Akademia Marynarki Wojennej
im. Bohaterów Westerplatte
ul. Śmidowicza 69 81-127 Gdynia
tel. (+48) 261 26 25 14, fax. (+48) 261 26 29 63

Załącznik do uchwały nr 38/2022 Senatu Akademii Marynarki Wojennej im. Bohaterów Westerplatte z dnia 23 czerwca 2022 roku w sprawie ustalenia programu studiów podyplomowych Doctor of Business Administration na kierunku Zarządzanie cyberbezpieczeństwem i usługami cyfrowymi

WYDZIAŁ DOWODZENIA I OPERACJI MORSKICH

PROGRAM STUDIÓW PODYPLOMOWYCH DOCTOR OF BUSINESS ADMINISTRATION

KIERUNEK

ZARZĄDZANIE CYBERBEZPIECZEŃSTWEM I USŁUGAMI CYFROWYMI

GDYNIA

Czerwiec 2022

SPIS TREŚCI

1. OGÓLNA CHARAKTERYSTYKA STUDIÓW

1.1. Informacje podstawowe

Nazwa studiów podyplomowych	**Doctor of Business Administration** **Kierunek** **Zarządzanie Cyberbezpieczeństwem i Usługami Cyfrowymi**
Forma studiów	**niestacjonarne**
Łączna liczba godzin zajęć dydaktycznych	**176**
Czas trwania studiów	**2 semestry**
Liczba punktów ECTS konieczna do ukończenia studiów	**30**

Studia podyplomowe *Doctor of Business Administration* na kierunku *Zarządzanie Cyberbezpieczeństwem i Usługami Cyfrowymi*, realizowane przez Akademię Marynarki Wojennej w Gdyni w partnerstwie z Pocztą Polską S.A., stanowią kontynuację prowadzonych studiów podyplomowych *Executive Master of Business Administration* o tym samym kierunku. Wychodzą one naprzeciw oczekiwaniom w zakresie pogłębienia wiedzy i umiejętności wyższej kadry zarządzającej odpowiedzialnej za budowanie odporności podmiotów z sektora publicznego, militarnego i prywatnego na zagrożenia z cyberprzestrzeni. Celem studiów jest również rozwijanie umiejętności studentów w zakresie prowadzenia badań naukowych w dyscyplinie nauki o bezpieczeństwie ze szczególnym uwzględnieniem cyberbezpieczeństwa.

Studenci zdobędą wiedzę umożliwiającą rewizję istniejących paradygmatów, obejmującą podstawy teoretyczne oraz zagadnienia ogólne i wybrane zagadnienia szczegółowe dotyczące bezpieczeństwa, główne tendencje rozwojowe dyscypliny nauki o bezpieczeństwie, metodologię badań naukowych oraz zasady upowszechniania wyników działalności naukowej. Studenci zostaną zapoznani z fundamentalnymi dylematami cywilizacji cyfrowej oraz ekonomicznymi, prawnymi i etycznymi uwarunkowaniami prowadzenia działalności naukowej. Będą znali podstawowe zasady transferu wiedzy do sfery gospodarczej i społecznej oraz komercjalizacji wyników badań z zakresu zarządzania cyberbezpieczeństwem i usługami cyfrowymi.

Nowatorski program kształcenia pozwoli studentom nabyć umiejętności umożliwiające aktywne uczestnictwo w międzynarodowym środowisku naukowym oraz upowszechniać wyniki prowadzonej działalności naukowej. Będą oni potrafili inicjować debatę oraz

uczestniczyć w dyskursie naukowym dotyczącym zarządzania cyberbezpieczeństwem i usługami cyfrowymi. Nabędą również umiejętności planowania i realizacji indywidualnych i zespołowych przedsięwzięć badawczych zarówno w środowisku krajowym jak i międzynarodowym z wykorzystaniem zaawansowanych narzędzi analitycznych.

Kompleksowy system nauczania przygotuje studentów do krytycznej oceny dorobku w dyscyplinie nauki o bezpieczeństwie oraz uznawania znaczenia wiedzy w rozwiązywaniu problemów poznawczych i praktycznych dotyczących zarządzania cyberbezpieczeństwem i usługami cyfrowymi. Absolwenci zostaną zaznajomieni z zasadami prowadzenia działalności naukowej w sposób niezależny i respektowania własności wyników działalności naukowej, z uwzględnieniem zasad ochrony własności intelektualnej.

Studia realizowane są w formie studiów niestacjonarnych. Zajęcia dydaktyczne prowadzone są w strukturze roku akademickiego obejmującego 2 semestry (zimowy i letni) Rozpoczynają się w październiku i kończą się w czerwcu następnego roku kalendarzowego. Łączny bilans programowych zajęć dydaktycznych wynosi 176 godzin.

Szczegółowy tok i organizację procesu dydaktycznego w danym semestrze reguluje „Rozkład zajęć dydaktycznych dla grupy" opracowywany według aktualnego kalendarza. Zajęcia teoretyczne prowadzone są metodą audytoryjną z wykorzystaniem różnych technik audiowizualnych (w trybie stacjonarnym lub zdalnym), natomiast zajęcia praktyczne prowadzone są w oparciu o studia przypadków, ćwiczenia oraz pracę w laboratorium komputerowym. Cały proces dydaktyczny odbywa się przy aktywnym udziale studentów. Wiedza przekazywana jest przez wysokokwalifikowanych specjalistów, wykładowców oraz praktyków specjalizujących się w problematyce prowadzenia badań naukowych, zarządzania bezpieczeństwem narodowym oraz cyberbezpieczeństwa i usług cyfrowych.

Warunkiem ukończenia studiów jest spełnienie wszystkich wymagań określonych programem studiów oraz przygotowanie pracy końcowej w formie opracowania zawierającego koncepcję rozprawy doktorskiej, której problematyka obejmuje obszar szeroko rozumianego bezpieczeństwa narodowego, cyberbezpieczeństwa, usług cyfrowych i mieści się w dyscyplinie nauki o bezpieczeństwie. Dodatkowym wymogiem ukończenia studiów jest wydanie publikacji naukowej w recenzowanym czasopiśmie naukowym o zasięgu co najmniej krajowym.

1.2. Cele kształcenia

Studia podyplomowe *Doctor of Business Administration* na kierunku *Zarządzanie Cyberbezpieczeństwem i Usługami Cyfrowymi* w Akademii Marynarki Wojennej poszerzą dotychczasowe doświadczenia w tym zakresie wynikające z realizacji specjalności

Cybebrezpieczeństwo w ramach studiów cywilnych i wojskowych prowadzonych na kierunku *Systemy Informacyjne w Bezpieczeństwie*, studiów podyplomowych *Cyberbezpieczeństwo* oraz *studiów podyplomowych Executive Master of Business Administration na kierunku Zarządzanie Cyberbezpieczeństwem i Usługami Cyfrowymi*. Dodatkowo przyczynią się do rozwoju dalszej współpracy z Pocztą Polską S.A., która będzie pełniła nadzór merytoryczny nad studiami jako największa firma infrastrukturalna w Polsce, świadcząca w szerokim i coraz bardziej rozległym zakresie usługi cyfrowe.

Wykorzystując potencjał Akademii Marynarki Wojennej oraz Poczty Polskiej S.A. studenci pogłębią wiedzę z zakresu metodologii badań, zarządzania bezpieczeństwem narodowym, zarządzania cyberbezpieczeństwem oraz usługami cyfrowymi, która została szczegółowa omówiona w kartach przedmiotów (pkt. 3.1).

1.3. Potrzeby społeczno-gospodarcze

Studia podyplomowe *Doctor of Business Administration* na kierunku *Zarządzanie Cyberbezpieczeństwem i Usługami Cyfrowymi* to odpowiedź na zmiany rewolucjonizujące cyfrowe życie obywateli. Szybkość tych zmian czyni nas podatnymi na zagrożenia płynące z cyberprzestrzeni, co spowodowało, że ochrona przed nimi stanowi jeden z priorytetów polskiego rządu, czego efektem są zapisy w „Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2020". Zapisy te dotyczą m.in.:

- zwiększania poziomu odporności systemów informacyjnych wykorzystywanych w sferze publicznej i prywatnej oraz militarnej i cywilnej oraz osiągania zdolności do skutecznego zapobiegania, zwalczania oraz reagowania na cyberzagrożenia;
- wzmacniania defensywnego potencjału państwa poprzez zapewnienie ciągłego rozwoju krajowego systemu cyberbezpieczeństwa;
- uzyskania zdolności do prowadzenia pełnego spektrum działań militarnych w cyberprzestrzeni;
- rozwijania krajowych zdolności w obszarze testowania, badania, oceny i certyfikacji rozwiązań i usług z obszaru cyberbezpieczeństwa;
- rozwijania kompetencji, wiedzy oraz świadomości zagrożeń i wyzwań wśród kadr administracji publicznej oraz w społeczeństwie w obszarze cyberbezpieczeństwa;
- wzmacniania i rozbudowy potencjału państwa m.in. poprzez rozwój rodzimych rozwiązań w zakresie cyberbezpieczeństwa oraz prowadzenia finansowanych przez państwo prac badawczo-rozwojowych w obszarze nowoczesnych technologii, m.in. uczenia maszynowego, Internetu Rzeczy, szerokopasmowych sieci łączności

stacjonarnej i mobilnej (5G i kolejnych generacji), w tym także współpracy z uczelniami i instytucjami naukowymi oraz przedsiębiorstwami – zarówno z sektora publicznego, jak i prywatnego.

Studia podyplomowe *Doctor of Business Administration* na kierunku *Zarządzanie Cyberbezpieczeństwem i Usługami Cyfrowymi* doskonale wpisują się w wyżej określone działania umożliwiając studentom rozwijanie wiedzy i umiejętności w zakresie szeroko pojętego zarządzania cyberbezpieczeństwem oraz prowadzenia badań naukowych.

Należy również podkreślić, że obecnie brakuje tego typu studiów na polskim rynku, które dotyczą zarządzania cyberbezpieczeństwem i ukierunkowane są na badania naukowe.

1.4. Związek z misją uczelni i jej strategią rozwoju

Realizacja studiów podyplomowych *Doctor of Business Administration* na kierunku *Zarządzanie Cyberbezpieczeństwem i Usługami Cyfrowymi* jest bezpośrednio związana z procesem dydaktycznym i doskonaleniem zawodowym, a jednocześnie wpisuje się w treść Uchwały nr 5/2021 z dnia 21.01.2021 roku. Senat Akademii Marynarki Wojennej przyjął dokument pt. *„Strategia Akademii Marynarki Wojennej im. Bohaterów Westerplatte na lata 2021-2025”,* w której określone zostały cele strategiczne Akademii Marynarki Wojennej oraz działania zmierzające do osiągnięcia m. in. uzyskania wysokiej jakości i atrakcyjności kształcenia i szkolenia oraz dostosowania programów kształcenia do potrzeb krajowego, międzynarodowego rynku pracy i służb mundurowych.

Realizacja studiów podyplomowych *Doctor of Business Administration* na kierunku *Zarządzanie Cyberbezpieczeństwem i Usługami Cyfrowymi* umożliwia optymalizowanie i udoskonalenie oferty edukacyjnej Uczelni oraz uzyskiwanie wyższej pozycji w rankingu uczelni wyższych.

2. EFEKTY UCZENIA SIĘ

Studia, objęte niniejszym programem, adresowane są do przyszłych lub obecnych kierowników, menedżerów oraz osób zarządzających działalnością Operatorów Usług Kluczowych, podmiotów stanowiących Infrastrukturę Krytyczną Państwa oraz przedstawicieli administracji centralnej i służb, którzy posiadają tytuł zawodowy magistra lub magistra inżyniera i ukończyli studia podyplomowe *Executive Master of Business Administration na kierunku Zarządzanie Cyberbezpieczeństwem i Usługami Cyfrowymi*, realizowane przez Akademię Marynarki Wojennej w Gdyni w partnerstwie z Pocztą Polską S.A., studia podyplomowe *Master of Business Administration na kierunku Zarządzanie*

Cyberbezpieczeństwem realizowane przez Wojskową Akademię Techniczną w Warszawie lub studia podyplomowe *Master of Business Administration* o podobnym profilu. Kształcenie zakłada kreowanie postaw, nabywanie oraz korzystanie z wiedzy i doświadczeń określających podbudowę i reguły prawidłowego zarządzania infrastrukturą teleinformatyczną narażoną na rozmaite rodzaje cyberzagrożeń. Zakłada się także uzyskanie wiedzy i umiejętności przydatnych do samodzielnego rozwiązywania późniejszych problemów zawodowych i naukowych dotyczących zarządzania cyberbezpieczeństwem i usługami cyfrowymi umiejscowionych w problematyce bezpieczeństwa narodowego. Zdobywana wiedza i umiejętności będą weryfikowane podczas komisyjnej obrony koncepcji rozprawy doktorskiej, będącej podstawą ukończenia studiów.

Symbol	**Kierunkowe efekty uczenia się**	**Odniesienie do:** **- uniwersalnych charakterystyk pierwszego stopnia PRK** **- charakterystyk drugiego stopnia dla kwalifikacji na poziomie 8 PRK typowe dla kwalifikacji uzyskiwanych w ramach systemu szkolnictwa wyższego i nauki po uzyskaniu kwalifikacji pełnej na poziomie 7**
1	**2**	**3**
Wiedza		
ZCU_W01	Zna i rozumie w stopniu umożliwiającym rewizję istniejących paradygmatów – światowy dorobek, obejmujący podstawy teoretyczne oraz zagadnienia ogólne i wybrane z zakresu zarządzania bezpieczeństwem narodowym, zarządzania cyberbezpieczeństwem i usługami cyfrowymi	P8U_W, P8S_WG
ZCU_W02	Zna i rozumie główne tendencje rozwojowe oraz metodologię badań naukowych w dyscyplinie nauki o bezpieczeństwie	P8U_W, P8S_WG
ZCU_W03	Zna i rozumie nowoczesne narzędzia analityczne wykorzystywane w badaniach oraz zasady upowszechniania wyników działalności naukowej	P8U_W, P8S_WG
ZCU_W04	Zna i rozumie fundamentalne dylematy cywilizacji cyfrowej	P8U_W, P8S_WK
ZCU_W05	Zna i rozumie ekonomiczne, prawne, etyczne i inne uwarunkowania działalności naukowej w dyscyplinie nauki o bezpieczeństwie	P8U_W, P8S_WK
ZCU_W06	Zna i rozumie podstawowe zasady transferu wiedzy z zakresu zarządzania cyberbezpieczeństwem i usługami cyfrowymi do sfery gospodarczej i społecznej oraz komercjalizacji wyników działalności naukowej i know-how związanego z tymi wynikami	P8U_W, P8S_WK
Umiejętności		
ZCU_U01	Potrafi wykorzystać posiadaną wiedzę z zakresu zarządzania bezpieczeństwem narodowym, zarządzania	P8U_U, P8S_UW

	cyberbezpieczeństwem oraz usługami cyfrowymi do twórczego identyfikowania, formułowania i innowacyjnego rozwiązywania złożonych problemów lub wykonywania zadań o charakterze badawczym, a w szczególności: – definiować cel i przedmiot badań naukowych, formułować hipotezę badawczą; – rozwijać metody, techniki i narzędzia badawcze oraz twórczo je stosować; – wnioskować na podstawie wyników badań naukowych	
ZCU_U02	Potrafi dokonywać krytycznej analizy i oceny wyników badań naukowych, działalności eksperckiej i innych prac o charakterze twórczym oraz ich wkładu w rozwój wiedzy z zakresu zarządzania bezpieczeństwem narodowym, zarządzania cyberbezpieczeństwem i usługami cyfrowymi	P8U_U, P8S_UW
ZCU_U03	Potrafi transferować wyniki działalności naukowej do sfery gospodarczej i społecznej w zakresie zarządzania bezpieczeństwem narodowym i cyberbezpieczeństwa	P8U_U, P8S_UW
ZCU_U04	Potrafi komunikować się na tematy specjalistyczne w stopniu umożliwiającym aktywne uczestnictwo w międzynarodowym środowisku naukowym oraz upowszechniać wyniki działalności naukowej z zakresu zarządzania bezpieczeństwem narodowym, cyberbezpieczeństwa i usług cyfrowych	P8U_U, P8S_UK
ZCU_U05	Potrafi inicjować debatę i uczestniczyć w dyskursie naukowym z zakresu zarządzania bezpieczeństwem narodowym, cyberbezpieczeństwem i usługami cyfrowymi	P8U_U, P8S_UK
ZCU_U06	Potrafi planować i realizować indywidualne i zespołowe przedsięwzięcia badawcze lub twórcze, także w środowisku międzynarodowym, dotyczące zarządzania bezpieczeństwem narodowym, cyberbezpieczeństwa i usług cyfrowych	P8U_U, P8S_UO
ZCU_U07	Potrafi samodzielnie planować i działać na rzecz własnego rozwoju oraz inspirować i organizować rozwój innych osób w zakresie zarządzania bezpieczeństwem narodowym, cyberbezpieczeństwem i usługami cyfrowymi	P8U_U, P8S_UO
Kompetencje społeczne		
ZCU_K01	Krytycznie ocenia dorobek naukowy w ramach dyscypliny nauki o bezpieczeństwie ze szczególnym uwzględnieniem zarządzania cyberbezpieczeństwem i usługami cyfrowymi	P8U_K, P8S_KK
ZCU_K02	Uznaje znaczenie wiedzy w rozwiązywaniu problemów poznawczych i praktycznych z zakresu zarządzania bezpieczeństwem narodowym, cyberbezpieczeństwem i usługami cyfrowymi	P8U_K, P8S_KK
ZCU_K03	Jest przygotowany do inicjowania działań na rzecz interesu publicznego oraz myślenia i działania w sposób przedsiębiorczy w zakresie zarządzania bezpieczeństwem narodowym, cyberbezpieczeństwem i usługami cyfrowymi	P8U_K, P8S_KO
ZCU_K04	Jest przygotowany do prowadzenia działalności naukowej w sposób niezależny oraz respektowania zasady publicznej własności wyników działalności naukowej, z uwzględnieniem zasad ochrony własności intelektualnej	P8U_K, P8S_KR

Objaśnienie oznaczeń:

a) kody dla kierunkowych efektów uczenia się**:**

- **ZCU** – zakładany efekt uczenia się
- **W** – kategoria wiedzy
- **U** – kategoria umiejętności
- **K** – kategoria kompetencji społecznych
- **01, 02, 03** i kolejne – numer efektu uczenia się

b) charakterystyki poziomów PRK typowe dla kwalifikacji uzyskiwanych w ramach szkolnictwa wyższego (drugiego stopnia):

- **P** – poziom PRK (8)
- **W** –wiedza
  - **G** – zakres i głębia
  - **K** – kontekst
- **U** – umiejętności
  - **W** – wykorzystanie wiedzy
  - **K** – komunikowanie się
  - **O** – organizacja pracy
  - **U** – uczenie się
- **K** – kompetencje społeczne
  - **K** – oceny
  - **O** – odpowiedzialność
  - **R** – rola zawodowa

3. MODUŁY ZAJĘĆ

3.1. Karty przedmiotów

3.1.1 Badania nad bezpieczeństwem

K A R T A P R Z E D M I O T U		**AKADEMIA MARYNARKI WOJENNEJ WYDZIAŁ DOWODZENIA I OPERACJI MORSKICH**	

I.	**CHARAKTERYSTYKA PRZEDMIOTU**		
Nazwa przedmiotu:	**Badania nad bezpieczeństwem**	*Kod:*	**Tbz**
Kierunek studiów:	Zarządzanie cyberbezpieczeństwem i usługami cyfrowymi		
Poziom studiów:	Studia podyplomowe DBA		
Forma studiów:	Studia niestacjonarne		
Liczba ECTS:	6		
Semestr:	1, 2		
Wymagania wstępne:	-		
Język wykładowy:	polski		
Cel przedmiotu:	**C01**	zaznajomienie studentów z metodologią badań w bezpieczeństwie, etyką w badaniach, prawami autorskimi, upowszechnianiem i komercjalizacją wyników badań	
	C02	zaznajomienie studentów z wykorzystaniem metod statystycznych w badaniach nad bezpieczeństwem	

II.	**EFEKTY UCZENIA SIĘ**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Tbz_W01**	Znajomość głównych tendencji rozwojowych oraz metodologii badań naukowych w dyscyplinie nauki o bezpieczeństwie	Dyskusja
	Tbz_W02	Znajomość etyki w badaniach, praw autorskich, oraz zasad upowszechniania i komercjalizacji wyników badań	Dyskusja
	Tbz_W03	Znajomość metod statystycznych w badaniach nad bezpieczeństwem	Praca zaliczeniowa
Umiejętności:	**Tbz_U01**	Potrafi wykorzystać posiadaną wiedzę z zakresu zarządzania cyberbezpieczeństwem oraz usługami cyfrowymi do twórczego identyfikowania, formułowania i innowacyjnego rozwiązywania złożonych problemów lub wykonywania zadań o charakterze badawczym	Praca zaliczeniowa
	Tbz_U02	Potrafi dokonywać krytycznej analizy i oceny wyników badań naukowych, działalności eksperckiej i innych prac o charakterze twórczym oraz ich wkładu w rozwój wiedzy z zakresu zarządzania cyberbezpieczeństwem i usługami cyfrowymi	Dyskusja
	Tbz_U03	Potrafi transferować wyniki działalności naukowej do sfery gospodarczej i społecznej w zakresie cyberbezpieczeństwa i usług cyfrowych	Praca zaliczeniowa
Kompetencje społeczne:	**Tbz_K01**	Krytycznie ocenia dorobek naukowy w ramach dyscypliny nauki o bezpieczeństwie ze szczególnym uwzględnieniem zarządzania cyberbezpieczeństwem i usługami cyfrowymi	Dyskusja
	Tbz_K02	Jest przygotowany do prowadzenia działalności naukowej w sposób niezależny oraz respektowania zasady publicznej własności wyników działalności naukowej, z uwzględnieniem zasad ochrony własności intelektualnej	Dyskusja

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
W01	Metodologia badań	4

W02	Etyka	4
W03	Prawa autorskie	4
W04	Statystyka w badaniach	4
W05	Badania finansowane przez NCBiR	4
W06	Badania finansowane przez NCN	4
C01	Metodologia badań	4
C02	Statystyka w badaniach	12

IV. KORELACJA EFEKTÓW UCZENIA SIĘ

Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyki PRK*
W01	*Tbz_W01*	*ZCU_W02*	*P8U_W, P8S_WG*
W02	*Tbz_W02*	*ZCU_W06*	*P8U_W, P8S_WK*
W03	*Tbz_W02*	*ZCU_W06*	*P8U_W, P8S_WK*
W04	*Tbz_W03*	*ZCU_W03*	*P8U_W, P8S_WG*
W05	*Tbz_W02, Tbz_U03*	*ZCU_W05, ZCU_W06, ZCU_U03, ZCU_U06, ZCU_K03*	*P8U_W, P8S_WK, P8U_U, P8S_UW, P8S_UO, P8U_K, P8S_KO*
W06	*Tbz_W02, Tbz_U03*	*ZCU_W05, ZCU_W06, ZCU_U03, ZCU_U06, ZCU_K03*	*P8U_W, P8S_WK, P8U_U, P8S_UW, P8S_UO, P8U_K, P8S_KO*
C01	*Tbz_U01, Tbz_K01, Tbz_K02*	*ZCU_U01, ZCU_K04*	*P8U_U, P8S_UW, P8U_K, P8S_KK, P8U_K, P8S_KR*
C02	*Tbz_U02, Tbz_K02*	*ZCU_U02, ZCU_K01*	*P8U_U, P8S_UW, P8U_K, P8S_KK*

NAKŁAD PRACY STUDENTA

	Liczba godzin kontaktowych	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**24**	**X**	**150**	**6**
Ćwiczenia	**16**			
Konsultacje (zaliczenie nieobecności, rozliczenie rygorów, poprawy)	**2**			
Przygotowanie do ćwiczeń	**X**	**32**		
Opanowanie informacji		**36**		
Przygotowanie do rozliczenia rygorów		**40**		
RAZEM	**42**	**108**		

VI. METODY I NARZĘDZIA DYDAKTYCZNE

1.	Wykład informacyjny, wykład problemowy
2.	Konwersatorium, studium przypadku
3.	Ćwiczenia/Laboratoria

VII. FORMA ZALICZENIA PRZEDMIOTU

Rygor	*Kryteria składowe*	*Waga*
Zaliczenie	Wykonanie ćwiczeń	0,4
	Wykonanie pracy zaliczeniowej	0,6

VIII. LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

OBOWIĄZKOWA

1.	J. Gierszewski, A. Pieczywok, *Metodologiczne podstawy badania problemów bezpieczeństwa*, Difin, Warszawa, 2020
2.	*Kodeks Etyki Pracownika Naukowego*, Wyd. III, PAN, Warszawa 2020
3.	*Europejski kodeks postępowania w zakresie rzetelności badawczej*, Berlin 2020
	M. Poźniak-Niedzielska, J. Szczotka, *Prawo autorskie. Zarys problematyki*, Wolters Kluwer Polska, Warszawa, 2020
	M. Piłatowska, *Repetytorium ze statystyki*, Wydawnictwo Naukowe PWN, Warszawa, 2022

UZUPEŁNIAJĄCA

1.	Materiały przygotowane przez wykładowców
IX.	**PROWADZĄCY PRZEDMIOT**
Stopień, imię i nazwisko	dr. hab. Jarosław Teska + zespół
adres e-mail	j.teska@amw.gdynia.pl

3.1.2 Zarządzanie bezpieczeństwem narodowym

K A R T A P R Z E D M I O T U	**AKADEMIA MARYNARKI WOJENNEJ WYDZIAŁ DOWODZENIA I OPERACJI MORSKICH**	

I.	**CHARAKTERYSTYKA PRZEDMIOTU**		
Nazwa przedmiotu:	**Zarządzanie bezpieczeństwem narodowym**	*Kod:*	**Zbn**
Kierunek studiów:	Zarządzanie cyberbezpieczeństwem i usługami cyfrowymi		
Poziom studiów:	Studia podyplomowe DBA		
Forma studiów:	Studia niestacjonarne		
Liczba ECTS:	4		
Semestr:	1		
Wymagania wstępne:	Podstawowa wiedza z zakresu bezpieczeństwa narodowego		
Język wykładowy:	polski		
Cel przedmiotu:	**C01**	zaznajomienie studentów z problematyką bezpieczeństwa XXI wieku	
	C02	zaznajomienie studentów ze współczesnymi wyzwaniami polityki bezpieczeństwa UE i NATO	
	C03	zaznajomienie studentów z systemem bezpieczeństwa narodowego RP i umiejscowieniem w nim problematyki cyberbezpieczeństwa	

II.	**EFEKTY UCZENIA SIĘ**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Zbn_W01**	Znajomość podstawowych pojęć z zakresu bezpieczeństwa narodowego	Dyskusja
	Zbn_W02	Znajomość współczesnych wyzwań polityki bezpieczeństwa UE i NATO	Dyskusja
	Zbn_W03	Znajomość systemu bezpieczeństwa narodowego RP ze szczególnym uwzględnieniem elementów cyberbezpieczeństwa	Dyskusja
Umiejętności:	**Zbn_U01**	Potrafi wykorzystywać posiadaną wiedzę z zakresu zarządzania bezpieczeństwem narodowym do twórczego identyfikowania, formułowania i innowacyjnego rozwiązywania złożonych problemów lub wykonywania zadań o charakterze badawczym	Dyskusja
	Zbn_U02	Potrafi planować i realizować indywidualne i zespołowe przedsięwzięcia badawcze lub twórcze, także w środowisku międzynarodowym dotyczące problematyki bezpieczeństwa	Praca zaliczeniowa
Kompetencje społeczne:	**Zbn_K01**	Uznaje znaczenie wiedzy w rozwiązywaniu problemów poznawczych i praktycznych z zakresu zarządzania bezpieczeństwem narodowym	Dyskusja
	Zbn_K02	Jest przygotowany do inicjowania działań na rzecz interesu publicznego oraz myślenia i działania w sposób przedsiębiorczy w zakresie zarządzania bezpieczeństwem narodowym	Dyskusja

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
W01	Środowisko bezpieczeństwa XXI wieku	4
W02	Współczesne wyzwania polityki bezpieczeństwa UE i NATO	4
W03	System bezpieczeństwa narodowego RP	4
C01	System bezpieczeństwa narodowego RP	4

IV.	**KORELACJA EFEKTÓW UCZENIA SIĘ**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyki PRK*
W01	*Zbn_W01, Zbn_U01*	*ZCU_W01, ZCU_W04, ZCU_U01*	*P8U_W, P8S_WG, P8U_W, P8S_WK, P8U_U, P8S_UW,*
W02	*Zbn_W02, Zbn_U01*	*ZCU_W01, ZCU_W04, ZCU_U01*	*P8U_W, P8S_WG, P8U_W, P8S_WK, P8U_U, P8S_UW,*
W03	*Zbn_W03, Zbn_U01*	*ZCU_W01, ZCU_W04,*	*P8U_W, P8S_WG, P8U_W,*

		ZCU_U01	*P8S_WK, P8U_U, P8S_UW,*
C01	*Zbn_W03, Zbn_U02, Zbn_K01, Zbn_K02*	*ZCU_W01, ZCU_U06, ZCU_K02, ZCU_K03*	*P8U_W, P8S_WG, P8U_U, P8S_UO, P8U_K, P8S_KK, P8U_K, P8S_KO*

NAKŁAD PRACY STUDENTA

	Liczba godzin kontaktowych	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**12**	**X**	**100**	**4**
Ćwiczenia	**4**			
Konsultacje (zaliczenie nieobecności, rozliczenie rygorów, poprawy)	**2**			
Przygotowanie do ćwiczeń	**X**	**20**		
Opanowanie informacji		**40**		
Przygotowanie do rozliczenia rygorów		**22**		
RAZEM	**18**	**82**		

VI. METODY I NARZĘDZIA DYDAKTYCZNE

1. Wykład informacyjny, wykład problemowy
2. Konwersatorium
3. Ćwiczenia

VII. FORMA ZALICZENIA PRZEDMIOTU

Rygor	*Kryteria składowe*	*Waga*
Zaliczenie	Wykonanie ćwiczeń	0,4
	Przygotowanie pracy zaliczeniowej	0,6

VIII. LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

OBOWIĄZKOWA

1.
2. A. Wejkszner (red.), S. Wojciechowski, *Współczesne bezpieczeństwo Polski. Międzynarodowy wymiar instytucjonalny*, Difin, Warszawa, 2019
3. *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2020*

UZUPEŁNIAJĄCA

1. Materiały przygotowane przez wykładowców

IX. PROWADZĄCY PRZEDMIOT

Stopień, imię i nazwisko	dr hab. Bartłomiej Pączek+ zespół
adres e-mail	b.paczek@amw.gdynia.pl

3.1.3 Zarządzanie cyberbezpieczeństwem

K A R T A P R Z E D M I O T U	**AKADEMIA MARYNARKI WOJENNEJ WYDZIAŁ DOWODZENIA I OPERACJI MORSKICH**	

I.	**CHARAKTERYSTYKA PRZEDMIOTU**		
Nazwa przedmiotu:	**Zarządzanie cyberbezpieczeństwem**	*Kod:*	**Lxe**
Kierunek studiów:	Zarządzanie cyberbezpieczeństwem i usługami cyfrowymi		
Poziom studiów:	Studia podyplomowe DBA		
Forma studiów:	Studia niestacjonarne		
Liczba ECTS:	10		
Semestr:	1, 2		
Wymagania wstępne:	Zaawansowana wiedza z zakresu cyberbezpieczeństwa		
Język wykładowy:	polski		
Cel przedmiotu:	**C01**	usystematyzowanie wiedzy z zakresu aparatu pojęciowego cyberbezpieczeństwa	
	C02	zaznajomienie studentów z metodami monitorowania cyberprzestrzeni oraz budowania świadomości w zakresie cyberbezpieczeństwa	
	C03	pogłębienie wiedzy studentów z zakresu zarządzania cyberbezpieczeństwem	

II.	**EFEKTY UCZENIA SIĘ**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Lxe_W01**	Znajomość podstaw teoretycznych oraz zagadnień ogólnych i wybranych z zakresu cyberbezpieczeństwa	Dyskusja
	Lxe_W02	Znajomość nowoczesnych narzędzi analitycznych wykorzystywanych w badaniach z zakresu cyberbezpieczeństwa	Dyskusja
	Lxe_W03	Znajomość procesu zarządzania cyberbezpieczeństwem	Dyskusja
Umiejętności:	**Lxe_U01**	Potrafi dokonywać krytycznej analizy i oceny wyników badań naukowych, działalności eksperckiej i innych prac o charakterze twórczym oraz ich wkładu w rozwój wiedzy z zakresu zarządzania cyberbezpieczeństwem	Dyskusja
	Lxe_U02	Potrafi komunikować się na tematy specjalistyczne w stopniu umożliwiającym aktywne uczestnictwo w międzynarodowym środowisku naukowym oraz upowszechniać wyniki działalności naukowej z zakresu zarządzania cyberbezpieczeństwem	Dyskusja
	Lxe_U03	Potrafi inicjować debatę i uczestniczyć w dyskursie naukowym z zakresu zarządzania cyberbezpieczeństwem	Dyskusja
	Lxe_U04	Potrafi planować i realizować indywidualne i zespołowe przedsięwzięcia badawcze lub twórcze, także w środowisku międzynarodowym, dotyczące zarządzania cyberbezpieczeństwem	Praca zaliczeniowa
Kompetencje społeczne:	**Lxe_K01**	Krytycznie ocenia dorobek naukowy w ramach dyscypliny nauki o bezpieczeństwie ze szczególnym uwzględnieniem zarządzania cyberbezpieczeństwem	Dyskusja
	Lxe_K02	Uznaje znaczenie wiedzy w rozwiązywaniu problemów poznawczych i praktycznych z zakresu zarządzania cyberbezpieczeństwem	Dyskusja
	Lxe_K03	Jest przygotowany do inicjowania działań na rzecz interesu publicznego oraz myślenia i działania w sposób przedsiębiorczy w zakresie zarządzania cyberbezpieczeństwem	Dyskusja

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
W01	Paradygmaty cyberbezpieczeństwa	6
W02	Krajowy System Cyberbezpieczeństwa	8
W03	Monitoring cyberbezpieczeństwa (Microsoft)	2

W04	Monitoring cyberbezpieczeństwa (CISCO)	2
W05	Rekonesans w cyberprzestrzeni	4
W06	Dojrzałość systemów zarządzania bezpieczeństwem informacji	8
W07	Budowa i weryfikacja scenariuszy reakcji na cyberincydenty	4
W08	AI w cyberbezpieczeństwie	4
C01	Paradygmaty cyberbezpieczeństwa	2
C02	Monitoring cyberbezpieczeństwa (Microsoft)	6
C03	Monitoring cyberbezpieczeństwa (CISCO)	6
C04	Programy budowania świadomości w zakresie cyberbezpieczeństwa	4

IV. KORELACJA EFEKTÓW UCZENIA SIĘ

Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyki PRK*
W01	*Lxe_W01*	*ZCU_W01, ZCU_W03*	*P8U_W, P8S_WG*
W02	*Lxe_W01, Lxe_K03*	*ZCU_W01, ZCU_W03, ZCU_K03*	*P8U_W, P8S_WG, P8U_K, P8S_KO*
W03	*Lxe_W02*	*ZCU_W01, ZCU_W03*	*P8U_W, P8S_WG*
W04	*Lxe_W02*	*ZCU_W01, ZCU_W03*	*P8U_W, P8S_WG*
W05	*Lxe_W02, Lxe_U02, Lxe_K03*	*ZCU_W01, ZCU_W03, ZCU_U04, ZCU_K03*	*P8U_W, P8S_WG, P8U_U, P8S_UK, P8U_K, P8S_KO*
W06	*Lxe_W03, Lxe_U02*	*ZCU_W01, ZCU_W03, ZCU_U04*	*P8U_W, P8S_WG, P8S_UK*
W07	*Lxe_W03, Lxe_U02, Lxe_K03*	*ZCU_W01, ZCU_W03, ZCU_U04, ZCU_K03*	*P8U_W, P8S_WG, P8S_UK, P8U_K, P8S_KO*
W08	*Lxe_W03, Lxe_U02*	*ZCU_W01, ZCU_W03, ZCU_U04*	*P8U_W, P8S_WG, P8S_UK*
C01	*Lxe_U01, Lxe_K01*	*ZCU_U02, ZCU_K01,*	*P8U_U, P8S_UW, P8U_K, P8S_KK*
C02	*Lxe_U04, Lxe_K02*	*ZCU_U06, ZCU_K02*	*P8U_U, P8S_UO, P8U_K, P8S_KK*
C03	*Lxe_U04, Lxe_K02*	*ZCU_U06, ZCU_K02*	*P8U_U, P8S_UO, P8U_K, P8S_KK*
C04	*Lxe_W03, Lxe_U03*	*ZCU_W01, ZCU_U05*	*P8U_W, P8S_WG, P8U_U, P8S_UK*

V. NAKŁAD PRACY STUDENTA

Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**38**	**X**	**250**	**10**
Ćwiczenia	**18**			
Konsultacje (zaliczenie nieobecności, rozliczenie rygorów, poprawy)	**2**			
Przygotowanie do ćwiczeń	**X**	**50**		
Opanowanie informacji		**100**		
Przygotowanie do rozliczenia rygorów		**42**		
RAZEM	**58**	**192**		

VI. METODY I NARZĘDZIA DYDAKTYCZNE

1.	Wykład informacyjny, wykład problemowy
2.	Konwersatorium, studium przypadku
3.	Ćwiczenia/Laboratoria

VII. FORMA ZALICZENIA PRZEDMIOTU

Rygor	*Kryteria składowe*	*Waga*
Zaliczenie	Wykonanie ćwiczeń	0,4
	Wykonanie pracy zaliczeniowej	0,6

VIII. LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

OBOWIĄZKOWA	
1.	J. Kosiński, *Paradygmaty cyberprzestępczości*, Difin, Warszawa 2015
2.	*Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa*
3.	D. Dylski i inni, *Księga dobrych praktyk w zakresie zarządzania ciągłością działania,* ZBP, Warszawa 2012
4.	K. Liderman, *Bezpieczeństwo informacyjne. Nowe wyzwania*, PWN, Warszawa 2017
UZUPEŁNIAJĄCA	
1.	Materiały przygotowane przez wykładowców
IX.	**PROWADZĄCY PRZEDMIOT**
Stopień, imię i nazwisko	dr inż. Jakub Syta + zespół
adres e-mail	j.syta@amw.gdynia.pl

3.1.4 Zarządzanie usługami cyfrowymi

K A R T A P R Z E D M I O T U	AKADEMIA MARYNARKI WOJENNEJ WYDZIAŁ DOWODZENIA I OPERACJI MORSKICH	

I.	CHARAKTERYSTYKA PRZEDMIOTU		
Nazwa przedmiotu:	**Zarządzanie usługami cyfrowymi**	*Kod:*	**Lxf**
Kierunek studiów:	Zarządzanie cyberbezpieczeństwem i usługami cyfrowymi		
Poziom studiów:	Studia podyplomowe DBA		
Forma studiów:	Studia niestacjonarne		
Liczba ECTS:	8		
Semestr:	1, 2		
Wymagania wstępne:	Zaawansowana wiedza z zakresu usług cyfrowych		
Język wykładowy:	polski		
Cel przedmiotu:	**C01**	pogłębienie wiedzy studentów na temat wybranych zagadnień z zakresu realizacji usług cyfrowych	
	C02	zaznajomienie studentów z fundamentalnymi dylematami cywilizacji cyfrowej	

II.	EFEKTY UCZENIA SIĘ		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Lxf_W01**	Znajomość zagadnień ogólnych i wybranych z zakresu zarządzania usługami cyfrowymi	Dyskusja
	Lxf_W02	Znajomość fundamentalnych dylematów cywilizacji cyfrowej	Dyskusja
Umiejętności:	**Lxf_U01**	Potrafi dokonywać krytycznej analizy i oceny wyników badań naukowych, działalności eksperckiej i innych prac o charakterze twórczym oraz ich wkładu w rozwój wiedzy z zakresu zarządzania usługami cyfrowymi	Dyskusja
	Lxf_U02	Potrafi komunikować się na tematy specjalistyczne w stopniu umożliwiającym aktywne uczestnictwo w międzynarodowym środowisku naukowym oraz upowszechniać wyniki działalności naukowej z zakresu zarządzania usługami cyfrowymi	Dyskusja
	Lxf_U03	Potrafi inicjować debatę i uczestniczyć w dyskursie naukowym z zakresu zarządzania usługami cyfrowymi	
	Lxf_U04	Potrafi planować i realizować indywidualne i zespołowe przedsięwzięcia badawcze lub twórcze, także w środowisku międzynarodowym, dotyczące zarządzania usługami cyfrowymi	Praca zaliczeniowa
Kompetencje społeczne:	**Lxf_K01**	Krytycznie ocenia dorobek naukowy w ramach dyscypliny nauki o bezpieczeństwie ze szczególnym uwzględnieniem zarządzania usługami cyfrowymi	Dyskusja
	Lxf_K02	Uznaje znaczenie wiedzy w rozwiązywaniu problemów poznawczych i praktycznych z zakresu zarządzania usługami cyfrowymi	Dyskusja
	Lxf_K03	Jest przygotowany do inicjowania działań na rzecz interesu publicznego oraz myślenia i działania w sposób przedsiębiorczy w zakresie zarządzania usługami cyfrowymi	Dyskusja

III.	TREŚCI PROGRAMOWE	
Forma	*Tematyka*	*Liczba godzin*
W01	Weryfikowanie poziomu gotowości na przypadki utraty ciągłości działania	4
W02	Budowanie i rozwijanie strategii korporacyjnej	4
W03	Narzędzia typu GRC (Governance, Risk & Control)	4
W04	Zarządzanie projektami i programami	4
W05	Modele współpracy ze startupami	4
W06	Umowy dotyczące cyberbezpieczeństwa	4
W07	Odpowiedzialność za niedochowanie należytej staranności	4

W08	Dylematy cywilizacji cyfrowej	4
C01	Weryfikowanie poziomu gotowości na przypadki utraty ciągłości działania	4
C02	Budowanie i rozwijanie strategii korporacyjnej	4
C03	Narzędzia typu GRC (Governance, Risk & Control)	4
C04	Zarządzanie projektami i programami	4

IV. KORELACJA EFEKTÓW UCZENIA SIĘ

Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyki PRK*
W01	*Lxf_W01*	*ZCU_W01*	*P8U_W, P8S_WG*
W02	*Lxf_W01, Lxf_U03*	*ZCU_W01, ZCU_U05*	*P8U_W, P8S_WG, P8U_U, P8S_UK*
W03	*Lxf_W01, Lxf_K01*	*ZCU_W01, ZCU_K01*	*P8U_W, P8S_WG, P8U_K, P8S_KK*
W04	*Lxf_W01*	*ZCU_W01*	*P8U_W, P8S_WG*
W05	*Lxf_W01, Lxf_U03, Lxf_K03*	*ZCU_W01, ZCU_U05, ZCU_K03*	*P8U_W, P8S_WG, P8U_U, P8S_UK, P8U_K, P8S_KO*
W06	*Lxf_W01, Lxf_K03*	*ZCU_W01, ZCU_K03*	*P8U_W, P8S_WG, P8U_K, P8S_KO*
W07	*Lxf_W01, Lxf_U03*	*ZCU_W01, ZCU_U05*	*P8U_W, P8S_WG, P8U_U, P8S_UK*
W08	*Lxf_W02, Lxf_U01, Lxf_U03, Lxf_K02*	*ZCU_W04, ZCU_U02, ZCU_U05, ZCU_K02*	*P8U_W, P8S_WK, P8U_U, P8S_UW, P8U_K, P8S_KK*
C01	*Lxf_U02, Lxf_U04*	*ZCU_U04, ZCU_U06*	*P8U_U, P8S_UK, P8U_U, P8S_UO*
C02	*Lxf_U02, Lxf_U04*	*ZCU_U04, ZCU_U06*	*P8U_U, P8S_UK, P8U_U, P8S_UO*
C03	*Lxf_U02*	*ZCU_U04*	*P8U_U, P8S_UK*
C04	*Lxf_U02*	*ZCU_U04*	*P8U_U, P8S_UK*

V. NAKŁAD PRACY STUDENTA

Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**32**	**X**	**200**	**8**
Ćwiczenia	**16**			
Konsultacje (zaliczenie nieobecności, rozliczenie rygorów, poprawy)	**2**			
Przygotowanie do ćwiczeń	**X**	**40**		
Opanowanie informacji		**60**		
Przygotowanie do rozliczenia rygorów		**50**		
RAZEM	**50**	**150**		

VI. METODY I NARZĘDZIA DYDAKTYCZNE

1.	Wykład informacyjny, wykład problemowy
2.	Konwersatorium, studium przypadku
3.	Ćwiczenia

VII. FORMA ZALICZENIA PRZEDMIOTU

Rygor	*Kryteria składowe*	*Waga*
Zaliczenie	Wykonanie ćwiczeń	0,4
	Wykonanie pracy zaliczeniowej	0,6

VIII. LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

OBOWIĄZKOWA

1.	*NIST Special Publication 800-82,Guide to Industrial Control Systems (ICS) Security rev.2*
2.	*GRC Capability Model (Condensed Red Book) – OCEG*
3.	*GTAG® 17 - Audytowanie ładu informatycznego - https://www.iia.org.pl/publikacje/gtagr-17-audytowanie-ladu-informatycznego*
4.	*GTAG® 4 - Zarządzanie Audytem IT - https://www.iia.org.pl/publikacje/gtagr-4-zarzadzanie-audytem-it*

UZUPEŁNIAJĄCA	
1.	Materiały przygotowane przez wykładowców
IX.	**PROWADZĄCY PRZEDMIOT**
Stopień, imię i nazwisko	dr hab. Jerzy Kosiński+ zespół
adres e-mail	j.kosinski@amw.gdynia.pl

3.1.5 Seminarium dyplomowe

K A R T A P R Z E D M I O T U	**AKADEMIA MARYNARKI WOJENNEJ WYDZIAŁ DOWODZENIA I OPERACJI MORSKICH**	

I.	**CHARAKTERYSTYKA PRZEDMIOTU**		
Nazwa przedmiotu:	**Seminarium dyplomowe**	*Kod:*	**Ax**
Kierunek studiów:	Zarządzanie cyberbezpieczeństwem i usługami cyfrowymi		
Poziom studiów:	Studia podyplomowe DBA		
Forma studiów:	Studia niestacjonarne		
Liczba ECTS:	2		
Semestr:	1, 2		
Wymagania wstępne:	-		
Język wykładowy:	polski		
Cel przedmiotu:	**C01**	przygotowanie studentów do prowadzenia dyskusji naukowej	
	C02	przygotowanie publikacji wyników badań wstępnych	
	C03	przygotowanie koncepcji rozprawy doktorskiej	

II.	**EFEKTY UCZENIA SIĘ**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Ax_W01**	Znajomość podstaw teoretycznych oraz zagadnień ogólnych i wybranych z zakresu zarządzania bezpieczeństwem narodowym, zarządzania cyberbezpieczeństwem i usługami cyfrowymi	Dyskusja
Umiejętności:	**Ax_U01**	Potrafi komunikować się na tematy specjalistyczne w stopniu umożliwiającym aktywne uczestnictwo w międzynarodowym środowisku naukowym oraz upowszechniać wyniki działalności naukowej z zakresu zarządzania bezpieczeństwem narodowym, cyberbezpieczeństwem i usługami cyfrowymi	Dyskusja
Kompetencje społeczne:	**Ax_K01**	Krytycznie ocenia dorobek naukowy w ramach dyscypliny nauki o bezpieczeństwie ze szczególnym uwzględnieniem zarządzania cyberbezpieczeństwem i usługami cyfrowymi	Dyskusja

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
C01	Wybór tematyki doktoratu oraz publikacji naukowych	4
C02	Prezentacja wyników badań wstępnych	4
C03	Prezentacja publikacji naukowych	4
C04	Prezentacja koncepcji doktoratu	

IV.	**KORELACJA EFEKTÓW UCZENIA SIĘ**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyki PRK*
C01	*Ax_W01, Ax_U01, Ax_K01*	*ZCU_W01, ZCU_U04, ZCU_U07, ZCU_K01*	*P8U_W, P8S_WG, P8U_U, P8S_UK, P8S_UO, P8U_K, P8S_KK*
C02	*Ax_W01, Ax_U01, Ax_K01*	*ZCU_W01, ZCU_U04, ZCU_U07, ZCU_K01*	*P8U_W, P8S_WG, P8U_U, P8S_UK, P8S_UO, P8U_K, P8S_KK*
C03	*Ax_W01, Ax_U01, Ax_K01*	*ZCU_W01, ZCU_U04, ZCU_U07, ZCU_K01*	*P8U_W, P8S_WG, P8U_U, P8S_UK, P8S_UO, P8U_K, P8S_KK*
C04	*Ax_W01, Ax_U01, Ax_K01*	*ZCU_W01, ZCU_U04, ZCU_U07, ZCU_K01*	*P8U_W, P8S_WG, P8U_U, P8S_UK, P8S_UO, P8U_K, P8S_KK*

V.	**NAKŁAD PRACY STUDENTA**			
Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*

Wykład	-	X	50	2
Ćwiczenia	16			
Konsultacje (zaliczenie nieobecności, rozliczenie rygorów, poprawy)	-			
Przygotowanie do ćwiczeń	X	-		
Opanowanie informacji		-		
Przygotowanie do rozliczenia rygorów		34		
RAZEM	16	34		

VI.	**METODY I NARZĘDZIA DYDAKTYCZNE**
1.	Zajęcia seminaryjne
2.	
3.	

VII.	**FORMA ZALICZENIA PRZEDMIOTU**	
Rygor	*Kryteria składowe*	*Waga*
Zaliczenie	Opracowanie artykułu naukowego	0,4
	Opracowanie koncepcji rozprawy doktorskiej	0,6

VIII.	**LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA**
	OBOWIĄZKOWA
1.	J. Gierszewski, A. Pieczywok, *Metodologiczne podstawy badania problemów bezpieczeństwa,* Difin, Warszawa, 2020
2.	P. Siuda, P. Wasylczyk, *Publikacje naukowe. Praktyczny poradnik dla studentów, doktorantów i nie tylko*, Wydawnictwo Naukowe PWN, Warszawa 2018
	UZUPEŁNIAJĄCA
1.	

IX.	**PROWADZĄCY PRZEDMIOT**
Stopień, imię i nazwisko	dr hab. Grzegorz Krasnodębski + zespół
adres e-mail	g.krasnodebski@amw.gdynia.pl

3.2. Matryca efektów uczenia się

Przedmiot/ Symbol	Badania nad bezpieczeństwem	Zarządzanie bezpieczeństwem narodowym	Zarządzanie cyberbezpieczeństwem	Zarządzanie usługami cyfrowymi	Seminarium dyplomowe	PODSUMOWANIE
Wiedza						
ZCU_W01		X	X	X	X	4
ZCU_W02	X					1
ZCU_W03	X		X	X		3
ZCU_W04		X		X		2
ZCU_W05	X					1
ZCU_W06	X					1
Umiejętności						
ZCU_U01	X	X				2
ZCU_U02	X		X	X		3
ZCU_U03	X					1
ZCU_U04			X	X	X	3
ZCU_U05			X	X		2
ZCU_U06	X	X	X	X		4
ZCU_U07					X	1
Kompetencje społeczne						
ZCU_K01	X		X	X	X	4
ZCU_K02		X	X	X		3
ZCU_K03	X	X	X	X		4
ZCU_K04	X					1

4. SPOSOBY WERYFIKACJI I OCENY EFEKTÓW UCZENIA SIĘ

Osiągnięcie efektów uczenia się weryfikowane jest na różnych etapach kształcenia: poprzez rozliczanie rygorów przedmiotów oraz przygotowanie pracy końcowej w formie koncepcji rozprawy doktorskiej, której problematyka obejmuje obszar zarządzania cyberbezpieczeństwem i usługami cyfrowymi. Terminy rozliczenia tych rygorów zależne są od przedmiotów oraz ich prowadzących – kadra ekspercka, spoza Akademii rozlicza studentów w trakcie bądź na zakończenie zajęć.

Sposoby weryfikacji efektów uczenia się osiąganych przez studenta dla poszczególnych przedmiotów (modułów) określono w kartach przedmiotów (modułów), które są integralną częścią niniejszego programu. Wśród najczęściej stosowanych metod weryfikacji osiągnięcia zakładanych efektów uczenia się wyróżnić można następujące:

- rozwiązywanie zadań problemowych,
- projekty,
- wypowiedzi ustne, aktywność w dyskusji,
- zadania wykonywane w grupie, zarówno w trakcie zajęć z nauczycielem akademickim, jak i w trakcie czasu przeznaczonego na pracę własną studenta,
- analiza przypadków case study.

Najważniejszymi źródłami weryfikacji osiągnięcia zakładanych efektów uczenia się są:

- analiza pracy studenta w trakcie i po zakończeniu kształcenia w ramach danego przedmiotu/modułu,
- przygotowanie i analiza pracy końcowej w formie koncepcji rozprawy doktorskiej,
- opinie interesariuszy wewnętrznych i zewnętrznych.

Szczególnej uwadze poddano weryfikację efektów uczenia się o charakterze umiejętnościowym/praktycznym, realizowanych zarówno na zajęciach tzw. kontaktowych, jak i w ramach pracy własnej studenta.

Osiągnięcie efektów uczenia się dla przedmiotów/modułów powoduje pokrycie określonych efektów uczenia się dla kierunku, czyli kierunkowych efektów uczenia się. W kartach przedmiotów sformułowano efekty uczenia się dla danego przedmiotu, które odnoszą się do efektów uczenia się dla kierunku, uniwersalnych charakterystyk poziomów w PRK oraz charakterystyk drugiego stopnia PRK.

Znajdująca się w programie studiów matryca efektów uczenia się przedstawia pokrycie kierunkowych efektów uczenia się dla poszczególnych przedmiotów i modułów.

5. HARMONOGRAM REALIZACJI PROGRAMU STUDIÓW

Plan studiów podyplomowych obejmuje dwa semestry zajęć, które podzielone są na wykłady, ćwiczenia oraz formę zaliczeń, zgodnie z poniższą tabelą.

		Przedmiot	Forma zajęć/ Wymiar godzin					Forma zaliczenia	ECTS
			W	**Ć**	**P**	**S**	**R**		
Semestr 1	1.	Badania nad bezpieczeństwem	8	16			24	Z	3
	2.	Zarządzanie bezpieczeństwem narodowym	12	4			16	Z	4
	3.	Zarządzanie cyberbezpieczeństwem	18	14			32	Z	6
	4.	Zarządzanie usługami cyfrowymi	8	8			16	Z	2
	5.	Seminarium dyplomowe				8	8	Z	1
	Razem		**46**	**42**	**0**	**8**	**96**		**16**
Semestr 2	1.	Badania nad bezpieczeństwem	16	0			16	Z	3
	2.	Zarządzanie cyberbezpieczeństwem	20	4			24	Z	4
	3.	Zarządzanie usługami cyfrowymi	24	8			32	Z	6
	4.	Seminarium dyplomowe				8	8	Z	1
	Razem		**60**	**12**	**0**	**8**	**80**		**14**
Ogółem			**106**	**54**	**0**	**16**	**176**		**30**