzeni* „Cybersecurity and Law" 2023/2 .s. 133 – 155. 6. Skoczylas D., Cyberzagrożenia w cyberprzestrzeni. Cyberprzestepczośc, cyberterroryznm i incydenty sieciowe „Prawo w działaniu. Sprawy karne" 2023/53, s/ 97-113. 7. Prawne i społeczne aspekty cyberbezpieczenstwa, red. S. Gwoździewicz, K. Tomaszycki, Warszawa 2017 8. Aleksandrowicz T., Bezpieczenstwo w cyberprzestrzeni ze stanowiska prawa międzynarodowego „Przegląd Bezpieczeństwa wewnętrznego" 2016/15, s. 11 - 26
Bilans punktów ECTS	udział w wykładach = 26h udział w ćwiczeniach=13h przygotowanie do kolokwium = 10h realizacja zadań projektowych = 29h łączna liczba godzin: 78 h w bezpośrednim kontakcie z prowadzącym 50% godzin liczba punktów ECTS = 3 pkt. Minimalna ilość godzin nakładu pracy studenta 3(pkt ECTS) x 26h = 78h

Forma oceny efektów uczenia się			
Efekty uczenia się	**Forma oceny**		
	Praktyczny	Pisemny	Ustny
W1	X	X	
W2	X	X	
U1	X		X
U2	X	X	
U3			X
K1	X		X
K2			X
K3	X		X

<table>
<tr><td colspan="4">KARTA ZAJĘĆ</td></tr>
<tr><td colspan="4">Akademia Wychowania Fizycznego im. Jerzego Kukuczki w Katowicach
Wydział Zarządzania Sportem i Turystyką</td></tr>
<tr><td colspan="4">Zarządzanie studia I stopnia, profil ogólnoakademicki</td></tr>
<tr><td>Nazwa zajęć / nazwa grupy zajęć</td><td colspan="3">TECHNOLOGIE CYFROWE I SZTUCZNA INTELIGENCJA W ZARZĄDZANIU BEZPIECZEŃSTWEM</td></tr>
<tr><td rowspan="12">Efekty uczenia się</td><td colspan="3">Wiedza</td></tr>
<tr><td>K_W20</td><td>W1</td><td>Ma pogłębioną wiedzę na temat wpływu narzędzi sztucznej inteligencji (SI) na zarządzanie bezpieczeństwem, przetwarzanie informacji, podejmowanie decyzji i analizę danych.</td></tr>
<tr><td>K_W21</td><td>W2</td><td>Zna metody analizy strategicznej z wykorzystaniem narzędzi cyfrowych w kontekście bezpieczeństwa i zarządzania kryzysowego.</td></tr>
<tr><td>K_W17</td><td>W3</td><td>Zna terminologię z zakresu nauk o kulturze fizycznej i zdrowiu w odniesieniu do technologii wspierających bezpieczeństwo społeczności</td></tr>
<tr><td colspan="3">Umiejętności</td></tr>
<tr><td>K_U21</td><td>U1</td><td>Potrafi zastosować narzędzia analityczne i cyfrowe systemy wspierające decyzje w sytuacjach zagrożenia bezpieczeństwa.</td></tr>
<tr><td>K_U03</td><td>U2</td><td>Potrafi analizować wpływ nowoczesnych technologii na procesy zarządzania kryzysowego oraz interpretować złożone problemy techniczno-organizacyjne.</td></tr>
<tr><td>K_U26</td><td>U3</td><td>Potrafi w sposób precyzyjny konstruować wypowiedzi ustne i pisemne dotyczące roli sztucznej inteligencji i narzędzi cyfrowych w obszarze bezpieczeństwa.</td></tr>
<tr><td colspan="3">Kompetencje społeczne</td></tr>
<tr><td>K_K06
P6S_KR</td><td>K1</td><td>Wykazuje aktywność i gotowość do podejmowania działań w zespole, szczególnie w kontekście nowych technologii i zagrożeń.</td></tr>
<tr><td>K_K09
P6S_KR</td><td>K2</td><td>Rozpoznaje dylematy etyczne związane z zastosowaniem AI w zarządzaniu ludźmi i bezpieczeństwem publicznym.</td></tr>
<tr><td>K_K04
P6S_KO</td><td>K3</td><td>Jest przygotowany do organizowania pracy zespołu przy wdrażaniu innowacyjnych technologii wspomagających bezpieczeństwo.</td></tr>
<tr><td>Treści zajęć</td><td colspan="3">1. Geneza badan nad sztuczna inteligencją
2. Kierunki rozwoju sztucznej inteligancji
3. Sztuczna inteligencja jako czynnik zwiększający poziom bezpieczeństwa w sferze bezpieczeństwa militarnego i informacyjnego
4. Zagrożenia i wyzwania związane z wykorzystaniem sztucznej inteligencji w sferze bezpieczeństwa militarnego i informacyjnego
5. Wpływ sztucznej inteligencji na zwiększenie zdolności państwa do ochrony swoich interesów i jego obywateli.</td></tr>
</table>

	6. Nowe technologii w zakresie bezpieczeństwa i ochrony społeczności przed wzrastającą przestępczością. 7. Standardy prawne i etyczne w obszarze AI. 8. Rola lidera i menedżera bezpieczeństwa w świecie cyfrowym – nowe kompetencje, zagrożenia i odpowiedzialność
Metody dydaktyczne	1. Wykład z prezentacją 2. Praca projektowa zespołowa 3. Dyskusja problemowa 4. Test
Kryteria oceny efektów uczenia się	I. Praktyczny/projekt Kryteria oceny efektów uczenia się: 2,0 – Student nie osiągnął wymaganych efektów uczenia się. 3,0 – Student wykazuje braki, które jednak nie dyskwalifikują dalszej edukacji i mogą zostać usunięte. Zwykle wiadomości zestawione luźno, brak połączeń i związków logicznych. Rozwiązuje problemy typowe o niewielkim stopniu trudności. 3,5 – Student wykazuje poprawne rozumienie pojęć, wyjaśnia ważniejsze zjawiska. Rozwiązuje problemy typowe, przeważnie poprawnie operuje posiadanymi informacjami. 4,0 – Zakres wiedzy studenta obejmuje podstawowe treści przedmiotu ze znajomością powiązań logicznych. Poprawnie rozumuje w kategoriach przyczynowo-skutkowych. 4,5 – Wyczerpujące opanowanie całego materiału programowego. Student sprawnie wykorzystuje wiedzę. Umiejętnie dokonuje oceny problemów, procesów i zjawisk. 5,0 – Ponad przeciętne opanowanie całego materiału programowego. II. Pisemny/test Kryteria oceny efektów uczenia się: 2,0 – student nie osiągnął wymaganych efektów uczenia się (punktacja poniżej 50%). 3,0 – student osiągnął efekty uczenia się w stopniu dostatecznym (51 do 60%). 3,5 – student osiągnął efekty uczenia się w stopniu dostatecznym plus (61 do 70%). 4,0 – student osiągnął efekty uczenia się w stopniu dobrym (71 do 80%). 4,5 – student osiągnął efekty uczenia się w stopniu dobrym plus (81 do 90%). 5,0 – student osiągnął efekty uczenia się w stopniu bardzo dobrym (91 do 100%). III. Ustny/aktywność Kryteria oceny efektów uczenia się: 2,0 – Student niezaangażowany. 3,0 – Student pracuje niesystematycznie. 3,5 – Student przejawia przeciętną aktywność.

	4,0 – Student wykazuje dobre przygotowanie w sferze komunikacji i umiejętności interpersonalnych. Jest aktywny, podejmuje zadania dodatkowe. 4,5 – Student jest zainteresowany problematyką przedmiotu. Przejawia postawę racjonalną, krytyczną i kreatywną. 5,0 – Student twórczy w odpowiedzi, nie unika krytyki, posiada własne zdanie. Umiejętnie wyciąga wnioski. Jest aktywny, chętnie stawia pytania oraz problemy do dyskusji.
Literatura	1. Albrycht I., Autolitano S., Gęborys P. i in., Wyzwania w cyberprzestrzeni. Przykłady rozwiązań, zagrożenia, regulacje, Instytut Kościuszki, Kraków 2019. 2. Banasik M., Znaczenie nowoczesnych technologii dla bezpieczeństwa, „Rocznik Bezpieczeństwa Międzynarodowego" 2018, t. 12, nr 3. Sienkiewicz-Małyjurek K., Mozliwosci i problemy zastosowania sztucznej inteligencji w zarzadzaniu kryzysowym, [w:] Bezpieczenstwo. Teoria i praktyka, 2024, z. 1, s. 43 - 60
Bilans punktów ECTS	udział w wykładach = 26h udział w ćwiczeniach = 26h przygotowanie do ćwiczeń = 20h przygotowanie do kolokwium = 15h realizacja zadań projektowych = 15h kolokwium = 2h łączna liczba godzin: 104h w bezpośrednim kontakcie z prowadzącym 50% godzin liczba punktów ECTS = 4pkt. Minimalna ilość godzin nakładu pracy studenta 4 (pkt ECTS) x 26h = 104h

Forma oceny efektów uczenia się			
Efekty uczenia się	**Forma oceny**		
	Praktyczny	Pisemny	Ustny
W1	X	X	
W2	X	X	
W3	X		X
U1	X		X
U2	X	X	
U3			X
K1	X		X
K2			X
K3	X		X

<table>
<tr><td colspan="4">KARTA ZAJĘĆ</td></tr>
<tr><td colspan="4">Akademia Wychowania Fizycznego im. Jerzego Kukuczki w Katowicach
Wydział Zarządzania Sportem i Turystyką</td></tr>
<tr><td colspan="4">Zarządzanie studia I stopnia, profil ogólnoakademicki</td></tr>
<tr><td>Nazwa zajęć / nazwa grupy zajęć</td><td colspan="3">OCHRONA INFRASTRUKTURY KRYTYCZNEJ I ZARZĄDZANIE RYZYKIEM</td></tr>
<tr><td rowspan="12">Efekty uczenia się</td><td colspan="3">Wiedza</td></tr>
<tr><td>K_W01</td><td>W1</td><td>Ma zaawansowaną wiedzę na temat kluczowych pojęć i zależności występujących w procesie zarządzania ryzykiem oraz ochrony infrastruktury krytycznej.</td></tr>
<tr><td>K_W13</td><td>W2</td><td>Posiada zaawansowaną wiedzę dotyczącą funkcjonowania systemów bezpieczeństwa publicznego i zasad ochrony kluczowych zasobów państwa.</td></tr>
<tr><td>K_W07</td><td>W3</td><td>Rozumie wpływ otoczenia zewnętrznego i wewnętrznego na funkcjonowanie infrastruktury krytycznej oraz zagrożeń dla jej bezpieczeństwa.</td></tr>
<tr><td colspan="3">Umiejętności</td></tr>
<tr><td>K_U06</td><td>U1</td><td>Potrafi przeanalizować złożone problemy związane z zagrożeniami dla infrastruktury i wskazać możliwe działania naprawcze.</td></tr>
<tr><td>K_U10</td><td>U2</td><td>Potrafi projektować proces zarządzania ryzykiem w organizacjach z uwzględnieniem obowiązujących regulacji i dobrych praktyk.</td></tr>
<tr><td>K_U26</td><td>U3</td><td>Potrafi jasno i precyzyjnie formułować wypowiedzi ustne i pisemne dotyczące zagadnień związanych z bezpieczeństwem infrastruktury i ryzykiem</td></tr>
<tr><td colspan="3">Kompetencje społeczne</td></tr>
<tr><td>K_K05</td><td>K1</td><td>Potrafi odpowiedzialnie współpracować z członkami zespołu w zakresie przygotowania strategii ochrony infrastruktury krytycznej.</td></tr>
<tr><td>K_K09</td><td>K2</td><td>Identyfikuje dylematy etyczne i społeczne wynikające z zarządzania ryzykiem i podejmowania decyzji w sytuacjach kryzysowych.</td></tr>
<tr><td>K_K03</td><td>K3</td><td>Wykazuje gotowość do ciągłego aktualizowania wiedzy i kompetencji w obszarze bezpieczeństwa publicznego i zarzadzania.</td></tr>
<tr><td>Treści zajęć</td><td colspan="3">1. Wprowadzenie do zarządzania ryzykiem na potrzeby infrastruktury krytycznej
2. Etapy zarządzania ryzykiem.
3. Przygotowanie procesu zarzadzania ryzykiem na potrzeby infrastruktury krytycznej
4. Identyfikacja xródeł ryzyka na potrzeby infrastruktury krytycznej
5. Szacowanie wielkości prawdopodobieństwa i skutków zaistnienia zidentyfikowanych ryzyk dla infrastruktury krytycznej</td></tr>
</table>

	6. Podejmowanie działań związanych z ryzykiem dla infrastruktury krytycznej 7. Kontrola statusu zidentyfikowanych ryzyk dla infrastruktury krytycznej
Metody dydaktyczne	1. Wykład interaktywny z prezentacją multimedialną 2. Praca projektowa 3. Dyskusja moderowana 4. Test
Kryteria oceny efektów uczenia się	I. Praktyczny/projekt Kryteria oceny efektów uczenia się: 2,0 – Student nie osiągnął wymaganych efektów uczenia się. 3,0 – Student wykazuje braki, które jednak nie dyskwalifikują dalszej edukacji i mogą zostać usunięte. Zwykle wiadomości zestawione luźno, brak połączeń i związków logicznych. Rozwiązuje problemy typowe o niewielkim stopniu trudności. 3,5 – Student wykazuje poprawne rozumienie pojęć, wyjaśnia ważniejsze zjawiska. Rozwiązuje problemy typowe, przeważnie poprawnie operuje posiadanymi informacjami. 4,0 – Zakres wiedzy studenta obejmuje podstawowe treści przedmiotu ze znajomością powiązań logicznych. Poprawnie rozumuje w kategoriach przyczynowo-skutkowych. 4,5 – Wyczerpujące opanowanie całego materiału programowego. Student sprawnie wykorzystuje wiedzę. Umiejętnie dokonuje oceny problemów, procesów i zjawisk. 5,0 – Ponad przeciętne opanowanie całego materiału programowego. II. Pisemny/test Kryteria oceny efektów uczenia się: 2,0 – student nie osiągnął wymaganych efektów uczenia się (punktacja poniżej 50%). 3,0 – student osiągnął efekty uczenia się w stopniu dostatecznym (51 do 60%). 3,5 – student osiągnął efekty uczenia się w stopniu dostatecznym plus (61 do 70%). 4,0 – student osiągnął efekty uczenia się w stopniu dobrym (71 do 80%). 4,5 – student osiągnął efekty uczenia się w stopniu dobrym plus (81 do 90%). 5,0 – student osiągnął efekty uczenia się w stopniu bardzo dobrym (91 do 100%). III. Ustny/aktywność Kryteria oceny efektów uczenia się: 2,0 – Student niezaangażowany. 3,0 – Student pracuje niesystematycznie. 3,5 – Student przejawia przeciętną aktywność. 4,0 – Student wykazuje dobre przygotowanie w sferze komunikacji i umiejętności interpersonalnych. Jest aktywny, podejmuje zadania dodatkowe.

	4,5 – Student jest zainteresowany problematyką przedmiotu. Przejawia postawę racjonalną, krytyczną i kreatywną. 5,0 – Student twórczy w odpowiedzi, nie unika krytyki, posiada własne zdanie. Umiejętnie wyciąga wnioski. Jest aktywny, chętnie stawia pytania oraz problemy do dyskusji.
Literatura	1. Jakubiak E., *Ochrona infrastruktury krytycznej w Polsce*, „Zeszyty Naukowe SGSP" 2018,/1, s. 165 – 175. 2. Niedźwiecki-Zawiła J., *Metodyka analizy ryzyka w ochronie infrastruktury krytycznej państw*a, „Zeszyty Naukowe Uniwersytetu Szczecińskiego" 2014/65, s. 791 – 797 3. Molendowska M., Ostrowska M., Górski P., *Infrastruktura krytyczna jako element bezpieczeństwa: wymiar europejski i krajowy.* Toruń 2021.
Bilans punktów ECTS	udział w wykładach = 26h Udział w ćwiczeniach=13h przygotowanie do kolokwium = 10h realizacja zadań projektowych = 29h łączna liczba godzin: 78 h w bezpośrednim kontakcie z prowadzącym 50% godzin liczba punktów ECTS = 3 pkt. Minimalna ilość godzin nakładu pracy studenta 3(pkt ECTS) x 26h = 78h

Forma oceny efektów uczenia się			
Efekty uczenia się	**Forma oceny**		
	Praktyczny	Pisemny	Ustny
W1	X	X	
W2	X	X	
W3	X		X
U1	X		X
U2	X	X	
U3			X
K1	X		X
K2			X
K3	X		X

<table>
<tr><td colspan="4">KARTA ZAJĘĆ</td></tr>
<tr><td colspan="4">Akademia Wychowania Fizycznego im. Jerzego Kukuczki w Katowicach
Wydział Zarządzania Sportem i Turystyką</td></tr>
<tr><td colspan="4">Zarządzanie studia I stopnia, profil ogólnoakademicki</td></tr>
<tr><td>Nazwa zajęć / nazwa grupy zajęć</td><td colspan="3">NEGOCJACJE I MEDIACJE W ZARZĄDZANIU KRYZYSOWYM.</td></tr>
<tr><td rowspan="11">Efekty uczenia się</td><td colspan="3">Wiedza</td></tr>
<tr><td>K_W08</td><td>W1</td><td>Ma wiedzę o relacjach międzyludzkich, komunikacji społecznej oraz zasadach prowadzenia negocjacji i mediacji w sytuacjach kryzysowych.</td></tr>
<tr><td>K_W09</td><td>W2</td><td>Zna normy prawne i etyczne związane z prowadzeniem mediacji i negocjacji w sferze bezpieczeństwa publicznego.</td></tr>
<tr><td>K_W05</td><td>W3</td><td>Posiada wiedzę o strukturach społecznych oraz dynamice konfliktów w sytuacjach kryzysowych.</td></tr>
<tr><td colspan="3">Umiejętności</td></tr>
<tr><td>K_U08</td><td>U1</td><td>Potrafi przeprowadzić analizę sytuacji kryzysowej oraz dobrać odpowiednią strategię negocjacyjną lub mediacyjną.</td></tr>
<tr><td>K_U11</td><td>U2</td><td>Potrafi stosować techniki komunikacji werbalnej i niewerbalnej w procesie negocjacji i mediacji.</td></tr>
<tr><td>K_U26
P6S_UK</td><td>U3</td><td>Potrafi jasno i precyzyjnie formułować argumenty w mowie i piśmie, z uwzględnieniem dynamiki sytuacji kryzysowej.</td></tr>
<tr><td colspan="3">Kompetencje społeczne</td></tr>
<tr><td>K_K04</td><td>K1</td><td>Jest gotowy do pracy zespołowej i odpowiedzialnego pełnienia funkcji mediatora/negocjatora w grupie zadaniowej.</td></tr>
<tr><td>K_K09</td><td>K2</td><td>Rozpoznaje dylematy etyczne związane z komunikacją w sytuacjach wysokiego ryzyka i podejmuje działania zgodne z etyką zawodu.</td></tr>
<tr><td>K_K06</td><td>K3</td><td>Wykazuje gotowość do podejmowania wyzwań zawodowych w obszarze mediacji i negocjacji, również w warunkach stresu i napięcia.</td></tr>
<tr><td>Treści zajęć</td><td colspan="3">1. Pojęcia i definicje: negocjacja, mediacja, konflikt, zarządzanie kryzysem
2. Dekalog negocjatora kryzysowego – kluczowe zasady skutecznego działania
3. Rola i zadania mediatora w procesie rozwiązywania konfliktów kryzysowych
4. Regulacje prawne dotyczące negocjacji i mediacji – ustawy, standardy, etyka
5. Komunikacja werbalna i niewerbalna w procesie negocjacji i mediacji – analiza przypadków
6. Emocje, presja czasu i napięcie – jak wpływają na decyzje w negocjacjach</td></tr>
</table>

	7. Typowe błędy komunikacyjne i taktyki manipulacyjne – jak je rozpoznać i przeciwdziałać 8. Strategie negocjacyjne – twarda vs miękka linia, BATNA, modele hybrydowe 9. Ćwiczenia symulacyjne – scenariusze sytuacji kryzysowych
Metody dydaktyczne	1. Wykład interaktywny 2. Ćwiczenia symulacyjne (symulacje negocjacji i mediacji) 3. Praca w grupach (przygotowanie scenariuszy mediacyjnych) 4. Dyskusja moderowana 5. Test
Kryteria oceny efektów uczenia się	I. Praktyczny/projekt Kryteria oceny efektów uczenia się: 2,0 – Student nie osiągnął wymaganych efektów uczenia się. 3,0 – Student wykazuje braki, które jednak nie dyskwalifikują dalszej edukacji i mogą zostać usunięte. Zwykle wiadomości zestawione luźno, brak połączeń i związków logicznych. Rozwiązuje problemy typowe o niewielkim stopniu trudności. 3,5 – Student wykazuje poprawne rozumienie pojęć, wyjaśnia ważniejsze zjawiska. Rozwiązuje problemy typowe, przeważnie poprawnie operuje posiadanymi informacjami. 4,0 – Zakres wiedzy studenta obejmuje podstawowe treści przedmiotu ze znajomością powiązań logicznych. Poprawnie rozumuje w kategoriach przyczynowo-skutkowych. 4,5 – Wyczerpujące opanowanie całego materiału programowego. Student sprawnie wykorzystuje wiedzę. Umiejętnie dokonuje oceny problemów, procesów i zjawisk. 5,0 – Ponad przeciętne opanowanie całego materiału programowego. II. Pisemny/test Kryteria oceny efektów uczenia się: 2,0 – student nie osiągnął wymaganych efektów uczenia się (punktacja poniżej 50%). 3,0 – student osiągnął efekty uczenia się w stopniu dostatecznym (51 do 60%). 3,5 – student osiągnął efekty uczenia się w stopniu dostatecznym plus (61 do 70%). 4,0 – student osiągnął efekty uczenia się w stopniu dobrym (71 do 80%). 4,5 – student osiągnął efekty uczenia się w stopniu dobrym plus (81 do 90%). 5,0 – student osiągnął efekty uczenia się w stopniu bardzo dobrym (91 do 100%). III. Ustny/aktywność Kryteria oceny efektów uczenia się: 2,0 – Student niezaangażowany. 3,0 – Student pracuje niesystematycznie.

	3,5 – Student przejawia przeciętną aktywność. 4,0 – Student wykazuje dobre przygotowanie w sferze komunikacji i umiejętności interpersonalnych. Jest aktywny, podejmuje zadania dodatkowe. 4,5 – Student jest zainteresowany problematyką przedmiotu. Przejawia postawę racjonalną, krytyczną i kreatywną. 5,0 – Student twórczy w odpowiedzi, nie unika krytyki, posiada własne zdanie. Umiejętnie wyciąga wnioski. Jest aktywny, chętnie stawia pytania oraz problemy do dyskusji.
Literatura	1. Stawnicka J., *Negocjacje w sytuacjach kryzysowych Podręcznik dla studentów bezpieczeństwa wewnętrznego i narodowego*, Katowice: Wyd. AWF Katowice 2024. 2. *Jak prowadzić negocjacje kryzysowe. Dekalog negocjatora*. Zeszyty Naukowe Kujawskiej Szkoły Wyższej 2018/4, s. 137 – 154. 3. Stawnicka J., *Wykorzystanie strategii negocjacyjnych w celu zapewnienia bezpieczeństwa w sytuacjach o wysokim stopniu ryzyka – z perspektywy negocjacji policyjnych*. Wydawnictwo AWF Katowice: Katowice 2019. 4. Stawnicka J., *Bezpieczeństwo w negocjacjach kryzysowych*. *Między rytuałem, rutyną a kreatywnością.* Gliwice: WiS Opcjon, Uniwersytet Śląski 2013. 5. Stawnicka Jadwiga, *Police negotiations. Communicative strategies from the perspective of the theory of speech acts*., [w:] *Strategia bezpieczeństwa narodowego w ujęciu interdyscyplinarnym 3.0,* red. M. Kamper-Kubańska, K. Kaszlińńska, P.Sobierajski, Wydawnictwo Państwowej Akademii Nauk Stosowanych we Włocławku: Włocławek 2022, s. 171 – 186. 6. Tabernacka M., Negocjacje i mediacje w sferze publicznej, Warszawa: Wolters Kluwer 2018.
Bilans punktów ECTS	udział w wykładach = 26h Udział w ćwiczeniach=13h przygotowanie do kolokwium = 10h realizacja zadań projektowych = 29h łączna liczba godzin: 78 h w bezpośrednim kontakcie z prowadzącym 50% godzin liczba punktów ECTS = 3 pkt. Minimalna ilość godzin nakładu pracy studenta 3(pkt ECTS) x 26h = 78h

Forma oceny efektów uczenia się			
Efekty uczenia się	**Forma oceny**		
	Praktyczny	Pisemny	Ustny
W1	X	X	
W2	X	X	
W3	X		X
U1	X		X
U2	X		X
U3			X
K1	X		X
K2			X
K3	X		X

<table>
<tr><td colspan="4">KARTA ZAJĘĆ</td></tr>
<tr><td colspan="4">Akademia Wychowania Fizycznego im. Jerzego Kukuczki w Katowicach
Wydział Zarządzania Sportem i Turystyką</td></tr>
<tr><td colspan="4">Zarządzanie studia I stopnia, profil ogólnoakademicki</td></tr>
<tr><td>Nazwa zajęć / nazwa grupy zajęć</td><td colspan="3">TECHNIKI ATAKÓW I OBRONY W CYBERPRZESTRZENI</td></tr>
<tr><td rowspan="12">Efekty uczenia się</td><td colspan="3">Wiedza</td></tr>
<tr><td>K_W02</td><td>W1</td><td>Ma zaawansowaną wiedzę specjalistyczną z zakresu cyberbezpieczeństwa, w szczególności dotyczącą klasyfikacji cyberataków, ich przebiegu, skutków oraz charakterystyki zagrożeń związanych z infrastrukturą cyfrową.</td></tr>
<tr><td>K_W20</td><td>W2</td><td>Zna nowoczesne technologie i narzędzia ochrony systemów informatycznych</td></tr>
<tr><td>K_W12</td><td>W3</td><td>Posiada wiedzę na temat krajowego i międzynarodowego systemu bezpieczeństwa cyberprzestrzeni.</td></tr>
<tr><td colspan="3">Umiejętności</td></tr>
<tr><td>K_U21
P6S_UW</td><td>U1</td><td>Potrafi zastosować wybrane techniki i narzędzia informatyczne w zakresie identyfikacji zagrożeń i ochrony przed cyberatakami.</td></tr>
<tr><td>K_U22</td><td>U2</td><td>Potrafi analizować przypadki ataków i zaproponować odpowiednie działania zabezpieczające, zgodne z dobrymi praktykami.</td></tr>
<tr><td>K_U26</td><td>U3</td><td>Potrafi precyzyjnie i logicznie przedstawiać problemy związane z cyberbezpieczeństwem, zarówno ustnie, jak i pisemnie.</td></tr>
<tr><td colspan="3">Kompetencje społeczne</td></tr>
<tr><td>K_K06</td><td>K1</td><td>Jest gotów do podejmowania działań zespołowych w sytuacjach zagrożeń informacyjnych i infrastrukturalnych.</td></tr>
<tr><td>K_K09</td><td>K2</td><td>Rozpoznaje dylematy etyczne związane z bezpieczeństwem cyfrowym i przeciwdziałaniem przestępczości elektronicznej.</td></tr>
<tr><td>K_K04</td><td>K3</td><td>Posiada gotowość do systematycznego poszerzania wiedzy w zakresie nowych technik ataków i obrony w cyberprzestrzeni.</td></tr>
<tr><td></td><td colspan="3">1. Wprowadzenie do zagrożeń cybernetycznych – klasyfikacja ataków, przegląd aktualnych trendów
2. Ataki na urządzenia sieciowe– charakterystyka oraz strategie zabezpieczeń
3. Ransomware – analiza działania, przykłady, tworzenie polityki ochrony i backupu
4. Wykorzystanie luk systemowych – aktualizacje, dobre praktyki kodowania, zabezpieczenia warstwowe
5. Ataki DDoS – metody przeprowadzania, skutki i sposoby obrony (w tym rozwiązania chmurowe)</td></tr>
</table>

	6. Phishing i socjotechnika – metody ataku, rola edukacji użytkowników, rozwiązania antyspamowe 7. Advanced Persistent Threat (APT) – analiza zagrożeń i strategii długofalowych ataków 8. Infrastruktura bezpieczeństwa IT – firewalle, systemy detekcji zagrożeń, analiza logów
Metody dydaktyczne	1. Wykład z elementami multimedialnymi 2. Praca projektowa 3. Dyskusja problemowa 4. Test
Kryteria oceny efektów uczenia się	I. Praktyczny/projekt Kryteria oceny efektów uczenia się: 2,0 – Student nie osiągnął wymaganych efektów uczenia się. 3,0 – Student wykazuje braki, które jednak nie dyskwalifikują dalszej edukacji i mogą zostać usunięte. Zwykle wiadomości zestawione luźno, brak połączeń i związków logicznych. Rozwiązuje problemy typowe o niewielkim stopniu trudności. 3,5 – Student wykazuje poprawne rozumienie pojęć, wyjaśnia ważniejsze zjawiska. Rozwiązuje problemy typowe, przeważnie poprawnie operuje posiadanymi informacjami. 4,0 – Zakres wiedzy studenta obejmuje podstawowe treści przedmiotu ze znajomością powiązań logicznych. Poprawnie rozumuje w kategoriach przyczynowo-skutkowych. 4,5 – Wyczerpujące opanowanie całego materiału programowego. Student sprawnie wykorzystuje wiedzę. Umiejętnie dokonuje oceny problemów, procesów i zjawisk. 5,0 – Ponad przeciętne opanowanie całego materiału programowego. II. Pisemny/test Kryteria oceny efektów uczenia się: 2,0 – student nie osiągnął wymaganych efektów uczenia się (punktacja poniżej 50%). 3,0 – student osiągnął efekty uczenia się w stopniu dostatecznym (51 do 60%). 3,5 – student osiągnął efekty uczenia się w stopniu dostatecznym plus (61 do 70%). 4,0 – student osiągnął efekty uczenia się w stopniu dobrym (71 do 80%). 4,5 – student osiągnął efekty uczenia się w stopniu dobrym plus (81 do 90%). 5,0 – student osiągnął efekty uczenia się w stopniu bardzo dobrym (91 do 100%). III. Ustny/aktywność Kryteria oceny efektów uczenia się: 2,0 – Student niezaangażowany. 3,0 – Student pracuje niesystematycznie. 3,5 – Student przejawia przeciętną aktywność.

	4,0 – Student wykazuje dobre przygotowanie w sferze komunikacji i umiejętności interpersonalnych. Jest aktywny, podejmuje zadania dodatkowe. 4,5 – Student jest zainteresowany problematyką przedmiotu. Przejawia postawę racjonalną, krytyczną i kreatywną. 5,0 – Student twórczy w odpowiedzi, nie unika krytyki, posiada własne zdanie. Umiejętnie wyciąga wnioski. Jest aktywny, chętnie stawia pytania oraz problemy do dyskusji.
Literatura	1. Rot A., Olszewski B., Wybrane metody i narzędzia przeciwdziałania zaawansowanym atakom APT w cyberprzestrzeni, (PDF) Wybrane metody i narzędzia przeciwdziałania zaawansowanym atakom APT w cyberprzestrzeni; Selected Methods and Tools Preventing Advanced APT Attacks in Cyberspace 2. Kitler W., Chalubinska-Jentkiewicz, Badxmirowska-Masłowska, *System bezpieczeństwa w cyberprzestrzeni*, Warszawa 2024. 3. Alanezi M., „Phishing Detection Methods: A Review," Technium, tom 3, nr 9, pp. 19-35, 2021.
Bilans punktów ECTS	udział w wykładach = 26h Udział w ćwiczeniach=13h przygotowanie do kolokwium = 10h realizacja zadań projektowych = 29h łączna liczba godzin: 78 h w bezpośrednim kontakcie z prowadzącym 50% godzin liczba punktów ECTS = 3 pkt. Minimalna ilość godzin nakładu pracy studenta 3(pkt ECTS) x 26h = 78h

Forma oceny efektów uczenia się			
Efekty uczenia się	**Forma oceny**		
	Praktyczny	Pisemny	Ustny
W1	X	X	
W2	X	X	
W3	X		X
U1	X		X
U2	X	X	
U3			X
K1	X		X
K2			X
K3	X		X

<table>
<tr><td colspan="4">KARTA ZAJĘĆ</td></tr>
<tr><td colspan="4">Akademia Wychowania Fizycznego im. Jerzego Kukuczki w Katowicach
Wydział Zarządzania Sportem i Turystyką</td></tr>
<tr><td colspan="4">Zarządzanie studia I stopnia, profil ogólnoakademicki</td></tr>
<tr><td>Nazwa zajęć / nazwa grupy zajęć</td><td colspan="3">Aspekty lingwosecuritologiczne zarządzania kryzysowego</td></tr>
<tr><td rowspan="13">Efekty uczenia się</td><td colspan="3">Wiedza</td></tr>
<tr><td>K_W08
P6S_WG</td><td>W1</td><td>Ma wiedzę o relacjach międzyludzkich i procesach komunikacji społecznej w kontekście sytuacji kryzysowych oraz specyfice dyskursu bezpieczeństwa.</td></tr>
<tr><td>K_W09
P6S_WG</td><td>W2</td><td>Zna normy i zasady komunikacji instytucjonalnej oraz specjalistycznej z uwzględnieniem etyki języka w przestrzeni publicznej.</td></tr>
<tr><td>K_W03
P6S_WK</td><td>W3</td><td>Rozumie znaczenie języka jako narzędzia zarządzania społecznymi aspektami kryzysu oraz jako składnika dyskursu władzy i bezpieczeństwa</td></tr>
<tr><td colspan="3">Umiejętności</td></tr>
<tr><td>K_U08
P6S_UW</td><td>U1</td><td>Potrafi przeanalizować komunikaty językowe w kontekście bezpieczeństwa i wskazać ich wpływ na postawy i zachowania uczestników interakcji kryzysowych</td></tr>
<tr><td>K_U11
P6S_UO</td><td>U2</td><td>Stosuje strategie skutecznej i profesjonalnej komunikacji w sytuacjach kryzysowych, z uwzględnieniem mechanizmów językowego wpływu.</td></tr>
<tr><td>K_U26
P6S_UK</td><td>U3</td><td>Formułuje jasne, logiczne i etycznie poprawne komunikaty ustne i pisemne w kontekście zarządzania kryzysem i bezpieczeństwem informacji</td></tr>
<tr><td colspan="3">Kompetencje społeczne</td></tr>
<tr><td>K_K04
P6S_KO</td><td>K1</td><td>Jest gotów do podejmowania odpowiedzialnej współpracy zespołowej w warunkach komunikacji kryzysowej.</td></tr>
<tr><td>K_K09
P6S_KR</td><td>K2</td><td>Identyfikuje i rozumie dylematy etyczne w komunikacji instytucjonalnej i społecznej związanej z bezpieczeństwem.</td></tr>
<tr><td>K_K06
P6S_KR</td><td>K3</td><td>Wykazuje gotowość do pogłębiania wiedzy z zakresu języka bezpieczeństwa i świadomego kształtowania przekazów medialnych.</td></tr>
<tr><td>Treści zajęć</td><td colspan="3">1. Securitologia jako nauka o bezpieczeństwie człowieka i organizacji społecznych
2. Wyjaśnienie pojęcia lingwosecuritologia
3. Badania linwosecuritologiczne w literaturze przedmiotu</td></tr>
</table>

	4. Dyskurs kryzysowy a bezpieczeństwo uczestników interakcji 5. Język – narzędziem neutralizującym działanie mechanizmów hamujących agresję 6. Wykorzystanie wiedzy lingwistycznej w ramach działań na rzecz bezpieczeństwa i porządku publicznego 7. Profesjonalna komunikacja w sytuacjach kryzysowych 8. Aspekt pragmalingwistyczny dyskursu kryzysowego
Metody dydaktyczne	1. Wykład interaktywny z elementami analizy tekstu 2. Praca projektowa 3. Dyskusje moderowane 4. Prace grupowe – redagowanie komunikatów w sytuacjach symulowanych 5. Test
Kryteria oceny efektów uczenia się	I. Praktyczny/projekt Kryteria oceny efektów uczenia się: 2,0 – Student nie osiągnął wymaganych efektów uczenia się. 3,0 – Student wykazuje braki, które jednak nie dyskwalifikują dalszej edukacji i mogą zostać usunięte. Zwykle wiadomości zestawione luźno, brak połączeń i związków logicznych. Rozwiązuje problemy typowe o niewielkim stopniu trudności. 3,5 – Student wykazuje poprawne rozumienie pojęć, wyjaśnia ważniejsze zjawiska. Rozwiązuje problemy typowe, przeważnie poprawnie operuje posiadanymi informacjami. 4,0 – Zakres wiedzy studenta obejmuje podstawowe treści przedmiotu ze znajomością powiązań logicznych. Poprawnie rozumuje w kategoriach przyczynowo-skutkowych. 4,5 – Wyczerpujące opanowanie całego materiału programowego. Student sprawnie wykorzystuje wiedzę. Umiejętnie dokonuje oceny problemów, procesów i zjawisk. 5,0 – Ponad przeciętne opanowanie całego materiału programowego. II. Pisemny/test Kryteria oceny efektów uczenia się: 2,0 – student nie osiągnął wymaganych efektów uczenia się (punktacja poniżej 50%). 3,0 – student osiągnął efekty uczenia się w stopniu dostatecznym (51 do 60%). 3,5 – student osiągnął efekty uczenia się w stopniu dostatecznym plus (61 do 70%). 4,0 – student osiągnął efekty uczenia się w stopniu dobrym (71 do 80%).

	4,5 – student osiągnął efekty uczenia się w stopniu dobrym plus (81 do 90%). 5,0 – student osiągnął efekty uczenia się w stopniu bardzo dobrym (91 do 100%). III. Ustny/aktywność Kryteria oceny efektów uczenia się: 2,0 – Student niezaangażowany. 3,0 – Student pracuje niesystematycznie. 3,5 – Student przejawia przeciętną aktywność. 4,0 – Student wykazuje dobre przygotowanie w sferze komunikacji i umiejętności interpersonalnych. Jest aktywny, podejmuje zadania dodatkowe. 4,5 – Student jest zainteresowany problematyką przedmiotu. Przejawia postawę racjonalną, krytyczną i kreatywną. 5,0 – Student twórczy w odpowiedzi, nie unika krytyki, posiada własne zdanie. Umiejętnie wyciąga wnioski. Jest aktywny, chętnie stawia pytania oraz problemy do dyskusji.
Literatura	1. Stawnicka J., *Dyskurs o bezpieczeństwie z perspektywy lingwosecuritologii*. Wyd. Uniwersytetu Śląskiego. Katowice 2016. 2. Stawnicka J., *Lingwosecuritologia – istota i przedmiot badań*. W: *Świat za tekstem*. Red. J. Lubocha-Kruglik, O. Małysa. Katowice 2017, s. 477 – 487. 3. Stawnicka J., *Lingwosecuritologia. Diagnozy i prognozy.* W: *Odcienie bezpieczeństwa. Obszary badań, kierunki rozwoju.* Red. P. Polko, M. Walancik. Dąbrowa Górnicza 2016, s. 51 – 59.
Bilans punktów ECTS	udział w wykładach = 26h udział w ćwiczeniach = 26h przygotowanie do ćwiczeń = 20h przygotowanie do kolokwium = 15h realizacja zadań projektowych = 15h kolokwium = 2h łączna liczba godzin: 104h w bezpośrednim kontakcie z prowadzącym 50% godzin liczba punktów ECTS = 4pkt. Minimalna ilość godzin nakładu pracy studenta 4 (pkt ECTS) x 26h = 104h

Forma oceny efektów uczenia się			
Efekty uczenia się	**Forma oceny**		
	Praktyczny	Pisemny	Ustny
W1	X	X	
W2	X	X	
W3	X		X
U1	X		X
U2	X		X
U3			X
K1	X		X
K2			X
K3	X		X

<table>
<tr><td colspan="4">KARTA ZAJĘĆ</td></tr>
<tr><td colspan="4">Akademia Wychowania Fizycznego im. Jerzego Kukuczki w Katowicach
Wydział Zarządzania Sportem i Turystyką</td></tr>
<tr><td colspan="4">Zarządzanie studia I stopnia, profil ogólnoakademicki</td></tr>
<tr><td>Nazwa zajęć / nazwa grupy zajęć</td><td colspan="3">SYSTEM ZARZĄDZANIA KRYZYSOWEGO W POLSCE I NA ŚWIECIE</td></tr>
<tr><td rowspan="12">Efekty uczenia się</td><td colspan="3">Wiedza</td></tr>
<tr><td>K_W12</td><td>W1</td><td>Zna strukturę i zasady funkcjonowania systemów zarządzania kryzysowego w Polsce i innych krajach oraz instytucjonalne i prawne podstawy ich działania.</td></tr>
<tr><td>K_W07</td><td>W2</td><td>Rozumie znaczenie otoczenia międzynarodowego i geopolitycznego dla budowania odporności państwa na zagrożenia.</td></tr>
<tr><td>K_W05</td><td>W3</td><td>Posiada wiedzę na temat społecznych i organizacyjnych aspektów reagowania kryzysowego, w tym roli administracji i społeczeństwa obywatelskiego</td></tr>
<tr><td colspan="3">Umiejętności</td></tr>
<tr><td>K_U10</td><td>U1</td><td>Potrafi zidentyfikować zagrożenia i ocenić zdolność reagowania systemów zarządzania kryzysowego w różnych państwach.</td></tr>
<tr><td>K_U21</td><td>U2</td><td>Stosuje metody i narzędzia analityczne do oceny struktur bezpieczeństwa i efektywności działań kryzysowych.</td></tr>
<tr><td>K_U26</td><td>U3</td><td>Formułuje przejrzyste i logiczne wypowiedzi (pisemne i ustne) dotyczące rozwiązań organizacyjnych i prawnych w zarządzaniu kryzysowym.</td></tr>
<tr><td colspan="3">Kompetencje społeczne</td></tr>
<tr><td>K_K06</td><td>K1</td><td>Wykazuje gotowość do podejmowania działań w sytuacjach kryzysowych oraz odpowiedzialnej współpracy w zespole.</td></tr>
<tr><td>K_K09</td><td>K2</td><td>Rozpoznaje etyczne i społeczne dylematy związane z zarządzaniem kryzysowym i podejmowaniem decyzji pod presją.</td></tr>
<tr><td>K_K03</td><td>K3</td><td>Jest gotów do pogłębiania wiedzy o systemach bezpieczeństwa i politykach reagowania kryzysowego w wymiarze krajowym i globalnym</td></tr>
<tr><td>Treści zajęć</td><td colspan="3">1. Podstawy teoretyczne zarządzania kryzysowego – pojęcia, zakres, funkcje
2. System zarządzania kryzysowego w Polsce – struktura, akty prawne, instytucje
3. Modele zarządzania kryzysowego w wybranych państwach (USA, Niemcy, Szwecja, Izrael)
4. Rola administracji publicznej, służb i społeczeństwa w reagowaniu kryzysowym
5. Współpraca międzynarodowa – NATO, UE, ONZ w działaniach kryzysowych</td></tr>
</table>

	6. Fazy zarządzania kryzysowego – zapobieganie, przygotowanie, reagowanie, odbudowa 7. Systemy ostrzegania i informowania ludności (np. RCB, Alert Publiczny) 8. Analiza przypadków (pandemia, klęski żywiołowe, kryzys uchodźczy, cyberataki) 9. Odporność państwa i społeczeństwa – resilience jako paradygmat nowoczesnego zarządzania
Metody dydaktyczne	1. Wykład informacyjny z elementami interaktywnymi 2. Praca projektowa, praca grupowa 3. Dyskusje moderowane 4. Test
Kryteria oceny efektów uczenia się	I. Praktyczny/projekt Kryteria oceny efektów uczenia się: 2,0 – Student nie osiągnął wymaganych efektów uczenia się. 3,0 – Student wykazuje braki, które jednak nie dyskwalifikują dalszej edukacji i mogą zostać usunięte. Zwykle wiadomości zestawione luźno, brak połączeń i związków logicznych. Rozwiązuje problemy typowe o niewielkim stopniu trudności. 3,5 – Student wykazuje poprawne rozumienie pojęć, wyjaśnia ważniejsze zjawiska. Rozwiązuje problemy typowe, przeważnie poprawnie operuje posiadanymi informacjami. 4,0 – Zakres wiedzy studenta obejmuje podstawowe treści przedmiotu ze znajomością powiązań logicznych. Poprawnie rozumuje w kategoriach przyczynowo-skutkowych. 4,5 – Wyczerpujące opanowanie całego materiału programowego. Student sprawnie wykorzystuje wiedzę. Umiejętnie dokonuje oceny problemów, procesów i zjawisk. 5,0 – Ponad przeciętne opanowanie całego materiału programowego. II. Pisemny/test Kryteria oceny efektów uczenia się: 2,0 – student nie osiągnął wymaganych efektów uczenia się (punktacja poniżej 50%). 3,0 – student osiągnął efekty uczenia się w stopniu dostatecznym (51 do 60%). 3,5 – student osiągnął efekty uczenia się w stopniu dostatecznym plus (61 do 70%). 4,0 – student osiągnął efekty uczenia się w stopniu dobrym (71 do 80%). 4,5 – student osiągnął efekty uczenia się w stopniu dobrym plus (81 do 90%). 5,0 – student osiągnął efekty uczenia się w stopniu bardzo dobrym (91 do 100%). III. Ustny/aktywność Kryteria oceny efektów uczenia się:

	2,0 – Student niezaangażowany. 3,0 – Student pracuje niesystematycznie. 3,5 – Student przejawia przeciętną aktywność. 4,0 – Student wykazuje dobre przygotowanie w sferze komunikacji i umiejętności interpersonalnych. Jest aktywny, podejmuje zadania dodatkowe. 4,5 – Student jest zainteresowany problematyką przedmiotu. Przejawia postawę racjonalną, krytyczną i kreatywną. 5,0 – Student twórczy w odpowiedzi, nie unika krytyki, posiada własne zdanie. Umiejętnie wyciąga wnioski. Jest aktywny, chętnie stawia pytania oraz problemy do dyskusji.
Literatura	9. Wąsik K. *Międzynarodowe regulacje prawne dotyczące cyberprzestrzeni* „Cybersecurity and Law" 2023/2 .s. 133 – 155. 10. Skoczylas D., Cyberzagrożenia w cyberprzestrzeni. Cyberprzestępczość, cyberterroryznm i incydenty sieciowe „Prawo w działaniu. Sprawy karne" 2023/53, s/ 97-113. 11. Prawne i społeczne aspekty cyberbezpieczeństwa, red. S. Gwoździewicz, K. Tomaszycki, Warszawa 2017 12. Aleksandrowicz T., Bezpieczeństwo w cyberprzestrzeni ze stanowiska prawa międzynarodowego „Przegląd Bezpieczeństwa wewnętrznego" 2016/15, s. 11 - 26
Bilans punktów ECTS	udział w wykładach = 26h Udział w ćwiczeniach=13h przygotowanie do kolokwium = 10h realizacja zadań projektowych = 29h łączna liczba godzin: 78 h w bezpośrednim kontakcie z prowadzącym 50% godzin liczba punktów ECTS = 3 pkt. Minimalna ilość godzin nakładu pracy studenta 3(pkt ECTS) x 26h = 78h

Forma oceny efektów uczenia się			
Efekty uczenia się	**Forma oceny**		
	Praktyczny	Pisemny	Ustny
W1	X	X	
W2	X	X	
W3	X		X
U1	X		X
U2	X	X	
U3			X
K1	X		X
K2			X
K3	X		X