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 20/2021 Senatu Akademii Marynarki Wojennej im. Bohaterów Westerplatte z dnia 17 czerwca 2021 roku w sprawie ustalenia programu studiów podyplomowych Executive MBA na kierunku Zarządzanie cyberbezpieczeństwem i usługami cyfrowymi

WYDZIAŁ DOWODZENIA I OPERACJI MORSKICH

PROGRAM STUDIÓW PODYPLOMOWYCH EXECUTIVE MASTER OF BUSINESS ADMINISTRATION

KIERUNEK

ZARZĄDZANIE CYBERBEZPIECZEŃSTWEM I USŁUGAMI CYFROWYMI

GDYNIA

Czerwiec 2021

SPIS TREŚCI

1. OGÓLNA CHARAKTERYSTYKA STUDIÓW

1.1. Informacje podstawowe

Nazwa studiów podyplomowych	**Zarządzanie cyberbezpieczeństwem i usługami cyfrowymi**
Forma studiów	**niestacjonarne**
Łączna liczba godzin zajęć dydaktycznych	**256**
Czas trwania studiów	**2 semestry**
Liczba punktów ECTS konieczna do ukończenia studiów	**30**

Bezpieczeństwo cyberprzestrzeni oraz usług cyfrowych jest jednym z największych priorytetów stawianych za podstawowy cel zarówno w sektorze prywatnym jak i publicznym. Wraz z rozwojem nowoczesnych technologii natrafić można na zagrożenia, które wynikają z niewłaściwego zabezpieczenia i niepoprawnego korzystania z zasobów systemów i sieci teleinformatycznych. Czynniki te powodują, że bardzo istotnym zadaniem realizowanym przez system bezpieczeństwa narodowego jest podniesienie poziomu odporności na cyberzagrożenia oraz zwiększenie poziomu ochrony informacji w sektorze publicznym, militarnym, prywatnym oraz promowanie wiedzy i dobrych praktyk umożliwiających obywatelom lepszą ochronę ich informacji.

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., wychodzą naprzeciw tym oczekiwaniom i ukierunkowane są na rozwijanie kompetencji, wiedzy oraz świadomości zagrożeń i wyzwań wśród kadr administracji publicznej oraz w społeczeństwie w obszarze cyberbezpieczeństwa.

Studia skupiają się przede wszystkim na zajęciach praktycznych. Słuchacze zdobędą wiedzę i umiejętności z zakresu ekonomii i finansów dla kadry zarządzającej, prawnych aspektów zarządzania usługami kluczowymi, zarządzania ryzykiem dla bezpieczeństwa informacji, zarządzania usługami kluczowymi, nowoczesnych technologii, nowoczesnych metod doskonalenia organizacji, zarządzania bezpieczeństwem informacji, monitorowania i reagowania na cyberincydenty oraz skutecznych metody zarządzania projektami i usługami.

Kompleksowy system nauczania pozwoli absolwentom studiów skutecznie podnosić poziom bezpieczeństwa usług cyfrowych realizowanych przez organizacje.

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 256 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 słuchaczy. Wiedza przekazywana jest przez wysokokwalifikowanych specjalistów, wykładowców oraz praktyków specjalizujących się w problematyce cyberbezpieczeństwa oraz usług cyfrowych.

Warunkiem ukończenia studiów jest spełnienie wszystkich wymagań określonych programem studiów oraz przygotowanie pracy końcowej w formie projektu, którego problematyka obejmuje obszar szeroko rozumianego cyberbezpieczeństwa i usług cyfrowych. Tematy poszczególnych projektów ustalane są nie później niż przed rozpoczęciem ostatniego (drugiego) semestru studiów podyplomowych, odpowiada za to kierownik studiów.

1.2. Cele kształcenia

Studia podyplomowe *Executive Master 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* oraz studiów podyplomowych *Cyberbezpieczeństwo*. 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, przygotowując się do przyjęcia roli Narodowego Operatora Cyfrowego.

Wykorzystując potencjał Akademii Marynarki Wojennej oraz Poczty Polskiej S.A. słuchacze zostaną zaznajomieni z problematyką zarządzania cyberbezpieczeństwem oraz usługami cyfrowymi, która została szczegółowa omówiona w kartach przedmiotów (pkt. 3.1).

1.3. Potrzeby społeczno-gospodarcze

Studia podyplomowe *Executive Master 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 *Executive Master of Business Administration* na kierunku *Zarządzanie Cyberbezpieczeństwem i Usługami Cyfrowymi* doskonale wpisują się w wyżej określone działania umożliwiając kształcenie słuchaczy w kontekście rosnącego znacznie usług kluczowych oraz coraz większej ekspozycji na cyberataki związane z adaptacją nowoczesnych technologii przez operatorów tych usług.

Należy również podkreślić, że obecnie brakuje studiów na polskim rynku dotyczących zarządzania cyberbezpieczeństwem i ukierunkowanych na operatorów usług kluczowych.

1.4. Związek z misją uczelni i jej strategią rozwoju

Realizacja studiów podyplomowych *Executive Master 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 *Executive Master 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. 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. Zdobywana wiedza i umiejętności będą weryfikowane w trakcie projektu będącego podstawą zaliczenia.

Symbol	Kierunkowe efekty uczenia się	Odniesienie do: - uniwersalnych charakterystyk pierwszego stopnia PRK - charakterystyk drugiego stopnia dla kwalifikacji na poziomach 6-8 PRK typowe dla kwalifikacji uzyskiwanych w ramach systemu szkolnictwa wyższego i nauki po uzyskaniu kwalifikacji pełnej na poziomie 4
1	2	3
Wiedza		
ZCU_W01	Zna i rozumie w zaawansowanym stopniu – fakty, teorie, metody oraz złożone zależności między elementami procesu zarządzania cyberbezpieczeństwem	P6U_W, P6S_WG
ZCU_W02	Zna i rozumie w zaawansowanym stopniu – fakty, teorie, metody oraz złożone zależności między elementami procesu zarządzania usługami cyfrowymi	P6U_W, P6S_WG
ZCU_W03	Zna i rozumie w pogłębiony sposób fundamentalne dylematy współczesnej cywilizacji ze szczególnym uwzględnieniem zarządzania cyberbezpieczeństwem	P7U_W, P7S_WG, P7S_WK
ZCU_W04	Zna i rozumie w pogłębiony sposób fundamentalne dylematy współczesnej cywilizacji ze szczególnym uwzględnieniem zarządzania usługami cyfrowymi	P7U_W, P7S_WG, P7S_WK
ZCU_W05	Zna i rozumie podstawy ekonomiczne, prawne, etyczne i inne uwarunkowania różnych rodzajów działalności zawodowej związanej zarządzaniem cyberbezpieczeństwem oraz usługami cyfrowymi	P7U_W, P7S_WK
ZCU_W06	Zna i rozumie w pogłębiony sposób podstawowe zasady tworzenia różnych form przedsiębiorczości związane z zarządzaniem cyberbezpieczeństwem	P7U_W, P7S_WK
ZCU_W07	Zna i rozumie w pogłębiony sposób podstawowe zasady tworzenia różnych form przedsiębiorczości związane z zarządzaniem usługami cyfrowymi	P7U_W, P7S_WK
Umiejętności		
ZCU_U01	Potrafi wykorzystać posiadaną wiedzę z zakresu zarządzania cyberbezpieczeństwem oraz usługami cyfrowymi oraz formułować i rozwiązywać złożone i nietypowe problemy oraz wykonywać zadania w warunkach nie w pełni przewidywalnych poprzez: – właściwy dobór źródeł i informacji z nich pochodzących, dokonywanie oceny, krytycznej analizy i syntezy tych informacji; – dobór oraz zastosowanie właściwych metod i narzędzi, w tym zaawansowanych technik informacyjno-komunikacyjnych	P6U_U, P6S_UW
ZCU_U02	Potrafi formułować i testować hipotezy związane z problemami badawczymi dotyczącymi zarządzania cyberbezpieczeństwem oraz usługami cyfrowymi	P7U_U, P7S_UW
ZCU_U03	Potrafi komunikować się z otoczeniem z użyciem specjalistycznej technologii w sposób bezpieczny	P7U_U, P7S_UK

ZCU_U04	Potrafi brać udział w debacie z zakresu zarządzania cyberbezpieczeństwem oraz usługami cyfrowymi - przedstawiać i oceniać różne opinie i stanowiska oraz dyskutować o nich	P7U_U, P7S_UK
ZCU_U05	Potrafi planować i organizować pracę indywidualną oraz kierować pracą zespołu w ramach realizacji zadań dotyczących zarządzania cyberbezpieczeństwem oraz usługami cyfrowymi	P7U_U, P7S_UO
Kompetencje społeczne		
ZCU_K01	Krytycznie ocenia posiadaną wiedzę i odbierane treści z zakresu zarządzania cyberbezpieczeństwem oraz usługami cyfrowymi	P6U_K, P6S_KK
ZCU_K02	Uznaje znaczenie wiedzy w rozwiązywaniu problemów badawczych i praktycznych oraz zasięga opinii ekspertów w przypadku trudności z samodzielnych rozwiązywaniem problemów dotyczących zarządzania cyberbezpieczeństwem oraz usługami cyfrowymi	P7U_K, P7S_KK
ZCU_K03	Inicjuje i uczestniczy konstruktywnie w przygotowaniu projektów dotyczących zarządzania cyberbezpieczeństwem oraz usługami cyfrowymi, uwzględniając ich różne aspekty, planując i zarządzając przy tym czasem własnym oraz czasem w przedsięwzięciach zespołowych	P7U_K, P7S_KO
ZCU_K04	Planuje przedsięwzięcia własne i zespołów, z uwzględnieniem zmieniających się potrzeb społecznych, rozwiązuje problemy o różnym poziomie złożoności dotyczące zarządzania cyberbezpieczeństwem oraz usługami cyfrowymi	P7U_K, P7S_KR
ZCU_K05	Przewiduje zachowania członków zespołów, analizuje ich zachowania i motywacje, postępuje etycznie w ramach wyznaczonych ról organizacyjnych i społecznych, bierze odpowiedzialność za powierzone zadania przed przełożonymi i współpracownikami	P7U_K, P7S_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) uniwersalne charakterystyki poziomów PRK (pierwszego stopnia):

- **P** – poziom PRK (6-7)
- **U** – charakterystyka uniwersalna
  - **W** –wiedza
  - **U** –umiejętności
  - **K** –kompetencje społeczne

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

- **P** – poziom PRK (6-7)

- **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 Ekonomia i finanse dla kadry zarządzającej

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:	**Ekonomia i finanse dla kadry zarządzającej**	*Kod:*	**Cfz**
Kierunek studiów:	Zarządzanie cyberbezpieczeństwem i usługami cyfrowymi		
Poziom studiów:	Studia podyplomowe Executive MBA		
Forma studiów:	Studia niestacjonarne		
Liczba ECTS:	3		
Semestr:	1		
Wymagania wstępne:	Podstawowa wiedza z zakresu ekonomii		
Język wykładowy:	polski		
Cel przedmiotu: **C01**	zaznajomienie studentów z elementami ekonomii menadżerskiej		
Cel przedmiotu: **C02**	zaznajomienie studentów z zasadami zarządzania finansami przedsiębiorstwa		

II.	**EFEKTY UCZENIA SIĘ**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Cfz_W01**	Znajomość podstawowych pojęć z zakresu ekonomii menadżerskiej	Dyskusja
	Cfz_W02	Znajomość zarządzania finansami przedsiębiorstwa	Dyskusja
Umiejętności:	**Cfz_U01**	Potrafi wykorzystywać zasady ekonomii menadżerskiej w zarządzaniu cyberbezpieczeństwem i usługami cyfrowymi w przedsiębiorstwie	Praca zaliczeniowa
	Cfz_U02	Potrafi prowadzić analizę finansową przedsiębiorstwa w obszarze cyberbezpieczeństwa i usług cyfrowych	Praca zaliczeniowa
	Cfz_U03	Potrafi dokonać wyceny wartości intelektualnej i marki	Praca zaliczeniowa
Kompetencje społeczne:	**Cfz_K01**	Krytycznie ocenia posiadaną wiedzę i odbierane treści z zakresu zarządzania finansami przedsiębiorstwa w obszarze cyberbezpieczeństwa i usług cyfrowych	Dyskusja
	Cfz_K01	Inicjuje i uczestniczy konstruktywnie w przygotowaniu finansowania projektów dotyczących zarządzania cyberbezpieczeństwem oraz usługami cyfrowymi	Dyskusja

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
W01	Wybrane zagadnienia makroekonomii	2
W02	Wybrane zagadnienia mikroekonomii	2
W03	Rachunkowość zarządcza	2
W04	Finanse przedsiębiorstw	2
W05	Analiza finansowa i wskaźnikowa	2
W06	Analiza dokumentów finansowych	2
W07	Wycena wartości intelektualnej i marki	2
W08	Programy UE	2
C01	Ekonomia menadżerska	4
C02	Zarządzanie finansami przedsiębiorstwa	12

IV.	**KORELACJA EFEKTÓW UCZENIA SIĘ**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyki PRK*

W01	*Cfz_W01, Cfz_W02*	*ZCU_W05, ZCU_W06, ZCU_W07*	*P7U_W, P7S_WG, P7S_WK*
W02	*Cfz_W01, Cfz_W02*	*ZCU_W05, ZCU_W06, ZCU_W07*	*P7U_W, P7S_WG, P7S_WK*
W03	*Cfz_W01, Cfz_W02*	*ZCU_W05, ZCU_W06, ZCU_W07*	*P7U_W, P7S_WG, P7S_WK*
W04	*Cfz_W01, Cfz_W02*	*ZCU_W05, ZCU_W06, ZCU_W07*	*P7U_W, P7S_WG, P7S_WK*
W05	*Cfz_W01, Cfz_W02*	*ZCU_W05, ZCU_W06, ZCU_W07*	*P7U_W, P7S_WG, P7S_WK*
W06	*Cfz_W01, Cfz_W02*	*ZCU_W05, ZCU_W06, ZCU_W07*	*P7U_W, P7S_WG, P7S_WK*
W07	*Cfz_W01, Cfz_W02*	*ZCU_W05, ZCU_W06, ZCU_W07*	*P7U_W, P7S_WG, P7S_WK*
W08	*Cfz_W01, Cfz_W02*	*ZCU_W05, ZCU_W06, ZCU_W07*	*P7U_W, P7S_WG, P7S_WK*
C01	*Cfy_U01, Cfy_U02, Cfy_K01, Cfy_K01*	*ZCU_U01, ZCU_U05, CU_K01, ZCU_K03*	*P6U_U, P6S_UW, P7U_U, P7S_UO, P6U_K, P6S_KK, P7U_K, P7S_KO*
C02	*Cfy_U01, Cfy_U02, Cfy_K01, Cfy_K01*	*ZCU_U01, ZCU_U05, CU_K01, ZCU_K03*	*P6U_U, P6S_UW, P7U_U, P7S_UO, P6U_K, P6S_KK, P7U_K, P7S_KO*

NAKŁAD PRACY STUDENTA

	Liczba godzin kontaktowych	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**16**	**X**	**75**	**3**
Ćwiczenia	**16**			
Konsultacje (zaliczenie nieobecności, rozliczenie rygorów, poprawy)	**2**			
Przygotowanie do ćwiczeń	**X**	**15**		
Opanowanie informacji		**15**		
Przygotowanie do rozliczenia rygorów		**11**		
RAZEM	**34**	**41**		

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 projektu	0,6

VIII. LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

OBOWIĄZKOWA

1.	D. Begg, R. Dombush, S. Fisher, G. Vernasca, *Mikroekonomia*, PWE, Warszawa 2021
2.	D. Begg, R. Dombush, S. Fisher, G. Vernasca, Makroekonomia, PWE, Warszawa 2020
3.	E. Brigham, J. Houston, *Zarządzanie finansami*, PWN, Warszawa 2021

UZUPEŁNIAJĄCA

1.	Materiały przygotowane przez wykładowców

IX. PROWADZĄCY PRZEDMIOT

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

3.1.2 Prawne aspekty zarządzania usługami kluczowymi

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:	**Prawne aspekty zarządzania usługami kluczowymi**	*Kod:*	**Cfy**
Kierunek studiów:	Zarządzanie cyberbezpieczeństwem i usługami cyfrowymi		
Poziom studiów:	Studia podyplomowe Executive MBA		
Forma studiów:	Studia niestacjonarne		
Liczba ECTS:	2		
Semestr:	1		
Wymagania wstępne:	Podstawowa wiedza z zakresu prawa		
Język wykładowy:	polski		
Cel przedmiotu:	**C01**	zaznajomienie studentów z elementami prawa gospodarczego	
	C02	zaznajomienie studentów z regulacjami prawnymi nowoczesnych technologii	

II.	**EFEKTY UCZENIA SIĘ**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Cfy_W01**	Znajomość podstawowych pojęć z zakresu prawa gospodarczego	Dyskusja
	Cfy_W02	Znajomość regulacji prawnych w obszarze nowoczesnych technologii	Dyskusja
Umiejętności:	**Cfy_U01**	Potrafi wykorzystywać regulacje prawa gospodarczego w zarządzaniu usługami kluczowymi	Praca zaliczeniowa
	Cfy_U02	Potrafi wykorzystywać regulacje prawa nowoczesnych technologii w zarządzaniu usługami kluczowymi	Praca zaliczeniowa
Kompetencje społeczne:	**Cfy_K01**	Uznaje znaczenie wiedzy w rozwiązywaniu problemów badawczych i praktycznych oraz zasięga opinii ekspertów w przypadku trudności z samodzielnych rozwiazywaniem problemów prawnych dotyczących zarządzania usługami kluczowymi	Dyskusja
	Cfy_K01	Inicjuje i uczestniczy konstruktywnie w przygotowaniu regulacji formalno-prawnych dotyczących zarządzania usługami kluczowymi	Dyskusja

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
W01	Kodeks spółek handlowych	2
W02	Prawo przedsiębiorców	1
W03	Odpowiedzialność prawna członków organów spółek	1
W04	Prawo autorskie podczas zamawiania usług i systemów IT	2
W05	Rodzaje otwartych licencji (CC, GNU itp.)	2
C01	Prawo gospodarcze – sporządzanie i weryfikacja zapisów umownych	4
C02	Prawne aspekty obsługi naruszeń danych osobowych	4

IV.	**KORELACJA EFEKTÓW UCZENIA SIĘ**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyki PRK*
W01	*Cfy_W01, Cfy_W02*	*ZCU_W02, ZCU_W05, ZCU_W06, ZCU_W07*	*P6U_W, P6S_WG, P7U_W, P7S_WK*
W02	*Cfy_W01, Cfy_W02*	*ZCU_W02, ZCU_W05, ZCU_W06, ZCU_W07*	*P6U_W, P6S_WG, P7U_W, P7S_WK*
W03	*Cfy_W01, Cfy_W02*	*ZCU_W02, ZCU_W05, ZCU_W06, ZCU_W07*	*P6U_W, P6S_WG, P7U_W, P7S_WK*
W04	*Cfy_W01, Cfy_W02*	*ZCU_W02, ZCU_W05, ZCU_W06, ZCU_W07*	*P6U_W, P6S_WG, P7U_W, P7S_WK*
W05	*Cfy_W01, Cfy_W02*	*ZCU_W02, ZCU_W05,*	*P6U_W, P6S_WG, P7U_W,*

		ZCU_W06, ZCU_W07	*P7S_WK*
C01	*Cfy_U01, Cfy_U02, Cfy_K01, Cfy_K01*	*ZCU_U01, ZCU_U04*	*P6U_U, P6S_UW, P7U_U, P7S_UK, P7U_K, P7S_KK, P7U_K, P7S_KO*
C02	*Cfy_U01, Cfy_U02, Cfy_K01, Cfy_K01*	*ZCU_U01, ZCU_U04*	*P6U_U, P6S_UW, P7U_U, P7S_UK, P7U_K, P7S_KK, P7U_K, P7S_KO*

NAKŁAD PRACY STUDENTA

	Liczba godzin kontaktowych	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**8**	**X**	**50**	**2**
Ćwiczenia	**8**			
Konsultacje (zaliczenie nieobecności, rozliczenie rygorów, poprawy)	**2**			
Przygotowanie do ćwiczeń	**X**	**10**		
Opanowanie informacji		**10**		
Przygotowanie do rozliczenia rygorów		**12**		
RAZEM	**18**	**32**		

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 projektu	0,6

VIII. LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

	OBOWIĄZKOWA
1.	J. Bieniak i inni, *Kodeks spółek handlowych. Komentarz*, C.H.Beck, Warszawa 2019
2.	K. Chałubińska-Jentkiewicz, M. Nowikowska, *Bezpieczeństwo, tożsamość, prywatność – aspekty prawne*, C.H.Beck, Warszawa 2020
3.	
	UZUPEŁNIAJĄCA
1.	S. Williams, *W obronie wolności – krucjata hakera na rzecz wolnego oprogramowania*, Helion, Gliwice 2003
2.	Materiały przygotowane przez wykładowców

IX. PROWADZĄCY PRZEDMIOT

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

3.1.3 Zarządzanie ryzykiem dla bezpieczeństwa informacji

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 ryzykiem dla bezpieczeństwa informacji**	*Kod:*	**Lbi**
Kierunek studiów:	Zarządzanie cyberbezpieczeństwem i usługami cyfrowymi		
Poziom studiów:	Studia podyplomowe Executive MBA		
Forma studiów:	Studia niestacjonarne		
Liczba ECTS:	2		
Semestr:	1		
Wymagania wstępne:	Podstawowa wiedza z zakresu oceny ryzyka i bezpieczeństwa informacji		
Język wykładowy:	polski		
Cel przedmiotu:	**C01**	zaznajomienie studentów z metodami identyfikacji zagrożeń i zasadami zarządzanie ryzykiem IT	
	C02	zaznajomienie studentów z kryminologicznymi aspektami cyberprzestępczości	
	C03	zaznajomienie studentów ze zjawiskiem dezinformacji, manipulacji i wojny informacyjnej	
	C04	zaznajomienie studentów z metodami modelowania zagrożeń w cyberprzestrzeni	

II.	**EFEKTY UCZENIA SIĘ**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Lbi_W01**	Znajomość metod identyfikacji zagrożeń i zarządzania ryzykiem IT	Dyskusja
	Lbi_W02	Znajomość kryminologicznych aspektów cyberprzestępczości	Dyskusja
	Lbi_W03	Znajomość zjawiska dezinformacji, manipulacji i wojny informacyjnej	Dyskusja
	Lbi_W04	Znajomość metod modelowania zagrożeń w cyberprzestrzeni	Dyskusja
Umiejętności:	**Lbi_U01**	Potrafi identyfikować ryzyka metodą hierarchii celów	Praca zaliczeniowa
	Lbi_U02	Potrafi rozpoznać działalność w cyberprzestrzeni wskazującą na możliwy cyberatak oraz wskazać miejsca, w których należy szukać śladów umożliwiających analizę zdarzenia i wstępne określenie potencjalnych sprawców	Praca zaliczeniowa
	Lbi_U03	Potrafi identyfikować oraz reagować na wykryte elementy walki informacyjnej, dezinformacji i propagandy	Praca zaliczeniowa
	Lbi_U03	Potrafi samodzielnie tworzyć schematy blokowe dla prostych procesów celem identyfikacji zagrożeń	Praca zaliczeniowa
Kompetencje społeczne:	**Lbi_K01**	Rozwiązuje problemy o różnym poziomie złożoności dotyczące oceny ryzyka i bezpieczeństwa informacji	Dyskusja
	Lbi_K01	Bierze odpowiedzialność za powierzone zadania dotyczące oceny ryzyka i bezpieczeństwa informacji przed przełożonymi i współpracownikami	Dyskusja

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
W01	Zjawisko ryzyka, identyfikacja oraz postępowanie z ryzykiem, taksonomie cyberzagrożeń, podział cyberzagrożeń metodą AF	1
W02	Zjawisko cyberprzestępczości, charakterystyka sprawców i ich modus operandi, cechy wskazujące na cyberatak, rodzaje i miejsca występowania śladów elektronicznych	2
W03	Wojna (walka) informacyjna oraz jej cele, proces dezinformacji i propagandy, techniki dezinformacji i propagandy, charakterystyka źródeł informacji, znaczenie cyberprzestrzeni w walce informacyjnej	2
W04	Identyfikacja ryzyk, cyberkill chain, MITRE ATT&CK (zmiany w środowiskach	1

	chmurowych), modelowanie zagrożeń na bazie instant threat modeling, STRIDE (narzędzia wspierające typu MS Threat Modelling Tool)	
C01	Identyfikacja ryzyk dla bezpieczeństwa IT oraz sposoby zarządzania ryzykiem	3
C02	Kryminologiczne aspekty cyberprzestępczości	2
C03	Dezinformacja, manipulacja i wojna informacyjna	2
C04	Metody modelowania zagrożeń w cyberprzestrzeni	3

IV. KORELACJA EFEKTÓW UCZENIA SIĘ

Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyki PRK*
W01	*Lbi_W01, Lbi_W02, Lbi_W03, Lbi_W04*	*ZCU_W01, ZCU_W03*	*P6U_W, P6S_WG, P7U_W, P7S_WG, P7S_WK*
W02	*Lbi_W01, Lbi_W02, Lbi_W03, Lbi_W04*	*ZCU_W01, ZCU_W03*	*P6U_W, P6S_WG, P7U_W, P7S_WG, P7S_WK*
W03	*Lbi_W01, Lbi_W02, Lbi_W03, Lbi_W04*	*ZCU_W01, ZCU_W03*	*P6U_W, P6S_WG, P7U_W, P7S_WG, P7S_WK*
W04	*Lbi_W01, Lbi_W02, Lbi_W03, Lbi_W04*	*ZCU_W01, ZCU_W03*	*P6U_W, P6S_WG, P7U_W, P7S_WG, P7S_WK*
C01	*Lbi_U01, Lbi_U02, Lbi_U03, Lbi_U03, Lbi_K01, Lbi_K01*	*ZCU_U01, ZCU_U02, ZCU_U04, ZCU_K04, ZCU_K05*	*P6U_U, P6S_UW, P7U_U, P7S_UW, P7U_K, P7S_KR, P7U_K, P7S_KR*
C02	*Lbi_U01, Lbi_U02, Lbi_U03, Lbi_U03, Lbi_K01, Lbi_K01*	*ZCU_U01, ZCU_U02, ZCU_U04, ZCU_K04, ZCU_K05*	*P6U_U, P6S_UW, P7U_U, P7S_UW, P7U_K, P7S_KR, P7U_K, P7S_KR*
C03	*Lbi_U01, Lbi_U02, Lbi_U03, Lbi_U03, Lbi_K01, Lbi_K01*	*ZCU_U01, ZCU_U02, ZCU_U04, ZCU_K04, ZCU_K05*	*P6U_U, P6S_UW, P7U_U, P7S_UW, P7U_K, P7S_KR, P7U_K, P7S_KR*
C04	*Lbi_U01, Lbi_U02, Lbi_U03, Lbi_U03, Lbi_K01, Lbi_K01*	*ZCU_U01, ZCU_U02, ZCU_U04, ZCU_K04, ZCU_K05*	*P6U_U, P6S_UW, P7U_U, P7S_UW, P7U_K, P7S_KR, P7U_K, P7S_KR*

V. NAKŁAD PRACY STUDENTA

Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**6**	**X**	**50**	**2**
Ćwiczenia	**10**			
Konsultacje (zaliczenie nieobecności, rozliczenie rygorów, poprawy)	**2**			
Przygotowanie do ćwiczeń	**X**	**10**		
Opanowanie informacji		**10**		
Przygotowanie do rozliczenia rygorów		**12**		
RAZEM	**18**	**32**		

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 projektu	0,6

VIII. LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

OBOWIĄZKOWA

1.	R. Godston, J. J. Wirtz, *Strategic denial and decption: the twenty-first century challenge*, National Strategy-Information Center, Washington, D. C., 2012.
2.	G. S. Jowert, V.O'Donnell, *Propaganda and persuasion, Sage Publications*, Washington D. C. 2006
3.	E. M. Hutchins, M. J. Cloppert, R. M. Amin, *Intelligence-Driven Computer Network Defense Informed*

	by Analysis of Adversary Campaigns and Intrusion Kill Chains
2.	A. Shostack, *Threat Modeling: Designing for Security*
3.	J. Zawiła-Niedźwiecki, *Zarządzanie ryzykiem operacyjnym w zapewnianiu ciągłości działania organizacji*, Edu-Libri, Kraków-Warszawa 2013
UZUPEŁNIAJĄCA	
1.	https://www.securing.pl/pl/thinking-what-can-go-wrong-introduction-to-threat-modeling/
2.	https://www.securing.pl/pl/threat-modeling-how-to-start-doing-it/
3.	MITRE ATT&CK
4.	Materiały przygotowane przez wykładowców
IX.	**PROWADZĄCY PRZEDMIOT**
Stopień, imię i nazwisko	dr hab. Piotr Dela+ zespół
adres e-mail	p.dela@amw.gdynia.pl

3.1.4 Zarządzanie usługami kluczowymi

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 kluczowymi**	*Kod:*	**Zbu**
Kierunek studiów:	Zarządzanie cyberbezpieczeństwem i usługami cyfrowymi		
Poziom studiów:	Studia podyplomowe Executive MBA		
Forma studiów:	Studia niestacjonarne		
Liczba ECTS:	7		
Semestr:	1,2		
Wymagania wstępne:	Podstawowa wiedza z zakresu usług kluczowych		
Język wykładowy:	polski		
Cel przedmiotu:	**C01**	zaznajomienie studentów z metodami zarządzania strategicznego	
	C02	zaznajomienie studentów z procesem zarządzania zmianą	
	C03	zaznajomienie studentów z Krajowy System Cyberbezpieczeństwa	
	C04	zaznajomienie studentów z procesem kierowania zespołem i zarządzania zasobami ludzkimi	
	C05	zaznajomienie studentów z zarządzaniem procesowym przedsiębiorstwem	
	C06	zaznajomienie studentów z metodami negocjacji i mediacji	
	C07	zaznajomienie studentów ze znaczeniem przywództwa w organizacji	
	C08	zaznajomienie studentów ze znaczeniem marketingu i PR w gospodarce cyfrowej	

II.	**EFEKTY UCZENIA SIĘ**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Zbu_W01**	Znajomość metod zarządzania strategicznego	Dyskusja
	Zbu_W02	Znajomość procesu zarządzania zmianą	Dyskusja
	Zbu_W03	Znajomość Krajowego Systemu Cyberbezpieczeństwa	Dyskusja
	Zbu_W04	Znajomość procesu kierowania zespołem i zarządzania zasobami ludzkimi	Dyskusja
	Zbu_W05	Znajomość zarządza procesowego przedsiębiorstwem	Dyskusja
	Zbu_W06	Znajomość metod negocjacji i mediacji	Dyskusja
	Zbu_W07	Znajomość znaczenia przywództwa w organizacji	Dyskusja
	Zbu_W08	Znajomość znaczenia marketingu i PR w gospodarce cyfrowej	Dyskusja
Umiejętności:	**Zbu_U01**	Potrafi zaplanować rozwój przedsiębiorstwa w zakresie zarządzania cyberbezpieczeństwem i usługami cyfrowymi	Praca zaliczeniowa
	Zbu_U02	Potrafi wykorzystać nowoczesne metody zarządzania przedsiębiorstwem w obszarze cyberbezpieczeństwa i usług cyfrowych	Praca zaliczeniowa
Kompetencje społeczne:	**Zbu_K01**	Krytycznie ocenia posiadaną wiedzę i odbierane treści z zakresu zarządzania przedsiębiorstwem w obszarze cyberbezpieczeństwa i usług cyfrowych	Dyskusja
	Zbu_K02	Rozwiązuje problemy o różnym poziomie złożoności dotyczące cyberbezpieczeństwa i usług cyfrowych	Dyskusja
	Zbu_K03	Bierze odpowiedzialność za powierzone zadania dotyczące oceny ryzyka i bezpieczeństwa informacji przed przełożonymi i współpracownikami	Dyskusja

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba*

		godzin
W01	Zarządzanie strategiczne	6
W02	Zarządzanie zmianą	6
W03	Krajowy System Cyberbezpieczeństwa	4
W04	Kierowanie zespołem i zarządzanie zasobami ludzkimi	6
W05	Zarządzanie procesowe	6
W06	Negocjacje i mediacje	4
W07	Przywództwo	6
W08	Marketing i PR w gospodarce cyfrowej	4
C01	Przygotowywanie strategii rozwoju w zakresie cyberbezpieczeństwa	3
C02	Planowanie i komunikowanie zmian	3
C03	Organizowanie przedsiębiorstwa pod kątem spełniania wymagań KSC	2
C04	Dokumentowanie procesów i ich wzajemnych zależności	3
C05	Negocjacje i mediacje w przypadku cyberincydentów	2
C06	Budowanie zespołów zadaniowych	3
C07	Gromadzenie i automatyczne analizowanie dużych ilości danych	2

IV.	**KORELACJA EFEKTÓW UCZENIA SIĘ**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyki PRK*
W01	*Zbu_W01*	*ZCU_W01, ZCU_W02, ZCU_W03, ZCU_W04, ZCU_W07*	*P6U_W, P6S_WG, P7U_W, P7S_WG, P7S_WK, P7U_W, P7S_WK*
W02	*Zbu_W02*	*ZCU_W01, ZCU_W02, ZCU_W03, ZCU_W04, ZCU_W07*	*P6U_W, P6S_WG, P7U_W, P7S_WG, P7S_WK, P7U_W, P7S_WK*
W03	*Zbu_W03*	*ZCU_W01, ZCU_W02, ZCU_W03, ZCU_W04, ZCU_W07*	*P6U_W, P6S_WG, P7U_W, P7S_WG, P7S_WK, P7U_W, P7S_WK*
W04	*Zbu_W04*	*ZCU_W01, ZCU_W02, ZCU_W03, ZCU_W04, ZCU_W07*	*P6U_W, P6S_WG, P7U_W, P7S_WG, P7S_WK, P7U_W, P7S_WK*
W05	*Zbu_W05*	*ZCU_W01, ZCU_W02, ZCU_W03, ZCU_W04, ZCU_W07*	*P6U_W, P6S_WG, P7U_W, P7S_WG, P7S_WK, P7U_W, P7S_WK*
W06	*Zbu_W06*	*ZCU_W01, ZCU_W02, ZCU_W03, ZCU_W04, ZCU_W07*	*P6U_W, P6S_WG, P7U_W, P7S_WG, P7S_WK, P7U_W, P7S_WK*
W07	*Zbu_W07*	*ZCU_W01, ZCU_W02, ZCU_W03, ZCU_W04, ZCU_W07*	*P6U_W, P6S_WG, P7U_W, P7S_WG, P7S_WK, P7U_W, P7S_WK*
W08	*Zbu_W08*	*ZCU_W01, ZCU_W02, ZCU_W03, ZCU_W04, ZCU_W07*	*P6U_W, P6S_WG, P7U_W, P7S_WG, P7S_WK, P7U_W, P7S_WK*
C01	*Zbu_U01, Zbu_U02, Zbu_K01, Zbu_K02, Zbu_K03*	*ZCU_U01, ZCU_U03, ZCU_U05, ZCU_K04, ZCU_K05*	*P6U_U, P6S_UW, P7U_U, P7S_UK, P7S_UO, P7U_K, P7S_KR, P7S_KR*
C02	*Zbu_U01, Zbu_U02, Zbu_K01, Zbu_K02, Zbu_K03*	*ZCU_U01, ZCU_U03, ZCU_U05, ZCU_K04, ZCU_K05*	*P6U_U, P6S_UW, P7U_U, P7S_UK, P7S_UO, P7U_K, P7S_KR, P7S_KR*
C03	*Zbu_U01, Zbu_U02, Zbu_K01, Zbu_K02, Zbu_K03*	*ZCU_U01, ZCU_U03, ZCU_U05, ZCU_K04, ZCU_K05*	*P6U_U, P6S_UW, P7U_U, P7S_UK, P7S_UO, P7U_K, P7S_KR, P7S_KR*
C04	*Zbu_U01, Zbu_U02, Zbu_K01, Zbu_K02, Zbu_K03*	*ZCU_U01, ZCU_U03, ZCU_U05, ZCU_K04, ZCU_K05*	*P6U_U, P6S_UW, P7U_U, P7S_UK, P7S_UO, P7U_K, P7S_KR, P7S_KR*
C05	*Zbu_U01, Zbu_U02, Zbu_K01, Zbu_K02, Zbu_K03*	*ZCU_U01, ZCU_U03, ZCU_U05, ZCU_K04, ZCU_K05*	*P6U_U, P6S_UW, P7U_U, P7S_UK, P7S_UO, P7U_K, P7S_KR, P7S_KR*
C06	*Zbu_U01, Zbu_U02, Zbu_K01,*	*ZCU_U01, ZCU_U03,*	*P6U_U, P6S_UW, P7U_U,*

	Zbu_K02, Zbu_K03	*ZCU_U05, ZCU_K04, ZCU_K05*	*P7S_UK, P7S_UO, P7U_K, P7S_KR, P7S_KR*
C07	*Zbu_U01, Zbu_U02, Zbu_K01, Zbu_K02, Zbu_K03*	*ZCU_U01, ZCU_U03, ZCU_U05, ZCU_K04, ZCU_K05*	*P6U_U, P6S_UW, P7U_U, P7S_UK, P7S_UO, P7U_K, P7S_KR, P7S_KR*

V. NAKŁAD PRACY STUDENTA

Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**42**	**X**	**175**	**7**
Ćwiczenia	**18**			
Konsultacje (zaliczenie nieobecności, rozliczenie rygorów, poprawy)	**4**			
Przygotowanie do ćwiczeń	**X**	**30**		
Opanowanie informacji		**60**		
Przygotowanie do rozliczenia rygorów		**21**		
RAZEM	**64**	**111**		

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 projektu	0,6

VIII. LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

OBOWIĄZKOWA

1.	*Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, t.j. Dz. U. z 2020 r. poz. 1369.*
2.	S. Capparell, *Shackleton's Way: Leadership Lessons from the Great Antarctic Explorer*
3.	D. O. Relin, Three Cups of Tea

UZUPEŁNIAJĄCA

1.	Materiały przygotowane przez wykładowców

IX. PROWADZĄCY PRZEDMIOT

Stopień, imię i nazwisko	dr inż. Robert Janczewski+ zespół
adres e-mail	r.janczewski@amw.gdynia.pl

3.1.5 Nowoczesne technologie

KARTA PRZEDMIOTU	AKADEMIA MARYNARKI WOJENNEJ WYDZIAŁ DOWODZENIA I OPERACJI MORSKICH	

I.	CHARAKTERYSTYKA PRZEDMIOTU		
Nazwa przedmiotu:	**Nowoczesne technologie**	*Kod:*	**Znu**
Kierunek studiów:	Zarządzanie cyberbezpieczeństwem i usługami cyfrowymi		
Poziom studiów:	Studia podyplomowe Executive MBA		
Forma studiów:	Studia niestacjonarne		
Liczba ECTS:	3		
Semestr:	1		
Wymagania wstępne:	Podstawowa wiedza z zakresu technologii informacyjnych		
Język wykładowy:	polski		
Cel przedmiotu:	**C01**	Zaznajomienie studentów z systemami IT i OT	
	C02	Zaznajomienie studentów ze wschodzącymi technologiami w kontekście cyberbezpieczeństwa	
	C03	Zaznajomienie studentów z globalnym rozwojem nowoczesnych technologii	
	C04	Zaznajomienie studentów z bezpieczeństwem usług chmurowych	

II.	EFEKTY UCZENIA SIĘ		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Znu_W01**	Znajomość IT i OT	Dyskusja
	Znu_W02	Znajomość wschodzących technologii w kontekście cyberbezpieczeństwa	Dyskusja
	Znu_W03	Znajomość trendów rozwojowych współczesnej gospodarki światowej, roli rynków finansowych i ich wpływu na funkcjonowanie przedsiębiorstw, strategii międzynarodowych państwa w zakresie polityki gospodarczej oraz nowych technologii w kontekście pracy zdalnej	Dyskusja
	Znu_W04	Znajomość usług chmur obliczeniowych	Dyskusja
Umiejętności:	**Znu_U01**	Potrafi identyfikować ryzyka związane z udanym atakiem na wykorzystywane systemy OT	Praca zaliczeniowa
	Znu_U02	Potrafi identyfikować szanse dla organizacji, które płyną z wykorzystania nowych technologii oraz posiada świadomość związanych z tym zagrożeń	Praca zaliczeniowa
	Znu_U03	Potrafi zaplanować działania zmierzające do migracji systemów teleinformatycznych do chmury obliczeniowej	Praca zaliczeniowa
Kompetencje społeczne:	**Znu_K01**	Krytycznie ocenia posiadaną wiedzę i odbierane treści z zakresu zarządzania usługami cyfrowymi	Dyskusja
	Znu_K02	Inicjuje i uczestniczy konstruktywnie w przygotowaniu projektów dotyczących zarządzania usługami cyfrowymi	Dyskusja

III.	TREŚCI PROGRAMOWE	
Forma	*Tematyka*	*Liczba godzin*
W01	IT a OT	2
W02	Wschodzące technologie a cyberbezpieczeństwo	4
W03	Gospodarka globalna	4
W04	Bezpieczeństwo usług chmurowych	2
C01	Identyfikacja ryzyk związanych z systemami OT oraz definiowanie podstawowych zabezpieczeń	2
C02	Identyfikowanie ryzyk związanych ze wschodzącymi technologiami	4
C03	Migracja systemów teleinformatycznych do chmury obliczeniowej	2

IV.	KORELACJA EFEKTÓW UCZENIA SIĘ

Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyki PRK*
W01	*Znu_W01*	*ZCU_W02, ZCU_W04*	*P6U_W, P6S_WG, P7U_W, P7S_WG, P7S_WK*
W02	*Znu_W02*	*ZCU_W02, ZCU_W04*	*P6U_W, P6S_WG, P7U_W, P7S_WG, P7S_WK*
W03	*Znu_W03*	*ZCU_W02, ZCU_W04*	*P6U_W, P6S_WG, P7U_W, P7S_WG, P7S_WK*
W04	*Znu_W04*	*ZCU_W02, ZCU_W04*	*P6U_W, P6S_WG, P7U_W, P7S_WG, P7S_WK*
C01	*Znu_U01, Znu_K01, Znu_K02*	*ZCU_U01, ZCU_U03, ZCU_K01, ZCU_K03*	*P6U_U, P6S_UW, P7U_U, P7S_UK, P6U_K, P6S_KK, P7U_K, P7S_KO*
C02	*Znu_U02, Znu_K01, Znu_K02*	*ZCU_U01, ZCU_U03, ZCU_K01, ZCU_K03*	*P6U_U, P6S_UW, P7U_U, P7S_UK, P6U_K, P6S_KK, P7U_K, P7S_KO*
C03	*Znu_U03, Znu_K01, Znu_K02*	*ZCU_U01, ZCU_U03, ZCU_K01, ZCU_K03*	*P6U_U, P6S_UW, P7U_U, P7S_UK, P6U_K, P6S_KK, P7U_K, P7S_KO*

V. NAKŁAD PRACY STUDENTA

Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**12**	**X**	**75**	**3**
Ćwiczenia	**8**			
Konsultacje (zaliczenie nieobecności, rozliczenie rygorów, poprawy)	**2**			
Przygotowanie do ćwiczeń	**X**	**20**		
Opanowanie informacji		**20**		
Przygotowanie do rozliczenia rygorów		**13**		
RAZEM	**22**	**53**		

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 projektu	0,6

VIII. LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

OBOWIĄZKOWA

1.	*IoT Security Compliance Framework - IoT Security Foundation*
2.	*NIST Special Publication 800-82,Guide to Industrial Control Systems (ICS) Security rev.2*
3.	

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

3.1.6 Nowoczesne metody doskonalenia organizacji

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:	**Nowoczesne metody doskonalenia organizacji**	*Kod:*	**Zpj**
Kierunek studiów:	Zarządzanie cyberbezpieczeństwem i usługami cyfrowymi		
Poziom studiów:	Studia podyplomowe Executive MBA		
Forma studiów:	Studia niestacjonarne		
Liczba ECTS:	3		
Semestr:	1		
Wymagania wstępne:	Podstawowa wiedza z zakresu zarządzania organizacją		
Język wykładowy:	polski		
Cel przedmiotu:	**C01**	Zaznajomienie studentów z wykorzystywanie audytu wewnętrznego dla rzeczywistego doskonalenia organizacji	
	C02	Zaznajomienie studentów zasadami etyki w biznesie i CSR	
	C03	Zaznajomienie studentów z zagadnieniami psychologii biznesu	
	C04	Zaznajomienie studentów z zasadami lean management	

II.	**EFEKTY UCZENIA SIĘ**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Zpj_W01**	Znajomość prowadzenia audytu wewnętrznego organizacji	Dyskusja
	Zpj_W02	Znajomość zasad etyki w biznesie i CSR	Dyskusja
	Zpj_W03	Znajomość psychologii biznesu	Dyskusja
	Zpj_W04	Znajomość lean management	Dyskusja
Umiejętności:	**Zpj_U01**	Potrafi wykorzystać wyniki audytu wewnętrznego dla doskonalenia organizacji	Praca zaliczeniowa
	Zpj_U02	Potrafi tworzyć strategiczne cele w zakresie zrównoważonego rozwoju	Praca zaliczeniowa
	Zpj_U03	Potrafi wykorzystać lean management do zarządzania organizacją	Praca zaliczeniowa
Kompetencje społeczne:	**Zpj_K01**	Rozwiązuje problemy o różnym poziomie złożoności dotyczące doskonalenia organizacji	Dyskusja
	Zpj_K02	Postępuje etycznie w ramach wyznaczonych ról organizacyjnych i społecznych, bierze odpowiedzialność za powierzone zadania przed przełożonymi i współpracownikami	Dyskusja

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
W01	Wykorzystywanie audytu wewnętrznego dla rzeczywistego doskonalenia organizacji	2
W02	Etyka w biznesie i CSR	4
W03	Psychologia biznesu	4
W04	Lean management	4
C01	Definiowanie celów dla audytu wewnętrznego oraz wykorzystywanie jego wyników	2
C02	Zarządzanie trudnymi sytuacjami w firmach	4
C03	Identyfikacja przeszkód oraz doskonalenie organizacji	4

IV.	**KORELACJA EFEKTÓW UCZENIA SIĘ**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyki PRK*
W01	*Zpj_W01*	*ZCU_W02, ZCU_W03, ZCU_W04, ZCU_W06, ZCU_W07*	*P6U_W, P6S_WG, P7U_W, P7S_WG, P7S_WK, P7U_W, P7S_WK*
W02	*Zpj_W02*	*ZCU_W02, ZCU_W03, ZCU_W04, ZCU_W06,*	*P6U_W, P6S_WG, P7U_W, P7S_WG, P7S_WK, P7U_W,*

		ZCU_W07	*P7S_WK*
W03	*Zpj_W03*	*ZCU_W02, ZCU_W03, ZCU_W04, ZCU_W06, ZCU_W07*	*P6U_W, P6S_WG, P7U_W, P7S_WG, P7S_WK, P7U_W, P7S_WK*
W04	*Zpj_W04*	*ZCU_W02, ZCU_W03, ZCU_W04, ZCU_W06, ZCU_W07*	*P6U_W, P6S_WG, P7U_W, P7S_WG, P7S_WK, P7U_W, P7S_WK*
C01	*Zpj_U01, Zpj_K01, Zpj_K02*	*ZCU_U01, ZCU_U04, ZCU_U05, ZCU_K01, ZCU_K03*	*P6U_U, P6S_UW, P7U_U, P7S_UK, P7S_UO, P6U_K, P6S_KK, P7U_K, P7S_KO*
C02	*Zpj_U02, Zpj_K01, Zpj_K02*	*ZCU_U01, ZCU_U04, ZCU_U05, ZCU_K01, ZCU_K03*	*P6U_U, P6S_UW, P7U_U, P7S_UK, P7S_UO, P6U_K, P6S_KK, P7U_K, P7S_KO*
C03	*Zpj_U03, Zpj_K01, Zpj_K02*	*ZCU_U01, ZCU_U04, ZCU_U05, ZCU_K01, ZCU_K03*	*P6U_U, P6S_UW, P7U_U, P7S_UK, P7S_UO, P6U_K, P6S_KK, P7U_K, P7S_KO*

V. NAKŁAD PRACY STUDENTA

Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**14**	**X**	**75**	**3**
Ćwiczenia	**10**			
Konsultacje (zaliczenie nieobecności, rozliczenie rygorów, poprawy)	**2**			
Przygotowanie do ćwiczeń	**X**	**20**		
Opanowanie informacji		**15**		
Przygotowanie do rozliczenia rygorów		**14**		
RAZEM	**26**	**49**		

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 projektu	0,6

VIII. LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

OBOWIĄZKOWA

1.	*GRC Capability Model (Condensed Red Book) – OCEG*
2.	*GTAG® 17 - Audytowanie ładu informatycznego - https://www.iia.org.pl/publikacje/gtagr-17-audytowanie-ladu-informatycznego*
3.	*GTAG® 4 - Zarządzanie Audytem IT - https://www.iia.org.pl/publikacje/gtagr-4-zarzadzanie-audytem-it*
4.	*The Internal Audit Foundation, Sawyer's Internal Auditing: Enhancing and Protecting Organizational Value, 7th Edition, Usa 2019*

UZUPEŁNIAJĄCA

1.	*Trzy linie obrony – zaktualizowany model trzech linii obrony IIA, 2020 r. – IIA –- https://www.iia.org.pl/aktualnosci/trzy-linie-obrony-zaktualizowany-model-trzech-linii-obrony-iia-2020-r*
2.	D. J. Anderson, G. Eubanks, *Wykorzystanie COSO w trzech liniach obrony, - https://www.iia.org.pl/publikacje/wykorzystanie-coso-w-trzech-liniach-obrony*
3.	Materiały przygotowane przez wykładowców

IX. PROWADZĄCY PRZEDMIOT

Stopień, imię i nazwisko	dr inż. Jakub Syta + zespół
adres e-mail	j.syta@amw.gdynia.pl

3.1.7 Zarządzanie bezpieczeństwem informacji

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 informacji**	*Kod:*	**Zbi**
Kierunek studiów:	Zarządzanie cyberbezpieczeństwem i usługami cyfrowymi		
Poziom studiów:	Studia podyplomowe Executive MBA		
Forma studiów:	Studia niestacjonarne		
Liczba ECTS:	5		
Semestr:	2		
Wymagania wstępne:	Podstawowa wiedza z zakresu bezpieczeństwa informacji		
Język wykładowy:	polski		
Cel przedmiotu:	**C01**	Zaznajomienie studentów IT Governance w praktyce	
	C02	Zaznajomienie studentów z procesem zarządzania ciągłością działania	
	C03	Zaznajomienie studentów z problematyką interoperacyjności w cyberbezpieczeństwie	
	C04	Zaznajomienie studentów z tworzeniem bezpiecznej architektura IT	
	C05	Zaznajomienie studentów z zarządzaniem systemem antykorupcyjnym	
	C06	Zaznajomienie studentów z wielowarstwowym zarządzaniem bezpieczeństwem informacji	
	C07	Zaznajomienie studentów z usługami z zakresu cyberbezpieczeństwa	
	C08	Zaznajomienie studentów z fundamentami cyberbezpieczeństwa	
	C09	Zaznajomienie studentów z problematyką cyberbezpieczeństwo VIP'ów	

II.	**EFEKTY UCZENIA SIĘ**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Zbi_W01**	Znajomość problematyki IT Governance w praktyce	Dyskusja
	Zbi_W02	Znajomość procesu zarządzania ciągłością działania	Dyskusja
	Zbi_W03	Znajomość problematyki interoperacyjności w cyberbezpieczeństwie	Dyskusja
	Zbi_W04	Znajomość zasad tworzenia bezpiecznej architektura IT	Dyskusja
	Zbi_W05	Znajomość zarządzania systemem antykorupcyjnym	Dyskusja
	Zbi_W06	Znajomość wielowarstwowego zarządzania bezpieczeństwem informacji	Dyskusja
	Zbi_W07	Znajomość usług z zakresu cyberbezpieczeństwa	Dyskusja
	Zbi_W08	Znajomość fundamentów cyberbezpieczeństwa	Dyskusja
	Zbi_W09	Znajomość problematyki cyberbezpieczeństwa VIP'ów	Dyskusja
Umiejętności:	**Zbi_U01**	Potrafi samodzielnie przygotowywać BIA	Praca zaliczeniowa
	Zbi_U02	Potrafi planować, organizować, brać udział oraz kontrolować interoperacyjną działalność na rzecz cyberbezpieczeństwa	Praca zaliczeniowa
	Zbi_U03	Potrafi ocenić odporność infrastruktury IT na cyberataki	Praca zaliczeniowa
	Zbi_U04	Potrafi reagować na sytuacje korupcyjne	Praca zaliczeniowa
	Zbi_U05	Potrafi identyfikować luki w zakresie realizowanych zadań dotyczących bezpieczeństwa informacji	Praca zaliczeniowa
	Zbi_U06	Potrafi identyfikować niezbędne kompetencje w zakresie cyberbezpieczeństwa	Praca zaliczeniowa
	Zbi_U07	Potrafi wykorzystywać fundamentalne zasady cyberbezpieczeństwa	Praca zaliczeniowa
	Zbi_U08	Potrafi gromadzić informację o podatnościach VIP-ów na	Praca

		cyberataki	zaliczeniowa
Kompetencje społeczne:	**Zbi_K01**	Uznaje znaczenie wiedzy w rozwiązywaniu problemów badawczych i praktycznych dotyczących zarządzania cyberbezpieczeństwem oraz usługami cyfrowymi	Dyskusja
	Zbi_K02	Inicjuje i uczestniczy konstruktywnie w przygotowaniu projektów dotyczących zarządzania cyberbezpieczeństwem	Dyskusja
	Zbi_K03	Rozwiązuje problemy o różnym poziomie złożoności dotyczące cyberbezpieczeństwa	Dyskusja
	Zbi_K04	Postępuje etycznie w ramach wyznaczonych ról organizacyjnych i społecznych, bierze odpowiedzialność za powierzone zadania przed przełożonymi i współpracownikami	Dyskusja

III. TREŚCI PROGRAMOWE

Forma	*Tematyka*	*Liczba godzin*
W01	IT Governance w praktyce	2
W02	Zarządzanie ciągłością działania	4
W03	Interoperacyjność w cyberbezpieczeństwie	2
W04	Bezpieczna architektura IT	2
W05	Zarządzanie systemem antykorupcyjnym	2
W06	Wielowarstwowe zarządzanie bezpieczeństwem informacji	3
W07	Usługi z zakresu cyberbezpieczeństwa	2
W08	Fundamenty cyberbezpieczeństwa	2
W09	Cyberbezpieczeństwo dla VIP'ów	1
C01	Definiowanie celów dla IT spójnych z celami organizacyjnymi	2
C02	Przygotowywania BIA oraz ustalanie strategii ciągłości działania	10
C03	Kontrola interoperacyjnej działalności na rzecz cyberbezpieczeństwa	2
C04	Definiowanie strategicznych wymagań dla architektury bezpieczeństwa	2
C05	Reagowanie na sytuacje korupcyjne	2
C06	Identyfikowanie luk kompetencyjnych w zakresie procesów cyberbezpieczeństwa	1
C07	Definiowanie wymagań dla usługodawców w zakresie cyberbezpieczeństwa	2
C08	Konfigurowanie podstawowych zabezpieczeń	2
C09	Podstawowe zasady OPSEC dla VIP'ów	3

IV. KORELACJA EFEKTÓW UCZENIA SIĘ

Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyki PRK*
W01	*Zbi_W01*	*ZCU_W01, ZCU_W05, ZCU_W06, ZCU_W07*	*P6U_W, P6S_WG, P7U_W, P7S_WK*
W02	*Zbi_W02*	*ZCU_W01, ZCU_W05, ZCU_W06, ZCU_W07*	*P6U_W, P6S_WG, P7U_W, P7S_WK*
W03	*Zbi_W03*	*ZCU_W01, ZCU_W05, ZCU_W06, ZCU_W07*	*P6U_W, P6S_WG, P7U_W, P7S_WK*
W04	*Zbi_W04*	*ZCU_W01, ZCU_W05, ZCU_W06, ZCU_W07*	*P6U_W, P6S_WG, P7U_W, P7S_WK*
W05	*Zbi_W05*	*ZCU_W01, ZCU_W05, ZCU_W06, ZCU_W07*	*P6U_W, P6S_WG, P7U_W, P7S_WK*
W06	*Zbi_W06*	*ZCU_W01, ZCU_W05, ZCU_W06, ZCU_W07*	*P6U_W, P6S_WG, P7U_W, P7S_WK*
W07	*Zbi_W07*	*ZCU_W01, ZCU_W05, ZCU_W06, ZCU_W07*	*P6U_W, P6S_WG, P7U_W, P7S_WK*
W08	*Zbi_W08*	*ZCU_W01, ZCU_W05, ZCU_W06, ZCU_W07*	*P6U_W, P6S_WG, P7U_W, P7S_WK*
W09	*Zbi_W09*	*ZCU_W01, ZCU_W05, ZCU_W06, ZCU_W07*	*P6U_W, P6S_WG, P7U_W, P7S_WK*
C01	*Zbi_U01, Zbi_K01, Zbi_K02, Zbi_K03, Zbi_K04*	*ZCU_U01, ZCU_U02, ZCU_U03, ZCU_U05, ZCU_K02, ZCU_K03, ZCU_K04, ZCU_K05*	*P6U_U, P6S_UW, P7U_U, P7S_UW, P7S_UO, P7U_K, P7S_KK, P7S_KO, P7S_KR*

C02	*Zbi_U01, Zbi_K01, Zbi_K02, Zbi_K03, Zbi_K04*	*ZCU_U01, ZCU_U02, ZCU_U03, ZCU_U05, ZCU_K02, ZCU_K03, ZCU_K04, ZCU_K05*	*P6U_U, P6S_UW, P7U_U, P7S_UW, P7S_UO, P7U_K, P7S_KK, P7S_KO, P7S_KR*
C03	*Zbi_U02, Zbi_K01, Zbi_K02, Zbi_K03, Zbi_K04*	*ZCU_U01, ZCU_U02, ZCU_U03, ZCU_U05, ZCU_K02, ZCU_K03, ZCU_K04, ZCU_K05*	*P6U_U, P6S_UW, P7U_U, P7S_UW, P7S_UO, P7U_K, P7S_KK, P7S_KO, P7S_KR*
C04	*Zbi_U03, Zbi_K01, Zbi_K02, Zbi_K03, Zbi_K04*	*ZCU_U01, ZCU_U02, ZCU_U03, ZCU_U05, ZCU_K02, ZCU_K03, ZCU_K04, ZCU_K05*	*P6U_U, P6S_UW, P7U_U, P7S_UW, P7S_UO, P7U_K, P7S_KK, P7S_KO, P7S_KR*
C05	*Zbi_U04, Zbi_K01, Zbi_K02, Zbi_K03, Zbi_K04*	*ZCU_U01, ZCU_U02, ZCU_U03, ZCU_U05, ZCU_K02, ZCU_K03, ZCU_K04, ZCU_K05*	*P6U_U, P6S_UW, P7U_U, P7S_UW, P7S_UO, P7U_K, P7S_KK, P7S_KO, P7S_KR*
C06	*Zbi_U05, Zbi_K01, Zbi_K02, Zbi_K03, Zbi_K04*	*ZCU_U01, ZCU_U02, ZCU_U03, ZCU_U05, ZCU_K02, ZCU_K03, ZCU_K04, ZCU_K05*	*P6U_U, P6S_UW, P7U_U, P7S_UW, P7S_UO, P7U_K, P7S_KK, P7S_KO, P7S_KR*
C07	*Zbi_U06, Zbi_K01, Zbi_K02, Zbi_K03, Zbi_K04*	*ZCU_U01, ZCU_U02, ZCU_U03, ZCU_U05, ZCU_K02, ZCU_K03, ZCU_K04, ZCU_K05*	*P6U_U, P6S_UW, P7U_U, P7S_UW, P7S_UO, P7U_K, P7S_KK, P7S_KO, P7S_KR*
C08	*Zbi_U07, Zbi_K01, Zbi_K02, Zbi_K03, Zbi_K04*	*ZCU_U01, ZCU_U02, ZCU_U03, ZCU_U05, ZCU_K02, ZCU_K03, ZCU_K04, ZCU_K05*	*P6U_U, P6S_UW, P7U_U, P7S_UW, P7S_UO, P7U_K, P7S_KK, P7S_KO, P7S_KR*
C09	*Zbi_U08, Zbi_K01, Zbi_K02, Zbi_K03, Zbi_K04*	*ZCU_U01, ZCU_U02, ZCU_U03, ZCU_U05, ZCU_K02, ZCU_K03, ZCU_K04, ZCU_K05*	*P6U_U, P6S_UW, P7U_U, P7S_UW, P7S_UO, P7U_K, P7S_KK, P7S_KO, P7S_KR*

V. NAKŁAD PRACY STUDENTA

Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**20**	**X**	**125**	**5**
Ćwiczenia	**26**			
Konsultacje (zaliczenie nieobecności, rozliczenie rygorów, poprawy)	**4**			
Przygotowanie do ćwiczeń	**X**	**30**		
Opanowanie informacji		**30**		
Przygotowanie do rozliczenia rygorów		**15**		
RAZEM	**50**	**75**		

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 projektu	0,6

VIII. LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

OBOWIĄZKOWA

1.	*Norma ISO 27001*

2.	*Norma ISO 22301*
3.	*Norma NIST 800-53*
4.	D. Dylski i inni, *Księga dobrych praktyk w zakresie zarządzania ciągłością działania,* ZBP, Warszawa 2012
5.	K. Liderman, *Bezpieczeństwo informacyjne. Nowe wyzwania*, PWN, Warszawa 2017
6.	J. Bil, *Korupcja w prywatnym sektorze gospodarczym*, WSPol, Szczytno 2015
7.	W. Jasiński, *Nadużycia w przedsiębiorstwie przeciwdziałanie i wykrywanie*, Poltext, Warszawa 2013
8.	W. Ignaczak, *Analiza śledcza w procesie kontroli*, PIKW, Warszawa 2016
9	*Ustawa z dnia 6 marca 2018 r. - Przepisy wprowadzające ustawę - Prawo przedsiębiorców oraz inne ustawy dotyczące działalności gospodarczej, Dz.U. 2018 poz. 650*
10.	*A.* Bela, E. Bolesławska, *Oszustwa finansowe. Podręcznik dla audytora*, InfoAudit, Warszawa 2005
11.	G. Wesołowski, *Ochrona informacji*, Wydawnictwo Trans, Białystok 2011
	J. Syta, Model: *Wielowarstwowe zarządzanie bezpieczeństwem informacji*
	J. Syta Model: *Podział zagrożeń metodą A:F*
UZUPEŁNIAJĄCA	
1.	Materiały przygotowane przez wykładowców
	K. Popplewell, *Enterprise Interoperability VIII*, Springer Nature, 2019.
	M. Zelm i in., *Enterprise Interoperability: Smart Services and Business Impact of Enterprise Interoperability*, ISTE Ltd, 2018.
	Y. Charalabidis, F. Lampathaki, R. Jardim-Goncalves, *Revolutionizing Enterprise Interoperability through Scientific Foundations*, IGI Global, 2014.

IX.	**PROWADZĄCY PRZEDMIOT**
Stopień, imię i nazwisko	dr inż. Robert Janczewski + zespół
adres e-mail	r.janczewski@amw.gdynia.pl

3.1.8 Monitorowanie oraz reagowanie na cyberincydenty

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:	**Monitorowanie oraz reagowanie na cyberincydenty**	*Kod:*	**Lxb**
Kierunek studiów:	Zarządzanie cyberbezpieczeństwem i usługami cyfrowymi		
Poziom studiów:	Studia podyplomowe Executive MBA		
Forma studiów:	Studia niestacjonarne		
Liczba ECTS:	2		
Semestr:	2		
Wymagania wstępne:	Podstawowa wiedza z zakresu bezpieczeństwa informacji		
Język wykładowy:	polski		
Cel przedmiotu:	**C01**	Zaznajomienie studentów z zasadami komunikacji kryzysowej	
	C02	Zaznajomienie studentów z technicznymi i organizacyjnymi zagadnieniami monitorowania bezpieczeństwa informacji	
	C03	Zaznajomienie studentów z procesem zarządzania cyberincydentami	
	C04	Zaznajomienie studentów z zasadami doboru najskuteczniejszych zabezpieczeń w sytuacji ograniczonego budżetu	

II.	**EFEKTY UCZENIA SIĘ**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Lxb_W01**	Znajomość zasad komunikacji kryzysowej	Dyskusja
	Lxb_W02	Znajomość technicznych i organizacyjnych zagadnień monitorowania bezpieczeństwa informacji	Dyskusja
	Lxb_W03	Znajomość procesu zarządzania cyberincydentami	Dyskusja
	Lxb_W04	Znajomość zasad doboru najskuteczniejszych zabezpieczeń w sytuacji ograniczonego budżetu	Dyskusja
Umiejętności:	**Lxb_U01**	Potrafi dokonać doboru najskuteczniejszych zabezpieczeń w sytuacji ograniczonego budżetu	Praca zaliczeniowa
	Lxb_U02	Potrafi przygotować materiały informacyjne dotyczące cyberincydentu	Praca zaliczeniowa
	Lxb_U03	Potrafi przeprowadzić analizę opłacalności tworzenia własnego zespołu SOC bazując na zasobach organizacji	Praca zaliczeniowa
	Lxb_U04	Potrafi identyfikować priorytety dla incydentów oraz ustalać ścieżki eskalacyjne	Praca zaliczeniowa
Kompetencje społeczne:	**Lxb_K01**	Inicjuje i uczestniczy konstruktywnie w przygotowaniu projektów dotyczących zarządzania cyberbezpieczeństwem	Dyskusja
	Lxb_K02	Rozwiązuje problemy o różnym poziomie złożoności dotyczące cyberbezpieczeństwa	Dyskusja

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
W01	Komunikacja kryzysowa	2
W02	Techniczne i organizacyjne zagadnienia monitorowania bezpieczeństwa informacji	2
W03	Proces zarządzania cyberincydentami	2
C01	CyberTwierdza	6
C02	Przygotowywanie komunikatów prasowych dot potężnego cyberincydentu	2
C03	Definiowanie zasobów niezbędnych do stworzenia i utrzymania SOC	2
C04	Identyfikacja priorytetów w zakresie cyberincydentów	2

IV.	**KORELACJA EFEKTÓW UCZENIA SIĘ**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyki PRK*
W01	*Lxb_W01*	*ZCU_W01, ZCU_W05*	*P6U_W, P6S_WG, P7U_W,*

			P7S_WK
W02	*Lxb_W02*	*ZCU_W01, ZCU_W05*	*P6U_W, P6S_WG, P7U_W, P7S_WK*
W03	*Lxb_W03*	*ZCU_W01, ZCU_W05*	*P6U_W, P6S_WG, P7U_W, P7S_WK*
C01	*Lxb_W04, Lxb_U01, Lxb_K01, Lxb_K02*	*ZCU_W01, ZCU_W05, ZCU_U01, ZCU_U02, ZCU_U03, ZCU_U05, ZCU_K03, ZCU_K04*	*P6U_W, P6S_WG, P7U_W, P7S_WK, P6U_U, P6S_UW, P7U_U, P7S_UW, P7S_UK, P7S_UO, P7U_K, P7S_KO, P7S_KR*
C02	*Lxb_U02, Lxb_K01, Lxb_K02*	*ZCU_U01, ZCU_U02, ZCU_U03, ZCU_U05, ZCU_K03, ZCU_K04*	*P6U_U, P6S_UW, P7U_U, P7S_UW, P7S_UK, P7S_UO, P7U_K, P7S_KO, P7S_KR*
C03	*Lxb_U03, Lxb_K01, Lxb_K02*	*ZCU_U01, ZCU_U02, ZCU_U03, ZCU_U05, ZCU_K03, ZCU_K04*	*P6U_U, P6S_UW, P7U_U, P7S_UW, P7S_UK, P7S_UO, P7U_K, P7S_KO, P7S_KR*
C04	*Lxb_U04, Lxb_K01, Lxb_K02*	*ZCU_U01, ZCU_U02, ZCU_U03, ZCU_U05, ZCU_K03, ZCU_K04*	*P6U_U, P6S_UW, P7U_U, P7S_UW, P7S_UK, P7S_UO, P7U_K, P7S_KO, P7S_KR*

V. NAKŁAD PRACY STUDENTA

Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**6**	**X**	**50**	**2**
Ćwiczenia	**12**			
Konsultacje (zaliczenie nieobecności, rozliczenie rygorów, poprawy)	**2**			
Przygotowanie do ćwiczeń	**X**	**10**		
Opanowanie informacji		**10**		
Przygotowanie do rozliczenia rygorów		**10**		
RAZEM	**20**	**30**		

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 projektu	0,6

VIII. LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

OBOWIĄZKOWA

1.	*ISO 27035*
2.	M.Syed. *Metoda czarnej skrzynki. Zaskakująca prawda o naturze sukcesu,* Insignis 2017
	J. Syta, Model: *Skuteczne monitorowanie cyberbezpieczeństwa*

UZUPEŁNIAJĄCA

1.	*MITRE ATT&CK*
2.	Materiały przygotowane przez wykładowców

IX. PROWADZĄCY PRZEDMIOT

Stopień, imię i nazwisko	dr hab. Jerzy Kosiński + zespół
adres e-mail	j.kosinski@amw.gdynia.pl

3.1.9 Skuteczne metody zarządzania projektami i usługami

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:	**Skuteczne metody zarządzania projektami i usługami**	*Kod:*	**Zyp**
Kierunek studiów:	Zarządzanie cyberbezpieczeństwem i usługami cyfrowymi		
Poziom studiów:	Studia podyplomowe Executive MBA		
Forma studiów:	Studia niestacjonarne		
Liczba ECTS:	3		
Semestr:	2		
Wymagania wstępne:	Podstawowa wiedza z zakresu zarządzania projektami		
Język wykładowy:	polski		
Cel przedmiotu:	**C01**	Zaznajomienie studentów z problematyką ochrona danych osobowych	
	C02	Zaznajomienie studentów z procesem zarządzania projektami IT	
	C03	Zaznajomienie studentów z procesem zarządzania usługami IT	
	C04	Zaznajomienie studentów z narzędziami wspierającymi zarządzanie wiedzą	
	C05	Zaznajomienie studentów z procesem rozwoju oprogramowania w sposób zwinny i bezpieczny	

II.	EFEKTY UCZENIA SIĘ		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Zyp_W01**	Znajomość problematyki ochrona danych osobowych	Dyskusja
	Zyp_W02	Znajomość procesu zarządzania projektami IT	Dyskusja
	Zyp_W03	Znajomość procesu zarządzania usługami IT	Dyskusja
	Zyp_W04	Znajomość narzędzi wspierających zarządzanie wiedzą	Dyskusja
	Zyp_W05	Znajomość procesu rozwoju oprogramowania w sposób zwinny i bezpieczny	Dyskusja
Umiejętności:	**Zyp_U01**	Potrafi przygotować zgłoszenie incydentu do UODO	Praca zaliczeniowa
	Zyp_U02	Potrafi generować wymagania SMART	Praca zaliczeniowa
	Zyp_U03	Potrafi identyfikować klientów (stron zainteresowanych) oraz wartość dodaną, którą należy im dostarczyć	Praca zaliczeniowa
	Zyp_U04	Potrafi przygotować wymagania w zakresie funkcjonalności systemów zarządzania wiedzą	Praca zaliczeniowa
	Zyp_U05	Potrafi przygotować *user stories* i *backlog*	Praca zaliczeniowa
Kompetencje społeczne:	**Zyp_K01**	Inicjuje i uczestniczy konstruktywnie w przygotowaniu projektów dotyczących zarządzania cyberbezpieczeństwem	Dyskusja
	Zyp_K02	Rozwiązuje problemy o różnym poziomie złożoności dotyczące cyberbezpieczeństwa	Dyskusja

III.	TREŚCI PROGRAMOWE	
Forma	*Tematyka*	*Liczba godzin*
W01	Ochrona danych osobowych	2
W02	Zarządzanie projektami IT	2
W03	Zarządzanie usługami IT	2
W04	Narzędzia wspierające zarządzanie wiedzą	2
W05	Rozwój oprogramowania w sposób zwinny i bezpieczny	2
C01	Analiza skutków oraz przygotowywanie zgłoszenia incydentu do UoDO	2
C02	Generowanie wymagań dla nowych rozwiązań zgodnie z metodą SMART	2
C03	Identyfikacja wewnętrznych i zewnętrznych klientów, określanie usług oraz definiowanie	6

	„wartości dodanej”	
C04	Dokumentowanie wiedzy z wykorzystaniem narzędzi zapewniających współpracę	2
C05	Tworzenie zbiorów wymagań dla rozwijanego oprogramowanie w sposób „zwinny”	2

IV. KORELACJA EFEKTÓW UCZENIA SIĘ

Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyki PRK*
W01	*Zyp_W01*	*ZCU_W02, ZCU_W03, ZCU_W04, ZCU_W06, ZCU_W07*	*P6U_W, P6S_WG, P7U_W, P7S_WG, P7S_WK, P7U_W, P7S_WK*
W02	*Zyp_W02*	*ZCU_W02, ZCU_W03, ZCU_W04, ZCU_W06, ZCU_W07*	*P6U_W, P6S_WG, P7U_W, P7S_WG, P7S_WK, P7U_W, P7S_WK*
W03	*Zyp_W03*	*ZCU_W02, ZCU_W03, ZCU_W04, ZCU_W06, ZCU_W07*	*P6U_W, P6S_WG, P7U_W, P7S_WG, P7S_WK, P7U_W, P7S_WK*
W04	*Zyp_W04*	*ZCU_W02, ZCU_W03, ZCU_W04, ZCU_W06, ZCU_W07*	*P6U_W, P6S_WG, P7U_W, P7S_WG, P7S_WK, P7U_W, P7S_WK*
W05	*Zyp_W05*	*ZCU_W02, ZCU_W03, ZCU_W04, ZCU_W06, ZCU_W07*	*P6U_W, P6S_WG, P7U_W, P7S_WG, P7S_WK, P7U_W, P7S_WK*
C01	*Zyp_U01, Zyp_K01, Zyp_K02*	*ZCU_U01, ZCU_U03, ZCU_U04, ZCU_K03, ZCU_K04*	*P6U_U, P6S_UW, P7U_U, P7S_UK, P7U_K, P7S_KO, P7S_KR*
C02	*Zyp_U02, Zyp_K01, Zyp_K02*	*ZCU_U01, ZCU_U03, ZCU_U04, ZCU_K03, ZCU_K04*	*P6U_U, P6S_UW, P7U_U, P7S_UK, P7U_K, P7S_KO, P7S_KR*
C03	*Zyp_U03, Zyp_K01, Zyp_K02*	*ZCU_U01, ZCU_U03, ZCU_U04, ZCU_K03, ZCU_K04*	*P6U_U, P6S_UW, P7U_U, P7S_UK, P7U_K, P7S_KO, P7S_KR*
C04	*Zyp_U04, Zyp_K01, Zyp_K02*	*ZCU_U01, ZCU_U03, ZCU_U04, ZCU_K03, ZCU_K04*	*P6U_U, P6S_UW, P7U_U, P7S_UK, P7U_K, P7S_KO, P7S_KR*
C05	*Zyp_U05, Zyp_K01, Zyp_K02*	*ZCU_U01, ZCU_U03, ZCU_U04, ZCU_K03, ZCU_K04*	*P6U_U, P6S_UW, P7U_U, P7S_UK, P7U_K, P7S_KO, P7S_KR*

V. NAKŁAD PRACY STUDENTA

Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**10**	**X**	**75**	**3**
Ćwiczenia	**14**			
Konsultacje (zaliczenie nieobecności, rozliczenie rygorów, poprawy)	**2**			
Przygotowanie do ćwiczeń	**X**	**20**		
Opanowanie informacji		**20**		
Przygotowanie do rozliczenia rygorów		**19**		
RAZEM	**16**	**59**		

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 projektu	0,6

VIII.	LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA
	OBOWIĄZKOWA
1.	E. M. Goldratt. *Cel 1 i 2 - Doskonałość w produkcji*, Mint Books, Warszawa 2007, 2008
2.	J. K. Liker, *Droga Toyoty (TPS*), MT Biznes, Warszawa 2016
3.	J. Humbel, *Continous Delivery*, 2010
	UZUPEŁNIAJĄCA
1.	G. Kim, *Projekt Fenix*, Helion, Gliwice 2016
2.	G. Kim, Projekt jednorożec, Helion, Gliwice 2020
3.	T. Gilb, *Value Agile*
4.	Materiały przygotowane przez wykładowców

IX.	PROWADZĄCY PRZEDMIOT
Stopień, imię i nazwisko	dr inż. Jakub Syta + zespół
adres e-mail	j.syta@amw.gdynia.pl

3.2. Matryca efektów uczenia się

Przedmiot/ Symbol	Ekonomia i finanse dla kadry zarządzającej	Prawne aspekty zarządzania usługami kluczowymi	Zarządzanie ryzykiem dla bezpieczeństwa informacji	Zarządzanie usługami kluczowymi	Nowoczesne technologie	Nowoczesne metody doskonalenia organizacji	Zarządzanie bezpieczeństwem informacji	Monitorowanie oraz reagowanie na cyberincydenty	Skuteczne metody zarządzania projektami i usługami	PODSUMOWANIE
Wiedza										
ZCU_W01			X	X			X	X		4
ZCU_W02		X		X	X	X			X	5
ZCU_W03			X	X		X			X	4
ZCU_W04				X	X	X			X	4
ZCU_W05	X	X					X	X		4
ZCU_W06	X	X				X	X		X	5
ZCU_W07	X	X		X		X	X		X	6
Umiejętności										
ZCU_U01	X	X	X	X	X	X	X	X	X	9
ZCU_U02			X				X	X		3
ZCU_U03				X	X		X	X	X	5
ZCU_U04		X	X			X			X	4
ZCU_U05	X			X		X	X	X		5
Kompetencje społeczne										
ZCU_K01	X			X	X					3
ZCU_K02		X					X			2
ZCU_K03	X	X			X		X	X	X	6
ZCU_K04			X	X		X	X	X	X	6
ZCU_K05			X	X		X	X			4

3.3. 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 projektu, którego 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 projektu,
- 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. Założono, że już sam charakter tych zajęć i nałożonych zadań zmusza studenta do wyrabiania określonych umiejętności związanych z praktycznym przygotowaniem zawodowym.

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.

3.4. 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.	Ekonomia i finanse dla kadry zarządzającej	16	16			32	Z	3
	2.	Prawne aspekty zarządzania usługami kluczowymi	8	8			16	Z	2
	3.	Zarządzanie ryzykiem dla bezpieczeństwa informacji	6	10			16	Z	2
	4.	Zarządzanie usługami kluczowymi	6	6			12	Z	2
	5.	Nowoczesne technologie	12	8			20	Z	3
	6.	Nowoczesne metody doskonalenia organizacji	14	10			24	Z	3
	Razem		**62**	**58**			**120**		**15**
Semestr 2	1.	Zarządzanie usługami kluczowymi	36	12			48	Z	5
	2.	Zarządzanie bezpieczeństwem informacji	20	26			46	Z	5
	3.	Monitorowanie oraz reagowanie na cyberincydenty	6	12			18	Z	2
	4.	Skuteczne metody zarządzania projektami i usługami	10	14			24	Z	3
	Razem		**72**	**64**			**136**		**15**
Ogółem							**256**		**30**