Akademia Marynarki Wojennej
im. Bohaterów Westerplatte
Ul. Śmidowicza 69 81-127 Gdynia
tel. (+48) 261 26 25 14, fax. (+48) 261 26 2963

Załącznik do uchwały nr ……. Senatu Akademii Marynarki Wojennej im. Bohaterów Westrplatte z dnia ……. roku w sprawie dostosowania programów studiów drugiego stopnia na kierunku Systemy informacyjne w bezpieczeństwie o profilu ogólnoakademickim.

PROGRAM STUDIÓW

WYDZIAŁ DOWODZENIA I OPERACJI MORSKICH

SYSTEMY INFORMACYJNE W BEZPIECZEŃSTWIE

PROFIL OGÓLNOAKADEMICKI

Studia drugiego stopnia (magisterskie):

- ***Stacjonarne***
- ***Niestacjonarne***

GDYNIA 2024

SPIS TREŚCI

1. OGÓLNA CHARAKTERYSTYKA STUDIÓW DRUGIEGO STOPNIA 6

1.1. Informacje podstawowe 6

1.2. Przyporządkowanie kierunku studiów do dziedzin oraz dyscyplin, do których odnoszą się efekty uczenia się 11

1.3. Cele kształcenia 11

1.4. Potrzeby społeczno-gospodarcze 13

1.5. Związek z misją uczelni i z jej strategią rozwoju 15

2. EFEKTY UCZENIA SIĘ 16

3. MODUŁY ZAJĘĆ 20

3.1. Karty przedmiotów modułu zajęć podstawowych studiów stacjonarnych – A 31

3.2. Karty przedmiotów modułu zajęć kierunkowych studiów stacjonarnych– B 88

3.3. Karty przedmiotów modułu kształceniastudiów stacjonarnych w zakresie Cyberbezpieczeństwo – C 121

3.4. Karty przedmiotów modułu kształceniastudiów stacjonarnych w zakresie Analiza danych i informatyka śledcza – C 160

3.5. Karta przedmiotu modułu dyplomowego studiów stacjonarnych – D 195

3.6. Karty przedmiotów modułu zajęć podstawowych studiów niestacjonarnych – A 198

3.7. Karty przedmiotów modułu zajęć kierunkowych studiów niestacjonarnych– B 255

3.8. Karty przedmiotów modułu kształceniastudiów studiów niestacjonarnych w zakresie Cyberbezpieczeństwo – C 288

3.9. Karty przedmiotów modułu kształcenia studiów niestacjonarnych w zakresie Analiza danych i informatyka śledcza – C 327

3.10. Karta przedmiotu modułu dyplomowego studiów niestacjonarnych – D 362

3.11. Matryca efektów uczenia się w zakresie Cyberbezpieczeństwo studiów stacjonarnych i niestacjonarnych 365

3.12. Matryca efektów uczenia się w zakresie Analiza danych i informatyka śledczastudiów stacjonarnych i niestacjonarnych 366

4. SPOSOBY WERYFIKACJI I OCENY EFEKTÓW UCZENIA SIĘ OSIĄGANYCH PRZEZ STUDENTA W TRAKCIE CAŁEGO CYKLU KSZTAŁCENIA 367

5. HARMONOGRAM REALIZACJI PROGRAMU STUDIÓW (PLAN STUDIÓW) . 368

5.1. Plan studiów stacjonarnych dla zakresu Cyberbezpieczeństwo 369

5.2. Plan studiów stacjonarnych dla zakresu Analiza danych i informatyka śledcza 371

5.3. Plan studiów niestacjonarnych dla zakresu Cyberbezpieczeństwo 373

5.4. Plan studiów niestacjonarnych dla zakresu Analiza danych i informatyka śledcza 375
6. BILANS PUNKTÓW ECTS 377
6.1. Wskaźniki łączne dotyczące programu studiów stacjonarnych II stopnia – zakres Cyberbezpieczeństwo 377
6.1.1. Łączna liczba punktów ECTS jaką student musi uzyskać w ramach zajęć prowadzonych z bezpośrednim udziałem nauczycieli akademickich lub innych osób prowadzących zajęcia 377
6.1.2. Łączna liczba punktów ECTS w ramach zajęć związanych z prowadzoną w uczelni działalnością naukową w dyscyplinie nauki o bezpieczeństwie (więcej niż 50% punktów ECTS) 378
6.1.3. Łączna liczba punktów ECTS w ramach zajęć do wyboru, nie mniej niż 30% liczby punktów ECTS 378
6.2. Wskaźniki łączne dotyczące programu studiów stacjonarnych II stopnia – zakres Analiza danych i informatyka śledcza 379
6.2.1. Łączna liczba punktów ECTS jaką student musi uzyskać w ramach zajęć prowadzonych z bezpośrednim udziałem nauczycieli akademickich lub innych osób prowadzących zajęcia 379
6.2.2. Łączna liczba punktów ECTS w ramach zajęć związanych z prowadzoną w uczelni działalnością naukową w dyscyplinie nauki o bezpieczeństwie (więcej niż 50% punktów ECTS) 380
6.2.3. Łączna liczba punktów ECTS w ramach zajęć do wyboru, nie mniej niż 30% liczby punktów ECTS 380
6.3. Wskaźniki łączne dotyczące programu studiów niestacjonarnych II stopnia – zakres Cyberbezpieczeństwo 381
6.3.1. Łączna liczba punktów ECTS jaką student musi uzyskać w ramach zajęć prowadzonych z bezpośrednim udziałem nauczycieli akademickich lub innych osób prowadzących zajęcia 381
6.3.2. Łączna liczba punktów ECTS w ramach zajęć związanych z prowadzoną w uczelni działalnością naukową w dyscyplinie nauki o bezpieczeństwie (więcej niż 50% punktów ECTS) 382
6.3.3. Łączna liczba punktów ECTS w ramach zajęć do wyboru, nie mniej niż 30% liczby punktów ECTS 382
6.4. Wskaźniki łączne dotyczące programu studiów niestacjonarnych II stopnia – zakres Analiza danych i informatyka śledcza 383
6.4.1. Łączna liczba punktów ECTS jaką student musi uzyskać w ramach zajęć prowadzonych z bezpośrednim udziałem nauczycieli akademickich lub innych osób prowadzących zajęcia 383

6.4.2. Łączna liczba punktów ECTS w ramach zajęć związanych z prowadzoną w uczelni działalnością naukową w dyscyplinie nauki o bezpieczeństwie (więcej niż 50% punktów ECTS) 384

6.4.3. Łączna liczba punktów ECTS w ramach zajęć do wyboru, nie mniej niż 30% liczby punktów ECTS..... 384

1. OGÓLNA CHARAKTERYSTYKA STUDIÓW DRUGIEGO STOPNIA

1.1. Informacje podstawowe

Tabela 1. Informacje podstawowe o kierunku studiów drugiego stopnia

Nazwa kierunku	Systemy informacyjne w bezpieczeństwie
Poziom kształcenia	Studia drugiego stopnia
Profil kształcenia	Ogólnoakademicki
Forma studiów	Stacjonarne Niestacjonarne
Czas trwania studiów	2 lata (4 semestry)
Liczba punktów ECTS konieczna do ukończenia studiów	120
Tytuł zawodowy nadany absolwentom	Magister

Przyjęty model studiów **drugiego stopnia** przewiduje, że na Wydziale Dowodzenia i Operacji Morskich Akademii Marynarki Wojennej na kierunku **Systemy informacyjne w bezpieczeństwie**:

- podstawową formą kształcenia są studia stacjonarne,
- studentami są absolwenci szkół wyższych legitymujący się dyplomem ukończenia studiów pierwszego stopnia,
- studia będą prowadzone na zasadach ogólnych, z możliwością wyboru fakultatywnych przedmiotów, zapewniających zdobycie pogłębionej wiedzy z zakresu szeroko rozumianego bezpieczeństwa i jego teleinformatycznego wymiaru.

Program studiów koncentruje się wokół dwóch zakresów, tj. Cyberbezpieczeństwo oraz Analiza danych i informatyka śledcza.

Studia na kierunku Systemy informacyjne w bezpieczeństwie drugiego stopnia realizowane są w formie studiów stacjonarnych i niestacjonarnych. Zajęcia dydaktyczne prowadzone są w strukturze roku akademickiego obejmującego 2 semestry (jesienny i letni), a każdy semestr kończy się sesją egzaminacyjną. Zajęcia dydaktyczne rozpoczynają się w październiku i kończą się w czerwcu następnego roku kalendarzowego. Łączny bilans programowych zajęć dydaktycznych w semestrze wynosi 15 tygodni, a łączna liczba godzin zajęć dydaktycznych (w tym konsultacje, rozliczenie rygorów):

- podczas studiów stacjonarnych dla dla dla zakresu Cyberbezpieczeństwo 1534 h, dla zakresu Analiza danych i informatyka śledcza 1534 h.

– podczas studiów niestacjonarnych dla zakresu Cyberbezpieczeństwo 966 h, dla zakresu Analiza danych i informatyka śledcza 961 h.

Tabela 2. Łączna liczba godzin w ramach zakresów studiów drugiego stopnia

Zakres	Liczba godzin (studia stacjonarne)	Liczba godzin (studia niestacjonarne)
Cyberbezpieczeństwo	1534	966
Analiza danych i informatyka śledcza	1534	961

Wszystkie przedmioty programowe podlegają określonym rygorom dydaktycznym, co implikuje w ramach studiów drugiego stopnia 9 egzaminów sesyjnych i uzyskanie 28 zaliczeń.

Warunkiem przystąpienia do egzaminu sesyjnego jest uzyskanie pozytywnej oceny z ćwiczeń, seminariów i kolokwiów kontrolnych, a warunkiem zaliczenia semestru jest zaliczenie wszystkich przedmiotów programowych (objętych zaliczeniem lub egzaminem) obowiązujących w danym semestrze.

Na początku III semestru studiów drugiego stopnia studenci otrzymują propozycje tematów prac magisterskich, które do końca semestru w ramach seminariów muszą być zaakceptowane i zakończone koncepcją metodologiczną pracy.

Warunkiem dopuszczenia studenta do obrony pracy magisterskiej po zaliczeniu IV semestru studiów drugiego stopnia, jest otrzymanie absolutorium dyplomowego oraz uzyskanie pozytywnej opinii od promotora pracy, a także od recenzenta pracy magisterskiej, wyznaczanego przez Dziekana WDiOM.

Szczegółowy tok i organizację procesu dydaktycznego w danym semestrze reguluje „Rozkład zajęć dydaktycznych dla grupy" opracowywany według aktualnego kalendarza.

Warunkiem **ukończenia studiów i uzyskania tytułu magistra** jest zaliczenie wszystkich przewidzianych programem wykładów, ćwiczeń, konwersatoriów, laboratoriów i projektów oraz złożenie i obrona pracy magisterskiej, poprzedzone uczestnictwem w seminarium dyplomowym, co przekłada się na obligatoryjne **uzyskanie przez studenta 120 punktów ECTS**.

Program **studiów stacjonarnych** drugiego stopnia dla zakresu **Cyberbezpieczeństwo** obejmuje 1534 godzin programowych (kontaktowych) zajęć dydaktycznych (3047 godzin łącznie z nakładem pracy własnej studenta):

A – przedmioty kształcenia podstawowego - 363 godziny odpowiadają 28 punktom ECTS (706 godzin łącznie z nakładem pracy własnej studenta),

B – przedmioty kierunkowe - 508 godzin odpowiadaja 39 punktom ECTS (978 godzin łącznie z nakładem pracy własnej studenta),

C – przedmioty dla zakresu – 578 godziny odpowiadają uzyskaniu 42 punktów ECTS (1088 godzin łącznie z nakładem pracy własnej studenta),

D – praca dyplomowa – 85 godzin (275 godzin łącznie z nakładem pracy własnej studenta), za przygotowanie pracy magistrskiej i przygotowanie do egzaminu magisterskiego student otrzymuje 11 punktów ECTS (w liczbie tej ujęty jest także nakład pracy własnej studenta).

Tabela 3. Grupy przedmiotów, godziny i punkty ECTS dla zakresu Cyberbezpieczeństwo studiów stacjonarnych drugiego stopnia

Treści kształcenia w zakresie Cyberbezpieczeństwo	Godziny	Punkty ECTS
A - przedmioty kształcenia podstawowego	363	28
B - przedmioty kierunkowe	508	39
C - przedmioty dla zakresu	578	42
D - praca dyplomowa	85	11
ŁĄCZNIE	**1534**	**120**

Program **studiów stacjonarnych** drugiego stopnia dla zakresu **Analiza danych i informatyka śledcza** obejmuje 1534 godzin programowych (kontaktowych) zajęć dydaktycznych (3047 godzin łącznie z nakładem pracy własnej studenta):

A – przedmioty kształcenia podstawowego - 363 godziny odpowiadają 28 punktom ECTS (706 godzin łącznie z nakładem pracy własnej studenta),

B – przedmioty kierunkowe - 508 godzin odpowiadaja 39 punktom ECTS (978 godzin łącznie z nakładem pracy własnej studenta),

C – przedmioty dla zakresu – 578 godziny odpowiadają uzyskaniu 42 punktów ECTS (1088 godzin łącznie z nakładem pracy własnej studenta),

D – praca dyplomowa – 85 godzin (275 godzin łącznie z nakładem pracy własnej studenta), za przygotowanie pracy magistrskiej i przygotowanie do egzaminu magisterskiego student otrzymuje 11 punktów ECTS (w liczbie tej ujęty jest także nakład pracy własnej studenta).

Tabela 4. Grupy przedmiotów, godziny i punkty ECTS dla zakresu Analiza danych i informatyka śledcza studiów stacjonarnych drugiego stopnia

Treści kształcenia w zakresie Analiza danych i informatyka śledcza	Godziny	Punkty ECTS
A - przedmioty kształcenia podstawowego	363	28
B - przedmioty kierunkowe	508	39
C - przedmioty dla zakresu	578	42

D - praca dyplomowa	85	11
ŁĄCZNIE	**1534**	**120**

Program **studiów niestacjonarnych** drugiego stopnia dla zakresu **Cyberbezpieczeństwo** obejmuje 966 godziny programowe (kontaktowe) zajęć dydaktycznych (3047 godzin łącznie z nakładem pracy własnej studenta):

A – przedmioty kształcenia podstawowego - 230 godzin odpowiada 28 punktom ECTS (706 godzin łącznie z nakładem pracy własnej studenta),

B – przedmioty kierunkowe - 313 godzin odpowiada 39 punktom ECTS (978 godzin łącznie z nakładem pracy własnej studenta),

C – przedmioty dla zakresu – 338 godzin odpowiada uzyskaniu 42 punktów ECTS (1088 godzin łącznie z nakładem pracy własnej studenta),

D – praca dyplomowa – 85 godzin (275 godzin łącznie z nakładem pracy własnej studenta), za przygotowanie pracy licencjackiej i przygotowanie do egzaminu dyplomowego student otrzymuje 11 punktów ECTS (w liczbie tej ujęty jest także nakład pracy własnej studenta).

Tabela 5. Grupy przedmiotów, godziny i punkty ECTS dla zakresu Cyberbezpieczeństwo studiów niestacjonarnych drugiego stopnia

Treści kształcenia w zakresie Cyberbezpieczeństwo	Godziny	Punkty ECTS
A - przedmioty kształcenia podstawowego	230	28
B - przedmioty kierunkowe	313	39
C - przedmioty dla zakresu	338	42
D - praca dyplomowa	85	11
ŁĄCZNIE	**966**	**120**

Program **studiów niestacjonarnych** drugiego stopnia dla zakresu **Analiza danych i informatyka śledcza** obejmuje 961 godziny programowe (kontaktowe) zajęć dydaktycznych (3047 godzin łącznie z nakładem pracy własnej studenta):

A – przedmioty kształcenia podstawowego - 230 godzin odpowiada 28 punktom ECTS (706 godzin łącznie z nakładem pracy własnej studenta),

B – przedmioty kierunkowe - 313 godzin odpowiada 39 punktom ECTS (978 godzin łącznie z nakładem pracy własnej studenta),

C – przedmioty dla zakresu – 333 godzin odpowiada uzyskaniu 42 punktów ECTS (1088 godzin łącznie z nakładem pracy własnej studenta),

D – praca dyplomowa – 85 godzin (275 godzin łącznie z nakładem pracy własnej studenta), za przygotowanie pracy licencjackiej i przygotowanie do egzaminu dyplomowego student otrzymuje 11 punktów ECTS (w liczbie tej ujęty jest także nakład pracy własnej studenta).

Tabela 6. Grupy przedmiotów, godziny i punkty ECTS dla zakresu Analiza danych i informatyka śledcza studiów niestacjonarnych drugiego stopnia

Treści kształcenia w zakresie Analiza danych i informatyka śledcza	Godziny	Punkty ECTS
A - przedmioty kształcenia podstawowego	230	28
B - przedmioty kierunkowe	313	39
C - przedmioty dla zakresu	333	42
D - praca dyplomowa	85	11
ŁĄCZNIE	**961**	**120**

Przedmioty kształcenia podstawowego i kierunkowego skoncentrowane są w pierwszych 2 semestrach studiów, a przedmioty obejmujące jeden z trzech zakresów realizowane są na ostatnich 2 semestrach studiów. Seminarium dyplomowe (15 godzin) realizowane jest w semestrze 3, natomiast redakcja i edycja pracy magisterskiej realizowane są sukcesywnie przez dwa ostatnie semestry.

Na ogólną liczbą 1534 godzin programowych dla zakresu **Cyberbezpieczeństwo** studiów **stacjonarnych** składa się:

- 840 godzin wykładów,
- 495 godzin ćwiczeń,
- 285 godzin laboratoriów,
- 194 godziny konsultacji i rozliczenia rygorów.

Na ogólną liczbą 1534 godzin programowych dla zakresu **Analiza danych i informatyka śledcza** studiów **stacjonarnych** składa się:

- 850 godzin wykładów,
- 480 godzin ćwiczeń,
- 290 godzin laboratoriów,
- 194 godziny konsultacji i rozliczenia rygorów.

Na ogólną liczbą 966 godzin programowych dla zakresu **Cyberbezpieczeństwo** studiów **niestacjonarnych** składa się:

- 470 godzin wykładów,

- 300 godzin ćwiczeń,
- 170 godzin laboratoriów,
- 194 godzin konsultacji i rozliczenia rygorów.

Na ogólną liczbą 961 godzin programowych dla zakresu **Analiza danych i informatyka śledcza** studiów **niestacjonarnych** składa się:

- 465 godzin wykładów,
- 300 godzin ćwiczeń,
- 170 godzin laboratoriów,
- 194 godzin konsultacji i rozliczenia rygorów.

1.2. Przyporządkowanie kierunku studiów do dziedzin oraz dyscyplin, do których odnoszą się efekty uczenia się

Kierunek studiów przyporządkowany jest do dziedziny **nauki społeczne**, w dyscyplinie **nauki o bezpieczeństwie**. Dyscyplina ta jest dyscypliną wiodąca, i w jej ramach będą uzyskiwane efekty uczenia się.

Tabela 7. Przyporządkowanie kierunku studiów do dziedzin i dyscyplin

Procentowy udział liczby punktów ECTS przyporządkowanych do poszczególnych dyscyplin naukowych	Nauki o bezpieczeństwie	100%

1.3. Cele kształcenia

Głównym celem kształcenia studentów na studiach drugiego stopnia na kierunku Systemy informacyjne w bezpieczeństwie jest wyposażenie absolwentów w nowoczesną, utylitarną i pogłębioną wiedzę teoretyczną oraz umiejętności praktyczne, stwarzające możliwość podjęcia pracy w jednostkach organizacyjnych i instytucjach państwowych odpowiedzialnych za bezpieczeństwo informacyjne na stanowiskach analityków oraz operatorów systemów i sieci teleinformatycznych, jak również w sektorze prywatnym w przedsiębiorstwach realizujących usługi związane z cyberbezpieczeństwem i analizą danych. Uzupełnieniem celu głównego jest wypełnienie postulatów przyjętych w 2023 roku przez Komisję Europejską „Europejska deklaracja praw i zasad cyfrowych w cyfrowej dekadzie", który w części poświęconej edukacji cyfrowej zobowiązuje do: Wspierania wysiłków umożliwiających wszystkim osobom uczącym się i nauczycielom nabywanie niezbędnych

umiejętności i kompetencji cyfrowych, w tym umiejętności korzystania z mediów i krytycznego myślenia, oraz dzielenie się tymi umiejętnościami i kompetencjami, aby mogli oni aktywnie uczestniczyć w gospodarce, społeczeństwie i procesach demokratycznych. Propagowania i wspierania wysiłków na rzecz wyposażenia wszystkich instytucji kształcenia i szkolenia w łączność i infrastrukturę cyfrową oraz narzędzia cyfrowe.

Celem naukowym kształcenia na kierunku Systemy informacyjne w bezpieczeństwie w Akademii Marynarki Wojennej jest przekazanie nowoczesnej, pogłębionej wiedzy teoretycznej i umiejętności praktycznych potrzebnych absolwentom do pomyślnego wywiązywania się z obowiązków zawodowych na różnych stanowiskach służbowych w organach administracji publicznej, w zespołach reagowania na incydenty komputerowe, w administracji rządowej i samorządowej, służbach, inspekcjach i strażach oraz u przedsiębiorców świadczących usługi w zakresie bezpieczeństwa i analizy danych oraz szeroko rozumianego cyberbezpieczeństwa.

Misją dydaktyczną studiów drugiego stopnia na kierunku Systemy informacyjne w bezpieczeństwie jest przekazanie pogłębionej wiedzy teoretycznej oraz praktycznej z zakresu: zarządzanie systemami bezpieczeństwa wewnętrznego, inżynierii systemów i projektowanie procesów, audytu i certyfikacja systemów informatycznych, oceny ryzyka i prognozowanie w bezpieczeństwie, zarządzania projektem, komunikacji społecznej, certyfikacja Systemu Zarządzania ISO/IEC 27001 oraz sztucznej inteligencji.

Studia drugiego stopnia na kierunku Systemy informacyjne w bezpieczeństwie mają charakter studiów zawodowych, których celem jest dostarczenie wiedzy teoretycznej i praktycznych umiejętności niezbędnych do wykonywania pracy zawodowej w zakresie cyberbezpieczerństwa, w tym: zarządzanie projektami informatycznymi, akredytacja bezpieczeństwa teleinformatycznego, testy penetracyjne, bezpieczeństwo sieci komputerowych i bezprzewodowych, elementy kryptologii, administrowanie systemem Linux, cyberbezpieczeństwo, prognozowanie cyberzagrożeń, symulacja komputerowa, podstawy prawne cyberbezpieczeństwa. W zakresie analizy danych i informatyki śledczej, w tym: pozyskiwanie i analiza danych z technologii bezzałogowych, zastosowanie kryptologii w informatyce śledczej, testy penetracyjne, bezpieczeństwo sieci komputerowych i bezprzewodowych, techniki pozyskiwania cyfrowego materiału dowodowego, biały wywiad – techniki zaawansowane, zarzadzanie ryzykiem bezpieczeństwa systemów, zagrożenia bezpieczeństwa aplikacji i systemów, metody ataku i obrony w cyberprzestrzeni, podstawy prawne cyberbezpieczeństwa.

1.4. Potrzeby społeczno-gospodarcze

Studia na kierunku Systemy informacyjne w bezpieczeństwie stanowią odpowiedź na potrzeby społeczno-gospodarcze kraju, z uwzględnieniem specyfiki województwa pomorskiego. Kierunek zakłada efektywne i wielowymiarowe współdziałanie z otoczeniem Akademii Marynarki Wojennej, w tym współpracę z interesariuszami istotną dla osiągnięcia zakładanych efektów uczenia się i właściwej diagnozy potrzeb rynku pracy. Wspomniana współpraca dotyczy m.in. konsultacji w zakresie pożądanych efektów uczenia się, wspólnej organizacji przedsięwzięć naukowych i dydaktycznych, czego wymiernym efektem jest bieżąca modyfikacja oferty dydaktycznej i obowiązujących programów studiów.

Warto podkreślić, że kierunek Systemy informacyjne w bezpieczeństwie jest ściśle skorelowany z obszarami badań naukowych kadry WDiOM i stanowi odpowiedź na dynamicznie zmieniające się uwarunkowania bezpieczeństwa RP, zwłaszcza w aspekcie międzynarodowej współpracy Polski realizowanej w ramach takich organizacji jak UE, NATO, ONZ czy OBWE, w ramach której podejmowane są działania w walce z rosnącą liczbą incydentów powodowanych nielegalną aktywnością w cyberprzestrzeni, prowadzącą do strat materialnych i wizerunkowych. Proponowane zakresy na drugim stopniu studiów kierunku Systemy informacyjne w bezpieczeństwie są zatem odzwierciedleniem zarówno potrzeb instytucji rządowych, samorządowych i gospodarczych w zakresie utrzymania systemów teleinformatycznych, ale także zadań, które stawia sobie Wydział i Uczelnia w ramach kształtowania systemu bezpieczeństwa RP.

Przyjęty program studiów dla kierunku Systemy informacyjne w bezpieczeństwie drugiego stopnia prezentuje interdyscyplinarne podejście do problematyki bezpieczeństwa. Profil studiów ma charakter ogólnoakademicki.

Absolwenci po ukończeniu studiów na kierunku Systemy informacyjne w bezpieczeństwie będą przygotowani do podjęcia pracy w jednostkach organizacyjnych organów administracji publicznej oraz instytucjach i podmiotach gospodarczych odpowiedzialnych za bezpieczeństwo informacyjne na stanowiskach analityków, inspektorów oraz osób odpowiedzialnych za utrzymanie systemów i sieci teleinformatycznych.

Potencjalnym rynkiem zatrudnienia dla absolwentów o najwyższych kwalifikacjach są potrzeby kadrowe resortu obrony narodowej, innych służb mundurowych oraz administracji publicznej. Inną sferą zatrudnienia cywilnych absolwentów są instytucje naukowo-badawcze, ośrodki wdrożeniowe, placówki kulturalno-oświatowe, szkolnictwo wyższe, sektor przemysłu obronnego oraz dynamicznie rozwijany sektor współpracy cywilno-wojskowej i różne instytucje obsługujące wielonarodowe siły sojusznicze.

Opracowane plany studiów zapewniają absolwentom wiedzę, ale także umiejętności, które umożliwiają przygotowanie ich do wykonywania obowiązków w ramach pracy zawodowej.

Biorąc pod uwagę moduły przedmiotów określonych planami studiów dla zakresów Cyberbezpieczeństwo oraz Analiza danych i informatyka śledcza, absolwent studiów drugiego stopnia na kierunku Systemy informacyjne w bezpieczeństwie posiada wiedzę na temat politycznych, prawnych i gospodarczych aspektów bezpieczeństwa (podstawy bezpieczeństwa narodowego, podstawy stosunków międzynarodowych, strategia bezpieczeństwa wewnętrznego, geografia bezpieczeństwa), a także kwestii związanych z bezpieczeństwem systemów informacji (inżynieria systemów i projektowanie procesów, audyt i certyfikacja systemów informatycznych, ocena ryzyka i prognozowanie w bezpieczeństwie, sztuczna inteligencja). Absolwent posiada również umiejętności wykorzystywania systemów informacyjnych na potrzeby realizacji funkcji współczesnej administracji (zarządzanie projektem, komunikacja społeczna, certyfikacja Systemu Zarządzania ISO/IEC 27001).

Ponadto, absolwent potrafi również scharakteryzować system bezpieczeństwa państwa i jego elementy, wskazać rolę Sił Zbrojnych RP w tym systemie, ze szczególnym uwzględnieniem bezpieczeństwa państwa i obywateli (ochrona ludności i obrona cywilna, ochrona prawna, zarządzanie systemami bezpieczeństwa wewnętrznego).

Absolwent kierunku Systemy informacyjne w bezpieczeństwie drugiego stopnia o specjalności Cyberbezpieczeństwo potrafi wykryć, zidentyfikować oraz zareagować na cyberzagrożenia, jak również oszacować poziom bezpieczeństwa informacji przetwarzanych przez systemy teleinformacyjne (testy penetracyjne, akredytacja bezpieczeństwa teleinformatycznego, prognozowanie cyberzagrożeń, podstawy prawne cyberbezpieczeństwa). Absolwent posiada również umiejętność w zakresie utrzymania i zarządzania systemami teleinformatycznymi (administrowanie systemem Linux, cyberbezpieczeństwo, bezpieczeństwo sieci komputerowych i bezprzewodowych, elementy kryptologii, symulacja komputerowa, zarządzanie projektami informatycznymi).

Absolwent kierunku Systemy informacyjne w bezpieczeństwie drugiego stopnia o specjalności Analiza danych i informatyka śledcza potrafi przeprowadzić szczegółową analizę danych oraz oszacować poziom bezpieczeństwa informacji przetwarzanych przez systemy teleinformacyjne (testy penetracyjne, bezpieczeństwo sieci komputerowych i bezprzewodowych, zarzadzanie ryzykiem bezpieczenstwa systemów, zagrożenia bezpieczeństwa aplikacji i systemów, ryzyka związane z aplikacjami, podstawy prawne cyberbezpieczeństwa). Absolwent posiada również umiejętność w zakresie pozyskiwania i

gromadzenia materiałów na potrzeby analizy śledczej (biały wywiad – techniki zaawansowane, pozyskiwanie i analiza danych z technologii bezzałogowych, zastosowanie kryptologii w informatyce śledczej, techniki pozyskiwania cyfrowego materiału dowodowego).

Absolwent studiów drugiego stopnia na kierunku Systemy informacyjne w bezpieczeństwie jest przygotowany do podjęcia pracy zawodowej, ale także do kontynuowania nauki na studiach trzeciego stopnia.

1.5. Związek z misją uczelni i z jej strategią rozwoju

Misja i strategia rozwoju Akademii Marynarki Wojennej została określona Strategią rozwoju Akademii Marynarki Wojennej im. Bohaterów Westerplatte na lata 2021–2025. Jest to dokument precyzujący długoterminową politykę, którą powinny kierować się władze Uczelni we wszystkich działaniach mających na celu jej wszechstronny rozwój i pomyślność. Dla potrzeb budowania i wdrażania strategii Akademii Marynarki Wojennej posłużono się metodyką SWOT obejmującą analizę słabych i mocnych stron oraz szacowanie perspektywicznych szans i zagrożeń jej realizacji.

Dla zakładanej koncepcji kształcenia kluczowe są co najmniej trzy mocne strony, tj. wysokie kwalifikacje części nauczycieli akademickich i ich wysoka aktywność w procesie dydaktycznym i naukowym, rozwinięta baza dydaktyczna i szkoleniowa przeznaczona do kształcenia i szkolenia, dynamiczny rozwój Uczelni w obszarze kształcenia i inwestycji oraz dobra pozycja i współpraca Uczelni w środowisku lokalnym i regionalnym. Należy mieć także na względzie słabe strony, wśród których wskazano niedofinansowanie działań edukacyjnych. Warto jednak dodać, że ten element w ostatnich latach uległ istotnej poprawie i to głównie dzięki programom finansowanym przez Unię Europejską, tj. **Zintegrowany program wsparcia Akademii Marynarki Wojennej w Gdyni - II edycja, na lata 2019-2023** (numer naboru POWR.03.05.00-IP.08-00-PZ1/18). Obecnie w Uczelni uruchomiony zostały projekt „**Wykwalifikowane kadry w branży OZE**”, nr projektu FERS.01.05-IP.08-0003/23 w ramach Program Fundusze Europejskie dla Rozwoju Społecznego 2021-2027 współfinansowanego ze środków Europejskiego Funduszu Społecznego. Programy te umożliwiają studentom kierunku Systemy informacyjne w bezpieczeństwie, pierwszego i drugiego stopnia, podnoszenie kompetencji zawodowych i społecznych przez udział w specjalistycznych kursach, ale także realizację staży studenckich w instytucjach z którymi Uczelnia podpisuje stosowne porozumienia. Dodatkowo realizowane są w Uczelni działania w ramach programu „**Zintegrowany program wsparcia Akademii Marynarki Wojennej w Gdyni na rzecz rozwoju województwa pomorskiego**” (nr projektu: POWR.03.05.00-IP.08-00-REG/18).

Celem głównym projektu jest wzmocnienie potencjału Akademii Marynarki Wojennej w Gdyni poprzez realizację kompleksowego programu rzecz rozwoju województwa pomorskiego zakładającego podniesienie jakości usług edukacyjnych, wzrost kompetencji i kwalifikacji oraz praktycznych umiejętności studentów.

Należy również podkreślić, że program studiów dla kierunku Systemy informacyjne w bezpieczeństwie wpisuje się w jeden z kluczowych celów strategicznych Uczelni w obszarze kształcenia i doskonalenia zawodowego, w którym określono *uzyskanie wysokiej jakości i zdolności kształcenia kadr Sił Zbrojnych RP, w szczególności Marynarki Wojennej RP i studentów cywilnych*. W ramach tego celu wyróżniono określone cele operacyjne. W silnej korelacji z koncepcją kształcenia pozostają co najmniej trzy z nich, tj.:

- unowocześnienie i uatrakcyjnienie oferty studiów poprzez wprowadzenie nowych specjalności (zakresów) studiów,
- poprawienie jakości kształcenia,
- zacieśnienie współpracy z pracodawcami przy ustalaniu programów studiów, efektów uczenia się, realizacji treści programowych, organizacji praktyk i stażów.

Takie działania zdecydowanie zwiększają szanse studentów na rynku pracy, ale także przyczyniają się do wzrostu zainteresowania i rozwoju kierunków społecznych, a także pozwalają dostrzec rolę Akademii Marynarki Wojennej w rozwoju gospodarki opartej na wiedzy.

2. EFEKTY UCZENIA SIĘ

Studia na kierunku Systemy informacyjne w bezpieczeństwie skierowane są do osób, których celem jest rzetelne i profesjonalne przygotowanie się do służby i pracy w strukturach podległych resortowi obrony narodowej oraz spraw wewnętrznych i administracji, a także w innych instytucjach rządowych i samorządowych w zakresie szeroko pojmowanego bezpieczeństwa informacji. Absolwent tego kierunku przygotowywany jest do samodzielnych bądź pomocniczych funkcji w obszarze bezpieczeństwa militarnego i pozamilitarnego państwa, zarządzania i administrowania bezpieczeństwem, instytucjonalnego reagowania na zagrożenia. Wiedza oraz kwalifikacje nabyte podczas zajęć, umożliwiają absolwentom prowadzenie działań operacyjnych w cyberprzestrzeni tak samo skutecznie jak w powietrzu, na lądzie i na morzu. Potencjał, uzyskany w trakcie studiów, pozwoli na realizację szerokiego spektrum działań militarnych w cyberprzestrzeni, które obejmują: rozpoznawanie zagrożeń, ochronę i obronę systemów teleinformatycznych, zarządzanie bezpieczeństwem informacyjnym oraz

zwalczanie źródeł cyberzagrożeń ze szczególnym uwzględnieniem specyfiki środowiska Marynarki Wojennej.

Absolwent kończąc studia drugiego stopnia posiada ogólną wiedzę interdyscyplinarną z zakresu nauk społecznych oraz umiejętność wykorzystania jej w pracy zawodowej i życiu z zachowaniem zasad etycznych. Rozumie oraz potrafi analizować i stosować przepisy prawa oraz procedury bezpieczeństwa w systemach teleinformatycznych. Zna istotę bezpieczeństwa oraz jego uwarunkowania, zasady funkcjonowania podmiotów bezpieczeństwa. Potrafi rozwiązywać problemy zawodowe, gromadzić, przetwarzać oraz udostępniać informacje z wykorzystaniem nowoczesnych technologii. Podejmuje wyzwania zawodowe zarówno w wymiarze indywidualnym, jak również zespołowym. Zna język obcy na poziomie B2 Europejskiego Systemu Opisu Kształcenia Językowego Rady Europy oraz potrafi posługiwać się językiem specjalistycznym niezbędnym do wykonywania zawodu. Absolwent jest przygotowany do pracy w strukturach administracji publicznej, organizacjach i podmiotach gospodarczych zajmujących się bezpieczeństwem informacji oraz w strukturach zespołów reagowania na incydenty komputerowe, jak również do podjęcia studiów trzeciego stopnia.

Tabela 8. Kierunkowe efekty uczenia się

Oznaczenie kierunkowego efektu kształcenia	Opis kierunkowego efektu kształcenia	Odniesienie do uniwersalnych charakterystyk poziomów w PRK	Odniesienie do charakterystyk drugiego stopnia PRK
Wiedza			
SIB2_W01	Zna i rozumie w pogłębiony sposób wybrane fakty, teorie, metody oraz złożone zależności między nimi, także w powiązaniu z innymi dziedzinami różnorodne, złożone uwarunkowania i aksjologiczny kontekst prowadzonej działalności z zakresu teorii bezpieczeństwa, cyberbezpieczeństwa oraz analizy danych i informatyki śledczej	P7U_W	P7S_WG
SIB2_W02	Zna i rozumie w pogłębiony sposób fundamentalne dylematy współczesnej cywilizacji ze szczególnym uwzględnieniem bezpieczeństwa oraz technologii informacyjnych	P7U_W	P7S_WK
SIB2_W03	Zna i rozumie podstawy ekonomiczne, prawne, etyczne i inne uwarunkowania różnych rodzajów działalności zawodowej związanej z wykorzystaniem systemów informacyjnych w bezpieczeństwie, w tym podstawowe pojęcia i zasady z zakresu ochrony własności przemysłowej i prawa autorskiego	P7U_W	P7S_WK
SIB2_W04	Zna i rozumie w pogłębiony sposób podstawowe zasady tworzenia różnych form przedsiębiorczości	P7U_W	P7S_WK

Oznaczenie kierunkowego efektu kształcenia	Opis kierunkowego efektu kształcenia	Odniesienie do uniwersalnych charakterystyk poziomów w PRK	Odniesienie do charakterystyk drugiego stopnia PRK
	związane z wykorzystaniem systemów informacyjnych w bezpieczeństwie		
Umiejętności			
SIB2_U01	Potrafi wykorzystać posiadaną wiedzę z zakresu bezpieczeństwa, cyberbezpieczeństwa oraz analizy danych i informatyki śledczej oraz formułować i rozwiązywać złożone i nietypowe problemy oraz innowacyjnie wykonywać zadania w warunkach nieprzewidywalnych 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; - przystosowanie istniejących lub opracowanie nowych metod i narzędzi.	P7U_U	P7S_UW
SIB2_U02	Potrafi formułować i testować hipotezy związane z prostymi problemami badawczymi dotyczącymi wykorzystania systemów informacyjnych w bezpieczeństwie	P7U_U	P7S_UW
SIB2_U03	Potrafi komunikować się z otoczeniem z użyciem specjalistycznej technologii	P7U_U	P7S_UK
SIB2_U04	Potrafi brać udział w debacie z zakresu wykorzystania systemów informacyjnych w bezpieczeństwie - przedstawiać i oceniać różne opinie i stanowiska oraz dyskutować o nich	P7U_U	P7S_UK
SIB2_U05	Potrafi posługiwać się językiem obcym na poziomie B2 Europejskiego Systemu Opisu Kształcenia Językowego ze szczególnym uwzględnienie specjalistycznej terminologii z zakresu wykorzystania systemów informacyjnych w bezpieczeństwie	P7U_U	P7S_UK
SIB2_U06	Potrafi planować i organizować pracę indywidualną oraz kierować pracą zespołu w ramach realizacji zadań	P7U_U	P7S_UO
SIB2_U07	Potrafi samodzielnie planować i realizować własne uczenie się przez całe życie i ukierunkowywać innych w tym zakresie	P7U_U	P7S_UU
Kompetencje społeczne			
SIB2_K01	Krytycznie ocenia posiadaną wiedzę i odbierane treści z zakresu teorii bezpieczeństwa, cyberbezpieczeństwa oraz analizy danych i informatyki śledczej	P7U_K	P7S_KK
SIB2_K02	Uznaje znaczenie wiedzy w rozwiązywaniu problemów badawczych i praktycznych oraz zasięga opinii ekspertów w przypadku trudności z samodzielnych rozwiazywaniem problemów dotyczących wykorzystania systemów informacyjnych w bezpieczeństwie	P7U_K	P7S_KK
SIB2_K03	Inicjuje i uczestniczy konstruktywnie w przygotowaniu projektów społecznych (politycznych, gospodarczych, obywatelskich), uwzględniając ich	P7U_K	P7S_KO

Oznaczenie kierunkowego efektu kształcenia	Opis kierunkowego efektu kształcenia	Odniesienie do uniwersalnych charakterystyk poziomów w PRK	Odniesienie do charakterystyk drugiego stopnia PRK
	różne aspekty, planując i zarządzając przy tym czasem własnym oraz czasem w przedsięwzięciach zespołowych		
SIB2_K04	Planuje przedsięwzięcia własne i zespołów, z uwzględnieniem zmieniających się potrzeb społecznych, rozwiązuje problemy organizacyjne i inne o różnym poziomie złożoności	P7U_K	P7S_KR
SIB2_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**:**

– **SIB2** – 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)
– **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)
– **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

Plan studiów składa się z czterech zasadniczych modułów zajęć (działy przedmiotowe; w nawiasie oznaczenie kodu działu):

- podstawowego (A),
- kierunkowego (B),
- kształcenia w określonym zakresie (C),
- dyplomowego (D).

Poszczególne moduły zajęć grupują określone w Planie studiów przedmioty. We wszystkich modułach zajęć występują przedmioty (moduły), których realizacja zapewnia przygotowanie zawodowe studentów, a także przygotowanie do prowadzenia działalności naukowej.

Moduły zajęć tworzą zestawy przedmiotów, dla których (dla każdego osobno) sporządzono kartę przedmiotu. Zawiera ona obszar kształcenia, cel zajęć, efekty uczenia się w zakresie wiedzy, umiejętności i kompetencji społecznych, liczbę punktów ECTS oraz ich rozkład na różne formy pracy studenta, wymagania wstępne, formę zajęć, metody oraz sposoby weryfikacji efektów uczenia się, w tym formę i warunki zaliczenia przedmiotu, metody dydaktyczne, treści programowe, wykaz literatury podstawowej i uzupełniającej.

W poszczególnych modułach zajęć punkty ECTS przyporządkowano poszczególnym przedmiotom zgodnie z uchwałą nr 14/2024 Senatu Akademii Marynarki Wojennej im. Bohaterów Westerplatte z dnia 15 lutego 2024 r. w sprawie wytycznych dotyczących opracowywania programów studiów wyższych na kierunkach studiów realizowanych w Akademii Marynarki Wojennej. Przyjęto, że jeden punkt ECTS (dla danej grupy zajęć) odpowiada 25 godzinom pracy studenta obejmującym zajęcia organizowane przez uczelnię oraz jego indywidualną pracę związaną z tymi zajęciami.

Szczegółową charakterystykę poszczególnych modułów zajęć przedstawiono w poniższych zestawieniach tabelarycznych.

Moduł zajęć podstawowych A – studia stacjonarne

Kod	Nazwa przedmiotu	Łączna liczba godzin*	Liczba punktów ECTS			
			RAZEM	KONTAKTOWE	PRACA WŁASNA	NAUKI O BEZP.
Moduł zajęć podstawowych – A						
A.1	Język angielski	50	2	1,4	0,6	0,0
A.2	Geografia bezpieczeństwa	125	5	2,6	2,4	5,0
A.3	Historia bezpieczeństwa	75	3	1,4	1,6	3,0
A.4	Strategia bezpieczeństwa wewnętrznego	150	6	2,6	3,4	3,0
A.5	Metodologia badań nad bezpieczeństwem	75	3	1,4	1,6	3,0
A.6	Podstawy ekonomii**	50	2	1,4	0,6	0,0
A.7	Podstawy prawa**	50	2	1,4	0,6	0,0
A.8	Wprowadzenie do psychologii społecznej**	50	2	1,4	0,6	0,0
A.9	Podstawy socjologii**	50	2	1,4	0,6	0,0
A.10	Podstawy stosunków międzynarodowych**	50	2	1,4	0,6	0,0
A.11	Podstawy bezpieczenstwa narodowego (pol./ang.)**	75	3	1,4	1,6	3,0
A.12	Podstawy zarządzania i organizacji**	75	3	1,4	1,6	0,0
A.13	Podstawy filozofii i logiki**	75	3	1,4	1,6	0,0
A.14	Podstawy pedagogiki**	75	3	1,4	1,6	0,0
A.15	Historia techniki**	75	3	1,4	1,6	0,0
A.16	Ochrona ludności i obrona cywilna	106	4	2,1	1,9	4,0
RAZEM ZA MODUŁ		**706**	**28**	**14,4**	**13,6**	**21,0**

* Liczba ta obejmuje nakład pracy własnej studenta

** Spośród tych przedmiotów student wybiera co najmniej po jednym przedmiocie na semestrze II i III, tak by uzyskać w sumie co najmniej 5 pkt ECTS.

Moduł zajęć kierunkowych – B – studia stacjonarne

Kod	Nazwa przedmiotu	Łączna liczba godzin*	Liczba punktów ECTS			
			RAZEM	KONTAKTOWE	PRACA WŁASNA	NAUKI O BEZP.
Moduł zajęć kierunkowych - B						
B.1	Zarządzanie systemami bezpieczeństwa wewnętrznego	125	5	2,6	2,4	3,0
B.2	Inżynieria systemów i projektowanie procesów	125	5	2,6	2,4	4,0
B.3	Audyt i certyfikacja systemów informatycznych	125	5	2,6	2,4	3,0
B.4	Ocena ryzyka i prognozowanie w bezpieczeństwie	126	5	2,6	2,4	3,0
B.5	Zarządzanie projektem	125	5	2,6	2,4	4,0
B.6	Komunikacja społeczna	75	3	1,6	1,4	2,0
B.7	Certyfikacja Systemu Zarządzania ISO/IEC 27001	151	6	3,0	3,0	4,0
B.8	Sztuczna inteligencja	126	5	2,6	2,4	2,0
RAZEM ZA MODUŁ		**978**	**39**	**20,3**	**18,7**	**25,0**
* Liczba ta obejmuje nakład pracy własnej studenta						

Moduł kształcenia w zakresie Cyberbezpieczeństwo – C – studia stacjonarne

Kod	Nazwa przedmiotu	Łączna liczba godzin*	Liczba punktów ECTS			
			RAZEM	KONTAKTOWE	PRACA WŁASNA	NAUKI O BEZP.
Moduł kształcenia w zakresie Cyberbezpieczeństwo – C						
C.1	Zarządzanie projektami informatycznymi	126	5	2,6	2,4	3,0
C.2	Akredytacja bezpieczeństwa teleinformatycznego	80	3	1,9	1,1	4,0
C.3	Testy penetracyjne	110	4	2,2	1,8	2,0
C.4	Bezpieczeństwo sieci komputerowych i bezprzewodowych	126	5	2,6	2,4	3,0
C.5	Elementy kryptologii	126	5	2,6	2,4	4,0
C.6	Administrowanie systemem Linux	100	4	2,0	2,0	3,0
C.7	Cyberbezpieczeństwo	105	4	2,1	1,9	3,0
C.8	Prognozowanie cyberzagrożeń	105	4	2,1	1,9	5,0
C.9	Symulacja komputerowa	105	4	2,1	1,9	3,0
C.10	Podstawy prawne cyberbezpieczeństwa	105	4	2,1	1,9	2,0
RAZEM ZA MODUŁ		**1088**	**42**	**22,3**	**19,7**	**32,0**
* Liczba ta obejmuje nakład pracy własnej studenta						

Moduł kształcenia w zakresie Analiza danych i informatyka śledcza– C – studia stacjonarne

Kod	Nazwa przedmiotu	Łączna liczba godzin*	Liczba punktów ECTS			
			RAZEM	KONTAKTOWE	PRACA WŁASNA	NAUKI O BEZP.
Moduł kształcenia w zakresie Analiza danych i informatyka śledcza – C						
C.1	Pozyskiwanie i analiza danych z technologii bezzałogowych	126	5	2,6	2,4	3,0
C.2	Zastosowanie kryptologii w informatyce śledczej	80	3	1,9	1,1	4,0
C.3	Testy penetracyjne	110	4	2,2	1,8	2,0
C.4	Bezpieczeństwo sieci komputerowych i bezprzewodowych	126	5	2,6	2,4	3,0
C.5	Techniki pozyskiwania cyfrowego materiału dowodowego	126	5	2,6	2,4	4,0
C.6	Biały wywiad – techniki zaawansowane	100	4	2,0	2,0	3,0
C.7	Zarzadzanie ryzykiem bezpieczeństwa systemów	105	4	2,1	1,9	3,0
C.8	Zagrożenia bezpieczeństwa aplikacji i systemów	105	4	2,1	1,9	5,0
C.9	Metody ataku i obrony w cyberprzestrzeni	105	4	2,1	1,9	3,0
C.10	Podstawy prawne cyberbezpieczeństwa	105	4	2,1	1,9	2,0
RAZEM ZA MODUŁ		**1088**	**42**	**22,3**	**19,7**	**32,0**
* Liczba ta obejmuje nakład pracy własnej studenta						

Moduł dyplomowy – D – studia stacjonarne

Kod	Nazwa przedmiotu	Łączna liczba godzin*	Liczba punktów ECTS			
			RAZEM	KONTAKTOWE	PRACA WŁASNA	NAUKI O BEZP.
Moduł dyplomowy - D						
D.1	Seminarium dyplomowe i prawa autorskie	25	1	0,6	0,4	1,0
D.2	Praca dyplomowa	250	10	2,8	7,2	10,0
RAZEM ZA MODUŁ		**275**	**11**	**3,4**	**7,6**	**11,0**
* Liczba ta obejmuje nakład pracy własnej studenta						

Moduł zajęć podstawowych A – studia niestacjonarne

Kod	Nazwa przedmiotu	Łączna liczba godzin*	Liczba punktów ECTS			
			RAZEM	KONTAKTOWE	PRACA WŁASNA	NAUKI O BEZP.
Moduł zajęć podstawowych – A						
A.1	Język angielski	50	2	1,4	0,6	0,0
A.2	Geografia bezpieczeństwa	125	5	1,4	3,6	5,0
A.3	Historia bezpieczeństwa	75	3	1,0	2,0	3,0
A.4	Strategia bezpieczeństwa wewnętrznego	150	6	1,4	4,6	3,0
A.5	Metodologia badań nad bezpieczeństwem	75	3	1,0	2,0	3,0
A.6	Podstawy ekonomii**	50	2	0,8	1,2	0,0
A.7	Podstawy prawa**	50	2	0,8	1,2	0,0
A.8	Wprowadzenie do psychologii społecznej**	50	2	0,8	1,2	0,0
A.9	Podstawy socjologii**	50	2	0,8	1,2	0,0
A.10	Podstawy stosunków międzynarodowych**	50	2	0,8	1,2	0,0
A.11	Podstawy bezpieczenstwa narodowego (pol./ang.)**	75	3	0,8	2,2	3,0
A.12	Podstawy zarządzania i organizacji**	75	3	0,8	2,2	0,0
A.13	Podstawy filozofii i logiki**	75	3	0,8	2,2	0,0
A.14	Podstawy pedagogiki**	75	3	0,8	2,2	0,0
A.15	Historia techniki**	75	3	0,8	2,2	0,0
A.16	Ochrona ludności i obrona cywilna	106	4	1,2	2,8	4,0
RAZEM ZA MODUŁ		**706**	**28**	**9,1**	**18,9**	**21,0**

* Liczba ta obejmuje nakład pracy własnej studenta

** Spośród tych przedmiotów student wybiera co najmniej po jednym przedmiocie na semestrze II i III, tak by uzyskać w sumie co najmniej 5 pkt ECTS.

Moduł zajęć kierunkowych – B – studia niestacjonarne

Kod	Nazwa przedmiotu	Łączna liczba godzin*	Liczba punktów ECTS			
			RAZEM	KONTAKTOWE	PRACA WŁASNA	NAUKI O BEZP.
Moduł zajęć kierunkowych - B						
B.1	Zarządzanie systemami bezpieczeństwa wewnętrznego	125	5	1,6	3,4	3,0
B.2	Inżynieria systemów i projektowanie procesów	125	5	1,6	3,4	4,0
B.3	Audyt i certyfikacja systemów informatycznych	125	5	1,6	3,4	3,0
B.4	Ocena ryzyka i prognozowanie w bezpieczeństwie	126	5	1,6	3,4	3,0
B.5	Zarządzanie projektem	125	5	1,6	3,4	4,0
B.6	Komunikacja społeczna	75	3	1,0	2,0	2,0
B.7	Certyfikacja Systemu Zarządzania ISO/IEC 27001	151	6	1,8	4,2	4,0
B.8	Sztuczna inteligencja	126	5	1,6	3,4	3,0
RAZEM ZA MODUŁ		**978**	**39**	**12,5**	**26,5**	**26,0**
* Liczba ta obejmuje nakład pracy własnej studenta						

Moduł kształcenia w zakresie Cyberbezpieczeństwo – C – studia niestacjonarne

Kod	Nazwa przedmiotu	Łączna liczba godzin*	Liczba punktów ECTS			
			RAZEM	KONTAKTOWE	PRACA WŁASNA	NAUKI O BEZP.
Moduł kształcenia w zakresie Cyberbezpieczeństwo – C						
C.1	Zarządzanie projektami informatycznymi	126	5	1,6	3,4	2,0
C.2	Akredytacja bezpieczeństwa teleinformatycznego	80	3	0,9	2,1	3,0
C.3	Testy penetracyjne	110	4	1,3	2,7	3,0
C.4	Bezpieczeństwo sieci komputerowych i bezprzewodowych	126	5	1,4	3,6	4,0
C.5	Elementy kryptologii	126	5	1,4	3,6	2,0
C.6	Administrowanie systemem Linux	100	4	1,0	3,0	4,0
C.7	Cyberbezpieczeństwo	105	4	1,3	2,7	3,0
C.8	Prognozowanie cyberzagrożeń	105	4	1,3	2,7	5,0
C.9	Symulacja komputerowa	105	4	1,3	2,7	3,0
C.10	Podstawy prawne cyberbezpieczeństwa	105	4	1,3	2,7	2,0
RAZEM ZA MODUŁ		**1088**	**42**	**13,0**	**29,0**	**31,0**
* Liczba ta obejmuje nakład pracy własnej studenta						

Moduł kształcenia w zakresie Analiza danych i informatyka śledcza – C – studia niestacjonarne

Kod	Nazwa przedmiotu	Łączna liczba godzin*	Liczba punktów ECTS			
			RAZEM	KONTAKTOWE	PRACA WŁASNA	NAUKI O BEZP.
Moduł kształcenia w zakresie Analiza danych i informatyka śledcza – C						
C.1	Pozyskiwanie i analiza danych z technologii bezzałogowych	126	5	1,4	3,6	2,0
C.2	Zastosowanie kryptologii w informatyce śledczej	80	3	0,9	2,1	3,0
C.3	Testy penetracyjne	110	4	1,3	2,7	3,0
C.4	Bezpieczeństwo sieci komputerowych i bezprzewodowych	126	5	1,4	3,6	4,0
C.5	Techniki pozyskiwania cyfrowego materiału dowodowego	126	5	1,4	3,6	2,0
C.6	Biały wywiad – techniki zaawansowane	100	4	1,0	3,0	4,0
C.7	Zarzadzanie ryzykiem bezpieczeństwa systemów	105	4	1,3	2,7	3,0
C.8	Zagrożenia bezpieczeństwa aplikacji i systemów	105	4	1,3	2,7	5,0
C.9	Metody ataku i obrony w cyberprzestrzeni	105	4	1,3	2,7	3,0
C.10	Podstawy prawne cyberbezpieczeństwa	105	4	1,3	2,7	2,0
RAZEM ZA MODUŁ		**1088**	**42**	**12,8**	**29,2**	**31,0**
* Liczba ta obejmuje nakład pracy własnej studenta						

Moduł dyplomowy – D – studia niestacjonarne

Kod	Nazwa przedmiotu	Łączna liczba godzin*	Liczba punktów ECTS			
			RAZEM	KONTAKTOWE	PRACA WŁASNA	NAUKI O BEZP.
Moduł dyplomowy – D						
D.1	Seminarium dyplomowe i prawa autorskie	25	1	0,6	0,4	1,0
D.2	Praca dyplomowa	250	10	2,8	7,2	10,0
RAZEM ZA MODUŁ		**275**	**11**	**3,4**	**7,6**	**11,0**
* Liczba ta obejmuje nakład pracy własnej studenta						

3.1. Karty przedmiotów modułu zajęć podstawowych studiów stacjonarnych – A

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:	**Język angielski**	*Kod*:	**Ja**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Stacjonarne		
Kształcenie w zakresie:	Cyberbezpieczeństwo, Analiza danych i informatyka śledcza		
Profil:	Ogólnoakademicki		
Liczba ECTS:	2		
Semestr:	1		
Wymagania wstępne:	Znajomość języka angielskiego na poziomie B2		
Język wykładowy:	Polski, angielski		
Cel przedmiotu:	**C01**	Realizacja przedmiotu w celu wyposażenia studentów w wiedzę, umiejętności i kompetencje społeczne umożliwiające posługiwanie się językiem angielskim do celów ogólnych	
	C02	Realizacja przedmiotu w celu wyposażenia studentów w wiedzę, umiejętności i kompetencje społeczne umożliwiające posługiwanie się językiem angielskim do celów zawodowych	
II.	**EFEKTY UCZENIA SIĘ**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Ja_W01**	Ma rozszerzoną wiedzę o miejscu i znaczeniu języków obcych w systemie nauk oraz o ich specyfice przedmiotowej	Aktywność, Kolokwium
	Ja_W02	Zna terminologię obcojęzyczną właściwą dla studiowanego kierunku na poziomie rozszerzonym	Aktywność, Kolokwium
	Ja_W03	Ma podstawową wiedzę o instytucjach kultury i orientację we współczesnym życiu kulturalnym krajów angielskiego obszaru językowego	Aktywność, Kolokwium
	Ja_W04	Ma pogłębioną wiedzę o kompleksowej naturze języka i historycznej zmienności jego znaczeń	Aktywność, Kolokwium
Umiejętności:	**Ja_U01**	Ma umiejętności językowe właściwe dla studiowanego kierunku zgodnie z wymaganiami określonymi dla poziomu co najmniej B2+ Europejskiego Systemu Opisu Kształcenia Językowego	Aktywność, Kolokwium
	Ja_U02	Umie samodzielnie zdobywać wiedzę wykorzystując znajomość języka obcego	Aktywność, Kolokwium
	Ja_U03	Posiada umiejętność merytorycznego argumentowania i prezentacji własnych poglądów oraz poglądów innych osób w języku obcym	Aktywność, Kolokwium

	Ja_U04	Posiada pogłębioną umiejętność przygotowania różnych prac pisemnych w języku angielskim właściwych dla studiowanego kierunku studiów	Aktywność, Kolokwium
	Ja_U05	Posiada pogłębioną umiejętność przygotowania wystąpień ustnych w języku angielskim w zakresie dziedzin nauki i dyscyplin naukowych właściwych dla studiowanego kierunku studiów	Aktywność, Kolokwium
Kompetencje społeczne:	**Ja_K01**	Rozumie potrzebę uczenia się przez całe życie, potrafi inspirować i organizować proces uczenia się innych osób	Aktywność, Kolokwium
	Ja_K02	Potrafi i współdziałać pracować w grupie, używając języka obcego, przyjmując różne role przy wykonywaniu wspólnych projektów i prowadzonej dyskusji	Aktywność, Kolokwium
	Ja_K03	Aktywnie uczestniczy w działaniach na rzecz zachowania dziedzictwa kulturowego Europy	Aktywność, Kolokwium
	Ja_K04	Systematycznie uczestniczy w życiu kulturalnym	Aktywność, Kolokwium

III.	**TREŚCI PROGRAMOWE**	
Forma	*Temat, zagadnienia*	*Liczba godzin*
C01	Relacjonowanie i dyskutowanie zdarzeń teraźniejszych	4
C02	Relacjonowanie i dyskutowanie zdarzeń przeszłych	4
C03	Planowanie, obiecywanie, informowanie o decyzjach dotyczących przyszłości	4
C04	Rozwijanie umiejętności czytania ze zrozumieniem tekstów odnoszących się do zagadnień bezpieczeństwa publicznego	4
C05	Rozwijanie umiejętności rozumienia wykładów i prezentacji na tematy z zakresu bezpieczeństwa publicznego	4
C06	Rozwijanie umiejętności wypowiadania się na tematy odnoszące się do problematyki bezpieczeństwa publicznego	4
C07	Przygotowanie i przeprowadzenie prezentacji dotyczącej zagadnień bezpieczeństwa publicznego	2
C08	Konsolidacja materiału	2
C09	Kolokwium	2

IV.	**KORELACJA EFEKTÓW UCZENIA SIĘ**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyki PRK*
C01	Ja_W02, Ja_U01, Ja_U03, Ja_K02	SIB2_U07, SIB2_U05, SIB2_K03	P7U_U P7S_UU P7U_U P7S_UK P7U_K P7S_KO
C02	Ja_W02, Ja_U01, Ja_U03, Ja_K02	SIB2_U07, SIB2_U05, SIB2_K03	P7U_U P7S_UU P7U_U P7S_UK P7U_K P7S_KO
C03	Ja_W02, Ja_U01, Ja_03, Ja_K02	SIB2_U07, SIB2_U05, SIB2_K03	P7U_U P7S_UU P7U_U P7S_UK P7U_K P7S_KO
C04	Ja_W01, Ja_W02, Ja_W04, Ja_U01, Ja_K01	SIB2_U07, SIB2_U05,	P7U_U P7S_UU P7U_U P7S_UK

C05	Ja_W01, Ja_W02, Ja_W04, Ja_U0I, Ja_U02, Ja_03, Ja_K01, Ja_K02	SIB2_U07, SIB2_U05, SIB2_K02	P7U_U P7S_UU P7U_U P7S_UK P7U_K P7S_KK
C06	Ja_W01, Ja_W02, Ja_W03, Ja_W04, Ja_U01, Ja_U02, Ja_U03, Ja_U04, Ja_K01, Ja_K02, Ja_K04	SIB2_U07, SIB2_U05, SIB2_K02, SIB2_K03	P7U_U P7S_UU P7U_U P7S_UK P7U_K P7S_KK P7U_K P7S_KO
C07	Ja_W01, Ja_W02, Ja_W03, Ja_W04, Ja_U01, Ja_U02, Ja_U03, Ja_U04, Ja_U05, Ja_K01, Ja_K02, Ja_K03, Ja_K04	SIB2_U07, SIB2_U05, SIB2_K02, SIB2_K03	P7U_U P7S_UU P7U_U P7S_UK P7U_K P7S_KK P7U_K P7S_KO
C08	Ja_W02, Ja_U01, Ja_U02, Ja_K01	SIB2_U07, SIB2_U05, SIB2_K02	P7U_U P7S_UU P7U_U P7S_UK P7U_K P7S_KK
C09	Ja_W02, Ja_W04, Ja_U01	SIB2_U07, SIB2_U05, SIB2_K02	P7U_U P7S_UU P7U_U P7S_UK P7U_K P7S_KK

V. NAKŁAD PRACY STUDENTA

Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład		**X**	**50**	**2**
Ćwiczenia	**30**			
Seminaria				
Konwersatoria				
Konsultacje (zaliczenie nieobecności, rozliczenie rygorów, poprawy)	**5**			
Przygotowanie do ćwiczeń	**X**	**5**		
Opanowanie informacji		**5**		
Przygotowanie do rozliczenia rygorów		**5**		
RAZEM	**35**	**15**		

VI. METODY I NARZĘDZIA DYDAKTYCZNE

Zajęcia realizowane w oparciu o podejście eklektyczne wykorzystujące techniki nauczania adekwatne do zakładanych celów poszczególnych zajęć i celu przedmiotu z szerokim wykorzystaniem technologii cyfrowych i internetowych (Technology Enhanced Language Learning) oraz promowaniem autonomicznego uczenia się (Autonomous Learning Fostering).
- ćwiczenie;
- praca w grupach i inne formy aktywizujące
- prezentacja multimedialna;;

VII. FORMA ZALICZENIA PRZEDMIOTU

Rygor	*Kryteria składowe*	*Waga*
Zaliczenie	Średnia ze sprawdzianów na ćwiczeniach	0,2
	Średnia z ocen uzyskanych za postępy	0,2
	Ocena z kolokwium	0,6

VIII. LITERATURA

	OBOWIĄZKOWA
1.	Podręcznik studenta do nauki języka angielskiego – poziom zaawansowany
2.	Zeszyt ćwiczeń do podręcznika
3.	Classware do podręcznika
4.	Podręcznik nauczyciela wraz z zestawem testów
5.	Nagrania dźwiękowe do podręcznika studenta i zeszytu ćwiczeń
	UZUPEŁNIAJĄCA
1.	The Guardian Weekly - materiały udostępniane w sieci przez One Stop English
2.	Materiałyautentycznedostępne w sieci – British Council Learning Zone, One Stop English, BBC, CNN Student News

IX. PROWADZĄCY PRZEDMIOT

Stopień, Imię i nazwisko	dr Daria ŁĘSKA-OSIAK i zespól
adres e-mail, tel.	tel.: 261 262 737, e-mail: d.osiak@amw.gdynia.pl

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:	**Geografia bezpieczeństwa**	*Kod*:	**Dj**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Stacjonarne		
Kształcenie w zakresie:	Cyberbezpieczeństwo, Analiza danych i informatyka śledcza		
Profil:	Ogólnoakademicki		
Liczba ECTS:	5		
Semestr:	1		
Wymagania wstępne:	Podstawowa wiedza z geografii, podstawowa wiedza z bezpieczeństwa		
Język wykładowy:	Polski		
Cel przedmiotu:	**C01**	Zapoznanie słuchaczy z pojęciem geografii bezpieczeństwa oraz wskazanie zakresu badań na gruncie tej dyscypliny naukowej w systemie nauk o bezpieczeństwie.	
	C02	Przedstawić jak wykorzystywać informację geograficzną do rozwiązywania problemów bezpieczeństwa.	
	C03	Zapoznanie z praktycznym wymiarem geografii bezpieczeństwa dla wspomagania działalności w sferze bezpieczeństwa narodowego.	

II.	EFEKTY UCZENIA SIĘ		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Dj_W01**	Wyjaśnia relacje występujące w obszarze nauk o bezpieczeństwie i nauk o obronności oraz ich związek z innymi naukami społecznymi.	Kolokwium
	Dj_W02	Opisuje kulturowe, polityczne, prawne i ekonomiczne procesy występujące na poziomie państwa i układów międzynarodowych wraz z ich przełożeniem na problemy bezpieczeństwa narodowego.	Sprawdzian
	Dj_W03	Posiada pogłębioną wiedzę dotyczącą strategii bezpieczeństwa państwa jej prawnych regulacji i konsekwencji w zakresie ich stosowania.	Praca Pisemna
Umiejętności:	**Dj_U01**	Określa zagrożenia bezpieczeństwa narodowego płynące z obszarów społecznych, ekonomicznych, politycznych, prawnych i kulturowych.	Sprawdzian
	Dj_U02	Interpretuje rozwój zjawisk społecznych, ekonomicznych, politycznych, prawnych i kulturowych oraz płynące z tych obszarów zagrożenia bezpieczeństwa narodowego.	Kolokwium
	Dj_U03	Interpretuje poprawnie zależności między zjawiskami społecznymi, ekonomicznymi, politycznymi, prawnymi i kulturowymi tworzącymi bezpieczeństwo narodowe lub oddziaływującymi na nie, a także system oddziaływania normatywnych regulacji na wspomniane obszary (normy prawne,	Praca Pisemna

		standardy zawodowe, systemy normalizacji i standaryzacji, normy moralne, normy kulturowej.	
Kompetencje społeczne:	**Dj_K01**	Akceptuje potrzebę uczenia się przez całe życie.	Praca Pisemna
	Dj_K02	Podejmuje wyzwania związane z wykonywaniem zawodów w obszarze bezpieczeństwa narodowego.	Odpowiedź tablicowa
	Dj_K03	Akceptuje uzupełnianie i doskonalenie nabytej wiedzy i umiejętności, potrafi ocenić ofertę kształcenia kursowego i podyplomowego.	Praca Pisemna

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
W01	**Wprowadzenie do geografii bezpieczeństwa** (czym zajmuje się geografia bezpieczeństwa; geograficzny wymiar bezpieczeństwa państwa; istota bezpieczeństwa międzynarodowego; strefy bezpieczeństwa narodowego).	2
W02	**Zagrożenia dla bezpieczeństwa państwa** (problemy i wyzwania współczesnego świata; współczesne postrzeganie zagrożeń militarnych; współczesne zagrożenia pozamilitarne /niemilitarne/ państwa).	2
W03	**Geopolityka i geostrategia** (wybrane aspekty globalizacji; geografia wojenna i geografia wojskowa; geografia bezpieczeństwa a inne nauki – związki i zależności).	2
W04	**Geografia bezpieczeństwa** (geografia bezpieczeństwa na tle polityki strategii bezpieczeństwa państwa).	2
W05	**Geografia bezpieczeństwa** (próba zdefiniowania; funkcje).	2
W06	**Zakres badań geografii bezpieczeństwa** (przestrzeń geograficzna; geodane i geoinformacje – znaczenie w systemie informacyjnym; geoprzestrzeń).	2
W07	**Metody i techniki badawcze na gruncie geografii bezpieczeństwa** (metody i techniki badawcze; badania jakościowe).	2
W08	**Działalność struktur państwa w sferze bezpieczeństwa narodowego** (wybrane instytucje państwowe działające na rzecz bezpieczeństwa państwa; geografia bezpieczeństwa oraz systemy informacji geograficznej).	2
W09	**Geodane i geoinformacje** (zasady geoinformacyjne tworzone na gruncie militarnym; zasoby geoinformacyjne strefy pozamilitarnej).	2
W10	**Geografia bezpieczeństwa** (Krajowy System Informacji Geograficznej).	2
W11	**Systemy geoinformacyjne** (GEOserver; teledetekcja; Państwowy Monitoring Środowiska).	2
W12	**Systemy geoinformacyjne** (System Informacji Przestrzennej; infrastruktura geoinformacyjna państwa).	2
W13	**Podział geostrategiczny świata** (przestrzeń euroatlantycka w ujęciu geostrategicznym; ogólna charakterystyka regionów geostrategicznych).	1
C01	Charakterystyka Morza Bałtyckiego jako regionu gospodarczego i militarnego.	2
C02	Charakterystyka zasobów i ich wpływu na rozwój gospodarki narodowej.	2

C03	Ocena zagrożeń naturalnych w stosunku do polski.	2
C04	Ocena zagrożeń naturalnych na świecie.	2
C05	Poleżenie polski a uwarunkowania konfliktowe/asymetryczne.	2
C06	Ocena infrastruktury morskiej Polski w aspekcie zagrożeń i bezpieczeństwa.	2
C07	Charakterystyka zagrożeń naturalnych w państwach UE.	2
C08	Charakterystyka zagrożeń naturalnych w państwach ameryki północnej i południowej.	3
C09	Energia wód – stan obecny oraz perspektywy wykorzystania w Polsce.	2
C10	Energia wiatru – stan obecny oraz perspektywy wykorzystania w Polsce.	2
C11	Energia słoneczna – stan obecny oraz perspektywy wykorzystania w Polsce.	2
C12	System informacji geoprzestrzennej.	2

IV.	**KORELACJA EFEKTÓW UCZENIA SIĘ**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyki PRK*
W01	Dj_W01, Dj_U01, Dj_K02	SIB2_W01, SIB2_U01, SIB2_K04	P7U_W P7S_WG, P7U_U P7S _UW, P7U_K P7S_KR
W02	Dj_W02, Dj_K03	SIB2_W01, SIB2_K03	P7U_W P7S_WG, P7U_K P7S_KO
W03	Dj_W01, Dj_W03, Dj_K03	SIB2_W01, SIB2_W03, SIB2_K01	P7U_W P7S_WG, P7U W P7S_WK, P7U_K P7S_KK
W04	Dj_W02, Dj_W03, Dj_K02	SIB2_W01, SIB2_W03, SIB2_K05	P7U_W P7S_WG, P7U W P7S_WK, P7U_K P7S_KR
W05	Dj_W01, Dj_W02, Dj_K02	SIB2_W01, SIB2_K05	P7U_W P7S_WG, P7U_K P7S_KR,
W06	Dj_W01, Dj_U02, Dj_K03	SIB2_W01, SIB2_U01, SIB2_K03	P7U_W P7S_WG, P7U_U P7S_UW, P7U_K P7S_KO
W07	Dj_W01, Dj_U01, Dj_U03, Dj_K03	SIB2_W01, SIB2_U01, SIB2_U04, SIB2_K03	P7U_W P7S_WG, P7U_U P7S _UW, P7U_U P7S_UK, P7U_K P7S_KO
W08	Dj_W01, Dj_U01, Dj_U03, Dj_K03	SIB2_W01, SIB2_U01, SIB2_U04, SIB2_K03	P7U_W P7S_WG, P7U_U P7S_UW, P7U_U P7S_UK, P7U_K P7S_KO
W09	Dj_W01, Dj_U01, Dj_K03	SIB2_W01, SIB2_U01, SIB2_K03	P7U_W P7S_WG, P7U_U P7S _UW, P7U_K P7S_KO
W10	Dj_W01, Dj_U01, Dj_K03	SIB2_W01, SIB2_U01, SIB2_K03	P7U_W P7S_WG, P7U_U P7S _UW, P7U_K P7S_KO
W11	Dj_W01, Dj_U01, Dj_K03	SIB2_W01, SIB2_U01, SIB2_K03	P7U_W P7S_WG, P7U_U P7S_ UW, P7U_K P7S_KO
W12	Dj_W01, Dj_U01, Dj_K03	SIB2_W01, SIB2_U01, SIB2_K03	P7U_W P7S_WG, P7U_U P7S _UW, P7U_K P7S_KO
W13	Dj_W01, Dj_U01, Dj_K03	SIB2_W01, SIB2_U01, SIB2_K03	P7U_W P7S_WG, P7U_U P7S _UW, P7U_K P7S_KO
C01	Dj_U01, Dj_K03	SIB2_U02, SIB2_K03	P7U_U P7S _UW, P7U_K P7S_KO
C02	Dj_W02, Dj_K03	SIB2_W01, SIB2_K03	P7U_W P7S_WG, P7U_K P7S_KO
C03	Dj_W03, Dj_K03	SIB2_W02, SIB2_K03	P7U W P7S_WK, P7U_K P7S_KO
C04	Dj_W03, Dj_K03	SIB2_W03, SIB2_K03	P7U W P7S_WK, P7U_K P7S_KO
C05	Dj_W02, Dj_K03	SIB2_W01, SIB2_K03	P7U_W P7S_WG, P7U_K P7S_KO
C06	Dj_W01, Dj_W03, Dj_U02, Dj_K01,	SIB2_W01, SIB2_W02, BN2 _U01, SIB2_K05	P7U_W P7S_WG, P7U W P7S_WK, P7U_U P7S_UW, P7U_K P7S_KK,
C07	Dj_W02, Dj_U01, Dj_U03, Dj_K01, Dj_K02,	SIB2_W01, BN2 _U01, SIB2_U01, SIB2_K01, SIB2_K05	P7U_W P7S_WG, P7U_U P7S _UW, P7U_U P7S_UK, P7U_K P7S_KK, P7U_K P7S_KR,
C08	Dj_W02, Dj_U01, Dj_K01, Dj_K03	SIB2_W01, BN2 _U01, SIB2_K05, SIB2_K03	P7U_W P7S_WG, P7U_U P7S _UW, P7U_K P7S_KK, P7U_K P7S_KO
C09	Dj_W02, Dj_U01, Dj_K01, Dj_K02,	SIB2_W01, BN2 _U01, SIB2_K05, SIB2_K04	P7U_W P7S_WG, P7U_U P7S _UW, P7U_K P7S_KK, P7U_K P7S_KR,
C10	Dj_W01, Dj_W02, Dj_U02, Dj_K03	SIB2_W01, BN2 _U01, SIB2_K03	P7U_W P7S_WG, P7U_U P7S_UW, P7U_K P7S_KO
C11	Dj_W01, Dj_W02, Dj_U02, Dj_K03	SIB2_W01, BN2 _U01, SIB2_K03	P7U_W P7S_WG, P7U_U P7S_UW, P7U_K P7S_KO

C12	Dj_W01, Dj_W02, Dj_U01, Dj_K03	SIB2_W01, BN2 _U01, SIB2_K03	P7U_W P7S_WG, P7U_U P7S _UW, P7U_K P7S_KO

V. NAKŁAD PRACY STUDENTA

Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**30**	**X**	**125**	**5**
Ćwiczenia	**30**			
Seminaria	**0**			
Konwersatoria	**0**			
Konsultacje (zaliczenie nieobecności, rozliczenie rygorów, poprawy)	**6**			
Przygotowanie do ćwiczeń	**X**	**18**		
Opanowanie informacji		**18**		
Przygotowanie do rozliczenia rygorów		**20**		
RAZEM	**66**	**56**		

VI. METODY I NARZĘDZIA DYDAKTYCZNE

1.	- wykład;	- wykaz tez do dyskusji;
2.	- ćwiczenie;	- prezentacja multimedialna.
3.	- praca w grupach i inne aktywizujące;	

VII. FORMA ZALICZENIA PRZEDMIOTU

Rygor	*Kryteria składowe*	*Waga*
Zaliczenie	Średnia ze sprawdzianów na ćwiczeniach	0,2
	Ocena z kolokwium	0,2
	Ocena z pracy proseminaryjnej	0,1
Egzamin	Ocena z egzaminu	0,5

VIII. LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

OBOWIĄZKOWA

1. I. Fierla, *Geografia gospodarcza świata*, PWE, Warszawa 2003
2. Z. Lach, *Informator geograficzny. Państwa członkowskie NATO*, AON, Warszawa 2005
3. K. Żurkowska (red.), *Bezpieczeństwo międzynarodowe. Teoria i praktyka*, SGH, Warszawa 2006

UZUPEŁNIAJĄCA

1. J. Barbar, *Geografia gospodarki świata*, PWN, Warszawa 1984
2. S. Otok, *Geografia polityczna świata*, Warszawa 2003
3. M. Pietras, *Bezpieczeństwo ekologiczne w Europie*, Lublin 1996
4. M. Kozub, B. Panek, *Siły zbrojne jako narzędzie polityki bezpieczeństwa międzynarodowego*, SWSPiZ, Łódź-Warszawa 2010
5. A. Łaszczuk, *Geografia bezpieczeństwa*, AON, Warszawa 2004
6. M. Żuber, *Katastrofy naturalne i cywilizacyjne*, WSOWLąd., Wrocław 2006

IX. PROWADZĄCY PRZEDMIOT

Stopień, Imię i nazwisko	dr hab. Krzysztof LIGĘZA, dr Krzysztof GAWRYSIAK
adres e-mail	k.ligeza@amw.gdynia.pl k.gawrysiak@amw.gdynia.pl

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:	**Historia bezpieczeństwa**	*Kod*:	**Yt**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Stacjonarne		
Kształcenie w zakresie:	Cyberbezpieczeństwo, Analiza danych i informatyka śledcza		
Profil:	Ogólnoakademicki		
Liczba ECTS:	3		
Semestr:	1		
Wymagania wstępne:	Podstawowa wiedza z historii Polski i Europy		
Język wykładowy:	Polski		
Cel przedmiotu:	**C01**	Prezentacja procesów wpływających na bezpieczeństwo Polski i państw Europejskich	
	C02	Zapoznanie się z możliwościami interpretacyjnymi wydarzeń oraz ich oceną w kontekście obecnych wydarzeń	

II.	**EFEKTY UCZENIA**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Yt_W01**	Student opisuje kulturowe, polityczne oraz ekonomiczne procesy występujące na poziomie państwa i układów międzynarodowych wraz z ich przełożeniem na problemy bezpieczeństwa narodowego	Kolokwium
	Yt_W02	Student wyjaśnia historyczny rozwój instytucji i organizacji państwowych, samorządowych, pozarządowych, a także innych spontanicznie tworzonych na rzecz bezpieczeństwa narodowego	Kolokwium;
Umiejętności:	**Yt_U01**	Student interpretuje rozwój zjawisk społecznych, ekonomicznych i politycznych oraz płynące z tych obszarów zagrożenia dla bezpieczeństwa państwa w wymiarze narodowym	Kolokwium; Wypowiedź ustna
	Yt_U02	Student interpretuje poprawnie zależności między zjawiskami politycznymi i ekonomicznymi tworzącymi bezpieczeństwo narodowe	Kolokwium, wypowiedź ustna
Kompetencje społeczne:	**Yt_K01**	Student akceptuje potrzebę uczenia się historii przez całe życie	Wypowiedź ustna
	Yt_K02	Student wykazuje odpowiedzialność za zadania określone przez siebie oraz posługuje się harmonogramem ich uporządkowanej realizacji	Wypowiedź ustna

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
W01	Udział Polski w tworzeniu bezpieczeństwa regionalnego w okresie międzywojennym	10

W02	Bezpieczeństwo europejskie na przełomie XIX i XX wieku	10
W03	Bezpieczeństwo Europy i Polski po II wojnie światowej	10

IV.	**KORELACJA EFEKTÓW UCZENIA SIĘ**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyki PRK*
W01	Yt_W01, Yt_U01, Yt_K01	SIB2_W01, SIB2_U02, SIB2_K02	P7U_W, P7S_WG; P7U_U,P7S_UW; P7U_K, P7S_KK
W02	Yt_W02, Yt_U02, Yt_K02	SIB2_W01, SIB2_U04, SIB2_K03	P7U_W, P7S_WG; P7U_U,P7S_UK; P7S_KO
W03	Yt_W01, Yt_U01, Yt_K01	SIB2_W01, SIB2_U02, SIB2_K02	P7U_W, P7S_WG; P7U_U,P7S_UW; P7U_K, P7S_KK
W04	Yt_W02, Yt_U02, Yt_K02	SIB2_W01, SIB2_U04, SIB2_K03	P7U_W, P7S_WG; P7U_U,P7S_UK; P7S_KO

V. NAKŁAD PRACY STUDENTA

Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**30**	**X**	**75**	**3**
Ćwiczenia				
Seminaria				
Konwersatoria				
Konsultacje (zaliczenie nieobecności, rozliczenie rygorów, poprawy)	**5**			
Przygotowanie do ćwiczeń	**X**			
Opanowanie informacji		**20**		
Przygotowanie do rozliczenia rygorów		**20**		
RAZEM	**35**	**40**		

VI. METODY DYDAKTYCZNE

1.	Konwersatorium

VII. FORMA ZALICZENIA PRZEDMIOTU

Rygor	*Kryteria składowe*	*Waga*
Zaliczenie	Kolokwium ustne	1,0

VIII. LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

OBOWIĄZKOWA

1.	R. Kużniar, *Bezpieczeństwo międzynarodowe*, wyd. Scholar, Warszawa 2012
2.	P. Żurawski vel Grajewski, *Bezpieczeństwo międzynarodowe: wymiar militarny*, wyd. PWN, Warszawa 2012
3.	R. Zięba, *Bezpieczeństwo międzynarodowe w XXI wieku*, wyd. Poltext, Warszawa 2018
4.	E. Haliżak, *Stosunki międzynarodowe: geneza, struktura, dynamika*, wyd. UW, Warszawa 2001

UZUPEŁNIAJĄCA

1.	H. Batowski, *Zachód wobec granic Polski 1920-1940. Niektóre fakt mniej znane*, Łódź 1995
2.	W. Dobrzycki, *Historia stosunków międzynarodowych 1815-1945*, Warszawa 1998
3.	A. Gaca, K. Kamińska, Z. Naworski, *Historia i współczesność, Świat i Polska ludzie i poglądy*, t. 1-2, Toruń 2000
4.	G. Friedman, *Następna dekada. Gdzie byliśmy i dokąd zmierzamy*, Kraków 2012
5.	J. Holzer, *Europa zimnej wojny*, Kraków 2012

IX. PROWADZĄCY PRZEDMIOT

Stopień, Imię i nazwisko	prof. dr hab. Jerzy Będźmirowski
adres e-mail	j.bedzmirowski@amw.gdynia.pl

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:	**Strategia bezpieczeństwa wewnętrznego**	*Kod*:	**Ig**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Stacjonarne		
Kształcenie w zakresie:	Cyberbezpieczeństwo, Analiza danych i informatyka śledcza		
Profil:	Ogólnoakademicki		
Liczba ECTS:	6		
Semestr:	2		
Wymagania wstępne:	Podstawy wiedzy o bezpieczeństwie państwa		
Język wykładowy:	Polski		
Cel przedmiotu:	**C01**	Zapoznanie się z teoretycznymi i praktycznymi aspektami strategii bezpieczeństwa wewnętrznego.	
	C02	Umiejętność implementowania zapisów strategii bezpieczeństwa wewnętrznego w różnych jednostkach podziału administracyjnego państwa	
	C03	Umiejętność krytycznej analizy strategii bezpieczeństwa wewnętrznego wybranych państw oraz w oparciu o strategię bezpieczeństwa wewnętrznego - określenia priorytetów bezpieczeństwa	

II.	**EFEKTY KSZTAŁCENIA**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Ig_W01**	Student posiada rozszerzoną wiedzę na temat teoretycznego i praktycznego wymiaru bezpieczeństwa, wyzwań i zagrożeń dla bezpieczeństwa wewnętrznego państwa (publicznego, powszechnego i ustrojowego); cech strategii i ich znaczenia, dokumentów strategicznych Polski i Unii Europejskiej	kolokwium, praca pisemna podczas zajęć
	Ig_W 02	Student posiada rozszerzoną wiedzę umożliwiającą identyfikację i opis struktur oraz zadań instytucji bezpieczeństwa publicznego, ich znaczenia dla bezpieczeństwa wewnętrznego państwa oraz Unii Europejskiej	kolokwium
	Ig_W03	Posiada wiedze pozwalającą na opis relacji pomiędzy poszczególnymi strukturami i instytucjami bezpieczeństwa wewnętrznego oraz ich wzajemnych powiązań i relacji	kolokwium, praca pisemna podczas zajęć

	Ig_W04	Student zna podstawowe źródła prawne regulujące funkcjonowanie poszczególnych instytucji bezpieczeństwa wewnętrznego (konstytucja, strategie, ustawy)	kolokwium, praca pisemna podczas zajęć
Umiejętności:	**Ig_U01**	Student potrafi prawidłowo interpretować rodzaje zagrożeń dla bezpieczeństwo wewnętrznego, określać ich zakres oraz przyporządkowywać do zadań poszczególnych instytucji	kolokwium, praca pisemna podczas zajęć
	Ig_U02	Student potrafi analizować oraz opisać zagrożenia bezpieczeństwa wewnętrznego oraz ich wpływu na funkcjonowanie jednostki, społeczeństwa i państwa	Praca pisemna w domu, odpowiedź ustna
	Ig_U03	Student posiada umiejętność korzystania z różnych źródeł pozyskiwania wiedzy, używania pojęć i terminów naukowych	praca pisemna w domu, odpowiedź ustna
	Ig_U04	Student posiada umiejętności rzeczowego argumentowania stanowiska w zakresie zapewnienia porządku i bezpieczeństwa wewnętrznego przez państwo	Odpowiedź ustna
Kompetencje społeczne	**Ig_K01**	Student potrafi pracować w grupie nad rozwiązaniem różnych problemów społecznych, bronić swoich poglądów oraz przyjmować argumentacje innych osób	Projekty grupowe podczas zajęć, odpowiedź ustna
	Ig_K02	Student potrafi wykorzystać nabytą wiedzę w celu rozwiązywania problemów	Praca pisemna podczas zajęć, odpowiedź ustna
	Ig_K03	Student potrafi (w oparciu o uzyskaną poszerzoną wiedzę) szukać potrzebnych informacji i wykorzystywać źródła oraz doskonalić swoją wiedzę i umiejętności z tego obszaru	Praca pisemna w domu, odpowiedź ustna

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
W01	Zajęcia wprowadzające. Istota bezpieczeństwa i bezpieczeństwa wewnętrznego państwa – aspekty teoretyczne i praktyczne.	6
W02	Teoretyczne aspekty strategii w obszarze militarnym i niemilitarnym.	4
W03	Poglądy wybranych klasyków strategii.	4
W04	Bezpieczeństwo wewnętrzne w ujęciu dziejowym.	4
W05	Współczesne zagrożenia bezpieczeństwa wewnętrznego.	8
W06	Podmioty kształtujące bezpieczeństwo wewnętrzne państwa.	6
W07	Dokumenty strategiczne z obszaru bezpieczeństwa wewnętrznego wybranych podmiotów.	4
W08	Metodologia tworzenia strategii bezpieczeństwa wewnętrznego.	4
C01	Projekt semestralny:	20

	1. Analiza środowiska bezpieczeństwa wewnętrznego w aspekcie wybranego sektora (zagrożenia) bezpieczeństwa 2. Identyfikacja i analiza kluczowych determinant (uwarunkowań) sektora bezpieczeństwa 3. Identyfikacja bezpieczeństwa wewnętrznego jako podmiotu bezpieczeństwa – interesy i cele 4. Metody: a. Identyfikacja słabych i mocnych stron oraz szans wyzwań i zagrożeń bezpieczeństwa wewnętrznego w ramach wybranego sektora (zagrożenia) bezpieczeństwa. Analiza SWOT/TOWS. b. Macierz wielokryterialna opisu czynników bazowych dla wybranego sektora (zagrożenia). c. Projektowanie udziału struktur państwa biorących udział w realizacji celów. 5. Synteza i wnioski wypływających z analiz

IV.	**KORELACJA EFEKTÓW KSZTAŁCENIA**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyczny PRK*
W01	Ig_W01, Ig_K03	SIB2_W01, SIB2_U02, SIB2_K01	P7U_W, P7S_WG, P7U_U, P7S_UW, P7U_K, P7S_KK
W02	Ig_W01, Ig_U04, Ig_K03	SIB2_W01, SIB2_U02, SIB2_K01	P7U_W, P7S_WG, P7U_U, P7S_UW, P7U_K, P7S_KK
W03	Ig_W01, Ig_K03	SIB2_W01, SIB2_W03, SIB2_U02, SIB2_K01	P7U_W, P7S_WK, P7U_W, P7S_WG, P7U_U, P7S_UW, P7U_K, P7S_KK
W04	Ig_W01, Ig_U03, Ig_K03	SIB2_W01, SIB2_W03, SIB2_K01	P7U_W, P7S_WK, P7U_W, P7S_WG,P7U_K, P7S_KK
W05	Ig_W01, Ig_W04, Ig_U02, Ig_U03, Ig_K03	SIB2_W01, SIB2_W03, SIB2_K01	P7U_W, P7S_WG,P7U_W, P7S_WK,P7U_K, P7S_KK
W06	Ig_W02, Ig_W03, Ig_U01, Ig_K03	SIB2_W01, SIB2_U07, SIB2_K01	P7U_W, P7S_WG,P7U_U, P7S_UU, P7U_K, P7S_KK
W07	Ig_W01, Ig_W04, Ig_U04, Ig_ K01, Ig_K03	SIB2_W01, SIB2_U04, SIB2_U07, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UK, P7U_U, P7S_UU, P7U_K, P7S_KK
W08	Ig_W02, Ig_W03, Ig_U01, Ig_K03	SIB2_W01, SIB2_U04, SIB2_U07, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UK, P7U_U, P7S_UU, P7U_K, P7S_KK
C01	Ig_W01, Ig_W04, Ig_U02, Ig_K02, Ig_K03	SIB2_W01, SIB2_W03, SIB2_U07, SIB2_U02, SIB2_K02, SIB2_K04	P7U_W, P7S_WG,P7U_W, P7S_WK,P7U_U, P7S_UU, P7U_U, P7S_UW, P7U_K, P7S_KK, P7U_K, P7S_KO, P7U_K, P7S_KR

V.	**NAKŁAD PRACY STUDENTA**			
Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**40**	**X**	**150**	**6**
Ćwiczenia	**20**			
Seminaria				
Konwersatoria				
Konsultacje (zaliczenie nieobecności, rozliczenie rygorów, poprawy)	**6**			
Przygotowanie do ćwiczeń	**X**	**27**		
Opanowanie informacji		**27**		
Przygotowanie do rozliczenia rygorów		**30**		
RAZEM	**66**	**84**		

VI.	**METODY DYDAKTYCZNE**

1.	- wykład; - wykład z prezentacją multimedialną;
2.	- ćwiczenie; - ćwiczenia przedmiotowe wykaz tez do dyskusji;
3.	- praca w grupach i inne aktywizujące; - prezentacja multimedialna analiza przypadków;

VII.	**FORMA ZALICZENIA PRZEDMIOTU**	
Rygor	*Kryteria składowe*	*Waga*
Zaliczenie	Ocena z projektu semestralnego	0,4
	ocena z kolokwium	0,6
Egzamin	Test końcowy z treści wykładu	0,7
	Rozliczenie projektu semestralnego	0,3

VIII.	**LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA**
	OBOWIĄZKOWA
1.	S. Kamiński, Przegląd bezpieczeństwa narodowego w planowaniu strategicznym Polski, Warszawa 2015
2.	P. Majer, *Bezpieczeństwo wewnętrzne Polski w rozwoju dziejowym*, Szczytno, 2012
3.	S. Sulowski (red), M. Brzeziński, *Bezpieczeństwo wewnętrzne państwa. Wybrane zagadnienia*, Wydawnictwo Elipsa, Warszawa 2009
4.	T. Szubrycht, *Strategie doktryny morskie*, AMW, Gdynia 2013
5.	Z. Ścibiorek, B. Wiśniewski, R.B. Kuc, A. Dawidczyk, *Bezpieczeństwo wewnętrzne. Podręcznik akademicki*, Wyd. Adam Marszałek, Toruń 2015
6.	Wawrzyk P., *Bezpieczeństwo wewnętrzne Unii Europejskiej*, Wydawnictwo Akademickie i Profesjonalne, Warszawa 2009
	UZUPEŁNIAJĄCA
1.	M. Gąsior, E. Daniiloudi-Zielińska, Be*zpieczeństwo Rzeczypospolitej Polskiej: wymiar przedmiotowy i instytucjonalny*, Gdynia 2018
2.	A. Misiuk, *Administracja porządku i bezpieczeństwa publicznego: zagadnienia prawno-ustrojowe*, Wydawnictwo Akademickie i Profesjonalne, Warszawa 2008

IX.	**PROWADZĄCY PRZEDMIOT**
Stopień, Imię i nazwisko	prof. dr hab. Tomasz Szubrycht, dr Eleni Daniiloudi-Zielińska
adres e-mail	t.szubrycht@amw.gdynia.pl, edaniiloudi@interia.pl

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:	**Metodologia badań nad bezpieczeństwem**	*Kod*:	**Cxm**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Stacjonarne		
Kształcenie w zakresie:	Cyberbezpieczeństwo, Analiza danych i informatyka śledcza		
Profil:	Ogólnoakademicki		
Liczba ECTS:	3		
Semestr:	2		
Wymagania wstępne:	Wiedza merytoryczna z przedmiotów kierunkowych		
Język wykładowy:	Polski		
Cel przedmiotu:	**C01**	Zapoznać z procesem badań naukowych w zakresie bezpieczeństwa	
	C02	Nauczyć zasad i metod prowadzenia badan naukowych	
	C03	Przygotować do samodzielnego formułowania i rozwiązywania problemów naukowych w zakresie bezpieczeństwa	
	C04	Przygotować do opracowania pracy dyplomowej odpowiadającej regułom pracy naukowej	

II.	**EFEKTY UCZENIA SIĘ**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Cxm_W01**	Znajomość miejsca i roli nauki we współczesnym świecie	Sprawdzian pisemny
	Cxm_W02	Znajomość podstawowych pojęć z metodyki prowadzenia badań	Sprawdzian pisemny
	Cxm_W03	Wiedza o podstawowych metod badawczych i operacjach myślowych stosowanych w badaniach nad bezpieczeństwem	Sprawdzian pisemny
	Cxm_W04	Zrozumienie istoty procesu badań naukowych i możliwości zastosowania go w badaniach nad bezpieczeństwem	Sprawdzian pisemny
	Cxm_W05	Znajomość zasad naukowego opisu i wyjaśniania zagrożeń bezpieczeństwa narodowego	Sprawdzian pisemny
Umiejętności:	**Cxm_U01**	Dostrzeganie sytuacji problemowych w zakresie bezpieczeństwa w życiu codziennym i w pracy zawodowej	Wypowiedzi ustne
	Cxm_U02	Formułowania problemów badawczych i hipotez roboczych	Opracowanie pisemne
	Cxm_U03	Wybór odpowiedniej metody badawczej i sporządzanie adekwatnych narzędzi badawczych	Opracowanie pisemne
	Cxm_U04	Przeprowadzanie badań	Opracowanie pisemne

	Cxm_U05	Przedstawiania wyników badań w formie publikacji	Opracowanie pisemne
Kompetencje społeczne:	**Cxm_K01**	Zrozumienie istoty i potrzeb pogłębiania wiedzy	Wypowiedzi ustne
	Cxm_K02	Dostrzeganie zagrożeń bezpieczeństwa i poszukiwanie środków zaradczych	Wypowiedzi ustne
	Cxm_K03	Akceptacja roli i zadań formacji bezpieczeństwa i wsparcie ich działań	Rozwiązania ustne i pisemne
	Cxm_K04	Wnikliwa obserwacja środowiska bezpieczeństwa i podejmowanie działań zapobiegawczych zagrożeniom	Wypowiedzi ustne

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
W01	**Praca magisterska – istota i wymagania** (praca magisterska jako praca promocyjna; cel pracy magisterskiej; wymagania formalne; kryteria naukowości; ogólny tok postępowania; zasady wyboru tematu; układ pracy; układ i treść procedury badawczej; etapy opracowania, rola promotora)	2
W02	**Nauka – istota i klasyfikacja** (wieloznaczność pojęcia nauki; cele nauki i poznania naukowego; funkcje nauki; treść nauki; zasady i czynności poznania naukowego, teoria naukowa; podejścia naukowe; proces badawczy; klasyfikacja nauk; stopnie, tytuły i stanowiska naukowe)	2
W03	**Proces badań naukowych** (pojęcie procesu badawczego; etapy przygotowania i prowadzenia badań; cel i przedmiot badań w naukach o bezpieczeństwie; metody badań naukowych)	2
W04	**Problemy, hipotezy i zmienne w procesie badań naukowych** (sytuacja problemowa, sens i sposób wyrażania problemu naukowego, hipotezy wstępne, robocze i naukowe, rodzaje hipotez, zmienne badawcze , współzmienność, wskaźniki, ich rodzaje i znaczenie, skale pomiarowe)	2
W05	**Metody, techniki i narzędzia badawcze** (pojęcie metody naukowej i metod badawczych; techniki badawcze; podstawowe – empiryczne metody badawcze; metody teoretyczne – rozumowanie proste i złożone; schematy wnioskowania, narzędzia badawcze)	2
W06	**Podejścia i metody badawcze w badaniach nad bezpieczeństwem (**cel i przedmiot badań, badania ilościowe i jakościowe, metody teoretyczne i empiryczne, narzędzia badawcze w badaniach ilościowych i jakościowych}	2
W07	**Wykorzystanie materiałów źródłowych w pracach promocyjnych** (bibliografia a literatura przedmiotu badań, rodzaje literatury naukowej, sposoby poszukiwania literatury przedmiotu badań, kolejność i etapy studiowania literatury, sporządzanie notatek, porządkowanie i uogólnienie uzyskanego materiału, analiza dokumentów, wykorzystanie Internetu, sposoby sprawdzania wiarygodności źródeł, cytowanie i parafrazowanie)	2
W08	Sprawdzian pisemny – zaliczenie przedmiotu	1
C01	Opis sytuacji problemowych	2
C02	Formułowanie problemów i hipotez badawczych	2
C03	Wybór i zastosowanie adekwatnej metody badawczej	2
C04	Przygotowanie narzędzi badawczych	2
C05	Organizowanie badań	2

C06	Zbieranie materiałów źródłowych i ich wykorzystanie w badaniach nad bezpieczeństwem (fakty, cytaty, parafrazy)	2
C07	Opracowanie koncepcji pracy dyplomowej – zaliczenie ćwiczeń	3

IV.	**KORELACJA EFEKTÓW UCZENIA SIĘ**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyki PRK*
W01	Cxm_W01, Cxm_K03	SIB2_W01, SIB2_K04	P7U_W, P7S_WG, P7U_K, P7S_KR
W02	Cxm_W02, Cxm_K02	SIB2_W01, SIB2_K02	P7U_W, P7S_WG, P7U_K, P7S_KK
W03	Cxm_W04	SIB2_W01	P7U_W, P7S_WG
W04	Cxm_W03, Cxm_K02	SIB2_W01, SIB2_K03	P7U_W, P7S_WG, P7U_K, P7S_KO
W05	Cxm_W03	SIB2_W01	P7U_W, P7S_WG
W06	Cxm_W05	SIB2_W01	P7U_W, P7S_WG
W07	Cxm_W05	SIB2_W01, SIB2_U02	P7U_W, P7S_WG, P7U_U, P7S_UW
C01	Cxm_U01, Cxm_K04	SIB2_U01, SIB2_U02	P7U_U, P7S_UW
C02	Cxm_U02	SIB2_U07	P7U_U, P7S_UU
C03	Cxm_U03	SIB2_U07	P7U_U, P7S_UU
C04	Cxm_U03	SIB2_U07	P7U_U, P7S_UU
C05	Cxm_U04	SIB2_U07	P7U_U, P7S_UU
C06	Cxm_U05	SIB2_U07	P7U_U, P7S_UU
C07	Cxm_U05	SIB2_U07	P7U_U, P7S_UU

V.	**NAKŁAD PRACY STUDENTA**			
Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**15**	**X**	**75**	**3**
Ćwiczenia	**15**			
Seminaria	**-**			
Konwersatoria	**-**			
Konsultacje (zaliczenie nieobecności, rozliczenie rygorów, poprawy)	**5**			
Przygotowanie do ćwiczeń	**X**	**10**		
Opanowanie informacji		**20**		
Przygotowanie do rozliczenia rygorów		**10**		
RAZEM	**35**	**40**		

VI.	**METODY I NARZĘDZIA DYDAKTYCZNE**
1.	Wykłady – oddziaływanie słowne i prezentacje multimedialne. Zagadnienia do pisemnego sprawdzianu wiedzy. Wykaz literatury do samodzielnego studiowania w celu pogłębienia wiedzy.
2.	Ćwiczenia - zadania do dyskusji i pisemnego rozwiązania.

VII.	**FORMA ZALICZENIA PRZEDMIOTU**	
Rygor	*Kryteria składowe*	*Waga*
Zaliczenie	Ocena wystąpień i rozwiązań prezentowanych na ćwiczeniach	0.5
	Ocena za znajomość teoretyczną przedmiotu.	0.5

VIII.	**LITERATURA**
	OBOWIĄZKOWA
1.	S. Nowak, *Metodologia badań społecznych*, PWN, Warszawa 2010.
2.	W. Zaczyński, *Praca badawcza nauczyciela*, Wydawnictwa Szkolne i Pedagogiczne, Warszawa 1995.
3.	R. Zenderowski, *Praca magisterska, licencjat*, wyd. CeDeWu.pl, Warszawa
	UZUPEŁNIAJĄCA

1.	A. Chalmers, *Czym jest to co zwiemy nauką?*, wyd. Siedmiogród, Wrocław 1977
2.	E. Babbie, *Podstawy nauk społecznych*, PWN, Warszawa 2009
3.	K. Pawlik, R. Zenderowski, *Dyplom z Internetu. Jak korzystać z Internetu pisząc prace dyplomowe*, Wydawnictwa Fachowe, Warszawa 2010
4.	J. Sztumski, *Wstęp do metod i technik badań społecznych*, wyd. „Śląsk", Katowice 2010
5.	Ch. Frankfort-Nachmias, *Metody badawcze w naukach społecznych*, wyd. Zysk i Ska, Poznań 2001

IX.	**PROWADZĄCY PRZEDMIOT**
Stopień, Imię i nazwisko	Prof. dr hab. Czesław JARECKI, Dr Stefan KOWALSKI
adres e-mail, tel.	c.jarecki@amw.gdynia.pl , s.kowalski@amw.gdynia.pl

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:	**Podstawy ekonomii**	*Kod*:	**Cea**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Stacjonarne		
Kształcenie w zakresie:	Cyberbezpieczeństwo, Analiza danych i informatyka śledcza		
Profil:	Ogólnoakademicki		
Liczba ECTS:	2		
Semestr:	2		
Wymagania wstępne:	Podstawowa wiedza z matematyki		
Język wykładowy:	Polski		
Cel przedmiotu:	**C01**	Prezentacja miejsca, znaczenia i motywacji podejmowania decyzji przez gospodarstwa domowe, przedsiębiorstwa i państwo	
	C02	Przybliżenie roli państwa w gospodarce rynkowej oraz jego aktywnej roli w rozwiązywaniu problemów gospodarczych i społecznych w tym problemów bezpieczeństwa narodowego	
	C03	Zapoznanie z cechami gospodarki rynkowej oraz uwarunkowaniami skuteczności mechanizmu rynkowego w warunkach społecznej gospodarki rynkowej (państwa dobrobytu)	

II.	**EFEKTY UCZENIA SIĘ**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Cea_W01**	Posiada wiedzę umożliwiają identyfikację i opis struktur, relacji, oraz konsekwencji funkcjonowania podmiotów rynkowych w skali mikro i makro	Kolokwium
	Cea_W02	Zna podstawowe podmioty gospodarki rynkowej oraz relacje między nimi występujące, a szczególnie funkcje państwa w gospodarce rynkowej	Kolokwium
	Cea_W03	Zna motywacje i uwarunkowania podejmowania decyzji alokacyjnych gospodarstwa domowego, przedsiębiorstwa i państwa	Kolokwium
Umiejętności:	**Cea_U01**	Potrafi interpolować wnioski z obszaru ekonomii na problemy bezpieczeństwa (potrafi identyfikować problem ekonomizacji bezpieczeństwa)	Kolokwium
	Cea_U02	Dokonuje obserwacji zjawisk i procesów w gospodarce oraz potrafi opisać i zinterpretować problemy ekonomiczne stosując podstawowe pojęcia teoretyczne	Kolokwium
	Cea_U03	Dokonuje oceny proponowanych rozwiązań problemów gospodarczych z uwzględnieniem skutków dla bezpieczeństwa narodowego	Kolokwium

Kompetencje społeczne:	**Cea_K01**	Posiada umiejętność rzeczowego argumentowania stanowiska w zakresie zaspokajania potrzeb publicznych przez państwo	Kolokwium
	Cea_K02	Potrafi prezentować i bronić swoich poglądów i uznawać argumentację innych	Kolokwium
	Cea_K03	W oparciu o uzyskaną podstawową wiedzę z ekonomii potrafi doskonalić swoją wiedzę i umiejętności z tego obszaru	Samokształcenie

III.	**TREŚCI PROGRAMOWE**	
Forma	*Temat, zagadnienia*	*Liczba godzin*
W01	**Wprowadzenie do gospodarki i ekonomii** (czym zajmuje się ekonomia; gospodarowanie; ekonomia a inne nauki; z historii myśli ekonomicznej; ekonomia pozytywna i normatywna; mikroekonomia i makroekonomia; rzadkość i inne problemy ekonomiczne; potrzeby; źródła zaspokajania potrzeb; racjonalność rzeczowa a racjonalność metodologiczna; prawa Engla; prawo Voblena; prawo Giffena; dylematy dobrobytu ekonomicznego i społecznego; współczesne systemy społeczno-gospodarcze)	3
W02	**Popyt, podaż i rynek** (rynek i jego cechy; popyt, cena, równowaga rynkowa.; krzywe popytu i podaży; co kryje się za krzywą popytu; przesunięcia krzywej popytu; co kryje się za krzywą podaży?; przesunięcia krzywej podaży; wolny rynek i kontrola cen; co, jak i dla kogo wytwarzać?)	3
W03	**Teoria wyboru konsumenta i elastyczność popytu** (zasady wyboru konsumenta; dostosowanie do zmian dochodu; dostosowania do zmian cen; od indywidualnej do rynkowej krzywej; popytu; dobra komplementarne i dobra substytucyjne; transfery gotówkowe i rzeczowe; reakcje popytu na zmiany cen; cena, wielkość popytu i suma wydatków; inne przykłady zastosowań elastyczności; elastyczność mieszana popytu; wpływ dochodu na popyt; wpływ inflacji na kształtowanie się popytu)	3
W04	**Funkcja produkcji** (organizacja przedsiębiorstwa; przychody, koszty i zyski; maksymalizacja zysku w przedsiębiorstwie; decyzje produkcyjne przedsiębiorstwa: analiza ogólna; izokwanta, izokoszta, efektywność produkcji, koszt krańcowy i utarg krańcowy)	3
W05	**Struktury rynku, konkurencja doskonała, niedoskonałai pełny monopol** (konkurencja doskonała; decyzje produkcyjne przedsiębiorstwa w warunkach konkurencji doskonałej; krzywe podaży gałęzi; statyka porównawcza w przypadku gałęzi wolnokonkurencyjnej; konkurencja na rynkach światowych; konkurencja monopolistyczna; oligopol i współzależność; wejście i potencjalna konkurencja; strategiczne odstraszanie kandydatów do wejścia; produkcja i cena w warunkach monopolu i konkurencji doskonałej; monopol a postęp techniczny; koszt społeczny monopolu)	3
W06	**Udział państwa w gospodarce w ujęciu mikroekonomicznym** (argumenty za udziałem państwa; argumenty przeciw udziałowi państwa; rola przypisywana państwu w różnych systemach gospodarczych i przez różne nurty ekonomiczne; równość i	3

	efektywność; konkurencja doskonała a efektywność w sensie Pareta; zawodność rynku; problemy ze środowiskiem; jakość, zdrowie i bezpieczeństwo)	
W07	**Determinanty dochodu narodowego. Analiza krótkookresowa i długookresowa** (zarys głównych stanowisk teoretycznych; produkt i dochód narodowy; pojęcie i podstawowe problemy makroekonomii; problem agregacji; metody obliczania produktu krajowego brutto; produkt narodowy brutto i dochód narodowy; produkt i dochód narodowy jako miary poziomu rozwoju gospodarczego i dobrobytu; pojęcie i mechanizm równowagi; funkcja konsumpcji; równowaga w uproszczonym modelu gospodarki; równość inwestycji i oszczędności; mnożnik; równowaga w rozwiniętym modelu gospodarki; czynniki wzrostu gospodarczego; pełne zatrudnienie a potencjalny PKB; model wzrostu Solowa; formuła wzrostu gospodarczego; polityka pobudzania wzrostu; płace a zwolnienie tempa wzrostu wydajności pracy; zrost gospodarczy a tendencje postępu technicznego; popytowe czynniki wzrostu; granice wzrostu gospodarczego.)	3
W08	**Budżet państwa** (pojęcie i funkcje budżetu państwa; dochody budżetu państwa; wydatki budżetu państwa; podatki i wydatki państwa jako instrumenty 3stabilizacji koniunktury; mnożnikowy efekt wydatków, podatków i zrównoważenia budżetu; aktywna i pasywna polityka fiskalna; automatyczne stabilizatory koniunktury; deficyt budżetowy i dług publiczny; budżet państwa w Polsce w okresie transformacji gospodarki)	3
W09	**System pieniężno-kredytowy** (istota i funkcje pieniądza; ewolucja pieniądza i systemu pieniężnego; zasoby pieniądza; koszt posiadania pieniądza; popyt na pieniądz i podaż pieniądza; czynniki determinujące popyt na pieniądz; powstanie i funkcje banków; bank centralny. Instrumenty kontroli podaży pieniądza; czynniki determinujące podaż pieniądza; równowaga na rynku pieniężnym; niebankowe instytucje pośrednictwa finansowego; rynek pieniężny i kapitałowy; pieniądz i banki w okresie transformacji gospodarki polskiej)	3
W10	**Cykl koniunkturalny** (pojęcie cyklu koniunkturalnego; fazy cyklu; rodzaje wahań cyklicznych; cykl a wzrost gospodarczy; teorie wahań cyklicznych; metody oddziaływania państwa na przebieg cyklu koniunkturalnego; wahania stopy wzrostu i kryzysy w gospodarce centralnie planowanej)	2
W11	**Bezrobocie i inflacja** (pojęcie bezrobocia; typy bezrobocia; bezrobocie w wybranych krajach; przyczyny bezrobocia; bezrobocie a działalność państwa; zatrudnienie i bezrobocie w gospodarce centralnie planowanej; bezrobocie w Polsce w okresie transformacji; pojęcie, sposoby pomiaru oraz nasilenie inflacji; społeczno-ekonomiczne skutki inflacji; główne teorie inflacji; inflacja a bezrobocie; koncepcja krzywej Phillipsa; inflacja w Polsce w okresie transformacji	2

IV.	**KORELACJA EFEKTÓW UCZENIA SIĘ**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyki PRK*
W01	Cea_W01, Cea_U01, Cea_K03	SIB2_W01; SIB2_U02; SIB2_K01	P7U_W P7S_WG P7U_W P7U_U P7U_UW; P7U_KP7S_KK
W02	Cea_W02, Cea_K03	SIB2_W01; SIB2_U02, SIB2_K01	P7U_W; P7S_WG; P7U_UW; P7U_K; P7S_KK

W03	Cea_W01, Cea_W03, Cea_K03	SIB2_W01; SIB2_W02, SIB2_U02; SIB2_W05; SIB2_K01	P7U_W; P7S_WG; P7U_W; P7S_WK; P7U_UW; P7U_K; P7S_KK
W04	Cea_W02, Cea_W03, Cea_K03	SIB2_W01; SIB2_W02, SIB2_U02; SIB2_W05; SIB2_K01	P7U_W; P7S_WG; P7U_W; P7S_WK; P7U_UW; P7U_K; P7S_KK
W05	Cea_W01, Cea_W02, Cea_K03	SIB2_W01; SIB2_W02, SIB2_U02; SIB2_K01	P7U_W; P7S_WG; P7U_W; P7S_WK; P7U_UW; P7U_K; P7S_KK
W06	Cea_W01, Cea_U02,Cea_K03	SIB2_W01; SIB2_W02, SIB2_U02; SIB2_K01	P7U_W; P7S_WG; P7U_W; P7S_WK; P7U_UW; P7U_K; P7S_KK
W07	Cea_W01, Cea_U01, Cea_K01,Cea_K03	SIB2_W01, SIB2_U02; SIB2_K02, SIB2_K03	P7U_W; P7S_WG; P7U_W; P7U_U; P7U_UW; P7U_K; P7S_KO; P7U_K; P7S_KK
W08	Cea_W01, Cea_U01, Cea_K01,Cea_K03	SIB2_W01, SIB2_U02; SIB2_K02, SIB2_K03	P7U_W; P7S_WG; P7U_U; P7U_UW; P7U_K; P7S_KO; P7U_K; P7S_KK
W09	Cea_W01, Cea_U01,Cea_K01	SIB2_W01; SIB2_U02; SIB2_K02;	P7U_W; P7S_WG; P7U_U; P7U_UW; P7U_K; P7S_KO;
W10	Cea_W01, Cea_U01, Cea_K02, Cea_K03	SIB2_W01; SIB2_U02; SIB2_K02; SIB2_K03	P7U_W; P7S_WG; P7U_U; P7U_UW; P7U_K; P7S_KO; P7U_K; P7S_KK
W11	Cea_W01, Cea_U01, Cea_K03	SIB2_W01; SIB2_U02; SIB2_K03	P7U_W; P7S_WG; P7U_U; P7U_UW; P7U_K; P7S_KK

V. NAKŁAD PRACY STUDENTA

Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**30**	**X**	**50**	**2**
Ćwiczenia	**0**			
Seminaria	**0**			
Konwersatoria	**0**			
Konsultacje (zaliczenie nieobecności, rozliczenie rygorów, poprawy)	**5**			
Przygotowanie do ćwiczeń	**X**	**0**		
Opanowanie informacji		**10**		
Przygotowanie do rozliczenia rygorów		**5**		
RAZEM	**35**	**15**		

VI. METODY I NARZĘDZIA DYDAKTYCZNE

- wykład; - formy aktywizujące; - wykaz tez do dyskusji	- prezentacja multimedialna;

VII. FORMA ZALICZENIA PRZEDMIOTU

Rygor	*Kryteria składowe*	*Waga*
Zaliczenie	Ocena z kolokwium	1,0

VIII. LITERATURA

OBOWIĄZKOWA

1. D. Begg, *Ekonomia – Makroekonomia*, PWE
2. D. Begg, *Ekonomia – Mikroekonomia*, PWE;
3. B . Czarny, *Podstawy ekonomii*, Polsof-AKADEMIA

UZUPEŁNIAJĄCA

1. R. E. Hall, J. B. Taylor, *Makroekonomia*, PWN
2. N. G. Mankiw, M. P. Taylor, *Mikroekonomia*, PWE
3. P. A. Samuelson, *Ekonomia*, PWN
4. M. Szczepaniec, Makroekonomia, Wydawnictwo UG
5. H. R. Varian, *Mikroekonomia*, PWN

IX.	PROWADZĄCY PRZEDMIOT
Stopień, Imię i nazwisko	dr hab. Jarosław TESKA
adres e-mail, tel.	j.teska@amw.gdynia.pl

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:	**Podstawy prawa**	*Kod*:	**Cap**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Stacjonarne		
Kształcenie w zakresie:	Cyberbezpieczeństwo, Analiza danych i informatyka śledcza		
Profil:	Ogólnoakademicki		
Liczba ECTS:	2		
Semestr:	2		
Wymagania wstępne:	-		
Język wykładowy:	Polski		
Cel przedmiotu:	**C01**	Zaznajomienie z podstawowymi pojęciami z zakresu nauki o prawie	
	C02	Przedstawienie charakterystyki systemu prawa	
	C03	Zaznajomienie z wiadomościami z zakresu podmiotów, przedmiotu, tworzenia i stosowania prawa	

II.	**EFEKTY UCZENIA SIĘ**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Cap_W01**	Student ma wiedzę z zakresu definiowania prawa i znajomości systematyzacji prawa	Kolokwium
	Cap0_W2	Student ma podstawową wiedzę z zakresu znajomości podstawowych instytucji prawa i jego funkcji	Kolokwium
	Cap_W03	Student zna źródła prawa (ich umiejscowienie w systemie prawa i poprawną hierarchię oraz budowę), zna zasady tworzenia, stosowania i interpretowania prawa	Kolokwium
	Cap_W04	Student ma wiedzę z zakresu struktury stosunku prawnego, jego powstawania i zmian oraz skutków tym wywoływanych	Kolokwium
Umiejętności:	**Cap_U01**	Student potrafi dokonać analizy prostego aktu prawnego, zdarzenia prawnego	Kolokwium
	Cap_U02	Student potrafi zastosować konstrukcje prawne w celu rozwiązania problemów pojawiających się podczas tworzenia, przestrzegania i stosowania prawa	Kolokwium
	Cap_U03	Student potrafi zastosować dyrektywy wykładni prawa	Kolokwium
Kompetencje społeczne:	**Cap_K01**	Student potrafi współdziałać w grupie w celu rozwiązania problemów związanych z danym stanem faktycznym	Kolokwium

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

W01	Zajęcia wprowadzające (zapoznanie z celem nauczania przedmiotu, przedstawienie literatury przedmiotu, podanie wymagań na zaliczenie przedmiotu)	2
W02	Nauki prawne (podział nauk, przedmiot badań nauk prawnych)	4
W03	Źródła prawa (historyczne źródła prawa, konstytucja i inne źródła prawa)	4
W04	System prawa (historyczne systemy prawa, współczesne pojęcie i rodzaje systemów prawa)	4
W05	Stanowienie i obowiązywanie prawa (formy tworzenia prawa, procesy stanowienia prawa, pojęcie aktu normatywnego i jego budowy, obowiązywanie prawa w miejscu i czasie)	4
W06	Podmioty i przedmioty prawa	4
W07	Wykładnia prawa (pojęcie wykładni, racjonalny prawodawca, luki w prawie)	4
W08	Stosowanie prawa (aspekt proceduralny i merytoryczny), zaliczenie	4

IV. KORELACJA EFEKTÓW UCZENIA SIĘ

Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyki PRK*
W01	Cap_W02	SIB2_W01	P7U_W P7S_WG
W02	Cap_W01, Cap_W02	SIB2_W01, SIB2_W03	P7U_W P7S_WK P7U_W P7S_WG
W03	Cap_W03	SIB2_W03	P7U_W P7S_WK
W04	Cap_W01,Cap_W02,Cap_W03,Cap_U01	SIB2_W03; SIB2_U01	P7U_W P7S_WK P7U_U P7S_UW
W05	Cap_W04, Cap_U02	SIB2_W03; SIB2_U07	P7U_W P7S_WK P7U_U P7S_UU
W06	Cap_W02,Cap_W04	SIB2_U01	P7U_W P7S_WG
W07	Ca_W01,Cap_W02, Cap_W03	SIB2_U01	P7U_W P7S_WK P7U_W P7S_WG
W08	Cap_W03,Cap_W04,Cap_U03,Cap_K01	SIB2_W03; SIB2_U07; SIB2_K04	P7U_W P7S_WK P7U_U P7S_UU P7U_K P7S_KR

V. NAKŁAD PRACY STUDENTA

Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**30**	**X**	**50**	**2**
Ćwiczenia				
Seminaria				
Konwersatoria				
Konsultacje (zaliczenie nieobecności, rozliczenie rygorów, poprawy)	**5**			
Przygotowanie do ćwiczeń	**X**	**0**		
Opanowanie informacji		**10**		
Przygotowanie do rozliczenia rygorów		**5**		
RAZEM	**35**	**15**		

VI. METODY DYDAKTYCZNE

1. Wykład - Prezentacja multimedialna

VII. FORMA ZALICZENIA PRZEDMIOTU

Rygor	*Kryteria składowe*	*Waga*
Zaliczenie	Ocena z kolokwium	1,0

VIII. LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

OBOWIĄZKOWA

1. A. Bator, W. Gromski, A. Kozak, S. Kaźmierczyk, Z. Pulka, *Wprowadzenie do nauk prawnych, Leksykon tematyczny*, Wydanie I, Wydawnictwo Prawnicze LexisNexis, Warszawa 2006

2.	S. Korycki, J. Kuciński, Z. Trzciński, J. Zaborowski, *Zarys prawa*, pod red. S. Koryckiego i J. Kucińskiego, Wydanie V, LexisNexis, Warszawa 2006
3.	T. Stawecki, P. Winczorek, *Wstęp do prawoznawstwa*, Wydawnictwo C. H. Beck, Warszawa 2003
UZUPEŁNIAJĄCA	
1.	M. Zirk-Sadowski, *Wprowadzenie do filozofii prawa*, Zakamycze, Kraków 2000
2.	L. Morawski, *Główne problemy współczesnej filozofii prawa. Prawo w toku przemian*, Wydanie III, LexisNexis, Warszawa 2003
3.	R. Dworkin, *Biorąc prawa poważnie*, PWN, Warszawa 1998
IX.	**PROWADZĄCY PRZEDMIOT**
Stopień, Imię i nazwisko	Dr hab. Dariusz BUGAJSKI
adres e-mail	d.bugajski@awm.gdynia.pl

KARTA PRZEDMIOTU	AKADEMIA MARYNARKI WOJENNEJ WYDZIAŁ DOWODZENIA I OPERACJI MORSKICH	

I.	CHARAKTERYSTYKA PRZEDMIOTU		
Nazwa przedmiotu:	**Wprowadzenie do psychologii społecznej**	*Kod*:	**Pps**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Stacjonarne		
Kształcenie w zakresie:	Cyberbezpieczeństwo, Analiza danych i informatyka śledcza		
Profil:	Ogólnoakademicki		
Liczba ECTS:	2		
Semestr:	2		
Wymagania wstępne:	Brak		
Język wykładowy:	Polski		
Cel przedmiotu:	**C01**	Rozumie związek problematyki bezpieczeństwa z zagadnieniami psychologicznymi	
	C02	Zna mechanizmy i funkcje procesów psychicznych orientujących jednostkę w świecie oraz regulujące zachowanie człowieka	
	C03	Identyfikuje różne stanowiska teoretyczne wyjaśniające mechanizmy przebiegu funkcji poznawczych	

II.	EFEKTY UCZENIA		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Pps_W01**	Student rozumie bezpieczeństwo jako podstawową potrzebę człowieka; zna relacje pomiędzy bezpieczeństwem i zagrożeniem a przebiegiem różnorodnych procesów psychicznych, w tym – poznawczych i emocjonalnych	Kolokwium
	Pps_W02	Posiada wiedzę w zakresie psychologicznych koncepcji człowieka	Kolokwium
Umiejętności:	**Pps_U01**	Potrafi identyfikować grupy potrzeb człowieka, rozumiejąc warunki ich zaspokajania i wskazując potencjalne obszary deprywacji potrzeb jako sytuacje generujące zagrożenia dla bezpieczeństwa (w tym psychologicznego) jednostek i zbiorowości	Wypowiedź ustna
	Pps_U02	Student potrafi płynnie wypowiadać się na tematy związane z problematyką zajęć.	Wypowiedź ustna
Kompetencje społeczne:	**Pps_K01**	Student docenia znaczenie całożyciowego poszerzania swojej wiedzy w zakresie psychologii człowieka	Wypowiedź ustna

III.	TREŚCI PROGRAMOWE	
Forma	*Tematyka*	*Liczba godzin*
W01	Wprowadzenie do psychologii. Samoświadomość.	3
W02	Samoocena i poczucie własnej wartości.	4
W03	Człowiek w ujęciu psychologii poznawczej. Wybrane funkcje i procesy poznawcze (percepcja, pamięć, uwaga, skrypty i schematy poznawcze,	6

	myślenie i jego rodzaje). Błędy poznawcze i kontrola poznawcza. Podejmowanie decyzji i źródła błędów w podejmowaniu decyzji.	
W04	Wpływ sytuacji społecznej na zachowania ludzi i „sytuacyjne przemiany charakteru". Autorytet, konformizm, przemoc w relacjach międzyludzkich. Deprywacja potrzeb a sytuacyjne przemiany charakteru,	6
W05	Człowiek w relacjach społecznych – atrakcyjność interpersonalna, budowanie relacji i związki z innymi.	4
W06	Ocenianie innych, uprzedzenia i dyskryminacja – psychologiczne źródła i społeczne konsekwencje.	4
W07	Stres i jego rodzaje. Konsekwencje stresu. Profilaktyka.	3

IV.	**KORELACJA EFEKTÓW UCZENIA SIĘ**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyki PRK*
W01	Pps_W01, Pps_W02, Pps_U01, Pps_U02, Pps_K01	SIB2_W01, SIB2_U01, SIB2_U07, SIB2_K01	P7U_W P7S_WG P7U_U P7S_UW P7U_U P7S_UU P7U_K P7S_KK
W02	Pps_W01, Pps_W02, Pps_U01, Pps_U02, Pps_K01	SIB2_W01, SIB2_U01, SIB2_U07, SIB2_K01	P7U_W P7S_WG P7U_U P7S_UW P7U_U P7S_UU P7U_K P7S_KK
W03	Pps_W01, Pps_W02, Pps_U01, Pps_U02, Pps_K01	SIB2_W01, SIB2_U01, SIB2_U07, SIB2_K01	P7U_W P7S_WG P7U_U P7S_UW P7U_U P7S_UU P7U_K P7S_KK
W04	Pps_W01, Pps_W02, Pps_U01, Pps_U02, Pps_K01	SIB2_W01, SIB2_U01, SIB2_U07, SIB2_K01	P7U_W P7S_WG P7U_U P7S_UW P7U_U P7S_UU P7U_K P7S_KK
W05	Pps_W01, Pps_W02, Pps_U01, Pps_U02, Pps_K01	SIB2_W01, SIB2_U01, SIB2_U07, SIB2_K01	P7U_W P7S_WG P7U_U P7S_UW P7U_U P7S_UU P7U_K P7S_KK
W06	Pps_W01, Pps_W02, Pps_U01, Pps_U02, Pps_K01	SIB2_W01, SIB2_U01, SIB2_U07, SIB2_K01	P7U_W P7S_WG P7U_U P7S_UW P7U_U P7S_UU P7U_K P7S_KK
W07	Pps_W01, Pps_W02, Pps_U01, Pps_U02, Pps_K01	SIB2_W01, SIB2_U01, SIB2_U07, SIB2_K01	P7U_W P7S_WG P7U_U P7S_UW P7U_U P7S_UU P7U_K P7S_KK

V.	**NAKŁAD PRACY STUDENTA**			
Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**30**	**X**	**50**	**2**
Ćwiczenia	**-**			
Seminaria	**-**			
Konwersatoria	**-**			
Konsultacje (zaliczenie nieobecności, rozliczenie rygorów, poprawy)	**5**			
Przygotowanie do ćwiczeń	**X**	**-**		
Opanowanie informacji		**10**		
Przygotowanie do rozliczenia rygorów		**5**		
RAZEM	**35**	**15**		

VI.	**METODY DYDAKTYCZNE**
1.	Wykład problemowy z elementami dyskusji grupowej

VII.	FORMA ZALICZENIA PRZEDMIOTU	
Rygor	*Kryteria składowe*	*Waga*
Zaliczenie	Kolokwium pisemne, pytania otwarte i zamknięte	1,0
VIII.	**LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA**	
OBOWIĄZKOWA		
1.	P. G. Zimbardo, R. L. Johnson, V. McCain (red.), *Psychologia. Kluczowe koncepcje*, t. 1-5, PWN, Warszawa 2014 i in. (wybrane fragmenty).	
2.	Ph. G. Zimbardo, *Efekt Lucyfera. Dlaczego dobrzy ludzie czynią zło*, PWN, Warszawa 2008.	
UZUPEŁNIAJĄCA		
1.	J. Kozielecki, *Koncepcje psychologiczne człowieka*, Wydawnictwo Akademickie Żak, Warszawa 1997.	
2.	B. Wojciszke, Psychologia społeczna. GWP, Gdańsk 2011.	
IX.	**PROWADZĄCY PRZEDMIOT**	
Stopień, Imię i nazwisko	Dr hab. Iwona PIETKIEWICZ	
adres e-mail	i.pietkiewicz@amw.gdynia.pl	

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:	**Podstawy socjologii**	*Kod*:	**Isx**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Stacjonarne		
Kształcenie w zakresie:	Cyberbezpieczeństwo, Analiza danych i informatyka śledcza		
Profil:	Ogólnoakademicki		
Liczba ECTS:	2		
Semestr:	2		
Wymagania wstępne:	Brak		
Język wykładowy:	Polski		
Cel przedmiotu:	**C01**	Prezentacja podstawowych problemów społecznych i zachodzących w świecie zmian.	
	C02	Przybliżenie istoty socjologicznych zachowań społecznych oraz podstawowych problemów związanych z procesami modernizacji społecznej.	

II.	EFEKTY UCZENIA SIĘ		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Isx_W01**	Student wyjaśnia kluczowe koncepcje z zakresu logiki, wnioskowania i metodologii badań socjologicznych.	Kolokwium
	Isx_W02	Student objaśnia i ilustruje kulturowe, polityczne i społeczne procesy występujące na poziomie państwa i układów międzynarodowych wraz z ich przełożeniem na problemy bezpieczeństwa narodowego.	Kolokwium
	Isx_W03	Student ma pogłębioną wiedzę z zakresu kierunków rozwoju nowych gałęzi wiedzy, gospodarki i technologii, w tym informatycznych.	Kolokwium
	Isx_W04	Student w sposób poszerzony zna i objaśnia potrzeby kulturowe, religijne, gospodarcze, polityczne i inne, zwłaszcza społeczne, których zachwianie zaspokajania może powodować stany labilne i niebezpieczne.	Kolokwium
	Isx_W05	Student rozróżnia i wyjaśnia zasady tworzenia formalnych i nieformalnych społecznych struktur organizacyjnych oraz mechanizmy w nich rządzące na rzecz osiągania zamierzonych celów.	Kolokwium
Umiejętności:	**Isx_U01**	Student formułuje objaśnienia zjawisk społecznych, politycznych i kulturowych przebiegających zarówno w skali państwa jak i w skali międzynarodowej, a także oceniać zależności między przyczynami a poziomem intensywności zakłóceń występujących w tych obszarach.	Kolokwium
	Isx_U02	Student identyfikuje poprawnie zależności między zjawiskami społecznymi, politycznymi i	Kolokwium

		kulturowymi tworzącymi bezpieczeństwo narodowe lub oddziaływującymi na nie a także system oddziaływania normatywnych regulacji na wspomniane obszary (normy prawne, standardy zawodowe, systemy normalizacji i standaryzacji, normy moralne, normy kulturowe).	
	Isx_U03	Student posiada umiejętność rozumienia i analizowania różnorodnych zjawisk, w tym społecznych mających związek z bezpieczeństwem narodowym.	Kolokwium
Kompetencje społeczne:	**Isx_K01**	Student inicjuje i moderuje pracę w grupie, przyjmując w niej różne role, potrafi podporządkować się celom grupy ale także przyjmować funkcje lidera zadaniowego.	Odpowiedź tablicowa
	Isx_K02	Student działa z poszanowaniem zasad formalnych i metodycznie rozwiązuje problemy organizacyjne i inne.	Odpowiedź tablicowa

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
W01	Społeczeństwo jako przedmiot badań socjologicznych (socjologiczna wyobraźnia i język socjologii; współczesne perspektywy socjologiczne; socjologiczne metody badawcze; proces badawczy; rozumienie związków przyczynowo-skutkowych; metody badawcze).	2
W02	Socjologiczne pojęcie kultury (pojęcie kultury, tradycja kulturowa i tworzenie kultury; socjalizacja i kontrola społeczna; świadomość społeczna).	2
W03	Zmiana społeczna, rozwój i postęp (czynniki zmiany społecznej; zmiana w epoce nowoczesnej).	2
W04	Elementy teorii zachowań społecznych. Grupy i więzi społeczne (zachowania, czynności i działania społeczne; klasyfikacja grup społecznych).	2
W05	Klasy, stratyfikacja i nierówności (funkcje i geneza nierówności; warstwy i klasy społeczne; ruchliwość społeczna).	2
W06	Socjologia organizacji (gospodarka jako system społeczny; teorie organizacji; struktury społeczne; zmiany sposobów zarządzania; zmiany w systemie pracy; gospodarka oparta na wiedzy).	2
W07	Państwo i zbiorowości terytorialne nowoczesne państwo; pojęcie państwa; systemy polityczne; opiekuńczość państwa; zmiana polityczna i społeczna).	2
W08	Społeczeństwo jako przedmiot badań socjologicznych.	2
W09	Socjologiczne pojęcie kultury.	2
W10	Zmiana społeczna, rozwój i postęp.	2
W11	Elementy teorii zachowań społecznych. Grupy i więzi społeczne.	2
W12	Klasy, stratyfikacja i nierówności.	2
W13	Socjologia organizacji.	2
W14	Państwo i zbiorowości terytorialne.	2
W15	Kolokwium.	2

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

W01	Isx_W01, Isx_W03, Isx_U03, Isx_K02	SIB2_W01, SIB2_W02, SIB2_U02, SIB2_U07, SIB2_K03	P7U_W, P7S_WG, P7U_W P7S_WK, P7S_UW, P7U_U, P7S_UU, P7U_K, P7S_KO
W02	Isx_W02, Isx_W03, Isx_W04, Isx_U01, Isx_U02, Isx_U03	SIB2_W01, SIB2_W02, SIB2_U02, SIB2_U07, SIB2_K03	P7U_W, P7S_WG, P7U_W P7S_WK, P7S_UW, P7U_U, P7S_UU, P7U_K, P7S_KO
W03	Isx_W02, Isx_W03, Isx_U01, Isx_U02, Isx_U03, Isx_K01, Isx_K02	SIB2_W01, SIB2_W02, SIB2_U02, SIB2_U07, SIB2_K03	P7U_W, P7S_WG, P7U_W P7S_WK, P7S_UW, P7U_U, P7S_UU, P7U_K, P7S_KO
W04	Isx_W02, Isx_W03, Isx_W04, Isx_W05, Isx_U01, Isx_U02, Isx_U03, Isx_K01, Isx_K02	SIB2_W01, SIB2_W02, SIB2_U02, SIB2_U07, SIB2_K03	P7U_W, P7S_WG, P7U_W P7S_WK, P7S_UW, P7U_U, P7S_UU, P7U_K, P7S_KO
W05	Isx_W02, Isx_W03, Isx_W04, Isx_W05, Isx_U01, Isx_U02, Isx_U03, Isx_K01, Isx_K02	SIB2_W01, SIB2_W02, SIB2_U02, SIB2_U07, SIB2_K03	P7U_W, P7S_WG, P7U_W P7S_WK, P7S_UW, P7U_U, P7S_UU, P7U_K, P7S_KO
W06	Isx_W02, Isx_W03, Isx_W04, Isx_W05, Isx_U01, Isx_U02, Isx_U03, Isx_K01, Isx_K02	SIB2_W01, SIB2_W02, SIB2_U02, SIB2_U07, SIB2_K03	P7U_W, P7S_WG, P7U_W P7S_WK, P7S_UW, P7U_U, P7S_UU, P7U_K, P7S_KO
W07	Isx_W02, Isx_W03, Isx_W04, Isx_W05, Isx_U01, Isx_U02, Isx_U03, Isx_K01, Isx_K02	SIB2_W01, SIB2_W02, SIB2_U02, SIB2_U07, SIB2_K03	P7U_W, P7S_WG, P7U_W P7S_WK, P7S_UW, P7U_U, P7S_UU, P7U_K, P7S_KO
W08	Isx_W02, Isx_W03, Isx_W04, Isx_W05, Isx_U01, Isx_U02, Isx_U03, Isx_K01, Isx_K02	SIB2_W01, SIB2_W02, SIB2_U02, SIB2_U07, SIB2_K03	P7U_W, P7S_WG, P7U_W P7S_WK, P7S_UW, P7U_U, P7S_UU, P7U_K, P7S_KO
W09	Isx_W02, Isx_W03, Isx_W04, Isx_W05, Isx_U01, Isx_U02, Isx_U03, Isx_K01, Isx_K02	SIB2_W01, SIB2_W02, SIB2_U02, SIB2_U07, SIB2_K03	P7U_W, P7S_WG, P7U_W P7S_WK, P7S_UW, P7U_U, P7S_UU, P7U_K, P7S_KO
W10	Isx_W02, Isx_W03, Isx_W04, Isx_W05, Isx_U01, Isx_U02, Isx_U03, Isx_K01, Isx_K02	SIB2_W01, SIB2_W02, SIB2_U02, SIB2_U07, SIB2_K03	P7U_W, P7S_WG, P7U_W P7S_WK, P7S_UW, P7U_U, P7S_UU, P7U_K, P7S_KO
W11	Isx_W02, Isx_W03, Isx_W04, Isx_W05, Isx_U01, Isx_U02, Isx_U03, Isx_K01, Isx_K02	SIB2_W01, SIB2_W02, SIB2_U02, SIB2_U07, SIB2_K03	P7U_W, P7S_WG, P7U_W P7S_WK, P7S_UW, P7U_U, P7S_UU, P7U_K, P7S_KO
W12	Isx_W02, Isx_W03, Isx_W04, Isx_W05, Isx_U01, Isx_U02, Isx_U03, Isx_K01, Isx_K02	SIB2_W01, SIB2_W02, SIB2_U02, SIB2_U07, SIB2_K03	P7U_W, P7S_WG, P7U_W P7S_WK, P7S_UW, P7U_U, P7S_UU, P7U_K, P7S_KO
W13	Isx_W02, Isx_W03, Isx_W04, Isx_W05, Isx_U01, Isx_U02, Isx_U03, Isx_K01, Isx_K02	SIB2_W01, SIB2_W02, SIB2_U02, SIB2_U07, SIB2_K03	P7U_W, P7S_WG, P7U_W P7S_WK, P7S_UW, P7U_U, P7S_UU, P7U_K, P7S_KO
W14	Isx_W02, Isx_W03, Isx_W04, Isx_W05, Isx_U01, Isx_U02, Isx_U03, Isx_K01, Isx_K02	SIB2_W01, SIB2_W02, SIB2_U02, SIB2_U07, SIB2_K03	P7U_W, P7S_WG, P7U_W P7S_WK, P7S_UW, P7U_U, P7S_UU, P7U_K, P7S_KO
W15	Isx_W02, Isx_W03, Isx_W04, Isx_W05, Isx_U01, Isx_U02, Isx_U03, Isx_K01, Isx_K02	SIB2_W01, SIB2_W02, SIB2_U02, SIB2_U07, SIB2_K03	P7U_W, P7S_WG, P7U_W P7S_WK, P7S_UW, P7U_U, P7S_UU, P7U_K, P7S_KO

V.	**NAKŁAD PRACY STUDENTA**			
Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**30**	**X**	**50**	**2**
Ćwiczenia				
Seminaria				
Konwersatoria				

Konsultacje (zaliczenie nieobecności, rozliczenie rygorów, poprawy)	**5**			
Przygotowanie do ćwiczeń	**X**			
Opanowanie informacji		**10**		
Przygotowanie do rozliczenia rygorów		**5**		
RAZEM	**35**	**15**		

VI.	**METODY DYDAKTYCZNE**
1.	Wykład
2.	Ćwiczenia
3.	Praca w grupach i inne formy aktywizujące
4.	Wykaz tez do dyskusji
5.	Prezentacja multimedialna

VII.	**FORMA ZALICZENIA PRZEDMIOTU**	
Rygor	*Kryteria składowe*	*Waga*
Zaliczenie	Odpowiedzi ustne i udział w dyskusji na zajęciach	0,4
	Ocena z kolokwium	0,6

VIII.	**LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA**
	OBOWIĄZKOWA
1.	A. Giddens, *Socjologia*, wyd. PWN, Warszawa 2005
2.	P. Sztompka, *Socjologia. Analiza społeczeństwa*, wyd. Znak, Kraków 2002
3.	P. Sztompka, Kucia M. red., *Socjologia. Lektury*, wyd. Znak, Kraków 2009
	UZUPEŁNIAJĄCA
1.	A. Touraine, *O socjologii*, wyd. PWN, Warszawa 2010
2.	A. Kłoskowska, *Socjologia kultury*, wyd. PWN, Warszawa 2007
3.	E. Babbie, *Podstawy badań społecznych*, wyd. PWN, Warszawa 2013

IX.	**PROWADZĄCY PRZEDMIOT**
Stopień, Imię i nazwisko	dr Andrzej ŁAPA
adres e-mail	a.lapa@amw.gdynia.pl

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:	**Podstawy stosunków międzynarodowych (pol./ang)**	*Kod*:	**Ysq**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Stacjonarne		
Kształcenie w zakresie:	Cyberbezpieczeństwo, Analiza danych i informatyka śledcza		
Profil:	Ogólnoakademicki		
Liczba ECTS:	2		
Semestr:	2		
Wymagania wstępne:	Brak		
Język wykładowy:	Polski		
Cel przedmiotu:	**C01**	Zapoznanie studenta z podstawowymi problemami współczesnych stosunków międzynarodowych.	
	C02	Wskazanie podstawowych zagrożeń dla trwałości systemu międzynarodowego.	
	C03	Wskazanie podstawowych obszarów współpracy międzynarodowej.	

II.	**EFEKTY UCZENIA SIĘ**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Ysq_W01**	Określa związki nauk o bezpieczeństwie ze stosunkami międzynarodowymi	Test
	Ysq_W02	Charakteryzuje określone instytucje polityczne i gospodarcze w wymiarze międzynarodowym	Test
	Ysq_W03	Tłumaczy procesy zachodzące na poziomie państwa i układów międzynarodowych oraz ich znaczenie dla problemów bezpieczeństwa międzynarodowego	Test
	Ysq_W04	Wyróżnia istotne wyzwania i zagrożenia dla współczesnego świata o charakterze politycznym, militarnym, religijnym i społecznym	Test
Umiejętności:	**Ysq_U01**	Analizuje przyczyny i przebieg procesów i zjawisk politycznych i ekonomicznych w sferze międzynarodowej oraz płynące z tych obszarów zagrożenia bezpieczeństwa narodowego	Test
	Ysq_U02	Analizuje zależności między zjawiskami społecznymi, ekonomicznymi, politycznymi, prawnymi i kulturowymi tworzącymi bezpieczeństwo narodowe	Test
Kompetencje społeczne:	**Ysq_K01**	Akceptuje potrzebę poszerzania swojej wiedzy i umiejętności przez całe życie	Test

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
W01	Wprowadzenie do przedmiotu, kryteria zaliczenia	1

W02	Stosunki międzynarodowe jako dyscyplina naukowa. Co nam daje badanie stosunków międzynarodowych	2
W03	Kontekst historyczny w rozwoju stosunków międzynarodowych	2
W04	Podmioty relacji w stosunkach międzynarodowych – państwa – organizacje międzynarodowe – organizacje transnarodowe	2
W05	Podstawowe dylematy współczesnych stosunków międzynarodowych – polityka, prawo międzynarodowe, ekonomia	2
W06	Główne kierunki rozważań o stosunkach międzynarodowych – przykłady doktryn polityki zagranicznej współczesnych państw	2
W07	Realizm i neorealizm, liberalizm i neoliberalizm	2
W08	Szkoła angielska, konstruktywizm, feminizm	2
W09	Teorie integracji europejskiej	2
W10	Globalizm	2
W11	Hegemonia	2
W12	Rola organizacji międzynarodowych	2
W13	Konflikty w stosunkach międzynarodowych	2
W14	Rola dyplomacji	2
W15	Bezpieczeństwo w stosunkach międzynarodowych – instytucjonalizacja	2
W16	Zaliczenie przedmiotu – kolokwium	1

IV.	**KORELACJA EFEKTÓW UCZENIA SIĘ**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyki PRK*
W01	Ysq_W01, Ysq_W02, Ysq_W03, Ysq_W04, Ysq_U01, Ysq_U02, Ysq_K01	SIB2_W01, SIB2_U01, SIB2_U04, SIB2_K02,	P7U_W P7S_WG, P7U_U P7S_UW, P7U_U P7S_UK, P7U K P7S_KK
W02	Ysq_W01, Ysq_K01	SIB2_W01, SIB2_K02	P7U_W P7S_WG, P7U K P7S_KK
W03	Ysq_W01, Ysq_W02, Ysq_W03, Ysq_W04, Ysq_U01, Ysq_U02	SIB2_K02, SIB2_U01, SIB2_U04	P7U_W P7S_WG, P7U_U P7S_UW, P7U_U P7S_UK
W04	Ysq_W01, Ysq_W02, Ysq_W03, Ysq_W04, Ysq_U01, Ysq_U02	SIB2_K02, SIB2_U01, SIB2_U04	P7U_W P7S_WG, P7U_U P7S_UW, P7U_U P7S_UK
W05	Ysq_W01, Ysq_W02, Ysq_W03, Ysq_W04, Ysq_U01, Ysq_U02	SIB2_K02, SIB2_U01, SIB2_U04	P7U_W P7S_WG, P7U_U P7S_UW, P7U_U P7S_UK
W06	Ysq_W01, Ysq_W02, Ysq_W03, Ysq_W04, Ysq_U01, Ysq_U02	SIB2_K02, SIB2_U01, SIB2_U04	P7U_W P7S_WG, P7U_U P7S_UW, P7U_U P7S_UK
W07	Ysq_W01, Ysq_W02, Ysq_W03, Ysq_W04, Ysq_U01, Ysq_U02	SIB2_K02, SIB2_U01, SIB2_U04	P7U_W P7S_WG, P7U_U P7S_UW, P7U_U P7S_UK
W08	Ysq_W01, Ysq_W02, Ysq_W03, Ysq_W04, Ysq_U01, Ysq_U02	SIB2_K02, SIB2_U01, SIB2_U04	P7U_W P7S_WG, P7U_U P7S_UW, P7U_U P7S_UK
W09	Ysq_W01, Ysq_W02, Ysq_W03, Ysq_W04, Ysq_U01, Ysq_U02	SIB2_K02, SIB2_U01, SIB2_U04	P7U_W P7S_WG, P7U_U P7S_UW, P7U_U P7S_UK
W10	Ysq_W01, Ysq_W02, Ysq_W03, Ysq_W04, Ysq_U01, Ysq_U02	SIB2_K02, SIB2_U01, SIB2_U04	P7U_W P7S_WG, P7U_U P7S_UW, P7U_U P7S_UK
W11	Ysq_W01, Ysq_W02, Ysq_W03, Ysq_W04, Ysq_U01, Ysq_U02	SIB2_K02, SIB2_U01, SIB2_U04	P7U_W P7S_WG, P7U_U P7S_UW, P7U_U P7S_UK

W12	Ysq_W01, Ysq_W02, Ysq_W03, Ysq_W04, Ysq_U01, Ysq_U02	SIB2_K02, SIB2_U01, SIB2_U04	P7U_W P7S_WG, P7U_U P7S_UW, P7U_U P7S_UK
W13	Ysq_W01, Ysq_W02, Ysq_W03, Ysq_W04, Ysq_U01, Ysq_U02	SIB2_K02, SIB2_U01, SIB2_U04	P7U_W P7S_WG, P7U_U P7S_UW, P7U_U P7S_UK
W14	Ysq_W01, Ysq_W02, Ysq_W03, Ysq_W04, Ysq_U01, Ysq_U02	SIB2_K02, SIB2_U01, SIB2_U04	P7U_W P7S_WG, P7U_U P7S_UW, P7U_U P7S_UK
W15	Ysq_W01, Ysq_W02, Ysq_W03, Ysq_W04, Ysq_U01, Ysq_U02	SIB2_K02, SIB2_U01, SIB2_U04	P7U_W P7S_WG, P7U_U P7S_UW, P7U_U P7S_UK
W16	Ysq_W01, Ysq_W02, Ysq_W03, Ysq_W04, Ysq_U01, Ysq_U02, Ysq_K01	SIB2_K02, SIB2_U01, SIB2_U04, SIB2_K01	P7U_W P7S_WG, P7U_U P7S_UW, P7U_U P7S_UK, P7U K P7S_KK

V. NAKŁAD PRACY STUDENTA

Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**30**	**X**	**50**	**2**
Ćwiczenia				
Seminaria				
Konwersatoria				
Konsultacje (zaliczenie nieobecności, rozliczenie rygorów, poprawy)	**5**			
Przygotowanie do ćwiczeń	**X**			
Opanowanie informacji		**10**		
Przygotowanie do rozliczenia rygorów		**5**		
RAZEM	**35**	**15**		

VI. METODY DYDAKTYCZNE

1.	Wykład problemowy
2.	Prezentacja multimedialna

VII. FORMA ZALICZENIA PRZEDMIOTU

Rygor	*Kryteria składowe*	*Waga*
Zaliczenie	Test	1

VIII. LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

OBOWIĄZKOWA

1.	E. Haliżak, R. Kuźniar, *Stosunki międzynarodowe. Geneza, struktura, dynamika*, Warszawa 2006
2.	R. Jackson, G. Sorensen, *Wprowadzenie do stosunków międzynarodowych. Teorie i kierunki badawcze*, Kraków 2012
3.	K. Mingst, *Podstawy stosunków międzynarodowych*, Warszawa 2008

UZUPEŁNIAJĄCA

1.	P. Ostaszewski, *Międzynarodowe stosunki polityczne. Zarys wykładów*, Warszawa 2008
2.	J. Czaputowicz, *Teorie stosunków międzynarodowych. Krytyka i systematyzacja*, Warszawa 2008
3.	E. Cziomer, L. W. Zyblikiewicz, *Zarys współczesnych stosunków międzynarodowych*, Warszawa 2006
4.	S. Sur, *Stosunki Międzynarodowe*, Warszawa 2012

IX. PROWADZĄCY PRZEDMIOT

Stopień, Imię i nazwisko	dr hab. Bogusław GOGOL, prof. AMW; dr Iwona JAKIMOWICZ-PISARSKA
adres e-mail	b.gogol@amw.gdynia.pl; i.pisarska@amw.gdynia.pl

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:	**Podstawy bezpieczeństwa narodowego (pol./ang)**	*Kod*:	**Ybc**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Stacjonarne		
Kształcenie w zakresie:	Cyberbezpieczeństwo, Analiza danych i informatyka śledcza		
Profil:	Ogólnoakademicki		
Liczba ECTS:	3		
Semestr:	3		
Wymagania wstępne:	Podstawowa wiedza z teorii bezpieczeństwa		
Język wykładowy:	Polski		
Cel przedmiotu:	**C01**	Zapoznać się z terminologią dotyczącą relacji międzynarodowych	
	C02	Zapoznać się z terminologią dotyczącą bezpieczeństwa	
	C03	Nauczyć się metod analizy politologicznej kryzysów bezpieczeństwa na świecie	

II.	**EFEKTY UCZENIA SIĘ**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Ybc_W01**	Ma podstawową wiedzę o istocie systemu bezpieczeństwa narodowego	Test pisemny
	Ybc_W02	Zna strukturę systemu bezpieczeństwa	Test pisemny
Umiejętności:	**Ybc_U01**	Potrafi przedstawić kompetencje organów władzy i administracji publicznej w procesie kierowania bezpieczeństwem narodowym	Odpowiedź ustna
	Ybc_U02	Dostrzega problemy z zakresu bezpieczeństwa narodowego państwa	Odpowiedź ustna
	Ybc_U03	Posiada umiejętność rozumienia i analizowania różnorodnych zjawisk, związanych z bezpieczeństwem narodowym	Odpowiedź ustna
Kompetencje społeczne:	**Ybc_K01**	Rozumie potrzebę ciągłego diagnozowania stanu bezpieczeństwa narodowego	Odpowiedź ustna
	Ybc_K02	Potrafi rzeczowo argumentować stanowiska w zakresie bezpieczeństwa narodowego państwa	Odpowiedź ustna

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
W01	Zajęcia organizacyjne, prezentacja na temat współczesnych typów debaty	4
W02	Bezpieczeństwo narodowe – uwarunkowania i specyfika	8
W03	Bezpieczeństwo narodowe w perspektywie państw członkowskich Unii Europejskiej	4
W04	Bezpieczeństwo międzynarodowe	5
W05	Bezpieczeństwo narodowe Rzeczypospolitej Polskiej	8
W06	Kolokwium	1

IV.	**KORELACJA EFEKTÓW UCZENIA SIĘ**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyki PRK*
W01	Ybc_W01, Ybc_U01, Ybc_K01	SIB2_W01, SIB2_U01, SIB2_U07, SIB2_K02	P7U_W P7S_WG P7U_U P7S_UW

			P7U_U P7S_UU P7U_K P7S_KK
W02	Ybc_W01, Ybc_W02, Ybc_U02, Ybc_U03	SIB2_W01, SIB2_W03, , SIB2_U07, SIB2_U04	P7U_W P7S_WG P7U_W P7S_WK P7U_U P7S_UU P7U_U P7S_UK
W03	Ybc_W01, Ybc_W02, Ybc_U02, Ybc_U03, Ybc_K01, Ybc_K02	SIB2_W01, SIB2_W03, SIB2_U01, SIB2_U07, SIB2_U04	P7U_W P7S_WG P7U_W P7S_WK P7U_U P7S_UU P7U_U P7S_UK P7U_U P7S_UW
W04	Ybc_W01, Ybc_W02, Ybc_U02, Ybc_K01, Ybc_K02	SIB2_W01, SIB2_W03, SIB2_U01, SIB2_U07, SIB2_U04, SIB2_K02	P7U_W P7S_WG P7U_W P7S_WK P7U_U P7S_UU P7U_U P7S_UK P7U_U P7S_UW P7U_K P7S_KK
W05	Ybc_W01, Ybc_W02, Ybc_U01, Ybc_K01, Ybc_K02	SIB2_W01, SIB2_W03, SIB2_U01, SIB2_U07, SIB2_U04, SIB2_K02	P7U_W P7S_WG P7U_W P7S_WK P7U_U P7S_UU P7U_U P7S_UK P7U_U P7S_UW P7U_K P7S_KK
W06	-	-	-

V. NAKŁAD PRACY STUDENTA

Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**30**	**X**	**75**	**3**
Ćwiczenia				
Seminaria				
Konwersatoria				
Konsultacje (zaliczenie nieobecności, rozliczenie rygorów, poprawy)	**5**			
Przygotowanie do ćwiczeń	**X**			
Opanowanie informacji		**20**		
Przygotowanie do rozliczenia rygorów		**20**		
RAZEM	**35**	**40**		

VI. METODY DYDAKTYCZNE

1. Wykład z elementami konwersatorium
2. Wykład z elementami debaty

VII. FORMA ZALICZENIA PRZEDMIOTU

Rygor	*Kryteria składowe*	*Waga*
Zaliczenie	Kolokwium	0,7
	Obecność i aktywność na zajęciach	0,3

VIII. LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

OBOWIĄZKOWA

1. A. Ciupiński, K. Malak, *Bezpieczeństwo polityczne i wojskowe*, AON, Warszawa 2004
2. A. Wawrzusiszyn, *Bezpieczeństwo, Strategia, system. Teoria i praktyka w zarysie*, Warszawa 2015
3. R. Jakubczak , J. Flis, *Bezpieczeństwo narodowe Polski w XXI wieku. Wyzwania i strategie*, Bellona, Warszawa 2006
4. *Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej,* Warszawa 2013

UZUPEŁNIAJĄCA

1. W. Fehler (red.), *Współczesne bezpieczeństwo*, Wydawnictwo Naukowe Grado, Toruń 2005
2. J. Wojnarowski, *System obronności państwa: materiały do studiowania*, AON, Warszawa 2005
3. S. Koziej, *Między piekłem a rajem. Bezpieczeństwo u progu XXI wieku*, Wyd. Adam Marszałek, Toruń 2006

4.	R. Jakubczak (red.), *Podstawy bezpieczeństwa narodowego Polski w erze globalizacji*, AON, Warszawa 2008
IX.	**PROWADZĄCY PRZEDMIOT**
Stopień, Imię i nazwisko	dr hab. Krzysztof LIGĘZA, prof. AMW
adres e-mail	k.ligeza@amw.gdynia.pl

KARTA PRZEDMIOTU	AKADEMIA MARYNARKI WOJENNEJ WYDZIAŁ DOWODZENIA I OPERACJI MORSKICH	

I.	CHARAKTERYSTYKA PRZEDMIOTU		
Nazwa przedmiotu:	**Podstawy zarządzania i organizacji**	***Kod*:**	**Pko**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Stacjonarne		
Kształcenie w zakresie:	Cyberbezpieczeństwo, Analiza danych i informatyka śledcza		
Profil:	Ogólnoakademicki - wybieralny		
Liczba ECTS:	3		
Semestr:	3		
Wymagania wstępne:	Podstawowa wiedza z przedsiębiorczości		
Język wykładowy:	Polski		
Cel przedmiotu:	**C01**	Rozwinięcie umiejętności analizy otoczenia organizacji i podejmowania decyzji strategicznych.	
	C02	Zdobycie wiedzy na temat procesów zarządczych, takich jak planowanie, organizowanie, motywowanie i kontrolowanie.	
	C03	Zrozumienie podstawowych koncepcji i teorii związanych z organizacją i zarządzaniem.	
	C04	Zrozumienie roli przywództwa w zarządzaniu organizacją oraz rozwijanie umiejętności przywódczych.	
	C05	Nauka efektywnej komunikacji i pracy zespołowej w kontekście organizacyjnym.	
	C06	Zdobycie umiejętności zarządzania zmianą i adaptacji do dynamicznie zmieniającego się otoczenia biznesowego.	
	C07	Przygotowanie do ciągłego rozwoju osobistego i zawodowego w dziedzinie zarządzania.	

II.	EFEKTY UCZENIA SIĘ		
Zakres	***Kod***	***Opis efektu***	***Sposób oceny***
Wiedza:	**Pko_W01**	**Zrozumienie podstaw organizacji i zarządzania** - studenci będą mieli wiedzę na temat kluczowych pojęć, teorii i modeli związanych z zarządzaniem.	Kolokwium
	Pko_W02	**Wiedza o otoczeniu organizacji** - zrozumienie wpływu czynników zewnętrznych na działalność organizacji.	Kolokwium
	Pko_W03	**Znajomość teorii przywództwa** - studenci zdobędą wiedzę na temat różnych stylów przywództwa i ich zastosowania w praktyce.	Kolokwium
	Pko_W04	**Znajomość funkcji zarzadzania -** co to są funkcje kierowania oraz zna zasady ich stosowania; na czym polega planowanie, organizowanie, motywowanie i kontrolowanie oraz z jakich narzędzi organizatorskich korzystać, aby te funkcje efektywnie wypełniać; na czym polega podejmowanie decyzji oraz zna podstawowe etapy tego procesu.	Kolokwium

Umiejętności:	**Pko_U01**	**Umiejętność analizy otoczenia organizacyjnego -** studenci nauczą się oceniać wpływ otoczenia na decyzje organizacyjne.	Praca projektowa
	Pko_U02	**Umiejętność planowania i organizowania -** zdobędą umiejętności tworzenia celów, planowania działań i organizowania pracy.	Praca projektowa
	Pko_U03	**Umiejętność komunikacji i zarządzania zespołem -** studenci będą mogli efektywnie współpracować z innymi..	Praca projektowa
Kompetencje społeczne:	**Pko_K01**	**Komunikacja interpersonalna -** zdolność do efektywnej komunikacji z innymi członkami organizacji.	Obserwacja
	Pko_K02	**Praca zespołowa -** umiejętność współpracy, rozwiązywania konfliktów i osiągania wspólnych celów.	Obserwacja
	Pko_K03	**Zarządzanie sobą i innymi -** zdolność do motywowania siebie i innych, rozpoznawania potrzeb pracowników i tworzenia odpowiednich warunków pracy.	Obserwacja

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
W01	**Istota organizacji i zarządzania:** miejsce przedmiotu w systemie innych nauk, szkoły i prekursorzy nauki o zarządzaniu, definicja organizacji, definicja organizacji rzeczywistej i nierzeczywistej, dwunastoelementowy model organizacji Brukego i Litwina, definicja zarządzania, funkcje zarządzania, zasady zarządzania.	**2**
W02	**Otoczenie organizacji:** definicja otoczenia organizacji, wewnętrzne vs zewnętrzne otoczenie, analiza otoczenia – podstawy, interesariusze i ich wpływ na organizację, otoczenie technologiczne, otoczenie ekonomiczne, otoczenie kulturowe, otoczenie polityczno-prawne, otoczenie konkurencyjne, adaptacja organizacji do zmian w otoczeniu.	**2**
W03	**Przywództwo w organizacji:** podstawowe definicje, przywództwa, różnice między przywódcą a menedżerem, styl autokratyczny i demokratyczny, przywództwo przez przykład, komunikacja w przywództwie, motywowanie pracowników, delegowanie zadań, rozwój kompetencji przywódczych, przywództwo a kultura organizacyjna, przywództwo etyczne.	**2**
W04	**Praktyka zarządzania**: podstawy decydowania planowanie - pierwsze kroki, organizowanie pracy podstawy motywowania, kontrola jako element zarządzania zarządzanie czasem, zarządzanie konfliktem, zarządzanie zespołem, podstawy zarządzania projektami, zarządzanie zmianą.	**5**
W05	**Cele i strategia organizacji:** definicja i znaczenie celów, proces formułowania celów, misja i wizja organizacji, strategia - co to jest? poziomy strategii w organizacji, proces tworzenia strategii, analiza strategiczna, strategie	**2**

	konkurencyjne, implementacja strategii, ocena skuteczności strategii.	
W06	**Struktury organizacyjne:** definicja struktury organizacyjnej elementy struktury organizacyjnej, typy struktur organizacyjnych, struktura funkcjonalna, struktura dywizjonalna, struktura matrycowa, centralizacja vs decentralizacja, formalizacja w strukturze, koordynacja w strukturze, elastyczność struktury organizacyjnej.	**2**
W07	**Wymagania i indywidualne możliwości:**. definicja wymagań organizacyjnych, kompetencje pracowników, dopasowanie osoby do stanowiska, proces rekrutacji, selekcja kandydatów, szkolenia i rozwój pracowników, ocena pracownicza, kariera i ścieżki rozwoju, rola motywacji w pracy, zarządzanie talentami.	**2**
W08	**Kultura organizacyjna:** co to jest kultura organizacyjna? elementy kultury organizacyjnej, typy kultur organizacyjnych, rola liderów w kształtowaniu kultury, kultura a efektywność organizacji, zmiana kultury organizacyjnej, symbole i rytuały w kulturze, kultura a etyka w biznesie, kultura a innowacyjność, kultura a zarządzanie wiedzą.	**2**
W09	**Polityka i procedury:** definicja polityki organizacyjnej, rola procedur w organizacji, tworzenie polityk organizacyjnych, procedury operacyjne, procedury jakościowe, procedury bezpieczeństwa, dokumentacja procedur, audyt procedur, procedury a kultura organizacyjna, procedury a zarządzanie zmianą.	**2**
W10	**Indywidualne potrzeby i wartości:** podstawowe potrzeby pracowników, wartości w miejscu pracy, rola wartości w motywacji, zaspokajanie potrzeb w organizacji, różnice indywidualne, rola wartości w zarządzaniu, wartości a kultura organizacyjna, wartości a przywództwo, wartości a etyka pracy, wartości a satysfakcja z pracy.	**2**
W11	**Klimat w miejscu pracy:** Definicja klimatu organizacyjnego, Czynniki wpływające na klimat, Klimat a motywacja, Klimat a wydajność pracy, Klimat a satysfakcja z pracy, Klimat a zdrowie psychiczne, Klimat a komunikacja, Klimat a konflikty, Klimat a zarządzanie zmianą, Klimat a rozwój pracowników.	**2**
W12	**Motywacja wewnętrzna pracowników:** definicja motywacji wewnętrznej, teorie motywacji, motywacja a zaangażowanie, motywacja a wydajność, motywacja a satysfakcja, motywacja a cele osobiste, motywacja a rozwój zawodowy, motywacja a nagrody, motywacja a feedback, motywacja a środowisko pracy.	**2**
W13	**Indywidualne i organizacyjne wyniki pracy:** definicja wyników pracy, pomiar wyników pracy, wyniki a cele organizacji, wyniki a motywacja, wyniki a satysfakcja, wyniki a rozwój pracowników, wyniki a ocena pracownicza, wyniki a nagrody, wyniki a feedback, wyniki a zarządzanie zmianą.	**2**

W14	Zaliczenie: test jednokrotnego wyboru		**1**
IV.	**KORELACJA EFEKTÓW UCZENIA SIĘ**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyki PRK*
W01	Pko_W01; Pko_W02; Pko_W03; Pko_U01; Pko_U02; Pko_U03; Pko_K01; Pko_K02; Pko_K03.	SIB2_W01;SIB2_W02; SIB2_W03;SIB2_W04; SIB2_U01; SIB2_U02; SIB2_U03; SIB2_K01; SIB2_K02; SIB2_K03; SIB2_K04; SIB2_K05;	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK, P7S_KO, , P7S_KR
W02	Pko_W01; Pko_W02; Pko_U01; Pko_U02; Pko_K02.	SIB2_W01;SIB2_W02; SIB2_W03;SIB2_W04; SIB2_U01; SIB2_U02; SIB2_U03; SIB2_K01; SIB2_K02; SIB2_K03; SIB2_K04; SIB2_K05;	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK, P7S_KO, , P7S_KR
W03	Pko_W01; Pko_W02; Pko_W03; Pko_U01; Pko_U02; Pko_U03; Pko_K01; Pko_K02; Pko_K03.	SIB2_W01;SIB2_W02; SIB2_W03;SIB2_W04; SIB2_U01; SIB2_U02; SIB2_U03; SIB2_K01; SIB2_K02; SIB2_K03; SIB2_K04; SIB2_K05;	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK, P7S_KO, , P7S_KR
W04	Pko_W01; Pko_W02; Pko_W03; Pko_U01; Pko_U02; Pko_U03; Pko_K01; Pko_K02; Pko_K03.	SIB2_W01;SIB2_W02; SIB2_W03;SIB2_W04; SIB2_U01; SIB2_U02; SIB2_U03; SIB2_K01; SIB2_K02; SIB2_K03; SIB2_K04; SIB2_K05;	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK, P7S_KO, , P7S_KR
W05	Pko_W01; Pko_W02; Pko_W03; Pko_U01; Pko_U02; Pko_U03; Pko_K01; Pko_K03.	SIB2_W01;SIB2_W02; SIB2_W03;SIB2_W04; SIB2_U01; SIB2_U02; SIB2_U03; SIB2_K01; SIB2_K02; SIB2_K03; SIB2_K04; SIB2_K05;	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK, P7S_KO, , P7S_KR
W06	Pko_W01; Pko_W02; Pko_U01; Pko_U02;	SIB2_W01;SIB2_W02; SIB2_W03;SIB2_W04; SIB2_U01; SIB2_U02; SIB2_U03; SIB2_K01; SIB2_K02; SIB2_K03; SIB2_K04; SIB2_K05;	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK, P7S_KO, , P7S_KR
W07	Pko_W02; Pko_U01; Pko_U02; Pko_U03; Pko_K01; Pko_K02; Pko_K03	SIB2_W01;SIB2_W02; SIB2_W03;SIB2_W04; SIB2_U01; SIB2_U02; SIB2_U03; SIB2_K01; SIB2_K02; SIB2_K03; SIB2_K04; SIB2_K05;	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK, P7S_KO, , P7S_KR
W08	Pko_W01; Pko_W02; Pko_W03; Pko_U02; Pko_K01; Pko_K02; Pko_K03.	SIB2_W01;SIB2_W02; SIB2_W03;SIB2_W04; SIB2_U01; SIB2_U02; SIB2_U03; SIB2_K01; SIB2_K02; SIB2_K03; SIB2_K04; SIB2_K05;	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK, P7S_KO, , P7S_KR
W09	Pko_W01; Pko_W02; Pko_U01; Pko_U02;	SIB2_W01;SIB2_W02; SIB2_W03;SIB2_W04; SIB2_U01; SIB2_U02; SIB2_U03; SIB2_K01; SIB2_K02; SIB2_K03; SIB2_K04; SIB2_K05;	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK, P7S_KO, , P7S_KR

W10	Pko_W01; Pko_W02; Pko_W03; Pko_K01; Pko_K03.	SIB2_W01;SIB2_W02; SIB2_W03;SIB2_W04; SIB2_U01; SIB2_U02; SIB2_U03; SIB2_K01; SIB2_K02; SIB2_K03; SIB2_K04; SIB2_K05;	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK, P7S_KO, , P7S_KR
W11	Pko_W03; Pko_U01; Pko_U02; Pko_U03; Pko_K01; Pko_K02; Pko_K03.	SIB2_W01;SIB2_W02; SIB2_W03;SIB2_W04; SIB2_U01; SIB2_U02; SIB2_U03; SIB2_K01; SIB2_K02; SIB2_K03; SIB2_K04; SIB2_K05;	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK, P7S_KO, , P7S_KR
W12	Pko_W01; Pko_W02; Pko_U02; Pko_U03; Pko_K01; Pko_K02; Pko_K03.	SIB2_W01;SIB2_W02; SIB2_W03;SIB2_W04; SIB2_U01; SIB2_U02; SIB2_U03; SIB2_K01; SIB2_K02; SIB2_K03; SIB2_K04; SIB2_K05;	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK, P7S_KO, , P7S_KR
W13	Pko_W01; Pko_W02; Pko_W03; Pko_U02; Pko_U03; Pko_K01; Pko_K02; Pko_K03.	SIB2_W01;SIB2_W02; SIB2_W03;SIB2_W04; SIB2_U01; SIB2_U02; SIB2_U03; SIB2_K01; SIB2_K02; SIB2_K03; SIB2_K04; SIB2_K05;	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK, P7S_KO, , P7S_KR

V. NAKŁAD PRACY STUDENTA

Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin Nie kontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**30**		**75**	**3**
Ćwiczenia				
Seminarium				
Konwersatoria				
Konsultacje (zaliczenie nieobecności, rozliczenie rygorów, poprawy)	**5**			
Praca projektowa	**X**			
Opanowanie informacji		**20**		
Przygotowanie do rozliczenia		**20**		
RAZEM	**35**	**40**		

VI. METODY I NARZĘDZIA DYDAKTYCZNE

- wykład;
- prezentacja multimedialna;
- case study;
- dyskusja.

VII. FORMA ZALICZENIA PRZEDMIOTU

Rygor	***Kryteria składowe***	***Waga***
Zaliczenie	Ocena z kolokwium - warunek konieczny	0,7
	Zaliczenie pracy projektowej - warunek istotny	0,2
	Obserwacja - warunek istotny	0,1

VIII. LITERATURA

OBOWIĄZKOWA

1. R. W. Gryffin, Podstawy zarządzania organizacjami, PWN, Warszawa, 2004.
2. A. J. Blikle, Doktryna jakości. Rzecz o skutecznym zarządzaniu, Helion, Warszawa, 2013.
3. A. J. Blikle, Doktryna jakości. Rzecz o turkusowej samoorganizacji, Helion, Warszawa, 2018.

UZUPEŁNIAJĄCA

1. M. Ćwiklicki, Hubert Obora, *Metody TQM w zarządzaniu firmą, praktyczne przykłady zastosowań*, Poltext, Warszawa, 2009.

2.	J. Stoner, E. Freeman, D. Gilbert, *Kierowanie*, PWE, Warszawa, 2014.
3.	Cz. Flanek, *Elementy teorii podejmowania decyzji*, CSOPK, Koszalin, 2000.
4.	A. Koźmiński, W. Piotrowski, *Zarządzanie, teoria i praktyka*, PWN, Warszawa, 1990
IX.	**PROWADZĄCY PRZEDMIOT**
Stopień, Imię i nazwisko	dr Jerzy KUPIŃSKI
adres email	j.kupinski@amw.gdynia.pl

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:	**Podstawy filozofii i logiki****	*Kod*:	**Itn**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Stacjonarne		
Kształcenie w zakresie:	Cyberbezpieczeństwo, Analiza danych i informatyka śledcza		
Profil:	Ogólnoakademicki		
Liczba ECTS:	3		
Semestr:	3		
Wymagania wstępne:	Brak		
Język wykładowy:	Polski		
Cel przedmiotu:	**C01**	Zaznajomienie z podstawowymi pojęciami z zakresu filozofii oraz logiki.	
	C02	Przedstawienie głównych problemów filozoficznych oraz sposobów ich rozstrzygania.	
	C03	Charakterystyka języka naturalnego oraz głównych rodzajów i reguł rozumowania; ich wykorzystanie w nauce, w procesie komunikacji oraz w konstruowaniu własnej wizji świata.	
	C04	Wyjaśnienie najważniejszych praw logicznych oraz zasad budowania poprawnych definicji.	

II.	**EFEKTY UCZENIA SIĘ**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Itn_W01**	Student wyjaśnia najważniejsze pojęcia i zagadnienia z dziedziny filozofii oraz logiki; przedstawia rolę i znaczenie tych dyscyplin w procesie poznania i opisu rzeczywistości; wskazuje ich powiązania z innymi dziedzinami.	kolokwium
	Itn_W02	Student charakteryzuje różne koncepcje prawdy, rolę języka w procesie myślenia, sposoby definiowania pojęć, rodzaje rozumowań oraz podstawowe prawa logiczne; dostrzega ich przydatność w procesie badawczym.	kolokwium
Umiejętności:	**Itn_U01**	Student odwołuje się do ustaleń epistemologii oraz zaleceń logiki dla zapewnienia skutecznego myślenia i komunikowania się; unika błędów logicznych w rozumowaniach.	kolokwium
	Itn_U02	Student analizuje poprawność pojęć, sądów i wnioskowań oraz ocenia prawdziwość zdań na podstawie ich struktury logicznej.	kolokwium
Kompetencje społeczne:	**Itn_K01**	Student wykazuje samodzielność i niezależność w postrzeganiu rzeczywistości oraz krytycyzm w interpretowaniu odbieranych treści.	obserwacja na zajęciach

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
W01	Zajęcia wprowadzające. Specyfika myślenia filozoficznego.	2

W02	Przedmiot, struktura i dziedziny filozofii oraz jej relacje do nauki i religii.	2
W03	Najważniejsze zagadnienia i kierunki filozoficzne.	2
W04	Główne etapy rozwoju myśli filozoficznej.	4
W05	Koncepcje poznania oraz prawdziwości wiedzy w ujęciu wybranych nurtów filozoficznych.	2
W06	Przedmiot, działy oraz funkcje logiki; logika jako dziedzina filozofii.	2
W07	Język jako narzędzie myślenia; jego rola w procesie poznawania i opisu rzeczywistości oraz w komunikacji międzyludzkiej.	2
W08	Semantyczna teoria definicji. Błędy definicji sprawozdawczych.	2
W09	Podstawowe rodzaje rozumowań – dedukcja, redukcja, indukcja.	2
W10	Błędy w rozumowaniach – błąd formalny i błąd materialny.	2
W11	Założenia klasycznego rachunku zdań.	2
W12	Wybrane prawa logiczne. Sprawdzanie niezawodności rozumowań.	4
W13	Przyczyny nieporozumień o charakterze logicznym.	2

IV.	**KORELACJA EFEKTÓW UCZENIA SIĘ**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyki PRK*
W01	Itn_W01	SIB2_W01	P7U_W P7S_WG
W02	Itn_W01	SIB2_W01	P7U_W P7S_WG
W03	Itn_W01	SIB2_W01	P7U_W P7S_WG
W04	Itn_W01	SIB2_W01	P7U_W P7S_WG
W05	Itn_W01; Itn_K01	SIB2_W01; SIB2_K01	P7U_W P7S_WG; P7U_K P7S_KK
W06	Itn_W01	SIB2_W01	P7U_W P7S_WG
W07	Itn_W02; Itn_K01	SIB2_W01; SIB2_K01	P7U_W P7S_WG; P7U_K P7S_KK
W08	Itn_W02	SIB2_W01	P7U_W P7S_WG
W09	Itn_W02; Itn_U02	SIB2_W01; SIB2_U02	P7U_W P7S_WG; P7U_U P7S_UW
W10	Itn_U01	SIB2_U01	P7U_U P7S_UW
W11	Itn_U02	SIB2_U01	P7U_U P7S_UW
W12	Itn_W02; Itn_U02	SIB2_W01; SIB2_U01	P7U_W P7S_WG; P7U_U P7S_UW
W13	Itn_U01	SIB2_U01	P7U_U P7S_UW

V.	**NAKŁAD PRACY STUDENTA**			
Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**30**	**X**	**75**	**3**
Ćwiczenia				
Seminaria				
Konwersatoria				
Konsultacje (zaliczenie nieobecności, rozliczenie rygorów, poprawy)	**5**			
Przygotowanie do ćwiczeń	**X**			
Opanowanie informacji		**20**		
Przygotowanie do rozliczenia rygorów		**20**		
RAZEM	**35**	**40**		

VI.	**METODY DYDAKTYCZNE**
1.	Wykład: prezentacje multimedialne
2.	Konsultacje, sprawdzanie wiedzy i umiejętności: testy, zadania
VII.	**FORMA ZALICZENIA PRZEDMIOTU**

Rygor	*Kryteria składowe*	*Waga*
Zaliczenie	Ocena z kolokwium	0,8
	Obowiązkowa obecność na wykładach – 80%	0,2

VIII.	**LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA**
	OBOWIĄZKOWA
1.	Hempoliński M., *Filozofia współczesna. Wprowadzenie do zagadnień i kierunków*, Warszawa 1989.
2.	Popkin R.H., *Historia filozofii zachodniej*, Poznań 2003.
3.	Przybyłowski J., *Logika z ogólną metodologią nauk*, Gdańsk 1999.
4.	Ziembiński Z., *Logika praktyczna*, Warszawa 2007.
	UZUPEŁNIAJĄCA
1.	Bocheński J.M., *Zarys historii filozofii*, Kraków 1993.
2.	Hołówka T., *Kultura logiczna w przykładach*, Warszawa 2005.
3.	Kraszewski Z., *Logika. Nauka rozumowania*, Warszawa 1981.
4.	Tatarkiewicz W., *Historia filozofii, t. 1-3*, Warszawa 1990.

IX.	**PROWADZĄCY PRZEDMIOT**
Stopień, Imię i nazwisko	dr Wincenty KARAWAJCZYK
adres e-mail	w.karawajczyk@amw.gdynia.pl

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:	**Podstawy pedagogiki**	*Kod*:	**Ped**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Stacjonarne		
Kształcenie w zakresie:	Cyberbezpieczeństwo, Analiza danych i informatyka śledcza		
Profil:	Ogólnoakademicki		
Liczba ECTS:	3		
Semestr:	3		
Wymagania wstępne:	Brak		
Język wykładowy:	Polski		
Cel przedmiotu:	**C01**	Zapoznanie studentów z podstawowymi kategoriami pedagogicznymi i procesami edukacyjnymi	
	C02	Ukazanie sposobów współczesnych rozwiązań praktycznych w zakresie kształcenia, opieki i wychowania oraz ich historycznych korzeni	
	C03	Wyposażenie w umiejętności i kompetencje niezbędne w procesie kształtowania własnej drogi edukacyjnej	

II.	**EFEKTY UCZENIA SIĘ**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Ped_W01**	Zna podstawowe pojęcia, kategorie i wybrane koncepcje pedagogiczne	Kolokwium
	Ped_W02	Rozumie historyczne,-społeczne i polityczne uwarunkowania rozwoju praktyki pedagogicznej	Kolokwium
	Ped_W03	Zna współczesne rozwiązania w zakresie kształcenia, uczenia się, opieki i wychowania	Kolokwium
Umiejętności:	**Ped_U01**	Potrafi interpretować podstawową wiedzę z zakresu pedagogiki/edukacji w kontekście własnego uczenia się i rozwoju	Kolokwium, bieżąca ocena aktywności
	Ped_U02	Analizuje i ocenia praktyczne skutki współczesnych idei i koncepcji pedagogicznych	Kolokwium, bieżąca ocena aktywności
Kompetencje społeczne:	**Ped_K01**	Jest gotów do brania odpowiedzialności za własne uczenie się i podejmowanie różnych form praktycznej działalności edukacyjnej, opiekuńczej i wychowawczej wobec innych	Kolokwium, bieżąca ocena aktywności

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
W01	Zajęcia wprowadzające. Podstawowe pojęcia pedagogiczne.	3
W02	Etymologia pedagogiki. Pedagogika jako nauka o wychowaniu	3
W03	Rodzina i grupy rówieśnicze	5

W04	Szkoła i nauczyciel	3
W05	Filozoficzne, społeczno-historyczne uwarunkowania współczesnych rozwiązań pedagogicznych	3
W06	Systemy edukacyjne wybranych państw świata	4
W07	Uczelnia wyższa jako środowisko uczenia się dawniej i dziś	3
W08	Najważniejsze wyzwania współczesnej teorii i praktyki pedagogicznej	3
W09	Zajęcia podsumowujące. Kolokwium	3

IV.	**KORELACJA EFEKTÓW UCZENIA SIĘ**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod efektu PRK*
W01	Ped_W01, Ped_W03	SIB2_W01, SIB2_K02	P7U_W P7S_WG, P7U_K P7S_KK
W02	Ped_W01, Ped_W03, Ped_U02	SIB2_W01, SIB2_K02	P7U_W P7S_WG P7U_K P7S_KK
W03	Ped_W02, Ped_W03	SIB2_W01, SIB2_K02	P7U_W P7S_WG P7U_K P7S_KK
W04	Ped_W02, Ped_W03, Ped_U01, Ped_U02, Ped_K01	SIB2_W01, SIB2_U03, SIB2_U06, SIB2_K02, SIB2_K03, SIB2_K04	P7U_W P7S_WG P7U_U P7S_UK P7U_U P7S_UO P7U_K P7S_KK P7U_K P7S_KO P7U_K P7S_KR
W05	Ped_W01, Ped_W02, Ped_W03, Ped_U01, Ped_U02, Ped_K01	SIB2_W01, SIB2_U01, SIB2_U06, SIB2_U07, SIB2_K02	P7U_W P7S_WG P7U_U P7S_UW P7U_U P7U_UO P7U_U P7U_UU P7U_K P7S_KK
W06	Ped_W03, Ped_U01, Ped_U02	SIB2_W01, SIB2_U01, SIB2_U02	P7U_W P7S_WG P7U_U P7S_UW
W07	Ped_W01, Ped_W02, Ped_W03, Ped_U01, Ped_U02, Ped_K01	SIB2_W01, SIB2_U01 SIB2_U07, SIB2_K02	P7U_W P7S_WG P7U_U P7S_UW P7U_U P7U_UU P7U_K P7S_KK
W08	Ped_W02, Ped_U01, Ped_U02, Ped_K01	SIB2_W01, SIB2_U07, SIB2_K02	P7U_W P7S_WG P7U_U P7S_UU P7U_K P7S_KK
W09	Ped_W01, Ped_W02, Ped_W03, Ped_U01, Ped_U02, Ped_K01	SIB2_W01, SIB2_U01, SIB2_U07, SIB2_K02	P7U_W P7S_WG P7U_U P7U_UW P7U_U P7S_UU P7U_K P7S_KK

V.	**NAKŁAD PRACY STUDENTA**			
Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**30**	**X**	**75**	**3**
Ćwiczenia				
Seminaria				
Konwersatoria				
Konsultacje (zaliczenie nieobecności, rozliczenie rygorów, poprawy)	**5**			
Przygotowanie do ćwiczeń	**X**			
Opanowanie informacji		**20**		
Przygotowanie do rozliczenia rygorów		**20**		
RAZEM	**35**	**40**		

VI.	METODY DYDAKTYCZNE
1.	Wykład konwersatoryjny
2.	Wykład z wykorzystaniem multimediów
3.	Analiza tekstów źródłowych

VII. FORMA ZALICZENIA PRZEDMIOTU		
Rygor	*Kryteria składowe*	*Waga*
Zaliczenie	Kolokwium	0.75
	Obecność i aktywny udział w dyskusjach	0.25

VIII.	LIFIERATURA PODSTAWOWA I UZUPEŁNIAJĄCA
	OBOWIĄZKOWA
1.	HEJNICKA-BEZWIŃSKA T.: Pedagogika ogólna. Pedagogika wobec współczesności. Warszawa 2008.
2.	KWIECIŃSKI Z., ŚLIWERSKI B. (red.): Pedagogika. Podręcznik akademicki. Warszawa 2019.
3.	BARTNICKA K., SZYBIAK I.: Zarys historii wychowania. Warszawa 2001.
	UZUPEŁNIAJĄCA
1.	PRůCHA J.: Pedagogika porównawcza. Podręcznik akademicki. Warszawa 2006.
2.	GUTEK G.L.: Filozoficzne i ideologiczne podstawy edukacji. Gdańsk 2003.
3.	Wybrane artykuły z czasopism: „Colloquium", „Problemy Opiekuńczo-Wychowawcze", „Rocznik Andragogiczny".

IX.	PROWADZĄCY PRZEDMIOT
Stopień, Imię i nazwisko	dr hab. Elżbieta GAWEŁ-LUTY, prof. AMW
adres e-mail	e.luty@amw.gdynia.pl

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:	**Historia techniki**	*Kod*:	**Hta**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Stacjonarne		
Kształcenie w zakresie:	Cyberbezpieczeństwo, Analiza danych i informatyka śledcza		
Profil:	Ogólnoakademicki		
Liczba ECTS:	3		
Semestr:	3		
Wymagania wstępne:	Umiejętność obserwowania i interpretacji zjawisk historycznych, kulturowych i społecznych, odpowiedzialne przygotowanie się do swojej pracy		
Język wykładowy:	Polski		
Cel przedmiotu:	**C01**	Wyposażenie studentów w wiedzę dotyczącą funkcjonowania instytucji zajmujących się techniką i jej historią	
	C02	Nabycie umiejętności analizowania i projektowania działań praktycznych w powiązaniu z historią techniki	
	C03	Zapoznanie studentów z wiedzą niezbędną do rozumienia społecznych uwarunkowań działalności człowieka	

II.	**EFEKTY UCZENIA SIĘ**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Hta_W01**	Student ma niezbędną wiedzę do rozumienia pozatechnicznych, kulturowo-społecznych uwarunkowań działalności człowieka	Kolokwium
Umiejętności:	**Hta_U01**	Student potrafi pozyskiwać i integrować informacje pozyskane z literatury przedmiotu, baz danych oraz innych źródeł, potrafi dokonywać ich interpretacji i właściwej oceny w celu określenia ich znaczeń oddziaływania społecznego i miejsca w procesie historyczno-kulturowym	Kolokwium/ Odpowiedź ustna
Kompetencje społeczne:	**Hta_K01**	Student ma świadomość ważności i rozumie pozatechniczne aspekty i skutki działalności człowieka, w tym wpływu jej na środowisko społeczno-kulturowe i związanej z tym odpowiedzialności za podejmowane decyzje	Odpowiedź ustna

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
W01	Wprowadzenie. Ogólna historia techniki /od drewnianej do murowanej/	2
W02	Historia fortyfikacji i budownictwa obronnego	2
W03	Historia żeglugi światowej	4
W04	Historia techniki nawigacyjnej i nurkowej	4
W05	Historia żeglarstwa	2
W06	Polski udział w rozwoju techniki	2
W07	Technika w marynarce wojennej	4

W08	Rola polskich stoczni w rozwoju techniki morskiej	4
W09	Muzealnictwo morskie a historia techniki morskiej	4
W10	Kolokwium zaliczeniowe	2

IV.	**KORELACJA EFEKTÓW UCZENIA SIĘ**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyki PRK*
W01	Hta_W01	SIB2_W01	P7U_W P7S_WG
W02	Hta_W01, Hta_U01	SIB2_W01, SIB2_U01	P7U_W P7S_WG P7U_U P7S_UW
W03	Hta_W01, Hta_U01	SIB2_W01, SIB2_U01	P7U_W P7S_WG P7U_U P7S_UW
W04	Hta_W01, Hta_U01, Yo_K01	SIB2_W01, SIB2_U01, SIB2_K02	P7U_W P7S_WG P7U_U P7S_UW P7U_K P7S_KK
W05	Hta_W01, Hta_U01, Hta_K01	SIB2_W01, SIB2_U01, SIB2_K02	P7U_W P7S_WG P7U_U P7S_UW P7U_K P7S_KK
W06	Hta_W01, Hta_U01, Hta_K01	SIB2_W01, SIB2_U01, SIB2_K02	P7U_W P7S_WG P7U_U P7S_UW P7U_K P7S_KK
W07	Hta_W01, Hta_U01, Hta_K01	SIB2_W01, SIB2_U01, SIB2_K02	P7U_W P7S_WG P7U_U P7S_UW P7U_K P7S_KK
W08	Hta_W01, Hta_U01, Yo_K01	SIB2_W01, SIB2_U01, SIB2_K02	P7U_W P7S_WG P7U_U P7S_UW P7U_K P7S_KK
W09	Hta_W01, Hta_U01, Yo_K01	SIB2_W01, SIB2_U01, SIB2_K02	P7U_W P7S_WG P7U_U P7S_UW P7U_K P7S_KK
W10	Hta_W01, Hta_U01, Hta_K01	SIB2_W01, SIB2_U01, SIB2_K02	P7U_W P7S_WG P7U_U P7S_UW P7U_K P7S_KK

V.	**NAKŁAD PRACY STUDENTA**			
Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**30**	**X**	**75**	**3**
Ćwiczenia				
Seminaria				
Konwersatoria				
Konsultacje (zaliczenie nieobecności, rozliczenie rygorów, poprawy)	**5**			
Przygotowanie do ćwiczeń	**X**			
Opanowanie informacji		**20**		
Przygotowanie do rozliczenia rygorów		**20**		
RAZEM	**35**	**40**		

VI.	**METODY DYDAKTYCZNE**
1.	Wykład problemowy
2.	Wykład informacyjny
3.	Wykład z prezentacją multimedialną

VII.	**FORMA ZALICZENIA PRZEDMIOTU**	
Rygor	*Kryteria składowe*	*Waga*
Zaliczenie	Ocena z kolokwium zaliczeniowego	1,0

VIII.	**LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA**
	OBOWIĄZKOWA
1.	A. Komorowski, *Historia techniki nawigacyjnej,* AMW Gdynia 1999.
2.	A. Komorowski, *Historia techniki nurkowej,* Torun 2005.

UZUPEŁNIAJĄCA	
1.	B. Orłowski, *Historia techniki polskiej*, Radom 2008.
IX.	**PROWADZĄCY PRZEDMIOT**
Stopień, Imię i nazwisko	dr Mariusz KARDAS
adres e-mail	m.kardas@amw.gdynia.pl

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:	**Ochrona ludności i obrona cywilna**	*Kod*:	**Fc**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Stacjonarne		
Kształcenie w zakresie:	Cyberbezpieczeństwo, Analiza danych i informatyka śledcza		
Profil:	Ogólnoakademicki		
Liczba ECTS:	4		
Semestr:	3		
Wymagania wstępne:			
Język wykładowy:	Polski		
Cel przedmiotu:	**C01**	Zapoznanie z uwarunkowaniami prawnymi w zakresie ochrony ludności i Obrony Cywilnej w Polsce	
	C02	Zapoznanie z krajowymi systemami ochrony ludności	
	C03	Zapoznanie z podstawowymi zasadami funkcjonowania obrony cywilnej w czasie konfliktów zbrojnych	
	C04	Ukształtowanie prawidłowych reakcji w przypadku wystąpienia zagrożenia	

II.	**EFEKTY UCZENIA SIĘ**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Fc_W01**	Zna i interpretuje przepisy prawa regulujące funkcjonowanie obrony cywilnej w Polsce	Kolokwium
	Fc_W02	Wyjaśnia szczegółowo miejsce, znaczenie i rolę obrony cywilnej	Test sprawdzający podczas zajęć, krótka praca domowa
	Fc_W03	Szczegółowo zna zadania obrony cywilnej w zakresie przeciwdziałania stanom zagrożenia zdrowia i życia.	Praca pisemna podczas zajęć
Umiejętności:	**Fc_U01**	Posiada umiejętność rozumienia i analizowania różnorodnych zjawisk, mających wpływ na bezpieczeństwo obywateli	Kolokwium
	Fc_U02	Dostrzega problemy z obrony cywilnej oraz składa propozycje ich rozstrzygnięć oraz stosuje argumentację własnego stanowiska	Praca pisemna podczas zajęć
	Fc_U03	Interpretuje i prognozuje rozwój zjawisk społecznych, ekonomicznych, politycznych, prawnych i kulturowych wywołanych konfliktem zbrojnym	Kolokwium
Kompetencje społeczne:	**Fc_K01**	Priorytetyzuje zadnia określone przez siebie lub innych oraz posługuje się harmonogramem ich uporządkowanej realizacji	Wykonanie projektu
	Fc_K02	Inicjuje i moderuje pracę w grupie, przyjmując w niej różne role, potrafi podporządkować się	Odpowiedź tablicowa

		celom grupy, ale także przyjmować funkcje lidera zadaniowego	
	Fc_K03	Samodzielnie uzupełnia i doskonali nabytą wiedzę i umiejętności, potrafi ocenić ofertę kształcenia kursowego i podyplomowego	Krótka praca domowa

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
W01	Prawne uwarunkowania funkcjonowania obrony cywilnej w Polsce	2
W02	Instytucje odpowiedzialne za obronę cywilną w Polsce	4
W03	Charakterystyka zadań obrony cywilnej oraz zasady ich realizacji w czasie pokoju i podczas wojny	6
W04	Organizacja powszechnego systemu ochrony ludności	4
W05	Zasady ochrony ludności wynikające z zagrożeń czasu wojny, krajowy system wykrywania skażeń i alarmowania	4
C01	Zadania i kompetencje organów administracji publicznej oraz służb, inspekcji i straży w zakresie ochrony ludności i obrony cywilnej	4
C02	Prawa i obowiązki obywateli w zakresie obrony cywilnej i ochrony ludności, świadczenia na rzecz obrony	6
C03	Organizacja i prowadzenie akcji ratunkowej, udzielanie pomocy medycznej poszkodowanym, ewakuacja	8
C04	Pomoc w ratowaniu żywności i innych dóbr niezbędnych do przetrwania	4
C05	Zasady reagowania na sygnały alarmowe, ochrona przed zagrożeniami	8

IV.	**KORELACJA EFEKTÓW UCZENIA SIĘ**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyki PRK*
W01	Fc_W01, Fc_U04	SIB2_W03, SIB2_U07	P7U_W, P7S _WK, P7U_U; P7S_UU
W02	Fc_W02	SIB2_W02	P7U_W; P7S_WK
W03	Fc_W01, Fc_W03	SIB2_W02, SIB2_W03	P7U_W, P7S _WK,
W04	Fc_W01, Fc_W02, Fc_W03	SIB2_W02, SIB2_W03	P7U_W, P7S _WK,
W05	Fc_W03, Fc_U06	SIB2_W03, SIB2_U01	P7U_W; P7S_WK, P7U_U; P7S_UW
C01	Fc_W01, Fc_W02, Fc_K09	SIB2_W03, SIB2_W01, SIB2_K03	P7U_W, P7S _WK, P7U_W, P7S _WG; P7U_K; P7S_KO
C02	Fc_W01, Fc_W02,Fc_K08	SIB2_W03, SIB2_U07	P7U_W; P7S_WK, P7U_U; P7S_UU
C03	Fc_W03, Fc_W05, Fc_U07	SIB2_W02, SIB2_U07	P7U_W; P7S_WK, P7U_U; P7S_UU
C04	Fc_W03, Fc_U05,Fc_U06	SIB2_W03, SIB2_U07	P7U_W; P7S_WK, P7U_U; P7S_UU
C05	Fc_W03, Fc_K07	SIB2_W02, SIB2_U07	P7U_W; P7S_WK, P7U_U; P7S_UU

V.	**NAKŁAD PRACY STUDENTA**			
Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**20**	**X**	**106**	**4**
Ćwiczenia	**30**			
Seminaria				
Konwersatoria				
Konsultacje (zaliczenie nieobecności, rozliczenie rygorów, poprawy)	**6**			

Przygotowanie do ćwiczeń		**20**		
Opanowanie informacji	**X**	**20**		
Przygotowanie do rozliczenia rygorów		**10**		
RAZEM	**56**	**50**		

VI.	**METODY DYDAKTYCZNE**
1.	Wykład z prezentacją multimedialną
2.	Ćwiczenia audytoryjne: projekt praktyczny
3.	Ćwiczenia audytoryjne: praca w grupach

VII.	**FORMA ZALICZENIA PRZEDMIOTU**	
Rygor	*Kryteria składowe*	*Waga*
Zaliczenie	Kolokwium	50%
	Wykonanie projektów	35%
	Oceny z krótkich prac pisemnych	10%
	Ocena z krótkich prac domowych	5%
Egzamin	Zaliczenie testu	100%

VIII.	**LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA**
	OBOWIĄZKOWA
1.	R. Jakubczak, A. Skrabacz, K. Gąsiorek (red.), *Obrona Narodowa w tworzeniu bezpieczeństwa Polski w XXI wieku*, Warszawa 2008
2.	K. Przeworski, *Ewakuacja jako sposób ochrony ludności*, Warszawa 2002
3.	*Rozporządzenie Rady Ministrów z dnia 25 czerwca 2002 r. w sprawie szczegółowego zakresu działania Szefa Obrony Cywilnej Kraju, szefów obrony cywilnej województw, powiatów i gmin*. (Dz. U. z dnia 1 lipca 2002 r. z późniejszymi zmianami)
4.	W. Kitler, A. Skrabacz, *Bezpieczeństwo ludności cywilnej. Pojęcie, organizacja i zadania w czasie pokoju, kryzysu i wojny*, Warszawa 2010
	UZUPEŁNIAJĄCA
1.	M. Fleming, *Międzynarodowe prawo humanitarne konfliktów zbrojnych*. Zbiór dokumentów, (M. Gąska, E. Mikos – Skuza uzupełnienie i redakcja), Warszawa 2003
2.	W. Kitler (red.), *Obrona Cywilna (niemilitarna) w obronie narodowej III RP*, Warszawa 2001
3.	W. Skomra, *Zarządzanie kryzysowe – praktyczny przewodnik po nowelizacji ustawy*, Wrocław 2010
4.	G. Abgarowicz, *Kierowanie obroną cywilną*, (w:) Zdrodowski B., Wiśniewski B., red., Kierowanie Bezpieczeństwem Narodowym, Warszawa 2008
5.	R. Kalinowski, *Obrona cywilna w Polsce*. Siedlce 2009
6.	W. Kitler, A. Skrabacz, *Bezpieczeństwo ludności cywilnej. Pojęcie, organizacja i zadania w czasie pokoju, kryzysu i wojny*, Warszawa 2010

IX.	**PROWADZĄCY PRZEDMIOT**
Stopień, Imię i nazwisko	dr hab. Jarosław MICHALAK, prof. AMW; mgr Krzysztof BLUMKA
adres e-mail	j.michalak@amw.gdynia.pl, k.blumka@amw.gdynia.pl

3.2. Karty przedmiotów modułu zajęć kierunkowych studiów stacjonarnych– B

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 Systemami Bezpieczeństwa Wewnętrznego**	*Kod*:	**Zog**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Stacjonarne		
Specjalność:	Cyberbezpieczeństwo, Analiza danych i informatyka śledcza		
Profil:	Ogólnoakademicki		
Liczba ECTS:	5		
Semestr:	1		
Wymagania wstępne:	Umiejętność pracy samodzielnej oraz w grupie.		
	Umiejętności zdobywania, pogłębiania i wykorzystania wiedzy w procesie studiowania.		
	Umiejętności komunikacji interpersonalnej.		
Język wykładowy:	Polski		
Cel przedmiotu: **C01**	Przekazanie wiedzy z zakresu zarządzania systemami bezpieczeństwa wewnętrznego państwa w kontekście ideologicznym, kulturowym, socjologicznym i psychologicznym.		
Cel przedmiotu: **C02**	Wyrobienie umiejętności identyfikowania, analizy i prognozowania zagrożeń dla systemu bezpieczeństwa wewnętrznego państwa.		
Cel przedmiotu: **C03**	Wyrobienie u studentów unikalnej umiejętności całościowego spojrzenia na procesy organizacyjne, mechanizmy nimi rządzące oraz wzajemne powiązania w czasie zarządzania systemami bezpieczeństwa wewnętrznego.		
Cel przedmiotu: **C04**	Przygotowanie studentów do zastosowania zdobytej wiedzy z zakresu zarządzania systemami bezpieczeństwa wewnętrznego państwa w czasie wykonywania zadań służbowych.		

II.	**EFEKTY KSZTAŁCENIA**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Zog_01**	Zna instrumentarium pojęciowe z zakresu zarządzania systemami bezpieczeństwa wewnętrznego.	Kolokwium
	Zog_02	Zna zasady i mechanizmy działania elementów systemu bezpieczeństwa wewnętrznego państwa. Posiada rozszerzoną wiedzę z zakresu zarządzania systemami bezpieczeństwa wewnętrznego. Zna i interpretuje relacje występujące w systemie bezpieczeństwa wewnętrznego państwa oraz ich związek z bezpieczeństwem narodowym.	Test sprawdzający podczas zajęć, krótka praca domowa
	Zog_03	Posiada wiedzę na temat realizacji procesu oraz metod wykorzystywanych podczas szacowania ryzyka, identyfikacji zagrożeń, określania podatności i wymagań dotyczących systemu bezpieczeństwa wewnętrznego państwa.	Praca pisemna podczas zajęć

	Zog_04	Posiada wiedzę o podstawowych koncepcjach i metodach funkcjonowania gminnych, powiatowych i wojewódzkich systemów bezpieczeństwa oraz zarządzania tymi strukturami a także stosowaniu podstawowych metod i technik zarządzania gminnych, powiatowych i wojewódzkich systemów bezpieczeństwa, w tym będącymi w sytuacjach kryzysowych.	Test sprawdzający podczas zajęć, krótka praca domowa
Umiejętności:	**Zog_05**	Potrafi identyfikować zagrożenia dla bezpieczeństwa wewnętrznego państwa wynikające z podatności systemu bezpieczeństwa wewnętrznego państwa.	Kolokwium
	Zog_06	Posiada umiejętność identyfikowania, analizowania i proponowania rozwiązań problemów związanych z zarządzaniem systemami bezpieczeństwa wewnętrznego państwa.	Praca pisemna podczas zajęć
	Zog_07	Potrafi wykorzystać zdobytą wiedzę do analizowania i interpretowania zjawisk politycznych; samodzielnej oceny sytuacji i szacowania ryzyka.	Kolokwium
	Zog_08	Ma wyrobioną unikalną umiejętność całościowego spojrzenia na złożoność systemu bezpieczeństwa wewnętrznego państwa, wzajemne powiązania między jego podsystemami oraz ich elementami.	Wykonanie projektu
Kompetencje społeczne:	**Zog_09**	Potrafi dokonać prawidłowej analizy bezpieczeństwa wewnętrznego państwa. Docenia konieczność prowadzenia audytów bezpieczeństwa oraz dyskutuje o różnych sposobach ich realizacji.	Wykonanie projektu
	Zog_10	Rozróżnia i diagnozuje współczesne zagrożenia dla bezpieczeństwa a mające wpływ na funkcjonowanie systemu bezpieczeństwa wewnętrznego państwa w różnych środowiskach społecznych oraz potrafi sprostać otrzymanym zadaniom wynikającym z pełnionych w nim ról.	Odpowiedź tablicowa
	Zog_11	Formułuje nowe wyzwania zawodowe a jednocześnie odznacza się odpowiedzialnością za podejmowane decyzje i prowadzone działania oraz ich skutki wyrażając swoją postawę w środowisku specjalistów i pośrednio modelując to podejście wśród innych.	Krótka praca domowa

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
W01	Zajęcia organizacyjne. Wprowadzenie do problematyki zajęć (zakres, terminologia, akty prawne i normatywne). Organizacja systemu bezpieczeństwa wewnętrznego państwa.	2
W02	Podmiotowy i przedmiotowy zakres systemu bezpieczeństwa wewnętrznego.	3

W03	Państwo jako podmiot bezpieczeństwa: koncepcje bezpieczeństwa państwa, funkcje ochronne państwa, typologia bezpieczeństwa wewnętrznego.	2
W04	Człowiek jako podmiot bezpieczeństwa: postrzeganie zagrożeń, społeczne poczucie bezpieczeństwa.	2
W05	Doktrynalne i instytucjonalne przesłanki bezpieczeństwa.	2
W06	Ideologiczne, religijne i narodowościowe czynniki zagrożeń bezpieczeństwa wewnętrznego państwa.	2
W07	Zarządzanie systemowe bezpieczeństwem wewnętrznym państwa.	2
W08	Zarządzanie strategiczne bezpieczeństwem wewnętrznym państwa.	2
W09	Przestępczość zorganizowana.	2
W10	Bezpieczeństwo sektorowe państwa.	2
W11	Szacowanie ryzyka.	2
W12	Rola sił zbrojnych w bezpieczeństwie wewnętrznym państwa.	3
W13	Obiekty ataków terrorystycznych.	2
W14	Cyberbezpieczeństwo państwa.	2
C01	Charakterystyka zagrożeń dla bezpieczeństwa wewnętrznego państwa.	2
C02	Czynniki zagrożeń bezpieczeństwa wewnętrznego państwa.	2
C03	Systemy zarządzania bezpieczeństwem gminy, powiatu, województwa.	3
C04	Komplementarność narodu i państwa a problem bezpieczeństwa.	3
C05	Współczesne uwarunkowania interwencji militarnych w kontekście bezpieczeństwa wewnętrznego państwa.	2
C06	Przywództwo i kierowanie w tworzeniu bezpieczeństwa.	3
C07	Analiza systemowa bezpieczeństwa.	3
C08	Podsystem wykonawczy systemu bezpieczeństwa wewnętrznego RP. Policja.	2
C09	Podsystem wykonawczy systemu bezpieczeństwa wewnętrznego RP. Straż Graniczna.	2
C10	Podsystem wykonawczy systemu bezpieczeństwa wewnętrznego RP. Państwowa Straż Pożarna.	2
C11	Wpływ geopolitycznego położenia Polski na jej bezpieczeństwo wewnętrzne.	3
C12	Perspektywy ewolucji systemu bezpieczeństwa wewnętrznego Polski.	2
C13	Egzamin	1

IV.	**KORELACJA EFEKTÓW KSZTAŁCENIA**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod efektu obszarowego*
W01	Zog_01, Zog_02, Zog_03	SIB2_W01, SIB2_W03, SIB2_W04	P7U_W, P7S_WG, P7S_WK
W02	Zog_01, Zog_02	SIB2_W01, SIB2_W03, SIB2_W04	P7U_W, P7S_WG, P7S_WK
W03	Zog_01, Zog_02	SIB2_W01, SIB2_W03, SIB2_W04	P7U_W, P7S_WG, P7S_WK
W04	Zog_02, Zog_06	SIB2_W01, SIB2_W03, SIB2_W04	P7U_W, P7S_WG, P7S_WK
W05	Zog_01, Zog_02. Zog_06	SIB2_W01, SIB2_W03, SIB2_W04	P7U_W, P7S_WG, P7S_WK
W06	Zog_02, Zog_03, Zog_05	SIB2_W01, SIB2_W03, SIB2_W04	P7U_W, P7S_WG, P7S_WK
W07	Zog_02, Zog_05, Zog_07	SIB2_W01, SIB2_W03, SIB2_W04	P7U_W, P7S_WG, P7S_WK
W08	Zog_02, Zog_05, Zog_07	SIB2_W01, SIB2_W03, SIB2_W04	P7U_W, P7S_WG, P7S_WK
W09	Zog_02, Zog_03	SIB2_W01, SIB2_W03, SIB2_W04	P7U_W, P7S_WG, P7S_WK

W10	Zog_04, Zog_06, Zog_07	SIB2_W01, SIB2_W03, SIB2_W04	P7U_W, P7S_WG, P7S_WK
W11	Zog_01, Zog_03, Zog_05, Zog_07	SIB2_W01, SIB2_W03, SIB2_W04	P7U_W, P7S_WG, P7S_WK
W12	Zog_01, Zog_04	SIB2_W01, SIB2_W03, SIB2_W04	P7U_W, P7S_WG, P7S_WK
W13	Zog_05, Zog_06, Zog_07	SIB2_W01, SIB2_W03, SIB2_W04	P7U_W, P7S_WG, P7S_WK
W14	Zog_01, Zog_02, Zog_03, Zog_07	SIB2_W01, SIB2_W03, SIB2_W04	P7U_W, P7S_WG, P7S_WK
C01	Zog_05, Zog_09	SIB2_U01, SIB2_U02, SIB2_U04, SIB2_U07, SIB2_K01, SIB2_K04	P7U_U, P7S_UW, P7U_K, P7S_KK, P7S_KR
C02	Zog_06, Zog_07	SIB2_U01, SIB2_U02, SIB2_U04, SIB2_U07, SIB2_K01, SIB2_K04	P7U_U, P7S_UW, P7U_K, P7S_KK, P7S_KR
C03	Zog_05, Zog_07	SIB2_U01, SIB2_U02, SIB2_U04, SIB2_U07, SIB2_K01, SIB2_K04	P7U_U, P7S_UW, P7U_K, P7S_KK, P7S_KR
C04	Zog_07, Zog_08	SIB2_U01, SIB2_U02, SIB2_U04, SIB2_U07, SIB2_K01, SIB2_K04	P7U_U, P7S_UW, P7U_K, P7S_KK, P7S_KR
C05	Zog_08, Zog_09, Zog_10	SIB2_U01, SIB2_U02, SIB2_U04, SIB2_U07, SIB2_K01, SIB2_K04	P7U_U, P7S_UW, P7U_K, P7S_KK, P7S_KR
C06	Zog_07, Zog_09, Zog_10	SIB2_U01, SIB2_U02, SIB2_U04, SIB2_U07, SIB2_K01, SIB2_K04	P7U_U, P7S_UW, P7U_K, P7S_KK, P7S_KR
C07	Zog_08, Zog_09, Zog_11	SIB2_U01, SIB2_U02, SIB2_U04, SIB2_U07, SIB2_K01, SIB2_K04	P7U_U, P7S_UW, P7U_K, P7S_KK, P7S_KR
C08	Zog_06, Zog_09, Zog_11	SIB2_U01, SIB2_U02, SIB2_U04, SIB2_U07, SIB2_K01, SIB2_K04	P7U_U, P7S_UW, P7U_K, P7S_KK, P7S_KR
C09	Zog_06, Zog_09, Zog_11	SIB2_U01, SIB2_U02, SIB2_U04, SIB2_U07, SIB2_K01, SIB2_K04	P7U_U, P7S_UW, P7U_K, P7S_KK, P7S_KR
C10	Zog_06, Zog_09, Zog_11	SIB2_U01, SIB2_U02, SIB2_U04, SIB2_U07, SIB2_K01, SIB2_K04	P7U_U, P7S_UW, P7U_K, P7S_KK, P7S_KR
C11	Zog_05, Zog_06, Zog_09, Zog_10	SIB2_U01, SIB2_U02, SIB2_U04, SIB2_U07, SIB2_K01, SIB2_K04	P7U_U, P7S_UW, P7U_K, P7S_KK, P7S_KR
C12	Zog_09, Zog_11	SIB2_U01, SIB2_U02, SIB2_U04, SIB2_U07, SIB2_K01, SIB2_K04	P7U_U, P7S_UW, P7U_K, P7S_KK, P7S_KR
C13	Zog_06, Zog_07, Zog_8	SIB2_U01, SIB2_U02, SIB2_U04, SIB2_U07, SIB2_K01, SIB2_K04	P7U_U, P7S_UW, P7U_K, P7S_KK, P7S_KR

V.	**NAKŁAD PRACY STUDENTA**			
Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**30**		**125**	**5**
Ćwiczenia	**30**			
Seminaria				
Konwersatoria				
Konsultacje	**5**			
Rozliczenie rygorów przedmiotu				
Przygotowanie do ćwiczeń		**30**		

Opanowanie informacji		**20**		
Przygotowanie do rozliczenia rygorów		**10**		
RAZEM	**65**	**60**		

VI.	**METODY DYDAKTYCZNE**
1.	Metody podające: wykład informacyjny w formie prezentacji multimedialnej, wykład problemowy.
2.	Wykład konwersatoryjny.
3.	Metody aktywizujące: pogadanka, obserwacja, praca z dokumentacją, praca w grupach, case study, praca multimedialna (prowadzący).
4.	Ćwiczenia audytoryjne: praca w grupach, projekt praktyczny, burza mózgów, analiza tekstów z wnioskowaniem.

VII.	**FORMA ZALICZENIA PRZEDMIOTU**	
Rygor	*Kryteria składowe*	*Waga*
Zaliczenie	Kolokwium	50%
	Wykonanie projektów	35%
	Oceny z krótkich prac pisemnych	10%
	Ocena z krótkich prac domowych	5%
Egzamin		

VIII.	**LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA**
	OBOWIĄZKOWA
1.	R. Jakubczak, *Bezpieczeństwo narodowe Polski w XXI wieku*, Bellona, Warszawa 2006
2.	R. Jakubczak, J. Flis (red.), *Bezpieczeństwo narodowe Polski w XXI wieku*, Warszawa 2006
3.	J. Stańczyk, *Współczesne pojmowanie bezpieczeństwa*, Warszawa 1996
4.	R. Zięba, *Pojęcie bezpieczeństwa wewnętrznego*, Warszawa 1981
5.	*Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2020*
6.	K. Ficoń, *Inżynieria zarządzania kryzysowego. Podejście systemowe*, Warszawa 2007
7.	S. Sulowski, M. Brzeziński (red.), *Bezpieczeństwo wewnętrzne państwa. Wybrane zagadnienia*, Warszawa 2009
	UZUPEŁNIAJĄCA
1.	T. Kiziukiewicz, *Audyt wewnętrzny w jednostkach sektora finansów publicznych*, INFOR 2007
2.	W. Stankiewicz, *Bezpieczeństwo narodowe a walki niezbrojne.* Studium, Warszawa 1991
3.	P. Bączek, *Zagrożenie informacyjne a bezpieczeństwo państwa polskiego*, Marszałek, Toruń 2005
4.	J. Czaja, *Kulturowe czynniki bezpieczeństwa*, KSW Kraków 2008
5.	B. Wiśniewski, S. Zalewski, *Bezpieczeństwo wewnętrzne RP w ujęciu systemowym*, WSA Bielsko-Biała 2006
6.	*Ustawa o krajowym systemie cyberbezpieczeństwa z 5 lipca 2018 r.*, 1 sierpnia podpisał ją Prezydent RP, a następnie została opublikowana w Dzienniku Ustaw RP 13 sierpnia br. (Dz. U. 2018 poz. 1560)
7.	*Ustawa z dnia 12 października 1990 r. o Straży Granicznej* (t.j. Dz.U. z 2014 r., poz. 1402 ze zm.)
8.	*Ustawa z dnia 6 kwietnia 1990 r. o Policji* (t.j. Dz.U. z 2015 r., poz. 355 ze zm.)
9.	*Ustawa z dnia 21 listopada 1967 r. o powszechnym obowiązku obrony Rzeczypospolitej Polskiej* (t.j. Dz.U. z 2015 r., poz. 827 ze zm.)
10.	*Słownik podstawowych terminów bezpieczeństwa państwa*, pr . zbiorowa, Warszawa 1994
11.	*Słownik terminów z zakresu bezpieczeństwa narodowego*, Warszawa 2009

IX.	**PROWADZĄCY PRZEDMIOT**
Stopień, Imię i nazwisko	dr inż. Robert Janczewski
adres e-mail	r.janczewskiski@amw.gdynia.pl

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:	**Inżynieria systemów i projektowanie procesów**	*Kod*:	**Ois**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Stacjonarne		
Specjalność:	Cyberbezpieczeństwo, Analiza danych i informatyka śledcza		
Profil:	Ogólnoakademicki		
Liczba ECTS:	5		
Semestr:	1		
Wymagania wstępne:	Znajomość systemów bezpieczeństwa narodowego		
	Umiejętności zdobywania, pogłębiania i wykorzystania wiedzy w procesie studiowania.		
Język wykładowy:	Polski		
Cel przedmiotu:	**C01**	Przekazanie wiedzy z zakresu inżynieria systemów i projektowanie procesów	
	C02	Wykształcenie umiejętności identyfikacji struktury obiektu/przedmiotu projektowania systemów informacyjnych	
	C03	Wykształcenie umiejętności prowadzenia analizy systemowej oraz stosowania metod i narzędzi projektowania systemów informacyjnych wykorzystywanych w bezpieczeństwie	

II.	**EFEKTY KSZTAŁCENIA**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Ois_W01**	Student zna i rozumie podstawowe pojęcia z zakresu ogólnej teorii systemów i projektowania procesów	Kolokwium
	Ois_W02	Student zna i rozumie podstawowe pojęcia z zakresu analizy systemowej	Test
	Ois_W03	Ma pogłębioną wiedzę o budowie i funkcjonowaniu informacyjnych systemów bezpieczeństwa	Projekt
	Ois_W04	Zna metody służące do identyfikacji elementów otoczenia zewnętrznego i elementów wewnętrznych systemów informacyjnych	Projekt
Umiejętności:	**Ois_U01**	Potrafi zastosować właściwe metody analizy systemowej do opisu informacyjnych systemów bezpieczeństwa	Projekt
	Ois_U02	Potrafi projektować i modelować systemy i procesy informacyjne	Projekt
	Ois_U03	Potrafi ocenić przydatność znanych metod analizy systemowej oraz modelowania dla potrzeb budowy modeli informacyjnych systemów bezpieczeństwa	Projekt
	Ois_U04	Potrafi wykorzystywać specjalistyczne oprogramowania do modelowania	Projekt

		informacyjnych systemów bezpieczeństwa oraz procesów	
Kompetencje społeczne:	**Ois_K01**	Krytycznie ocenia posiadaną wiedzę i odbierane treści z zakresu inżynierii systemów i projektowania procesów	Obserwacja
	Ois_K02	Inicjuje i uczestniczy konstruktywnie w przygotowaniu projektów systemów informacyjnych	Projekt

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
W01	Wprowadzenie do ogólnej teorii systemów (koncepcje systemowe, podejście systemowe, analiza systemowa, system procesów)	1
W02	Identyfikacja elementów systemów informacyjnych(identyfikacja otoczenia systemu, identyfikacja elementów i relacji w systemie)	1
W03	System informacyjny jako obiekt projektowania (systemowe ujęcie bezpieczeństwa, orientacja funkcjonalna i procesowa w zarządzaniu bezpieczeństwem, klasyfikacja systemów bezpieczeństwa, struktura systemów bezpieczeństwa, wydarzenia, procesy, zasoby, relacje)	2
W04	Modelowanie systemów informacyjnych w bezpieczeństwie(diagramy kontekstowe, diagramy przepływu strumieni informacyjnych)	2
W05	Metody i narzędzia projektowania systemów informacyjnych (metody jakościowe, metody ilościowe, informatyczne wsparcie projektowania systemów informacyjnych)	2
W06	Model informacyjnego systemu bezpieczeństwa (zespołowa budowa modelu systemu informacyjnego z wykorzystaniem informatycznych narzędzi projektowych)	2
W07	Wprowadzenie do ogólnej teorii zarządzania procesami (proces, system procesów, zarządzanie procesami)	1
W08	Identyfikacja elementów procesów w informacyjnych systemach bezpieczeństwa (identyfikacja procesów, identyfikacja relacji między procesami)	1
W09	Proces w informacyjnych systemach bezpieczeństwa, jako obiekt projektowania (systemowe ujęcie bezpieczeństwa, orientacja funkcjonalna i procesowa w zarządzaniu bezpieczeństwem, klasyfikacja systemów bezpieczeństwa, wydarzenia, procesy, zasoby, relacje)	2
W10	Modelowanie procesów w informacyjnych systemach bezpieczeństwa (mapy procesów)	2
W11	Metody i narzędzia projektowania procesów w informacyjnych systemach bezpieczeństwa (schematy blokowe, metodyka EPC, standard BPMN)	2
W12	Model systemu procesów w informacyjnym systemie bezpieczeństwa (zespołowa budowa modelu systemu procesów w informacyjnym systemie bezpieczeństwa z wykorzystaniem informatycznych narzędzi projektowych)	2
C01	Model informacyjnego systemu bezpieczeństwa - identyfikacja otoczenia systemu	2
C02	Model informacyjnego systemu bezpieczeństwa - identyfikacja elementów systemu	4

C03	Model informacyjnego systemu bezpieczeństwa - identyfikacja relacji w systemie	2
C04	Model informacyjnego systemu bezpieczeństwa - diagramy przepływu strumieni informacyjnych	4
C05	Model informacyjnego systemu bezpieczeństwa - identyfikacja procesów w systemie informacyjnym	4
C06	Model systemu procesów - charakterystyka informacyjnego systemu bezpieczeństwa	4
C07	Model systemu procesów - identyfikacja procesów w informacyjnym systemie bezpieczeństwa (cel procesu, właściciel procesu, struktura procesu, wejście/wyjście procesu, dostawcy/odbiorcy procesu, parametry procesu, mierniki procesu)	4
C08	Model systemu procesów - identyfikacja relacji w systemie procesów	4
C09	Model systemu procesów - mapy procesów	12

IV.	**KORELACJA EFEKTÓW KSZTAŁCENIA**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod efektu obszarowego*
W01	Ois_W01, Ois_W02, Ois_W03, Ois_W04	SIB2_W01, SIB2_W04	P7U_W, P7S_WG, P7S_WK
W02	Ois_W01, Ois_W02, Ois_W03, Ois_W04	SIB2_W01, SIB2_W04	P7U_W, P7S_WG, P7S_WK
W03	Ois_W01, Ois_W02, Ois_W03, Ois_W04	SIB2_W01, SIB2_W04	P7U_W, P7S_WG, P7S_WK
W04	Ois_W01, Ois_W02, Ois_W03, Ois_W04	SIB2_W01, SIB2_W04	P7U_W, P7S_WG, P7S_WK
W05	Ois_W01, Ois_W02, Ois_W03, Ois_W04	SIB2_W01, SIB2_W04	P7U_W, P7S_WG, P7S_WK
W06	Ois_W01, Ois_W02, Ois_W03, Ois_W04	SIB2_W01, SIB2_W04	P7U_W, P7S_WG, P7S_WK
W07	Ois_W01, Ois_W02, Ois_W03, Ois_W04	SIB2_W01, SIB2_W04	P7U_W, P7S_WG, P7S_WK
W08	Ois_W01, Ois_W02, Ois_W03, Ois_W04	SIB2_W01, SIB2_W04	P7U_W, P7S_WG, P7S_WK
W09	Ois_W01, Ois_W02, Ois_W03, Ois_W04	SIB2_W01, SIB2_W04	P7U_W, P7S_WG, P7S_WK
W10	Ois_W01, Ois_W02, Ois_W03, Ois_W04	SIB2_W01, SIB2_W04	P7U_W, P7S_WG, P7S_WK
W11	Ois_W01, Ois_W02, Ois_W03, Ois_W04	SIB2_W01, SIB2_W04	P7U_W, P7S_WG, P7S_WK
W12	Ois_W01, Ois_W02, Ois_W03, Ois_W04	SIB2_W01, SIB2_W04	P7U_W, P7S_WG, P7S_WK
C01	Ois_U01, Ois_U02, Ois_U03, Ois_U04, Ois_K01, Ois_K02	SIB2_U01, SIB2_U02, SIB2_U04, SIB2_U06, SIB2_U07, SIB2_K01, SIB2_K02, SIB2_K03, SIB2_K05	P7U_U, P7S_UW, P7S_UK, P7S_UO, P7U_K, P7S_KK, P7S_KO, P7S_KR
C02	Ois_U01, Ois_U02, Ois_U03, Ois_U04, Ois_K01, Ois_K02	SIB2_U01, SIB2_U02, SIB2_U04, SIB2_U06, SIB2_U07, SIB2_K01, SIB2_K02, SIB2_K03, SIB2_K05	P7U_U, P7S_UW, P7S_UK, P7S_UO, P7U_K, P7S_KK, P7S_KO, P7S_KR
C03	Ois_U01, Ois_U02, Ois_U03, Ois_U04, Ois_K01, Ois_K02	SIB2_U01, SIB2_U02, SIB2_U04, SIB2_U06, SIB2_U07, SIB2_K01, SIB2_K02, SIB2_K03, SIB2_K05	P7U_U, P7S_UW, P7S_UK, P7S_UO, P7U_K, P7S_KK, P7S_KO, P7S_KR

C04	Ois_U01, Ois_U02, Ois_U03, Ois_U04, Ois_K01, Ois_K02	SIB2_U01, SIB2_U02, SIB2_U04, SIB2_U06, SIB2_U07, SIB2_K01, SIB2_K02, SIB2_K03, SIB2_K05	P7U_U, P7S_UW, P7S_UK, P7S_UO, P7U_K, P7S_KK, P7S_KO, P7S_KR
C05	Ois_U01, Ois_U02, Ois_U03, Ois_U04, Ois_K01, Ois_K02	SIB2_U01, SIB2_U02, SIB2_U04, SIB2_U06, SIB2_U07, SIB2_K01, SIB2_K02, SIB2_K03, SIB2_K05	P7U_U, P7S_UW, P7S_UK, P7S_UO, P7U_K, P7S_KK, P7S_KO, P7S_KR
C06	Ois_U01, Ois_U02, Ois_U03, Ois_U04, Ois_K01, Ois_K02	SIB2_U01, SIB2_U02, SIB2_U04, SIB2_U06, SIB2_U07, SIB2_K01, SIB2_K02, SIB2_K03, SIB2_K05	P7U_U, P7S_UW, P7S_UK, P7S_UO, P7U_K, P7S_KK, P7S_KO, P7S_KR
C07	Ois_U01, Ois_U02, Ois_U03, Ois_U04, Ois_K01, Ois_K02	SIB2_U01, SIB2_U02, SIB2_U04, SIB2_U06, SIB2_U07, SIB2_K01, SIB2_K02, SIB2_K03, SIB2_K05	P7U_U, P7S_UW, P7S_UK, P7S_UO, P7U_K, P7S_KK, P7S_KO, P7S_KR
C08	Ois_U01, Ois_U02, Ois_U03, Ois_U04, Ois_K01, Ois_K02	SIB2_U01, SIB2_U02, SIB2_U04, SIB2_U06, SIB2_U07, SIB2_K01, SIB2_K02, SIB2_K03, SIB2_K05	P7U_U, P7S_UW, P7S_UK, P7S_UO, P7U_K, P7S_KK, P7S_KO, P7S_KR
C09	Ois_U01, Ois_U02, Ois_U03, Ois_U04, Ois_K01, Ois_K02	SIB2_U01, SIB2_U02, SIB2_U04, SIB2_U06, SIB2_U07, SIB2_K01, SIB2_K02, SIB2_K03, SIB2_K05	P7U_U, P7S_UW, P7S_UK, 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**		**125**	**5**
Ćwiczenia	**40**			
Seminaria				
Konwersatoria				
Konsultacje	**5**			
Rozliczenie rygorów przedmiotu				
Przygotowanie do ćwiczeń	**X**	**30**		
Opanowanie informacji		**20**		
Przygotowanie do rozliczenia rygorów		**10**		
RAZEM	**65**	**60**		

VI. METODY DYDAKTYCZNE

1.	Prezentacje multimedialne
2.	Ćwiczenia laboratoryjne

VII. FORMA ZALICZENIA PRZEDMIOTU

Rygor	*Kryteria składowe*	*Waga*
Zaliczenie	Kolokwium	0,5
	Wykonanie projektów	0,5
Egzamin		

VIII. LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

OBOWIĄZKOWA

1. C. Cempel, *Teoria i inżynieria systemów. Zasady i zastosowania myślenia systemowego*, ITE Radom 2008

2.	W. Findeisen (red.), *Analiza systemowa. Podstawy i metodologia*, PWN, 1985
3.	P. Sienkiewicz, *Analiza systemowa. Podstawy i zastosowania*, Bellona, 1994
4.	W. Bojarski, *Podstawy analizy i inżynierii systemów*, WNT, 1983
5.	E. Skrzypek, M. Hofman, *Zarządzanie procesami w przedsiębiorstwie*, Wolters Kluwer Polska, 2010
6.	A. Bitkowska, *Zarządzanie procesami biznesowymi w przedsiębiorstwie*, Vizja Press & IT, Warszawa 2009.
UZUPEŁNIAJĄCA	
1.	J. Konieczny, *Inżynieria systemów działania*, WNT, 1983
2.	P. Sienkiewicz, *Inżynieria systemów kierowania*, PWE, 1988
3.	P. Sienkiewicz, *Inżynieria systemów*, Wydawnictwo, MON, 1983
4.	E. Yourdon, *Współczesna analiza strukturalna*, WNT, 1996

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

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:	**Audyt i certyfikacja systemów informatycznych**	*Kod*:	**Oes**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Stacjonarne		
Kształcenie w zakresie:	Cyberbezpieczeństwo, Analiza danych i informatyka śledcza		
Profil:	Ogólnoakademicki		
Liczba ECTS:	5		
Semestr:	1		
Wymagania wstępne:	Podstawowa wiedza nt. zasad organizacji systemów zarządzania bezpieczeństwem informacyjnym.		
Język wykładowy:	Polski		
Cel przedmiotu:	**C01**	Zapoznanie z uwarunkowaniami charakterystycznymi dla tworzenia systemów zarządzania bezpieczeństwem informacyjnym oraz organizacji ochrony informacji jako szczególnie ważnego elementu zasobów instytucji.	
	C02	Zapoznanie z zasadami inwentaryzacji, klasyfikacji oraz oceny zasobów informacyjnych przetwarzanych w systemach teleinformatycznych w aspekcie zagrożeń oraz podatności ocenianych systemów.	
	C03	Zapoznanie z zasadami realizacji audytów bezpieczeństwa teleinformatycznego, oceny i zarządzania ryzykiem oraz metodami i standardami testowania i audytowania systemów bezpieczeństwa informacyjnego.	
	C04	Ukształtowanie prawidłowych wzorców sumienności, transparentności i niezawisłości w działaniu	

II.	**Kierunkowe efekty uczenia się**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Oes_W01**	student ma wiedzę w zakresie podstawowych pojęć i definicji dotyczących audytu, kontroli, certyfikacji i akredytacji	wypowiedź ustna, praca pisemna lub sprawdzian
	Oes_W02	student ma wiedzę w zakresie regulacji formalno-prawnych w obszarze audytu i certyfikacji osób, systemów zarządzania oraz produktów	wypowiedź ustna, praca pisemna lub sprawdzian
	Oes_W03	student rozumie cele certyfikacji oraz audytu oraz zna zasady ich przeprowadzania	wypowiedź ustna, praca pisemna lub sprawdzian
	Oes_W04	student ma wiedzę w zakresie zarządzania ryzykiem	wypowiedź ustna, praca pisemna lub sprawdzian
	Oes_W05	student ma wiedzę w zakresie mechanizmów kontrolnych	wypowiedź ustna/sprawdzian/kolokwium

		wymaganych normami bezpieczeństwa	
Umiejętości:	**Oes_U01**	student rozumie i potrafi oceniać skuteczność systemu zarządzania bezpieczeństwem informacji	wypowiedź ustna, praca pisemna lub sprawdzian
	Oes_U02	student potrafi identyfikować główne zagrożenia w obszarze bezpieczeństwa informacji oraz proponować adekwatne mechanizmy kontrolne	wypowiedź ustna, praca pisemna lub sprawdzian
	Oes_U03	student potrafi przygotować program audytu, oraz zidentyfikować i udokumentować niezgodności, a także analizować ich ewentualny wpływ na bezpieczeństwo przetwarzanych informacji	wypowiedź ustna, praca pisemna lub sprawdzian
	Oes_U04	student potrafi nazwać i sklasyfikować zidentyfikowane ryzyko	wypowiedź ustna, praca pisemna lub sprawdzian
Kompetencje społeczne:	**Oes_K01**	Krytycznie ocenia posiadaną wiedzę i odbierane treści z zakresu audytu i certyfikacja systemów informatycznych	Obserwacja
	Oes_K02	Inicjuje i uczestniczy konstruktywnie w przygotowaniu zadań z zakresu audytu i certyfikacja systemów informatycznych	praca pisemna

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
W01	Audyt i certyfikacja systemów informatycznych - wprowadzenie	1
W02	Podstawy audytowania	2
W03	Rosnąca rola cyberbezpieczeństwa	1
W04	Cyberbezpieczeństwo w pigułce	1
W05	SZBI zgodny z ISO 27001	1
W06	Mechanizmy kontrolne ISO 27001	2
W07	Zarządzanie ryzykiem	1
W08	Kluczowe akty prawne i normalizacyjne	1
W09	Taksonomia cyberzagrożeń	2
W10	Ład korporacyjny w zakresie IT	1
W11	Podstawowe procesy bezpieczeństwa informacji	2
W12	Podstawowe zasady bezpieczeństwa	1
W13	Wdrażanie SZBI	1
W14	Certyfikacja osób, systemów zarządzania i produktów	1
W15	Sprawdzian	1

C01	Charakterystyka krajowych i międzynarodowych aktów prawnych i normatywnych regulujących proces audytowania i certyfikacji systemów zarządzania bezpieczeństwem informacyjnym. Referat studenta.	3
C02	Charakterystyka zasad inwentaryzacji, klasyfikacji i oceny wartości zasobów informacyjnych. Pomiary bezpieczeństw teleinformatycznego. Referat studenta.	4
C03	Charakterystyka procesu zarządzania ryzykiem. Analiza ryzyka w zakresie identyfikacji zagrożeń, podatności i środowiska. Dobór adekwatnych środków ochrony. Studium przypadku. Referat studenta.	3
C04	Zarządzanie projektowaniem i budową systemu bezpieczeństwa teleinformatycznego. Dokumentowanie prac projektowych. Referat studenta.	4
C05	Audyt bezpieczeństwa teleinformatycznego. Referat studenta.	3
C06	Audyt i certyfikowanie systemu zarządzania bezpieczeństwem informacyjnym.	3

IV.	**KORELACJA EFEKTÓW KSZTAŁCENIA**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod efektu obszarowego*
W01	-	-	-
W02	Oes_W01, Oes_W02, Oes_W03, Oes_U01, Oes_U03	SIB2_W01, SIB2_W02, SIB2_W03	P7U_W, P7S_WG, P7S_WK
W03	Oes_W04, Oes_U02, Oes_U04	SIB2_W01, SIB2_W02, SIB2_W03	P7U_W, P7S_WG, P7S_WK
W04	Oes_W03, Oes_W04, Oes_W05, Oes_U01, Oes_U02, Oes_U04	SIB2_W01, SIB2_W02, SIB2_W03	P7U_W, P7S_WG, P7S_WK
W05	Oes_W01, Oes_W02, Oes_W03, Oes_W04, Oes_U01, Oes_U02, Oes_U03	SIB2_W01, SIB2_W02, SIB2_W03	P7U_W, P7S_WG, P7S_WK
W06	Oes_W01, Oes_W03, Oes_W05, Oes_U03	SIB2_W01, SIB2_W02, SIB2_W03	P7U_W, P7S_WG, P7S_WK
W07	Oes_W01, Oes_W03, Oes_W04, Oes_W05, Oes_U01, Oes_U02, Oes_U04	SIB2_W01, SIB2_W02, SIB2_W03	P7U_W, P7S_WG, P7S_WK
W08	Oes_W01, Oes_W02, Oes_W04	SIB2_W01, SIB2_W02, SIB2_W03	P7U_W, P7S_WG, P7S_WK
W09	Oes_W04, Oes_U02, Oes_U04	SIB2_W01, SIB2_W02, SIB2_W03	P7U_W, P7S_WG, P7S_WK

W10	Oes_W01, Oes_W02, Oes_W04, Oes_U01	SIB2_W01, SIB2_W02, SIB2_W03	P7U_W, P7S_WG, P7S_WK
W11	Oes_W03, Oes_W05, Oes_U02	SIB2_W01, SIB2_W02, SIB2_W03	P7U_W, P7S_WG, P7S_WK
W12	Oes_W03, Oes_W05, Oes_U02	SIB2_W01, SIB2_W02, SIB2_W03	P7U_W, P7S_WG, P7S_WK
W13	Oes_W01, Oes_W03, Oes_U01	SIB2_W01, SIB2_W02, SIB2_W03	P7U_W, P7S_WG, P7S_WK
W14	Oes_W01, Oes_W02, Oes_W03, Oes_U02	SIB2_W01, SIB2_W02, SIB2_W03	P7U_W, P7S_WG, P7S_WK
W15			
C01	Oes_W01, Oes_W03, Oes_K01, Oes_K02	-	-
C02	Oes_W02, Oes_W04, Oes_W05, Oes_U01, Oes_U02, Oes_K01, Oes_K02	SIB2_U01, SIB2_U04, SIB2_U06, SIB2_K02, SIB2_K04	P7U_U, P7S_UW, P7S_UK, P7S_UO, P7U_K, P7S_KK, P7S_KR
C03	Oes_W01, Oes_W04, Oes_W05, Oes_U01, Oes_U02, Oes_U03, Oes_U04, Oes_K01, Oes_K02	SIB2_U01, SIB2_U04, SIB2_U06, SIB2_K02, SIB2_K04	P7U_U, P7S_UW, P7S_UK, P7S_UO, P7U_K, P7S_KK, P7S_KR
C04	Oes_W05, Oes_U03, Oes_K01, Oes_K02	SIB2_U01, SIB2_U04, SIB2_U06, SIB2_K02, SIB2_K04	P7U_U, P7S_UW, P7S_UK, P7S_UO, P7U_K, P7S_KK, P7S_KR
C05	Oes_W01, Oes_W03, Oes_W04, Oes_U01, Oes_U03, Oes_U04, Oes_K01, Oes_K02	SIB2_U01, SIB2_U04, SIB2_U06, SIB2_K02, SIB2_K04	P7U_U, P7S_UW, P7S_UK, P7S_UO, P7U_K, P7S_KK, P7S_KR
C06	Oes_W01, Oes_W02, Oes_W03, Oes_W04, Oes_U01, Oes_U03, Oes_U04, Oes_K01, Oes_K02	-	-

V.	**NAKŁAD PRACY STUDENTA**			
Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**30**		**125**	**5**
Ćwiczenia	**30**			
Seminaria				
Konwersatoria				
Konsultacje	**5**			
Rozliczenie rygorów przedmiotu				
Przygotowanie do ćwiczeń		**30**		
Opanowanie informacji		**20**		
Przygotowanie do rozliczenia rygorów		**10**		

RAZEM	**65**	**60**		

VI.	**METODY DYDAKTYCZNE**
1.	Wykład z prezentacją multimedialną/dyskusja
2.	Ćwiczenia audytoryjne: projekt praktyczny
3.	Ćwiczenia audytoryjne: praca w grupach

VII.	**FORMA ZALICZENIA PRZEDMIOTU**	
Rygor	*Kryteria składowe*	*Waga*
Zaliczenie	ocena ze sprawdzianu	0,4
	aktywność podczas wykładów	0,1
	praca zaliczeniowa	0,2
	ocena z przygotowania i aktywności na ćwiczeniach	0,1
	ocena z projektu	0,2
	obecność na ćwiczeniach obowiązkowa (w przypadku nieobecności pow. 50% - student nieklasyfikowany)	

VIII.	**LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA**
	OBOWIĄZKOWA
1.	K. Lidermann, *Bezpieczeństwo informacyjne. Nowe wyzwania*, PWN Warszawa 2017
2.	T. Polaczek, *Audyt bezpieczeństwa informacji w praktyce : praktyczny przewodnik po zagadnieniach ochrony informacji*, Gliwice, Helion, 2006
3.	K. Jajuga (red. naukowa);, *Zarządzanie ryzykiem* autorzy: Krzysztof Jajuga, Wanda Ronka-Chmielowiec, Andrzej Stopczyński, Agnieszka Wojtasik-Terech. Wydanie II. – Warszawa, Wydawnictwo Naukowe PWN SA, 2019.
4.	*Polska norma PN-EN ISO/IEC 27001:2017-06 - wersja polska*, PKN; Warszawa 2017
	UZUPEŁNIAJĄCA
1.	B. Noga, M. Noga, *Zarządzanie ryzykiem w procesie podejmowania decyzji ekonomicznych przez organizacje*, Wydanie I, - Warszawa, CeDeWu, 2019.
2.	*Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 roku w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego*, Dz.U.2011.159.948
3.	*Decyzja nr 7/MON Ministra Obrony Narodowej z dnia 20 stycznia 2012 roku w sprawie organizacji ochrony systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych w resorcie obrony narodowej*, Dz.Urz.MON.2012.8
4.	*Polska norma PN-EN ISO/IEC 27002:2017-06 - wersja polska*, PKN; Warszawa 2017

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

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:	**Ocena ryzyka i prognozowanie w bezpieczeństwie**	*Kod*:	**Zpa**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Stacjonarne		
Kształcenie w zakresie:	Cyberbezpieczeństwo, Analiza danych i informatyka śledcza		
Profil:	Ogólnoakademicki		
Liczba ECTS:	5		
Semestr:	1		
Wymagania wstępne:	Podstawy matematyki, statystyki		
Język wykładowy:	Polski		
Cel przedmiotu:	**C01**	Przedstawienie teorii oraz metod oceny ryzyka w bezpieczeństwie	
	C02	Przedstawienie metod prognozowania w bezpieczeństwie	
	C03	Zaprezentowanie nowoczesnych technologii do oceny ryzyka oraz prognozowania	

II.	**EFEKTY UCZENIA SIĘ**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Zpa_W01**	Posiada wiedzę z zakresu oceny ryzyka	Kolokwium
	Zpa_W02	Posiada wiedzę z zakresu prognozowania	Kolokwium
Umiejętności:	**Zpa_U01**	Potrafi oceniać ryzyko w bezpieczeństwie	Zadanie
	Zpa_U02	Potrafi opracowywać prognozy w bezpieczeństwie	Projektowe
	Zpa_U03	Potrafi wykorzystywać nowoczesne technologie do oceny ryzyka i prognozowania	Zadanie
	Zpa_U04	Posiada umiejętność rozwijania swojej wiedzy dotyczącej oceny ryzyka i prognozowania	Projektowe
Kompetencje społeczne:	**Zpa_K01**	Potrafi współdziałać i pracować w grupie	Zadanie

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
W01	Geneza, pojęcie, definicje ryzyka	4
W02	(geneza i historia ryzyka, etymologia pojęcia ryzyka, definicje i mechanizm ryzyka, dualność pojęcia ryzyka, ryzyko w teorii decyzji, rodzaje ryzyka, gotowość podejmowania ryzyka)	4
W03	Taksonomia ryzyka	4
W04	(ryzyko ekonomiczne, ryzyko prawno-organizacyjne, ryzyko polityczne, ryzyko ekologiczne, ryzyko medyczne, ryzyko społeczne, ryzyko medialne, ryzyko kulturowo-religijne)	2
W05	Miary ryzyka	4
W06	(szacowanie prawdopodobieństwo wystąpienia określonego rodzaju zagrożenia lub straty, a także zysku i korzyści)	4

W07	Symulacja komputerowa do oceny ryzyka i prognozowania (pojęcie symulacji, technika symulacji, symulacja komputerowa, obiekty symulacji, zalety symulacji)	3
C01	Ocena ryzyka (realizacja projektu)	10
C02	Ocena ryzyka - kolokwium	2
C03	Opracowania prognozy (realizacja projektu)	12
C04	Prognozowanie - kolokwium	1

IV.	**KORELACJA EFEKTÓW UCZENIA SIĘ**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyki PRK*
W01	Zpa_W01, Zpa_W02	SIB2_W01, SIB2_W02	P7U_W, P7S_WG, P7S_WK
W02	Zpa_W01, Zpa_W02	SIB2_W01, SIB2_W02	P7U_W, P7S_WG, P7S_WK
W03	Zpa_W01, Zpa_W02	SIB2_W01, SIB2_W02	P7U_W, P7S_WG, P7S_WK
W04	Zpa_W01, Zpa_W02	SIB2_W01, SIB2_W02	P7U_W, P7S_WG, P7S_WK
W05	Zpa_W01, Zpa_W02	SIB2_W01, SIB2_W02	P7U_W, P7S_WG, P7S_WK
W06	Zpa_W01, Zpa_W02	SIB2_W01, SIB2_W02	P7U_W, P7S_WG, P7S_WK
W07	Zpa_W01, Zpa_W02	SIB2_W01, SIB2_W02	P7U_W, P7S_WG, P7S_WK
C01	Zpa_U01, Zpa_U02, Zpa_U03, Zpa_U04, Zpa_K01	SIB2_U01, SIB2_U02, SIB2_U04, SIB2_U06, SIB2_U07, SIB2_K01, SIB2_K02, SIB2_K03	P7U_U, P7S_UW, P7S_UK, P7S_UO, P7U_K, P7S_KK, P7S_KO
C02	Zpa_U01, Zpa_U02, Zpa_U03, Zpa_U04, Zpa_K01	SIB2_U01, SIB2_U02, SIB2_U04, SIB2_U06, SIB2_U07, SIB2_K01, SIB2_K02, SIB2_K03	P7U_U, P7S_UW, P7S_UK, P7S_UO, P7U_K, P7S_KK, P7S_KO
C03	Zpa_U01, Zpa_U02, Zpa_U03, Zpa_U04, Zpa_K01	SIB2_U01, SIB2_U02, SIB2_U04, SIB2_U06, SIB2_U07, SIB2_K01, SIB2_K02, SIB2_K03	P7U_U, P7S_UW, P7S_UK, P7S_UO, P7U_K, P7S_KK, P7S_KO
C04	Zpa_U01, Zpa_U02, Zpa_U03, Zpa_U04, Zpa_K01	SIB2_U01, SIB2_U02, SIB2_U04, SIB2_U06, SIB2_U07, SIB2_K01, SIB2_K02, SIB2_K03	P7U_U, P7S_UW, P7S_UK, P7S_UO, P7U_K, P7S_KK, P7S_KO

V.	**NAKŁAD PRACY STUDENTA**			
Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**20**	**X**	**126**	**5**
Ćwiczenia	**40**			
Seminaria				
Konwersatoria				
Konsultacje (zaliczenie nieobecności, rozliczenie rygorów, poprawy)	**6**			
Przygotowanie do ćwiczeń	**X**	**30**		
Opanowanie informacji		**20**		
Przygotowanie do rozliczenia rygorów		**10**		
RAZEM	**66**	**60**		

VI.	**METODY DYDAKTYCZNE**
1.	Wykład
2.	Ćwiczenia
3.	Laboratorium
4.	Praca w grupach

VII.	**FORMA ZALICZENIA PRZEDMIOTU**	
Rygor	*Kryteria składowe*	*Waga*

Zaliczenie	Ocena z ćwiczeń - sprawozdania	0,4
	Ocena z kolokwium (materiał z wykładów)	0,6
Egzamin	Ocena z egzaminu	1,0

VIII.	**LITERATURA**
	OBOWIĄZKOWA
1.	J. Bizon-Górecka, *Ryzyko. Zarządzanie ryzykiem w przedsiębiorstwie. Modelowanie systemu zarządzania ryzykiem w przedsiębiorstwie - ujęcie holistyczne*, Towarzystwo Naukowe Organizacji i Kierownictwa, Bydgoszcz 2007
2.	M. Cieślik, *Prognozowanie gospodarcze*, 2004
3.	T. T. Kaczmarek, *Ryzyko i zarządzanie ryzykiem. Ujęcie interdyscyplinarne*, Warszawa 2005
	UZUPEŁNIAJĄCA
1.	W. Kasperek, K. Pelc, *Wyzwania technologiczne - Prognozy i strategie*, 2002
2.	P. Matkowski, *Zarządzanie ryzykiem operacyjnym*, Oficyna Ekonomiczna, Kraków 2006
3.	S. Strzelczak, *Operational Risk Management*, Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa 2008

IX.	**PROWADZĄCY PRZEDMIOT**
Stopień, Imię i nazwisko	Prof. dr hab. Krzysztof FICOŃ, mgr Martyna BARTKOWSKA
adres e-mail	k.ficon@amw.gdynia.pl m.bartkowska@amw.gdynia.pl

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 projektem**	***Kod*:**	**Za**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Stacjonarne		
Kształcenie w zakresie:	Cyberbezpieczeństwo, Analiza danych i informatyka śledcza		
Profil:	Ogólnoakademicki		
Liczba ECTS:	5		
Semestr:	2		
Wymagania wstępne:	Podstawowa wiedza z zarządzania i organizacji oraz ekonomii		
Język wykładowy:	Polski		
Cel przedmiotu: **C01**	Zapoznanie studentów z zasadami zarządzania projektami w organizacji.		

II.	**EFEKTY UCZENIA SIĘ**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Za_W01**	Student rozumie powody i potrzeby wprowadzenia zasad zarządzania projektami w organizacjach.	Kolokwium
	Za_W02	Student zna ogólne zasady metody planowania oraz realizowania projektów, tworzenia harmonogramów i planów projektu, budowania zespołu, zarządzania ryzykiem i zmianami w projekcie.	Kolokwium
Umiejętności:	**Za_U01**	Student umie wybierać i proponować sposób planowania i realizacji projektu.	Praca projektowa
	Za_U02	Student umie wykorzystywać podstawowe narzędzia organizatorskie w zakresie planowania i realizacji projektów.	Praca projektowa
Kompetencje społeczne:	**Za_K01**	Student potrafi współdziałać i pracować w zespole projektowym, przyjmując w nim różne role.	Praca projektowa
	Za_K02	Student potrafi odpowiednio określić priorytety projektowe służące realizacji określonego przez siebie celu projektowego.	Praca projektowa
	Za_K03	Student potrafi przewidywać wielokierunkowe skutki społeczne wdrażanych projektów.	Praca projektowa

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
W01	**Podstawy zarządzania projektami:** definicja projektu, najważniejsze cechy projektów, rodzaje projektów, zarządzanie projektem, cykl życia	2

	projektu, procesy zarządzania projektem(inicjowanie projektu, planowanie projektu, realizowanie projektu, kontrolowanie projektu, zamykanie projektu), środowisko projektu, Interesariusze projektu, źródła sukcesu projektu, przyczyny niepowodzeń, rola i znaczenie projektów w funkcjonowaniu organizacji.	
W02	**Kontekst projektu:** strategia zarządzania projektem, struktury projektowe, kierownik projektu, przywództwo, zespół projektowy, umiejętności zespołu projektowego, miejsce i rola pracownika w projekcie.	2
W03	**Obszary Wiedzy Zarządzania Projektami:** zarządzanie integracją projektu, zarządzanie zakresem projektu, zarządzanie czasem projektu, zarządzanie kosztami projektu, zarządzanie jakością projektu, zarządzanie zasobami ludzkimi projektu, zarządzanie komunikacją projektu, zarządzanie ryzykiem projektu, zarządzanie zaopatrzeniem projektu.	4
W04	**Inicjowanie projektu:**analizy przedprojektowe (analiza udziałowców projektu, analiza potencjalnych problemów projektowych, analiza produktów projektu, Karta Projektu, czynniki powodzenia projektu, metody oceny rentowności projektów – kryteria wyboru projektu.	4
W05	**Planowanie projektu:** zakres projektu, struktura podziału pracy (WBS), zależności między nimi i dodatkowe, ograniczenia zadań w czasie, szacowanie czasu zadania, określenie i przydział zasobów, rozwiązywanie problemu przeciążenia zasobów, harmonogram projektu (harmonogram projektu w postaci sieci CPM, metody PERT, Łańcuch Krytyczny, Harmonogram Gntta), budżet projektu, metody budżetowania projektu, planowanie organizacji projektu (macierz odpowiedzialności oraz schemat organizacyjny projektu), zasady pracy w projekcie - procedury i standardy projektowe, plan projektu i jego elementy (plan komunikacji, plan zarządzania jakością, plan zarządzania zmianami, plan zarządzania zasobami ludzkimi).	3
W06	**Realizacja i controlling projektu:** procesy realizacji projektu, Controlling projektu - podstawowe zasady, kontrola przebiegu projektu: spotkania przeglądowe i dokumenty, kontrola projektu: raportowanie i eskalowanie problemów, kontrola zmian w projekcie.	3
W07	**Zamknięcie projektu:** procesy zamknięcia projektu, procedury akceptacji i zamknięcia projektu, dokumentacja projektu.	2
C01	**Planowanie projektu za pomocą MS Project – środowisko programu**	4
C02	**Planowanie projektu organizacyjnego dla dowolnej inicjatywy w obszarze bezpieczeństwa państwa za pomocą programu MS Project:**ustalanie celów projektowych, planowanie zakresu, doprecyzowywanie zakresu, określenie działań, określenie kolejności działań, planowanie zasobów, szacowanie czasu trwania działań, opracowanie harmonogramu, oszacowanie kosztów, budżetowanie kosztów, analiza opłacalności projektu, analiza ryzyka projektu, opracowanie planu projektu.	32
C03	**Zaliczenie przedmiotu.**	4

IV.	**KORELACJA EFEKTÓW UCZENIA SIĘ**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyki PRK*
W01	Za_W01, Za_W02	SIB2_W01, SIB2_W04	P7U_W, P7S_WG, P7S_WK

W02	Za_W01, Za_W02	SIB2_W01, SIB2_W04	P7U_W, P7S_WG, P7S_WK
W03	Za_W01, Za_W02	SIB2_W01, SIB2_W04	P7U_W, P7S_WG, P7S_WK
W04	Za_W01, Za_W02	SIB2_W01, SIB2_W04	P7U_W, P7S_WG, P7S_WK
W05	Za_W01, Za_W02	SIB2_W01, SIB2_W04	P7U_W, P7S_WG, P7S_WK
W06	Za_W01, Za_W02	SIB2_W01, SIB2_W04	P7U_W, P7S_WG, P7S_WK
W07	Za_W01, Za_W02	SIB2_W01, SIB2_W04	P7U_W, P7S_WG, P7S_WK
C01	Za_U01, Za_U02, Za_K01, Za_K02, Za_K03	SIB2_U01, SIB2_U02, SIB2_U04, SIB2_U06, SIB2_K03, SIB2_K04, SIB2_K05	P7U_U, P7S_UW, P7S_UK, P7S_UO, P7U_K, P7S_KO, P7S_KR
C02	Za_U01, Za_U02, Za_K01, Za_K02, Za_K03	SIB2_U01, SIB2_U02, SIB2_U04, SIB2_U06, SIB2_K03, SIB2_K04, SIB2_K05	P7U_U, P7S_UW, P7S_UK, P7S_UO, P7U_K, P7S_KO, P7S_KR
C03	Za_U01, Za_U02, Za_K01, Za_K02, Za_K03	SIB2_U01, SIB2_U02, SIB2_U04, SIB2_U06, SIB2_K03, SIB2_K04, SIB2_K05	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 Nie kontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**20**	**X**	**125**	**5**
Ćwiczenia	**40**			
Seminaria	**0**			
Konwersatoria	**0**			
Konsultacje (zaliczenie nieobecności, rozliczenie rygorów, poprawy)	**5**			
Przygotowanie do ćwiczeń	**X**	**20**		
Opanowanie informacji		**20**		
Przygotowanie do rozliczenia rygorów		**20**		
RAZEM	**65**	**60**		

VI. METODY DYDAKTYCZNE

- wykład; - prezentacja multimedialna;	- ćwiczenia – obsługa programu MS Project - praca projektowa indywidualna – z wykorzystaniem programu MS Project;

VII. FORMA ZALICZENIA PRZEDMIOTU

Rygor	*Kryteria składowe*	*Waga*
Zaliczenie	Ocena z kolokwium	0,5
	Ocena z ćwiczeń	0,5
	Razem	1,0

VIII. LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

OBOWIĄZKOWA

1. M. Trocki, *Zarządzanie projektami*, Wydawnictwo Naukowe PWN, 2012 r.
2. M. Pawlak, *Zarządzanie projektami*, Wydawnictwo Naukowe PWN, 2011 r.
3. J. Kisielnicki, *Zarządzanie projektami udzie, procedury, wyniki*, Wolter Kluwer, 2011

UZUPEŁNIAJĄCA

1. A. Kozarkiewicz, M. Łada, *Zarządzanie wartością projektów. Instrumenty rachunkowości zarządczej i controllingu*, C.H. Beck, 2010 r.
2. A. Koszlajda, *Zarządzanie projektami IT. Przewodnik po metodykach*, Helion 2010 r.
3. Zajączkowska A., *Koordynator projektu - instruktaż skutecznego zarządzania projektami unijnymi z suplementem elektronicznym do monitoringu zadań*, Ośrodek Doradztwa i Doskonalenia Kadr, 2010 r.
4. M. Flasiński, *Zarządzanie projektami informatycznymi*, Wydawnictwo Naukowe PWN, 2009 r.
5. S. Barker, R. Cole, *Zarządzanie projektem*, Wydawnictwo Naukowe PWN, 2010 r.

IX.	PROWADZĄCY PRZEDMIOT
Stopień, imię i nazwisko	dr. Jerzy KUPIŃSKI, dr Anna MILER
adres e-mai	j.kupiński@amw.gdynia.pl a.miler@amw.gdynia.pl

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:	**Komunikacja społeczna**	*Kod*:	**Iq**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Stacjonarne		
Kształcenie w zakresie:	Cyberbezpieczeństwo, Analiza danych i informatyka śledcza		
Profil:	Akademicki		
Liczba ECTS:	3		
Semestr:	2		
Wymagania wstępne:	Poszerzona wiedza z zakresu komunikacji		
Język wykładowy:	Polski		
Cel przedmiotu: **C01**	Przybliżenie wiedzy pozwalającej zrozumieć istotę zagadnień dotyczących komunikacji społecznej.		
C02	Zdobycie umiejętności w zakresie umiejętności miękkich.		

II.	**EFEKTY UCZENIA SIĘ**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Iq_W01**	Ma podstawową wiedzę o rożnych rodzajach struktur społecznych oraz rządzące nimi prawidłowości	Kolokwium ustne, praca na ćwiczeniach
	Iq_W02	Posiada elementarną wiedzę na temat efektywnego porozumiewania się w różnorodnych sytuacjach życia zawodowego oraz w kontaktach z cudzoziemcami	Kolokwium ustne, praca na ćwiczeniach
	Iq_W03	Posiada podstawową wiedzę o człowieku, jako podmiocie tworzącym struktury społecznie i działającym w ramach tych struktur	Kolokwium ustne, praca na ćwiczeniach
Umiejętności:	**Iq_U01**	Wykorzystuje zdobytą wiedzę do rozstrzygania dylematów pojawiających się w pracy zawodowej	Kolokwium ustne, praca na ćwiczeniach
	Iq_U02	Potrafi wykorzystać elementarna wiedzę teoretyczną, i pozyskiwać dane do analizowania procesów i zjawisk zachodzących w stosunkach międzyludzkich	Kolokwium ustne, praca na ćwiczeniach
	Iq_U03	Posiada umiejętność przygotowania wystąpień ustnych w języku polskim i obcym, z wykorzystaniem podstawowych ujęć teoretycznych oraz źródeł, związanej ze szczegółowymi kwestiami dotyczącymi stosunków międzyludzkich	Kolokwium ustne, praca na ćwiczeniach
Kompetencje społeczne	**Iq_K01**	Dysponuje umiejętnościami interdyscyplinarnymi, komunikacyjnymi, społecznymi, interpersonalnymi i interkulturowymi, które umożliwiają mu podjęcie pracy w biznesie, instytucjach	Kolokwium ustne, praca na ćwiczeniach

		samorządowych, instytucjach rządowych, mediach i instytucjach międzynarodowych	

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
W01	Istota i funkcje komunikacji społecznej	2
W02	Negocjacje i mediacje	4
W03	Bariery w komunikacji	4
W04	Manipulacja a perswazja – wywieranie wpływu na innych	4
W05	Stres i trema	3
C01	Przygotowanie wystąpień publicznych	2
C02	Komunikacja werbalna i niewerbalna w praktyce	5
C03	Mobbing i molestowanie w pracy zawodowej	5
C04	Jak zostać dobrym liderem	5
C05	Asertywność	3

IV.	**KORELACJA EFEKTÓW UCZENIA SIĘ**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod efektu obszarowego*
W01	Iq_W01, Iq_W03	SIB2_W01, SIB2_W02	P7U_W, P7S_WG, P7S_WK
W02	Iq_W02, Iq_W03	SIB2_W01, SIB2_W02	P7U_W, P7S_WG, P7S_WK
W03	Iq_W02	SIB2_W01, SIB2_W02	P7U_W, P7S_WG, P7S_WK
W04	Iq_W01, Iq_W02, Iq_W03	SIB2_W01, SIB2_W02	P7U_W, P7S_WG, P7S_WK
W05	Iq_W01, Iq_W02, Iq_W03	SIB2_W01, SIB2_W02	P7U_W, P7S_WG, P7S_WK
C01	Iq_W01, Iq_U01, Iq_K01	SIB2_U01, SIB2_U03, SIB2_U04, SIB2_K01	P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK
C02	Iq_W02, Iq_U02, Iq_K01	SIB2_U01, SIB2_U03, SIB2_U04, SIB2_K01	P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK
C03	Iq_W03, Iq_U02, Iq_K01	SIB2_U01, SIB2_U03, SIB2_U04, SIB2_K01	P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK
C04	Iq_W01, Iq_U03, Iq_K01	SIB2_U01, SIB2_U03, SIB2_U04, SIB2_K01	P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK
C05	Iq_W01, Iq_U01, Iq_K01	SIB2_U01, SIB2_U03, SIB2_U04, SIB2_K01	P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK

V.	**NAKŁAD PRACY STUDENTA**			
Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**15**	**X**	**75**	**3**
Ćwiczenia	**20**			
Seminaria				
Konwersatoria				
Konsultacje (zaliczenie nieobecności, rozliczenie rygorów, poprawy)	**5**			
Przygotowanie do ćwiczeń	**X**	**15**		
Opanowanie informacji		**10**		
Przygotowanie do rozliczenia rygorów		**10**		
RAZEM	**40**	**35**		

VI.	**METODY DYDAKTYCZNE**
1.	Wykład z prezentacją multimedialną
2.	Ćwiczenia audytoryjne: dyskusja
3.	Ćwiczenia audytoryjne: praca indywidualna i w grupach

VII.	**FORMA ZALICZENIA PRZEDMIOTU**	
Rygor	*Kryteria składowe*	*Waga*
Zaliczenie	Kolokwium ustne	1,0

VIII.	**LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA**

OBOWIĄZKOWA	
1.	E. Griffin (przekł. O. i W. Kubińscy), *Podstawy komunikacji społecznej*, Gdańskie Wydawnictwo Psychologiczne, Gdańsk 2003
2.	Ht Rückle (tł. T. Soróbka), *Mowa ciała dla menedżerów*, ASTRUM, Wrocław, 2001
UZUPEŁNIAJĄCA	
1.	M. Leary, *Wywieranie wrażenia na innych. O sztuce Autoprezentacji*, Gdańskie Wydawnictwo Psychologiczne, Gdańsk 2010
2.	S. Bębas, J. Plis, J, Bednarek (red. nauk.,), *Komunikacja w cyberświecie*, Wyższa Szkoła Handlowa w Radomiu, Wyższa Szkoła Handlowa, Radom, 2012
3,	L. Gracz, K. Słupińska (red. naukowa), *Negocjacje i komunikacja: wybrane aspekty*, autorzy U. Chrąchol-Barczyk, L. Gracz, I. Ostrowska, G. Rosa, K. Słupińska. Wydanie I, Legionowo: Wydawnictwo edu-Libri, Kraków, 2018
IX.	**PROWADZĄCY PRZEDMIOT**
Stopień, Imię i nazwisko	dr Karol Słowi
adres e-mail	k.slowi@amw.gdynia.pl

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:	**Certyfikacja Systemu Zarządzania ISO/IEC 27001**	*Kod*:	**Csz**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Stacjonarne		
Kształcenie w zakresie:	Cyberbezpieczeństwo, Analiza danych i informatyka śledcza		
Profil:	Ogólnoakademicki		
Liczba ECTS:	6		
Semestr:	2		
Wymagania wstępne:	Podstawowa znajomość systemu zarządzania bezpieczeństwem informacyjnym w organizacji		
Język wykładowy:	Polski		
Cel przedmiotu:	**C01**	Zapoznanie studentów z wymaganiami Normy ISO 27001.	
	C02	Zapoznanie studentów z procesami realizowanymi w przedsiębiorstwie raz zarządzaniem informacjami stanowiącymi tajemnicę służbową	
	C03	Zapoznanie studentów z wdrożeniem, utrzymanie i doskonaleniem systemu zarządzania bezpieczeństwem informacji według wymagań Normy ISO 27001.	
	C04	Nauczenie studentów przygotowania podstawowych dokumentacji wymaganych do wdrożenia systemu zarzadzania bezpieczeństwem informacji według normy ISO 27001	

II.	**EFEKTY UCZENIA SIĘ**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Csz_W01**	Student rozumie zapisy związane z wymaganiami Normy ISO 27001	egzamin
	Csz_W02	Student zna procesy realizowane w organizacji	egzamin
	Csz_W03	Student potrafi wskazać wymagania jakie należy spełnić aby wdrożyć, utrzymać i doskonalić system bezpieczeństwa informacji według Normy ISO 27001.	egzamin
	Csz_W04	Student zna zasady wyboru jednostki certyfikującej celem certyfikacji wdrożonego systemu zarzadzania bezpieczeństwem informacji.	egzamin
Umiejętności:	**Csz_U01**	Student potrafi badać i oceniać stan systemu ochrony informacji	projekt
	Csz_U02	Student potrafi przeprowadzić analizę ryzyka i ocenę poziomu zagrożeń	projekt
	Csz_U03	Student potrafi od podstaw przygotować dokumentację niezbędną do wdrożenia i certyfikowania systemu bezpieczeństwa informacji	projekt
	Csz_U04	Student potrafi przygotować plan ciągłości działania	projekt

Kompetencje Społeczne:	**Csz_K01**	Student rozumie potrzebę ciągłego dokształcania się zawodowego i rozwoju osobistego. Dokonuje samooceny własnych kompetencji, wyznacza kierunki własnego rozwoju i kształcenia. Samodzielnie podejmuje refleksje dotyczące etyki w odniesieniu do wykonywanej pracy.	obserwacja na zajęciach
	Csz_K02	Potrafi prezentować swoje poglądy oraz umiejętnie argumentować ich słuszność, a także uznawać argumentację innych	obserwacja na zajęciach

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
W01	Wprowadzenie do przedmiotu. Struktura i podział zajęć. Zasady zaliczenia przedmiotu.	1
W02	Ogólne informacje dotyczące Normy ISO 27001	2
W03	Polityki bezpieczeństwa informacji	2
W04	Organizacja bezpieczeństwa informacji	2
W05	Urządzenia mobilne i telepraca	3
W06	Bezpieczeństwo zasobów ludzkich	3
W07	Zarzadzanie aktywami	3
W08	Kontrola dostępu do informacji i zasobu danych. Kryptografia oraz bezpieczeństwo fizyczne i środowiskowe	3
W09	Sprzęt i bezpieczna eksploatacja, ochrona przed szkodliwym oprogramowaniem	3
W10	Pozyskiwanie, rozwój i utrzymanie systemów	3
W11	Relacje z dostawcami, zarzadzanie incydentami, ciągłość bezpieczeństwa informacji oraz zgodność z wymogami prawnymi	3
W12	Egzamin zaliczeniowe.	2
C01	Wdrożenie, utrzymanie systemu Bezpieczeństwa informacji. Zapoznanie z obowiązującymi zasadami certyfikacji organizacji przez niezależne jednostki certyfikujące. Przydział projektów.	4
C02	Opracowywanie dokumentacji/ informacji związanych z kontekstem organizacji	4
C03	Opracowywanie dokumentacji/ informacji związanych z przywództwem w organizacji	4
C04	Opracowywanie dokumentacji/ informacji związanych z planowaniem w organizacji	4
C05	Opracowywanie dokumentacji/ informacji związanych ze wsparciem	4
C06	Opracowywanie dokumentacji/ informacji związanych z działaniami operacyjnymi	4
C07	Opracowywanie dokumentacji/ informacji związanych z oceną wyników	4
C08	Opracowywanie dokumentacji/ informacji związanych z doskonaleniem systemu	4
C09	Realizacja projektów indywidualnych.	4
C10	Oddawanie indywidualnych projektów przez studentów. Uwagi prowadzącego, poprawki studentów. Wystawianie ocen końcowych.	4

IV.	**KORELACJA EFEKTÓW KSZTAŁCENIA**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyki PRK*
W01	Csz_W01	-	

W02	Csz_W01, Csz_W02	SIB2_W01, SIB2_W03	P7U_W, P7S_WG, P7S_WK
W03	Csz_W01, Csz_W03	SIB2_W01, SIB2_W03	P7U_W, P7S_WG, P7S_WK
W04	Csz_W01, Csz_W03	SIB2_W01, SIB2_W03	P7U_W, P7S_WG, P7S_WK
W05	Csz_W01, Csz_W02	SIB2_W01, SIB2_W03	P7U_W, P7S_WG, P7S_WK
W06	Csz_W01, Csz_W03	SIB2_W01, SIB2_W03	P7U_W, P7S_WG, P7S_WK
W07	Csz_W01, Csz_W02	SIB2_W01, SIB2_W03	P7U_W, P7S_WG, P7S_WK
W08	Csz_W01, Csz_W04	SIB2_W01, SIB2_W03	P7U_W, P7S_WG, P7S_WK
W09	Csz_W01, Csz_W03	SIB2_W01, SIB2_W03	P7U_W, P7S_WG, P7S_WK
W10	Csz_W01, Csz_W04	SIB2_W01, SIB2_W03	P7U_W, P7S_WG, P7S_WK
W11	Csz_W01, Csz_W03	SIB2_W01, SIB2_W03	P7U_W, P7S_WG, P7S_WK
W12	Csz_W01, Csz_W04	SIB2_W01, SIB2_W03	P7U_W, P7S_WG, P7S_WK
C01	Csz_W01,Csz_U01	SIB2_U01, SIB2_U04, SIB2_U06, SIB2_K02, SIB2_K03, SIB2_K05	P7U_U, P7S_UW, P7S_UK, P7S_UO, P7U_K, P7S_KK, P7S_KO, P7S_KR
C02	Csz_U01, Csz_U02, Csz_U04	SIB2_U01, SIB2_U04, SIB2_U06, SIB2_K02, SIB2_K03, SIB2_K05	P7U_U, P7S_UW, P7S_UK, P7S_UO, P7U_K, P7S_KK, P7S_KO, P7S_KR
C03	Csz_U01, Csz_U03	SIB2_U01, SIB2_U04, SIB2_U06, SIB2_K02, SIB2_K03, SIB2_K05	P7U_U, P7S_UW, P7S_UK, P7S_UO, P7U_K, P7S_KK, P7S_KO, P7S_KR
C04	Csz_U01, Csz_U03	SIB2_U01, SIB2_U04, SIB2_U06, SIB2_K02, SIB2_K03, SIB2_K05	P7U_U, P7S_UW, P7S_UK, P7S_UO, P7U_K, P7S_KK, P7S_KO, P7S_KR
C05	Csz_U01, Csz_U02, Csz_U04	SIB2_U01, SIB2_U04, SIB2_U06, SIB2_K02, SIB2_K03, SIB2_K05	P7U_U, P7S_UW, P7S_UK, P7S_UO, P7U_K, P7S_KK, P7S_KO, P7S_KR
C06	Csz_U01, Csz_U03	SIB2_U01, SIB2_U04, SIB2_U06, SIB2_K02, SIB2_K03, SIB2_K05	P7U_U, P7S_UW, P7S_UK, P7S_UO, P7U_K, P7S_KK, P7S_KO, P7S_KR
C07	Csz_U01, Csz_U04	SIB2_U01, SIB2_U04, SIB2_U06, SIB2_K02, SIB2_K03, SIB2_K05	P7U_U, P7S_UW, P7S_UK, P7S_UO, P7U_K, P7S_KK, P7S_KO, P7S_KR
C08	Csz_U01, Csz_U02	SIB2_U01, SIB2_U04, SIB2_U06, SIB2_K02, SIB2_K03, SIB2_K05	P7U_U, P7S_UW, P7S_UK, P7S_UO, P7U_K, P7S_KK, P7S_KO, P7S_KR
C09	Csz_U01, Csz_K01, Csz_K02	SIB2_U01, SIB2_U04, SIB2_U06, SIB2_K02, SIB2_K03, SIB2_K05	P7U_U, P7S_UW, P7S_UK, P7S_UO, P7U_K, P7S_KK, P7S_KO, P7S_KR
C10	Csz_U01, Csz_K01, Csz_K02	SIB2_U01, SIB2_U04, SIB2_U06, SIB2_K02, SIB2_K03, SIB2_K05	P7U_U, P7S_UW, P7S_UK, 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	**30**		**151**	**6**
Ćwiczenia	**40**			
Seminaria				
Konwersatoria				
Konsultacje				
Rozliczenie rygorów przedmiotu	**6**			
Przygotowanie do ćwiczeń		**25**		
Opanowanie informacji		**25**		
Przygotowanie do rozliczenia rygorów		**25**		
RAZEM	**76**	**75**		

VI. METODY DYDAKTYCZNE

1.	Wykład z prezentacją multimedialną

2.	Praktyczne ćwiczenia z zakresu tworzenia dokumentacji, audytu oraz wdrażania procedur bezpieczeństwa	
VII.	**FORMA ZALICZENIA PRZEDMIOTU**	
Rygor	*Kryteria składowe*	*Waga*
Egzamin	ocena z ćwiczeń - sprawozdania	0,25
	ocena z egzaminu (materiał z wykładów)	0,75
VIII.	**LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA**	
	OBOWIĄZKOWA	
1.	*„PN-EN ISO/IEC 27001 Technika informacyjna Techniki bezpieczeństwa Systemy zarządzania bezpieczeństwem informacji Wymagania”* PKN 2017	
2.	„*Bezpieczeństwo Informacyjne nowe wyzwania”* K. Liderman PWN 2017	
	UZUPEŁNIAJĄCA	
1.	Dariusz Wróblewski, Zarządzanie ryzykiem – przegląd wybranych metodyk, Wydawnictwo CNBOP-PIB, 2015	
IX.	**PROWADZĄCY PRZEDMIOT**	
Stopień, Imię i nazwisko		
adres e-mail		

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:	**Sztuczna inteligencja**	*Kod*:	**Osi**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Stacjonarne		
Specjalność:	Cyberbezpieczeństwo, Analiza danych i informatyka śledcza		
Profil:	Ogólnoakademicki		
Liczba ECTS:	5		
Semestr:	2		
Wymagania wstępne:	-		
Język wykładowy:	Polski		
Cel przedmiotu:	**C01**	zapoznanie z założeniami sztucznej inteligencji oraz jej rozwoju na przestrzeni lat	
	C02	wykształcenie umiejętność projektowania prostych programów przy pomocy języka C/C++	
	C03	wykształcenie umiejętność projektowania prostych programów przy pomocy języka drabinkowego do realizacji zagadnień związanych z automatyką procesów technologicznych	
	C04	wykształcenie umiejętność projektowania zależności w ramach systemów ekspertowych do wspomagania podejmowania decyzji przez sztuczną inteligencję	

II.	**EFEKTY KSZTAŁCENIA**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Osi_W01**	Student zna i potrafi określić genezę sztucznej inteligencji oraz etapy jej rozwoju	kolokwium
	Osi_W02	Student zna i rozumie podstawy programowania będące podstawą do projektowania systemów bazujących na sprzężeniach zwrotnych	kolokwium
	Osi_W03	Student zna kluczowe techniki realizacji zagadnień związanych z automatyką procesów oraz rozumie stojącą za nimi logiką	kolokwium
	Osi_W04	Student potrafi zdefiniować logikę systemu ekspertowego będącego elementem systemu wspomagania podejmowania decyzji opartego na sztucznej inteligencji	kolokwium
	Osi_W05	Student jest świadomy konsekwencji poddawania się procesom oceny przez sztuczną inteligencję w ramach m.in. kampanii marketingowych	kolokwium
Umiejętności:	**Osi_U01**	Student potrafi obsługiwać skrypty uczenia maszynowego w środowisku Python 3	kolokwium
	Osi_U02	Student zna i potrafi zdefiniować rodzaje sieci neurowych wraz z ich zastosowaniem	kolokwium
Kompetencje społeczne	**Osi_K01**	Potrafi efektywnie pracować i współdziałać w różnych grupach eksperckich i strukturach roboczych.	obserwacja

	Osi_K02	W oparciu o uzyskaną teoretyczną wiedzę programową potrafi samodzielnie aktualizować i doskonalić swoją wiedzę i umiejętności praktyczne w zakresie wykorzystania sztucznej inteligencji w bezpieczeństwie	obserwacja

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
W01	Charakterystyka przedmiotu. Struktura i podział zajęć. Rygory i ustalenia organizacyjne	3
W02	Rozwój technologii komputerowych – od assemblera do sieci neuronowych	3
W03	Pojęcie sztucznej inteligencji oraz jej potencjał w realizacji powierzonych zadań	3
W04	Definiowanie logiki systemów ekspertowych	3
W05	Realizacja zadań wspomagania podejmowania decyzji przez systemy ekspertowe oraz mechanizmy uczenia maszynowego	3
L01	Realizacja zadań w ramach programowania C/C++	1
L02	Realizacja zadań w ramach projektowania systemów automatycznych	4
L03	Projektowanie logiki systemów ekspertowych	5
L04	Projektowanie skrytpów uczenia maszynowego	7
L05	Otwarta analiza sprawozdań z ćwiczeń	3

IV.	**KORELACJA EFEKTÓW KSZTAŁCENIA**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyki PRK*
W01	-	-	-
W02	Osi_W01, Osi_W02, Osi_W03, Osi_W04, Osi_W05	SIB2_W01, SIB2_W02, SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W03	Osi_W01, Osi_W02, Osi_W03, Osi_W04, Osi_W05	SIB2_W01, SIB2_W02, SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W04	Osi_W01, Osi_W02, Osi_W03, Osi_W04, Osi_W05	SIB2_W01, SIB2_W02, SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W05	Osi_W01, Osi_W02, Osi_W03, Osi_W04, Osi_W05	SIB2_W01, SIB2_W02, SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W06	Osi_W01, Osi_W02, Osi_W03, Osi_W04, Osi_W05	SIB2_W01, SIB2_W02, SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W07	Osi_W01, Osi_W02, Osi_W03, Osi_W04, Osi_W05	SIB2_W01, SIB2_W02, SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK

W08	Osi_W01, Osi_W02, Osi_W03, Osi_W04, Osi_W05	SIB2_W01, SIB2_W02, SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W09	Osi_W01, Osi_W02, Osi_W03, Osi_W04, Osi_W05	SIB2_W01, SIB2_W02, SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
L01	-		
L02	Osi_U01, Osi_U02, Osi_K01, Osi_K02	SIB2_U01, SIB2_U03, SIB2_U05, SIB2_U06, SIB2_K01, SIB2_K02	P7U_U, P7S_UW, P7S_UK, P7S_UO, P7U_K, P7S_KK
L03	Osi_U01, Osi_U02, Osi_K01, Osi_K02	SIB2_U01, SIB2_U03, SIB2_U05, SIB2_U06, SIB2_K01, SIB2_K02	P7U_U, P7S_UW, P7S_UK, P7S_UO, P7U_K, P7S_KK
L04	Osi_U01, Osi_U02, Osi_K01, Osi_K02	SIB2_U01, SIB2_U03, SIB2_U05, SIB2_U06, SIB2_K01, SIB2_K02	P7U_U, P7S_UW, P7S_UK, P7S_UO, P7U_K, P7S_KK
L05	Osi_U01, Osi_U02, Osi_K01, Osi_K02	SIB2_U01, SIB2_U03, SIB2_U05, SIB2_U06, SIB2_K01, SIB2_K02	P7U_U, P7S_UW, P7S_UK, P7S_UO, P7U_K, P7S_KK

V.	**NAKŁAD PRACY STUDENTA**			
Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**30**		**126**	**5**
Laboratoria	**30**			
Seminaria				
Konwersatoria				
Konsultacje (zaliczenie nieobecności, rozliczenie rygorów, poprawy)	**6**			
Przygotowanie do ćwiczeń		**20**		
Opanowanie informacji		**20**		
Przygotowanie do rozliczenia rygorów		**20**		
RAZEM	**66**	**60**		

VI.	**METODY DYDAKTYCZNE**
1.	Wykład z prezentacją multimedialną
2.	Ćwiczenia na stanowiskach komputerowych

VII.	**FORMA ZALICZENIA PRZEDMIOTU**	
Rygor	*Kryteria składowe*	*Waga*
Egzamin	ocena z ćwiczeń - test	0,3
	egzamin (materiał z wykładów)	0,7

VIII.	**LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA**
OBOWIĄZKOWA	
1.	K. Ficoń, *Sztuczna inteligencja nie tylko dla humanistów*, BelStudio, Warszawa 2013

2.	J. Arabas*, Wykłady z algorytmów ewolucyjnych*, Wydawnictwa Naukowo-Techniczne, Warszawa 2001
3.	D. E. Goldberg, *Algorytmy genetyczne i ich zastosowania*, Wydawnictwa NaukowoTechniczne, Warszawa 1995
UZUPEŁNIAJĄCA	
4.	T. Masters, *Sieci neuronowe w praktyce*, WNT 1996
5.	J. Korbicz, A, Obuchowicz, D. Uciński, *Sztuczne sieci neuronowe*, PLJ 1994
IX.	**PROWADZĄCY PRZEDMIOT**
Stopień, Imię i nazwisko	mgr inż. Karol Gazda, por. mar. mgr Łukasz Grzyb (ćwiczenia)
adres e-mail	k.gazda@amw.gdynia.pl, l.grzyb@amw.gdynia.pl

3.3. Karty przedmiotów modułu kształceniastudiów stacjonarnych w zakresie Cyberbezpieczeństwo – C

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 projektami informatycznymi**	*Kod*:	**Ozo**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Stacjonarne		
Kształcenie w zakresie:	Cyberbezpieczeństwo		
Profil:	Ogólnoakademicki		
Liczba ECTS:	5		
Semestr:	3		
Wymagania wstępne:	-----		
Język wykładowy:	Polski z terminologią angielską		
Cel przedmiotu:	**C01**	Zademonstrowanie istotności precyzyjnego przygotowywania wymagań i elastycznego podejścia do ich wdrażania	
	C02	Pokazanie istotności procesów komunikacyjnych w trakcie projektów IT	
	C05	Zademonstrowanie przydatności różnych narzędzi informatycznych w osiąganiu różnych celów	
II.	**EFEKTY UCZENIA SIĘ**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Ozo_W01**	Zna i rozumie w pogłębiony sposób wybrane fakty, teorie, metody oraz złożone zależności między nimi, także w powiązaniu z innymi dziedzinami różnorodne, złożone uwarunkowania i aksjologiczny kontekst prowadzonej działalności z zakresu teorii bezpieczeństwa, systemów informatycznych, systemów administracji publicznej, cyberbezpieczeństwa, analizy danych oraz zarządzania projektami	Sprawdzian
	Ozo_W02	Zna i rozumie podstawowe procesy zachodzące w cyklu życia projektów dotyczących systemów teleinformatycznych	Sprawdzian
	Ozo_W03	Zna i rozumie w pogłębiony sposób podstawowe zasady tworzenia różnych form przedsiębiorczości związane z wykorzystaniem systemów informacyjnych w bezpieczeństwie	Sprawdzian, Wykonanie projektu
Umiejętności:	**Ozo_U01**	Wykorzystuje posiadaną wiedzę z zakresu bezpieczeństwa, systemów informatycznych, systemów administracji publicznej, cyberbezpieczeństwa oraz analizy danych oraz formułować i rozwiązywać złożone i nietypowe problemy oraz innowacyjnie wykonywać zadania w warunkach nieprzewidywalnych poprzez:	Wykonanie projektu

		- 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; - przystosowanie istniejących lub opracowanie nowych metod i narzędzi	
	Ozo_U02	Komunikuje się z otoczeniem z użyciem specjalistycznej technologii	Wykonanie projektu
	Ozo_U03	Potrafi brać udział w debacie z zakresu wykorzystania systemów informacyjnych w bezpieczeństwie - przedstawia i ocenia różne opinie i stanowiska oraz dyskutuje o nich	Prezentacja projektu, Wykonanie projektu
	Ozo_U04	Planuje i organizuje pracę indywidualną oraz kieruje pracą zespołu w ramach realizacji zadań	Wykorzystywanie narzędzi, Wykonanie projektu
Kompetencje społeczne:	**Ozo_K01**	Krytycznie ocenia posiadaną wiedzę i odbierane treści z zakresu teorii bezpieczeństwa, systemów informatycznych, systemów administracji publicznej, cyberbezpieczeństwa, analizy danych oraz zarządzania projektami	Wykonanie projektu, Sprawdzian
	Ozo_K02	Uznaje znaczenie wiedzy w rozwiązywaniu problemów badawczych i praktycznych oraz zasięga opinii ekspertów w przypadku trudności z samodzielnym rozwiązywaniem problemów dotyczących wykorzystania systemów informacyjnych w bezpieczeństwie	Wykonanie projektu, Praca grupowa
	Ozo_K03	Inicjuje i uczestniczy konstruktywnie w przygotowaniu projektów społecznych (politycznych, gospodarczych, obywatelskich), uwzględniając ich różne aspekty, planując i zarządzając przy tym czasem własnym oraz czasem w przedsięwzięciach zespołowych	Wykonanie projektu
	Ozo_K04	Planuje przedsięwzięcia własne i zespołów, z uwzględnieniem zmieniających się potrzeb społecznych, rozwiązuje problemy organizacyjne i inne o różnym poziomie złożoności	Wykonanie projektu, Wykorzystywanie narzędzi
	Ozo_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	Praca grupowa, Wykonanie projektu

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
W01	Organizacja zajęć	1
W02	Cele zarządzania projektami	2
W03	Procesy zarządzania projektami	4
W04	Tematy w ramach zarządzania projektami	4

W05	Zasady w zarządzaniu projektami	2
W06	Role w zarządzaniu projektami	2
W07	Wymagania dla projektów IT	2
W08	Metody prowadzenia projektów	3
W09	Wspieranie zarządzania projektami narzędziami IT	2
W10	Kończenie projektu	1
W11	Sprawdzian	2
C01	Organizacja zajęć	1
C02	Instalacja środowisk, rozpoznanie narzędzi	3
C03	Zarządzanie przebiegiem ćwiczeń (Kanban)	1
C04	Generowanie wymagań funkcjonalnych i bezpieczeństwa	3
C05	Identyfikacja ról	2
C06	Definiowanie wartości biznesowej	4
C07	2 Prezentacje śród-semestralne	3
C08	Rozpisanie kamieni milowych i zadań	3
C09	Opis artefaktów projektu	2
C10	Identyfikacja ryzyk projektowych	1
C11	Identyfikacja ryzyk produktowych	2
C12	Opis produktu (wymagań biznesowych)	3
C13	Przygotowanie makiety interface użytkownika	1
C14	Schemat logiczny architektury rozwiązania	2
C15	Plakat reklamowy	1
C16	Prezentacje zaliczeniowe	3

IV.	**KORELACJA EFEKTÓW UCZENIA SIĘ**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyk PRK*
W01	Ozo_W01, Ozo_W02, Ozo_W03, Ozo_K03, Ozo_K04, Ozo_K05	SIB2_W01, SIB2_W02, SIB2_W04, SIB2_K04, SIB2_K05	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KR
W02	Ozo_W01, Ozo_W02, Ozo_W03, Ozo_K05	SIB2_W01, SIB2_W02, SIB2_W04, SIB2_K04, SIB2_K05	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KR
W03	Ozo_W01, Ozo_W02	SIB2_W01, SIB2_W02	P7U_W, P7S_WG, P7S_WK,
W04	Ozo_W01, Ozo_W02, Ozo_W03, Ozo_U04, Ozo_K02	SIB2_W01, SIB2_W02, SIB2_W04, SIB2_U06, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UO, P7U_K, P7S_KK
W05	Ozo_W01, Ozo_W02, Ozo_W03, Ozo_U04, Ozo_K02, Ozo_K05	SIB2_W01, SIB2_W02, SIB2_W04, SIB2_U06, SIB2_K02, SIB2_K05	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UO, P7U_K, P7S_KK, P7S_KR
W06	Ozo_W01, Ozo_W02, Ozo_U04, Ozo_K02, Ozo_K05	SIB2_W01, SIB2_W02, SIB2_U06, SIB2_K02, SIB2_K05	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UO, P7U_K, P7S_KK, P7S_KR
W07	Ozo_W01, Ozo_W02, Ozo_W03	SIB2_W01, SIB2_W02, SIB2_W04	P7U_W, P7S_WG, P7S_WK
W08	Ozo_W01, Ozo_W02, Ozo_W03, Ozo_U04, Ozo_K05	SIB2_W01, SIB2_W02, SIB2_U06, SIB2_K05	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UO, P7U_K, P7S_KR
W09	Ozo_W01, Ozo_W02, Ozo_U02, Ozo_U04, Ozo_K05	SIB2_W01, SIB2_W02, SIB2_U03, SIB2_U06, SIB2_K05	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UK, P7S_UO, P7U_K, P7S_KR
W10	Ozo_W01, Ozo_W02, Ozo_W03, Ozo_K03, Ozo_K04, Ozo_K05	SIB2_W01, SIB2_W02, SIB2_W04, SIB2_K03, SIB2_K04, SIB2_K05	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KO, P7S_KR

W11	Ozo_W01, Ozo_W02, Ozo_W03, Ozo_U01, Ozo_K05	SIB2_W01, SIB2_W02, SIB2_W04, SIB2_U01, SIB2_K05	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7U_K, P7S_KR
C01	Ozo_W01, Ozo_W02, Ozo_U01, Ozo_U02, Ozo_K03, Ozo_K04	SIB2_W01, SIB2_W02, SIB2_U01, SIB2_U03, SIB2_K03, SIB2_K04	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KO, P7S_KR
C02	Ozo_W01, Ozo_W02, Ozo_U01, Ozo_U02	SIB2_W01, SIB2_W02, SIB2_U01, SIB2_U03	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7S_UK
C03	Ozo_W01, Ozo_W02, Ozo_W03, Ozo_U01, Ozo_U02, Ozo_U04, Ozo_K03, Ozo_K04, Ozo_K05	SIB2_W01, SIB2_W02, SIB2_W04, SIB2_U01, SIB2_U03, SIB2_U06, SIB2_K04, SIB2_K05	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7S_UK, P7S_UO, P7U_K, P7S_KR
C04	Ozo_W01, Ozo_W02, Ozo_W03, Ozo_U01, Ozo_U02, Ozo_U03, Ozo_K01	SIB2_W01, SIB2_W02, SIB2_W04, SIB2_U01, SIB2_U03, SIB2_U04, SIB2_K01	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK
C05	Ozo_W01, Ozo_W02, Ozo_U01, Ozo_U02, Ozo_U04, Ozo_K02, Ozo_K05	SIB2_W01, SIB2_W02, SIB2_U01, SIB2_U03, SIB2_U06, SIB2_K02, SIB2_K05	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7S_UK, P7S_UO, P7U_K, P7S_KK, P7S_KR
C06	Ozo_W01, Ozo_W02, Ozo_W03, Ozo_U01, Ozo_U02, Ozo_U03, Ozo_K01, Ozo_K05	SIB2_W01, SIB2_W02, SIB2_W04, SIB2_U01, SIB2_U03, SIB2_U04, SIB2_K01, SIB2_K05	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK, P7S_KR
C07	Ozo_W01, Ozo_W02, Ozo_W03, Ozo_U02, Ozo_U03, Ozo_U04, Ozo_K01	SIB2_W01, SIB2_W02, SIB2_W04, SIB2_U03, SIB2_U04, SIB2_U06, SIB2_K01	P7U_W, P7S_WG, P7S_WK, P7U_U P7S_UK, P7S_UO, P7U_K, P7S_KK
C08	Ozo_W01, Ozo_W02, Ozo_W03, Ozo_U01, Ozo_U02, Ozo_U03, Ozo_U04, Ozo_K02	SIB2_W01, SIB2_W02, SIB2_W04, SIB2_U01, SIB2_U03, SIB2_U04, SIB2_U06, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7S_UK, P7S_UO, P7U_K P7S_KK
C09	Ozo_W01, Ozo_W02, Ozo_W03, Ozo_U01, Ozo_U02, Ozo_U03	SIB2_W01, SIB2_W02, SIB2_W04, SIB2_U01, SIB2_U03, SIB2_U04,	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7S_UK,
C10	Ozo_W01, Ozo_W02, Ozo_W03, Ozo_U01, Ozo_U02, Ozo_U03, Ozo_K01	SIB2_W01, SIB2_W02, SIB2_W04, SIB2_U01, SIB2_U03, SIB2_U04, SIB2_K01	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK
C11	Ozo_W01, Ozo_W02, Ozo_W03, Ozo_U01, Ozo_U02, Ozo_U03, Ozo_K01, Ozo_K02, Ozo_K05	SIB2_W01, SIB2_W02, SIB2_W04, SIB2_U01, SIB2_U03, SIB2_U04, SIB2_K01, SIB2_K02, SIB2_K05	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK, P7S_KR
C12	Ozo_W01, Ozo_W02, Ozo_W03, Ozo_U01, Ozo_U02, Ozo_U03, Ozo_K05	SIB2_W01, SIB2_W02, SIB2_W04, SIB2_U01, SIB2_U03, SIB2_U04, SIB2_K05	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KR
C13	Ozo_W01, Ozo_W02, Ozo_W03, Ozo_U01, Ozo_U02	SIB2_W01, SIB2_W02, SIB2_W04, SIB2_U01, SIB2_U03,	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7S_UK,
C14	Ozo_W01, Ozo_W02, Ozo_W03, Ozo_U01, Ozo_U02, Ozo_U03	SIB2_W01, SIB2_W02, SIB2_W04, SIB2_U01, SIB2_U03, SIB2_U04,	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7S_UK,
C15	Ozo_W01, Ozo_W02, Ozo_W03, Ozo_U01, Ozo_U02	SIB2_W01, SIB2_W02, SIB2_W04, SIB2_U01, SIB2_U03,	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7S_UK,
C16	Ozo_W01, Ozo_W02, Ozo_W03, Ozo_U01, Ozo_U02, Ozo_U03, Ozo_K01, Ozo_K03, Ozo_K04	SIB2_W01, SIB2_W02, SIB2_W04, SIB2_U01, SIB2_U03, SIB2_U04, SIB2_K01, SIB2_K03, SIB2_K04	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7S_UK, 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	**25**	**X**	**126**	**5**
Ćwiczenia	**35**			
Seminaria	**0**			
Konwersatoria	**0**			
Konsultacje (zaliczenie nieobecności, rozliczenie rygorów, poprawy)	**6**			
Przygotowanie do ćwiczeń	**X**	**15**		
Opanowanie informacji		**25**		
Przygotowanie do rozliczenia rygorów		**20**		
RAZEM	**66**	**60**		

VI.	**METODY DYDAKTYCZNE**
1.	Wykład z prezentacją multimedialną
2.	Ćwiczenia z wykorzystywaniem narzędzi online
3.	Ćwiczenia z wykorzystywaniem narzędzi offline
4.	Praca w grupach
5.	Prezentacje

VII.	**FORMA ZALICZENIA PRZEDMIOTU**	
Rygor	*Kryteria składowe*	*Waga*
Egzamin	Egzamin	0,4
	Ocena z ćwiczeń	0,4
	Praca zaliczeniowa	0,2

VIII.	**LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA**
	OBOWIĄZKOWA
1.	Flasiński M.; Zarządzanie projektami informatycznymi
2.	Jasińska K., Szapiro T., Zarządzanie procesami realizacji projektów w sektorze ICT
	UZUPEŁNIAJĄCA
1.	Managing Successful Projects with PRINCE2® 2017 Edition
2.	K. Gene Projekt Jednorożec. Powieść o szansie w epoce przewrotów cyfrowych
3.	K. Gene Projekt Fenix. Powieść o IT, modelu DevOps

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

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:	**Akredytacja bezpieczeństwa teleinformatycznego**	*Kod*:	**Ljb**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Stacjonarne		
Kształcenie w zakresie:	Cyberbezpieczeństwo		
Profil:	Ogólnoakademicki		
Liczba ECTS:	3		
Semestr:	3		
Wymagania wstępne:	Brak		
Język wykładowy:	Polski		
Cel przedmiotu:	**C01**	Zapoznanie z celami i przeznaczeniem akredytacji bezpieczeństwa teleinformatycznego.	
	C02	Zapoznanie z przepisami definiującymi zasady akredytacji bezpieczeństwa.	
	C03	Przybliżenie sposobów realizacji procesu akredytacji bezpieczeństwa teleinformatycznego.	

II.	**EFEKTY UCZENIA SIĘ**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Ljb_W01**	Student zna i rozumie zasady wykonywania dokumentacji bezpieczeństwa teleinformatycznego	Egzamin
	Ljb_W02	Student zna mechanizmy bezpieczeństwa wykorzystywane w systemach teleinformatycznych	Egzamin
	Ljb_W03	Student zna zasady akredytacji bezpieczeństwa teleinformatycznego oraz szacowania ryzyka.	Egzamin
Umiejętności:	**Ljb_U01**	Student potrafi wykorzystać znajomość języka angielskiego w zakresie słownictwa specjalistycznego na poziomie gwarantującym poprawne posługiwanie się dokumentacją techniczną.	Egzamin; zadania
	Ljb_U02	Student potrafi wykonać szacowanie ryzyka dla systemów teleinformatycznych oraz zna podstawy akredytacji bezpieczeństwa.	Egzamin; zadania
Kompetencje społeczne:	**Ljb_K01**	Student dostrzega znaczenie wiedzy w zakresie rozwiązywania problemów zabezpieczenia technicznego i wprowadzania nowych rozwiązań oraz docenia znaczenie samodzielnego poszerzania wiedzy i umiejętności	Praca w grupach

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
W01	Wprowadzenie do akredytacji bezpieczeństwa teleinformatycznego	2
W02	Zarządzanie ryzykiem	4
W03	Szczególne Wymagania Bezpieczeństwa	2
W04	Procedury Bezpiecznej Eksploatacji	2
W05	Analiza Ryzyka	2
W06	Zasady akredytacji niejawnych systemów teleinformatycznych	2

W07	Rola i funkcje krajowej władzy bezpieczeństwa	2
W08	Zadania i zakres obowiązków poszczególnych osób funkcyjnych w procesie akredytacji bezpieczeństwa teleinformatycznego.	4
C01	Metodyka CRAMM	2
C02	Charakterystyka Systemu Teleinformatycznego	3
C03	Zarządzanie Systemem Teleinformatycznym	2
C04	Bezpieczeństwo osobowe	3
C05	Bezpieczeństwo urządzeń	2
C06	Bezpieczeństwo oprogramowania	3
C07	Ciągłość działania	2
C08	Monitorowanie i audyt	3
C09	Zarządzanie nośnikami danych	2
C10	Plany awaryjne	3

IV.	**KORELACJA EFEKTÓW UCZENIA SIĘ**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyk PRK*
W01	Ljb_W01, Ljb_W02, Ljb_W03, Ljb_K01	SIB2_W01, SIB2_W02, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W02	Ljb_W01, Ljb_W02, Ljb_W03, Ljb_K01	SIB2_W01, SIB2_W02, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W03	Ljb_W01, Ljb_W02, Ljb_W03, Ljb_K01	SIB2_W01, SIB2_W02, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W04	Ljb_W01, Ljb_W02, Ljb_W03, Ljb_K01	SIB2_W01, SIB2_W02, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W05	Ljb_W01, Ljb_W02, Ljb_W03, Ljb_K01	SIB2_W01, SIB2_W02, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W06	Ljb_W01, Ljb_W02, Ljb_W03, Ljb_K01	SIB2_W01, SIB2_W02, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W07	Ljb_W01, Ljb_W02, Ljb_W03, Ljb_K01	SIB2_W01, SIB2_W02, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W08	Ljb_W01, Ljb_W02, Ljb_W03, Ljb_K01	SIB2_W01, SIB2_W02, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
C01	Ljb_W03, Ljb_U01, Ljb_U02, Ljb_K01	SIB2_W01, SIB2_U01, SIB2_U05, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK
C02	Ljb_W03, Ljb_U01, Ljb_U02, Ljb_K01	SIB2_W01, SIB2_U01, SIB2_U05, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK
C03	Ljb_W03, Ljb_U01, Ljb_U02, Ljb_K01	SIB2_W01, SIB2_U01, SIB2_U05, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK
C04	Ljb_W03, Ljb_U01, Ljb_U02, Ljb_K01	SIB2_W01, SIB2_U01, SIB2_U05, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK
C05	Ljb_W03, Ljb_U01, Ljb_U02, Ljb_K01	SIB2_W01, SIB2_U01, SIB2_U05, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK
C06	Ljb_W03, Ljb_U01, Ljb_U02, Ljb_K01	SIB2_W01, SIB2_U01, SIB2_U05, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK
C07	Ljb_W03, Ljb_U01, Ljb_U02, Ljb_K01	SIB2_W01, SIB2_U01, SIB2_U05, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK
C08	Ljb_W03, Ljb_U01, Ljb_U02, Ljb_K01	SIB2_W01, SIB2_U01, SIB2_U05, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK

C09	Ljb_W03, Ljb_U01, Ljb_U02, Ljb_K01	SIB2_W01, SIB2_U01, SIB2_U05, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK
C10	Ljb_W03, Ljb_U01, Ljb_U02, Ljb_K01	SIB2_W01, SIB2_U01, SIB2_U05, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK

V. NAKŁAD PRACY STUDENTA

Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**20**		**80**	**3**
Ćwiczenia	**25**			
Seminaria				
Konwersatoria				
Konsultacje	**5**			
Rozliczenie rygorów przedmiotu				
Przygotowanie do ćwiczeń		**10**		
Wykonanie zadań domowych		**10**		
Przygotowanie do rozliczenia rygorów		**10**		
RAZEM	**50**	**30**		

VI. METODY DYDAKTYCZNE

1. Wykłady z prezentacjami multimedialnymi
2. Ćwiczenia na stanowiskach komputerowych

VII. FORMA ZALICZENIA PRZEDMIOTU

Rygor	*Kryteria składowe*	*Waga*
Zaliczenie	Egzamin	0,8
	Ocena z ćwiczeń	0,2

VIII. LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

OBOWIĄZKOWA

1. Krzysztof Liderman, Bezpieczeństwo teleinformatyczne Polityka bezpieczeństwa i ochrony informacji, WSISiZ, 2003.
2. Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. 2010 nr 182 poz. 1228)
3. Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz.U.2011.159.948)
4. Marek Anzel "Szacowanie ryzyka oraz zarządzanie ryzykiem w świetle nowej ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych - przykład metody analizy ryzyka opartej na gotowych macierzach"

UZUPEŁNIAJĄCA

1. Liderman Krzysztof, Bezpieczeństwo informacyjne, PWN , Warszawa 2012.

IX. PROWADZĄCY PRZEDMIOT

Stopień, Imię i nazwisko	mgr Krzysztof GAWIOR
adres e-mail	k.gawior@amw.gdynia.pl

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:	**Testy penetracyjne**	*Kod*:	**Mte**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Stacjonarne		
Specjalność:	Cyberbezpieczeństwo		
Profil:	Ogólnoakademicki		
Liczba ECTS:	4		
Semestr:	3		
Wymagania wstępne:	brak		
Język wykładowy:	Polski z terminologią angielską		
Cel przedmiotu:	**C01**	Zapoznanie studentów z metodyką prowadzenia testów penetracyjnych systemów i usług informatycznych.	
	C02	Pozyskanie umiejętności związanych z wykrywaniem podatności w systemach teleinformatycznych.	
	C03	Pozyskanie umiejętności przygotowania oraz przeprowadzenia testu penetracyjnego w systemie Windows oraz systemie Linux.	

II.	**EFEKTY KSZTAŁCENIA**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Mte_ W01**	Zna i rozumie w pogłębiony sposób wybrane fakty, teorie, metody oraz złożone zależności między nimi, także w powiązaniu z innymi dziedzinami różnorodne, złożone uwarunkowania i aksjologiczny kontekst prowadzonej działalności z zakresu teorii bezpieczeństwa, cyberbezpieczeństwa oraz analizy danych i informatyki śledczej. Zna zasady i metody prowadzenia testów penetracyjnych w sieciach komputerowych.	Pytania sprawdzające podczas zajęć. Kolokwium.
	Mte_ W02	Zna i rozumie w pogłębiony sposób zagadnienia związane z bezpieczeństwem informacji oraz wykorzystaniem technologii informacyjnych. Zna zasady i metody prowadzenia testów pod kątem wyszukiwania podatności w systemach i sieciach teleinformatycznych	Rozwiązanie zadań problemowych
Umiejętności:	**Mte_ U01**	Potrafi wykorzystać posiadaną wiedzę z zakresu bezpieczeństwa, cyberbezpieczeństwa oraz formułować i rozwiązywać złożone i nietypowe problemy. Potrafi przygotować oraz przeprowadzić testy penetracyjne w sieciach komputerowych.	Przygotowanie sprawozdania. Kolokwium.
	Mte U02	Potrafi brać udział w debacie z zakresu wykorzystania systemów informacyjnych w bezpieczeństwie - przedstawiać i oceniać różne opinie i stanowiska oraz dyskutować o nich. Potrafi przeprowadzić testy penetracyjne w systemach i sieciach teleinformatycznych pod kątem wyszukiwania podatności z uwzględnieniem właściwej metody ich realizacji.	Przygotowanie sprawozdania. Kolokwium.

	Mte_U03	Potrafi posługiwać się językiem obcym na poziomie B2 Europejskiego Systemu Opisu Kształcenia Językowego ze szczególnym uwzględnienie specjalistycznej terminologii z zakresu wykorzystania systemów informacyjnych w bezpieczeństwie.	Wykonanie ćwiczenia
	Mte_U04	Potrafi samodzielnie planować i realizować własne uczenie się przez całe życie i ukierunkowywać innych w tym zakresie.	Przygotowanie sprawozdania. Kolokwium.
Kompetencje społeczne:	**Mte_K01**	Krytycznie ocenia posiadaną wiedzę i odbierane treści z zakresu teorii bezpieczeństwa, cyberbezpieczeństw oraz analizy danych i informatyki śledczej.	Przygotowanie do zajęć
	Mte_K02	Uznaje znaczenie wiedzy w rozwiązywaniu problemów badawczych i praktycznych oraz zasięga opinii ekspertów w przypadku trudności z samodzielnych rozwiazywaniem problemów dotyczących wykorzystania systemów informacyjnych w bezpieczeństwie	Przygotowanie do zajęć

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
W01	Zajęcia organizacyjne. Wprowadzenie do przedmiotu. Sprawy organizacyjne.	10 min
W02	System teleinformatyczny: Podstawowe definicje; Atrybuty bezpieczeństwa; Bezpieczeństwo systemu teleinformatycznego.	2
W03	Polityka bezpieczeństwa: Podstawowe definicje; Elementy bezpieczeństwa; Zarządzanie bezpieczeństwem; Przykładowa polityka bezpieczeństwa.	2
W04	Metodyka testów penetracyjnych: Definicja testów penetracyjnych; Rodzaje i opis metodyk (OSSTMM, PTES, NIST800-115, Metasploit, Core Impact, OWASP Web Security Testing Guide, Testy penetracyjne ukierunkowane na cel).	4
W05	Etapy testów penetracyjnych: Czynności wstępne; Rozpoznanie pasywne.	2
W06	Etapy testów penetracyjnych: Aspekty prawne; Rozpoznanie aktywne.	4
W07	Etapy testów penetracyjnych: Faza penetracji / ataku;	2
W08	Etapy testów penetracyjnych: Uzyskanie dostępu – eksploracja środowiska.	2
W09	Etapy testów penetracyjnych: Przygotowanie raportu.	2
L01	Realizacja etapów testów penetracyjnych: Czynności wstępne; Rozpoznanie pasywne.	4
L02	Realizacja etapów testów penetracyjnych: Aspekty prawne; Rozpoznanie aktywne.	4
L03	Realizacja etapów testów penetracyjnych: Faza penetracji / ataku;	4
L04	Realizacja etapów testów penetracyjnych: Uzyskanie dostępu – eksploracja środowiska.	4
L05	Realizacja etapów testów penetracyjnych: Przygotowanie raportu.	4
C01	Analiza pakietów ruchu sieciowego z wykorzystaniem programu WireShark – analizy przypadków	15

IV.	**KORELACJA EFEKTÓW KSZTAŁCENIA**		
Forma	*Kod efektu przedmiotu*	*Kod symbolu*	*Kod charakterystyk PRK*
W01	Mte_W01, Mte_W02	SIB2_W01, SIB2_W02,	P7U_W, P7S_WG, P7S_WK,

	Mte_K01, Mte_K02	SIB2_K01, SIB2_K02	P7U_K, P7S_KK
W02	Mte_W01, Mte_W02 Mte_K01, Mte_K02	SIB2_W01, SIB2_W02, SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W03	Mte_W01, Mte_W02 Mte_K01, Mte_K02	SIB2_W01, SIB2_W02, SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W04	Mte_W01, Mte_W02 Mte_K01, Mte_K02	SIB2_W01, SIB2_W02, SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W05	Mte_W01, Mte_W02 Mte_K01, Mte_K02	SIB2_W01, SIB2_W02, SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W06	Mte_W01, Mte_W02 Mte_K01, Mte_K02	SIB2_W01, SIB2_W02, SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W07	Mte_W01, Mte_W02 Mte_K01, Mte_K02	SIB2_W01, SIB2_W02, SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W08	Mte_W01, Mte_W02 Mte_K01, Mte_K02	SIB2_W01, SIB2_W02, SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W09	Mte_W01, Mte_W02 Mte_K01, Mte_K02	SIB2_W01, SIB2_W02, SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
L01	Mte_W01, Mte_W02 Mte_U01, Mte_U02, Mte_U04, Mte_U04, Mte_K01, Mte_K02	SIB2_W01, SIB2_W02, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07, SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK P7U_U, P7S_UW, P7S_UK, P7S_UU P7U_K P7S_KK
L02	Mte_W01, Mte_W02 Mte_U01, Mte_U02, Mte_U04, Mte_U04, Mte_K01, Mte_K02	SIB2_W01, SIB2_W02, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07, SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK P7U_U, P7S_UW, P7S_UK, P7S_UU P7U_K P7S_KK
L03	Mte_W01, Mte_W02 Mte_U01, Mte_U02, Mte_U04, Mte_U04, Mte_K01, Mte_K02	SIB2_W01, SIB2_W02, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07, SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK P7U_U, P7S_UW, P7S_UK, P7S_UU P7U_K P7S_KK
L04	Mte_W01, Mte_W02 Mte_U01, Mte_U02, Mte_U04, Mte_U04, Mte_K01, Mte_K02	SIB2_W01, SIB2_W02, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07, SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK P7U_U, P7S_UW, P7S_UK, P7S_UU P7U_K P7S_KK
L05	Mte_W01, Mte_W02 Mte_U01, Mte_U02, Mte_U04, Mte_U04, Mte_K01, Mte_K02	SIB2_W01, SIB2_W02, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07, SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK P7U_U, P7S_UW, P7S_UK, P7S_UU P7U_K P7S_KK
C01	Mte_W01, Mte_W02 Mte_U01, Mte_U02, Mte_U04, Mte_U04, Mte_K01, Mte_K02	SIB2_W01, SIB2_W02, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07, SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK P7U_U, P7S_UW, P7S_UK, P7S_UU P7U_K P7S_KK

V.	**NAKŁAD PRACY STUDENTA**			
Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**20**		**110**	**4**
Laboratorium	**20**			
Ćwiczenia	**15**			
Konwersatoria				
Konsultacje	**3**			
Rozliczenie rygorów przedmiotu	**2**			
Przygotowanie do ćwiczeń i laboratorium	**x**	**15**		
Opanowanie informacji		**15**		
Przygotowanie do rozliczenia rygorów		**20**		
RAZEM	**60**	**50**		

VI.	METODY DYDAKTYCZNE	
1.	Wykład z prezentacją multimedialną	
2.	Praca przy stanowisku komputerowym	
3.	Rozwiązywanie zadań problemowych	
4.	Studiowanie literatury	
VII.	**FORMA ZALICZENIA PRZEDMIOTU**	
Rygor	*Kryteria składowe*	*Waga*
Zaliczenie	Ocena za aktywność na zajęciach	0,2
	Ocena z kolokwium	0,8
Zaliczenie	Aktywność na zajęciach laboratoryjnych	0,2
	Sprawozdania z laboratorium	0,8

VIII.	LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA
	OBOWIĄZKOWA
1.	Białas A., Bezpieczeństwo informacji i usług, Wydawnictwo Naukowo-Techniczne, Warszawa 2007;
2.	Khawaja G. Kali Linux i testy penetracyjne. Biblia. Wydawnictwo Helion, Gliwice 2022;
3.	Velu V. K., Kali Linux i zaawansowane testy penetracyjne. Zostań ekspertem cyberbezpieczeństwa za pomocą Metasploit, Nmap, Wireshark i Burp Suite. Wydanie IV., Wydawnictwo Helion, Gliwice 2023;
4.	Georgia W., Bezpieczny system w praktyce, Wyższa szkoła hackingu i testy penetracyjne, Wydawnictwo Helion, 2015;
5.	Kim P., Podręcznik pentestera. Bezpieczeństwo systemów informatycznych, Wydawnictwo Helion, Gliwice 2014;
6.	Tanner N. H., Blue Team i cyberbezpieczeństwo. Zestaw narzędzi dla specjalistów od zabezpieczenia sieci. Wydawnictwo Helion, Gliwice 2021;
	UZUPEŁNIAJĄCA
1.	Ustawa z dnia 16 lipca 2004r. Prawo telekomunikacyjne (Dz.U. 2004 Nr 171 poz. 1800, tekst ujednolicony);
2.	Ustawa z dnia 18 lipca 2002r. o świadczeniu usług drogą elektroniczną (Dz.U. 2002 Nr 144 poz. 1204, z późn. zm.);
3.	Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2018 r. poz. 1560, z 2019 r. poz. 2020, 2248);
4.	Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (Dz.U. 2020 poz. 1444, tekst jednolity);
5.	Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2017 poz. 2247, tekst jednolity);
6.	Rozporządzenie Rady Ministrów z dnia 11 września 2018 r. w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych;
7.	PN-13335-1, Technika informatyczna - Wytyczne do zarządzania bezpieczeństwem systemów informatycznych - Pojęcia i modele bezpieczeństwa systemów informatycznych, 1999;
8.	NIST National Institute of Standard and Technology - Special Publication 800-37, Revision 2. Risk Management Framework for Information Systems and Organizations, grudzień 2018;
9.	OSSTMM 3 The Open Source Security Testing Methodology Manual. Contemporary Security Testing and Analysis, Pete Herzog, ISECOM, grudzień 2010;

10.	Technical Guide to Information Security Testing and Assessment (SP 800-115). Recommendations of the National Institute of Standards and Technology, wrzesień 2008;	
11.	PTES Penetration Testing Execution Standard, http://www.pentest-standard.org;	
12.	OWASP The Open Web Application Security Project, https://owasp.org/;	
IX.	**PROWADZĄCY PRZEDMIOT**	
Stopień, Imię i nazwisko		kmdr por. dr inż. Adam Stojałowski
adres e-mail		a.stojalowski@amw.gdynia.pl

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:	**Bezpieczeństwo sieci komputerowych i bezprzewodowych**	*Kod*:	**Oxk**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Stacjonarne		
Kształcenie w zakresie:	Cyberbezpieczeństwo		
Profil:	Ogólnoakademicki		
Liczba ECTS:	5		
Semestr:	3		
Wymagania wstępne:	Brak		
Język wykładowy:	Polski		
Cel przedmiotu:	**C01**	Zapoznanie studentów z zasadami działania sieci komputerowych, ich klasyfikacją i charakterystyką oraz urządzeniami sieciowymi i wykorzystywanymi mediami transmisyjnymi.	
	C02	Zapoznanie studentów z warstwową architekturą sieci oraz protokołami sieciowymi wykorzystywanymi do komunikacji hostów na poziomie poszczególnych warstw.	
	C03	Wykształcenie umiejętności podstawowej konfiguracji urządzeń sieciowych dla realizacji komunikacji z wykorzystaniem sieci komputerowej, obserwacji i analizy działania sieci oraz ruchu sieciowego, diagnozowania podstawowych nieprawidłowości w działaniu sieci komputerowych	

II.	**EFEKTY UCZENIA SIĘ**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Oxk_W01**	Student zna podstawowe urządzenia i standardy sieciowe oraz ich rolę w transmisji danych w sieciach lokalnych i rozległych o różnych topologiach.	Egzamin
	Oxk_W02	Student zna podstawowe modele warstwowe sieci oraz role poszczególne warstwy w procesie transmisji danych między hostami sieci.	Egzamin
	Oxk_W03	Student zna podstawowe protokoły transmisyjne i ich przyporządkowanie do warstwy na poziomie której są wykorzystywane.	Egzamin
Umiejętności:	**Oxk_U01**	Student potrafi zbudować i skonfigurować prostą sieć lokalną.	Egzamin, rozwiązywanie zadań
	Oxk_U02	Student potrafi analizować ruch sieciowy na podstawie danych sterujących poszczególnych warstw sieciowych	Egzamin, rozwiązywanie zadań
	Oxk_U03	Student potrafi łączyć sieci lokalne i konfigurować parametry routingu.	Egzamin, rozwiązywanie zadań
	Oxk_U04	Student potrafi zarządzać przychodzącym do sieci ruchem oraz podejmować działania zwiększające bezpieczeństwo sieci.	Egzamin, rozwiązywanie zadań

Kompetencje społeczne:	**Oxk_K01**	Student w oparciu o uzyskaną podstawową wiedzę z zakresu sieci teleinformatycznych potrafi doskonalić swoją wiedzę i umiejętności z tego obszaru.	Praca w grupach

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
W01	Klasyfikacja i ogólna charakterystyka sieci komputerowych.	2
W02	Warstwowe architektury sieciowe.	3
W03	Warstwa łącza danych, adresacja MAC, standard Ethernet.	3
W04	Protokoły warstwy sieciowej, adresacja IPv4 i IPv6	3
W05	Protokoły warstwy transportowej vs protokoły aplikacji.	3
W06	Zasady i rodzaje routingu.	3
W07	Bezpieczeństwo sieci bezprzewodowych. Ataki na sieci bezprzewodowe WLAN.	3
L01	Wyznaczanie adresu sieci i rozgłoszeniowego sieci na podstawie różnych klas adresów IP hostów, zapoznanie z programem Cisco Packet Tracer – budowa sieci LAN z serwerem DHCP.	8
L02	Protokół TCP, analiza faz zestawiania i rozłączania sesji w warstwie transportowej. Analiza nagłówka protokołu TCP i UDP	5
L03	Routing statyczny i dynamiczny, konfiguracja routerów, podgląd i analiza tablicy routingu, porównanie metryk trasowania oraz dystansu administracyjnego protokołów routingu	5
L04	Konfiguracja usługi NAT oraz analiza tablicy NAT w ustawieniach routera, analiza przesyłanych pakietów IP pod kątem tłumaczenia adresów i portów.	5
L05	Podstawy bezpieczeństwa w sieciach komputerowych. Konfiguracja reguł zapory sieciowej na serwerze oraz weryfikacja ich działania. Konfigurowanie sieci VPN – tunelowanie GRE i IPsec. Tworzenie sieci VLAN oraz zapewnienie transmisji danych między nimi (metoda „router na patyku”, wykorzystanie podinterfejsów routera).	7
L06	Podstawy bezpieczeństwa w sieciach bezprzewodowych. Konfiguracja i zarządzanie AP. Mechanizmy bezpieczeństwa wykorzystywane w sieciach bezprzewodowych.	10

IV.	**KORELACJA EFEKTÓW UCZENIA SIĘ**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyk PRK*
W01	Oxk_W01, Oxk_W02, Oxk_W03, Oxk_K01	SIB2_W01, SIB2_W02, SIB2_K01	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W02	Oxk_W01, Oxk_W02, Oxk_W03, Oxk_K01	SIB2_W01, SIB2_W02, SIB2_K01	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W03	Oxk_W01, Oxk_W02, Oxk_W03, Oxk_K01	SIB2_W01, SIB2_W02, SIB2_K01	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W04	Oxk_W01, Oxk_W02, Oxk_W03, Oxk_K01	SIB2_W01, SIB2_W02, SIB2_K01	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W05	Oxk_W01, Oxk_W02, Oxk_W03, Oxk_K01	SIB2_W01, SIB2_W02, SIB2_K01	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W06	Oxk_W01, Oxk_W02, Oxk_W03, Oxk_K01	SIB2_W01, SIB2_W02, SIB2_K01	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W07	Oxk_W01, Oxk_W02, Oxk_W03, Oxk_K01	SIB2_W01, SIB2_W02, SIB2_K01	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
L01	Oxk_W01, Oxk_U01, Oxk_U02, Oxk_U03, Oxk_U04, Oxk_K01	SIB2_W01, SIB2_U01 SIB2_U02, SIB2_K01	P7U_W, P7S_WG, P7U_U, P7S_UW, P7U_K, P7S_KK

L02	Oxk_W01, Oxk_U01, Oxk_U02, Oxk_U03, Oxk_U04, Oxk_K01	SIB2_W01, SIB2_U01 SIB2_U02, SIB2_K01	P7U_W, P7S_WG, P7U_U, P7S_UW P7U_K, P7S_KK
L03	Oxk_W01, Oxk_U01, Oxk_U02, Oxk_U03, Oxk_U04, Oxk_K01	SIB2_W01, SIB2_U01 SIB2_U02, SIB2_K01	P7U_W, P7S_WG, P7U_U, P7S_UW P7U_K, P7S_KK
L04	Oxk_W01, Oxk_U01, Oxk_U02, Oxk_U03, Oxk_U04, Oxk_K01	SIB2_W01, SIB2_U01 SIB2_U02, SIB2_K01	P7U_W, P7S_WG, P7U_U, P7S_UW P7U_K, P7S_KK
L05	Oxk_W01, Oxk_U01, Oxk_U02, Oxk_U03, Oxk_U04, Oxk_K01	SIB2_W01, SIB2_U01 SIB2_U02, SIB2_K01	P7U_W, P7S_WG, P7U_U, P7S_UW P7U_K, P7S_KK
L06	Oxk_W01, Oxk_U01, Oxk_U02, Oxk_U03, Oxk_U04, Oxk_K01	SIB2_W01, SIB2_U01 SIB2_U02, SIB2_K01	P7U_W, P7S_WG, P7U_U, P7S_UW P7U_K, P7S_KK

V. NAKŁAD PRACY STUDENTA

Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**20**		**126**	**5**
Ćwiczenia				
Seminaria				
Laboratoria	**40**			
Konsultacje	**5**			
Rozliczenie rygorów przedmiotu	**1**			
Przygotowanie do ćwiczeń		**20**		
Wykonanie zadań domowych		**20**		
Przygotowanie do rozliczenia rygorów		**20**		
RAZEM	**66**	**60**		

VI. METODY DYDAKTYCZNE

1. Metody podające: Wykłady z prezentacjami multimedialnymi
2. Metody aktywizujące: pogadanka, obserwacja, praca z dokumentacją, praca w grupach, case study.
3. Ćwiczenia na stanowiskach komputerowych

VII. FORMA ZALICZENIA PRZEDMIOTU

Rygor	*Kryteria składowe*	*Waga*
Zaliczenie	Ocena z kolokwium (materiał z wykładów)	0,4
	Ocena z ćwiczeń	0,6

VIII. LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

OBOWIĄZKOWA

1. Józefiok A., *Budowa sieci komputerowych na przełącznikach i routerach Cisco*, Helion, Gliwice 2013
2. Wrotek W., *Sieci komputerowe*, Helion, Gliwice 2016

UZUPEŁNIAJĄCA

1. Tanenbaum, Wetherall, Sieci komputerowe, Helion, Gliwice 2012
2. Kluczewski J., Bezpieczeństwo sieci komputerowych (ebook), Itstart, Piekary Śląskie 2019
3. Sportack M., Sieci komputerowe. Księga eksperta, Helion, Gliwice 2004

IX. PROWADZĄCY PRZEDMIOT

Stopień, Imię i nazwisko	mgr Grzegorz PIOTROWSKI
adres e-mail	grzegorz.piotrowski@c2o.eu

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:	**Elementy kryptologii**	*Kod*:	**Mkr**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Stacjonarne		
Kształcenie w zakresie:	Cyberbezpieczeństwo		
Profil:	Ogólnoakademicki		
Liczba ECTS:	5		
Semestr:	4		
Wymagania wstępne:	Podstawowa wiedza na temat technologii komputerowych oraz systemów liczbowych.		
Język wykładowy:	Polski		
Cel przedmiotu:	**C01**	Zapoznanie studentów z podstawowymi pojęciami z zakresu kryptologii, w tym kryptografii i kryptoanalizy.	
	C02	Zapoznanie studentów z algorytmami i protokołami kryptograficznymi	
	C03	Wykształcenie umiejętności szyfrowania i deszyfrowania wiadomości używając współczesnych oraz historycznych algorytmów, a także podstawowych umiejętności z zakresu ich kryptoanalizy	

II.	**EFEKTY UCZENIA SIĘ**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Mkr_W01**	Student zna i rozumie istotę oraz potrzebę szyfrowania danych.	Egzamin
	Mkr_W02	Student zna i wie jak rozpoznać oraz wykorzystać mechanizmy szyfrów historycznych.	Egzamin
	Mkr_W03	Student zna współczesne algorytmy symetryczne oraz obowiązujący standard szyfrowania blokowego.	Egzamin
	Mkr_W04	Student zna i rozumie sposób działania współczesnych algorytmów asymetrycznych oraz protokołów kryptograficznych.	Egzamin
	Mkr_W05	Student zna i rozumie mechanizmy kryptoanalizy współczesnych algorytmów.	Egzamin
Umiejętności:	**Mkr_U01**	Student potrafi użyć mechanizmów wykorzystywanych w kryptologii klasycznej.	Zadania na ćwiczeniach
	Mkr_U02	Student potrafi szyfrować i deszyfrować wiadomości wykorzystując współczesne algorytmy symetryczne. Potrafi generować klucze prywatne i publiczne oparte o kryptografię asymetryczną oraz potrafi szyfrować i deszyfrować wiadomości przy ich wykorzystaniu.	Zadania na laboratorium, egzamin
	Mkr_U03	Student potrafi posługiwać się protokołami uzgadniania wspólnego klucza sesyjnego i wykorzystywać je w praktyce. Potrafi podpisywać przekazywane wiadomości wykorzystując współczesne algorytmu podpisu cyfrowego	Zadania na laboratorium

	Mkr_U04	Student potrafi ocenić bezpieczeństwo badanego algorytmu wykorzystując poznane mechanizmy kryptoanalizy.	Zadania na ćwiczeniach, egzamin
	Mkr_U05	Student potrafi przeprowadzić ataki kryptoanalityczne na proste szyfry symetryczne i asymetryczne	Zadania na laboratorium
Kompetencje społeczne:	**Mkr_K01**	Student krytycznie ocenia posiadaną wiedzę i odbierane treści z zakresu kryptologii oraz potrafi doskonalić swoją wiedzę i umiejętności z tego obszaru.	Praca w grupach

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
W01	Kryptografia klasyczna. Metody szyfrowania i deszyfrowania.	2
W02	Metody kryptoanalizy szyfrów historycznych.	2
W03	Kryptografia symetryczna. Szyfry blokowe.	2
W04	Kryptografia symetryczna. Szyfry strumieniowe.	2
W05	Kryptografia asymetryczna. Algorytm RSA	2
W06	Algorytmy oparte na teorii krzywych eliptycznych.	2
W07	Protokoły kryptograficzne – protokoły wymiany klucza.	2
W08	Protokoły podpisu elektronicznego.	2
W09	Metody kryptoanalizy szyfrów symetrycznych.	2
W10	Metody kryptoanalizy szyfrów asymetrycznych.	2
C01	Szyfrowanie wiadomości algorytmami klasycznymi	2
C02	Deszyfrowanie wiadomości algorytmami klasycznymi	2
C03	Metody kryptoanalizy algorytmów klasycznych	6
L01	Współczesne standardy szyfrowania blokowego	4
L02	Metody kryptoanalizy szyfrów blokowych. Kryptoanaliza różnicowa.	4
L03	Współczesne standardy szyfrowania strumieniowego.	2
L04	Metody kryptoanalizy szyfrów strumieniowych. Ataki algebraiczne.	4
L05	Kryptografia asymetryczna. Algorytm RSA.	2
L06	Algorytmy oparte na krzywych eliptycznych.	4
L07	Protokoły kryptograficzne – protokół Diffiego-Hellmana.	2
L08	Współczesne algorytmy podpisów cyfrowych.	2
L09	Metody kryptoanalizy algorytmów asymetrycznych.	6

IV.	**KORELACJA EFEKTÓW UCZENIA SIĘ**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyk PRK*
W01	Mkr_W01, Mkr_W02, Mkr_W03, Mkr_W04, Mkr_W05, Mkr_K01	SIB2_W01, SIB2_W02, SIB2_K01	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W02	Mkr_W01, Mkr_W02, Mkr_W03, Mkr_W04, Mkr_W05, Mkr_K01	SIB2_W01, SIB2_W02, SIB2_K01	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W03	Mkr_W01, Mkr_W02, Mkr_W03, Mkr_W04, Mkr_W05, Mkr_K01	SIB2_W01, SIB2_W02, SIB2_K01	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W04	Mkr_W01, Mkr_W02, Mkr_W03, Mkr_W04, Mkr_W05, Mkr_K01	SIB2_W01, SIB2_W02, SIB2_K01	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W05	Mkr_W01, Mkr_W02, Mkr_W03, Mkr_W04, Mkr_W05, Mkr_K01	SIB2_W01, SIB2_W02, SIB2_K01	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK

W06	Mkr_W01, Mkr_W02, Mkr_W03, Mkr_W04, Mkr_W05, Mkr_K01	SIB2_W01, SIB2_W02, SIB2_K01	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W07	Mkr_W01, Mkr_W02, Mkr_W03, Mkr_W04, Mkr_W05, Mkr_K01	SIB2_W01, SIB2_W02, SIB2_K01	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W08	Mkr_W01, Mkr_W02, Mkr_W03, Mkr_W04, Mkr_W05, Mkr_K01	SIB2_W01, SIB2_W02, SIB2_K01	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W09	Mkr_W01, Mkr_W02, Mkr_W03, Mkr_W04, Mkr_W05, Mkr_K01	SIB2_W01, SIB2_W02, SIB2_K01	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W10	Mkr_W01, Mkr_W02, Mkr_W03, Mkr_W04, Mkr_W05, Mkr_K01	SIB2_W01, SIB2_W02, SIB2_K01	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
C01	Mkr_W01, Mkr_W02 Mkr_U01, Mkr_U05, Mkr_K01	SIB2_W01, SIB2_U01, SIB2_K01	P7U_W, P7S_WG, P7U_U, P7S_UW, P7U_K, P7S_KK
C02	Mkr_W01, Mkr_W02 Mkr_U01, Mkr_U05, Mkr_K01	SIB2_W01, SIB2_U01, SIB2_K01	P7U_W, P7S_WG, P7U_U, P7S_UW, P7U_K, P7S_KK
C03	Mkr_W01, Mkr_W02 Mkr_U01, Mkr_U05, Mkr_K01	SIB2_W01, SIB2_U01, SIB2_K01	P7U_W, P7S_WG, P7U_U, P7S_UW, P7U_K, P7S_KK
L01	Mkr_W03, Mkr_W04, Mkr_U01, Mkr_U02, Mkr_U03, Mkr_U04, Mkr_U05, Mkr_K01	SIB2_W01, SIB2_U01, SIB2_U02, SIB2_K01	P7U_W, P7S_WG, P7U_U, P7S_UW, P7U_K, P7S_KK
L02	Mkr_W03, Mkr_W04, Mkr_U01, Mkr_U02, Mkr_U03, Mkr_U04, Mkr_U05, Mkr_K01	SIB2_W01, SIB2_U01, SIB2_U02, SIB2_K01	P7U_W, P7S_WG, P7U_U, P7S_UW, P7U_K, P7S_KK
L03	Mkr_W03, Mkr_W04, Mkr_U01, Mkr_U02, Mkr_U03, Mkr_U04, Mkr_U05, Mkr_K01	SIB2_W01, SIB2_U01, SIB2_U02, SIB2_K01	P7U_W, P7S_WG, P7U_U, P7S_UW, P7U_K, P7S_KK
L04	Mkr_W03, Mkr_W04, Mkr_U01, Mkr_U02, Mkr_U03, Mkr_U04, Mkr_U05, Mkr_K01	SIB2_W01, SIB2_U01, SIB2_U02, SIB2_K01	P7U_W, P7S_WG, P7U_U, P7S_UW, P7U_K, P7S_KK
L05	Mkr_W03, Mkr_W04, Mkr_U01, Mkr_U02, Mkr_U03, Mkr_U04, Mkr_U05, Mkr_K01	SIB2_W01, SIB2_U01, SIB2_U02, SIB2_K01	P7U_W, P7S_WG, P7U_U, P7S_UW, P7U_K, P7S_KK
L06	Mkr_W03, Mkr_W04, Mkr_U01, Mkr_U02, Mkr_U03, Mkr_U04, Mkr_U05, Mkr_K01	SIB2_W01, SIB2_U01, SIB2_U02, SIB2_K01	P7U_W, P7S_WG, P7U_U, P7S_UW, P7U_K, P7S_KK
L07	Mkr_W03, Mkr_W04, Mkr_U01, Mkr_U02, Mkr_U03, Mkr_U04, Mkr_U05, Mkr_K01	SIB2_W01, SIB2_U01, SIB2_U02, SIB2_K01	P7U_W, P7S_WG, P7U_U, P7S_UW, P7U_K, P7S_KK
L08	Mkr_W03, Mkr_W04, Mkr_U01, Mkr_U02, Mkr_U03, Mkr_U04, Mkr_U05, Mkr_K01	SIB2_W01, SIB2_U01, SIB2_U02, SIB2_K01	P7U_W, P7S_WG, P7U_U, P7S_UW, P7U_K, P7S_KK
L09	Mkr_W03, Mkr_W04, Mkr_U01, Mkr_U02, Mkr_U03, Mkr_U04, Mkr_U05, Mkr_K01	SIB2_W01, SIB2_U01, SIB2_U02, SIB2_K01	P7U_W, P7S_WG, P7U_U, P7S_UW, P7U_K, P7S_KK

V.	NAKŁAD PRACY STUDENTA			
Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**20**		**126**	**5**
Ćwiczenia	**10**			
Laboratorium	**30**			
Konwersatoria				
Konsultacje	**5**			
Rozliczenie rygorów przedmiotu	**1**			
Przygotowanie do ćwiczeń		**30**		
Wykonanie zadań domowych		**15**		
Przygotowanie do rozliczenia rygorów		**15**		
RAZEM	**66**	**60**		

VI.	METODY DYDAKTYCZNE
1.	Wykłady z prezentacjami multimedialnymi
2.	Ćwiczenia na stanowiskach komputerowych

VII.	FORMA ZALICZENIA PRZEDMIOTU	
Rygor	*Kryteria składowe*	*Waga*
Egzamin	Egzamin pisemny	0,8
	Ocena z ćwiczeń i laboratorium	0,2

VIII.	LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA
	OBOWIĄZKOWA
1.	J.Buchmann, Wprowadzenie do kryptografii, PWN 2006
2.	B.Schneier, Kryptografia dla praktyków. Protokoły, algorytmy i programy źródłowe w języku C, WNT 1995
	UZUPEŁNIAJĄCA
1.	Marcin Karbowski, Podstawy kryptografii. Wydanie III, Helion, Gliwice 2014
2.	A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, Kryptografia stosowana, WNT, Warszawa 2005

IX.	PROWADZĄCY PRZEDMIOT
Stopień, Imię i nazwisko	dr hab. Jerzy KOSIŃSKI, prof. AMW, mgr inż. Kamil SZCZEPANIUK
adres e-mail	j.kosinski@amw.gdynia.pl, k.szczepaniuk@amw.gdynia.pl

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:	**Administrowanie systemem Linux**	*Kod*:	**Oxl**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Stacjonarne		
Kształcenie w zakresie:	Cyberbezpieczeństwo		
Profil:	Ogólnoakademicki		
Liczba ECTS:	4		
Semestr:	4		
Wymagania wstępne:	Brak		
Język wykładowy:	Polski		
Cel przedmiotu:	**C01**	Zapoznanie studentów z procesem administrowania systemem operacyjnym Linux	
	C03	Zapoznanie studentów z metodami zabezpieczania usług w systemie operacyjnym Linux	

II.	**EFEKTY UCZENIA SIĘ**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Oxl_W01**	Zna i rozumie w pogłębiony sposób wybrane fakty, teorie, metody oraz zależności między nimi z zakresu systemów informatycznych.	Pytania sprawdzające podczas zajęć. Kolokwium.
Umiejętności:	**Oxl_U01**	Potrafi wykorzystać posiadaną wiedzę z zakresu systemów informatycznych oraz rozwiązywać złożone i nietypowe problemy poprzez dobór oraz zastosowanie właściwych metod i narzędzi.	Rozwiązanie zadań problemowych
	Oxl_U02	Potrafi brać udział w debacie z zakresu wykorzystania systemów informacyjnych w bezpieczeństwie - przedstawiać i oceniać różne opinie i stanowiska oraz dyskutować o nich.	Rozwiązanie zadań problemowych Wypowiedzi ustne, aktywność w ramach dyskusji.
	Oxl_U03	Potrafi posługiwać się językiem obcym ze szczególnym uwzględnienie specjalistycznej terminologii z zakresu wykorzystania systemów informacyjnych w bezpieczeństwie.	Rozwiązanie zadań problemowych
	Oxl_U04	Potrafi samodzielnie planować i realizować własne uczenie się przez całe życie i ukierunkowywać innych w tym zakresie.	Przygotowanie do zajęć

Kompetencje społeczne:	**Oxl_K01**	Krytycznie ocenia posiadaną wiedzę i odbierane treści z zakresu systemów informatycznych .	Sprawozdanie / przygotowanie do zajęć
	Oxl_K02	Uznaje znaczenie wiedzy w rozwiązywaniu problemów praktycznych oraz zasięga opinii ekspertów w przypadku trudności z samodzielnym rozwiazywaniem problemów dotyczących wykorzystania systemów informacyjnych w bezpieczeństwie.	Rozwiązanie zadań problemowych

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
W01	Wprowadzenie do przedmiotu. Sprawy organizacyjne. Zapoznanie z warunkami zaliczenia. Kontakt. Literatura. Wprowadzenie systemu Linux.	1
W02	Uzyskanie dostępu do systemu Linux. - Wprowadzenie do Bash Shell; - Sposoby logowania się do systemu.	1
W03	System plików. - Organizacja systemu plików; - Kontrola dostępu do plików; - Dowiązania.	2
W04	Zarządzanie kontami użytkowników i grupami systemu Linux. - Konta użytkowników systemu Linux; - Konta grup systemu Linux; - Zarządzanie kontami użytkowników.	2
W05	Operacje na plikach i katalogach - Tworzenie, kopiowanie, przenoszenie i usuwanie plików i katalogów; - Edycja i zapisywanie plików.	2
W06	Monitorowanie procesów - Proces i jego charakterystyka; - Operacje na procesach; - Monitorowanie procesów.	2
W07	Secure Shell (SSH) - Wprowadzenie do SSH; - Klient – serwer; - Zabezpieczenie usługi SSH.	2
W08	Konfiguracja sieci TCP/IP - Model TCP/IP i protokoły sieciowe; - Routing; - Analiza ruchu oraz troubleshooting; - Konfiguracja sieci.	2
W09	Logi i zdarzenia w systemie - Rejestrowanie zdarzeń; - Przegląd i monitorowanie logów.	2
W10	Zarządzanie oprogramowaniem i kontrola usług - zarządzenie oprogramowaniem; - zarządzenie usługami.	2
W11	Zarządzanie bezpieczeństwem systemu operacyjnego	2

	- zarządzanie bezpieczeństwem SELinux; - zarządzenie bezpieczeństwem sieci.	
L01	Uzyskanie dostępu do systemu Linux - Uzyskanie dostępu do systemu; - Korzystanie z powłoki Bash Shell.	2
L02	Konta użytkowników i grup - Zarządzanie kontami lokalnych użytkowników; - Zarządzanie grupami lokalnymi; - Zarządzanie hasłami.	3
L03	Operacje na plikach i katalogach - Tworzenie, kopiowanie, przenoszenie i usuwanie plików i katalogów; - Wyszukiwanie, edycja i zapisywanie plików.	3
L04	Monitorowanie procesów - Operacje na procesach; - Monitorowanie procesów.	2
L05	Secure Shell (SSH) - Komunikacja klient – serwer; - Zabezpieczenie usługi SSH.	2
L06	Konfiguracja sieci TCP/IP - Analiza ruchu sieciowego; - Przegląd konfiguracji sieci.	3
L07	Logi i zdarzenia w systemie - Rejestrowanie zdarzeń; - Przegląd i monitorowanie logów	2
L08	Zarządzanie oprogramowaniem i kontrola usług - zarządzenie oprogramowaniem; - zarządzenie usługami.	2
L09	Zarządzanie bezpieczeństwem - zarządzanie bezpieczeństwem SELinux; - zarządzenie bezpieczeństwem sieci.	2
L10	Wprowadzenie do kontenerów - Wprowadzenie do technologii kontenerowej; - Uruchamianie podstawowego kontenera.	4

IV.	**KORELACJA EFEKTÓW UCZENIA SIĘ**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyk PRK*
W01	Oxl_W01, Oxl_U02, Oxl_U03, Oxl_U04 Oxl_K01, Oxl_K02	SIB2_W01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UK, P7S_UU P7U_K, P7S_KK
W02	Oxl_W01, Oxl_U02, Oxl_U03, Oxl_U04 Oxl_K01, Oxl_K02	SIB2_W01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UK, P7S_UU P7U_K, P7S_KK
W03	Oxl_W01, Oxl_U02, Oxl_U03, Oxl_U04 Oxl_K01, Oxl_K02	SIB2_W01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K01	P7U_W, P7S_WG, P7U_U, P7S_UK, P7S_UU P7U_K, P7S_KK
W04	Oxl_W01, Oxl_U02, Oxl_U03, Oxl_U04 Oxl_K01, Oxl_K02	SIB2_W01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UK, P7S_UU P7U_K, P7S_KK
W05	Oxl_W01, Oxl_U02, Oxl_U03, Oxl_U04	SIB2_W01,	P7U_W, P7S_WG, P7U_U, P7S_UK, P7S_UU

	Oxl_K01, Oxl_K02	SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_K, P7S_KK
W06	Oxl_W01, Oxl_U02, Oxl_U03, Oxl_U04 Oxl_K01, Oxl_K02	SIB2_W01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UK, P7S_UU P7U_K, P7S_KK
W07	Oxl_W01, Oxl_U02, Oxl_U03, Oxl_U04 Oxl_K01, Oxl_K02	SIB2_W01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UK, P7S_UU P7U_K, P7S_KK
W08	Oxl_W01, Oxl_U02, Oxl_U03, Oxl_U04 Oxl_K01, Oxl_K02	SIB2_W01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UK, P7S_UU P7U_K, P7S_KK
W09	Oxl_W01, Oxl_ Oxl_U02, Oxl_U03, Oxl_U04 Oxl_K01, Oxl_K02	SIB2_W01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UK, P7S_UU P7U_K, P7S_KK
W10	Oxl_W01, Oxl_U02, Oxl_U03, Oxl_U04 Oxl_K01, Oxl_K02	SIB2_W01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UK, P7S_UU P7U_K, P7S_KK
L01	Oxl_W01, Oxl_U01, Oxl_U03, Oxl_K02	SIB2_W01, SIB2_U01, SIB2_U05, SIB2_K02	P7U_W, P7S_WG P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK
L02	Oxl_W01, Oxl_U01, Oxl_U03, Oxl_K02	SIB2_W01, SIB2_U01, SIB2_U05, SIB2_K02	P7U_W, P7S_WG P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK
L03	Oxl_W01, Oxl_U01, Oxl_U03, Oxl_K02	SIB2_W01, SIB2_U01, SIB2_U05, SIB2_K02	P7U_W, P7S_WG P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK
L04	Oxl_W01, Oxl_U01, Oxl_U03, Oxl_K02	SIB2_W01, SIB2_U01, SIB2_U05, SIB2_K02	P7U_W, P7S_WG P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK
L05	Oxl_W01, Oxl_U01, Oxl_U03, Oxl_K02	SIB2_W01, SIB2_U01, SIB2_U05, SIB2_K02	P7U_W, P7S_WG P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK
L06	Oxl_W01, Oxl_U01, Oxl_U03, Oxl_K02	SIB2_W01, SIB2_U01, SIB2_U05, SIB2_K02	P7U_W, P7S_WG P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK
L07	Oxl_W01, Oxl_U01, Oxl_U03, Oxl_K02	SIB2_W01, SIB2_U01, SIB2_U05, SIB2_K02	P7U_W, P7S_WG P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK
L08	Oxl_W01, Oxl_U01, Oxl_U03, Oxl_K02	SIB2_W01, SIB2_U01, SIB2_U05, SIB2_K02	P7U_W, P7S_WG P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK
L09	Oxl_W01, Oxl_U01, Oxl_U03, Oxl_K02	SIB2_W01, SIB2_U01, SIB2_U05, SIB2_K02	P7U_W, P7S_WG P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK
L10	Oxl_W01, Oxl_U01, Oxl_U03, Oxl_K02	SIB2_W01, SIB2_U01, SIB2_U05, SIB2_K02	P7U_W, P7S_WG P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK

V.	**NAKŁAD PRACY STUDENTA**			
Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**20**		**100**	**4**
Laboratorium	**25**			
Seminaria				

Konwersatoria				
Konsultacje	**5**			
Rozliczenie rygorów przedmiotu				
Przygotowanie do ćwiczeń		**20**		
Wykonanie zadań domowych		**20**		
Przygotowanie do rozliczenia rygorów		**10**		
RAZEM	**50**	**50**		

VI.	**METODY DYDAKTYCZNE**
1.	Wykład z prezentacją multimedialną
2.	Praca przy stanowisku komputerowym
3.	Rozwiązywanie zadań problemowych
4.	Studiowanie literatury

VII.	**FORMA ZALICZENIA PRZEDMIOTU**	
Rygor	*Kryteria składowe*	*Waga*
Zaliczenie	Aktywność na zajęciach laboratoryjnych	0,2
	Sprawozdania z laboratorium	0,8
Zaliczenie	Ocena za aktywność na zajęciach	0,2
	Ocena z kolokwium	0,8

VIII.	**LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA**
	OBOWIĄZKOWA
1.	E. Nemeth, G. Snyder, T. R. Hein, B. Whaley, D. Mackin, Unix i Linux. Przewodnik administratora systemów. Wydanie V, Helion, 2018
2.	B. Ward, Jak działa Linux: podręcznik administratora, Helion, 2015
3.	Ł. Sosna, Linux. Komendy i polecenia. Wydanie VI, Wydawnictwo Helion 2022
	UZUPEŁNIAJĄCA
1.	M. Ebrahim, A. Mallett, Skrypty powłoki systemu Linux. Zagadnienia zaawansowane. Wydanie II, Helion, Gliwice 2019
2.	Pablo Iranzo Gómez, Pedro Ibánez Requena, Miguel Pérez Colino, Scott McCarty, Red Hat Enterprise Linux 9 Administration. A comprehensive Linux system administration guide for RHCSA certification exam candidates - Second Edition, Wydawnictwo Packt Publishing 2022
3.	Eric McLeroy, Red Hat Certified Specialist in Services Management and Automation EX358 Exam Guide, Wydawnictwo Packt Publishing 2022

IX.	**PROWADZĄCY PRZEDMIOT**
Stopień, Imię i nazwisko	kmdr por. dr inż. Adam Stojałowski
adres e-mail	a.stojalowski@amw.gdynia.pl

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:	**Cyberbezpieczeństwo**	*Kod*:	**Lxc**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Stacjonarne		
Kształcenie w zakresie:	Cyberbezpieczeństwo		
Profil:	Ogólnoakademicki		
Liczba ECTS:	4		
Semestr:	4		
Wymagania wstępne:			
Język wykładowy:	Polski		
Cel przedmiotu: **C01**	zwiększenie świadomości użytkowników cyberprzestrzeni w zakresie metod i środków bezpieczeństwa w cyberprzestrzeni.		
Cel przedmiotu: **C02**	propagowanie powszechnej oraz specjalistycznej edukacji społecznej w zakresie bezpieczeństwa cyberprzestrzeni RP		
Cel przedmiotu: **C03**	uwrażliwienie na zagrożenia płynące z cyberprzestrzeni		

II.	**EFEKTY UCZENIA SIĘ**	
Zakres / *Kod*	*Opis efektu*	*Sposób oceny*
Wiedza: **Lxc_W01**	Zna podstawową terminologię związaną z problematyką zajęć. Posiada wiedzę o podstawowych regulacjach prawnych (polskich i międzynarodowych) w zakresie bezpieczeństwa w cyberprzestrzeni	kolokwium
Wiedza: **Lxc_W02**	Posiada wiedzę na temat standardów i norm obowiązujących w jednostkach sektora publicznego i prywatnego w zakresie bezpieczeństwa w cyberprzestrzeni	Test sprawdzający podczas zajęć, praca domowa
Wiedza: **Lxc_W03**	Posiada wiedzę na temat znaczenia, roli i kompetencji instytucji odpowiadających za bezpieczeństwo w cyberprzestrzeni, ich wzajemnych zależności w strukturach państwowych i międzynarodowych	praca pisemna podczas zajęć
Wiedza: **Lxc_W04**	Posiada wiedzę na temat znaczenia, roli i kompetencji osób administrujących bezpieczeństwem w cyberprzestrzeni	Test sprawdzający podczas zajęć, praca domowa
Umiejętności: **Lxc_U01**	Potrafi identyfikować zagrożenia dla bezpieczeństwa w cyberprzestrzeni	kolokwium
Umiejętności: **Lxc_U02**	Posiada umiejętność określenia, analizowania i proponowania rozwiązań dla konkretnych zagadnień związanych z obszarem ochrony bezpieczeństwa w cyberprzestrzeni w instytucjach państwowych i prywatnych	praca pisemna podczas zajęć
Umiejętności: **Lxc_U03**	Potrafi prognozować zagrożenia cyberprzestrzeni	praca pisemna podczas zajęć

Kompetencje społeczne:	**Lxc_K01**	Potrafi dokonać prawidłowej oceny systemu norm i reguł porządkujących system zarządzania bezpieczeństwem w cyberprzestrzeni.	wykonanie projektu
	Lxc_K02	Rozumie potrzebę uczenia się przez całe życie	odpowiedź tablicowa

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
W01	Wprowadzenie do problematyki zajęć (zakres, terminologia, akty prawne). Organizacja i funkcjonowanie systemu ochrony bezpieczeństwa w cyberprzestrzeni w RP, UE, NATO.	1
W02	Modele cyberprzestrzeni: określenie obszaru cyberprzestrzeni człowieka i państwa	1
W03	Prawne aspekty definiowania cyberprzestrzeni i zagrożeń w cyberprzestrzeni	1
W04	Źródła zagrożeń w cyberprzestrzeni. Charakterystyka cyberprzestępczości. Prognozy cyberprzestępczości	1
W05	Środki i metody ataków w cyberprzestrzeni	2
W06	Zagrożenia płatności i bankowości elektronicznych	2
W07	Organizacja „systemu" zwalczania cyberprzestępczości	2
C01	Rozpoznanie zagrożeń z obszaru „rzeczywistości materialnej" w „rzeczywistości wirtualnej"	10
L01	Ustalanie powiązań oraz tożsamości w Internecie	10
L02	Zabezpieczanie i analiza pozyskanego materiału	10
L03	Zasady i metody wyszukiwania informacji o zagrożeniach w Internecie	10

IV.	**KORELACJA EFEKTÓW UCZENIA SIĘ**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyk PRK*
W01	Lxc_W01, Lxc_W02, Lxc_W03, Lxc_W04	SIB2_W01, SIB2_W02	P7U_W, P7S_WG, P7S_WK
W02	Lxc_W01, Lxc_W02, Lxc_W03, Lxc_W04	SIB2_W01, SIB2_W02	P7U_W, P7S_WG, P7S_WK
W03	Lxc_W01, Lxc_W02, Lxc_W03, Lxc_W04	SIB2_W01, SIB2_W02	P7U_W, P7S_WG, P7S_WK
W04	Lxc_W01, Lxc_W02, Lxc_W03, Lxc_W04	SIB2_W01, SIB2_W02	P7U_W, P7S_WG, P7S_WK
W05	Lxc_W01, Lxc_W02, Lxc_W03, Lxc_W04	SIB2_W01, SIB2_W02	P7U_W, P7S_WG, P7S_WK
C01	Lxc_U01, Lxc_U02, Lxc_U03, Lxc_K01, Lxc_K02	SIB2_U01, SIB2_U02, SIB2_U04, SIB2_U07, SIB2_K01, SIB2_K02, SIB2_K04	P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK, P7S_KR
L01	Lxc_U01, Lxc_U02, Lxc_U03, Lxc_K01, Lxc_K02	SIB2_U01, SIB2_U02, SIB2_U04, SIB2_U07, SIB2_K01, SIB2_K02, SIB2_K04	P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK, P7S_KR
L02	Lxc_U01, Lxc_U02, Lxc_U03, Lxc_K01, Lxc_K02	SIB2_U01, SIB2_U02, SIB2_U04, SIB2_U07, SIB2_K01, SIB2_K02, SIB2_K04	P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK, P7S_KR
L03	Lxc_U01, Lxc_U02, Lxc_U03, Lxc_K01, Lxc_K02	SIB2_U01, SIB2_U02, SIB2_U04, SIB2_U07, SIB2_K01, SIB2_K02, SIB2_K04	P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK, P7S_KR

V.	**NAKŁAD PRACY STUDENTA**

Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**10**	**X**	**105**	**4**
Ćwiczenia	**10**			
Seminaria				
Laboratoria	**30**			
Konsultacje (zaliczenie nieobecności, rozliczenie rygorów, poprawy)	**5**			
Przygotowanie do ćwiczeń	**X**			
Opanowanie informacji		**20**		
Przygotowanie do rozliczenia rygorów		**30**		
RAZEM	**55**	**50**		

VI. METODY DYDAKTYCZNE

1.	Wykład interaktywny z prezentacją multimedialną
2	Ćwiczenia audytoryjne: symulacja zagrożeń, projekt praktyczny
3	Ćwiczenia audytoryjne: praca w grupach

VII. FORMA ZALICZENIA PRZEDMIOTU

Rygor	*Kryteria składowe*	*Waga*
Zaliczenie	Kolokwium - Test nabytej wiedzy	0,5
	Projekt	0,25
	Rozwiązanie zadań	0,25

VIII. LITERATURA

OBOWIĄZKOWA

1.	B. Hołyst, J. Pomykała, *Cyberprzestępczość i ochrona informacji*, Wydawnictwo WSM, 2012 r.
2.	J. Kosiński, *Paradygmaty cyberprzestępczości*, Warszawa 2015
3.	*Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa*, Dz.U. 2018 poz. 1560
4.	*Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii*, 32016L1148
5.	K. Liedel, *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*, Toruń 2005

UZUPEŁNIAJĄCA

1.	*Strategia Rozwoju Systemu Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2022*, BBN 2013
2.	*Informacja o wynikach kontroli. Realizacja przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni RP*, NIK 2015
3.	G. Szpor, CH Beck, *Ochrona wolności, własności i bezpieczeństwa*, 2011 r.

IX. PROWADZĄCY PRZEDMIOT

Stopień, Imię i nazwisko	dr hab. Jerzy KOSIŃSKI, prof. AMW
adres e-mail	j.kosinski@amw.gdynia.pl

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:	**Prognozowanie cyberzagrożeń**	*Kod*:	**Lcp**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Stacjonarne		
Kształcenie w zakresie:	Cyberbezpieczeństwo		
Profil:	Ogólnoakademicki		
Liczba ECTS:	4		
Semestr:	4		
Wymagania wstępne:	Podstawowa znajomość wektorów ataków oraz technik mitygacji, utwardzania i audytowania systemów IT		
Język wykładowy:	Polski		
Cel przedmiotu:	**C01**	Zapoznanie z teorią oraz metodą oceny ryzyka w cyberprzestrzeni.	
	C02	Zapoznanie z metodami prognozowania zagrożeń w cyberprzestrzeni.	
	C03	Zaprezentowanie nowoczesnych technologii do oceny ryzyka oraz prognozowania.	

II.	**EFEKTY UCZENIA SIĘ**	
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Lcp_W01**	Zna problematykę cyberbezpieczeństwa, metod oceny ryzyka w cyberprzestrzeni oraz zna podstawowe zagrożenia bezpieczeństwa informacji.	Egzamin
	Lcp_W02	Zna podstawy bezpieczeństwa systemów teleinformatycznych, mechanizmy bezpieczeństwa wykorzystywane w systemach teleinformatycznych.	Egzamin
	Lcp_W03	Zna podstawowe techniki kryptografii oraz ma wiedzę z zakresu bezpieczeństwa wirtualizacji.	Egzamin
	Lcp_W04	Posiada wiedzę z zakresu ocena ryzyka i prognozowanie cyberzagrożeń.	Egzamin
	Lcp_W05	Posiada wiedzę z zakresu inżynierii systemów i analiza systemowej.	Egzamin
	Lcp_W06	Posiada wiedzę z zakresu planowania operacji w cyberprzestrzeni.	Egzamin
Umiejętności:	**Lcp_U01**	Potrafi przeprowadzić ocenę ryzyka w cyberprzestrzeni oraz wskazać zagrożenia bezpieczeństwa informacji.	Zadania laboratoryjne
	Lcp_U02	Potrafi wykorzystywać metody i techniki zabezpieczenia informacji w systemach i sieciach teleinformatycznych.	Zadania laboratoryjne
	Lcp_U03	Potrafi analizować dane z zakresu bezpieczeństwa i obronności.	Zadania laboratoryjne
	Lcp_U04	Potrafi oceniać ryzyko i prognozować cyberzagrożenia w systemach i sieciach teleinformatycznych	Zadania laboratoryjne

	Lcp_U05	Zna język angielski w zakresie słownictwa specjalistycznego na poziomie gwarantującym poprawne posługiwanie się dokumentacją techniczną oraz komunikatywność.	Zadania laboratoryjne
Kompetencje społeczne:	**Lcp_K01**	Posiada umiejętność w dążeniu do opanowania nawyków w sprawnym wykonywaniu obowiązków i czynności służbowych podczas realizacji zadań w różnorodnych warunkach w czasie pokoju, kryzysu i wojny	Praca w grupach
	Lcp_K02	Ma świadomość odpowiedzialnego pełnienia ról zawodowych w ramach zadań realizowanych przez SZ RP, z uwzględnieniem zmieniających się potrzeb społecznych, a w szczególności w zakresie rozwijania dorobku kryptologii i cyberbezpieczeństwa.	Praca w grupach
	Lcp_K03	Dostrzega znaczenie wiedzy w zakresie rozwiązywania problemów zabezpieczenia technicznego i wprowadzania nowych rozwiązań oraz docenia znaczenie samodzielnego poszerzania wiedzy i umiejętności	Praca w grupach

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
W01	Charakterystyka Cyberzagrożeń	2
W02	Teoretyczne aspekty prognozowania	2
W03	Klasyfikacja prognoz	2
W04	Etapy prognozowania	2
W05	Reguły prognozowania	2
W06	Prognozowanie strukturalne	2
W07	Prognozowanie niestrukturalne	2
W08	Prognozy ex post i ex ante	2
W09	Metody prognozowania przyczynowo-skutkowego	2
W10	Ocena trafności prognozy	2
C01	Sformułowanie zadania prognostycznego	1
C02	Określenie przesłanek prognostycznych	2
C03	Wybór danych gromadzonych na potrzeby budowy prognoz	1
C04	Zebranie danych prognostycznych	2
C05	Statystyczna obróbka danych prognostycznych	1
C06	Analiza danych prognostycznych	2
C07	Transformacja danych	1
C08	Agregacja danych	2
C09	Uzupełnianie brakujących danych	1
C10	Wybór metody prognozowania	2
C11	Budowa modelu prognostycznego	3
C12	Scenariusze	2
C13	Gra decyzyjna wykorzystywana w prognozowaniu	3
C14	Burza mózgów	2
C15	Ocena dokładności prognozy	1
C16	Ocena trafności prognozy	3

C17	Zaliczenie		1
IV.	**KORELACJA EFEKTÓW UCZENIA SIĘ**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyk PRK*
W01	Lcp_W01, Lcp_W02, Lcp_W03, Lcp_K01	SIB2_W01, SIB2_W02, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W02	Lcp_W01, Lcp_W02, Lcp_W03, Lcp_K01	SIB2_W01, SIB2_W02, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W03	Lcp_W01, Lcp_W02, Lcp_W03, Lcp_K01	SIB2_W01, SIB2_W02, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W04	Lcp_W01, Lcp_W02, Lcp_W04, Lcp_K01	SIB2_W01, SIB2_W02, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W05	Lcp_W01, Lcp_W04, Lcp_W05, Lcp_K01	SIB2_W01, SIB2_W02, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W06	Lcp_W01, Lcp_W02, Lcp_W03, Lcp_K01	SIB2_W01, SIB2_W02, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W07	Lcp_W01, Lcp_W02, Lcp_W03, Lcp_K01	SIB2_W01, SIB2_W02, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W08	Lcp_W01, Lcp_W02, Lcp_W04, Lcp_K01	SIB2_W01, SIB2_W02, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W09	Lcp_W01, Lcp_W05, Lcp_W06, Lcp_K01	SIB2_W01, SIB2_W02, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W10	Lcp_W01, Lcp_W02, Lcp_W06, Lcp_K01	SIB2_W01, SIB2_W02, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
C01	Lcp_W03, Lcp_U01, Lcp_U02, Lcp_K01	SIB2_W01, SIB2_U01, SIB2_U05, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK
C02	Lcp_W03, Lcp_U01, Lcp_U02, Lcp_K01	SIB2_W01, SIB2_U01, SIB2_U05, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK
C03	Lcp_W03, Lcp_U01, Lcp_U02, Lcp_K01	SIB2_W01, SIB2_U01, SIB2_U05, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK
C04	Lcp_W03, Lcp_U01, Lcp_U02, Lcp_K01	SIB2_W01, SIB2_U01, SIB2_U05, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK
C05	Lcp_W03, Lcp_U01, Lcp_U03, Lcp_K01	SIB2_W01, SIB2_U01, SIB2_U05, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK
C06	Lcp_W03, Lcp_U01, Lcp_U03, Lcp_K01	SIB2_W01, SIB2_U01, SIB2_U05, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK
C07	Lcp_W03, Lcp_U01, Lcp_U04, Lcp_K01	SIB2_W01, SIB2_U01, SIB2_U05, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK
C08	Lcp_W03, Lcp_U01, Lcp_U02, Lcp_U05, Lcp_K01	SIB2_W01, SIB2_U01, SIB2_U05, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK
C09	Lcp_W03, Lcp_U01, Lcp_U02, Lcp_U05, Lcp_K01	SIB2_W01, SIB2_U01, SIB2_U05, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK
C10	Lcp_W03, Lcp_U01, Lcp_U02, Lcp_U05, Lcp_K01	SIB2_W01, SIB2_U01, SIB2_U05, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK
C11	Lcp_W05, Lcp_U01, Lcp_U05, Lcp_K01	SIB2_W01, SIB2_U01, SIB2_U05, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK
C12	Lcp_W05, Lcp_U01, Lcp_U04, Lcp_K01	SIB2_W01, SIB2_U01, SIB2_U05, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK

C13	Lcp_W04, Lcp_U01, Lcp_U05, Lcp_U05, Lcp_K01	SIB2_W01, SIB2_U01, SIB2_U05, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK
C14	Lcp_W03, Lcp_U01, Lcp_U02, Lcp_U05, Lcp_K01	SIB2_W01, SIB2_U01, SIB2_U05, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK
C15	Lcp_W03, Lcp_U01, Lcp_U02, Lcp_U05, Lcp_K01	SIB2_W01, SIB2_U01, SIB2_U05, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK
C15	Lcp_W03, Lcp_U01, Lcp_U02, Lcp_K01	SIB2_W01, SIB2_U01, SIB2_U05, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK
C16	Lcp_W03, Lcp_U01, Lcp_U04, Lcp_K01	SIB2_W01, SIB2_U01, SIB2_U05, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK

V. NAKŁAD PRACY STUDENTA

Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**20**		**105**	**4**
Ćwiczenia	**30**			
Seminaria				
Konwersatoria				
Konsultacje	**5**			
Rozliczenie rygorów przedmiotu				
Przygotowanie do ćwiczeń		**15**		
Wykonanie zadań domowych		**15**		
Przygotowanie do rozliczenia rygorów		**20**		
RAZEM	**55**	**50**		

VI. METODY DYDAKTYCZNE

1. Wykłady z prezentacjami multimedialnymi
2. Ćwiczenia na stanowiskach komputerowych

VII. FORMA ZALICZENIA PRZEDMIOTU

Rygor	*Kryteria składowe*	*Waga*
Egzamin	Egzamin	0,8
	Ocena z ćwiczeń	0,2

VIII. LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

OBOWIĄZKOWA

1. B. Guzik, D. Appenzeller, W. Jurek: Prognozowanie i symulacje. Wybrane zagadnienia. MD 153 lub 168, AE Poznań
2. M. Cieślak (red.): Prognozowanie gospodarcze. Metody i zastosowania. PWN, Warszawa 2001
3. M. Anholcer, H. Gaspars, A. Owczarkowski: Przykłady i zadania z badań operacyjnych i ekonometrii, MD 163, AE Poznań
4. Tetlock Philip E., Gardner Dan, Superprognozowanie. Sztuka i nauka prognozowania, CeDeWu Sp. z o.o., Warszawa 2016

UZUPEŁNIAJĄCA

1. Maciąg A., Pietroń R., Kukla S., Prognozowanie i symulacja w Przedsiębiorstwie, PWE, Warszawa 2013
2. Gajda B., Prognozowanie i symulacje w ekonomii i zarządzaniu, C.H. Beck, Warszawa 2017
3. Dittmann P., Dittmann I., A. Szpulak, E. Szabela - Pasierbińska, Prognozowanie w zarządzaniu przedsiębiorstwem, Wolters Kluwer Polska, Warszawa 2012
4. Dittmann P., Prognozowanie w przedsiębiorstwie. Metody i ich zastosowania, Oficyna Ekonomiczna, Kraków 2004
5. Cieślak M. (red.), Nieklasyczne Metody Prognozowania, PWN, Warszawa1983
6. Sułek M., Prognozowanie i symulacje międzynarodowe, PWN, Warszawa 2010
7. Świeboda H., Prognozowanie zagrożeń bezpieczeństwa narodowego Rzeczpospolitej Polskiej, ASzWoj, Warszawa 2017

IX. PROWADZĄCY PRZEDMIOT

Stopień, Imię i nazwisko	dr Robert Janczewski
adres e-mail	r.janczewski@amw.gdynia.pl

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:	**Symulacja komputerowa**	*Kod*:	**Oku**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Stacjonarne		
Kształcenie w zakresie:	Cyberbezpieczeństwo		
Profil:	Ogólnoakademicki		
Liczba ECTS:	4		
Semestr:	4		
Wymagania wstępne:	Technologia informacyjna, Podstawy statystyki, Architektura systemów i sieci komputerowych		
Język wykładowy:	Polski		
Cel przedmiotu:	**C01**	Zapoznanie studentów z narzędziami, metodami, technikami symulacyjnymi.	
	C02	Ćwiczenie elementów projektowania, modelowania i symulacji.	
	C03	Prezentacja wybranych symulatorów jako przykładów praktycznego zastosowania symulacji komputerowej.	

II.	**EFEKTY UCZENIA SIĘ**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Oku_W01**	Zna podstawowe zagadnienia związane z projektowaniem, modelowaniem i symulacją, w tym rodzaje zespołów projektowych, otoczenie bliższe i dalsze projektów cele modelowania, rodzaje i zmienne modeli, cele, rodzaje, warunki, wady i zalety symulacji.	test
	Oku_W02	Zna poszczególne etapy analizy symulacyjnej.	test
	Oku_W03	Ma podstawową wiedzę w zakresie wybranych symulacji.	test
Umiejętności:	**Oku_U01**	Potrafi omówić poszczególne etapy analizy symulacyjnej.	test
	Oku_U02	Posiada umiejętność zbierania i analizy danych wejściowych.	test
	Oku_U03	Potrafi omówić i wskazać przykłady praktycznego zastosowania symulacji komputerowych.	praca na symulatorach
Kompetencje społeczne:	**Oku_K01**	Posiada umiejętność praktycznego wykorzystania wybranych symulatorów.	praca na symulatorach
	Oku_K02	Potrafi efektywnie pracować i współdziałać w różnych grupach eksperckich i strukturach roboczych.	praca pisemna
	Oku_K03	W oparciu o uzyskaną teoretyczną wiedzę programową potrafi samodzielnie aktualizować i doskonalić swoją wiedzę i umiejętności praktyczne w zakresie symulacji komputerowej.	test

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

W01	**Wprowadzenie do symulacji i modelowania** (pojęcie projektu, modelu, symulacji, zmienne modeli, rodzaje zespołów projektowych, modeli symulacji, cele, wady, zalety i błędy symulacji, wybrane zastosowania symulacji).	4
W02	**Analiza symulacyjna** (sformułowanie problemu, zebranie i analiza danych, budowa modelu matematycznego, opracowanie programu komputerowego, walidacja i weryfikacja modelu, projektowanie układu eksperymentów, analiza wyników).	4
W03	**Zbieranie i analiza danych wejściowych** (sztuka zbierania danych, metoda reprezentacyjna, w tym etapy stosowania, podstawowe schematy losowania, parametryzacja podstawowych rozkładów ciągłych i dyskretnych).	4
W04	**Weryfikacja i walidacja modelu** (podstawowe definicje, zasady procesu weryfikacji i walidacji modelu, techniki walidacji i weryfikacji).	4
W05	**Planowanie eksperymentów symulacyjnych i analiza wyników** (aspekty planowania eksperymentów, metody redukcji wariancji, merytoryczne projektowanie układu eksperymentów, analiza statystyczna wyników).	4
L01	Symulator zdarzeń kryzysowych.	6
L02	Symulacje open-source w środowisku komputerowym	6
L03	Symulator mostka nawigacyjnego.	6
L04	Symulator strzelecki ŚNIEŻNIK.	6
L05	Symulatory i trenażery uzbrojenia okrętowego.	6

IV.	**KORELACJA EFEKTÓW UCZENIA SIĘ**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyk PRK*
W01	Oku_W01, Oku_W02, Oku_W03	SIB2_W01	P7U_W, P7S_WG
W02	Oku_W01, Oku_W02, Oku_W03	SIB2_W01	P7U_W, P7S_WG
W03	Oku_W01, Oku_W02, Oku_W03	SIB2_W01	P7U_W, P7S_WG
W04	Oku_W01, Oku_W02, Oku_W03	SIB2_W01	P7U_W, P7S_WG
W05	Oku_W01, Oku_W02, Oku_W03	SIB2_W01	P7U_W, P7S_WG
L01	Oku_U01, Oku_U02, Oku_U03, Oku_K01, Oku_K02, Oku_K03	SIB2_U01, SIB2_U06, SIB2_K01, SIB2_K05	P7U_U, P7S_UW, P7S_UO, P7U_K, P7S_KK, P7S_KR
L02	Oku_U01, Oku_U02, Oku_U03, Oku_K01, Oku_K02, Oku_K03	SIB2_U01, SIB2_U06, SIB2_K01, SIB2_K05	P7U_U, P7S_UW, P7S_UO, P7U_K, P7S_KK, P7S_KR
L03	Oku_U01, Oku_U02, Oku_U03, Oku_K01, Oku_K02, Oku_K03	SIB2_U01, SIB2_U06, SIB2_K01, SIB2_K05	P7U_U, P7S_UW, P7S_UO, P7U_K, P7S_KK, P7S_KR
L04	Oku_U01, Oku_U02, Oku_U03, Oku_K01, Oku_K02, Oku_K03	SIB2_U01, SIB2_U06, SIB2_K01, SIB2_K05	P7U_U, P7S_UW, P7S_UO, P7U_K, P7S_KK, P7S_KR
L05	Oku_U01, Oku_U02, Oku_U03, Oku_K01, Oku_K02, Oku_K03	SIB2_U01, SIB2_U06, SIB2_K01, SIB2_K05	P7U_U, P7S_UW, P7S_UO, P7U_K, P7S_KK, P7S_KR

V.	**NAKŁAD PRACY STUDENTA**			
Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**20**	**X**	**105**	**4**
Ćwiczenia	**0**			
Seminaria	**0**			
Laboratoria	**30**			
Konsultacje (zaliczenie nieobecności, rozliczenie rygorów, poprawy)	**5**			
Przygotowanie do ćwiczeń	**X**	**25**		
Opanowanie informacji		**25**		
Przygotowanie do rozliczenia rygorów		**20**		

RAZEM		55	50		
VI.	**METODY DYDAKTYCZNE**				
1.	prezentacja multimedialna				
2	wybrane symulatory				
3	praca w grupach i inne formy aktywizujące				
VII.	**FORMA ZALICZENIA PRZEDMIOTU**				
Rygor	*Kryteria składowe*			*Waga*	
Zaliczenie	wykonanie określonych ćwiczeń na symulatorach			0,4	
	test komputerowy			0,6	
VIII.	**LITERATURA**				
OBOWIĄZKOWA					
1.	G.S. Fishman, *Symulacja komputerowa. Pojęcia i metody*, PWE Warszawa 1981.				
2.	J. B. Gajda, *Prognozowanie i symulacja a decyzje gospodarcze*, C.H.Beck Warszawa, 2001.				
3.	B. Mielczarek, *Modelowanie symulacyjne w zarządzaniu,* Wyd. Politechniki Wrocławskiej, Wrocław 2009.				
UZUPEŁNIAJĄCA					
1.	K. Krupa, *Modelowanie symulacja i prognozowanie. Systemy ciągłe*, WNT Warszawa, 2008.				
2.	M. Nowak, *Symulacja komputerowa w problemach decyzyjnych*, AE Katowice, 2007.				
3.	R. F. Barton, *Wprowadzenie do symulacji i gier*, WNT, Warszawa 1974.				
4.	*Instrukcje poszczególnych symulatorów.*				
IX.	**PROWADZĄCY PRZEDMIOT**				
Stopień, Imię i nazwisko	mgr inż. Karol Gazda, mgr inż. Łukasz Grzyb				
adres e-mail	k.gazda@amw.gdynia.pl, l.grzyb@amw.gdynia.pl				

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:	**Podstawy prawne cyberbezpieczeństwa**	*Kod*:	**Ccq**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Stacjonarne		
Kształcenie w zakresie:	Cyberbezpieczeństwo		
Profil:	Ogólnoakademicki		
Liczba ECTS:	4		
Semestr:	4		
Wymagania wstępne:	Podstawowa wiedza z zakresu państwa i prawa		
Język wykładowy:	Polski		
Cel przedmiotu:	**C01**	Zapoznanie słuchaczy z najważniejszymi aktami prawnymi regulującymi problematykę cyberbezpieczeństwa w wymiarze krajowym.	
	C02	Zapoznanie słuchaczy z najważniejszymi aktami prawnymi regulującymi problematykę cyberbezpieczeństwa w wymiarze międzynarodowym.	

II.	**EFEKTY UCZENIA SIĘ**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Ccq_W01**	Posiada wiedzez zakresu prawa krajowego i międzynarodowego oraz norm postępowania w cyberprzestrzeni, wpływających na prawa i obowiązki państw na płaszczyźnie międzynarodowej	Kolowium/ dyskusja
Umiejętności:	**Oku_U01**	Umiejętność analizy krajowych i międzynarodowych aktów prawnych oraz norm z zakresu cyberbezpieczeństwa.	Kolowium/ dyskusja
	Oku_U02	Potrafi znaleźć legitymację do działań państw w cyberprzestrzeni	Kolowium/ dyskusja
Kompetencje społeczne:	**Oku_K01**	Potrafi dokonać subsumpcji normy prawnej w konkretnym stanie faktycznym	Obserwacja podczas zajęć
	Oku_K02	Przestrzega unormowań materialnych i proceduralnych krajowych oraz międzynarodowych dotyczących prowadzenia działań w cyberprzestrzeni	Obserwacja podczas zajęć
	Oku_K03	W oparciu o uzyskaną teoretyczną wiedzę programową potrafi samodzielnie aktualizować i doskonalić swoją wiedzę i umiejętności.	Obserwacja podczas zajęć

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
W01	Zasady poszanowania suwerenności terytorialnej.	5
W02	Zakaz interwencji w sprawy wewnętrzne; zakaz użycia siły.	5

W03	Zakaz przeciwdziałania wykorzystaniu własnego terytorium do czynności szkodliwych dla drugiego państwa (zasada dobrego sąsiedztwa); zasady przypisania cyberoperacji państwu.	5
W04	Naruszenie bezpieczeństwa informacyjnego systemów komputerowych w świetle konkretnych norm prawa międzynarodowego.	5
W05	Przepisy regulujące odpowiedzialność międzynarodową państwa za działania indywidualnych hakerów i grup hakerskich; prawne ramy operacji odwetowych; prawo do samoobrony przed napaścią zbrojną.	5
C01	Problemy z prawnym zdefiniowaniem pojęcia cyberprzestrzeń. Przegląd ustawodawstwa wybranych państw. Status prawny cyberprzestrzeni.	5
C02	Status prawny państw w cyberprzestrzeni. Prawa i obowiązki państw w cyberprzestrzeni.	5
C03	Regulacje międzynarodowe działań w cyberprzestrzeni	5
C04	Krajowa regulacja z zakresu cyberbezpieczeństwa.	5
C05	Unormowania dot. Przestępstw komputerowych	5

IV. KORELACJA EFEKTÓW UCZENIA SIĘ

Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyk PRK*
W01	Ccq_W01,	SIB2_W01	P7U_W, P7S_WG
W02	Ccq_W01,	SIB2_W01	P7U_W, P7S_WG
W03	Ccq_W01,	SIB2_W01	P7U_W, P7S_WG
W04	Ccq_W01,	SIB2_W01	P7U_W, P7S_WG
W05	Ccq_W01,	SIB2_W01	P7U_W, P7S_WG
L01	Ccq_U01, Ccq_U02, , Ccq_K01, Ccq_K02, Ccq_K03	SIB2_U01, SIB2_U06, SIB2_K01, SIB2_K05	P7U_U, P7S_UW, P7S_UO, P7U_K, P7S_KK, P7S_KR
L02	Ccq_U01, Ccq_U02, , Ccq_K01, Ccq_K02, Ccq_K03	SIB2_U01, SIB2_U06, SIB2_K01, SIB2_K05	P7U_U, P7S_UW, P7S_UO, P7U_K, P7S_KK, P7S_KR
L03	Ccq_U01, Ccq_U02, , Ccq_K01, Ccq_K02, Ccq_K03	SIB2_U01, SIB2_U06, SIB2_K01, SIB2_K05	P7U_U, P7S_UW, P7S_UO, P7U_K, P7S_KK, P7S_KR
L04	Ccq_U01, Ccq_U02, , Ccq_K01, Ccq_K02, Ccq_K03	SIB2_U01, SIB2_U06, SIB2_K01, SIB2_K05	P7U_U, P7S_UW, P7S_UO, P7U_K, P7S_KK, P7S_KR
L05	Ccq_U01, Ccq_U02, , Ccq_K01, Ccq_K02, Ccq_K03	SIB2_U01, SIB2_U06, SIB2_K01, SIB2_K05	P7U_U, P7S_UW, P7S_UO, P7U_K, P7S_KK, P7S_KR

V. NAKŁAD PRACY STUDENTA

Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**25**	**X**	**105**	**4**
Ćwiczenia	**25**			
Seminaria	**0**			
Laboratoria	**0**			
Konsultacje (zaliczenie nieobecności, rozliczenie rygorów, poprawy)	**5**			
Przygotowanie do ćwiczeń	**X**	**15**		
Opanowanie informacji		**20**		
Przygotowanie do rozliczenia rygorów		**15**		
RAZEM	**55**	**50**		

VI. METODY DYDAKTYCZNE

1.	prezentacja multimedialna
2	wybrane symulatory
3	praca w grupach i inne formy aktywizujące

VII. FORMA ZALICZENIA PRZEDMIOTU

Rygor	*Kryteria składowe*	*Waga*
Zaliczenie	wykonanie określonych zadań podczas ćwiczeń	0,4
	test	0,6

VIII.	LITERATURA
	OBOWIĄZKOWA
1.	Schmitt M.N., Tallinn Manual on the International law applicable to the cyber warfare, Cambridge 2013.
2.	Adamski A., Prawo karne komputerowe, Warszawa 2000..
	UZUPEŁNIAJĄCA
1.	Adamski A., Przestępczość w cyberprzestrzeni. Prawne środki przeciwdziałania zjawisku w Polsce na tle projektu Konwencji Rady Europy, Toruń 2001.
2.	Banasiński C., Rojszczak M. (red.), Cyberbezpieczeństwo, Warszawa 2020.
3.	Klimburg A., National Cyber Security. Framework Manual, NATO Cooperative Cyber Defence Centre of Excellence Tallin, Estonia 2012.

IX.	PROWADZĄCY PRZEDMIOT
Stopień, Imię i nazwisko	dr Alicja Żukowska
adres e-mail	a.zukowska@amw.gdynia.pl

3.4. Karty przedmiotów modułu kształceniastudiów stacjonarnych w zakresie Analiza danych i informatyka śledcza – C

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:	**Pozyskiwanie i analiza danych z technologii bezzałogowych**	*Kod*:	**Wyn**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Stacjonarne		
Kształcenie w zakresie:	Analiza danych i informatyka śledcza		
Profil:	Ogólnoakademicki		
Liczba ECTS:	5		
Semestr:	3		
Wymagania wstępne:	Brak		
Język wykładowy:	Polski z terminologią angielską		
Cel przedmiotu:	**C01**	Zapoznanie studentów z konstrukcjami, technikami budowy, komputerami, aparaturami i kontrolerami technologii bezzałogowych	
	C02	Zapoznanie studentów z metodami, technikami i narzędziami informatyki śledczej do pozyskiwania danych z technologii bezzałogowych	
	C03	Wykształcenie umiejętności analizy danych pozyskiwanych z technologii bezzałogowych.	

II.	**EFEKTY UCZENIA SIĘ**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Wyn _W01**	Student zna i rozumie budowę i zasadę działania bezzałogowych statków powietrznych, pojazdów lądowych i morskich.	Kolokwium
	Wyn _W02	Student zna metody, techniki i narzędzia do pozyskiwania danych z technologii bezzałogowych.	Kolokwium
	Wyn _W03	Student zna techniki i zasady analizowania pozyskanego materiału z technologii bezzałogowych	Kolokwium
Umiejętności:	**Wyn _U01**	Student potrafi pozyskiwać dane z urządzeń bezzałogowych zgodnie z etyką informatyki śledczej	Zadania na laboratorium / Kolokwium
	Wyn _U02	Student potrafi analizować i korelować pozyskane dane z urządzeń bezzałogowych	Zadania na laboratorium / Kolokwium
Kompetencje społeczne:	**Wyn _K01**	Student krytycznie ocenia posiadaną wiedzę i umiejętności z zakresu pozyskiwania danych z technologii bezzałogowych oraz potrafi je doskonalić	Zadania na laboratorium

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
W01	Budowa i zasada działania pojazdów bezzałogowych	4
W02	Komputery, aparatury, kontrolery i systemy telemetryczne technologii bezzałogowych	4

W03	Komunikacja pojazdów bezzałogowych	4
W04	Techniki pozyskiwania danych z urządzeń bezzałogowych	4
W05	Techniki analizy danych z pozyskanych urządzeń technologii bezzałogowych	4
C01	Analiza budowa i testowanie działania pojazdów bezzałogowych	4
C02	Analiza kontrolerów i komponentów zapisujących dane na pokładzie urządzeń bezzałogowych	4
C03	Testowanie komunikacji urządzeń bezzałogowych i analiza widma radiowego	4
C04	Pozyskiwanie danych z urządzeń bezzałogowych	4
C05	Analiza danych z pozyskanych urządzeń technologii bezzałogowych	4
L01	Analiza struktur i systemów plików na nośnikach pojazdów bezzałogowych	4
L02	Proces pozyskiwania danych z uszkodzonych urządzeń bezzałogowych	4
L03	Klasyfikacja danych	4
L04	Analiza narzędzi do informatyki śledczej pojazdów bezzałogowych	4
L05	Analiza LOGów odzyskanych z kontrolerów pojazdów bezzałogowych	4

IV.	**KORELACJA EFEKTÓW UCZENIA SIĘ**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyk PRK*
W01	Wyn_W01, Wyn _W02	SIB2_W01	P7U_W, P7S_WG
W02	Wyn_W01, Wyn _W02	SIB2_W01	P7U_W, P7S_WG
W03	Wyn_W01, Wyn _W02	SIB2_W01	P7U_W, P7S_WG
W04	Wyn_W01, Wyn _W02	SIB2_W01	P7U_W, P7S_WG
W05	Wyn_W01, Wyn _W02, Wyn_W03	SIB2_W01	P7U_W, P7S_WG
C01	Wyn_U01, Wyn_U02, Wyn_K01	SIB2_U01, SIB2_U06, K01	P7U_U, P7S_UW, P7S_UO, P7U_K, P7S_KK
C02	Wyn_U01, Wyn_U02, Wyn_K01	SIB2_U01, SIB2_U06, K01	P7U_U, P7S_UW, P7S_UO, P7U_K, P7S_KK
C03	Wyn_U01, Wyn_U02, Wyn_K01	SIB2_U01, SIB2_U06, K01	P7U_U, P7S_UW, P7S_UO, P7U_K, P7S_KK
C04	Wyn_U01, Wyn_U02, Wyn_K01	SIB2_U01, SIB2_U06, K01	P7U_U, P7S_UW, P7S_UO, P7U_K, P7S_KK
C05	Wyn_U01, Wyn_U02, Wyn_K01	SIB2_U01, SIB2_U06, K01	P7U_U, P7S_UW, P7S_UO, P7U_K, P7S_KK

V.	**NAKŁAD PRACY STUDENTA**			
Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**20**	**X**	**126**	**5**
Ćwiczenia	**20**			
Seminaria	**0**			
Laboratorium	**20**			
Konsultacje (zaliczenie nieobecności, rozliczenie rygorów, pOzoawy)	**6**			
Przygotowanie do ćwiczeń	**X**	**15**		
Opanowanie informacji		**25**		
Przygotowanie do rozliczenia rygorów		**20**		
RAZEM	**66**	**60**		

VI.	**METODY DYDAKTYCZNE**
1.	Wykład z prezentacjami multimedialnymi
2.	Praca z dokumentacją

3.	Laboratorium na stanowiskach komputerowych – praca indywidualna, praca w grupach	
VII.	**FORMA ZALICZENIA PRZEDMIOTU**	
Rygor	*Kryteria składowe*	*Waga*
Egzamin	Kolokwium	0,5
	Ocena z laboratorium	0,5
VIII.	LITERATURA **PODSTAWOWA I UZUPEŁNIAJĄCA**	
OBOWIĄZKOWA		
1.	Wiktor Wyszywacz, Drony Budowa, Loty, Przepisy	
2.	William Oettinger, Informatyka śledcza. Gromadzenie, analiza i zabezpieczanie dowodów elektronicznych dla początkujących	
UZUPEŁNIAJĄCA		
1.		
IX.	**PROWADZĄCY PRZEDMIOT**	
Stopień, Imię i nazwisko	por. mgr Łukasz GRZYB	
adres e-mail	l.grzyb@amw.gdynia.pl	

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:	**Zastosowanie kryptologii w informatyce śledczej**	*Kod*:	**Lju**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Stacjonarne		
Kształcenie w zakresie:	Analiza danych i informatyka śledcza		
Profil:	Ogólnoakademicki		
Liczba ECTS:	3		
Semestr:	3		
Wymagania wstępne:	Brak		
Język wykładowy:	Polski		
Cel przedmiotu:	**C01**	Zapoznanie studentów z podstawowymi technikami kryptologii wykorzystywanymi w informatyce śledczej.	
	C02	Zapoznanie studentów z praktycznym zastosowaniem metod kryptologicznych do analizy danych cyfrowych.	
	C03	Wykształcenie umiejętności rozwiązywania problemów kryptograficznych w kontekście śledztw informatycznych	

II.	**EFEKTY UCZENIA SIĘ**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Lju_W01**	Student zna i rozumie techniki kryptologii stosowane w informatyce śledczej.	Kolokwium
	Lju_W02	Student zna standardy i protokoły kryptograficzne wykorzystywane w analizie danych cyfrowych.	Kolokwium
	Lju_W03	Student rozumie zasady działania narzędzi kryptograficznych stosowanych w śledztwach cyfrowych.	Kolokwium
Umiejętności:	**Lju_U01**	Student potrafi zastosować techniki kryptologiczne do analizy danych zebranych podczas śledztwa.	Zadania na laboratorium
	Lju_U02	Student potrafi wykorzystywać narzędzia kryptograficzne do szyfrowania i deszyfrowania danych śledczych.	Zadania na laboratorium, kolokwium
Kompetencje społeczne:	**Lju_K01**	Student krytycznie ocenia posiadaną wiedzę i umiejętności z zakresu kryptologii oraz potrafi je doskonalić w kontekście śledztw informatycznych.	Zadania na laboratorium

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
W01	Wprowadzenie do kryptologii w informatyce śledczej	2
W02	Standardy i protokoły kryptograficzne	2
W03	Techniki szyfrowania i deszyfrowania danych	2
W04	Narzędzia kryptograficzne w śledztwach cyfrowych	2
W05	Praktyczne zastosowania kryptologii w analizie danych	2
L01	Szyfrowanie danych	4
L02	Deszyfrowanie danych	4

L03	Wykorzystanie narzędzi kryptograficznych	4
L04	Analiza danych śledczych	4
L05	Praktyczne studium przypadków	4
W01	Wprowadzenie do kryptologii w informatyce śledczej	2
W02	Standardy i protokoły kryptograficzne	2
W03	Techniki szyfrowania i deszyfrowania danych	2
W04	Narzędzia kryptograficzne w śledztwach cyfrowych	2
W05	Praktyczne zastosowania kryptologii w analizie danych	2
L01	Szyfrowanie danych	4

IV.	**KORELACJA EFEKTÓW UCZENIA SIĘ**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyk PRK*
W01	Lju_W01, Lju_W02, Lju _W03	SIB2_W01, SIB2_W02	P7U_W, P7S_WG, P7S_WK
W02	Lju_W01, Lju_W02, Lju _W03	SIB2_W01, SIB2_W02	P7U_W, P7S_WG, P7S_WK
W03	Lju_W01, Lju_W02, Lju _W03	SIB2_W01, SIB2_W02	P7U_W, P7S_WG, P7S_WK
W04	Lju_W01, Lju_W02, Lju _W03	SIB2_W01, SIB2_W02	P7U_W, P7S_WG, P7S_WK
W05	Lju_W01, Lju_W02, Lju _W03	SIB2_W01, SIB2_W02	P7U_W, P7S_WG, P7S_WK
L01	Lju_U01, Lju_U02, Lju_K01	SIB2_U01, SIB2_U02, SIB2_K01	P7U_U, P7S_UW, P7U_K, P7S_KK
L02	Lju_U01, Lju_U02, Lju_K01	SIB2_U01, SIB2_U02, SIB2_K01	P7U_U, P7S_UW, P7U_K, P7S_KK
L03	Lju_U01, Lju_U02, Lju_K01	SIB2_U01, SIB2_U02, SIB2_K01	P7U_U, P7S_UW, P7U_K, P7S_KK
L04	Lju_U01, Lju_U02, Lju_K01	SIB2_U01, SIB2_U02, SIB2_K01	P7U_U, P7S_UW, P7U_K, P7S_KK
L05	Lju_U01, Lju_U02, Lju_K01	SIB2_U01, SIB2_U02, SIB2_K01	P7U_U, P7S_UW, P7U_K, P7S_KK

V.	**NAKŁAD PRACY STUDENTA**			
Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**20**		**80**	**3**
Ćwiczenia				
Laboratorium	**25**			
Konwersatoria				
Konsultacje	**5**			
Rozliczenie rygorów przedmiotu				
Przygotowanie do ćwiczeń		**15**		
Wykonanie zadań domowych		**10**		
Przygotowanie do rozliczenia rygorów		**5**		
RAZEM	**50**	**30**		

VI.	**METODY DYDAKTYCZNE**
1.	Wykład z prezentacjami multimedialnymi
2.	Praca z dokumentacją
3.	Laboratorium na stanowiskach komputerowych – praca indywidualna, praca w grupach

VII.	**FORMA ZALICZENIA PRZEDMIOTU**	
Rygor	*Kryteria składowe*	*Waga*
Zaliczenie	Kolokwium	0,5
	Ocena z laboratorium	0,5

VIII.	**LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA**
	OBOWIĄZKOWA
1.	Marcin Karbowski, Podstawy kryptografii. Wydanie III, Helion, Gliwice 2014
2.	Harlan Carvey, "Windows Forensic Analysis Toolkit", Syngress 2018
	UZUPEŁNIAJĄCA
1.	Christopher L.T. Brown, "Computer Evidence: Collection and Preservation", Charles River Media 2012

2.	Eoghan Casey, "Handbook of Digital Forensics and Investigation", Academic Press 2010
IX.	**PROWADZĄCY PRZEDMIOT**
Stopień, Imię i nazwisko	mgr inż. Kamil SZCZEPANIUK
adres e-mail	k.szczepaniuk@amw.gdynia.pl

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:	**Testy penetracyjne**	*Kod*:	**Mte**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Stacjonarne		
Specjalność:	Analiza danych i informatyka śledcza		
Profil:	Ogólnoakademicki		
Liczba ECTS:	4		
Semestr:	3		
Wymagania wstępne:	brak		
Język wykładowy:	Polski z terminologią angielską		
Cel przedmiotu:	**C01**	Zapoznanie studentów z metodyką prowadzenia testów penetracyjnych systemów i usług informatycznych.	
	C02	Pozyskanie umiejętności związanych z wykrywaniem podatności w systemach teleinformatycznych.	
	C03	Pozyskanie umiejętności przygotowania oraz przeprowadzenia testu penetracyjnego w systemie Windows oraz systemie Linux.	

II.	**EFEKTY KSZTAŁCENIA**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Mte_ W01**	Zna i rozumie w pogłębiony sposób wybrane fakty, teorie, metody oraz złożone zależności między nimi, także w powiązaniu z innymi dziedzinami różnorodne, złożone uwarunkowania i aksjologiczny kontekst prowadzonej działalności z zakresu teorii bezpieczeństwa, cyberbezpieczeństwa oraz analizy danych i informatyki śledczej. Zna zasady i metody prowadzenia testów penetracyjnych w sieciach komputerowych.	Pytania sprawdzające podczas zajęć. Kolokwium.
	Mte_ W02	Zna i rozumie w pogłębiony sposób zagadnienia związane z bezpieczeństwem informacji oraz wykorzystaniem technologii informacyjnych. Zna zasady i metody prowadzenia testów pod kątem wyszukiwania podatności w systemach i sieciach teleinformatycznych	Rozwiązanie zadań problemowych
Umiejętności:	**Mte_ U01**	Potrafi wykorzystać posiadaną wiedzę z zakresu bezpieczeństwa, cyberbezpieczeństwa oraz formułować i rozwiązywać złożone i nietypowe problemy. Potrafi przygotować oraz przeprowadzić testy penetracyjne w sieciach komputerowych.	Przygotowanie sprawozdania. Kolokwium.
	Mte U02	Potrafi brać udział w debacie z zakresu wykorzystania systemów informacyjnych w bezpieczeństwie - przedstawiać i oceniać różne opinie i stanowiska oraz dyskutować o nich. Potrafi przeprowadzić testy penetracyjne w systemach i sieciach teleinformatycznych pod kątem wyszukiwania podatności z uwzględnieniem właściwej metody ich realizacji.	Przygotowanie sprawozdania. Kolokwium.

	Mte_U03	Potrafi posługiwać się językiem obcym na poziomie B2 Europejskiego Systemu Opisu Kształcenia Językowego ze szczególnym uwzględnienie specjalistycznej terminologii z zakresu wykorzystania systemów informacyjnych w bezpieczeństwie.	Wykonanie ćwiczenia
	Mte_U04	Potrafi samodzielnie planować i realizować własne uczenie się przez całe życie i ukierunkowywać innych w tym zakresie.	Przygotowanie sprawozdania. Kolokwium.
Kompetencje społeczne:	**Mte_K01**	Krytycznie ocenia posiadaną wiedzę i odbierane treści z zakresu teorii bezpieczeństwa, cyberbezpieczeństw oraz analizy danych i informatyki śledczej.	Przygotowanie do zajęć
	Mte_K02	Uznaje znaczenie wiedzy w rozwiązywaniu problemów badawczych i praktycznych oraz zasięga opinii ekspertów w przypadku trudności z samodzielnych rozwiazywaniem problemów dotyczących wykorzystania systemów informacyjnych w bezpieczeństwie	Przygotowanie do zajęć

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
W01	Zajęcia organizacyjne. Wprowadzenie do przedmiotu. Sprawy organizacyjne.	10 min
W02	System teleinformatyczny: Podstawowe definicje; Atrybuty bezpieczeństwa; Bezpieczeństwo systemu teleinformatycznego.	2
W03	Polityka bezpieczeństwa: Podstawowe definicje; Elementy bezpieczeństwa; Zarządzanie bezpieczeństwem; Przykładowa polityka bezpieczeństwa.	2
W04	Metodyka testów penetracyjnych: Definicja testów penetracyjnych; Rodzaje i opis metodyk (OSSTMM, PTES, NIST800-115, Metasploit, Core Impact, OWASP Web Security Testing Guide, Testy penetracyjne ukierunkowane na cel).	4
W05	Etapy testów penetracyjnych: Czynności wstępne; Rozpoznanie pasywne.	2
W06	Etapy testów penetracyjnych: Aspekty prawne; Rozpoznanie aktywne.	4
W07	Etapy testów penetracyjnych: Faza penetracji / ataku;	2
W08	Etapy testów penetracyjnych: Uzyskanie dostępu – eksploracja środowiska.	2
W09	Etapy testów penetracyjnych: Przygotowanie raportu.	2
L01	Realizacja etapów testów penetracyjnych: Czynności wstępne; Rozpoznanie pasywne.	4
L02	Realizacja etapów testów penetracyjnych: Aspekty prawne; Rozpoznanie aktywne.	4
L03	Realizacja etapów testów penetracyjnych: Faza penetracji / ataku;	4
L04	Realizacja etapów testów penetracyjnych: Uzyskanie dostępu – eksploracja środowiska.	4
L05	Realizacja etapów testów penetracyjnych: Przygotowanie raportu.	4
C01	Analiza pakietów ruchu sieciowego z wykorzystaniem programu WireShark – analizy przypadków	15

IV.	**KORELACJA EFEKTÓW KSZTAŁCENIA**		
Forma	*Kod efektu przedmiotu*	*Kod symbolu*	*Kod charakterystyk PRK*
W01	Mte_W01, Mte_W02	SIB2_W01, SIB2_W02,	P7U_W, P7S_WG, P7S_WK,

	Mte_K01, Mte_K02	SIB2_K01, SIB2_K02	P7U_K, P7S_KK
W02	Mte_W01, Mte_W02 Mte_K01, Mte_K02	SIB2_W01, SIB2_W02, SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W03	Mte_W01, Mte_W02 Mte_K01, Mte_K02	SIB2_W01, SIB2_W02, SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W04	Mte_W01, Mte_W02 Mte_K01, Mte_K02	SIB2_W01, SIB2_W02, SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W05	Mte_W01, Mte_W02 Mte_K01, Mte_K02	SIB2_W01, SIB2_W02, SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W06	Mte_W01, Mte_W02 Mte_K01, Mte_K02	SIB2_W01, SIB2_W02, SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W07	Mte_W01, Mte_W02 Mte_K01, Mte_K02	SIB2_W01, SIB2_W02, SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W08	Mte_W01, Mte_W02 Mte_K01, Mte_K02	SIB2_W01, SIB2_W02, SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W09	Mte_W01, Mte_W02 Mte_K01, Mte_K02	SIB2_W01, SIB2_W02, SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
L01	Mte_W01, Mte_W02 Mte_U01, Mte_U02, Mte_U04, Mte_U04, Mte_K01, Mte_K02	SIB2_W01, SIB2_W02, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07, SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK P7U_U, P7S_UW, P7S_UK, P7S_UU P7U_K P7S_KK
L02	Mte_W01, Mte_W02 Mte_U01, Mte_U02, Mte_U04, Mte_U04, Mte_K01, Mte_K02	SIB2_W01, SIB2_W02, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07, SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK P7U_U, P7S_UW, P7S_UK, P7S_UU P7U_K P7S_KK
L03	Mte_W01, Mte_W02 Mte_U01, Mte_U02, Mte_U04, Mte_U04, Mte_K01, Mte_K02	SIB2_W01, SIB2_W02, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07, SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK P7U_U, P7S_UW, P7S_UK, P7S_UU P7U_K P7S_KK
L04	Mte_W01, Mte_W02 Mte_U01, Mte_U02, Mte_U04, Mte_U04, Mte_K01, Mte_K02	SIB2_W01, SIB2_W02, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07, SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK P7U_U, P7S_UW, P7S_UK, P7S_UU P7U_K P7S_KK
L05	Mte_W01, Mte_W02 Mte_U01, Mte_U02, Mte_U04, Mte_U04, Mte_K01, Mte_K02	SIB2_W01, SIB2_W02, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07, SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK P7U_U, P7S_UW, P7S_UK, P7S_UU P7U_K P7S_KK
C01	Mte_W01, Mte_W02 Mte_U01, Mte_U02, Mte_U04, Mte_U04, Mte_K01, Mte_K02	SIB2_W01, SIB2_W02, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07, SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK P7U_U, P7S_UW, P7S_UK, P7S_UU P7U_K P7S_KK

V.	**NAKŁAD PRACY STUDENTA**			
Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**20**		**110**	**4**
Laboratorium	**20**			
Ćwiczenia	**15**			
Konwersatoria				
Konsultacje	**3**			
Rozliczenie rygorów przedmiotu	**2**			
Przygotowanie do ćwiczeń i laboratorium	**x**	**15**		
Opanowanie informacji		**15**		
Przygotowanie do rozliczenia rygorów		**20**		
RAZEM	**60**	**50**		

VI.	METODY DYDAKTYCZNE
1.	Wykład z prezentacją multimedialną
2.	Praca przy stanowisku komputerowym
3.	Rozwiązywanie zadań problemowych
4.	Studiowanie literatury

VII. FORMA ZALICZENIA PRZEDMIOTU		
Rygor	*Kryteria składowe*	*Waga*
Zaliczenie	Ocena za aktywność na zajęciach	0,2
	Ocena z kolokwium	0,8
Zaliczenie	Aktywność na zajęciach laboratoryjnych	0,2
	Sprawozdania z laboratorium	0,8

VIII.	LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA
	OBOWIĄZKOWA
1.	Białas A., Bezpieczeństwo informacji i usług, Wydawnictwo Naukowo-Techniczne, Warszawa 2007;
2.	Khawaja G. Kali Linux i testy penetracyjne. Biblia. Wydawnictwo Helion, Gliwice 2022;
3.	Velu V. K., Kali Linux i zaawansowane testy penetracyjne. Zostań ekspertem cyberbezpieczeństwa za pomocą Metasploit, Nmap, Wireshark i Burp Suite. Wydanie IV., Wydawnictwo Helion, Gliwice 2023;
4.	Georgia W., Bezpieczny system w praktyce, Wyższa szkoła hackingu i testy penetracyjne, Wydawnictwo Helion, 2015;
5.	Kim P., Podręcznik pentestera. Bezpieczeństwo systemów informatycznych, Wydawnictwo Helion, Gliwice 2014;
6.	Tanner N. H., Blue Team i cyberbezpieczeństwo. Zestaw narzędzi dla specjalistów od zabezpieczenia sieci. Wydawnictwo Helion, Gliwice 2021;
	UZUPEŁNIAJĄCA
1.	Ustawa z dnia 16 lipca 2004r. Prawo telekomunikacyjne (Dz.U. 2004 Nr 171 poz. 1800, tekst ujednolicony);
2.	Ustawa z dnia 18 lipca 2002r. o świadczeniu usług drogą elektroniczną (Dz.U. 2002 Nr 144 poz. 1204, z późn. zm.);
3.	Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2018 r. poz. 1560, z 2019 r. poz. 2020, 2248);
4.	Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (Dz.U. 2020 poz. 1444, tekst jednolity);
5.	Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2017 poz. 2247, tekst jednolity);
6.	Rozporządzenie Rady Ministrów z dnia 11 września 2018 r. w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych;
7.	PN-13335-1, Technika informatyczna - Wytyczne do zarządzania bezpieczeństwem systemów informatycznych - Pojęcia i modele bezpieczeństwa systemów informatycznych, 1999;
8.	NIST National Institute of Standard and Technology - Special Publication 800-37, Revision 2. Risk Management Framework for Information Systems and Organizations, grudzień 2018;
9.	OSSTMM 3 The Open Source Security Testing Methodology Manual. Contemporary Security Testing and Analysis, Pete Herzog, ISECOM, grudzień 2010;

10.	Technical Guide to Information Security Testing and Assessment (SP 800-115). Recommendations of the National Institute of Standards and Technology, wrzesień 2008;	
11.	PTES Penetration Testing Execution Standard, http://www.pentest-standard.org;	
12.	OWASP The Open Web Application Security Project, https://owasp.org/;	
IX.	**PROWADZĄCY PRZEDMIOT**	
Stopień, Imię i nazwisko		kmdr por. dr inż. Adam Stojałowski
adres e-mail		a.stojalowski@amw.gdynia.pl

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:	**Bezpieczeństwo sieci komputerowych i bezprzewodowych**	*Kod*:	**Oxk**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Stacjonarne		
Kształcenie w zakresie:	Analiza danych i informatyka śledcza		
Profil:	Ogólnoakademicki		
Liczba ECTS:	5		
Semestr:	3		
Wymagania wstępne:	Brak		
Język wykładowy:	Polski		
Cel przedmiotu:	**C01**	Zapoznanie studentów z zasadami działania sieci komputerowych, ich klasyfikacją i charakterystyką oraz urządzeniami sieciowymi i wykorzystywanymi mediami transmisyjnymi.	
	C02	Zapoznanie studentów z warstwową architekturą sieci oraz protokołami sieciowymi wykorzystywanymi do komunikacji hostów na poziomie poszczególnych warstw.	
	C03	Wykształcenie umiejętności podstawowej konfiguracji urządzeń sieciowych dla realizacji komunikacji z wykorzystaniem sieci komputerowej, obserwacji i analizy działania sieci oraz ruchu sieciowego, diagnozowania podstawowych nieprawidłowości w działaniu sieci komputerowych	

II.	**EFEKTY UCZENIA SIĘ**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Oxk_W01**	Student zna podstawowe urządzenia i standardy sieciowe oraz ich rolę w transmisji danych w sieciach lokalnych i rozległych o różnych topologiach.	Egzamin
	Oxk_W02	Student zna podstawowe modele warstwowe sieci oraz role poszczególne warstwy w procesie transmisji danych między hostami sieci.	Egzamin
	Oxk_W03	Student zna podstawowe protokoły transmisyjne i ich przyporządkowanie do warstwy na poziomie której są wykorzystywane.	Egzamin
Umiejętności:	**Oxk_U01**	Student potrafi zbudować i skonfigurować prostą sieć lokalną.	Egzamin, rozwiązywanie zadań
	Oxk_U02	Student potrafi analizować ruch sieciowy na podstawie danych sterujących poszczególnych warstw sieciowych	Egzamin, rozwiązywanie zadań
	Oxk_U03	Student potrafi łączyć sieci lokalne i konfigurować parametry routingu.	Egzamin, rozwiązywanie zadań
	Oxk_U04	Student potrafi zarządzać przychodzącym do sieci ruchem oraz podejmować działania zwiększające bezpieczeństwo sieci.	Egzamin, rozwiązywanie zadań

Kompetencje społeczne:	**Oxk_K01**	Student w oparciu o uzyskaną podstawową wiedzę z zakresu sieci teleinformatycznych potrafi doskonalić swoją wiedzę i umiejętności z tego obszaru.	Praca w grupach

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
W01	Klasyfikacja i ogólna charakterystyka sieci komputerowych.	2
W02	Warstwowe architektury sieciowe.	3
W03	Warstwa łącza danych, adresacja MAC, standard Ethernet.	3
W04	Protokoły warstwy sieciowej, adresacja IPv4 i IPv6	3
W05	Protokoły warstwy transportowej vs protokoły aplikacji.	3
W06	Zasady i rodzaje routingu.	3
W07	Bezpieczeństwo sieci bezprzewodowych. Ataki na sieci bezprzewodowe WLAN.	3
L01	Wyznaczanie adresu sieci i rozgłoszeniowego sieci na podstawie różnych klas adresów IP hostów, zapoznanie z programem Cisco Packet Tracer – budowa sieci LAN z serwerem DHCP.	8
L02	Protokół TCP, analiza faz zestawiania i rozłączania sesji w warstwie transportowej. Analiza nagłówka protokołu TCP i UDP	5
L03	Routing statyczny i dynamiczny, konfiguracja routerów, podgląd i analiza tablicy routingu, porównanie metryk trasowania oraz dystansu administracyjnego protokołów routingu	5
L04	Konfiguracja usługi NAT oraz analiza tablicy NAT w ustawieniach routera, analiza przesyłanych pakietów IP pod kątem tłumaczenia adresów i portów.	5
L05	Podstawy bezpieczeństwa w sieciach komputerowych. Konfiguracja reguł zapory sieciowej na serwerze oraz weryfikacja ich działania. Konfigurowanie sieci VPN – tunelowanie GRE i IPsec. Tworzenie sieci VLAN oraz zapewnienie transmisji danych między nimi (metoda „router na patyku”, wykorzystanie podinterfejsów routera).	7
L06	Podstawy bezpieczeństwa w sieciach bezprzewodowych. Konfiguracja i zarządzanie AP. Mechanizmy bezpieczeństwa wykorzystywane w sieciach bezprzewodowych.	10

IV.	**KORELACJA EFEKTÓW UCZENIA SIĘ**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyk PRK*
W01	Oxk_W01, Oxk_W02, Oxk_W03, Oxk_K01	SIB2_W01, SIB2_W02, SIB2_K01	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W02	Oxk_W01, Oxk_W02, Oxk_W03, Oxk_K01	SIB2_W01, SIB2_W02, SIB2_K01	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W03	Oxk_W01, Oxk_W02, Oxk_W03, Oxk_K01	SIB2_W01, SIB2_W02, SIB2_K01	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W04	Oxk_W01, Oxk_W02, Oxk_W03, Oxk_K01	SIB2_W01, SIB2_W02, SIB2_K01	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W05	Oxk_W01, Oxk_W02, Oxk_W03, Oxk_K01	SIB2_W01, SIB2_W02, SIB2_K01	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W06	Oxk_W01, Oxk_W02, Oxk_W03, Oxk_K01	SIB2_W01, SIB2_W02, SIB2_K01	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W07	Oxk_W01, Oxk_W02, Oxk_W03, Oxk_K01	SIB2_W01, SIB2_W02, SIB2_K01	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
L01	Oxk_W01, Oxk_U01, Oxk_U02, Oxk_U03, Oxk_U04, Oxk_K01	SIB2_W01, SIB2_U01 SIB2_U02, SIB2_K01	P7U_W, P7S_WG, P7U_U, P7S_UW, P7U_K, P7S_KK

L02	Oxk_W01, Oxk_U01, Oxk_U02, Oxk_U03, Oxk_U04, Oxk_K01	SIB2_W01, SIB2_U01 SIB2_U02, SIB2_K01	P7U_W, P7S_WG, P7U_U, P7S_UW P7U_K, P7S_KK
L03	Oxk_W01, Oxk_U01, Oxk_U02, Oxk_U03, Oxk_U04, Oxk_K01	SIB2_W01, SIB2_U01 SIB2_U02, SIB2_K01	P7U_W, P7S_WG, P7U_U, P7S_UW P7U_K, P7S_KK
L04	Oxk_W01, Oxk_U01, Oxk_U02, Oxk_U03, Oxk_U04, Oxk_K01	SIB2_W01, SIB2_U01 SIB2_U02, SIB2_K01	P7U_W, P7S_WG, P7U_U, P7S_UW P7U_K, P7S_KK
L05	Oxk_W01, Oxk_U01, Oxk_U02, Oxk_U03, Oxk_U04, Oxk_K01	SIB2_W01, SIB2_U01 SIB2_U02, SIB2_K01	P7U_W, P7S_WG, P7U_U, P7S_UW P7U_K, P7S_KK
L06	Oxk_W01, Oxk_U01, Oxk_U02, Oxk_U03, Oxk_U04, Oxk_K01	SIB2_W01, SIB2_U01 SIB2_U02, SIB2_K01	P7U_W, P7S_WG, P7U_U, P7S_UW P7U_K, P7S_KK

V. NAKŁAD PRACY STUDENTA

Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**20**		**126**	**5**
Ćwiczenia				
Seminaria				
Laboratoria	**40**			
Konsultacje	**5**			
Rozliczenie rygorów przedmiotu	**1**			
Przygotowanie do ćwiczeń		**20**		
Wykonanie zadań domowych		**20**		
Przygotowanie do rozliczenia rygorów		**20**		
RAZEM	**66**	**60**		

VI. METODY DYDAKTYCZNE

1.	Metody podające: Wykłady z prezentacjami multimedialnymi
2.	Metody aktywizujące: pogadanka, obserwacja, praca z dokumentacją, praca w grupach, case study.
3.	Ćwiczenia na stanowiskach komputerowych

VII. FORMA ZALICZENIA PRZEDMIOTU

Rygor	*Kryteria składowe*	*Waga*
Zaliczenie	Ocena z egzaminu (materiał z wykładów)	0,4
	Ocena z ćwiczeń	0,6

VIII. LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

OBOWIĄZKOWA

1.	Józefiok A., *Budowa sieci komputerowych na przełącznikach i routerach Cisco*, Helion, Gliwice 2013
2.	Wrotek W., *Sieci komputerowe*, Helion, Gliwice 2016

UZUPEŁNIAJĄCA

1.	Tanenbaum, Wetherall, Sieci komputerowe, Helion, Gliwice 2012
2.	Kluczewski J., Bezpieczeństwo sieci komputerowych (ebook), Itstart, Piekary Śląskie 2019
3.	Sportack M., Sieci komputerowe. Księga eksperta, Helion, Gliwice 2004

IX. PROWADZĄCY PRZEDMIOT

Stopień, Imię i nazwisko	mgr Grzegorz PIOTROWSKI
adres e-mail	grzegorz.piotrowski@c2o.eu

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:	**Techniki pozyskiwania cyfrowego materiału dowodowego**	*Kod*:	**Lkh**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Stacjonarne		
Kształcenie w zakresie:	Analiza danych i informatyka śledcza		
Profil:	Ogólnoakademicki		
Liczba ECTS:	5		
Semestr:	4		
Wymagania wstępne:	Brak		
Język wykładowy:	Polski		
Cel przedmiotu:	**C01**	Zapoznanie studentów z zasadami zachowania łańcucha dowodowego.	
	C02	Zapoznanie studentów z technikami pozyskiwania cyfrowego materiału dowodowego z wykorzstaniem specjalistycznych narzędzi oraz oprogramowania.	
	C03	Wykształcenie umiejętności dopasowania właściwych technik pozyskiwania cyfrowego materiału dowodowego względem badanych urządzeń.	

II.	**EFEKTY UCZENIA SIĘ**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Lkh_W01**	Student zna podstawowe urządzenia i oprogramowanie oraz ich rolę w zapewnieniu integralności danych łańcucha dowodowego.	Egzamin
	Lkh_W02	Student zna podstawowe techiniki pozyskiwania cyfrowego materiału dowodowego.	Egzamin
	Lkh_W03	Student zna etapy akwizycji danych w odniesieniu do badanych urządzeń.	Egzamin
Umiejętności:	**Lkh_U01**	Student potrafi przygotować urządzenie do zabezpieczenia danych.	Egzamin, rozwiązywanie zadań
	Lkh_U02	Student potrafi dopasować narzędzia i techniki do badanego urządzenia.	Rozwiązywanie zadań
	Lkh_U03	Student potrafi przeprowadzić proces akwizycji danych.	Rozwiązywanie zadań
	Lkh_U04	Student potrafi zapewnić integralność danych na potrzeby zachowania łańcucha dowodowego.	Rozwiązywanie zadań
Kompetencje społeczne:	**Lkh_K01**	Student w oparciu o uzyskaną podstawową wiedzę z zakresu pozyskiwania cyfrowego materiału dowodowego potrafi doskonalić swoją wiedzę i umiejętności z tego obszaru.	Praca w grupach

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

W01	Klasyfikacja i ogólna charakterystyka urządzeń poddawanych badaniom śledczym.	2
W02	Narzędzia sprzętowe oraz oprogramowania do informatyki śledczej.	3
W03	Zasady zachowania łańcucha dowodowego.	3
W04	Klasyczne techniki pozyskiwania cyfrowego materiału dowodowego	3
W05	Alternatywen techniki pozyskiwania cyfrowego materiału dowodowego	3
W06	Analiza zgromadzonego materiału dowodowego	3
W07	Raportowanie wyników badań	3
L01	Przegląd i analiza typów urządzeń mogących przechowywać cyfrowy materiał dowodowy	10
L02	Narzędzia do pozyskiwania cyfrowego materiału dowodowego	5
L03	Oprogramowanie do pozyskiwania cyfrowego materiału dowodowego	5
L04	Techiniki do pozyskiwania cyfrowego materiału dowodowego z systemów Windows, Linux, MacOS	5
L05	Narzędzia do pozyskiwania cyfrowego materiału dowodowego z urządzeń mobilnych	5
L06	Analiza oraz raportowanie ujawnionego materiału dowodowego.	10

IV.	**KORELACJA EFEKTÓW UCZENIA SIĘ**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyk PRK*
W01	Lkh_W01, Lkh_W02, Lkh_W03, Lkh_K01	SIB2_W01, SIB2_W02, SIB2_K01	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W02	Lkh_W01, Lkh_W02, Lkh_W03, Lkh_K01	SIB2_W01, SIB2_W02, SIB2_K01	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W03	Lkh_W01, Lkh_W02, Lkh_W03, Lkh_K01	SIB2_W01, SIB2_W02, SIB2_K01	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W04	Lkh_W01, Lkh_W02, Lkh_W03, Lkh_K01	SIB2_W01, SIB2_W02, SIB2_K01	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W05	Lkh_W01, Lkh_W02, Lkh_W03, Lkh_K01	SIB2_W01, SIB2_W02, SIB2_K01	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W06	Lkh_W01, Lkh_W02, Lkh_W03, Lkh_K01	SIB2_W01, SIB2_W02, SIB2_K01	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W07	Lkh_W01, Lkh_W02, Lkh_W03, Lkh_K01	SIB2_W01, SIB2_W02, SIB2_K01	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
L01	Lkh_W01, Lkh_U01, Lkh_U02, Lkh_U03, Lkh_U04, Lkh_K01	SIB2_W01, SIB2_U01 SIB2_U02, SIB2_K01	P7U_W, P7S_WG, P7U_U, P7S_UW, P7U_K, P7S_KK
L02	Lkh_W01, Lkh_U01, Lkh_U02, Lkh_U03, Lkh_U04, Lkh_K01	SIB2_W01, SIB2_U01 SIB2_U02, SIB2_K01	P7U_W, P7S_WG, P7U_U, P7S_UW P7U_K, P7S_KK
L03	Lkh_W01, Lkh_U01, Lkh_U02, Lkh_U03, Lkh_U04, Lkh_K01	SIB2_W01, SIB2_U01 SIB2_U02, SIB2_K01	P7U_W, P7S_WG, P7U_U, P7S_UW P7U_K, P7S_KK
L04	Lkh_W01, Lkh_U01, Lkh_U02, Lkh_U03, Lkh_U04, Lkh_K01	SIB2_W01, SIB2_U01 SIB2_U02, SIB2_K01	P7U_W, P7S_WG, P7U_U, P7S_UW P7U_K, P7S_KK
L05	Lkh_W01, Lkh_U01, Lkh_U02, Lkh_U03, Lkh_U04, Lkh_K01	SIB2_W01, SIB2_U01 SIB2_U02, SIB2_K01	P7U_W, P7S_WG, P7U_U, P7S_UW P7U_K, P7S_KK
L06	Lkh_W01, Lkh_U01, Lkh_U02, Lkh_U03, Lkh_U04, Lkh_K01	SIB2_W01, SIB2_U01 SIB2_U02, SIB2_K01	P7U_W, P7S_WG, P7U_U, P7S_UW P7U_K, P7S_KK

V.	**NAKŁAD PRACY STUDENTA**			
Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**20**		**126**	**5**

Ćwiczenia				
Seminaria				
Laboratoria	**40**			
Konsultacje	**5**			
Rozliczenie rygorów przedmiotu	**1**			
Przygotowanie do ćwiczeń		**20**		
Wykonanie zadań domowych		**20**		
Przygotowanie do rozliczenia rygorów		**20**		
RAZEM	**66**	**60**		

VI.	**METODY DYDAKTYCZNE**
1.	Metody podające: Wykłady z prezentacjami multimedialnymi
2.	Metody aktywizujące: obserwacja, praca z dokumentacją, praca w grupach, case study.
3.	Ćwiczenia na stanowiskach komputerowych

VII.	**FORMA ZALICZENIA PRZEDMIOTU**	
Rygor	*Kryteria składowe*	*Waga*
Zaliczenie	Ocena z egzaminu (materiał z wykładów)	0,4
	Ocena z ćwiczeń	0,6

VIII.	**LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA**
	OBOWIĄZKOWA
1.	Kasprzak W.A. (2015), Ślady cyfrowe. Studium prawno-kryminalistyczne, Difin, Warszawa.
2.	Kosiński J. (2015), Paradygmaty cyberprzestępczości, Difin, Warszawa.
	UZUPEŁNIAJĄCA
1.	ISO/IEC 27041:2015, Information Technology – Security Techniques – Guidance on Assuring Suitability and Adequacy of Incident Investigative Method.
2.	ISO/IEC 27042:2015, Information Technology – Security Techniques – Guidelines for the Analysis and Interpretation of Digital Evidence.
3.	ISO/IEC 27043:2015, Information Technology – Security Techniques – Incident Investigation Principles and Processes.

IX.	**PROWADZĄCY PRZEDMIOT**
Stopień, Imię i nazwisko	mgr Karol GAZDA
adres e-mail	k.gazda@amw.gdynia.pl

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:	**Biały wywiad – techniki zaawansowane**	*Kod*:	**Tbx**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Stacjonarne		
Kształcenie w zakresie:	Analiza danych i informatyka śledcza		
Profil:	Ogólnoakademicki		
Liczba ECTS:	4		
Semestr:	4		
Wymagania wstępne:	Brak		
Język wykładowy:	Polski		
Cel przedmiotu:	**C01**	Zapoznanie studentów z bezpiecznymi zasadami pozyskiwania informacji oraz pojęciami białego wywiadu i odróżnienie go od pozostałych technik wywiadowczych.	
	C02	Zapoznanie studentów z metodami i narzędziami do pozyskiwania informacji.	
	C03	Wykształcenie umiejętności analizy danych pozyskiwanych z otwartych źródeł.	

II.	**EFEKTY UCZENIA SIĘ**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Tbx_W01**	Student zna i rozumie różnicę pomiędzy białym wywiadem, a innymi formami wywiadu.	Kolokwium
	Tbx_W02	Student zna metody i narzędzia do pozyskiwania informacji z otwartych źródeł.	Kolokwium
	Tbx_W03	Student zna techniki i zasady analizowania pozyskanego materiału z otwartych źródeł.	Kolokwium
Umiejętności:	**Tbx_U01**	Student potrafi pozyskiwać informacje z otwartych źródeł zgodnie z etyką białego wywiadu.	Zadania na laboratorium / Kolokwium
	Tbx_U02	Student potrafi korzystać z metod, technik i narzędzi służących do pozyskiwania danych z otwartych źródeł narzędzi.	Zadania na laboratorium / Kolokwium
	Tbx_U03	Student potrafi analizować i korelować dane pozyskane z otwartych źródeł.	Zadania na laboratorium / Kolokwium
Kompetencje społeczne:	**Tbx_K01**	Student krytycznie ocenia posiadaną wiedzę i umiejętności z zakresu białego wywiadu oraz potrafi je doskonalić.	Zadania na laboratorium

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
W01	Definicje i pojęcia dotyczące białego wywiadu	4
W02	Źródła informacji	4
W03	Techniki wyszukiwania informacji	4
W04	Narzędzia i oprogramowanie	4
W05	Analiza i weryfikacja informacji	4

L01	Analiza otwartych źródeł informacji	4
L02	Pozyskiwanie danych z otwartych źródeł informacji	4
L03	Zastosowanie technik w procesie pozyskiwania danych	4
L04	Pozyskiwanie danych przy wykorzystaniu narzędzi i oprogramowania do białego wywiadu	4
L05	Weryfikacja autentyczności pozyskanych danych	4
L06	Praktyczne zastosowanie białego wywiadu	5

IV.	**KORELACJA EFEKTÓW UCZENIA SIĘ**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyk PRK*
W01	Tbx_W01, Tbx_W02	SIB2_W01	P7U_W, P7S_WG
W02	Tbx_W01, Tbx_W02	SIB2_W01	P7U_W, P7S_WG
W03	Tbx_W01, Tbx_W02	SIB2_W01	P7U_W, P7S_WG
W04	Tbx_W01, Tbx_W02	SIB2_W01	P7U_W, P7S_WG
W05	Tbx_W01, Tbx_W02, Tbx_W03	SIB2_W01	P7U_W, P7S_WG
L01	Tbx_U01, Tbx_U02, Tbx_U03 Tbx_K01	SIB2_U01, SIB2_U06, K01	P7U_U, P7S_UW, P7S_UO, P7U_K, P7S_KK
L02	Tbx_U01, Tbx_U02, Tbx_U03 Tbx_K01	SIB2_U01, SIB2_U06, K01	P7U_U, P7S_UW, P7S_UO, P7U_K, P7S_KK
L03	Tbx_U01, Tbx_U02, Tbx_U03 Tbx_K01	SIB2_U01, SIB2_U06, K01	P7U_U, P7S_UW, P7S_UO, P7U_K, P7S_KK
L04	Tbx_U01, Tbx_U02, Tbx_U03 Tbx_K01	SIB2_U01, SIB2_U06, K01	P7U_U, P7S_UW, P7S_UO, P7U_K, P7S_KK
L05	Tbx_U01, Tbx_U02, Tbx_U03 Tbx_K01	SIB2_U01, SIB2_U06, K01	P7U_U, P7S_UW, P7S_UO, P7U_K, P7S_KK
L06	Tbx_U01, Tbx_U02, Tbx_U03 Tbx_K01	SIB2_U01, SIB2_U06, K01	P7U_U, P7S_UW, P7S_UO, P7U_K, P7S_KK

V.	**NAKŁAD PRACY STUDENTA**			
Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**20**		**100**	**4**
Ćwiczenia	**0**			
Seminaria				
Laboratorium	**25**			
Konsultacje	**5**			
Rozliczenie rygorów przedmiotu				
Przygotowanie do ćwiczeń		**20**		
Wykonanie zadań domowych		**20**		
Przygotowanie do rozliczenia rygorów		**10**		
RAZEM	**50**	**50**		

VI.	**METODY DYDAKTYCZNE**
1.	Wykład z prezentacjami multimedialnymi
2.	Praca z dokumentacją
3.	Laboratorium na stanowiskach komputerowych – praca indywidualna, praca w grupach

VII.	**FORMA ZALICZENIA PRZEDMIOTU**	
Rygor	*Kryteria składowe*	*Waga*
Zaliczenie	Kolokwium	0,5
	Ocena z laboratorium	0,5

VIII.	**LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA**
	OBOWIĄZKOWA
1.	Krzysztof Wosiński, Bezpieczeństwo osób i systemów IT z wykorzystaniem białego wywiadu
2.	Dawid Kuciel, OSINT – Sztuka zdobywania informacji
	UZUPEŁNIAJĄCA

1.	Wojciech Filipkowski, Wiesław Mądrzejowski, Biały wywiad: otwarte źródła informacji – wokół teorii i praktyki
IX.	**PROWADZĄCY PRZEDMIOT**
Stopień, Imię i nazwisko	por. mgr Łukasz Grzyb
adres e-mail	l.grzyb@amw.gdynia.pl

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:	**Zarzadzanie ryzykiem bezpieczeństwa systemów**	*Kod*:	**Ojb**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Stacjonarne		
Kształcenie w zakresie:	Analiza danych i informatyka śledcza		
Profil:	Ogólnoakademicki		
Liczba ECTS:	4		
Semestr:	4		
Wymagania wstępne:			
Język wykładowy:	Polski		
Cel przedmiotu: **C01**	Zapoznanie studentów z współczesnymi sposobami zarządzania ryzykiem w kontekście bezpieczeństwa systemów IT		
C02	Zapoznanie studentów z metodologią przeprowadzania analizy ryzyka dla bezpieczeństwa systemów IT		

II.	**EFEKTY UCZENIA SIĘ**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Ojb_W01**	Zrozumienie teoretycznych podstaw zarządzania ryzykiem: Znajomość kluczowych koncepcji, metodologii i standardów związanych z identyfikacją, analizą oraz zarządzaniem ryzykiem w bezpieczeństwie systemów informatycznych.	Pytania sprawdzające podczas zajęć. Kolokwium.
	Ojb_W02	Znajomość narzędzi i technik oceny ryzyka: Umiejętność identyfikacji narzędzi i stosowania technik służących do oceny ryzyka, w tym analizy ilościowej i jakościowej.	Rozwiązanie zadań problemowych
	Ojb_W03	Wiedza o strategiach minimalizacji ryzyka: Zrozumienie metod redukcji, transferu, akceptacji i unikania ryzyka w kontekście bezpieczeństwa informacji.	Rozwiązanie zadań problemowych
	Ojb_W04	Zrozumienie prawnych i regulacyjnych aspektów zarządzania ryzykiem: Znajomość przepisów prawnych oraz standardów branżowych mających wpływ na procesy zarządzania ryzykiem w organizacji.	Pytania sprawdzające podczas zajęć. Kolokwium.
Umiejętności:	**Ojb_U01**	Umiejętność przeprowadzania analizy ryzyka: Zdolność do samodzielnego przeprowadzenia kompleksowej analizy ryzyka, w tym identyfikacji zagrożeń, oceny podatności i estymacji potencjalnych skutków.	Rozwiązanie zadań problemowych Wypowiedzi ustne, aktywność w ramach dyskusji.
	Ojb_U02	Projektowanie i implementacja strategii zarządzania ryzykiem: Umiejętność opracowywania efektywnych planów zarządzania ryzykiem oraz implementacji odpowiednich środków bezpieczeństwa.	Sprawozdanie
	Ojb_U03	Monitorowanie i aktualizacja planów zarządzania ryzykiem: Zdolność do ciągłego monitorowania efektywności stosowanych rozwiązań oraz dostosowywania strategii zarządzania ryzykiem do zmieniającego się środowiska.	Rozwiązanie zadań problemowych Wypowiedzi ustne, aktywność w ramach dyskusji.
Kompetencje społeczne:	**Ojb_K01**	Umiejętność pracy zespołowej w zarządzaniu ryzykiem: Zdolność do efektywnej współpracy z różnymi grupami interesariuszy przy analizie i zarządzaniu ryzykiem.	Sprawozdanie

	Ojb_K02	Komunikacja wyników analizy ryzyka: Umiejętność jasnego i przekonującego prezentowania wyników analizy ryzyka, strategii zarządzania i rekomendacji zarówno specjalistom, jak i niespecjalistom.	Rozwiązanie zadań problemowych Wypowiedzi ustne, aktywność w ramach dyskusji.

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
W01	Wprowadzenie do zarządzania ryzykiem w bezpieczeństwie informacji: Podstawy teoretyczne i kluczowe definicje.	4
W02	Metodologie oceny ryzyka: Przegląd popularnych metodologii, takich jak OCTAVE, EBIOS i CRAMM.	4
W03	Identyfikacja i analiza zagrożeń: Techniki identyfikacji zagrożeń i ocena ich potencjalnych skutków.	4
W04	Analiza podatności i ocena wpływu: Metody oceny podatności systemów na zagrożenia i metodologie estymacji wpływu.	4
W05	Strategie minimalizacji ryzyka: Omówienie różnych strategii, takich jak unikanie ryzyka, jego transfer, akceptacja i redukcja.	4
W06	Zarządzanie ryzykiem a przepisy prawne i standardy: Wpływ regulacji prawnych i standardów branżowych na procesy zarządzania ryzykiem.	2
W07	Przyszłość zarządzania ryzykiem w bezpieczeństwie IT: Najnowsze trendy i przewidywane zmiany w obszarze zarządzania ryzykiem.	3
C01	Przeprowadzenie analizy ryzyka krok po kroku: Ćwiczenie praktyczne wykorzystujące wybraną metodologię.	3
C02	Tworzenie macierzy ryzyka: Praktyczne ćwiczenia w budowaniu i analizie macierzy ryzyka.	3
C03	Case study: Analiza rzeczywistego incydentu bezpieczeństwa: Grupowe rozwiązanie studium przypadku.	4
C04	Zarządzanie kryzysowe i planowanie odpowiedzi na incydenty: Opracowywanie planów reagowania na incydenty.	4
C05	Warsztaty z narzędzi do zarządzania ryzykiem: Praktyczne ćwiczenia z użyciem oprogramowania wspomagającego zarządzanie ryzykiem.	3
C06	Negocjacje i komunikacja w zarządzaniu ryzykiem: Symulacje negocjacji z interesariuszami i efektywnej komunikacji wyników analizy ryzyka.	3
C07	Etyczne aspekty zarządzania ryzykiem: Dyskusje na temat dylematów etycznych w zarządzaniu ryzykiem.	3
C08	Projektowanie i ocena polityk bezpieczeństwa: Ćwiczenia związane z opracowywaniem i oceną polityk bezpieczeństwa, które pomagają w zarządzaniu ryzykiem.	2

IV.	**KORELACJA EFEKTÓW UCZENIA SIĘ**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyk PRK*
W01	Ojb_W01, Ojb_W02, Ojb_W03, Ojb_W04, Ojb_U01, Ojb_U02, Ojb_U03 Ojb_K01, Ojb_K02	SIB2_W01, SIB2_W03, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7S_UK P7S_UU, P7U_K, P7S_KK
W02	Ojb_W01, Ojb_W02, Ojb_W03, Ojb_W04, Ojb_U01, Ojb_U02, Ojb_U03 Ojb_K01, Ojb_K02	SIB2_W01, SIB2_W03, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7S_UK P7S_UU, P7U_K, P7S_KK
W03	Ojb_W01, Ojb_W02,	SIB2_W01, SIB2_W03,	P7U_W, P7S_WG, P7S_WK,

	Ojb_W03, Ojb_W04, Ojb_U01, Ojb_U02, Ojb_U03 Ojb_K01, Ojb_K02	SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_U, P7S_UW, P7S_UK P7S_UU, P7U_K, P7S_KK
W04	Ojb_W01, Ojb_W02, Ojb_W03, Ojb_W04, Ojb_U01, Ojb_U02, Ojb_U03 Ojb_K01, Ojb_K02	SIB2_W01, SIB2_W03, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7S_UK P7S_UU, P7U_K, P7S_KK
W05	Ojb_W01, Ojb_W02, Ojb_W03, Ojb_W04, Ojb_U01, Ojb_U02, Ojb_U03 Ojb_K01, Ojb_K02	SIB2_W01, SIB2_W03, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7S_UK P7S_UU, P7U_K, P7S_KK
W06	Ojb_W01, Ojb_W02, Ojb_W03, Ojb_W04, Ojb_U01, Ojb_U02, Ojb_U03 Ojb_K01, Ojb_K02	SIB2_W01, SIB2_W03, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7S_UK P7S_UU, P7U_K, P7S_KK
W07	Ojb_W01, Ojb_W02, Ojb_W03, Ojb_W04, Ojb_U01, Ojb_U02, Ojb_U03 Ojb_K01, Ojb_K02	SIB2_W01, SIB2_W03, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7S_UK P7S_UU, P7U_K, P7S_KK
C01	Ojb_W01, Ojb_W02, Ojb_W03, Ojb_W04, Ojb_U01, Ojb_U02, Ojb_U03 Ojb_K01, Ojb_K02	SIB2_W01, SIB2_W03, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7S_UK P7S_UU, P7U_K, P7S_KK
C02	Ojb_W01, Ojb_W02, Ojb_W03, Ojb_W04, Ojb_U01, Ojb_U02, Ojb_U03 Ojb_K01, Ojb_K02	SIB2_W01, SIB2_W03, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7S_UK P7S_UU, P7U_K, P7S_KK
C03	Ojb_W01, Ojb_W02, Ojb_W03, Ojb_W04, Ojb_U01, Ojb_U02, Ojb_U03 Ojb_K01, Ojb_K02	SIB2_W01, SIB2_W03, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7S_UK P7S_UU, P7U_K, P7S_KK
C04	Ojb_W01, Ojb_W02, Ojb_W03, Ojb_W04, Ojb_U01, Ojb_U02, Ojb_U03 Ojb_K01, Ojb_K02	SIB2_W01, SIB2_W03, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7S_UK P7S_UU, P7U_K, P7S_KK
C05	Ojb_W01, Ojb_W02, Ojb_W03, Ojb_W04, Ojb_U01, Ojb_U02, Ojb_U03 Ojb_K01, Ojb_K02	SIB2_W01, SIB2_W03, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7S_UK P7S_UU, P7U_K, P7S_KK
C06	Ojb_W01, Ojb_W02, Ojb_W03, Ojb_W04, Ojb_U01, Ojb_U02, Ojb_U03 Ojb_K01, Ojb_K02	SIB2_W01, SIB2_W03, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7S_UK P7S_UU, P7U_K, P7S_KK
C07	Ojb_W01, Ojb_W02, Ojb_W03, Ojb_W04, Ojb_U01, Ojb_U02, Ojb_U03 Ojb_K01, Ojb_K02	SIB2_W01, SIB2_W03, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7S_UK P7S_UU, P7U_K, P7S_KK
C08	Ojb_W01, Ojb_W02, Ojb_W03, Ojb_W04, Ojb_U01, Ojb_U02, Ojb_U03 Ojb_K01, Ojb_K02	SIB2_W01, SIB2_W03, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7S_UK P7S_UU, P7U_K, P7S_KK

V.	**NAKŁAD PRACY STUDENTA**			
Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**25**	**X**	**105**	**4**
Ćwiczenia	**25**			
Seminaria				
Laboratoria				

Konsultacje (zaliczenie nieobecności, rozliczenie rygorów, poprawy)	**5**			
Przygotowanie do ćwiczeń	**X**			
Opanowanie informacji		**20**		
Przygotowanie do rozliczenia rygorów		**30**		
RAZEM	**55**	**50**		

VI.	**METODY DYDAKTYCZNE**
1.	Wykład z prezentacją multimedialną
2.	Praca przy stanowisku komputerowym
3.	Rozwiązywanie zadań problemowych

VII.	**FORMA ZALICZENIA PRZEDMIOTU**	
Rygor	*Kryteria składowe*	*Waga*
Zaliczenie	Ocena za aktywność na zajęciach	0,2
	Ocena z kolokwium	0,4
	Sprawozdania z laboratorium	0,4

VIII.	**LITERATURA**
	OBOWIĄZKOWA
1.	John Stoneburner, Alice Goguen, and Alexis Feringa, "Risk Management Guide for Information Technology Systems"
2.	Douglas Hubbard, "The Failure of Risk Management: Why It's Broken and How to Fix It".
3.	Bruce Schneier, "Beyond Fear: Thinking Sensibly About Security in an Uncertain World".
4.	Chris Chapman and Stephen Ward, "Managing Project Risk and Uncertainty: A Constructively Simple Approach to Decision Making".
5.	Paul Hopkin, "Fundamentals of Risk Management: Understanding, Evaluating and Implementing Effective Risk Management".
	UZUPEŁNIAJĄCA
1.	Norman Marks, "World-Class Risk Management".
2.	David Vose, "Risk Analysis: A Quantitative Guide".
3.	Timothy J. Leech, "Implementing Enterprise Risk Management: From Methods to Applications".

IX.	
Stopień, Imię i nazwisko	mgr Tomasz Janczewski
adres e-mail	t.janczewski@amw.gdynia.pl

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:	**Zagrożenia bezpieczeństwa aplikacji i systemów**	*Kod*:	**Ojc**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Stacjonarne		
Kształcenie w zakresie:	Analiza danych i informatyka śledcza		
Profil:	Ogólnoakademicki		
Liczba ECTS:	4		
Semestr:	4		
Wymagania wstępne:	Brak		
Język wykładowy:	Polski		
Cel przedmiotu:	**C01**	Zapoznanie studentów z aktualnymi zagrożeniami związanymi z bezpieczeństwem aplikacji i systemów	
	C02	Zapoznanie studentów z aktualnymi sposobami, technikami zabezpieczania aplikacji oraz systemów	
	C03	Zaprezentowanie sposobów, technik i działań cyberprzestępców w kontekście aplikacji i systemów pracujących w sieci internet	

II.	**EFEKTY UCZENIA SIĘ**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Ojc_W01**	Zrozumienie podstawowych koncepcji związanych z bezpieczeństwem aplikacji i systemów, w tym zagrożeń, podatności oraz metod ich wykrywania i zapobiegania.	Pytania sprawdzające podczas zajęć. Kolokwium.
	Ojc_W02	Znajomość najnowszych technologii i narzędzi wykorzystywanych do ochrony aplikacji i systemów przed atakami zewnętrznymi i wewnętrznymi.	Pytania sprawdzające podczas zajęć. Kolokwium.
	Ojc_W03	Analiza przypadków zastosowania różnych metod ochrony w realnych scenariuszach, w celu identyfikacji ich efektywności i ograniczeń.	Pytania sprawdzające podczas zajęć. Kolokwium.
	Ojc_W04	Zdolność do identyfikacji i interpretacji przepisów prawnych oraz standardów bezpieczeństwa mających zastosowanie w różnych sektorach technologicznych.	Pytania sprawdzające podczas zajęć. Kolokwium.
Umiejętności:	**Ojc_U01**	**Projektowanie i implementacja zabezpieczeń w aplikacjach i systemach**, w celu minimalizacji ryzyka i zapewnienia zgodności z normami.	Rozwiązanie zadań problemowych Wypowiedzi ustne, aktywność w ramach dyskusji.
	Ojc_U02	**Umiejętność analizy i oceny bezpieczeństwa aplikacji i systemów** przy użyciu zaawansowanych technik testowania penetracyjnego i audytów.	Sprawozdanie
	Ojc_U03	**Praktyczne umiejętności w zakresie stosowania narzędzi bezpieczeństwa** do monitorowania, wykrywania i reagowania na incydenty bezpieczeństwa.	Rozwiązanie zadań problemowych
	Ojc_U04	**Zdolność do szybkiego identyfikowania i reagowania na nowo odkryte podatności** oraz aktualizacja systemów	Dyskusja

		zabezpieczeń w odpowiedzi na dynamicznie zmieniające się zagrożenia.	
Kompetencje społeczne:	**Ojc_K01**	Rozwój umiejętności pracy zespołowej poprzez współpracę przy projektach związanych z bezpieczeństwem, w tym dzielenie się wiedzą i odpowiedzialnością za projekty zabezpieczeń.	Rozwiązanie zadań problemowych
	Ojc_K02	Efektywna komunikacja zagrożeń i strategii bezpieczeństwa z różnymi grupami interesariuszy, w tym zarządem, pracownikami technicznymi i użytkownikami końcowymi.	Praca pisemna
	Ojc_K03	Podejmowanie etycznych decyzji w kontekście bezpieczeństwa informacji, z uwzględnieniem wpływu tych decyzji na użytkowników i organizację.	Sprawozdanie połączone z dyskusją w trakcie zajęć

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
W01	Podstawy bezpieczeństwa cybernetycznego: Wprowadzenie do kluczowych koncepcji, terminologii.	2
W02	Metody identyfikacji zagrożeń i podatności w systemach IT: Narzędzia i techniki używane do oceny bezpieczeństwa.	2
W03	Zarządzanie ryzykiem w bezpieczeństwie informacji: Procesy i metodyki stosowane w planowaniu i reagowaniu na ryzyko.	2
W04	Szyfrowanie i zarządzanie kluczami: Zasady i praktyki stosowania szyfrowania do ochrony danych.	2
W05	Bezpieczeństwo aplikacji webowych: Specyficzne zagrożenia, podatności i strategie obronne w aplikacjach internetowych.	2
W06	Inżynieria społeczna i phishing: Rozpoznawanie i przeciwdziałanie manipulacji psychologicznej.	2
W07	Zabezpieczanie infrastruktury krytycznej i chmurowej: Techniki ochrony zasobów wrażliwych i rozproszonych.	2
W08	Zarządzanie incydentami bezpieczeństwa: Procedury i narzędzia do wykrywania, reagowania i odzyskiwania po incydentach bezpieczeństwa.	2
W09	Przegląd regulacji i standardów w bezpieczeństwie IT: Międzynarodowe i krajowe regulacje wpływające na strategie bezpieczeństwa.	2
W10	Najnowsze trendy i przyszłość w bezpieczeństwie cybernetycznym: Analiza rozwijających się technologii i metod, takich jak sztuczna inteligencja i uczenie maszynowe w bezpieczeństwie.	2
C01	Analiza przypadków naruszeń bezpieczeństwa: Praktyczne studium przypadków znanych ataków i ich skutków.	2
C02	Scenariusze zarządzania ryzykiem: Symulacje oceny i zarządzania ryzykiem w różnych środowiskach IT.	2
C03	Warsztaty z szyfrowania danych: Ćwiczenia praktyczne z zastosowaniem różnych metod szyfrowania i zarządzania kluczami.	2
C04	Rozwiązywanie problemów związanych z bezpieczeństwem aplikacji webowych: Interaktywne zadania dotyczące wykrywania i naprawiania podatności.	2
C05	Ćwiczenia z inżynierii społecznej: Symulacje ataków phishingowych i obrony przed manipulacjami.	2
C06	Planowanie reakcji na incydenty: Tworzenie i ocena planów reakcji na incydenty bezpieczeństwa.	2

C07	Przegląd i analiza regulacji w bezpieczeństwie IT: Dyskusje grupowe na temat wpływu i implementacji różnych regulacji prawnych.	3
L01	Testowanie penetracyjne systemów: Praktyczne ćwiczenia w zakresie wykonywania testów penetracyjnych na przykładowych systemach.	2
L02	Implementacja zabezpieczeń w aplikacjach webowych: Laboratorium z zakresu stosowania technik obronnych do ochrony aplikacji webowych.	2
L03	Konfiguracja firewalli i systemów wykrywania intruzów: Praktyczne zajęcia z konfiguracji i testowania zapór sieciowych i IDS.	2
L04	Symulacja zarządzania incydentami bezpieczeństwa: Praktyczne ćwiczenia z reagowania na symulowane incydenty bezpieczeństwa.	2
L05	Zarządzanie kluczami i szyfrowanie w praktyce: Laboratorium z zakresu implementacji systemów zarządzania kluczami.	2
L06	Ochrona infrastruktury krytycznej i chmurowej: Ćwiczenia z zabezpieczania specyficznych środowisk IT, takich jak chmura.	2
L07	Wykorzystanie narzędzi do monitorowania bezpieczeństwa: Praktyczne zajęcia z wykorzystaniem nowoczesnych narzędzi do monitorowania i alarmowania w realnym czasie.	3
K1	Ocena i poprawa projektów zabezpieczeń: Konsultacje skupiają się na indywidualnych lub grupowych projektach studentów.	2
K2	Przygotowanie do egzaminów i ocena wiedzy: Konsultacje poświęcone przeglądowi i pogłębieniu wiedzy studentów przed kolokwium zaliczeniowym.	3

IV.	**KORELACJA EFEKTÓW UCZENIA SIĘ**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyk PRK*
W01	Ojc_W01, Ojc_W02, Ojc_W03, Ojc_W04, Ojc_U02, Ojc_U03, Ojc_U04 Ojc_K01, Ojc_K02, Ojc_K03	SIB2_W01, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7S_UU P7U_K, P7S_KK
W02	Ojc_W01, Ojc_W02, Ojc_W03, Ojc_W04, Ojc_U02, Ojc_U03, Ojc_U04 Ojc_K01, Ojc_K02, Ojc_K03	SIB2_W01, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7S_UU P7U_K, P7S_KK
W03	Ojc_W01, Ojc_W02, Ojc_W03, Ojc_W04, Ojc_U02, Ojc_U03, Ojc_U04 Ojc_K01, Ojc_K02, Ojc_K03	SIB2_W01, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7S_UU P7U_K, P7S_KK
W04	Ojc_W01, Ojc_W02, Ojc_W03, Ojc_W04, Ojc_U02, Ojc_U03, Ojc_U04 Ojc_K01, Ojc_K02, Ojc_K03	SIB2_W01, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7S_UU P7U_K, P7S_KK
W05	Ojc_W01, Ojc_W02, Ojc_W03, Ojc_W04, Ojc_U02, Ojc_U03, Ojc_U04 Ojc_K01, Ojc_K02, Ojc_K03	SIB2_W01, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7S_UU P7U_K, P7S_KK
W06	Ojc_W01, Ojc_W02, Ojc_W03, Ojc_W04, Ojc_U02, Ojc_U03, Ojc_U04 Ojc_K01, Ojc_K02, Ojc_K03	SIB2_W01, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7S_UU P7U_K, P7S_KK
W07	Ojc_W01, Ojc_W02, Ojc_W03, Ojc_W04, Ojc_U02, Ojc_U03, Ojc_U04 Ojc_K01, Ojc_K02, Ojc_K03	SIB2_W01, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7S_UU P7U_K, P7S_KK
W08	Ojc_W01, Ojc_W02, Ojc_W03, Ojc_W04, Ojc_U02, Ojc_U03, Ojc_U04	SIB2_W01, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7S_UU

	Ojc_K01, Ojc_K02, Ojc_K03	SIB2_K01, SIB2_K02	P7U_K, P7S_KK
W09	Ojc_W01, Ojc_W02, Ojc_W03, Ojc_W04, Ojc_U02, Ojc_U03, Ojc_U04 Ojc_K01, Ojc_K02, Ojc_K03	SIB2_W01, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7S_UU P7U_K, P7S_KK
W10	Ojc_W01, Ojc_W02, Ojc_W03, Ojc_W04, Ojc_U02, Ojc_U03, Ojc_U04 Ojc_K01, Ojc_K02, Ojc_K03	SIB2_W01, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7S_UU P7U_K, P7S_KK
C01	Ojc_W01, Ojc_W02, Ojc_W03, Ojc_W04, Ojc_U02, Ojc_U03, Ojc_U04 Ojc_K01, Ojc_K02, Ojc_K03	SIB2_W01, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7S_UU P7U_K, P7S_KK
C02	Ojc_W01, Ojc_W02, Ojc_W03, Ojc_W04, Ojc_U02, Ojc_U03, Ojc_U04 Ojc_K01, Ojc_K02, Ojc_K03	SIB2_W01, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7S_UU P7U_K, P7S_KK
C03	Ojc_W01, Ojc_W02, Ojc_W03, Ojc_W04, Ojc_U02, Ojc_U03, Ojc_U04 Ojc_K01, Ojc_K02, Ojc_K03	SIB2_W01, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7S_UU P7U_K, P7S_KK
C04	Ojc_W01, Ojc_W02, Ojc_W03, Ojc_W04, Ojc_U02, Ojc_U03, Ojc_U04 Ojc_K01, Ojc_K02, Ojc_K03	SIB2_W01, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7S_UU P7U_K, P7S_KK
C05	Ojc_W01, Ojc_W02, Ojc_W03, Ojc_W04, Ojc_U02, Ojc_U03, Ojc_U04 Ojc_K01, Ojc_K02, Ojc_K03	SIB2_W01, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7S_UU P7U_K, P7S_KK
C06	Ojc_W01, Ojc_W02, Ojc_W03, Ojc_W04, Ojc_U02, Ojc_U03, Ojc_U04 Ojc_K01, Ojc_K02, Ojc_K03	SIB2_W01, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7S_UU P7U_K, P7S_KK
C07	Ojc_W01, Ojc_W02, Ojc_W03, Ojc_W04, Ojc_U02, Ojc_U03, Ojc_U04 Ojc_K01, Ojc_K02, Ojc_K03	SIB2_W01, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7S_UU P7U_K, P7S_KK
L01	Ojc_W01, Ojc_W02, Ojc_W03, Ojc_W04, Ojc_U02, Ojc_U03, Ojc_U04 Ojc_K01, Ojc_K02, Ojc_K03	SIB2_W01, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7S_UU P7U_K, P7S_KK
L02	Ojc_W01, Ojc_W02, Ojc_W03, Ojc_W04, Ojc_U02, Ojc_U03, Ojc_U04 Ojc_K01, Ojc_K02, Ojc_K03	SIB2_W01, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7S_UU P7U_K, P7S_KK
L03	Ojc_W01, Ojc_W02, Ojc_W03, Ojc_W04, Ojc_U02, Ojc_U03, Ojc_U04 Ojc_K01, Ojc_K02, Ojc_K03	SIB2_W01, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7S_UU P7U_K, P7S_KK
L04	Ojc_W01, Ojc_W02, Ojc_W03, Ojc_W04, Ojc_U02, Ojc_U03, Ojc_U04 Ojc_K01, Ojc_K02, Ojc_K03	SIB2_W01, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7S_UU P7U_K, P7S_KK
L05	Ojc_W01, Ojc_W02, Ojc_W03, Ojc_W04, Ojc_U02, Ojc_U03, Ojc_U04 Ojc_K01, Ojc_K02, Ojc_K03	SIB2_W01, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7S_UU P7U_K, P7S_KK
L06	Ojc_W01, Ojc_W02, Ojc_W03, Ojc_W04, Ojc_U02, Ojc_U03, Ojc_U04	SIB2_W01, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7S_UU

	Ojc_K01, Ojc_K02, Ojc_K03	SIB2_K01, SIB2_K02	P7U_K, P7S_KK
L07	Ojc_W01, Ojc_W02, Ojc_W03, Ojc_W04, Ojc_U02, Ojc_U03, Ojc_U04 Ojc_K01, Ojc_K02, Ojc_K03	SIB2_W01, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7S_UU P7U_K, P7S_KK

V.

Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**20**		**105**	**4**
Ćwiczenia	**15**			
Seminaria				
Laboratorium	**15**			
Konsultacje	**5**			
Rozliczenie rygorów przedmiotu				
Przygotowanie do ćwiczeń		**15**		
Wykonanie zadań domowych		**15**		
Przygotowanie do rozliczenia rygorów		**20**		
RAZEM	**55**	**50**		

VI. METODY DYDAKTYCZNE

1.	Wykład z prezentacją multimedialną
2.	Praca przy stanowisku komputerowym
3.	Rozwiązywanie zadań problemowych

VII. FORMA ZALICZENIA PRZEDMIOTU

Rygor	*Kryteria składowe*	*Waga*
Zaliczenie	Aktywność na zajęciach laboratoryjnych	0,2
	Sprawozdania z laboratorium	0,8
Zaliczenie	Ocena za aktywność na zajęciach	0,2
	Ocena z kolokwium	0,8

VIII. LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

OBOWIĄZKOWA

1.	Charles P. Pfleeger, Shari Lawrence Pfleeger, "Security in Computing", 5th Edition
2.	Ross J. Anderson, "Security Engineering: A Guide to Building Dependable Distributed Systems", 3rd Edition.
3.	Michael Howard, David LeBlanc, "Writing Secure Code", 2nd Edition.
4.	Bruce Schneier, "Applied Cryptography: Protocols, Algorithms and Source Code in C", 2nd Edition.

UZUPEŁNIAJĄCA

1.	Stewart James, Mike Chapple, Darril Gibson, "CISSP: Certified Information Systems Security Professional Study Guide", 8th Edition.
2.	Kevin Mitnick, William L. Simon, "The Art of Deception: Controlling the Human Element of Security".
3.	Nina Godbole, Sunit Belapure, "Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives"
4.	Brian Carrier, "File System Forensic Analysis".

IX. PROWADZĄCY PRZEDMIOT

Stopień, Imię i nazwisko	mgr Tomasz Janczewski
adres e-mail	t.janczewski@amw.gdynia.pl

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:	**Metody ataku i obrony w cyberprzestrzeni**	*Kod*:	**Lxi**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Stacjonarne		
Kształcenie w zakresie:	Analiza danych i informatyka śledcza		
Profil:	Ogólnoakademicki		
Liczba ECTS:	4		
Semestr:	4		
Wymagania wstępne:			
Język wykładowy:	Polski		
Cel przedmiotu:	**C01**	Zapoznanie studentów z metodycznym podejściem do projektowania ataków w cyberprzestrzeni w celu zrozumienia doboru sposobu obrony.	
	C02	Zapoznanie słuchaczy z zasadami doboru narzędzi ataku i obrony w sieciach komputerowych, z uwzględnieniem specyfiki ruchu w warstwie aplikacyjnej.	
	C03	Zapoznanie studentów z metodami zabezpieczania usług przed potencjalnym atakiem.	

II.	**EFEKTY UCZENIA SIĘ**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Lxi_W01**	Zna i rozumie wybrane fakty, teorie, metody oraz zależności między nimi z zakresu ataku w cyberprzestrzeni.	Kolokwium
	Lxi_W02	Student zna sposoby zabezpieczania usług sieciowych przed typowymi atakami w sieciach teleinformatycznych	Kolokwium
Umiejętności:	**Lxi_U01**	Student potrafi zaprojektować wektor ataku i zgodnie z założeniami przeprowadzić akcję ofensywną	Kolokwium, rozwiązywanie zadań
	Lxi_U02	Słuchacz posiada umiejętności pozwalające mu na zabezpieczenie podstawowych usług w cyberprzestrzeni	Kolokwium, rozwiązywanie zadań
	Lxi_U03	Potrafi łączyć kilka technik obrony jak i ataku w celu otrzymania jak najbardziej kompleksowego rozwiązania w realizacji postawionych zadań	Kolokwium, rozwiązywanie zadań
Kompetencje społeczne:	**Lxi_K01**	Student w oparciu o uzyskaną podstawową wiedzę z zakresu sieci teleinformatycznych potrafi doskonalić swoją wiedzę i umiejętności z tego obszaru	Praca w grupach
	Lxi_K02	Uznaje znaczenie wiedzy w rozwiązywaniu problemów praktycznych oraz zasięga opinii ekspertów w przypadku trudności z samodzielnym rozwiazywaniem problemów dotyczących wykorzystania systemów informacyjnych w bezpieczeństwie.	Rozwiązanie zadań problemowych

	Lxi_K03	Krytycznie ocenia posiadaną wiedzę i odbierane treści z zakresu systemów informatycznych	Sprawozdanie / przygotowanie do zajęć

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
W01	Zrozumieć Cybersecurity Kill Chain	6
W02	Informacje o zagrożeniach	4
W03	Zarządzanie lukami w zabezpieczeniach	4
W04	DeepFake oraz narzędzia AI/ML Cyberbezpieczeństwie	4
W05	Innowacje w strategiach bezpieczeństwa	2
C01	Analizy przypadku ataków w cyberprzestrzeni (kluczowe obiekty dla państw)	4
C02	Dobór sił i środków do realizacji zadań w cyberprzestrzeni	4
C03	Wykorzystanie analizy zagrożeń do badania podejrzanych działań	2
L01	Rekonesans	4
L02	Przejmowanie sieci teleinformatycznych	4
L03	Naruszenie bezpieczeństwa systemu	4
L04	Przechwytywanie tożsamości użytkownika	4
L05	Urządzenia wbudowane i hakowanie RFID/Mifare	4

IV.	**KORELACJA EFEKTÓW UCZENIA SIĘ**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyk PRK*
W01	Lxi_W01, Lxi_W02, Lxi_K01, Lxi_K02, Lxi_K03	SIB2_W01, SIB2_W02, SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W02	Lxi_W01, Lxi_W02, Lxi_K01, Lxi_K02, Lxi_K03	SIB2_W01, SIB2_W02, SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W03	Lxi_W01, Lxi_W02, Lxi_K01, Lxi_K02, Lxi_K03	SIB2_W01, SIB2_W02, SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W04	Lxi_W01, Lxi_W02, Lxi_K01, Lxi_K02, Lxi_K03	SIB2_W01, SIB2_W02, SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W05	Lxi_W01, Lxi_W02, Lxi_K01, Lxi_K02, Lxi_K03	SIB2_W01, SIB2_W02, SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
C01	Lxi_W01, Lxi_U01, Lxi_U02, Lxi_U03, Lxi_K01, Lxi_K02, Lxi_K03	SIB2_W01, SIB2_U01, SIB2_U02, SIB2_K01, SIB2_K02, SIB2_K04	P7U_W, P7S_WG, P7U_U, P7S_UW P7U_K, P7S_KK, P7S_KR
C02	Lxi_W01, Lxi_U01, Lxi_U02, Lxi_U03, Lxi_K01, Lxi_K02, Lxi_K03	SIB2_W01, SIB2_U01, SIB2_U02, SIB2_K01, SIB2_K02, SIB2_K04	P7U_W, P7S_WG, P7U_U, P7S_UW P7U_K, P7S_KK, P7S_KR
C03	Lxi_W01, Lxi_U01, Lxi_U02, Lxi_U03, Lxi_K01, Lxi_K02, Lxi_K03	SIB2_W01, SIB2_U01, SIB2_U02, SIB2_K01, SIB2_K02, SIB2_K04	P7U_W, P7S_WG, P7U_U, P7S_UW P7U_K, P7S_KK, P7S_KR
L01	Lxi_W01, Lxi_U01, Lxi_U02, Lxi_U03, Lxi_K01, Lxi_K02, Lxi_K03	SIB2_W01, SIB2_U01, SIB2_U02, SIB2_K01, SIB2_K02, SIB2_K04	P7U_W, P7S_WG, P7U_U, P7S_UW P7U_K, P7S_KK, P7S_KR
L02	Lxi_W01, Lxi_U01, Lxi_U02, Lxi_U03, Lxi_K01, Lxi_K02, Lxi_K03	SIB2_W01, SIB2_U01, SIB2_U02, SIB2_K01, SIB2_K02, SIB2_K04	P7U_W, P7S_WG, P7U_U, P7S_UW P7U_K, P7S_KK, P7S_KR
L03	Lxi_W01, Lxi_U01, Lxi_U02, Lxi_U03, Lxi_K01, Lxi_K02, Lxi_K03	SIB2_W01, SIB2_U01, SIB2_U02,	P7U_W, P7S_WG, P7U_U, P7S_UW P7U_K, P7S_KK, P7S_KR

		SIB2_K01, SIB2_K02, SIB2_K04	
L04	Lxi_W01, Lxi_U01, Lxi_U02, Lxi_U03, Lxi_K01, Lxi_K02, Lxi_K03	SIB2_W01, SIB2_U01, SIB2_U02, SIB2_K01, SIB2_K02, SIB2_K04	P7U_W, P7S_WG, P7U_U, P7S_UW P7U_K, P7S_KK, P7S_KR
L05	Lxi_W01, Lxi_U01, Lxi_U02, Lxi_U03, Lxi_K01, Lxi_K02, Lxi_K03	SIB2_W01, SIB2_U01, SIB2_U02, SIB2_K01, SIB2_K02, SIB2_K04	P7U_W, P7S_WG, P7U_U, P7S_UW P7U_K, P7S_KK, P7S_KR

V. NAKŁAD PRACY STUDENTA

Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**20**	**X**	**105**	**4**
Ćwiczenia	**10**			
Seminaria	**0**			
Laboratoria	**20**			
Konsultacje (zaliczenie nieobecności, rozliczenie rygorów, poprawy)	**5**			
Przygotowanie do ćwiczeń	**X**	**15**		
Opanowanie informacji		**20**		
Przygotowanie do rozliczenia rygorów		**15**		
RAZEM	**55**	**50**		

VI. METODY DYDAKTYCZNE

1.	Metody podające: wykład problemowy / wykład konwersatoryjny / wykład z prezentacją multimedialną.
2.	Metody aktywizujące: pogadanka, obserwacja, praca z dokumentacją, praca w grupach, case study.
3.	Ćwiczenia/Laboratorium: praca w grupach / praca indywidualna z wykorzystaniem stanowisk komputerowych

VII. FORMA ZALICZENIA PRZEDMIOTU

Rygor	*Kryteria składowe*	*Waga*
Zaliczenie	Ocena z kolokwium (materiał z wykładów)	0,4
	Ocena z laboratoriów i ćwiczeń	0,6

VIII. LITERATURA

OBOWIĄZKOWA

1.	Dan Borges, Adversarial Tradecraft in Cybersecurity, ISBN 978-1-80107-620-3, 2021 Packt Publishing
2.	Yuri Diogenes, Erdal Ozkaya, Cybersecurity – Attack and Defense Strategies, ISBN 978-1-83882-779-3, 2019 Packt Publishing

UZUPEŁNIAJĄCA

1.	Maxie Reynolds, The Art of Attack, ISBN: 978-1-119-80546-5, 2021 Wiley
2.	Ben McCarty, Cyberjutsu : cybersecurity for the modern ninja, ISBN-13: 978-1-7185-0054-9, 2021 No Starch Press

IX. PROWADZĄCY PRZEDMIOT

Stopień, Imię i nazwisko	mgr Grzegorz Piotrowski
adres e-mail	grzegorz.piotrowski@c2o.eu

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:	**Podstawy prawne cyberbezpieczeństwa**	*Kod*:	**Ccq**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Stacjonarne		
Kształcenie w zakresie:	Analiza danych i informatyka śledcza		
Profil:	Ogólnoakademicki		
Liczba ECTS:	4		
Semestr:	4		
Wymagania wstępne:	Podstawowa wiedza z zakresu państwa i prawa		
Język wykładowy:	Polski		
Cel przedmiotu:	**C01**	Zapoznanie słuchaczy z najważniejszymi aktami prawnymi regulującymi problematykę cyberbezpieczeństwa w wymiarze krajowym.	
	C02	Zapoznanie słuchaczy z najważniejszymi aktami prawnymi regulującymi problematykę cyberbezpieczeństwa w wymiarze międzynarodowym.	

II.	**EFEKTY UCZENIA SIĘ**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Ccq_W01**	Posiada wiedzez zakresu prawa krajowego i międzynarodowego oraz norm postępowania w cyberprzestrzeni, wpływających na prawa i obowiązki państw na płaszczyźnie międzynarodowej	Kolowium/ dyskusja
Umiejętności:	**Oku_U01**	Umiejętność analizy krajowych i międzynarodowych aktów prawnych oraz norm z zakresu cyberbezpieczeństwa.	Kolowium/ dyskusja
	Oku_U02	Potrafi znaleźć legitymację do działań państw w cyberprzestrzeni	Kolowium/ dyskusja
Kompetencje społeczne:	**Oku_K01**	Potrafi dokonać subsumpcji normy prawnej w konkretnym stanie faktycznym	Obserwacja podczas zajęć
	Oku_K02	Przestrzega unormowań materialnych i proceduralnych krajowych oraz międzynarodowych dotyczących prowadzenia działań w cyberprzestrzeni	Obserwacja podczas zajęć
	Oku_K03	W oparciu o uzyskaną teoretyczną wiedzę programową potrafi samodzielnie aktualizować i doskonalić swoją wiedzę i umiejętności.	Obserwacja podczas zajęć

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
W01	Zasady poszanowania suwerenności terytorialnej.	5
W02	Zakaz interwencji w sprawy wewnętrzne; zakaz użycia siły.	5

W03	Zakaz przeciwdziałania wykorzystaniu własnego terytorium do czynności szkodliwych dla drugiego państwa (zasada dobrego sąsiedztwa); zasady przypisania cyberoperacji państwu.	5
W04	Naruszenie bezpieczeństwa informacyjnego systemów komputerowych w świetle konkretnych norm prawa międzynarodowego.	5
W05	Przepisy regulujące odpowiedzialność międzynarodową państwa za działania indywidualnych hakerów i grup hakerskich; prawne ramy operacji odwetowych; prawo do samoobrony przed napaścią zbrojną.	5
C01	Problemy z prawnym zdefiniowaniem pojęcia cyberprzestrzeń. Przegląd ustawodawstwa wybranych państw. Status prawny cyberprzestrzeni.	5
C02	Status prawny państw w cyberprzestrzeni. Prawa i obowiązki państw w cyberprzestrzeni.	5
C03	Regulacje międzynarodowe działań w cyberprzestrzeni	5
C04	Krajowa regulacja z zakresu cyberbezpieczeństwa.	5
C05	Unormowania dot. Przestępstw komputerowych	5

IV.	**KORELACJA EFEKTÓW UCZENIA SIĘ**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyk PRK*
W01	Ccq_W01,	SIB2_W01	P7U_W, P7S_WG
W02	Ccq_W01,	SIB2_W01	P7U_W, P7S_WG
W03	Ccq_W01,	SIB2_W01	P7U_W, P7S_WG
W04	Ccq_W01,	SIB2_W01	P7U_W, P7S_WG
W05	Ccq_W01,	SIB2_W01	P7U_W, P7S_WG
L01	Ccq_U01, Ccq_U02, , Ccq_K01, Ccq_K02, Ccq_K03	SIB2_U01, SIB2_U06, SIB2_K01, SIB2_K05	P7U_U, P7S_UW, P7S_UO, P7U_K, P7S_KK, P7S_KR
L02	Ccq_U01, Ccq_U02, , Ccq_K01, Ccq_K02, Ccq_K03	SIB2_U01, SIB2_U06, SIB2_K01, SIB2_K05	P7U_U, P7S_UW, P7S_UO, P7U_K, P7S_KK, P7S_KR
L03	Ccq_U01, Ccq_U02, , Ccq_K01, Ccq_K02, Ccq_K03	SIB2_U01, SIB2_U06, SIB2_K01, SIB2_K05	P7U_U, P7S_UW, P7S_UO, P7U_K, P7S_KK, P7S_KR
L04	Ccq_U01, Ccq_U02, , Ccq_K01, Ccq_K02, Ccq_K03	SIB2_U01, SIB2_U06, SIB2_K01, SIB2_K05	P7U_U, P7S_UW, P7S_UO, P7U_K, P7S_KK, P7S_KR
L05	Ccq_U01, Ccq_U02, , Ccq_K01, Ccq_K02, Ccq_K03	SIB2_U01, SIB2_U06, SIB2_K01, SIB2_K05	P7U_U, P7S_UW, P7S_UO, P7U_K, P7S_KK, P7S_KR

V.	**NAKŁAD PRACY STUDENTA**			
Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**25**	**X**	**105**	**4**
Ćwiczenia	**25**			
Seminaria	**0**			
Laboratoria	**0**			
Konsultacje (zaliczenie nieobecności, rozliczenie rygorów, poprawy)	**5**			
Przygotowanie do ćwiczeń	**X**	**15**		
Opanowanie informacji		**20**		
Przygotowanie do rozliczenia rygorów		**15**		
RAZEM	**55**	**50**		

VI.	**METODY DYDAKTYCZNE**
1.	Metody podające: wykład /wykład problemowy / wykład konwersatoryjny / wykład z prezentacją multimedialną.
2.	Metody aktywizujące: pogadanka, obserwacja, praca z dokumentacją, praca w grupach, case study.
3.	Ćwiczenia/Laboratorium: praca w grupach / praca indywidualna.

VII.	**FORMA ZALICZENIA PRZEDMIOTU**	
Rygor	*Kryteria składowe*	*Waga*
Zaliczenie	wykonanie określonych zadań podczas ćwiczeń	0,4

	test	0,6
VIII.	**LITERATURA**	
	OBOWIĄZKOWA	
1.	Schmitt M.N., Tallinn Manual on the International law applicable to the cyber warfare, Cambridge 2013.	
2.	Adamski A., Prawo karne komputerowe, Warszawa 2000..	
	UZUPEŁNIAJĄCA	
1.	Adamski A., Przestępczość w cyberprzestrzeni. Prawne środki przeciwdziałania zjawisku w Polsce na tle projektu Konwencji Rady Europy, Toruń 2001.	
2.	Banasiński C., Rojszczak M. (red.), Cyberbezpieczeństwo, Warszawa 2020.	
3.	Klimburg A., National Cyber Security. Framework Manual, NATO Cooperative Cyber Defence Centre of Excellence Tallin, Estonia 2012.	
IX.	**PROWADZĄCY PRZEDMIOT**	
Stopień, Imię i nazwisko	dr Alicja Żukowska	
adres e-mail	a.zukowska@amw.gdynia.pl	

3.5. Karta przedmiotu modułu dyplomowego studiów stacjonarnych – D

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 i prawa autorskie, praca dyplomowa**	*Kod*:	**Ax**
Kierunek studiów:	Systemy informacyjne w bezieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Stacjonarne		
Specjalność:	Cyberbezpieczeństwo, Analiza danych i informatyka śledcza		
Profil:	Ogólnoakademicki		
Liczba ECTS:	11		
Semestr:	3,4		
Wymagania wstępne:	Wiedza merytoryczna z przedmiotu metodologia badań nad bezpieczeństwem		
Język wykładowy:	Polski		
Cel przedmiotu:	**C01**	Zapoznać z procesem prowadzenia badań naukowych w zakresie bezpieczeństwa	
	C02	Nauczyć technik i narzędzi wykorzystywanych do prowadzenia badan naukowych	
	C03	Przygotować do opracowania pracy magisterskiej odpowiadającej regułom pracy naukowej	

II.	**EFEKTY UCZENIA**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Axp_W01**	Wiedza o podstawowych technikach i narzędziach badawczych stosowanych w badaniach nad bezpieczeństwem	Odpowiedź ustna
	Axp_W02	Zrozumienie istoty procesu badań naukowych i możliwości zastosowania go w badaniach nad bezpieczeństwem	Odpowiedź ustna
	Axp_W03	Znajomość podstawowych zasadach prawa autorskiego	Odpowiedź ustna
Umiejętności:	**Axp_U01**	Wybór i sporządzanie adekwatnych narzędzi badawczych do określonych metod badawczych	Odpowiedź ustna
	Axp_U02	Przeprowadzanie badań teoretycznych i empirycznych	Odpowiedź ustna
Kompetencje społeczne:	**Axp_K01**	Zrozumienie istoty i potrzeb pogłębiania wiedzy	Odpowiedź ustna
	Axp_K02	Dostrzeganie zagrożeń bezpieczeństwa i poszukiwanie środków zaradczych	Opracowanie pisemne

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

W01	**Zasady prowadzenia badań empirycznych** - pojęcie metod badawczych i technik badawczych; podstawowe – empiryczne metody badawcze; proste i złożone; schematy opracowania narzędzi badawczych	1
W02	**Pozyskiwanie materiału badawczego** – metodami empirycznymi, narzędzia badawcze w badaniach ilościowych i jakościowych	1
W03	**Wywiad i jego narzędzia badawcze** – zasady opracowywania kwestionariuszy wywiadu	2
W04	**Ankietowanie i narzędzia badawcze** – zasady opracowywania kwestionariuszy ankiety	2
W05	**Obserwacja i jej narzędzia badawcze** – zasady opracowywania dziennika obserwacji	1
W06	**Prawo autorskie** – zasady pisemnego sporządzania sprawozdań z procesu badawczych	2
W07	Sprawdzian pisemny – zaliczenie przedmiotu	1

IV.	**KORELACJA EFEKTÓW UCZENIA**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyki PRK*
W01	Axp_W01, Axp_K01	SIB2_W01, SIB2_K04	P7U_W P7S_WG P7U_K P7S_KR
W02	Axp_W01, Axp_W02, Axp_K02	SIB2_W01, SIB2_K02	P7U_W P7S_WG P7U_K P7S_KK
W03	Axp_W01, Axp_W02, Axp_W03	SIB2_W01	P7U_W P7S_WG
W04	Axp_W01, Axp_U02	SIB2_W01, SIB2_U01, SIB2_K03,	P7U_W P7S_WG P7U K P7S_KO P7U_U P7S_UW
W05	Axp_W01, Axp_U01	SIB2_W01, SIB2_U01,	P7U_W P7S_WG P7U_U P7S_UW
W06	Axp_W03 Axp_K01	SIB2_W01, SIB2_K02	P7U_W P7S_WG P7U_K P7S_KK
W07	Axp_K01	SIB2_K01, SIB2_K02	P7U_K P7S_KK

V.	**NAKŁAD PRACY STUDENTA**			
Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**10**	**X**	**275**	**11**
Ćwiczenia	**60**			
Seminaria	**-**			
Konwersatoria	**-**			
Konsultacje (zaliczenie nieobecności, rozliczenie rygorów, poprawy)	**55**			
Przygotowanie do ćwiczeń	**X**	**50**		
Opanowanie informacji		**10**		
Przygotowanie do rozliczenia rygorów		**90**		
RAZEM	**125**	**150**		

VI.	**METODY I NARZĘDZIA DYDAKTYCZNE**
1.	Wykłady – oddziaływanie słowne i prezentacje multimedialne.
2.	Zadania do dyskusji
3.	Wykaz literatury do samodzielnego studiowania

VII.	**FORMA ZALICZENIA PRZEDMIOTU**	
Rygor	*Kryteria składowe*	*Waga*
Zaliczenie	Ocena za znajomość teoretyczną przedmiotu.	1,0

VIII.	**LITERATURA**
OBOWIĄZKOWA	
1.	S. Nowak, *Metodologia badań społecznych*, PWN, Warszawa 2010.

2.	K. Pawlik, R. Zenderowski, *Dyplom z Internetu. Jak korzystać z Internetu pisząc prace dyplomowe*, Wydawnictwa Fachowe, Warszawa 2010.
3.	W. Zaczyński, *Praca badawcza nauczyciela*, Wydawnictwa Szkolne i Pedagogiczne, Warszawa 1995.
4.	R. Zenderowski, *Praca magisterska*, licencjat, Wyd. CeDeWu.pl, Warszawa
5.	Ch. Frankfort-Nachmias, *Metody badawcze w naukach społecznych*, wyd. Zysk i Ska, Poznań 2001.
UZUPEŁNIAJĄCA	
1.	E. Babbie, *Podstawy nauk społecznych*, PWN, Warszawa 2009.
2.	J. Apanowicz, *Metodologia nauk*, Dom Organizatora, Toruń 2003.
3.	A. Chalmers, *Czym jest to co zwiemy nauką?*, wyd. Siedmiogród, Wrocław 1977.
4.	J. Sztumski, *Wstęp do metod i technik badań społecznych*, wyd. „Śląsk", Katowice 2010
IX.	**PROWADZĄCY PRZEDMIOT**
Stopień, Imię i nazwisko	
adres e-mail, tel.	

3.6. Karty przedmiotów modułu zajęć podstawowych studiów niestacjonarnych – A

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:	**Język angielski**	*Kod*:	**Ja**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Niestacjonarne		
Kształcenie w zakresie:	Cyberbezpieczeństwo, Analiza danych i informatyka śledcza		
Profil:	Ogólnoakademicki		
Liczba ECTS:	2		
Semestr:	1		
Wymagania wstępne:	Znajomość języka angielskiego na poziomie B2		
Język wykładowy:	Polski, angielski		
Cel przedmiotu:	**C01**	Realizacja przedmiotu w celu wyposażenia studentów w wiedzę, umiejętności i kompetencje społeczne umożliwiające posługiwanie się językiem angielskim do celów ogólnych	
	C02	Realizacja przedmiotu w celu wyposażenia studentów w wiedzę, umiejętności i kompetencje społeczne umożliwiające posługiwanie się językiem angielskim do celów zawodowych	
II.	**EFEKTY UCZENIA SIĘ**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Ja_W01**	Ma rozszerzoną wiedzę o miejscu i znaczeniu języków obcych w systemie nauk oraz o ich specyfice przedmiotowej	Aktywność, Kolokwium
	Ja_W02	Zna terminologię obcojęzyczną właściwą dla studiowanego kierunku na poziomie rozszerzonym	Aktywność, Kolokwium
	Ja_W03	Ma podstawową wiedzę o instytucjach kultury i orientację we współczesnym życiu kulturalnym krajów angielskiego obszaru językowego	Aktywność, Kolokwium
	Ja_W04	Ma pogłębioną wiedzę o kompleksowej naturze języka i historycznej zmienności jego znaczeń	Aktywność, Kolokwium
Umiejętności:	**Ja_U01**	Ma umiejętności językowe właściwe dla studiowanego kierunku zgodnie z wymaganiami określonymi dla poziomu co najmniej B2+ Europejskiego Systemu Opisu Kształcenia Językowego	Aktywność, Kolokwium
	Ja_U02	Umie samodzielnie zdobywać wiedzę wykorzystując znajomość języka obcego	Aktywność, Kolokwium
	Ja_U03	Posiada umiejętność merytorycznego argumentowania i prezentacji własnych poglądów oraz poglądów innych osób w języku obcym	Aktywność, Kolokwium

	Ja_U04	Posiada pogłębioną umiejętność przygotowania różnych prac pisemnych w języku angielskim właściwych dla studiowanego kierunku studiów	Aktywność, Kolokwium
	Ja_U05	Posiada pogłębioną umiejętność przygotowania wystąpień ustnych w języku angielskim w zakresie dziedzin nauki i dyscyplin naukowych właściwych dla studiowanego kierunku studiów	Aktywność, Kolokwium
Kompetencje społeczne:	**Ja_K01**	Rozumie potrzebę uczenia się przez całe życie, potrafi inspirować i organizować proces uczenia się innych osób	Aktywność, Kolokwium
	Ja_K02	Potrafi i współdziałać pracować w grupie, używając języka obcego, przyjmując różne role przy wykonywaniu wspólnych projektów i prowadzonej dyskusji	Aktywność, Kolokwium
	Ja_K03	Aktywnie uczestniczy w działaniach na rzecz zachowania dziedzictwa kulturowego Europy	Aktywność, Kolokwium
	Ja_K04	Systematycznie uczestniczy w życiu kulturalnym	Aktywność, Kolokwium

III.	**TREŚCI PROGRAMOWE**	
Forma	*Temat, zagadnienia*	*Liczba godzin*
C01	Relacjonowanie i dyskutowanie zdarzeń teraźniejszych	4
C02	Relacjonowanie i dyskutowanie zdarzeń przeszłych	4
C03	Planowanie, obiecywanie, informowanie o decyzjach dotyczących przyszłości	4
C04	Rozwijanie umiejętności czytania ze zrozumieniem tekstów odnoszących się do zagadnień bezpieczeństwa publicznego	4
C05	Rozwijanie umiejętności rozumienia wykładów i prezentacji na tematy z zakresu bezpieczeństwa publicznego	4
C06	Rozwijanie umiejętności wypowiadania się na tematy odnoszące się do problematyki bezpieczeństwa publicznego	4
C07	Przygotowanie i przeprowadzenie prezentacji dotyczącej zagadnień bezpieczeństwa publicznego	2
C08	Konsolidacja materiału	2
C09	Kolokwium	2

IV.	**KORELACJA EFEKTÓW UCZENIA SIĘ**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyki PRK*
C01	Ja_W02, Ja_U01, Ja_U03, Ja_K02	SIB2_U07, SIB2_U05, SIB2_K03	P7U_U P7S_UU P7U_U P7S_UK P7U_K P7S_KO
C02	Ja_W02, Ja_U01, Ja_U03, Ja_K02	SIB2_U07, SIB2_U05, SIB2_K03	P7U_U P7S_UU P7U_U P7S_UK P7U_K P7S_KO
C03	Ja_W02, Ja_U01, Ja_03, Ja_K02	SIB2_U07, SIB2_U05, SIB2_K03	P7U_U P7S_UU P7U_U P7S_UK P7U_K P7S_KO
C04	Ja_W01, Ja_W02, Ja_W04, Ja_U01, Ja_K01	SIB2_U07, SIB2_U05,	P7U_U P7S_UU P7U_U P7S_UK

C05	Ja_W01, Ja_W02, Ja_W04, Ja_U0I, Ja_U02, Ja_03, Ja_K01, Ja_K02	SIB2_U07, SIB2_U05, SIB2_K02	P7U_U P7S_UU P7U_U P7S_UK P7U_K P7S_KK
C06	Ja_W01, Ja_W02, Ja_W03, Ja_W04, Ja_U01, Ja_U02, Ja_U03, Ja_U04, Ja_K01, Ja_K02, Ja_K04	SIB2_U07, SIB2_U05, SIB2_K02, SIB2_K03	P7U_U P7S_UU P7U_U P7S_UK P7U_K P7S_KK P7U_K P7S_KO
C07	Ja_W01, Ja_W02, Ja_W03, Ja_W04, Ja_U01, Ja_U02, Ja_U03, Ja_U04, Ja_U05, Ja_K01, Ja_K02, Ja_K03, Ja_K04	SIB2_U07, SIB2_U05, SIB2_K02, SIB2_K03	P7U_U P7S_UU P7U_U P7S_UK P7U_K P7S_KK P7U_K P7S_KO
C08	Ja_W02, Ja_U01, Ja_U02, Ja_K01	SIB2_U07, SIB2_U05, SIB2_K02	P7U_U P7S_UU P7U_U P7S_UK P7U_K P7S_KK
C09	Ja_W02, Ja_W04, Ja_U01	SIB2_U07, SIB2_U05, SIB2_K02	P7U_U P7S_UU P7U_U P7S_UK P7U_K P7S_KK

V. NAKŁAD PRACY STUDENTA

Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład		**X**	**50**	**2**
Ćwiczenia	**30**			
Seminaria				
Konwersatoria				
Konsultacje (zaliczenie nieobecności, rozliczenie rygorów, poprawy)	**5**			
Przygotowanie do ćwiczeń	**X**	**5**		
Opanowanie informacji		**5**		
Przygotowanie do rozliczenia rygorów		**5**		
RAZEM	**35**	**15**		

VI. METODY I NARZĘDZIA DYDAKTYCZNE

Zajęcia realizowane w oparciu o podejście eklektyczne wykorzystujące techniki nauczania adekwatne do zakładanych celów poszczególnych zajęć i celu przedmiotu z szerokim wykorzystaniem technologii cyfrowych i internetowych (Technology Enhanced Language Learning) oraz promowaniem autonomicznego uczenia się (Autonomous Learning Fostering).
- ćwiczenie;
- praca w grupach i inne formy aktywizujące
- prezentacja multimedialna;;

VII. FORMA ZALICZENIA PRZEDMIOTU

Rygor	*Kryteria składowe*	*Waga*
Zaliczenie	Średnia ze sprawdzianów na ćwiczeniach	0,2
	Średnia z ocen uzyskanych za postępy	0,2
	Ocena z kolokwium	0,6

VIII. LITERATURA

	OBOWIĄZKOWA
1.	Podręcznik studenta do nauki języka angielskiego – poziom zaawansowany
2.	Zeszyt ćwiczeń do podręcznika
3.	Classware do podręcznika
4.	Podręcznik nauczyciela wraz z zestawem testów
5.	Nagrania dźwiękowe do podręcznika studenta i zeszytu ćwiczeń
	UZUPEŁNIAJĄCA
1.	The Guardian Weekly - materiały udostępniane w sieci przez One Stop English
2.	Materiałyautentycznedostępne w sieci – British Council Learning Zone, One Stop English, BBC, CNN Student News

IX. PROWADZĄCY PRZEDMIOT

Stopień, Imię i nazwisko	dr Daria ŁĘSKA-OSIAK i zespól
adres e-mail, tel.	tel.: 261 262 737, e-mail: d.osiak@amw.gdynia.pl

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:	**Geografia bezpieczeństwa**	*Kod*:	**Dj**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Niestacjonarne		
Kształcenie w zakresie:	Cyberbezpieczeństwo, Analiza danych i informatyka śledcza		
Profil:	Ogólnoakademicki		
Liczba ECTS:	5		
Semestr:	1		
Wymagania wstępne:	Podstawowa wiedza z geografii, podstawowa wiedza z bezpieczeństwa		
Język wykładowy:	Polski		
Cel przedmiotu:	**C01**	Zapoznanie słuchaczy z pojęciem geografii bezpieczeństwa oraz wskazanie zakresu badań na gruncie tej dyscypliny naukowej w systemie nauk o bezpieczeństwie.	
	C02	Przedstawić jak wykorzystywać informację geograficzną do rozwiązywania problemów bezpieczeństwa.	
	C03	Zapoznanie z praktycznym wymiarem geografii bezpieczeństwa dla wspomagania działalności w sferze bezpieczeństwa narodowego.	

II.	**EFEKTY UCZENIA SIĘ**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Dj_W01**	Wyjaśnia relacje występujące w obszarze nauk o bezpieczeństwie i nauk o obronności oraz ich związek z innymi naukami społecznymi.	Kolokwium
	Dj_W02	Opisuje kulturowe, polityczne, prawne i ekonomiczne procesy występujące na poziomie państwa i układów międzynarodowych wraz z ich przełożeniem na problemy bezpieczeństwa narodowego.	Sprawdzian
	Dj_W03	Posiada pogłębioną wiedzę dotyczącą strategii bezpieczeństwa państwa jej prawnych regulacji i konsekwencji w zakresie ich stosowania.	Praca Pisemna
Umiejętności:	**Dj_U01**	Określa zagrożenia bezpieczeństwa narodowego płynące z obszarów społecznych, ekonomicznych, politycznych, prawnych i kulturowych.	Sprawdzian
	Dj_U02	Interpretuje rozwój zjawisk społecznych, ekonomicznych, politycznych, prawnych i kulturowych oraz płynące z tych obszarów zagrożenia bezpieczeństwa narodowego.	Kolokwium
	Dj_U03	Interpretuje poprawnie zależności między zjawiskami społecznymi, ekonomicznymi, politycznymi, prawnymi i kulturowymi tworzącymi bezpieczeństwo narodowe lub oddziaływującymi na nie, a także system oddziaływania normatywnych regulacji na wspomniane obszary (normy prawne,	Praca Pisemna

		standardy zawodowe, systemy normalizacji i standaryzacji, normy moralne, normy kulturowej.	
Kompetencje społeczne:	**Dj_K01**	Akceptuje potrzebę uczenia się przez całe życie.	Praca Pisemna
	Dj_K02	Podejmuje wyzwania związane z wykonywaniem zawodów w obszarze bezpieczeństwa narodowego.	Odpowiedź tablicowa
	Dj_K03	Akceptuje uzupełnianie i doskonalenie nabytej wiedzy i umiejętności, potrafi ocenić ofertę kształcenia kursowego i podyplomowego.	Praca Pisemna

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
W01	**Wprowadzenie do geografii bezpieczeństwa** (czym zajmuje się geografia bezpieczeństwa; geograficzny wymiar bezpieczeństwa państwa; istota bezpieczeństwa międzynarodowego; strefy bezpieczeństwa narodowego).	1
W02	**Zagrożenia dla bezpieczeństwa państwa** (problemy i wyzwania współczesnego świata; współczesne postrzeganie zagrożeń militarnych; współczesne zagrożenia pozamilitarne /niemilitarne/ państwa).	1
W03	**Geopolityka i geostrategia** (wybrane aspekty globalizacji; geografia wojenna i geografia wojskowa; geografia bezpieczeństwa a inne nauki – związki i zależności).	1
W04	**Geografia bezpieczeństwa** (geografia bezpieczeństwa na tle polityki strategii bezpieczeństwa państwa).	1
W05	**Geografia bezpieczeństwa** (próba zdefiniowania; funkcje).	1
W06	**Zakres badań geografii bezpieczeństwa** (przestrzeń geograficzna; geodane i geoinformacje – znaczenie w systemie informacyjnym; geoprzestrzeń).	1
W07	**Metody i techniki badawcze na gruncie geografii bezpieczeństwa** (metody i techniki badawcze; badania jakościowe).	1
W08	**Działalność struktur państwa w sferze bezpieczeństwa narodowego** (wybrane instytucje państwowe działające na rzecz bezpieczeństwa państwa; geografia bezpieczeństwa oraz systemy informacji geograficznej).	1
W09	**Geodane i geoinformacje** (zasady geoinformacyjne tworzone na gruncie militarnym; zasoby geoinformacyjne strefy pozamilitarnej).	1
W10	**Geografia bezpieczeństwa** (Krajowy System Informacji Geograficznej).	1
W11	**Systemy geoinformacyjne** (GEOserver; teledetekcja; Państwowy Monitoring Środowiska).	1
W12	**Systemy geoinformacyjne** (System Informacji Przestrzennej; infrastruktura geoinformacyjna państwa).	2
W13	**Podział geostrategiczny świata** (przestrzeń euroatlantycka w ujęciu geostrategicznym; ogólna charakterystyka regionów geostrategicznych).	1
C01	Charakterystyka Morza Bałtyckiego jako regionu gospodarczego i militarnego.	1
C02	Charakterystyka zasobów i ich wpływu na rozwój gospodarki narodowej.	1

C03	Ocena zagrożeń naturalnych w stosunku do polski.	1
C04	Ocena zagrożeń naturalnych na świecie.	1
C05	Poleżenie polski a uwarunkowania konfliktowe/asymetryczne.	1
C06	Ocena infrastruktury morskiej Polski w aspekcie zagrożeń i bezpieczeństwa.	1
C07	Charakterystyka zagrożeń naturalnych w państwach UE.	1
C08	Charakterystyka zagrożeń naturalnych w państwach ameryki północnej i południowej.	1
C09	Energia wód – stan obecny oraz perspektywy wykorzystania w Polsce.	1
C10	Energia wiatru – stan obecny oraz perspektywy wykorzystania w Polsce.	1
C11	Energia słoneczna – stan obecny oraz perspektywy wykorzystania w Polsce.	1
C12	System informacji geoprzestrzennej.	1

IV.	**KORELACJA EFEKTÓW UCZENIA SIĘ**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyki PRK*
W01	Dj_W01, Dj_U01, Dj_K02	SIB2_W01, SIB2_U01, SIB2_K04	P7U_W P7S_WG, P7U_U P7S _UW, P7U_K P7S_KR
W02	Dj_W02, Dj_K03	SIB2_W01, SIB2_K03	P7U_W P7S_WG, P7U_K P7S_KO
W03	Dj_W01, Dj_W03, Dj_K03	SIB2_W01, SIB2_W03, SIB2_K01	P7U_W P7S_WG, P7U W P7S_WK, P7U_K P7S_KK
W04	Dj_W02, Dj_W03, Dj_K02	SIB2_W01, SIB2_W03, SIB2_K05	P7U_W P7S_WG, P7U W P7S_WK, P7U_K P7S_KR
W05	Dj_W01, Dj_W02, Dj_K02	SIB2_W01, SIB2_K05	P7U_W P7S_WG, P7U_K P7S_KR,
W06	Dj_W01, Dj_U02, Dj_K03	SIB2_W01, SIB2_U01, SIB2_K03	P7U_W P7S_WG, P7U_U P7S_UW, P7U_K P7S_KO
W07	Dj_W01, Dj_U01, Dj_U03, Dj_K03	SIB2_W01, SIB2_U01, SIB2_U04, SIB2_K03	P7U_W P7S_WG, P7U_U P7S _UW, P7U_U P7S_UK, P7U_K P7S_KO
W08	Dj_W01, Dj_U01, Dj_U03, Dj_K03	SIB2_W01, SIB2_U01, SIB2_U04, SIB2_K03	P7U_W P7S_WG, P7U_U P7S_UW, P7U_U P7S_UK, P7U_K P7S_KO
W09	Dj_W01, Dj_U01, Dj_K03	SIB2_W01, SIB2_U01, SIB2_K03	P7U_W P7S_WG, P7U_U P7S _UW, P7U_K P7S_KO
W10	Dj_W01, Dj_U01, Dj_K03	SIB2_W01, SIB2_U01, SIB2_K03	P7U_W P7S_WG, P7U_U P7S _UW, P7U_K P7S_KO
W11	Dj_W01, Dj_U01, Dj_K03	SIB2_W01, SIB2_U01, SIB2_K03	P7U_W P7S_WG, P7U_U P7S_ UW, P7U_K P7S_KO
W12	Dj_W01, Dj_U01, Dj_K03	SIB2_W01, SIB2_U01, SIB2_K03	P7U_W P7S_WG, P7U_U P7S _UW, P7U_K P7S_KO
W13	Dj_W01, Dj_U01, Dj_K03	SIB2_W01, SIB2_U01, SIB2_K03	P7U_W P7S_WG, P7U_U P7S _UW, P7U_K P7S_KO
C01	Dj_U01, Dj_K03	SIB2_U02, SIB2_K03	P7U_U P7S _UW, P7U_K P7S_KO
C02	Dj_W02, Dj_K03	SIB2_W01, SIB2_K03	P7U_W P7S_WG, P7U_K P7S_KO
C03	Dj_W03, Dj_K03	SIB2_W02, SIB2_K03	P7U W P7S_WK, P7U_K P7S_KO
C04	Dj_W03, Dj_K03	SIB2_W03, SIB2_K03	P7U W P7S_WK, P7U_K P7S_KO
C05	Dj_W02, Dj_K03	SIB2_W01, SIB2_K03	P7U_W P7S_WG, P7U_K P7S_KO
C06	Dj_W01, Dj_W03, Dj_U02, Dj_K01,	SIB2_W01, SIB2_W02, BN2 _U01, SIB2_K05	P7U_W P7S_WG, P7U W P7S_WK, P7U_U P7S_UW, P7U_K P7S_KK,
C07	Dj_W02, Dj_U01, Dj_U03, Dj_K01, Dj_K02,	SIB2_W01, BN2 _U01, SIB2_U01, SIB2_K01, SIB2_K05	P7U_W P7S_WG, P7U_U P7S _UW, P7U_U P7S_UK, P7U_K P7S_KK, P7U_K P7S_KR,
C08	Dj_W02, Dj_U01, Dj_K01, Dj_K03	SIB2_W01, BN2 _U01, SIB2_K05, SIB2_K03	P7U_W P7S_WG, P7U_U P7S _UW, P7U_K P7S_KK, P7U_K P7S_KO
C09	Dj_W02, Dj_U01, Dj_K01, Dj_K02,	SIB2_W01, BN2 _U01, SIB2_K05, SIB2_K04	P7U_W P7S_WG, P7U_U P7S _UW, P7U_K P7S_KK, P7U_K P7S_KR,
C10	Dj_W01, Dj_W02, Dj_U02, Dj_K03	SIB2_W01, BN2 _U01, SIB2_K03	P7U_W P7S_WG, P7U_U P7S_UW, P7U_K P7S_KO
C11	Dj_W01, Dj_W02, Dj_U02, Dj_K03	SIB2_W01, BN2 _U01, SIB2_K03	P7U_W P7S_WG, P7U_U P7S_UW, P7U_K P7S_KO

C12	Dj_W01, Dj_W02, Dj_U01, Dj_K03	SIB2_W01, BN2 _U01, SIB2_K03	P7U_W P7S_WG, P7U_U P7S _UW, P7U_K P7S_KO

V. NAKŁAD PRACY STUDENTA

Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**15**	**X**	**125**	**5**
Ćwiczenia	**15**			
Seminaria	**0**			
Konwersatoria	**0**			
Konsultacje (zaliczenie nieobecności, rozliczenie rygorów, poprawy)	**6**			
Przygotowanie do ćwiczeń	**X**	**28**		
Opanowanie informacji		**28**		
Przygotowanie do rozliczenia rygorów		**33**		
RAZEM	**36**	**89**		

VI. METODY I NARZĘDZIA DYDAKTYCZNE

1.	- wykład;	- wykaz tez do dyskusji;
2.	- ćwiczenie;	- prezentacja multimedialna.
3.	- praca w grupach i inne aktywizujące;	

VII. FORMA ZALICZENIA PRZEDMIOTU

Rygor	*Kryteria składowe*	*Waga*
Zaliczenie	Średnia ze sprawdzianów na ćwiczeniach	0,2
	Ocena z kolokwium	0,2
	Ocena z pracy proseminaryjnej	0,1
Egzamin	Ocena z egzaminu	0,5

VIII. LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

OBOWIĄZKOWA

1. I. Fierla, *Geografia gospodarcza świata*, PWE, Warszawa 2003
2. Z. Lach, *Informator geograficzny. Państwa członkowskie NATO*, AON, Warszawa 2005
3. K. Żurkowska (red.), *Bezpieczeństwo międzynarodowe. Teoria i praktyka*, SGH, Warszawa 2006

UZUPEŁNIAJĄCA

1. J. Barbar, *Geografia gospodarki świata*, PWN, Warszawa 1984
2. S. Otok, *Geografia polityczna świata*, Warszawa 2003
3. M. Pietras, *Bezpieczeństwo ekologiczne w Europie*, Lublin 1996
4. M. Kozub, B. Panek, *Siły zbrojne jako narzędzie polityki bezpieczeństwa międzynarodowego*, SWSPiZ, Łódź-Warszawa 2010
5. A. Łaszczuk, *Geografia bezpieczeństwa*, AON, Warszawa 2004
6. M. Żuber, *Katastrofy naturalne i cywilizacyjne*, WSOWLąd., Wrocław 2006

IX. PROWADZĄCY PRZEDMIOT

Stopień, Imię i nazwisko	dr hab. Krzysztof LIGĘZA, dr Krzysztof GAWRYSIAK
adres e-mail	k.ligeza@amw.gdynia.pl k.gawrysiak@amw.gdynia.pl

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:	**Historia bezpieczeństwa**	*Kod*:	**Yt**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Niestacjonarne		
Kształcenie w zakresie:	Cyberbezpieczeństwo, Analiza danych i informatyka śledcza		
Profil:	Ogólnoakademicki		
Liczba ECTS:	3		
Semestr:	1		
Wymagania wstępne:	Podstawowa wiedza z historii Polski i Europy		
Język wykładowy:	Polski		
Cel przedmiotu:	**C01**	Prezentacja procesów wpływających na bezpieczeństwo Polski i państw Europejskich	
	C02	Zapoznanie się z możliwościami interpretacyjnymi wydarzeń oraz ich oceną w kontekście obecnych wydarzeń	

II.	**EFEKTY UCZENIA**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Yt_W01**	Student opisuje kulturowe, polityczne oraz ekonomiczne procesy występujące na poziomie państwa i układów międzynarodowych wraz z ich przełożeniem na problemy bezpieczeństwa narodowego	Kolokwium
	Yt_W02	Student wyjaśnia historyczny rozwój instytucji i organizacji państwowych, samorządowych, pozarządowych, a także innych spontanicznie tworzonych na rzecz bezpieczeństwa narodowego	Kolokwium;
Umiejętności:	**Yt_U01**	Student interpretuje rozwój zjawisk społecznych, ekonomicznych i politycznych oraz płynące z tych obszarów zagrożenia dla bezpieczeństwa państwa w wymiarze narodowym	Kolokwium; Wypowiedź ustna
	Yt_U02	Student interpretuje poprawnie zależności między zjawiskami politycznymi i ekonomicznymi tworzącymi bezpieczeństwo narodowe	Kolokwium, wypowiedź ustna
Kompetencje społeczne:	**Yt_K01**	Student akceptuje potrzebę uczenia się historii przez całe życie	Wypowiedź ustna
	Yt_K02	Student wykazuje odpowiedzialność za zadania określone przez siebie oraz posługuje się harmonogramem ich uporządkowanej realizacji	Wypowiedź ustna

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
W01	Udział Polski w tworzeniu bezpieczeństwa regionalnego w okresie międzywojennym	5

W02	Bezpieczeństwo europejskie na przełomie XIX i XX wieku	5
W03	Bezpieczeństwo Europy i Polski po II wojnie światowej	5

IV.	**KORELACJA EFEKTÓW UCZENIA SIĘ**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyki PRK*
W01	Yt_W01, Yt_U01, Yt_K01	SIB2_W01, SIB2_U02, SIB2_K02	P7U_W, P7S_WG; P7U_U,P7S_UW; P7U_K, P7S_KK
W02	Yt_W02, Yt_U02, Yt_K02	SIB2_W01, SIB2_U04, SIB2_K03	P7U_W, P7S_WG; P7U_U,P7S_UK; P7S_KO
W03	Yt_W01, Yt_U01, Yt_K01	SIB2_W01, SIB2_U02, SIB2_K02	P7U_W, P7S_WG; P7U_U,P7S_UW; P7U_K, P7S_KK
W04	Yt_W02, Yt_U02, Yt_K02	SIB2_W01, SIB2_U04, SIB2_K03	P7U_W, P7S_WG; P7U_U,P7S_UK; P7S_KO

V. NAKŁAD PRACY STUDENTA

Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**20**	**X**	**75**	**3**
Ćwiczenia				
Seminaria				
Konwersatoria				
Konsultacje (zaliczenie nieobecności, rozliczenie rygorów, poprawy)	**5**			
Przygotowanie do ćwiczeń	**X**			
Opanowanie informacji		**25**		
Przygotowanie do rozliczenia rygorów		**25**		
RAZEM	**25**	**50**		

VI. METODY DYDAKTYCZNE

1.	Konwersatorium

VII. FORMA ZALICZENIA PRZEDMIOTU

Rygor	*Kryteria składowe*	*Waga*
Zaliczenie	Kolokwium ustne	1,0

VIII. LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

OBOWIĄZKOWA

1.	R. Kużniar, *Bezpieczeństwo międzynarodowe*, wyd. Scholar, Warszawa 2012
2.	P. Żurawski vel Grajewski, *Bezpieczeństwo międzynarodowe: wymiar militarny*, wyd. PWN, Warszawa 2012
3.	R. Zięba, *Bezpieczeństwo międzynarodowe w XXI wieku*, wyd. Poltext, Warszawa 2018
4.	E. Haliżak, *Stosunki międzynarodowe: geneza, struktura, dynamika*, wyd. UW, Warszawa 2001

UZUPEŁNIAJĄCA

1.	H. Batowski, *Zachód wobec granic Polski 1920-1940. Niektóre fakt mniej znane*, Łódź 1995
2.	W. Dobrzycki, *Historia stosunków międzynarodowych 1815-1945*, Warszawa 1998
3.	A. Gaca, K. Kamińska, Z. Naworski, *Historia i współczesność, Świat i Polska ludzie i poglądy*, t. 1-2, Toruń 2000
4.	G. Friedman, *Następna dekada. Gdzie byliśmy i dokąd zmierzamy*, Kraków 2012
5.	J. Holzer, *Europa zimnej wojny*, Kraków 2012

IX. PROWADZĄCY PRZEDMIOT

Stopień, Imię i nazwisko	prof. dr hab. Jerzy Będźmirowski
adres e-mail	j.bedzmirowski@amw.gdynia.pl

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:	**Strategia bezpieczeństwa wewnętrznego**	*Kod*:	**Ig**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Niestacjonarne		
Kształcenie w zakresie:	Cyberbezpieczeństwo, Analiza danych i informatyka śledcza		
Profil:	akademicki		
Liczba ECTS:	6		
Semestr:	2		
Wymagania wstępne:	Podstawy wiedzy o bezpieczeństwie państwa		
Język wykładowy:	Polski		
Cel przedmiotu:	**C01**	Zapoznanie się z teoretycznymi i praktycznymi aspektami strategii bezpieczeństwa wewnętrznego.	
	C02	Umiejętność implementowania zapisów strategii bezpieczeństwa wewnętrznego w różnych jednostkach podziału administracyjnego państwa	
	C03	Umiejętność krytycznej analizy strategii bezpieczeństwa wewnętrznego wybranych państw oraz w oparciu o strategię bezpieczeństwa wewnętrznego - określenia priorytetów bezpieczeństwa	

II.	**EFEKTY KSZTAŁCENIA**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Ig_W01**	Student posiada rozszerzoną wiedzę na temat teoretycznego i praktycznego wymiaru bezpieczeństwa, wyzwań i zagrożeń dla bezpieczeństwa wewnętrznego państwa (publicznego, powszechnego i ustrojowego); cech strategii i ich znaczenia, dokumentów strategicznych Polski i Unii Europejskiej	kolokwium, praca pisemna podczas zajęć
	Ig_W 02	Student posiada rozszerzoną wiedzę umożliwiającą identyfikację i opis struktur oraz zadań instytucji bezpieczeństwa publicznego, ich znaczenia dla bezpieczeństwa wewnętrznego państwa oraz Unii Europejskiej	kolokwium
	Ig_W03	Posiada wiedze pozwalającą na opis relacji pomiędzy poszczególnymi strukturami i instytucjami bezpieczeństwa wewnętrznego oraz ich wzajemnych powiązań i relacji	kolokwium, praca pisemna podczas zajęć
	Ig_W04	Student zna podstawowe źródła prawne regulujące funkcjonowanie poszczególnych instytucji bezpieczeństwa wewnętrznego (konstytucja, strategie, ustawy)	kolokwium, praca pisemna podczas zajęć

Umiejętności:	**Ig_U01**	Student potrafi prawidłowo interpretować rodzaje zagrożeń dla bezpieczeństwo wewnętrznego, określać ich zakres oraz przyporządkowywać do zadań poszczególnych instytucji	kolokwium, praca pisemna podczas zajęć
	Ig_U02	Student potrafi analizować oraz opisać zagrożenia bezpieczeństwa wewnętrznego oraz ich wpływu na funkcjonowanie jednostki, społeczeństwa i państwa	Praca pisemna w domu, odpowiedź ustna
	Ig_U03	Student posiada umiejętność korzystania z różnych źródeł pozyskiwania wiedzy, używania pojęć i terminów naukowych	praca pisemna w domu, odpowiedź ustna
	Ig_U04	Student posiada umiejętności rzeczowego argumentowania stanowiska w zakresie zapewnienia porządku i bezpieczeństwa wewnętrznego przez państwo	Odpowiedź ustna
Kompetencje społeczne	**Ig_K01**	Student potrafi pracować w grupie nad rozwiązaniem różnych problemów społecznych, bronić swoich poglądów oraz przyjmować argumentacje innych osób	Projekty grupowe podczas zajęć, odpowiedź ustna
	Ig_K02	Student potrafi wykorzystać nabytą wiedzę w celu rozwiązywania problemów	Praca pisemna podczas zajęć, odpowiedź ustna
	Ig_K03	Student potrafi (w oparciu o uzyskaną poszerzoną wiedzę) szukać potrzebnych informacji i wykorzystywać źródła oraz doskonalić swoją wiedzę i umiejętności z tego obszaru	Praca pisemna w domu, odpowiedź ustna

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
W01	Zajęcia wprowadzające. Istota bezpieczeństwa i bezpieczeństwa wewnętrznego państwa – aspekty teoretyczne i praktyczne.	3
W02	Teoretyczne aspekty strategii w obszarze militarnym i niemilitarnym.	2
W03	Poglądy wybranych klasyków strategii.	2
W04	Bezpieczeństwo wewnętrzne w ujęciu dziejowym.	2
W05	Współczesne zagrożenia bezpieczeństwa wewnętrznego.	4
W06	Podmioty kształtujące bezpieczeństwo wewnętrzne państwa.	3
W07	Dokumenty strategiczne z obszaru bezpieczeństwa wewnętrznego wybranych podmiotów.	2
W08	Metodologia tworzenia strategii bezpieczeństwa wewnętrznego.	2
C01	Projekt semestralny: 6. Analiza środowiska bezpieczeństwa wewnętrznego w aspekcie wybranego sektora (zagrożenia) bezpieczeństwa 7. Identyfikacja i analiza kluczowych determinant (uwarunkowań) sektora bezpieczeństwa	10

	8. Identyfikacja bezpieczeństwa wewnętrznego jako podmiotu bezpieczeństwa – interesy i cele 9. Metody: a. Identyfikacja słabych i mocnych stron oraz szans wyzwań i zagrożeń bezpieczeństwa wewnętrznego w ramach wybranego sektora (zagrożenia) bezpieczeństwa. Analiza SWOT/TOWS. b. Macierz wielokryterialna opisu czynników bazowych dla wybranego sektora (zagrożenia). c. Projektowanie udziału struktur państwa biorących udział w realizacji celów. 10. Synteza i wnioski wypływających z analiz	

IV.	**KORELACJA EFEKTÓW KSZTAŁCENIA**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyczny PRK*
W01	Ig_W01, Ig_K03	SIB2_W01, SIB2_U02, SIB2_K01	P7U_W, P7S_WG, P7U_U, P7S_UW, P7U_K, P7S_KK
W02	Ig_W01, Ig_U04, Ig_K03	SIB2_W01, SIB2_U02, SIB2_K01	P7U_W, P7S_WG, P7U_U, P7S_UW, P7U_K, P7S_KK
W03	Ig_W01, Ig_K03	SIB2_W01, SIB2_W03, SIB2_U02, SIB2_K01	P7U_W, P7S_WK, P7U_W, P7S_WG, P7U_U, P7S_UW, P7U_K, P7S_KK
W04	Ig_W01, Ig_U03, Ig_K03	SIB2_W01, SIB2_W03, SIB2_K01	P7U_W, P7S_WK, P7U_W, P7S_WG,P7U_K, P7S_KK
W05	Ig_W01, Ig_W04, Ig_U02, Ig_U03, Ig_K03	SIB2_W01, SIB2_W03, SIB2_K01	P7U_W, P7S_WG,P7U_W, P7S_WK,P7U_K, P7S_KK
W06	Ig_W02, Ig_W03, Ig_U01, Ig_K03	SIB2_W01, SIB2_U07, SIB2_K01	P7U_W, P7S_WG,P7U_U, P7S_UU, P7U_K, P7S_KK
W07	Ig_W01, Ig_W04, Ig_U04, Ig_ K01, Ig_K03	SIB2_W01, SIB2_U04, SIB2_U07, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UK, P7U_U, P7S_UU, P7U_K, P7S_KK
W08	Ig_W02, Ig_W03, Ig_U01, Ig_K03	SIB2_W01, SIB2_U04, SIB2_U07, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UK, P7U_U, P7S_UU, P7U_K, P7S_KK
C01	Ig_W01, Ig_W04, Ig_U02, Ig_K02, Ig_K03	SIB2_W01, SIB2_W03, SIB2_U07, SIB2_U02, SIB2_K02, SIB2_K04	P7U_W, P7S_WG,P7U_W, P7S_WK,P7U_U, P7S_UU, P7U_U, P7S_UW, P7U_K, P7S_KK, P7U_K, P7S_KO, P7U_K, P7S_KR

V.	**NAKŁAD PRACY STUDENTA**			
Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**20**	**X**	**150**	**6**
Ćwiczenia	**10**			
Seminaria				
Konwersatoria				
Konsultacje (zaliczenie nieobecności, rozliczenie rygorów, poprawy)	**6**			
Przygotowanie do ćwiczeń	**X**	**40**		
Opanowanie informacji		**40**		
Przygotowanie do rozliczenia rygorów		**34**		
RAZEM	**36**	**114**		

VI.	**METODY DYDAKTYCZNE**
1.	- wykład; - wykład z prezentacją multimedialną;
2.	- ćwiczenie; - ćwiczenia przedmiotowe wykaz tez do dyskusji;
3.	- praca w grupach i inne aktywizujące; - prezentacja multimedialna analiza przypadków;
VII.	**FORMA ZALICZENIA PRZEDMIOTU**

Rygor	*Kryteria składowe*	*Waga*
Zaliczenie	Ocena z projektu semestralnego	0,4
	ocena z kolokwium	0,6
Egzamin	Test końcowy z treści wykładu	0,7
	Rozliczenie projektu semestralnego	0,3

VIII.	**LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA**
	OBOWIĄZKOWA
1.	S. Kamiński, Przegląd bezpieczeństwa narodowego w planowaniu strategicznym Polski, Warszawa 2015
2.	P. Majer, *Bezpieczeństwo wewnętrzne Polski w rozwoju dziejowym*, Szczytno, 2012
3.	S. Sulowski (red), M. Brzeziński, *Bezpieczeństwo wewnętrzne państwa. Wybrane zagadnienia*, Wydawnictwo Elipsa, Warszawa 2009
4.	T. Szubrycht, *Strategie doktryny morskie*, AMW, Gdynia 2013
5.	Z. Ścibiorek, B. Wiśniewski, R.B. Kuc, A. Dawidczyk, *Bezpieczeństwo wewnętrzne. Podręcznik akademicki*, Wyd. Adam Marszałek, Toruń 2015
6.	Wawrzyk P., *Bezpieczeństwo wewnętrzne Unii Europejskiej*, Wydawnictwo Akademickie i Profesjonalne, Warszawa 2009
	UZUPEŁNIAJĄCA
1.	M. Gąsior, E. Daniiloudi-Zielińska, Be*zpieczeństwo Rzeczypospolitej Polskiej: wymiar przedmiotowy i instytucjonalny*, Gdynia 2018
2.	A. Misiuk, *Administracja porządku i bezpieczeństwa publicznego: zagadnienia prawno-ustrojowe*, Wydawnictwo Akademickie i Profesjonalne, Warszawa 2008

IX.	**PROWADZĄCY PRZEDMIOT**
Stopień, Imię i nazwisko	prof. dr hab. Tomasz Szubrycht, dr Eleni Daniiloudi-Zielińska
adres e-mail	t.szubrycht@amw.gdynia.pl, edaniiloudi@interia.pl

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:	**Metodologia badań nad bezpieczeństwem**	*Kod*:	**Cxm**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Niestacjonarne		
Kształcenie w zakresie:	Cyberbezpieczeństwo, Analiza danych i informatyka śledcza		
Profil:	Ogólnoakademicki		
Liczba ECTS:	3		
Semestr:	2		
Wymagania wstępne:	Wiedza merytoryczna z przedmiotów kierunkowych		
Język wykładowy:	Polski		
Cel przedmiotu:	**C01**	Zapoznać z procesem badań naukowych w zakresie bezpieczeństwa	
	C02	Nauczyć zasad i metod prowadzenia badan naukowych	
	C03	Przygotować do samodzielnego formułowania i rozwiązywania problemów naukowych w zakresie bezpieczeństwa	
	C04	Przygotować do opracowania pracy dyplomowej odpowiadającej regułom pracy naukowej	

II.	**EFEKTY UCZENIA SIĘ**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Cxm_W01**	Znajomość miejsca i roli nauki we współczesnym świecie	Sprawdzian pisemny
	Cxm_W02	Znajomość podstawowych pojęć z metodyki prowadzenia badań	Sprawdzian pisemny
	Cxm_W03	Wiedza o podstawowych metod badawczych i operacjach myślowych stosowanych w badaniach nad bezpieczeństwem	Sprawdzian pisemny
	Cxm_W04	Zrozumienie istoty procesu badań naukowych i możliwości zastosowania go w badaniach nad bezpieczeństwem	Sprawdzian pisemny
	Cxm_W05	Znajomość zasad naukowego opisu i wyjaśniania zagrożeń bezpieczeństwa narodowego	Sprawdzian pisemny
Umiejętności:	**Cxm_U01**	Dostrzeganie sytuacji problemowych w zakresie bezpieczeństwa w życiu codziennym i w pracy zawodowej	Wypowiedzi ustne
	Cxm_U02	Formułowania problemów badawczych i hipotez roboczych	Opracowanie pisemne
	Cxm_U03	Wybór odpowiedniej metody badawczej i sporządzanie adekwatnych narzędzi badawczych	Opracowanie pisemne
	Cxm_U04	Przeprowadzanie badań	Opracowanie pisemne
	Cxm_U05	Przedstawiania wyników badań w formie publikacji	Opracowanie pisemne

Kompetencje społeczne:	**Cxm_K01**	Zrozumienie istoty i potrzeb pogłębiania wiedzy	Wypowiedzi ustne
	Cxm_K02	Dostrzeganie zagrożeń bezpieczeństwa i poszukiwanie środków zaradczych	Wypowiedzi ustne
	Cxm_K03	Akceptacja roli i zadań formacji bezpieczeństwa i wsparcie ich działań	Rozwiązania ustne i pisemne
	Cxm_K04	Wnikliwa obserwacja środowiska bezpieczeństwa i podejmowanie działań zapobiegawczych zagrożeniom	Wypowiedzi ustne

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
W01	**Praca magisterska – istota i wymagania** (praca magisterska jako praca promocyjna; cel pracy magisterskiej; wymagania formalne; kryteria naukowości; ogólny tok postępowania; zasady wyboru tematu; układ pracy; układ i treść procedury badawczej; etapy opracowania, rola promotora)	1
W02	**Nauka – istota i klasyfikacja** (wieloznaczność pojęcia nauki; cele nauki i poznania naukowego; funkcje nauki; treść nauki; zasady i czynności poznania naukowego, teoria naukowa; podejścia naukowe; proces badawczy; klasyfikacja nauk; stopnie, tytuły i stanowiska naukowe)	1
W03	**Proces badań naukowych** (pojęcie procesu badawczego; etapy przygotowania i prowadzenia badań; cel i przedmiot badań w naukach o bezpieczeństwie; metody badań naukowych)	1
W04	**Problemy, hipotezy i zmienne w procesie badań naukowych** (sytuacja problemowa, sens i sposób wyrażania problemu naukowego, hipotezy wstępne, robocze i naukowe, rodzaje hipotez, zmienne badawcze , współzmienność, wskaźniki, ich rodzaje i znaczenie, skale pomiarowe)	1
W05	**Metody, techniki i narzędzia badawcze** (pojęcie metody naukowej i metod badawczych; techniki badawcze; podstawowe – empiryczne metody badawcze; metody teoretyczne – rozumowanie proste i złożone; schematy wnioskowania, narzędzia badawcze)	1
W06	**Podejścia i metody badawcze w badaniach nad bezpieczeństwem (**cel i przedmiot badań, badania ilościowe i jakościowe, metody teoretyczne i empiryczne, narzędzia badawcze w badaniach ilościowych i jakościowych}	1
W07	**Wykorzystanie materiałów źródłowych w pracach promocyjnych** (bibliografia a literatura przedmiotu badań, rodzaje literatury naukowej, sposoby poszukiwania literatury przedmiotu badań, kolejność i etapy studiowania literatury, sporządzanie notatek, porządkowanie i uogólnienie uzyskanego materiału, analiza dokumentów, wykorzystanie Internetu, sposoby sprawdzania wiarygodności źródeł, cytowanie i parafrazowanie)	1
W08	Sprawdzian pisemny – zaliczenie przedmiotu	1
C01	Opis sytuacji problemowych	1
C02	Formułowanie problemów i hipotez badawczych	1
C03	Wybór i zastosowanie adekwatnej metody badawczej	1
C04	Przygotowanie narzędzi badawczych	1
C05	Organizowanie badań	1
C06	Zbieranie materiałów źródłowych i ich wykorzystanie w badaniach nad bezpieczeństwem (fakty, cytaty, parafrazy)	1

C07	Opracowanie koncepcji pracy dyplomowej – zaliczenie ćwiczeń	2

IV.	**KORELACJA EFEKTÓW UCZENIA SIĘ**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyki PRK*
W01	Cxm_W01, Cxm_K03	SIB2_W01, SIB2_K04	P7U_W, P7S_WG, P7U_K, P7S_KR
W02	Cxm_W02, Cxm_K02	SIB2_W01, SIB2_K02	P7U_W, P7S_WG, P7U_K, P7S_KK
W03	Cxm_W04	SIB2_W01	P7U_W, P7S_WG
W04	Cxm_W03, Cxm_K02	SIB2_W01, SIB2_K03	P7U_W, P7S_WG, P7U_K, P7S_KO
W05	Cxm_W03	SIB2_W01	P7U_W, P7S_WG
W06	Cxm_W05	SIB2_W01	P7U_W, P7S_WG
W07	Cxm_W05	SIB2_W01, SIB2_U02	P7U_W, P7S_WG, P7U_U, P7S_UW
C01	Cxm_U01, Cxm_K04	SIB2_U01, SIB2_U02	P7U_U, P7S_UW
C02	Cxm_U02	SIB2_U07	P7U_U, P7S_UU
C03	Cxm_U03	SIB2_U07	P7U_U, P7S_UU
C04	Cxm_U03	SIB2_U07	P7U_U, P7S_UU
C05	Cxm_U04	SIB2_U07	P7U_U, P7S_UU
C06	Cxm_U05	SIB2_U07	P7U_U, P7S_UU
C07	Cxm_U05	SIB2_U07	P7U_U, P7S_UU

V.	**NAKŁAD PRACY STUDENTA**			
Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**10**	**X**	**75**	**3**
Ćwiczenia	**10**			
Seminaria	**-**			
Konwersatoria	**-**			
Konsultacje (zaliczenie nieobecności, rozliczenie rygorów, poprawy)	**5**			
Przygotowanie do ćwiczeń	**X**	**15**		
Opanowanie informacji		**15**		
Przygotowanie do rozliczenia rygorów		**20**		
RAZEM	**25**	**50**		

VI.	**METODY I NARZĘDZIA DYDAKTYCZNE**
1.	Wykłady – oddziaływanie słowne i prezentacje multimedialne. Zagadnienia do pisemnego sprawdzianu wiedzy. Wykaz literatury do samodzielnego studiowania w celu pogłębienia wiedzy.
2.	Ćwiczenia - zadania do dyskusji i pisemnego rozwiązania.

VII.	**FORMA ZALICZENIA PRZEDMIOTU**	
Rygor	*Kryteria składowe*	*Waga*
Zaliczenie	Ocena wystąpień i rozwiązań prezentowanych na ćwiczeniach	0.5
	Ocena za znajomość teoretyczną przedmiotu.	0.5

VIII.	**LITERATURA**
	OBOWIĄZKOWA
1.	S. Nowak, *Metodologia badań społecznych*, PWN, Warszawa 2010.
2.	W. Zaczyński, *Praca badawcza nauczyciela*, Wydawnictwa Szkolne i Pedagogiczne, Warszawa 1995.
3.	R. Zenderowski, *Praca magisterska, licencjat*, wyd. CeDeWu.pl, Warszawa
	UZUPEŁNIAJĄCA
1.	A. Chalmers, *Czym jest to co zwiemy nauką?*, wyd. Siedmiogród, Wrocław 1977
2.	E. Babbie, *Podstawy nauk społecznych*, PWN, Warszawa 2009
3.	K. Pawlik, R. Zenderowski, *Dyplom z Internetu. Jak korzystać z Internetu pisząc prace dyplomowe*, Wydawnictwa Fachowe, Warszawa 2010

4.	J. Sztumski, *Wstęp do metod i technik badań społecznych*, wyd. „Śląsk", Katowice 2010
5.	Ch. Frankfort-Nachmias, *Metody badawcze w naukach społecznych*, wyd. Zysk i Ska, Poznań 2001

IX.	**PROWADZĄCY PRZEDMIOT**
Stopień, Imię i nazwisko	Prof. dr hab. Czesław JARECKI, Dr Stefan KOWALSKI
adres e-mail, tel.	c.jarecki@amw.gdynia.pl , s.kowalski@amw.gdynia.pl

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:	**Podstawy ekonomii**	*Kod*:	**Cea**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Niestacjonarne		
Kształcenie w zakresie:	Cyberbezpieczeństwo, Analiza danych i informatyka śledcza		
Profil:	Ogólnoakademicki		
Liczba ECTS:	2		
Semestr:	2		
Wymagania wstępne:	Podstawowa wiedza z matematyki		
Język wykładowy:	Polski		
Cel przedmiotu:	**C01**	Prezentacja miejsca, znaczenia i motywacji podejmowania decyzji przez gospodarstwa domowe, przedsiębiorstwa i państwo	
	C02	Przybliżenie roli państwa w gospodarce rynkowej oraz jego aktywnej roli w rozwiązywaniu problemów gospodarczych i społecznych w tym problemów bezpieczeństwa narodowego	
	C03	Zapoznanie z cechami gospodarki rynkowej oraz uwarunkowaniami skuteczności mechanizmu rynkowego w warunkach społecznej gospodarki rynkowej (państwa dobrobytu)	

II.	**EFEKTY UCZENIA SIĘ**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Cea_W01**	Posiada wiedzę umożliwiają identyfikację i opis struktur, relacji, oraz konsekwencji funkcjonowania podmiotów rynkowych w skali mikro i makro	Kolokwium
	Cea_W02	Zna podstawowe podmioty gospodarki rynkowej oraz relacje między nimi występujące, a szczególnie funkcje państwa w gospodarce rynkowej	Kolokwium
	Cea_W03	Zna motywacje i uwarunkowania podejmowania decyzji alokacyjnych gospodarstwa domowego, przedsiębiorstwa i państwa	Kolokwium
Umiejętności:	**Cea_U01**	Potrafi interpolować wnioski z obszaru ekonomii na problemy bezpieczeństwa (potrafi identyfikować problem ekonomizacji bezpieczeństwa)	Kolokwium
	Cea_U02	Dokonuje obserwacji zjawisk i procesów w gospodarce oraz potrafi opisać i zinterpretować problemy ekonomiczne stosując podstawowe pojęcia teoretyczne	Kolokwium
	Cea_U03	Dokonuje oceny proponowanych rozwiązań problemów gospodarczych z uwzględnieniem skutków dla bezpieczeństwa narodowego	Kolokwium

Kompetencje społeczne:	**Cea_K01**	Posiada umiejętność rzeczowego argumentowania stanowiska w zakresie zaspokajania potrzeb publicznych przez państwo	Kolokwium
	Cea_K02	Potrafi prezentować i bronić swoich poglądów i uznawać argumentację innych	Kolokwium
	Cea_K03	W oparciu o uzyskaną podstawową wiedzę z ekonomii potrafi doskonalić swoją wiedzę i umiejętności z tego obszaru	Samokształcenie

III.	**TREŚCI PROGRAMOWE**	
Forma	*Temat, zagadnienia*	*Liczba godzin*
W01	**Wprowadzenie do gospodarki i ekonomii** (czym zajmuje się ekonomia; gospodarowanie; ekonomia a inne nauki; z historii myśli ekonomicznej; ekonomia pozytywna i normatywna; mikroekonomia i makroekonomia; rzadkość i inne problemy ekonomiczne; potrzeby; źródła zaspokajania potrzeb; racjonalność rzeczowa a racjonalność metodologiczna; prawa Engla; prawo Voblena; prawo Giffena; dylematy dobrobytu ekonomicznego i społecznego; współczesne systemy społeczno-gospodarcze)	1
W02	**Popyt, podaż i rynek** (rynek i jego cechy; popyt, cena, równowaga rynkowa.; krzywe popytu i podaży; co kryje się za krzywą popytu; przesunięcia krzywej popytu; co kryje się za krzywą podaży?; przesunięcia krzywej podaży; wolny rynek i kontrola cen; co, jak i dla kogo wytwarzać?)	2
W03	**Teoria wyboru konsumenta i elastyczność popytu** (zasady wyboru konsumenta; dostosowanie do zmian dochodu; dostosowania do zmian cen; od indywidualnej do rynkowej krzywej; popytu; dobra komplementarne i dobra substytucyjne; transfery gotówkowe i rzeczowe; reakcje popytu na zmiany cen; cena, wielkość popytu i suma wydatków; inne przykłady zastosowań elastyczności; elastyczność mieszana popytu; wpływ dochodu na popyt; wpływ inflacji na kształtowanie się popytu)	2
W04	**Funkcja produkcji** (organizacja przedsiębiorstwa; przychody, koszty i zyski; maksymalizacja zysku w przedsiębiorstwie; decyzje produkcyjne przedsiębiorstwa: analiza ogólna; izokwanta, izokoszta, efektywność produkcji, koszt krańcowy i utarg krańcowy)	2
W05	**Struktury rynku, konkurencja doskonała, niedoskonałai pełny monopol** (konkurencja doskonała; decyzje produkcyjne przedsiębiorstwa w warunkach konkurencji doskonałej; krzywe podaży gałęzi; statyka porównawcza w przypadku gałęzi wolnokonkurencyjnej; konkurencja na rynkach światowych; konkurencja monopolistyczna; oligopol i współzależność; wejście i potencjalna konkurencja; strategiczne odstraszanie kandydatów do wejścia; produkcja i cena w warunkach monopolu i konkurencji doskonałej; monopol a postęp techniczny; koszt społeczny monopolu)	1
W06	**Udział państwa w gospodarce w ujęciu mikroekonomicznym** (argumenty za udziałem państwa; argumenty przeciw udziałowi państwa; rola przypisywana państwu w różnych systemach gospodarczych i przez różne nurty ekonomiczne; równość i	1

	efektywność; konkurencja doskonała a efektywność w sensie Pareta; zawodność rynku; problemy ze środowiskiem; jakość, zdrowie i bezpieczeństwo)	
W07	**Determinanty dochodu narodowego. Analiza krótkookresowa i długookresowa** (zarys głównych stanowisk teoretycznych; produkt i dochód narodowy; pojęcie i podstawowe problemy makroekonomii; problem agregacji; metody obliczania produktu krajowego brutto; produkt narodowy brutto i dochód narodowy; produkt i dochód narodowy jako miary poziomu rozwoju gospodarczego i dobrobytu; pojęcie i mechanizm równowagi; funkcja konsumpcji; równowaga w uproszczonym modelu gospodarki; równość inwestycji i oszczędności; mnożnik; równowaga w rozwiniętym modelu gospodarki; czynniki wzrostu gospodarczego; pełne zatrudnienie a potencjalny PKB; model wzrostu Solowa; formuła wzrostu gospodarczego; polityka pobudzania wzrostu; płace a zwolnienie tempa wzrostu wydajności pracy; zrost gospodarczy a tendencje postępu technicznego; popytowe czynniki wzrostu; granice wzrostu gospodarczego.)	1
W08	**Budżet państwa** (pojęcie i funkcje budżetu państwa; dochody budżetu państwa; wydatki budżetu państwa; podatki i wydatki państwa jako instrumenty 3stabilizacji koniunktury; mnożnikowy efekt wydatków, podatków i zrównoważenia budżetu; aktywna i pasywna polityka fiskalna; automatyczne stabilizatory koniunktury; deficyt budżetowy i dług publiczny; budżet państwa w Polsce w okresie transformacji gospodarki)	2
W09	**System pieniężno-kredytowy** (istota i funkcje pieniądza; ewolucja pieniądza i systemu pieniężnego; zasoby pieniądza; koszt posiadania pieniądza; popyt na pieniądz i podaż pieniądza; czynniki determinujące popyt na pieniądz; powstanie i funkcje banków; bank centralny. Instrumenty kontroli podaży pieniądza; czynniki determinujące podaż pieniądza; równowaga na rynku pieniężnym; niebankowe instytucje pośrednictwa finansowego; rynek pieniężny i kapitałowy; pieniądz i banki w okresie transformacji gospodarki polskiej)	1
W10	**Cykl koniunkturalny** (pojęcie cyklu koniunkturalnego; fazy cyklu; rodzaje wahań cyklicznych; cykl a wzrost gospodarczy; teorie wahań cyklicznych; metody oddziaływania państwa na przebieg cyklu koniunkturalnego; wahania stopy wzrostu i kryzysy w gospodarce centralnie planowanej)	1
W11	**Bezrobocie i inflacja** (pojęcie bezrobocia; typy bezrobocia; bezrobocie w wybranych krajach; przyczyny bezrobocia; bezrobocie a działalność państwa; zatrudnienie i bezrobocie w gospodarce centralnie planowanej; bezrobocie w Polsce w okresie transformacji; pojęcie, sposoby pomiaru oraz nasilenie inflacji; społeczno-ekonomiczne skutki inflacji; główne teorie inflacji; inflacja a bezrobocie; koncepcja krzywej Phillipsa; inflacja w Polsce w okresie transformacji	1

IV.	**KORELACJA EFEKTÓW UCZENIA SIĘ**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyki PRK*
W01	Cea_W01, Cea_U01, Cea_K03	SIB2_W01; SIB2_U02; SIB2_K01	P7U_W P7S_WG P7U_W P7U_U P7U_UW; P7U_KP7S_KK
W02	Cea_W02, Cea_K03	SIB2_W01; SIB2_U02, SIB2_K01	P7U_W; P7S_WG; P7U_UW; P7U_K; P7S_KK

W03	Cea_W01, Cea_W03, Cea_K03	SIB2_W01; SIB2_W02, SIB2_U02; SIB2_W05; SIB2_K01	P7U_W; P7S_WG; P7U_W; P7S_WK; P7U_UW; P7U_K; P7S_KK
W04	Cea_W02, Cea_W03, Cea_K03	SIB2_W01; SIB2_W02, SIB2_U02; SIB2_W05; SIB2_K01	P7U_W; P7S_WG; P7U_W; P7S_WK; P7U_UW; P7U_K; P7S_KK
W05	Cea_W01, Cea_W02, Cea_K03	SIB2_W01; SIB2_W02, SIB2_U02; SIB2_K01	P7U_W; P7S_WG; P7U_W; P7S_WK; P7U_UW; P7U_K; P7S_KK
W06	Cea_W01, Cea_U02,Cea_K03	SIB2_W01; SIB2_W02, SIB2_U02; SIB2_K01	P7U_W; P7S_WG; P7U_W; P7S_WK; P7U_UW; P7U_K; P7S_KK
W07	Cea_W01, Cea_U01, Cea_K01,Cea_K03	SIB2_W01, SIB2_U02; SIB2_K02, SIB2_K03	P7U_W; P7S_WG; P7U_W; P7U_U; P7U_UW; P7U_K; P7S_KO; P7U_K; P7S_KK
W08	Cea_W01, Cea_U01, Cea_K01,Cea_K03	SIB2_W01, SIB2_U02; SIB2_K02, SIB2_K03	P7U_W; P7S_WG; P7U_U; P7U_UW; P7U_K; P7S_KO; P7U_K; P7S_KK
W09	Cea_W01, Cea_U01,Cea_K01	SIB2_W01; SIB2_U02; SIB2_K02;	P7U_W; P7S_WG; P7U_U; P7U_UW; P7U_K; P7S_KO;
W10	Cea_W01, Cea_U01, Cea_K02, Cea_K03	SIB2_W01; SIB2_U02; SIB2_K02; SIB2_K03	P7U_W; P7S_WG; P7U_U; P7U_UW; P7U_K; P7S_KO; P7U_K; P7S_KK
W11	Cea_W01, Cea_U01, Cea_K03	SIB2_W01; SIB2_U02; SIB2_K03	P7U_W; P7S_WG; P7U_U; P7U_UW; P7U_K; P7S_KK

V. NAKŁAD PRACY STUDENTA

Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**16**	**X**	**50**	**2**
Ćwiczenia	**0**			
Seminaria	**0**			
Konwersatoria	**0**			
Konsultacje (zaliczenie nieobecności, rozliczenie rygorów, poprawy)	**5**			
Przygotowanie do ćwiczeń	**X**	**0**		
Opanowanie informacji		**15**		
Przygotowanie do rozliczenia rygorów		**14**		
RAZEM	**21**	**29**		

VI. METODY I NARZĘDZIA DYDAKTYCZNE

- wykład; - formy aktywizujące; - wykaz tez do dyskusji	- prezentacja multimedialna;

VII. FORMA ZALICZENIA PRZEDMIOTU

Rygor	*Kryteria składowe*	*Waga*
Zaliczenie	Ocena z kolokwium	1,0

VIII. LITERATURA

OBOWIĄZKOWA

1. D. Begg, *Ekonomia – Makroekonomia*, PWE
2. D. Begg, *Ekonomia – Mikroekonomia*, PWE;
3. B . Czarny, *Podstawy ekonomii*, Polsof-AKADEMIA

UZUPEŁNIAJĄCA

1. R. E. Hall, J. B. Taylor, *Makroekonomia*, PWN
2. N. G. Mankiw, M. P. Taylor, *Mikroekonomia*, PWE
3. P. A. Samuelson, *Ekonomia*, PWN
4. M. Szczepaniec, Makroekonomia, Wydawnictwo UG
5. H. R. Varian, *Mikroekonomia*, PWN

IX.	PROWADZĄCY PRZEDMIOT
Stopień, Imię i nazwisko	dr hab. Jarosław TESKA
adres e-mail, tel.	j.teska@amw.gdynia.pl

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:	**Podstawy prawa**	*Kod*:	**Cap**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Niestacjonarne		
Kształcenie w zakresie:	Cyberbezpieczeństwo, Analiza danych i informatyka śledcza		
Profil:	Ogólnoakademicki		
Liczba ECTS:	2		
Semestr:	2		
Wymagania wstępne:	-		
Język wykładowy:	Polski		
Cel przedmiotu:	**C01**	Zaznajomienie z podstawowymi pojęciami z zakresu nauki o prawie	
	C02	Przedstawienie charakterystyki systemu prawa	
	C03	Zaznajomienie z wiadomościami z zakresu podmiotów, przedmiotu, tworzenia i stosowania prawa	

II.	**EFEKTY UCZENIA SIĘ**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Cap_W01**	Student ma wiedzę z zakresu definiowania prawa i znajomości systematyzacji prawa	Kolokwium
	Cap0_W2	Student ma podstawową wiedzę z zakresu znajomości podstawowych instytucji prawa i jego funkcji	Kolokwium
	Cap_W03	Student zna źródła prawa (ich umiejscowienie w systemie prawa i poprawną hierarchię oraz budowę), zna zasady tworzenia, stosowania i interpretowania prawa	Kolokwium
	Cap_W04	Student ma wiedzę z zakresu struktury stosunku prawnego, jego powstawania i zmian oraz skutków tym wywoływanych	Kolokwium
Umiejętności:	**Cap_U01**	Student potrafi dokonać analizy prostego aktu prawnego, zdarzenia prawnego	Kolokwium
	Cap_U02	Student potrafi zastosować konstrukcje prawne w celu rozwiązania problemów pojawiających się podczas tworzenia, przestrzegania i stosowania prawa	Kolokwium
	Cap_U03	Student potrafi zastosować dyrektywy wykładni prawa	Kolokwium
Kompetencje społeczne:	**Cap_K01**	Student potrafi współdziałać w grupie w celu rozwiązania problemów związanych z danym stanem faktycznym	Kolokwium

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

W01	Zajęcia wprowadzające (zapoznanie z celem nauczania przedmiotu, przedstawienie literatury przedmiotu, podanie wymagań na zaliczenie przedmiotu)	1
W02	Nauki prawne (podział nauk, przedmiot badań nauk prawnych)	2
W03	Źródła prawa (historyczne źródła prawa, konstytucja i inne źródła prawa)	3
W04	System prawa (historyczne systemy prawa, współczesne pojęcie i rodzaje systemów prawa)	2
W05	Stanowienie i obowiązywanie prawa (formy tworzenia prawa, procesy stanowienia prawa, pojęcie aktu normatywnego i jego budowy, obowiązywanie prawa w miejscu i czasie)	2
W06	Podmioty i przedmioty prawa	2
W07	Wykładnia prawa (pojęcie wykładni, racjonalny prawodawca, luki w prawie)	2
W08	Stosowanie prawa (aspekt proceduralny i merytoryczny), zaliczenie	2

IV. KORELACJA EFEKTÓW UCZENIA SIĘ

Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyki PRK*
W01	Cap_W02	SIB2_W01	P7U_W P7S_WG
W02	Cap_W01, Cap_W02	SIB2_W01, SIB2_W03	P7U_W P7S_WK P7U_W P7S_WG
W03	Cap_W03	SIB2_W03	P7U_W P7S_WK
W04	Cap_W01,Cap_W02,Cap_W03,Cap_U01	SIB2_W03; SIB2_U01	P7U_W P7S_WK P7U_U P7S_UW
W05	Cap_W04, Cap_U02	SIB2_W03; SIB2_U07	P7U_W P7S_WK P7U_U P7S_UU
W06	Cap_W02,Cap_W04	SIB2_U01	P7U_W P7S_WG
W07	Ca_W01,Cap_W02, Cap_W03	SIB2_U01	P7U_W P7S_WK P7U_W P7S_WG
W08	Cap_W03,Cap_W04,Cap_U03,Cap_K01	SIB2_W03; SIB2_U07; SIB2_K04	P7U_W P7S_WK P7U_U P7S_UU P7U_K P7S_KR

V. NAKŁAD PRACY STUDENTA

Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**16**	**X**	**50**	**2**
Ćwiczenia	**0**			
Seminaria	**0**			
Konwersatoria	**0**			
Konsultacje (zaliczenie nieobecności, rozliczenie rygorów, poprawy)	**5**			
Przygotowanie do ćwiczeń	**X**	**0**		
Opanowanie informacji		**15**		
Przygotowanie do rozliczenia rygorów		**14**		
RAZEM	**21**	**29**		

VI. METODY DYDAKTYCZNE

1. Wykład - Prezentacja multimedialna

VII. FORMA ZALICZENIA PRZEDMIOTU

Rygor	*Kryteria składowe*	*Waga*
Zaliczenie	Ocena z kolokwium	1,0

VIII. LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

OBOWIĄZKOWA

1. A. Bator, W. Gromski, A. Kozak, S. Kaźmierczyk, Z. Pulka, *Wprowadzenie do nauk prawnych, Leksykon tematyczny*, Wydanie I, Wydawnictwo Prawnicze LexisNexis, Warszawa 2006

2.	S. Korycki, J. Kuciński, Z. Trzciński, J. Zaborowski, *Zarys prawa*, pod red. S. Koryckiego i J. Kucińskiego, Wydanie V, LexisNexis, Warszawa 2006
3.	T. Stawecki, P. Winczorek, *Wstęp do prawoznawstwa*, Wydawnictwo C. H. Beck, Warszawa 2003
UZUPEŁNIAJĄCA	
1.	M. Zirk-Sadowski, *Wprowadzenie do filozofii prawa*, Zakamycze, Kraków 2000
2.	L. Morawski, *Główne problemy współczesnej filozofii prawa. Prawo w toku przemian*, Wydanie III, LexisNexis, Warszawa 2003
3.	R. Dworkin, *Biorąc prawa poważnie*, PWN, Warszawa 1998
IX.	**PROWADZĄCY PRZEDMIOT**
Stopień, Imię i nazwisko	Dr hab. Dariusz BUGAJSKI
adres e-mail	d.bugajski@awm.gdynia.pl

KARTA PRZEDMIOTU	AKADEMIA MARYNARKI WOJENNEJ WYDZIAŁ DOWODZENIA I OPERACJI MORSKICH	

I.	CHARAKTERYSTYKA PRZEDMIOTU		
Nazwa przedmiotu:	**Wprowadzenie do psychologii społecznej**	*Kod*:	**Pps**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Niestacjonarne		
Kształcenie w zakresie:	Cyberbezpieczeństwo, Analiza danych i informatyka śledcza		
Profil:	Ogólnoakademicki		
Liczba ECTS:	2		
Semestr:	2		
Wymagania wstępne:	Brak		
Język wykładowy:	Polski		
Cel przedmiotu:	**C01**	Rozumie związek problematyki bezpieczeństwa z zagadnieniami psychologicznymi	
	C02	Zna mechanizmy i funkcje procesów psychicznych orientujących jednostkę w świecie oraz regulujące zachowanie człowieka	
	C03	Identyfikuje różne stanowiska teoretyczne wyjaśniające mechanizmy przebiegu funkcji poznawczych	

II.	EFEKTY UCZENIA		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Pps_W01**	Student rozumie bezpieczeństwo jako podstawową potrzebę człowieka; zna relacje pomiędzy bezpieczeństwem i zagrożeniem a przebiegiem różnorodnych procesów psychicznych, w tym – poznawczych i emocjonalnych	Kolokwium
	Pps_W02	Posiada wiedzę w zakresie psychologicznych koncepcji człowieka	Kolokwium
Umiejętności:	**Pps_U01**	Potrafi identyfikować grupy potrzeb człowieka, rozumiejąc warunki ich zaspokajania i wskazując potencjalne obszary deprywacji potrzeb jako sytuacje generujące zagrożenia dla bezpieczeństwa (w tym psychologicznego) jednostek i zbiorowości	Wypowiedź ustna
	Pps_U02	Student potrafi płynnie wypowiadać się na tematy związane z problematyką zajęć.	Wypowiedź ustna
Kompetencje społeczne:	**Pps_K01**	Student docenia znaczenie całożyciowego poszerzania swojej wiedzy w zakresie psychologii człowieka	Wypowiedź ustna

III.	TREŚCI PROGRAMOWE	
Forma	*Tematyka*	*Liczba godzin*
W01	Wprowadzenie do psychologii. Samoświadomość.	2
W02	Samoocena i poczucie własnej wartości.	2
W03	Człowiek w ujęciu psychologii poznawczej. Wybrane funkcje i procesy poznawcze (percepcja, pamięć, uwaga, skrypty i schematy poznawcze,	2

	myślenie i jego rodzaje). Błędy poznawcze i kontrola poznawcza. Podejmowanie decyzji i źródła błędów w podejmowaniu decyzji.	
W04	Wpływ sytuacji społecznej na zachowania ludzi i „sytuacyjne przemiany charakteru". Autorytet, konformizm, przemoc w relacjach międzyludzkich. Deprywacja potrzeb a sytuacyjne przemiany charakteru,	4
W05	Człowiek w relacjach społecznych – atrakcyjność interpersonalna, budowanie relacji i związki z innymi.	2
W06	Ocenianie innych, uprzedzenia i dyskryminacja – psychologiczne źródła i społeczne konsekwencje.	2
W07	Stres i jego rodzaje. Konsekwencje stresu. Profilaktyka.	2

IV.	**KORELACJA EFEKTÓW UCZENIA SIĘ**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyki PRK*
W01	Pps_W01, Pps_W02, Pps_U01, Pps_U02, Pps_K01	SIB2_W01, SIB2_U01, SIB2_U07, SIB2_K01	P7U_W P7S_WG P7U_U P7S_UW P7U_U P7S_UU P7U_K P7S_KK
W02	Pps_W01, Pps_W02, Pps_U01, Pps_U02, Pps_K01	SIB2_W01, SIB2_U01, SIB2_U07, SIB2_K01	P7U_W P7S_WG P7U_U P7S_UW P7U_U P7S_UU P7U_K P7S_KK
W03	Pps_W01, Pps_W02, Pps_U01, Pps_U02, Pps_K01	SIB2_W01, SIB2_U01, SIB2_U07, SIB2_K01	P7U_W P7S_WG P7U_U P7S_UW P7U_U P7S_UU P7U_K P7S_KK
W04	Pps_W01, Pps_W02, Pps_U01, Pps_U02, Pps_K01	SIB2_W01, SIB2_U01, SIB2_U07, SIB2_K01	P7U_W P7S_WG P7U_U P7S_UW P7U_U P7S_UU P7U_K P7S_KK
W05	Pps_W01, Pps_W02, Pps_U01, Pps_U02, Pps_K01	SIB2_W01, SIB2_U01, SIB2_U07, SIB2_K01	P7U_W P7S_WG P7U_U P7S_UW P7U_U P7S_UU P7U_K P7S_KK
W06	Pps_W01, Pps_W02, Pps_U01, Pps_U02, Pps_K01	SIB2_W01, SIB2_U01, SIB2_U07, SIB2_K01	P7U_W P7S_WG P7U_U P7S_UW P7U_U P7S_UU P7U_K P7S_KK
W07	Pps_W01, Pps_W02, Pps_U01, Pps_U02, Pps_K01	SIB2_W01, SIB2_U01, SIB2_U07, SIB2_K01	P7U_W P7S_WG P7U_U P7S_UW P7U_U P7S_UU P7U_K P7S_KK

V.	**NAKŁAD PRACY STUDENTA**			
Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**16**	**X**	**50**	**2**
Ćwiczenia	**0**			
Seminaria	**0**			
Konwersatoria	**0**			
Konsultacje (zaliczenie nieobecności, rozliczenie rygorów, poprawy)	**5**			
Przygotowanie do ćwiczeń	**X**	**0**		
Opanowanie informacji		**15**		
Przygotowanie do rozliczenia rygorów		**14**		
RAZEM	**21**	**29**		

VI.	**METODY DYDAKTYCZNE**
1.	Wykład problemowy z elementami dyskusji grupowej

VII.	FORMA ZALICZENIA PRZEDMIOTU	
Rygor	*Kryteria składowe*	*Waga*
Zaliczenie	Kolokwium pisemne, pytania otwarte i zamknięte	1,0
VIII.	**LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA**	
OBOWIĄZKOWA		
1.	P. G. Zimbardo, R. L. Johnson, V. McCain (red.), *Psychologia. Kluczowe koncepcje*, t. 1-5, PWN, Warszawa 2014 i in. (wybrane fragmenty).	
2.	Ph. G. Zimbardo, *Efekt Lucyfera. Dlaczego dobrzy ludzie czynią zło*, PWN, Warszawa 2008.	
UZUPEŁNIAJĄCA		
1.	J. Kozielecki, *Koncepcje psychologiczne człowieka,* Wydawnictwo Akademickie Żak, Warszawa 1997.	
2.	B. Wojciszke, Psychologia społeczna. GWP, Gdańsk 2011.	
IX.	**PROWADZĄCY PRZEDMIOT**	
Stopień, Imię i nazwisko	Dr hab. Iwona PIETKIEWICZ	
adres e-mail	i.pietkiewicz@amw.gdynia.pl	

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:	**Podstawy socjologii**	*Kod*:	**Isx**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Niestacjonarne		
Kształcenie w zakresie:	Cyberbezpieczeństwo, Analiza danych i informatyka śledcza		
Profil:	Ogólnoakademicki		
Liczba ECTS:	2		
Semestr:	2		
Wymagania wstępne:	Brak		
Język wykładowy:	Polski		
Cel przedmiotu:	**C01**	Prezentacja podstawowych problemów społecznych i zachodzących w świecie zmian.	
	C02	Przybliżenie istoty socjologicznych zachowań społecznych oraz podstawowych problemów związanych z procesami modernizacji społecznej.	

II.	**EFEKTY UCZENIA SIĘ**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Isx_W01**	Student wyjaśnia kluczowe koncepcje z zakresu logiki, wnioskowania i metodologii badań socjologicznych.	Kolokwium
	Isx_W02	Student objaśnia i ilustruje kulturowe, polityczne i społeczne procesy występujące na poziomie państwa i układów międzynarodowych wraz z ich przełożeniem na problemy bezpieczeństwa narodowego.	Kolokwium
	Isx_W03	Student ma pogłębioną wiedzę z zakresu kierunków rozwoju nowych gałęzi wiedzy, gospodarki i technologii, w tym informatycznych.	Kolokwium
	Isx_W04	Student w sposób poszerzony zna i objaśnia potrzeby kulturowe, religijne, gospodarcze, polityczne i inne, zwłaszcza społeczne, których zachwianie zaspokajania może powodować stany labilne i niebezpieczne.	Kolokwium
	Isx_W05	Student rozróżnia i wyjaśnia zasady tworzenia formalnych i nieformalnych społecznych struktur organizacyjnych oraz mechanizmy w nich rządzące na rzecz osiągania zamierzonych celów.	Kolokwium
Umiejętności:	**Isx_U01**	Student formułuje objaśnienia zjawisk społecznych, politycznych i kulturowych przebiegających zarówno w skali państwa jak i w skali międzynarodowej, a także oceniać zależności między przyczynami a poziomem intensywności zakłóceń występujących w tych obszarach.	Kolokwium
	Isx_U02	Student identyfikuje poprawnie zależności między zjawiskami społecznymi, politycznymi i	Kolokwium

		kulturowymi tworzącymi bezpieczeństwo narodowe lub oddziaływującymi na nie a także system oddziaływania normatywnych regulacji na wspomniane obszary (normy prawne, standardy zawodowe, systemy normalizacji i standaryzacji, normy moralne, normy kulturowe).	
	Isx_U03	Student posiada umiejętność rozumienia i analizowania różnorodnych zjawisk, w tym społecznych mających związek z bezpieczeństwem narodowym.	Kolokwium
Kompetencje społeczne:	**Isx_K01**	Student inicjuje i moderuje pracę w grupie, przyjmując w niej różne role, potrafi podporządkować się celom grupy ale także przyjmować funkcje lidera zadaniowego.	Odpowiedź tablicowa
	Isx_K02	Student działa z poszanowaniem zasad formalnych i metodycznie rozwiązuje problemy organizacyjne i inne.	Odpowiedź tablicowa

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
W01	Społeczeństwo jako przedmiot badań socjologicznych (socjologiczna wyobraźnia i język socjologii; współczesne perspektywy socjologiczne; socjologiczne metody badawcze; proces badawczy; rozumienie związków przyczynowo-skutkowych; metody badawcze).	1
W02	Socjologiczne pojęcie kultury (pojęcie kultury, tradycja kulturowa i tworzenie kultury; socjalizacja i kontrola społeczna; świadomość społeczna).	1
W03	Zmiana społeczna, rozwój i postęp (czynniki zmiany społecznej; zmiana w epoce nowoczesnej).	1
W04	Elementy teorii zachowań społecznych. Grupy i więzi społeczne (zachowania, czynności i działania społeczne; klasyfikacja grup społecznych).	2
W05	Klasy, stratyfikacja i nierówności (funkcje i geneza nierówności; warstwy i klasy społeczne; ruchliwość społeczna).	1
W06	Socjologia organizacji (gospodarka jako system społeczny; teorie organizacji; struktury społeczne; zmiany sposobów zarządzania; zmiany w systemie pracy; gospodarka oparta na wiedzy).	1
W07	Państwo i zbiorowości terytorialne nowoczesne państwo; pojęcie państwa; systemy polityczne; opiekuńczość państwa; zmiana polityczna i społeczna).	1
W08	Społeczeństwo jako przedmiot badań socjologicznych.	1
W09	Socjologiczne pojęcie kultury.	1
W10	Zmiana społeczna, rozwój i postęp.	1
W11	Elementy teorii zachowań społecznych. Grupy i więzi społeczne.	1
W12	Klasy, stratyfikacja i nierówności.	1
W13	Socjologia organizacji.	1
W14	Państwo i zbiorowości terytorialne.	1
W15	Kolokwium.	1

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

W01	Isx_W01, Isx_W03, Isx_U03, Isx_K02	SIB2_W01, SIB2_W02, SIB2_U02, SIB2_U07, SIB2_K03	P7U_W, P7S_WG, P7U_W P7S_WK, P7S_UW, P7U_U, P7S_UU, P7U_K, P7S_KO
W02	Isx_W02, Isx_W03, Isx_W04, Isx_U01, Isx_U02, Isx_U03	SIB2_W01, SIB2_W02, SIB2_U02, SIB2_U07, SIB2_K03	P7U_W, P7S_WG, P7U_W P7S_WK, P7S_UW, P7U_U, P7S_UU, P7U_K, P7S_KO
W03	Isx_W02, Isx_W03, Isx_U01, Isx_U02, Isx_U03, Isx_K01, Isx_K02	SIB2_W01, SIB2_W02, SIB2_U02, SIB2_U07, SIB2_K03	P7U_W, P7S_WG, P7U_W P7S_WK, P7S_UW, P7U_U, P7S_UU, P7U_K, P7S_KO
W04	Isx_W02, Isx_W03, Isx_W04, Isx_W05, Isx_U01, Isx_U02, Isx_U03, Isx_K01, Isx_K02	SIB2_W01, SIB2_W02, SIB2_U02, SIB2_U07, SIB2_K03	P7U_W, P7S_WG, P7U_W P7S_WK, P7S_UW, P7U_U, P7S_UU, P7U_K, P7S_KO
W05	Isx_W02, Isx_W03, Isx_W04, Isx_W05, Isx_U01, Isx_U02, Isx_U03, Isx_K01, Isx_K02	SIB2_W01, SIB2_W02, SIB2_U02, SIB2_U07, SIB2_K03	P7U_W, P7S_WG, P7U_W P7S_WK, P7S_UW, P7U_U, P7S_UU, P7U_K, P7S_KO
W06	Isx_W02, Isx_W03, Isx_W04, Isx_W05, Isx_U01, Isx_U02, Isx_U03, Isx_K01, Isx_K02	SIB2_W01, SIB2_W02, SIB2_U02, SIB2_U07, SIB2_K03	P7U_W, P7S_WG, P7U_W P7S_WK, P7S_UW, P7U_U, P7S_UU, P7U_K, P7S_KO
W07	Isx_W02, Isx_W03, Isx_W04, Isx_W05, Isx_U01, Isx_U02, Isx_U03, Isx_K01, Isx_K02	SIB2_W01, SIB2_W02, SIB2_U02, SIB2_U07, SIB2_K03	P7U_W, P7S_WG, P7U_W P7S_WK, P7S_UW, P7U_U, P7S_UU, P7U_K, P7S_KO
W08	Isx_W02, Isx_W03, Isx_W04, Isx_W05, Isx_U01, Isx_U02, Isx_U03, Isx_K01, Isx_K02	SIB2_W01, SIB2_W02, SIB2_U02, SIB2_U07, SIB2_K03	P7U_W, P7S_WG, P7U_W P7S_WK, P7S_UW, P7U_U, P7S_UU, P7U_K, P7S_KO
W09	Isx_W02, Isx_W03, Isx_W04, Isx_W05, Isx_U01, Isx_U02, Isx_U03, Isx_K01, Isx_K02	SIB2_W01, SIB2_W02, SIB2_U02, SIB2_U07, SIB2_K03	P7U_W, P7S_WG, P7U_W P7S_WK, P7S_UW, P7U_U, P7S_UU, P7U_K, P7S_KO
W10	Isx_W02, Isx_W03, Isx_W04, Isx_W05, Isx_U01, Isx_U02, Isx_U03, Isx_K01, Isx_K02	SIB2_W01, SIB2_W02, SIB2_U02, SIB2_U07, SIB2_K03	P7U_W, P7S_WG, P7U_W P7S_WK, P7S_UW, P7U_U, P7S_UU, P7U_K, P7S_KO
W11	Isx_W02, Isx_W03, Isx_W04, Isx_W05, Isx_U01, Isx_U02, Isx_U03, Isx_K01, Isx_K02	SIB2_W01, SIB2_W02, SIB2_U02, SIB2_U07, SIB2_K03	P7U_W, P7S_WG, P7U_W P7S_WK, P7S_UW, P7U_U, P7S_UU, P7U_K, P7S_KO
W12	Isx_W02, Isx_W03, Isx_W04, Isx_W05, Isx_U01, Isx_U02, Isx_U03, Isx_K01, Isx_K02	SIB2_W01, SIB2_W02, SIB2_U02, SIB2_U07, SIB2_K03	P7U_W, P7S_WG, P7U_W P7S_WK, P7S_UW, P7U_U, P7S_UU, P7U_K, P7S_KO
W13	Isx_W02, Isx_W03, Isx_W04, Isx_W05, Isx_U01, Isx_U02, Isx_U03, Isx_K01, Isx_K02	SIB2_W01, SIB2_W02, SIB2_U02, SIB2_U07, SIB2_K03	P7U_W, P7S_WG, P7U_W P7S_WK, P7S_UW, P7U_U, P7S_UU, P7U_K, P7S_KO
W14	Isx_W02, Isx_W03, Isx_W04, Isx_W05, Isx_U01, Isx_U02, Isx_U03, Isx_K01, Isx_K02	SIB2_W01, SIB2_W02, SIB2_U02, SIB2_U07, SIB2_K03	P7U_W, P7S_WG, P7U_W P7S_WK, P7S_UW, P7U_U, P7S_UU, P7U_K, P7S_KO
W15	Isx_W02, Isx_W03, Isx_W04, Isx_W05, Isx_U01, Isx_U02, Isx_U03, Isx_K01, Isx_K02	SIB2_W01, SIB2_W02, SIB2_U02, SIB2_U07, SIB2_K03	P7U_W, P7S_WG, P7U_W P7S_WK, P7S_UW, P7U_U, P7S_UU, P7U_K, P7S_KO

V.	**NAKŁAD PRACY STUDENTA**			
Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**16**	**X**	**50**	**2**
Ćwiczenia	**0**			
Seminaria	**0**			
Konwersatoria	**0**			

Konsultacje (zaliczenie nieobecności, rozliczenie rygorów, poprawy)	**5**			
Przygotowanie do ćwiczeń	**X**	**0**		
Opanowanie informacji		**15**		
Przygotowanie do rozliczenia rygorów		**14**		
RAZEM	**21**	**29**		

VI.	**METODY DYDAKTYCZNE**
1.	Wykład
2.	Ćwiczenia
3.	Praca w grupach i inne formy aktywizujące
4.	Wykaz tez do dyskusji
5.	Prezentacja multimedialna

VII.	**FORMA ZALICZENIA PRZEDMIOTU**	
Rygor	*Kryteria składowe*	*Waga*
Zaliczenie	Odpowiedzi ustne i udział w dyskusji na zajęciach	0,4
	Ocena z kolokwium	0,6

VIII.	**LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA**
	OBOWIĄZKOWA
1.	A. Giddens, *Socjologia*, wyd. PWN, Warszawa 2005
2.	P. Sztompka, *Socjologia. Analiza społeczeństwa*, wyd. Znak, Kraków 2002
3.	P. Sztompka, Kucia M. red., *Socjologia. Lektury*, wyd. Znak, Kraków 2009
	UZUPEŁNIAJĄCA
1.	A. Touraine, *O socjologii*, wyd. PWN, Warszawa 2010
2.	A. Kłoskowska, *Socjologia kultury*, wyd. PWN, Warszawa 2007
3.	E. Babbie, *Podstawy badań społecznych*, wyd. PWN, Warszawa 2013

IX.	**PROWADZĄCY PRZEDMIOT**
Stopień, Imię i nazwisko	dr Andrzej ŁAPA
adres e-mail	a.lapa@amw.gdynia.pl

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:	**Podstawy stosunków międzynarodowych (pol./ang)**	*Kod*:	**Ysq**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Niestacjonarne		
Kształcenie w zakresie:	Cyberbezpieczeństwo, Analiza danych i informatyka śledcza		
Profil:	Ogólnoakademicki		
Liczba ECTS:	2		
Semestr:	2		
Wymagania wstępne:	Brak		
Język wykładowy:	Polski		
Cel przedmiotu:	**C01**	Zapoznanie studenta z podstawowymi problemami współczesnych stosunków międzynarodowych.	
	C02	Wskazanie podstawowych zagrożeń dla trwałości systemu międzynarodowego.	
	C03	Wskazanie podstawowych obszarów współpracy międzynarodowej.	

II.	**EFEKTY UCZENIA SIĘ**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Ysq_W01**	Określa związki nauk o bezpieczeństwie ze stosunkami międzynarodowymi	Test
	Ysq_W02	Charakteryzuje określone instytucje polityczne i gospodarcze w wymiarze międzynarodowym	Test
	Ysq_W03	Tłumaczy procesy zachodzące na poziomie państwa i układów międzynarodowych oraz ich znaczenie dla problemów bezpieczeństwa międzynarodowego	Test
	Ysq_W04	Wyróżnia istotne wyzwania i zagrożenia dla współczesnego świata o charakterze politycznym, militarnym, religijnym i społecznym	Test
Umiejętności:	**Ysq_U01**	Analizuje przyczyny i przebieg procesów i zjawisk politycznych i ekonomicznych w sferze międzynarodowej oraz płynące z tych obszarów zagrożenia bezpieczeństwa narodowego	Test
	Ysq_U02	Analizuje zależności między zjawiskami społecznymi, ekonomicznymi, politycznymi, prawnymi i kulturowymi tworzącymi bezpieczeństwo narodowe	Test
Kompetencje społeczne:	**Ysq_K01**	Akceptuje potrzebę poszerzania swojej wiedzy i umiejętności przez całe życie	Test

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
W01	Wprowadzenie do przedmiotu, kryteria zaliczenia	1

W02	Stosunki międzynarodowe jako dyscyplina naukowa. Co nam daje badanie stosunków międzynarodowych	1
W03	Kontekst historyczny w rozwoju stosunków międzynarodowych	1
W04	Podmioty relacji w stosunkach międzynarodowych – państwa – organizacje międzynarodowe – organizacje transnarodowe	1
W05	Podstawowe dylematy współczesnych stosunków międzynarodowych – polityka, prawo międzynarodowe, ekonomia	1
W06	Główne kierunki rozważań o stosunkach międzynarodowych – przykłady doktryn polityki zagranicznej współczesnych państw	1
W07	Realizm i neorealizm, liberalizm i neoliberalizm	1
W08	Szkoła angielska, konstruktywizm, feminizm	1
W09	Teorie integracji europejskiej	1
W10	Globalizm	1
W11	Hegemonia	1
W12	Rola organizacji międzynarodowych	1
W13	Konflikty w stosunkach międzynarodowych	1
W14	Rola dyplomacji	1
W15	Bezpieczeństwo w stosunkach międzynarodowych – instytucjonalizacja	1
W16	Zaliczenie przedmiotu – kolokwium	1

IV.	**KORELACJA EFEKTÓW UCZENIA SIĘ**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyki PRK*
W01	Ysq_W01, Ysq_W02, Ysq_W03, Ysq_W04, Ysq_U01, Ysq_U02, Ysq_K01	SIB2_W01, SIB2_U01, SIB2_U04, SIB2_K02,	P7U_W P7S_WG, P7U_U P7S_UW, P7U_U P7S_UK, P7U K P7S_KK
W02	Ysq_W01, Ysq_K01	SIB2_W01, SIB2_K02	P7U_W P7S_WG, P7U K P7S_KK
W03	Ysq_W01, Ysq_W02, Ysq_W03, Ysq_W04, Ysq_U01, Ysq_U02	SIB2_K02, SIB2_U01, SIB2_U04	P7U_W P7S_WG, P7U_U P7S_UW, P7U_U P7S_UK
W04	Ysq_W01, Ysq_W02, Ysq_W03, Ysq_W04, Ysq_U01, Ysq_U02	SIB2_K02, SIB2_U01, SIB2_U04	P7U_W P7S_WG, P7U_U P7S_UW, P7U_U P7S_UK
W05	Ysq_W01, Ysq_W02, Ysq_W03, Ysq_W04, Ysq_U01, Ysq_U02	SIB2_K02, SIB2_U01, SIB2_U04	P7U_W P7S_WG, P7U_U P7S_UW, P7U_U P7S_UK
W06	Ysq_W01, Ysq_W02, Ysq_W03, Ysq_W04, Ysq_U01, Ysq_U02	SIB2_K02, SIB2_U01, SIB2_U04	P7U_W P7S_WG, P7U_U P7S_UW, P7U_U P7S_UK
W07	Ysq_W01, Ysq_W02, Ysq_W03, Ysq_W04, Ysq_U01, Ysq_U02	SIB2_K02, SIB2_U01, SIB2_U04	P7U_W P7S_WG, P7U_U P7S_UW, P7U_U P7S_UK
W08	Ysq_W01, Ysq_W02, Ysq_W03, Ysq_W04, Ysq_U01, Ysq_U02	SIB2_K02, SIB2_U01, SIB2_U04	P7U_W P7S_WG, P7U_U P7S_UW, P7U_U P7S_UK
W09	Ysq_W01, Ysq_W02, Ysq_W03, Ysq_W04, Ysq_U01, Ysq_U02	SIB2_K02, SIB2_U01, SIB2_U04	P7U_W P7S_WG, P7U_U P7S_UW, P7U_U P7S_UK
W10	Ysq_W01, Ysq_W02, Ysq_W03, Ysq_W04, Ysq_U01, Ysq_U02	SIB2_K02, SIB2_U01, SIB2_U04	P7U_W P7S_WG, P7U_U P7S_UW, P7U_U P7S_UK
W11	Ysq_W01, Ysq_W02, Ysq_W03, Ysq_W04, Ysq_U01, Ysq_U02	SIB2_K02, SIB2_U01, SIB2_U04	P7U_W P7S_WG, P7U_U P7S_UW, P7U_U P7S_UK

W12	Ysq_W01, Ysq_W02, Ysq_W03, Ysq_W04, Ysq_U01, Ysq_U02	SIB2_K02, SIB2_U01, SIB2_U04	P7U_W P7S_WG, P7U_U P7S_UW, P7U_U P7S_UK
W13	Ysq_W01, Ysq_W02, Ysq_W03, Ysq_W04, Ysq_U01, Ysq_U02	SIB2_K02, SIB2_U01, SIB2_U04	P7U_W P7S_WG, P7U_U P7S_UW, P7U_U P7S_UK
W14	Ysq_W01, Ysq_W02, Ysq_W03, Ysq_W04, Ysq_U01, Ysq_U02	SIB2_K02, SIB2_U01, SIB2_U04	P7U_W P7S_WG, P7U_U P7S_UW, P7U_U P7S_UK
W15	Ysq_W01, Ysq_W02, Ysq_W03, Ysq_W04, Ysq_U01, Ysq_U02	SIB2_K02, SIB2_U01, SIB2_U04	P7U_W P7S_WG, P7U_U P7S_UW, P7U_U P7S_UK
W16	Ysq_W01, Ysq_W02, Ysq_W03, Ysq_W04, Ysq_U01, Ysq_U02, Ysq_K01	SIB2_K02, SIB2_U01, SIB2_U04, SIB2_K01	P7U_W P7S_WG, P7U_U P7S_UW, P7U_U P7S_UK, P7U K P7S_KK

V. NAKŁAD PRACY STUDENTA

Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**16**	**X**	**50**	**2**
Ćwiczenia	**0**			
Seminaria	**0**			
Konwersatoria	**0**			
Konsultacje (zaliczenie nieobecności, rozliczenie rygorów, poprawy)	**5**			
Przygotowanie do ćwiczeń	**X**	**0**		
Opanowanie informacji		**15**		
Przygotowanie do rozliczenia rygorów		**14**		
RAZEM	**21**	**29**		

VI. METODY DYDAKTYCZNE

1.	Wykład problemowy
2.	Prezentacja multimedialna

VII. FORMA ZALICZENIA PRZEDMIOTU

Rygor	*Kryteria składowe*	*Waga*
Zaliczenie	Test	1

VIII. LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

OBOWIĄZKOWA

1.	E. Haliżak, R. Kuźniar, *Stosunki międzynarodowe. Geneza, struktura, dynamika*, Warszawa 2006
2.	R. Jackson, G. Sorensen, *Wprowadzenie do stosunków międzynarodowych. Teorie i kierunki badawcze*, Kraków 2012
3.	K. Mingst, *Podstawy stosunków międzynarodowych*, Warszawa 2008

UZUPEŁNIAJĄCA

1.	P. Ostaszewski, *Międzynarodowe stosunki polityczne. Zarys wykładów*, Warszawa 2008
2.	J. Czaputowicz, *Teorie stosunków międzynarodowych. Krytyka i systematyzacja*, Warszawa 2008
3.	E. Cziomer, L. W. Zyblikiewicz, *Zarys współczesnych stosunków międzynarodowych*, Warszawa 2006
4.	S. Sur, *Stosunki Międzynarodowe*, Warszawa 2012

IX. PROWADZĄCY PRZEDMIOT

Stopień, Imię i nazwisko	dr hab. Bogusław GOGOL, prof. AMW; dr Iwona JAKIMOWICZ-PISARSKA
adres e-mail	b.gogol@amw.gdynia.pl; i.pisarska@amw.gdynia.pl

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:	**Podstawy bezpieczeństwa narodowego (pol./ang)**	*Kod*:	**Ybc**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Niestacjonarne		
Kształcenie w zakresie:	Cyberbezpieczeństwo, Analiza danych i informatyka śledcza		
Profil:	Ogólnoakademicki		
Liczba ECTS:	3		
Semestr:	3		
Wymagania wstępne:	Podstawowa wiedza z teorii bezpieczeństwa		
Język wykładowy:	Polski		
Cel przedmiotu:	**C01**	Zapoznać się z terminologią dotyczącą relacji międzynarodowych	
	C02	Zapoznać się z terminologią dotyczącą bezpieczeństwa	
	C03	Nauczyć się metod analizy politologicznej kryzysów bezpieczeństwa na świecie	

II.	**EFEKTY UCZENIA SIĘ**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Ybc_W01**	Ma podstawową wiedzę o istocie systemu bezpieczeństwa narodowego	Test pisemny
	Ybc_W02	Zna strukturę systemu bezpieczeństwa	Test pisemny
Umiejętności:	**Ybc_U01**	Potrafi przedstawić kompetencje organów władzy i administracji publicznej w procesie kierowania bezpieczeństwem narodowym	Odpowiedź ustna
	Ybc_U02	Dostrzega problemy z zakresu bezpieczeństwa narodowego państwa	Odpowiedź ustna
	Ybc_U03	Posiada umiejętność rozumienia i analizowania różnorodnych zjawisk, związanych z bezpieczeństwem narodowym	Odpowiedź ustna
Kompetencje społeczne:	**Ybc_K01**	Rozumie potrzebę ciągłego diagnozowania stanu bezpieczeństwa narodowego	Odpowiedź ustna
	Ybc_K02	Potrafi rzeczowo argumentować stanowiska w zakresie bezpieczeństwa narodowego państwa	Odpowiedź ustna

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
W01	Zajęcia organizacyjne, prezentacja na temat współczesnych typów debaty	2
W02	Bezpieczeństwo narodowe – uwarunkowania i specyfika	2
W03	Bezpieczeństwo narodowe w perspektywie państw członkowskich Unii Europejskiej	4
W04	Bezpieczeństwo międzynarodowe	4
W05	Bezpieczeństwo narodowe Rzeczypospolitej Polskiej	3
W06	Kolokwium	1

IV.	**KORELACJA EFEKTÓW UCZENIA SIĘ**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyki PRK*
W01	Ybc_W01, Ybc_U01, Ybc_K01	SIB2_W01, SIB2_U01, SIB2_U07, SIB2_K02	P7U_W P7S_WG P7U_U P7S_UW

			P7U_U P7S_UU P7U_K P7S_KK
W02	Ybc_W01, Ybc_W02, Ybc_U02, Ybc_U03	SIB2_W01, SIB2_W03, , SIB2_U07, SIB2_U04	P7U_W P7S_WG P7U_W P7S_WK P7U_U P7S_UU P7U_U P7S_UK
W03	Ybc_W01, Ybc_W02, Ybc_U02, Ybc_U03, Ybc_K01, Ybc_K02	SIB2_W01, SIB2_W03, SIB2_U01, SIB2_U07, SIB2_U04	P7U_W P7S_WG P7U_W P7S_WK P7U_U P7S_UU P7U_U P7S_UK P7U_U P7S_UW
W04	Ybc_W01, Ybc_W02, Ybc_U02, Ybc_K01, Ybc_K02	SIB2_W01, SIB2_W03, SIB2_U01, SIB2_U07, SIB2_U04, SIB2_K02	P7U_W P7S_WG P7U_W P7S_WK P7U_U P7S_UU P7U_U P7S_UK P7U_U P7S_UW P7U_K P7S_KK
W05	Ybc_W01, Ybc_W02, Ybc_U01, Ybc_K01, Ybc_K02	SIB2_W01, SIB2_W03, SIB2_U01, SIB2_U07, SIB2_U04, SIB2_K02	P7U_W P7S_WG P7U_W P7S_WK P7U_U P7S_UU P7U_U P7S_UK P7U_U P7S_UW P7U_K P7S_KK
W06	-	-	-

V. NAKŁAD PRACY STUDENTA

Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**16**	**X**	**75**	**3**
Ćwiczenia				
Seminaria				
Konwersatoria				
Konsultacje (zaliczenie nieobecności, rozliczenie rygorów, poprawy)	**5**			
Przygotowanie do ćwiczeń	**X**			
Opanowanie informacji		**25**		
Przygotowanie do rozliczenia rygorów		**27**		
RAZEM	**21**	**54**		

VI. METODY DYDAKTYCZNE

1. Wykład z elementami konwersatorium
2. Wykład z elementami debaty

VII. FORMA ZALICZENIA PRZEDMIOTU

Rygor	*Kryteria składowe*	*Waga*
Zaliczenie	Kolokwium	0,7
	Obecność i aktywność na zajęciach	0,3

VIII. LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

OBOWIĄZKOWA

1. A. Ciupiński, K. Malak, *Bezpieczeństwo polityczne i wojskowe*, AON, Warszawa 2004
2. A. Wawrzusiszyn, *Bezpieczeństwo, Strategia, system. Teoria i praktyka w zarysie*, Warszawa 2015
3. R. Jakubczak , J. Flis, *Bezpieczeństwo narodowe Polski w XXI wieku. Wyzwania i strategie*, Bellona, Warszawa 2006
4. *Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej,* Warszawa 2013

UZUPEŁNIAJĄCA

1. W. Fehler (red.), *Współczesne bezpieczeństwo*, Wydawnictwo Naukowe Grado, Toruń 2005
2. J. Wojnarowski, *System obronności państwa: materiały do studiowania*, AON, Warszawa 2005
3. S. Koziej, *Między piekłem a rajem. Bezpieczeństwo u progu XXI wieku*, Wyd. Adam Marszałek, Toruń 2006

4.	R. Jakubczak (red.), *Podstawy bezpieczeństwa narodowego Polski w erze globalizacji*, AON, Warszawa 2008
IX.	**PROWADZĄCY PRZEDMIOT**
Stopień, Imię i nazwisko	dr hab. Krzysztof LIGĘZA, prof. AMW
adres e-mail	k.ligeza@amw.gdynia.pl

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:	**Podstawy zarządzania i organizacji**	***Kod*:**	**Pko**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Niestacjonarne		
Kształcenie w zakresie:	Cyberbezpieczeństwo, Analiza danych i informatyka śledcza		
Profil:	Ogólnoakademicki - wybieralny		
Liczba ECTS:	3		
Semestr:	3		
Wymagania wstępne:	Podstawowa wiedza z przedsiębiorczości		
Język wykładowy:	Polski		
Cel przedmiotu:	**C01**	Rozwinięcie umiejętności analizy otoczenia organizacji i podejmowania decyzji strategicznych.	
	C02	Zdobycie wiedzy na temat procesów zarządczych, takich jak planowanie, organizowanie, motywowanie i kontrolowanie.	
	C03	Zrozumienie podstawowych koncepcji i teorii związanych z organizacją i zarządzaniem.	
	C04	Zrozumienie roli przywództwa w zarządzaniu organizacją oraz rozwijanie umiejętności przywódczych.	
	C05	Nauka efektywnej komunikacji i pracy zespołowej w kontekście organizacyjnym.	
	C06	Zdobycie umiejętności zarządzania zmianą i adaptacji do dynamicznie zmieniającego się otoczenia biznesowego.	
	C07	Przygotowanie do ciągłego rozwoju osobistego i zawodowego w dziedzinie zarządzania.	

II.	**EFEKTY UCZENIA SIĘ**		
Zakres	***Kod***	***Opis efektu***	***Sposób oceny***
Wiedza:	**Pko_W01**	**Zrozumienie podstaw organizacji i zarządzania** - studenci będą mieli wiedzę na temat kluczowych pojęć, teorii i modeli związanych z zarządzaniem.	Kolokwium
	Pko_W02	**Wiedza o otoczeniu organizacji** - zrozumienie wpływu czynników zewnętrznych na działalność organizacji.	Kolokwium
	Pko_W03	**Znajomość teorii przywództwa** - studenci zdobędą wiedzę na temat różnych stylów przywództwa i ich zastosowania w praktyce.	Kolokwium
	Pko_W04	**Znajomość funkcji zarzadzania -** co to są funkcje kierowania oraz zna zasady ich stosowania; na czym polega planowanie, organizowanie, motywowanie i kontrolowanie oraz z jakich narzędzi organizatorskich korzystać, aby te funkcje efektywnie wypełniać; na czym polega podejmowanie decyzji oraz zna podstawowe etapy tego procesu.	Kolokwium

Umiejętności:	**Pko_U01**	**Umiejętność analizy otoczenia organizacyjnego -** studenci nauczą się oceniać wpływ otoczenia na decyzje organizacyjne.	Praca projektowa
	Pko_U02	**Umiejętność planowania i organizowania -** zdobędą umiejętności tworzenia celów, planowania działań i organizowania pracy.	Praca projektowa
	Pko_U03	**Umiejętność komunikacji i zarządzania zespołem -** studenci będą mogli efektywnie współpracować z innymi..	Praca projektowa
Kompetencje społeczne:	**Pko_K01**	**Komunikacja interpersonalna -** zdolność do efektywnej komunikacji z innymi członkami organizacji.	Obserwacja
	Pko_K02	**Praca zespołowa -** umiejętność współpracy, rozwiązywania konfliktów i osiągania wspólnych celów.	Obserwacja
	Pko_K03	**Zarządzanie sobą i innymi -** zdolność do motywowania siebie i innych, rozpoznawania potrzeb pracowników i tworzenia odpowiednich warunków pracy.	Obserwacja

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
W01	**Istota organizacji i zarządzania:** miejsce przedmiotu w systemie innych nauk, szkoły i prekursorzy nauki o zarządzaniu, definicja organizacji, definicja organizacji rzeczywistej i nierzeczywistej, dwunastoelementowy model organizacji Brukego i Litwina, definicja zarządzania, funkcje zarządzania, zasady zarządzania.	**1**
W02	**Otoczenie organizacji:** definicja otoczenia organizacji, wewnętrzne vs zewnętrzne otoczenie, analiza otoczenia – podstawy, interesariusze i ich wpływ na organizację, otoczenie technologiczne, otoczenie ekonomiczne, otoczenie kulturowe, otoczenie polityczno-prawne, otoczenie konkurencyjne, adaptacja organizacji do zmian w otoczeniu.	**1**
W03	**Przywództwo w organizacji:** podstawowe definicje, przywództwa, różnice między przywódcą a menedżerem, styl autokratyczny i demokratyczny, przywództwo przez przykład, komunikacja w przywództwie, motywowanie pracowników, delegowanie zadań, rozwój kompetencji przywódczych, przywództwo a kultura organizacyjna, przywództwo etyczne.	**1**
W04	**Praktyka zarządzania**: podstawy decydowania planowanie - pierwsze kroki, organizowanie pracy podstawy motywowania, kontrola jako element zarządzania zarządzanie czasem, zarządzanie konfliktem, zarządzanie zespołem, podstawy zarządzania projektami, zarządzanie zmianą.	**2**
W05	**Cele i strategia organizacji:** definicja i znaczenie celów, proces formułowania celów, misja i wizja organizacji, strategia - co to jest? poziomy strategii w organizacji, proces tworzenia strategii, analiza strategiczna, strategie	**1**

	konkurencyjne, implementacja strategii, ocena skuteczności strategii.	
W06	**Struktury organizacyjne:** definicja struktury organizacyjnej elementy struktury organizacyjnej, typy struktur organizacyjnych, struktura funkcjonalna, struktura dywizjonalna, struktura matrycowa, centralizacja vs decentralizacja, formalizacja w strukturze, koordynacja w strukturze, elastyczność struktury organizacyjnej.	**1**
W07	**Wymagania i indywidualne możliwości:**. definicja wymagań organizacyjnych, kompetencje pracowników, dopasowanie osoby do stanowiska, proces rekrutacji, selekcja kandydatów, szkolenia i rozwój pracowników, ocena pracownicza, kariera i ścieżki rozwoju, rola motywacji w pracy, zarządzanie talentami.	**1**
W08	**Kultura organizacyjna:** co to jest kultura organizacyjna? elementy kultury organizacyjnej, typy kultur organizacyjnych, rola liderów w kształtowaniu kultury, kultura a efektywność organizacji, zmiana kultury organizacyjnej, symbole i rytuały w kulturze, kultura a etyka w biznesie, kultura a innowacyjność, kultura a zarządzanie wiedzą.	**1**
W09	**Polityka i procedury:** definicja polityki organizacyjnej, rola procedur w organizacji, tworzenie polityk organizacyjnych, procedury operacyjne, procedury jakościowe, procedury bezpieczeństwa, dokumentacja procedur, audyt procedur, procedury a kultura organizacyjna, procedury a zarządzanie zmianą.	**1**
W10	**Indywidualne potrzeby i wartości:** podstawowe potrzeby pracowników, wartości w miejscu pracy, rola wartości w motywacji, zaspokajanie potrzeb w organizacji, różnice indywidualne, rola wartości w zarządzaniu, wartości a kultura organizacyjna, wartości a przywództwo, wartości a etyka pracy, wartości a satysfakcja z pracy.	**1**
W11	**Klimat w miejscu pracy:** Definicja klimatu organizacyjnego, Czynniki wpływające na klimat, Klimat a motywacja, Klimat a wydajność pracy, Klimat a satysfakcja z pracy, Klimat a zdrowie psychiczne, Klimat a komunikacja, Klimat a konflikty, Klimat a zarządzanie zmianą, Klimat a rozwój pracowników.	**1**
W12	**Motywacja wewnętrzna pracowników:** definicja motywacji wewnętrznej, teorie motywacji, motywacja a zaangażowanie, motywacja a wydajność, motywacja a satysfakcja, motywacja a cele osobiste, motywacja a rozwój zawodowy, motywacja a nagrody, motywacja a feedback, motywacja a środowisko pracy.	**1**
W13	**Indywidualne i organizacyjne wyniki pracy:** definicja wyników pracy, pomiar wyników pracy, wyniki a cele organizacji, wyniki a motywacja, wyniki a satysfakcja, wyniki a rozwój pracowników, wyniki a ocena pracownicza, wyniki a nagrody, wyniki a feedback, wyniki a zarządzanie zmianą.	**1**

W14	Zaliczenie: test jednokrotnego wyboru		**2**
IV.	**KORELACJA EFEKTÓW UCZENIA SIĘ**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyki PRK*
W01	Pko_W01; Pko_W02; Pko_W03; Pko_U01; Pko_U02; Pko_U03; Pko_K01; Pko_K02; Pko_K03.	SIB2_W01;SIB2_W02; SIB2_W03;SIB2_W04; SIB2_U01; SIB2_U02; SIB2_U03; SIB2_K01; SIB2_K02; SIB2_K03; SIB2_K04; SIB2_K05;	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK, P7S_KO, P7S_KR
W02	Pko_W01; Pko_W02; Pko_U01; Pko_U02; Pko_K02.	SIB2_W01;SIB2_W02; SIB2_W03;SIB2_W04; SIB2_U01; SIB2_U02; SIB2_U03; SIB2_K01; SIB2_K02; SIB2_K03; SIB2_K04; SIB2_K05;	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK, P7S_KO, P7S_KR
W03	Pko_W01; Pko_W02; Pko_W03; Pko_U01; Pko_U02; Pko_U03; Pko_K01; Pko_K02; Pko_K03.	SIB2_W01;SIB2_W02; SIB2_W03;SIB2_W04; SIB2_U01; SIB2_U02; SIB2_U03; SIB2_K01; SIB2_K02; SIB2_K03; SIB2_K04; SIB2_K05;	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK, P7S_KO, P7S_KR
W04	Pko_W01; Pko_W02; Pko_W03; Pko_U01; Pko_U02; Pko_U03; Pko_K01; Pko_K02; Pko_K03.	SIB2_W01;SIB2_W02; SIB2_W03;SIB2_W04; SIB2_U01; SIB2_U02; SIB2_U03; SIB2_K01; SIB2_K02; SIB2_K03; SIB2_K04; SIB2_K05;	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK, P7S_KO, P7S_KR
W05	Pko_W01; Pko_W02; Pko_W03; Pko_U01; Pko_U02; Pko_U03; Pko_K01; Pko_K03.	SIB2_W01;SIB2_W02; SIB2_W03;SIB2_W04; SIB2_U01; SIB2_U02; SIB2_U03; SIB2_K01; SIB2_K02; SIB2_K03; SIB2_K04; SIB2_K05;	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK, P7S_KO, P7S_KR
W06	Pko_W01; Pko_W02; Pko_U01; Pko_U02;	SIB2_W01;SIB2_W02; SIB2_W03;SIB2_W04; SIB2_U01; SIB2_U02; SIB2_U03; SIB2_K01; SIB2_K02; SIB2_K03; SIB2_K04; SIB2_K05;	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK, P7S_KO, P7S_KR
W07	Pko_W02; Pko_U01; Pko_U02; Pko_U03; Pko_K01; Pko_K02; Pko_K03	SIB2_W01;SIB2_W02; SIB2_W03;SIB2_W04; SIB2_U01; SIB2_U02; SIB2_U03; SIB2_K01; SIB2_K02; SIB2_K03; SIB2_K04; SIB2_K05;	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK, P7S_KO, P7S_KR
W08	Pko_W01; Pko_W02; Pko_W03; Pko_U02; Pko_K01; Pko_K02; Pko_K03.	SIB2_W01;SIB2_W02; SIB2_W03;SIB2_W04; SIB2_U01; SIB2_U02; SIB2_U03; SIB2_K01; SIB2_K02; SIB2_K03; SIB2_K04; SIB2_K05;	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK, P7S_KO, P7S_KR
W09	Pko_W01; Pko_W02; Pko_U01; Pko_U02;	SIB2_W01;SIB2_W02; SIB2_W03;SIB2_W04; SIB2_U01; SIB2_U02; SIB2_U03; SIB2_K01; SIB2_K02; SIB2_K03; SIB2_K04; SIB2_K05;	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK, P7S_KO, P7S_KR

W10	Pko_W01; Pko_W02; Pko_W03; Pko_K01; Pko_K03.	SIB2_W01;SIB2_W02; SIB2_W03;SIB2_W04; SIB2_U01; SIB2_U02; SIB2_U03; SIB2_K01; SIB2_K02; SIB2_K03; SIB2_K04; SIB2_K05;	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK, P7S_KO, P7S_KR
W11	Pko_W03; Pko_U01; Pko_U02; Pko_U03; Pko_K01; Pko_K02; Pko_K03.	SIB2_W01;SIB2_W02; SIB2_W03;SIB2_W04; SIB2_U01; SIB2_U02; SIB2_U03; SIB2_K01; SIB2_K02; SIB2_K03; SIB2_K04; SIB2_K05;	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK, P7S_KO, P7S_KR
W12	Pko_W01; Pko_W02; Pko_U02; Pko_U03; Pko_K01; Pko_K02; Pko_K03.	SIB2_W01;SIB2_W02; SIB2_W03;SIB2_W04; SIB2_U01; SIB2_U02; SIB2_U03; SIB2_K01; SIB2_K02; SIB2_K03; SIB2_K04; SIB2_K05;	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK, P7S_KO, P7S_KR
W13	Pko_W01; Pko_W02; Pko_W03; Pko_U02; Pko_U03; Pko_K01; Pko_K02; Pko_K03.	SIB2_W01;SIB2_W02; SIB2_W03;SIB2_W04; SIB2_U01; SIB2_U02; SIB2_U03; SIB2_K01; SIB2_K02; SIB2_K03; SIB2_K04; SIB2_K05;	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK, P7S_KO, P7S_KR

V. NAKŁAD PRACY STUDENTA

Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin Nie kontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**16**	**X**	**75**	**3**
Ćwiczenia				
Seminarium				
Konwersatoria				
Konsultacje (zaliczenie nieobecności, rozliczenie rygorów, poprawy)	**5**			
Praca projektowa	**X**			
Opanowanie informacji		**25**		
Przygotowanie do rozliczenia		**27**		
RAZEM	**21**	**54**		

VI. METODY I NARZĘDZIA DYDAKTYCZNE

- wykład;
- prezentacja multimedialna;
- case study;
- dyskusja.

VII. FORMA ZALICZENIA PRZEDMIOTU

Rygor	***Kryteria składowe***	***Waga***
Zaliczenie	Ocena z kolokwium - warunek konieczny	0,7
	Zaliczenie pracy projektowej - warunek istotny	0,2
	Obserwacja - warunek istotny	0,1

VIII. LITERATURA

OBOWIĄZKOWA

1. R. W. Gryffin, Podstawy zarządzania organizacjami, PWN, Warszawa, 2004.
2. A. J. Blikle, Doktryna jakości. Rzecz o skutecznym zarządzaniu, Helion, Warszawa, 2013.
3. A. J. Blikle, Doktryna jakości. Rzecz o turkusowej samoorganizacji, Helion, Warszawa, 2018.

UZUPEŁNIAJĄCA

1. M. Ćwiklicki, Hubert Obora, *Metody TQM w zarządzaniu firmą, praktyczne przykłady zastosowań*, Poltext, Warszawa, 2009.

2.	J. Stoner, E. Freeman, D. Gilbert, *Kierowanie*, PWE, Warszawa, 2014.
3.	Cz. Flanek, *Elementy teorii podejmowania decyzji*, CSOPK, Koszalin, 2000.
4.	A. Koźmiński, W. Piotrowski, *Zarządzanie, teoria i praktyka*, PWN, Warszawa, 1990
IX.	**PROWADZĄCY PRZEDMIOT**
Stopień, Imię i nazwisko	dr Jerzy KUPIŃSKI
adres email	j.kupinski@amw.gdynia.pl

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:	**Podstawy filozofii i logiki****	*Kod*:	**Itn**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Niestacjonarne		
Kształcenie w zakresie:	Cyberbezpieczeństwo, Analiza danych i informatyka śledcza		
Profil:	Ogólnoakademicki		
Liczba ECTS:	3		
Semestr:	3		
Wymagania wstępne:	Brak		
Język wykładowy:	Polski		
Cel przedmiotu:	**C01**	Zaznajomienie z podstawowymi pojęciami z zakresu filozofii oraz logiki.	
	C02	Przedstawienie głównych problemów filozoficznych oraz sposobów ich rozstrzygania.	
	C03	Charakterystyka języka naturalnego oraz głównych rodzajów i reguł rozumowania; ich wykorzystanie w nauce, w procesie komunikacji oraz w konstruowaniu własnej wizji świata.	
	C04	Wyjaśnienie najważniejszych praw logicznych oraz zasad budowania poprawnych definicji.	

II.	**EFEKTY UCZENIA SIĘ**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Itn_W01**	Student wyjaśnia najważniejsze pojęcia i zagadnienia z dziedziny filozofii oraz logiki; przedstawia rolę i znaczenie tych dyscyplin w procesie poznania i opisu rzeczywistości; wskazuje ich powiązania z innymi dziedzinami.	kolokwium
	Itn_W02	Student charakteryzuje różne koncepcje prawdy, rolę języka w procesie myślenia, sposoby definiowania pojęć, rodzaje rozumowań oraz podstawowe prawa logiczne; dostrzega ich przydatność w procesie badawczym.	kolokwium
Umiejętności:	**Itn_U01**	Student odwołuje się do ustaleń epistemologii oraz zaleceń logiki dla zapewnienia skutecznego myślenia i komunikowania się; unika błędów logicznych w rozumowaniach.	kolokwium
	Itn_U02	Student analizuje poprawność pojęć, sądów i wnioskowań oraz ocenia prawdziwość zdań na podstawie ich struktury logicznej.	kolokwium
Kompetencje społeczne:	**Itn_K01**	Student wykazuje samodzielność i niezależność w postrzeganiu rzeczywistości oraz krytycyzm w interpretowaniu odbieranych treści.	obserwacja na zajęciach

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
W01	Zajęcia wprowadzające. Specyfika myślenia filozoficznego.	1

W02	Przedmiot, struktura i dziedziny filozofii oraz jej relacje do nauki i religii.	1
W03	Najważniejsze zagadnienia i kierunki filozoficzne.	1
W04	Główne etapy rozwoju myśli filozoficznej.	2
W05	Koncepcje poznania oraz prawdziwości wiedzy w ujęciu wybranych nurtów filozoficznych.	1
W06	Przedmiot, działy oraz funkcje logiki; logika jako dziedzina filozofii.	1
W07	Język jako narzędzie myślenia; jego rola w procesie poznawania i opisu rzeczywistości oraz w komunikacji międzyludzkiej.	1
W08	Semantyczna teoria definicji. Błędy definicji sprawozdawczych.	1
W09	Podstawowe rodzaje rozumowań – dedukcja, redukcja, indukcja.	2
W10	Błędy w rozumowaniach – błąd formalny i błąd materialny.	1
W11	Założenia klasycznego rachunku zdań.	1
W12	Wybrane prawa logiczne. Sprawdzanie niezawodności rozumowań.	2
W13	Przyczyny nieporozumień o charakterze logicznym.	1

IV.	**KORELACJA EFEKTÓW UCZENIA SIĘ**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyki PRK*
W01	Itn_W01	SIB2_W01	P7U_W P7S_WG
W02	Itn_W01	SIB2_W01	P7U_W P7S_WG
W03	Itn_W01	SIB2_W01	P7U_W P7S_WG
W04	Itn_W01	SIB2_W01	P7U_W P7S_WG
W05	Itn_W01; Itn_K01	SIB2_W01; SIB2_K01	P7U_W P7S_WG; P7U_K P7S_KK
W06	Itn_W01	SIB2_W01	P7U_W P7S_WG
W07	Itn_W02; Itn_K01	SIB2_W01; SIB2_K01	P7U_W P7S_WG; P7U_K P7S_KK
W08	Itn_W02	SIB2_W01	P7U_W P7S_WG
W09	Itn_W02; Itn_U02	SIB2_W01; SIB2_U02	P7U_W P7S_WG; P7U_U P7S_UW
W10	Itn_U01	SIB2_U01	P7U_U P7S_UW
W11	Itn_U02	SIB2_U01	P7U_U P7S_UW
W12	Itn_W02; Itn_U02	SIB2_W01; SIB2_U01	P7U_W P7S_WG; P7U_U P7S_UW
W13	Itn_U01	SIB2_U01	P7U_U P7S_UW

V.	**NAKŁAD PRACY STUDENTA**			
Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**16**	**X**	**75**	**3**
Ćwiczenia				
Seminaria				
Konwersatoria				
Konsultacje (zaliczenie nieobecności, rozliczenie rygorów, poprawy)	**5**			
Przygotowanie do ćwiczeń	**X**			
Opanowanie informacji		**27**		
Przygotowanie do rozliczenia rygorów		**27**		
RAZEM	**21**	**54**		

VI.	**METODY DYDAKTYCZNE**
1.	Wykład: prezentacje multimedialne
2.	Konsultacje, sprawdzanie wiedzy i umiejętności: testy, zadania

VII.	**FORMA ZALICZENIA PRZEDMIOTU**

Rygor	*Kryteria składowe*	*Waga*
Zaliczenie	Ocena z kolokwium	0,8
	Obowiązkowa obecność na wykładach – 80%	0,2

VIII.	**LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA**
	OBOWIĄZKOWA
1.	Hempoliński M., *Filozofia współczesna. Wprowadzenie do zagadnień i kierunków*, Warszawa 1989.
2.	Popkin R.H., *Historia filozofii zachodniej*, Poznań 2003.
3.	Przybyłowski J., *Logika z ogólną metodologią nauk*, Gdańsk 1999.
4.	Ziembiński Z., *Logika praktyczna*, Warszawa 2007.
	UZUPEŁNIAJĄCA
1.	Bocheński J.M., *Zarys historii filozofii*, Kraków 1993.
2.	Hołówka T., *Kultura logiczna w przykładach*, Warszawa 2005.
3.	Kraszewski Z., *Logika. Nauka rozumowania*, Warszawa 1981.
4.	Tatarkiewicz W., *Historia filozofii, t. 1-3*, Warszawa 1990.

IX.	**PROWADZĄCY PRZEDMIOT**
Stopień, Imię i nazwisko	dr Wincenty KARAWAJCZYK
adres e-mail	w.karawajczyk@amw.gdynia.pl

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:	**Podstawy pedagogiki**	*Kod*:	**Ped**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Niestacjonarne		
Kształcenie w zakresie:	Cyberbezpieczeństwo, Analiza danych i informatyka śledcza		
Profil:	Ogólnoakademicki		
Liczba ECTS:	3		
Semestr:	3		
Wymagania wstępne:	Brak		
Język wykładowy:	Polski		
Cel przedmiotu:	**C01**	Zapoznanie studentów z podstawowymi kategoriami pedagogicznymi i procesami edukacyjnymi	
	C02	Ukazanie sposobów współczesnych rozwiązań praktycznych w zakresie kształcenia, opieki i wychowania oraz ich historycznych korzeni	
	C03	Wyposażenie w umiejętności i kompetencje niezbędne w procesie kształtowania własnej drogi edukacyjnej	

II.	**EFEKTY UCZENIA SIĘ**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Ped_W01**	Zna podstawowe pojęcia, kategorie i wybrane koncepcje pedagogiczne	Kolokwium
	Ped_W02	Rozumie historyczne,-społeczne i polityczne uwarunkowania rozwoju praktyki pedagogicznej	Kolokwium
	Ped_W03	Zna współczesne rozwiązania w zakresie kształcenia, uczenia się, opieki i wychowania	Kolokwium
Umiejętności:	**Ped_U01**	Potrafi interpretować podstawową wiedzę z zakresu pedagogiki/edukacji w kontekście własnego uczenia się i rozwoju	Kolokwium, bieżąca ocena aktywności
	Ped_U02	Analizuje i ocenia praktyczne skutki współczesnych idei i koncepcji pedagogicznych	Kolokwium, bieżąca ocena aktywności
Kompetencje społeczne:	**Ped_K01**	Jest gotów do brania odpowiedzialności za własne uczenie się i podejmowanie różnych form praktycznej działalności edukacyjnej, opiekuńczej i wychowawczej wobec innych	Kolokwium, bieżąca ocena aktywności

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
W01	Zajęcia wprowadzające. Podstawowe pojęcia pedagogiczne.	1
W02	Wybrane koncepcje pedagogiczne.	1
W03	Etymologia pedagogiki. Pedagogika jako nauka o wychowaniu	2
W04	Szkoła i rodzina jako podstawowe środowiska wychowania i kształcenia	2

W05	Filozoficzne, społeczno-historyczne uwarunkowania współczesnych rozwiązań pedagogicznych	2
W06	Systemy edukacyjne wybranych państw świata	2
W07	Uczelnia wyższa jako środowisko uczenia się dawniej i dziś	2
W08	Najważniejsze wyzwania współczesnej teorii i praktyki pedagogicznej	2
W09	Zajęcia podsumowujące. Kolokwium	2

IV.	**KORELACJA EFEKTÓW UCZENIA SIĘ**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod efektu PRK*
W01	Ped_W01, Ped_W03	SIB2_W01, SIB2_K02	P7U_W P7S_WG, P7U_K P7S_KK
W02	Ped_W01, Ped_W03, Ped_U02	SIB2_W01, SIB2_K02	P7U_W P7S_WG P7U_K P7S_KK
W03	Ped_W02, Ped_W03	SIB2_W01, SIB2_K02	P7U_W P7S_WG P7U_K P7S_KK
W04	Ped_W02, Ped_W03, Ped_U01, Ped_U02, Ped_K01	SIB2_W01, SIB2_U03, SIB2_U06, SIB2_K02, SIB2_K03, SIB2_K04	P7U_W P7S_WG P7U_U P7S_UK P7U_U P7S_UO P7U_K P7S_KK P7U_K P7S_KO P7U_K P7S_KR
W05	Ped_W01, Ped_W02, Ped_W03, Ped_U01, Ped_U02, Ped_K01	SIB2_W01, SIB2_U01, SIB2_U06, SIB2_U07, SIB2_K02	P7U_W P7S_WG P7U_U P7S_UW P7U_U P7U_UO P7U_U P7U_UU P7U_K P7S_KK
W06	Ped_W03, Ped_U01, Ped_U02	SIB2_W01, SIB2_U01, SIB2_U02	P7U_W P7S_WG P7U_U P7S_UW
W07	Ped_W01, Ped_W02, Ped_W03, Ped_U01, Ped_U02, Ped_K01	SIB2_W01, SIB2_U01 SIB2_U07, SIB2_K02	P7U_W P7S_WG P7U_U P7S_UW P7U_U P7U_UU P7U_K P7S_KK
W08	Ped_W02, Ped_U01, Ped_U02, Ped_K01	SIB2_W01, SIB2_U07, SIB2_K02	P7U_W P7S_WG P7U_U P7S_UU P7U_K P7S_KK
W09	Ped_W01, Ped_W02, Ped_W03, Ped_U01, Ped_U02, Ped_K01	SIB2_W01, SIB2_U01, SIB2_U07, SIB2_K02	P7U_W P7S_WG P7U_U P7U_UW P7U_U P7S_UU P7U_K P7S_KK

V.	**NAKŁAD PRACY STUDENTA**			
Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**16**	**X**	**75**	**3**
Ćwiczenia				
Seminaria				
Konwersatoria				
Konsultacje (zaliczenie nieobecności, rozliczenie rygorów, poprawy)	**5**			
Przygotowanie do ćwiczeń	**X**			
Opanowanie informacji		**27**		
Przygotowanie do rozliczenia rygorów		**27**		
RAZEM	**21**	**54**		

VI.	METODY DYDAKTYCZNE	
1.	Wykład konwersatoryjny	
2.	Wykład z wykorzystaniem multimediów	
3.	Analiza tekstów źródłowych	
VII.	**FORMA ZALICZENIA PRZEDMIOTU**	
Rygor	*Kryteria składowe*	*Waga*
Zaliczenie	Kolokwium	0.75
	Obecność i aktywny udział w dyskusjach	0.25
VIII.	**LIFIERATURA PODSTAWOWA I UZUPEŁNIAJĄCA**	
	OBOWIĄZKOWA	
1.	HEJNICKA-BEZWIŃSKA T.: Pedagogika ogólna. Pedagogika wobec współczesności. Warszawa 2008.	
2.	KWIECIŃSKI Z., ŚLIWERSKI B. (red.): Pedagogika. Podręcznik akademicki. Warszawa 2019.	
3.	BARTNICKA K., SZYBIAK I.: Zarys historii wychowania. Warszawa 2001.	
	UZUPEŁNIAJĄCA	
1.	PRůCHA J.: Pedagogika porównawcza. Podręcznik akademicki. Warszawa 2006.	
2.	GUTEK G.L.: Filozoficzne i ideologiczne podstawy edukacji. Gdańsk 2003.	
3.	Wybrane artykuły z czasopism: „Colloquium”, „Problemy Opiekuńczo-Wychowawcze”, „Rocznik Andragogiczny”.	
IX.	**PROWADZĄCY PRZEDMIOT**	
Stopień, Imię i nazwisko	dr hab. Elżbieta GAWEŁ-LUTY, prof. AMW	
adres e-mail	e.luty@amw.gdynia.pl	

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:	**Historia techniki**	*Kod*:	**Hta**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Niestacjonarne		
Kształcenie w zakresie:	Cyberbezpieczeństwo, Analiza danych i informatyka śledcza		
Profil:	Ogólnoakademicki		
Liczba ECTS:	3		
Semestr:	3		
Wymagania wstępne:	Umiejętność obserwowania i interpretacji zjawisk historycznych, kulturowych i społecznych, odpowiedzialne przygotowanie się do swojej pracy		
Język wykładowy:	Polski		
Cel przedmiotu:	**C01**	Wyposażenie studentów w wiedzę dotyczącą funkcjonowania instytucji zajmujących się techniką i jej historią	
	C02	Nabycie umiejętności analizowania i projektowania działań praktycznych w powiązaniu z historią techniki	
	C03	Zapoznanie studentów z wiedzą niezbędną do rozumienia społecznych uwarunkowań działalności człowieka	

II.	**EFEKTY UCZENIA SIĘ**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Hta_W01**	Student ma niezbędną wiedzę do rozumienia pozatechnicznych, kulturowo-społecznych uwarunkowań działalności człowieka	Kolokwium
Umiejętności:	**Hta_U01**	Student potrafi pozyskiwać i integrować informacje pozyskane z literatury przedmiotu, baz danych oraz innych źródeł, potrafi dokonywać ich interpretacji i właściwej oceny w celu określenia ich znaczeń oddziaływania społecznego i miejsca w procesie historyczno-kulturowym	Kolokwium/ Odpowiedź ustna
Kompetencje społeczne:	**Hta_K01**	Student ma świadomość ważności i rozumie pozatechniczne aspekty i skutki działalności człowieka, w tym wpływu jej na środowisko społeczno-kulturowe i związanej z tym odpowiedzialności za podejmowane decyzje	Odpowiedź ustna

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
W01	Wprowadzenie. Ogólna historia techniki /od drewnianej do murowanej/	1
W02	Historia fortyfikacji i budownictwa obronnego	2
W03	Historia żeglugi światowej	2
W04	Historia techniki nawigacyjnej i nurkowej	2
W05	Historia żeglarstwa	2
W06	Polski udział w rozwoju techniki	1
W07	Technika w marynarce wojennej	2

W08	Rola polskich stoczni w rozwoju techniki morskiej	2
W09	Muzealnictwo morskie a historia techniki morskiej	1
W10	Kolokwium zaliczeniowe	1

IV.	**KORELACJA EFEKTÓW UCZENIA SIĘ**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyki PRK*
W01	Hta_W01	SIB2_W01	P7U_W P7S_WG
W02	Hta_W01, Hta_U01	SIB2_W01, SIB2_U01	P7U_W P7S_WG P7U_U P7S_UW
W03	Hta_W01, Hta_U01	SIB2_W01, SIB2_U01	P7U_W P7S_WG P7U_U P7S_UW
W04	Hta_W01, Hta_U01, Yo_K01	SIB2_W01, SIB2_U01, SIB2_K02	P7U_W P7S_WG P7U_U P7S_UW P7U_K P7S_KK
W05	Hta_W01, Hta_U01, Hta_K01	SIB2_W01, SIB2_U01, SIB2_K02	P7U_W P7S_WG P7U_U P7S_UW P7U_K P7S_KK
W06	Hta_W01, Hta_U01, Hta_K01	SIB2_W01, SIB2_U01, SIB2_K02	P7U_W P7S_WG P7U_U P7S_UW P7U_K P7S_KK
W07	Hta_W01, Hta_U01, Hta_K01	SIB2_W01, SIB2_U01, SIB2_K02	P7U_W P7S_WG P7U_U P7S_UW P7U_K P7S_KK
W08	Hta_W01, Hta_U01, Yo_K01	SIB2_W01, SIB2_U01, SIB2_K02	P7U_W P7S_WG P7U_U P7S_UW P7U_K P7S_KK
W09	Hta_W01, Hta_U01, Yo_K01	SIB2_W01, SIB2_U01, SIB2_K02	P7U_W P7S_WG P7U_U P7S_UW P7U_K P7S_KK
W10	Hta_W01, Hta_U01, Hta_K01	SIB2_W01, SIB2_U01, SIB2_K02	P7U_W P7S_WG P7U_U P7S_UW P7U_K P7S_KK

V.	**NAKŁAD PRACY STUDENTA**			
Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**16**	**X**	**75**	**3**
Ćwiczenia				
Seminaria				
Konwersatoria				
Konsultacje (zaliczenie nieobecności, rozliczenie rygorów, poprawy)	**5**			
Przygotowanie do ćwiczeń	**X**			
Opanowanie informacji		**27**		
Przygotowanie do rozliczenia rygorów		**27**		
RAZEM	**21**	**54**		

VI.	**METODY DYDAKTYCZNE**
1.	Wykład problemowy
2.	Wykład informacyjny
3.	Wykład z prezentacją multimedialną

VII.	**FORMA ZALICZENIA PRZEDMIOTU**	
Rygor	*Kryteria składowe*	*Waga*
Zaliczenie	Ocena z kolokwium zaliczeniowego	1,0

VIII.	**LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA**
OBOWIĄZKOWA	

1.	A. Komorowski, *Historia techniki nawigacyjnej,* AMW Gdynia 1999.
2.	A. Komorowski, *Historia techniki nurkowej,* Torun 2005.
UZUPEŁNIAJĄCA	
1.	B. Orłowski, *Historia techniki polskiej,* Radom 2008.

IX.	**PROWADZĄCY PRZEDMIOT**
Stopień, Imię i nazwisko	dr Mariusz KARDAS
adres e-mail	m.kardas@amw.gdynia.pl

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:	**Ochrona ludności i obrona cywilna**	*Kod*:	**Fc**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Niestacjonarne		
Kształcenie w zakresie:	Cyberbezpieczeństwo, Analiza danych i informatyka śledcza		
Profil:	Ogólnoakademicki		
Liczba ECTS:	4		
Semestr:	3		
Wymagania wstępne:	brak		
Język wykładowy:	Polski		
Cel przedmiotu:	**C01**	Zapoznanie z uwarunkowaniami prawnymi w zakresie ochrony ludności i Obrony Cywilnej w Polsce	
	C02	Zapoznanie z krajowymi systemami ochrony ludności	
	C03	Zapoznanie z podstawowymi zasadami funkcjonowania obrony cywilnej w czasie konfliktów zbrojnych	
	C04	Ukształtowanie prawidłowych reakcji w przypadku wystąpienia zagrożenia	

II.	**EFEKTY UCZENIA SIĘ**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Fc_W01**	Zna i interpretuje przepisy prawa regulujące funkcjonowanie obrony cywilnej w Polsce	Kolokwium
	Fc_W02	Wyjaśnia szczegółowo miejsce, znaczenie i rolę obrony cywilnej	Test sprawdzający podczas zajęć, krótka praca domowa
	Fc_W03	Szczegółowo zna zadania obrony cywilnej w zakresie przeciwdziałania stanom zagrożenia zdrowia i życia.	Praca pisemna podczas zajęć
Umiejętności:	**Fc_U01**	Posiada umiejętność rozumienia i analizowania różnorodnych zjawisk, mających wpływ na bezpieczeństwo obywateli	Kolokwium
	Fc_U02	Dostrzega problemy z obrony cywilnej oraz składa propozycje ich rozstrzygnięć oraz stosuje argumentację własnego stanowiska	Praca pisemna podczas zajęć
	Fc_U03	Interpretuje i prognozuje rozwój zjawisk społecznych, ekonomicznych, politycznych, prawnych i kulturowych wywołanych konfliktem zbrojnym	Kolokwium
Kompetencje społeczne:	**Fc_K01**	Priorytetyzuje zadnia określone przez siebie lub innych oraz posługuje się harmonogramem ich uporządkowanej realizacji	Wykonanie projektu
	Fc_K02	Inicjuje i moderuje pracę w grupie, przyjmując w niej różne role, potrafi podporządkować się	Odpowiedź tablicowa

		celom grupy, ale także przyjmować funkcje lidera zadaniowego	
	Fc_K03	Samodzielnie uzupełnia i doskonali nabytą wiedzę i umiejętności, potrafi ocenić ofertę kształcenia kursowego i podyplomowego	Krótka praca domowa

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
W01	Prawne uwarunkowania funkcjonowania obrony cywilnej w Polsce	2
W02	Instytucje odpowiedzialne za obronę cywilną w Polsce	2
W03	Charakterystyka zadań obrony cywilnej oraz zasady ich realizacji w czasie pokoju i podczas wojny	4
W04	Organizacja powszechnego systemu ochrony ludności	3
W05	Zasady ochrony ludności wynikające z zagrożeń czasu wojny, krajowy system wykrywania skażeń i alarmowania	3
C01	Zadania i kompetencje organów administracji publicznej oraz służb, inspekcji i straży w zakresie ochrony ludności i obrony cywilnej	2
C02	Prawa i obowiązki obywateli w zakresie obrony cywilnej i ochrony ludności, świadczenia na rzecz obrony	4
C03	Organizacja i prowadzenie akcji ratunkowej, udzielanie pomocy medycznej poszkodowanym, ewakuacja	4
C04	Pomoc w ratowaniu żywności i innych dóbr niezbędnych do przetrwania	2
C05	Zasady reagowania na sygnały alarmowe, ochrona przed zagrożeniami	4

IV.	**KORELACJA EFEKTÓW UCZENIA SIĘ**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyki PRK*
W01	Fc_W01, Fc_U04	SIB2_W03, SIB2_U07	P7U_W, P7S _WK, P7U_U; P7S_UU
W02	Fc_W02	SIB2_W02	P7U_W; P7S_WK
W03	Fc_W01, Fc_W03	SIB2_W02, SIB2_W03	P7U_W, P7S _WK,
W04	Fc_W01, Fc_W02, Fc_W03	SIB2_W02, SIB2_W03	P7U_W, P7S _WK,
W05	Fc_W03, Fc_U06	SIB2_W03, SIB2_U01	P7U_W; P7S_WK, P7U_U; P7S_UW
C01	Fc_W01, Fc_W02, Fc_K09	SIB2_W03, SIB2_W01, SIB2_K03	P7U_W, P7S _WK, P7U_W, P7S _WG; P7U_K; P7S_KO
C02	Fc_W01, Fc_W02,Fc_K08	SIB2_W03, SIB2_U07	P7U_W; P7S_WK, P7U_U; P7S_UU
C03	Fc_W03, Fc_W05, Fc_U07	SIB2_W02, SIB2_U07	P7U_W; P7S_WK, P7U_U; P7S_UU
C04	Fc_W03, Fc_U05,Fc_U06	SIB2_W03, SIB2_U07	P7U_W; P7S_WK, P7U_U; P7S_UU
C05	Fc_W03, Fc_K07	SIB2_W02, SIB2_U07	P7U_W; P7S_WK, P7U_U; P7S_UU

V.	**NAKŁAD PRACY STUDENTA**			
Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**10**	**X**	**106**	**4**
Ćwiczenia	**15**			
Seminaria				
Konwersatoria				
Konsultacje (zaliczenie nieobecności, rozliczenie rygorów, poprawy)	**6**			

Przygotowanie do ćwiczeń	X	**20**		
Opanowanie informacji		**30**		
Przygotowanie do rozliczenia rygorów		**25**		
RAZEM	**31**	**75**		

VI.	**METODY DYDAKTYCZNE**
1.	Wykład z prezentacją multimedialną
2.	Ćwiczenia audytoryjne: projekt praktyczny
3.	Ćwiczenia audytoryjne: praca w grupach

VII.	**FORMA ZALICZENIA PRZEDMIOTU**	
Rygor	*Kryteria składowe*	*Waga*
Zaliczenie	Kolokwium	50%
	Wykonanie projektów	35%
	Oceny z krótkich prac pisemnych	10%
	Ocena z krótkich prac domowych	5%
Egzamin	Zaliczenie testu	100%

VIII.	**LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA**
	OBOWIĄZKOWA
1.	R. Jakubczak, A. Skrabacz, K. Gąsiorek (red.), *Obrona Narodowa w tworzeniu bezpieczeństwa Polski w XXI wieku*, Warszawa 2008
2.	K. Przeworski, *Ewakuacja jako sposób ochrony ludności*, Warszawa 2002
3.	*Rozporządzenie Rady Ministrów z dnia 25 czerwca 2002 r. w sprawie szczegółowego zakresu działania Szefa Obrony Cywilnej Kraju, szefów obrony cywilnej województw, powiatów i gmin*. (Dz. U. z dnia 1 lipca 2002 r. z późniejszymi zmianami)
4.	W. Kitler, A. Skrabacz, *Bezpieczeństwo ludności cywilnej. Pojęcie, organizacja i zadania w czasie pokoju, kryzysu i wojny*, Warszawa 2010
	UZUPEŁNIAJĄCA
1.	M. Fleming, *Międzynarodowe prawo humanitarne konfliktów zbrojnych*. Zbiór dokumentów, (M. Gąska, E. Mikos – Skuza uzupełnienie i redakcja), Warszawa 2003
2.	W. Kitler (red.), *Obrona Cywilna (niemilitarna) w obronie narodowej III RP*, Warszawa 2001
3.	W. Skomra, *Zarządzanie kryzysowe – praktyczny przewodnik po nowelizacji ustawy*, Wrocław 2010
4.	G. Abgarowicz, *Kierowanie obroną cywilną*, (w:) Zdrodowski B., Wiśniewski B., red., Kierowanie Bezpieczeństwem Narodowym, Warszawa 2008
5.	R. Kalinowski, *Obrona cywilna w Polsce*. Siedlce 2009
6.	W. Kitler, A. Skrabacz, *Bezpieczeństwo ludności cywilnej. Pojęcie, organizacja i zadania w czasie pokoju, kryzysu i wojny*, Warszawa 2010

IX.	**PROWADZĄCY PRZEDMIOT**
Stopień, Imię i nazwisko	dr hab. Jarosław MICHALAK, prof. AMW; mgr Krzysztof BLUMKA
adres e-mail	j.michalak@amw.gdynia.pl, k.blumka@amw.gdynia.pl

3.7. Karty przedmiotów modułu zajęć kierunkowych studiów niestacjonarnych– B

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 Systemami Bezpieczeństwa Wewnętrznego**	*Kod*:	**Zog**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Niestacjonarne		
Kształcenie w zakresie:	Cyberbezpieczeństwo, Analiza danych i informatyka śledcza		
Profil:	Ogólnoakademicki		
Liczba ECTS:	5		
Semestr:	1		
Wymagania wstępne:	Umiejętność pracy samodzielnej oraz w grupie.		
	Umiejętności zdobywania, pogłębiania i wykorzystania wiedzy w procesie studiowania.		
	Umiejętności komunikacji interpersonalnej.		
Język wykładowy:	Polski		
Cel przedmiotu: **C01**	Przekazanie wiedzy z zakresu zarządzania systemami bezpieczeństwa wewnętrznego państwa w kontekście ideologicznym, kulturowym, socjologicznym i psychologicznym.		
Cel przedmiotu: **C02**	Wyrobienie umiejętności identyfikowania, analizy i prognozowania zagrożeń dla systemu bezpieczeństwa wewnętrznego państwa.		
Cel przedmiotu: **C03**	Wyrobienie u studentów unikalnej umiejętności całościowego spojrzenia na procesy organizacyjne, mechanizmy nimi rządzące oraz wzajemne powiązania w czasie zarządzania systemami bezpieczeństwa wewnętrznego.		
Cel przedmiotu: **C04**	Przygotowanie studentów do zastosowania zdobytej wiedzy z zakresu zarządzania systemami bezpieczeństwa wewnętrznego państwa w czasie wykonywania zadań służbowych.		

II.	**EFEKTY KSZTAŁCENIA**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Zog_01**	Zna instrumentarium pojęciowe z zakresu zarządzania systemami bezpieczeństwa wewnętrznego.	Kolokwium
Wiedza:	**Zog_02**	Zna zasady i mechanizmy działania elementów systemu bezpieczeństwa wewnętrznego państwa. Posiada rozszerzoną wiedzę z zakresu zarządzania systemami bezpieczeństwa wewnętrznego. Zna i interpretuje relacje występujące w systemie bezpieczeństwa wewnętrznego państwa oraz ich związek z bezpieczeństwem narodowym.	Test sprawdzający podczas zajęć, krótka praca domowa
Wiedza:	**Zog_03**	Posiada wiedzę na temat realizacji procesu oraz metod wykorzystywanych podczas szacowania ryzyka, identyfikacji zagrożeń, określania podatności i wymagań dotyczących systemu bezpieczeństwa wewnętrznego państwa.	Praca pisemna podczas zajęć

	Zog_04	Posiada wiedzę o podstawowych koncepcjach i metodach funkcjonowania gminnych, powiatowych i wojewódzkich systemów bezpieczeństwa oraz zarządzania tymi strukturami a także stosowaniu podstawowych metod i technik zarządzania gminnych, powiatowych i wojewódzkich systemów bezpieczeństwa, w tym będącymi w sytuacjach kryzysowych.	Test sprawdzający podczas zajęć, krótka praca domowa
Umiejętności:	**Zog_05**	Potrafi identyfikować zagrożenia dla bezpieczeństwa wewnętrznego państwa wynikające z podatności systemu bezpieczeństwa wewnętrznego państwa.	Kolokwium
	Zog_06	Posiada umiejętność identyfikowania, analizowania i proponowania rozwiązań problemów związanych z zarządzaniem systemami bezpieczeństwa wewnętrznego państwa.	Praca pisemna podczas zajęć
	Zog_07	Potrafi wykorzystać zdobytą wiedzę do analizowania i interpretowania zjawisk politycznych; samodzielnej oceny sytuacji i szacowania ryzyka.	Kolokwium
	Zog_08	Ma wyrobioną unikalną umiejętność całościowego spojrzenia na złożoność systemu bezpieczeństwa wewnętrznego państwa, wzajemne powiązania między jego podsystemami oraz ich elementami.	Wykonanie projektu
Kompetencje społeczne:	**Zog_09**	Potrafi dokonać prawidłowej analizy bezpieczeństwa wewnętrznego państwa. Docenia konieczność prowadzenia audytów bezpieczeństwa oraz dyskutuje o różnych sposobach ich realizacji.	Wykonanie projektu
	Zog_10	Rozróżnia i diagnozuje współczesne zagrożenia dla bezpieczeństwa a mające wpływ na funkcjonowanie systemu bezpieczeństwa wewnętrznego państwa w różnych środowiskach społecznych oraz potrafi sprostać otrzymanym zadaniom wynikającym z pełnionych w nim ról.	Odpowiedź tablicowa
	Zog_11	Formułuje nowe wyzwania zawodowe a jednocześnie odznacza się odpowiedzialnością za podejmowane decyzje i prowadzone działania oraz ich skutki wyrażając swoją postawę w środowisku specjalistów i pośrednio modelując to podejście wśród innych.	Krótka praca domowa

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
W01	Zajęcia organizacyjne. Wprowadzenie do problematyki zajęć (zakres, terminologia, akty prawne i normatywne). Organizacja systemu bezpieczeństwa wewnętrznego państwa.	1
W02	Podmiotowy i przedmiotowy zakres systemu bezpieczeństwa wewnętrznego.	1

W03	Państwo jako podmiot bezpieczeństwa: koncepcje bezpieczeństwa państwa, funkcje ochronne państwa, typologia bezpieczeństwa wewnętrznego.	2
W04	Człowiek jako podmiot bezpieczeństwa: postrzeganie zagrożeń, społeczne poczucie bezpieczeństwa.	1
W05	Doktrynalne i instytucjonalne przesłanki bezpieczeństwa.	1
W06	Ideologiczne, religijne i narodowościowe czynniki zagrożeń bezpieczeństwa wewnętrznego państwa.	1
W07	Zarządzanie systemowe bezpieczeństwem wewnętrznym państwa.	1
W08	Zarządzanie strategiczne bezpieczeństwem wewnętrznym państwa.	1
W09	Przestępczość zorganizowana.	1
W10	Bezpieczeństwo sektorowe państwa.	1
W11	Szacowanie ryzyka.	1
W12	Rola sił zbrojnych w bezpieczeństwie wewnętrznym państwa.	1
W13	Obiekty ataków terrorystycznych.	1
W14	Cyberbezpieczeństwo państwa.	1
C01	Charakterystyka zagrożeń dla bezpieczeństwa wewnętrznego państwa.	1
C02	Czynniki zagrożeń bezpieczeństwa wewnętrznego państwa.	1
C03	Systemy zarządzania bezpieczeństwem gminy, powiatu, województwa.	2
C04	Komplementarność narodu i państwa a problem bezpieczeństwa.	2
C05	Współczesne uwarunkowania interwencji militarnych w kontekście bezpieczeństwa wewnętrznego państwa.	2
C06	Przywództwo i kierowanie w tworzeniu bezpieczeństwa.	2
C07	Analiza systemowa bezpieczeństwa.	2
C08	Podsystem wykonawczy systemu bezpieczeństwa wewnętrznego RP. Policja.	1
C09	Podsystem wykonawczy systemu bezpieczeństwa wewnętrznego RP. Straż Graniczna.	1
C10	Podsystem wykonawczy systemu bezpieczeństwa wewnętrznego RP. Państwowa Straż Pożarna.	1
C11	Wpływ geopolitycznego położenia Polski na jej bezpieczeństwo wewnętrzne.	1
C12	Perspektywy ewolucji systemu bezpieczeństwa wewnętrznego Polski.	1
C13	Egzamin	1

IV.	**KORELACJA EFEKTÓW KSZTAŁCENIA**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod efektu obszarowego*
W01	Zog_01, Zog_02, Zog_03	SIB2_W01, SIB2_W03, SIB2_W04	P7U_W, P7S_WG, P7S_WK
W02	Zog_01, Zog_02	SIB2_W01, SIB2_W03, SIB2_W04	P7U_W, P7S_WG, P7S_WK
W03	Zog_01, Zog_02	SIB2_W01, SIB2_W03, SIB2_W04	P7U_W, P7S_WG, P7S_WK
W04	Zog_02, Zog_06	SIB2_W01, SIB2_W03, SIB2_W04	P7U_W, P7S_WG, P7S_WK
W05	Zog_01, Zog_02. Zog_06	SIB2_W01, SIB2_W03, SIB2_W04	P7U_W, P7S_WG, P7S_WK
W06	Zog_02, Zog_03, Zog_05	SIB2_W01, SIB2_W03, SIB2_W04	P7U_W, P7S_WG, P7S_WK
W07	Zog_02, Zog_05, Zog_07	SIB2_W01, SIB2_W03, SIB2_W04	P7U_W, P7S_WG, P7S_WK
W08	Zog_02, Zog_05, Zog_07	SIB2_W01, SIB2_W03, SIB2_W04	P7U_W, P7S_WG, P7S_WK
W09	Zog_02, Zog_03	SIB2_W01, SIB2_W03, SIB2_W04	P7U_W, P7S_WG, P7S_WK

W10	Zog_04, Zog_06, Zog_07	SIB2_W01, SIB2_W03, SIB2_W04	P7U_W, P7S_WG, P7S_WK
W11	Zog_01, Zog_03, Zog_05, Zog_07	SIB2_W01, SIB2_W03, SIB2_W04	P7U_W, P7S_WG, P7S_WK
W12	Zog_01, Zog_04	SIB2_W01, SIB2_W03, SIB2_W04	P7U_W, P7S_WG, P7S_WK
W13	Zog_05, Zog_06, Zog_07	SIB2_W01, SIB2_W03, SIB2_W04	P7U_W, P7S_WG, P7S_WK
W14	Zog_01, Zog_02, Zog_03, Zog_07	SIB2_W01, SIB2_W03, SIB2_W04	P7U_W, P7S_WG, P7S_WK
C01	Zog_05, Zog_09	SIB2_U01, SIB2_U02, SIB2_U04, SIB2_U07, SIB2_K01, SIB2_K04	P7U_U, P7S_UW, P7U_K, P7S_KK, P7S_KR
C02	Zog_06, Zog_07	SIB2_U01, SIB2_U02, SIB2_U04, SIB2_U07, SIB2_K01, SIB2_K04	P7U_U, P7S_UW, P7U_K, P7S_KK, P7S_KR
C03	Zog_05, Zog_07	SIB2_U01, SIB2_U02, SIB2_U04, SIB2_U07, SIB2_K01, SIB2_K04	P7U_U, P7S_UW, P7U_K, P7S_KK, P7S_KR
C04	Zog_07, Zog_08	SIB2_U01, SIB2_U02, SIB2_U04, SIB2_U07, SIB2_K01, SIB2_K04	P7U_U, P7S_UW, P7U_K, P7S_KK, P7S_KR
C05	Zog_08, Zog_09, Zog_10	SIB2_U01, SIB2_U02, SIB2_U04, SIB2_U07, SIB2_K01, SIB2_K04	P7U_U, P7S_UW, P7U_K, P7S_KK, P7S_KR
C06	Zog_07, Zog_09, Zog_10	SIB2_U01, SIB2_U02, SIB2_U04, SIB2_U07, SIB2_K01, SIB2_K04	P7U_U, P7S_UW, P7U_K, P7S_KK, P7S_KR
C07	Zog_08, Zog_09, Zog_11	SIB2_U01, SIB2_U02, SIB2_U04, SIB2_U07, SIB2_K01, SIB2_K04	P7U_U, P7S_UW, P7U_K, P7S_KK, P7S_KR
C08	Zog_06, Zog_09, Zog_11	SIB2_U01, SIB2_U02, SIB2_U04, SIB2_U07, SIB2_K01, SIB2_K04	P7U_U, P7S_UW, P7U_K, P7S_KK, P7S_KR
C09	Zog_06, Zog_09, Zog_11	SIB2_U01, SIB2_U02, SIB2_U04, SIB2_U07, SIB2_K01, SIB2_K04	P7U_U, P7S_UW, P7U_K, P7S_KK, P7S_KR
C10	Zog_06, Zog_09, Zog_11	SIB2_U01, SIB2_U02, SIB2_U04, SIB2_U07, SIB2_K01, SIB2_K04	P7U_U, P7S_UW, P7U_K, P7S_KK, P7S_KR
C11	Zog_05, Zog_06, Zog_09, Zog_10	SIB2_U01, SIB2_U02, SIB2_U04, SIB2_U07, SIB2_K01, SIB2_K04	P7U_U, P7S_UW, P7U_K, P7S_KK, P7S_KR
C12	Zog_09, Zog_11	SIB2_U01, SIB2_U02, SIB2_U04, SIB2_U07, SIB2_K01, SIB2_K04	P7U_U, P7S_UW, P7U_K, P7S_KK, P7S_KR
C13	Zog_06, Zog_07, Zog_8	SIB2_U01, SIB2_U02, SIB2_U04, SIB2_U07, SIB2_K01, SIB2_K04	P7U_U, P7S_UW, P7U_K, P7S_KK, P7S_KR

V.	**NAKŁAD PRACY STUDENTA**			
Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**15**		**125**	**5**
Ćwiczenia	**20**			
Seminaria				
Konwersatoria				
Konsultacje	**5**			
Rozliczenie rygorów przedmiotu				
Przygotowanie do ćwiczeń		**40**		

Opanowanie informacji		**20**		
Przygotowanie do rozliczenia rygorów		**25**		
RAZEM	**40**	**85**		

VI.	**METODY DYDAKTYCZNE**
1.	Metody podające: wykład informacyjny w formie prezentacji multimedialnej, wykład problemowy.
2.	Wykład konwersatoryjny.
3.	Metody aktywizujące: pogadanka, obserwacja, praca z dokumentacją, praca w grupach, case study, praca multimedialna (prowadzący).
4.	Ćwiczenia audytoryjne: praca w grupach, projekt praktyczny, burza mózgów, analiza tekstów z wnioskowaniem.

VII.	**FORMA ZALICZENIA PRZEDMIOTU**	
Rygor	*Kryteria składowe*	*Waga*
Zaliczenie	Kolokwium	50%
	Wykonanie projektów	35%
	Oceny z krótkich prac pisemnych	10%
	Ocena z krótkich prac domowych	5%
Egzamin		

VIII.	**LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA**
	OBOWIĄZKOWA
1.	R. Jakubczak, *Bezpieczeństwo narodowe Polski w XXI wieku*, Bellona, Warszawa 2006
2.	R. Jakubczak, J. Flis (red.), *Bezpieczeństwo narodowe Polski w XXI wieku*, Warszawa 2006
3.	J. Stańczyk, *Współczesne pojmowanie bezpieczeństwa*, Warszawa 1996
4.	R. Zięba, *Pojęcie bezpieczeństwa wewnętrznego*, Warszawa 1981
5.	*Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2020*
6.	K. Ficoń, *Inżynieria zarządzania kryzysowego. Podejście systemowe*, Warszawa 2007
7.	S. Sulowski, M. Brzeziński (red.), *Bezpieczeństwo wewnętrzne państwa. Wybrane zagadnienia*, Warszawa 2009
	UZUPEŁNIAJĄCA
1.	T. Kiziukiewicz, *Audyt wewnętrzny w jednostkach sektora finansów publicznych*, INFOR 2007
2.	W. Stankiewicz, *Bezpieczeństwo narodowe a walki niezbrojne.* Studium, Warszawa 1991
3.	P. Bączek, *Zagrożenie informacyjne a bezpieczeństwo państwa polskiego*, Marszałek, Toruń 2005
4.	J. Czaja, *Kulturowe czynniki bezpieczeństwa*, KSW Kraków 2008
5.	B. Wiśniewski, S. Zalewski, *Bezpieczeństwo wewnętrzne RP w ujęciu systemowym*, WSA Bielsko-Biała 2006
6.	*Ustawa o krajowym systemie cyberbezpieczeństwa z 5 lipca 2018 r.*, 1 sierpnia podpisał ją Prezydent RP, a następnie została opublikowana w Dzienniku Ustaw RP 13 sierpnia br. (Dz. U. 2018 poz. 1560)
7.	*Ustawa z dnia 12 października 1990 r. o Straży Granicznej* (t.j. Dz.U. z 2014 r., poz. 1402 ze zm.)
8.	*Ustawa z dnia 6 kwietnia 1990 r. o Policji* (t.j. Dz.U. z 2015 r., poz. 355 ze zm.)
9.	*Ustawa z dnia 21 listopada 1967 r. o powszechnym obowiązku obrony Rzeczypospolitej Polskiej* (t.j. Dz.U. z 2015 r., poz. 827 ze zm.)
10.	*Słownik podstawowych terminów bezpieczeństwa państwa*, pr . zbiorowa, Warszawa 1994
11.	*Słownik terminów z zakresu bezpieczeństwa narodowego*, Warszawa 2009

IX.	**PROWADZĄCY PRZEDMIOT**
Stopień, Imię i nazwisko	dr inż. Robert Janczewski
adres e-mail	r.janczewskiski@amw.gdynia.pl

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:	**Inżynieria systemów i projektowanie procesów**	*Kod*:	**Ois**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Nietacjonarne		
Specjalność:	Cyberbezpieczeństwo, Analiza danych i informatyka śledcza		
Profil:	Ogólnoakademicki		
Liczba ECTS:	5		
Semestr:	1		
Wymagania wstępne:	Znajomość systemów bezpieczeństwa narodowego		
	Umiejętności zdobywania, pogłębiania i wykorzystania wiedzy w procesie studiowania.		
Język wykładowy:	Polski		
Cel przedmiotu:	**C01**	Przekazanie wiedzy z zakresu inżynieria systemów i projektowanie procesów	
	C02	Wykształcenie umiejętności identyfikacji struktury obiektu/przedmiotu projektowania systemów informacyjnych	
	C03	Wykształcenie umiejętności prowadzenia analizy systemowej oraz stosowania metod i narzędzi projektowania systemów informacyjnych wykorzystywanych w bezpieczeństwie	

II.	**EFEKTY KSZTAŁCENIA**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Ois_W01**	Student zna i rozumie podstawowe pojęcia z zakresu ogólnej teorii systemów i projektowania procesów	Kolokwium
	Ois_W02	Student zna i rozumie podstawowe pojęcia z zakresu analizy systemowej	Test
	Ois_W03	Ma pogłębioną wiedzę o budowie i funkcjonowaniu informacyjnych systemów bezpieczeństwa	Projekt
	Ois_W04	Zna metody służące do identyfikacji elementów otoczenia zewnętrznego i elementów wewnętrznych systemów informacyjnych	Projekt
Umiejętności:	**Ois_U01**	Potrafi zastosować właściwe metody analizy systemowej do opisu informacyjnych systemów bezpieczeństwa	Projekt
	Ois_U02	Potrafi projektować i modelować systemy i procesy informacyjne	Projekt
	Ois_U03	Potrafi ocenić przydatność znanych metod analizy systemowej oraz modelowania dla potrzeb budowy modeli informacyjnych systemów bezpieczeństwa	Projekt
	Ois_U04	Potrafi wykorzystywać specjalistyczne oprogramowania do modelowania	Projekt

		informacyjnych systemów bezpieczeństwa oraz procesów	
Kompetencje społeczne:	**Ois_K01**	Krytycznie ocenia posiadaną wiedzę i odbierane treści z zakresu inżynierii systemów i projektowania procesów	Obserwacja
	Ois_K02	Inicjuje i uczestniczy konstruktywnie w przygotowaniu projektów systemów informacyjnych	Projekt

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
W01	Wprowadzenie do ogólnej teorii systemów (koncepcje systemowe, podejście systemowe, analiza systemowa, system procesów)	1
W02	Identyfikacja elementów systemów informacyjnych(identyfikacja otoczenia systemu, identyfikacja elementów i relacji w systemie)	1
W03	System informacyjny jako obiekt projektowania (systemowe ujęcie bezpieczeństwa, orientacja funkcjonalna i procesowa w zarządzaniu bezpieczeństwem, klasyfikacja systemów bezpieczeństwa, struktura systemów bezpieczeństwa, wydarzenia, procesy, zasoby, relacje)	1
W04	Modelowanie systemów informacyjnych w bezpieczeństwie(diagramy kontekstowe, diagramy przepływu strumieni informacyjnych)	1
W05	Metody i narzędzia projektowania systemów informacyjnych (metody jakościowe, metody ilościowe, informatyczne wsparcie projektowania systemów informacyjnych)	1
W06	Model informacyjnego systemu bezpieczeństwa (zespołowa budowa modelu systemu informacyjnego z wykorzystaniem informatycznych narzędzi projektowych)	2
W07	Wprowadzenie do ogólnej teorii zarządzania procesami (proces, system procesów, zarządzanie procesami)	1
W08	Identyfikacja elementów procesów w informacyjnych systemach bezpieczeństwa (identyfikacja procesów, identyfikacja relacji między procesami)	1
W09	Proces w informacyjnych systemach bezpieczeństwa, jako obiekt projektowania (systemowe ujęcie bezpieczeństwa, orientacja funkcjonalna i procesowa w zarządzaniu bezpieczeństwem, klasyfikacja systemów bezpieczeństwa, wydarzenia, procesy, zasoby, relacje)	2
W10	Modelowanie procesów w informacyjnych systemach bezpieczeństwa (mapy procesów)	1
W11	Metody i narzędzia projektowania procesów w informacyjnych systemach bezpieczeństwa (schematy blokowe, metodyka EPC, standard BPMN)	1
W12	Model systemu procesów w informacyjnym systemie bezpieczeństwa (zespołowa budowa modelu systemu procesów w informacyjnym systemie bezpieczeństwa z wykorzystaniem informatycznych narzędzi projektowych)	2
C01	Model informacyjnego systemu bezpieczeństwa - identyfikacja otoczenia systemu	2
C02	Model informacyjnego systemu bezpieczeństwa - identyfikacja elementów systemu	2

C03	Model informacyjnego systemu bezpieczeństwa - identyfikacja relacji w systemie	2
C04	Model informacyjnego systemu bezpieczeństwa - diagramy przepływu strumieni informacyjnych	2
C05	Model informacyjnego systemu bezpieczeństwa - identyfikacja procesów w systemie informacyjnym	2
C06	Model systemu procesów - charakterystyka informacyjnego systemu bezpieczeństwa	2
C07	Model systemu procesów - identyfikacja procesów w informacyjnym systemie bezpieczeństwa (cel procesu, właściciel procesu, struktura procesu, wejście/wyjście procesu, dostawcy/odbiorcy procesu, parametry procesu, mierniki procesu)	2
C08	Model systemu procesów - identyfikacja relacji w systemie procesów	3
C09	Model systemu procesów - mapy procesów	3

IV.	**KORELACJA EFEKTÓW KSZTAŁCENIA**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod efektu obszarowego*
W01	Ois_W01, Ois_W02, Ois_W03, Ois_W04	SIB2_W01, SIB2_W04	P7U_W, P7S_WG, P7S_WK
W02	Ois_W01, Ois_W02, Ois_W03, Ois_W04	SIB2_W01, SIB2_W04	P7U_W, P7S_WG, P7S_WK
W03	Ois_W01, Ois_W02, Ois_W03, Ois_W04	SIB2_W01, SIB2_W04	P7U_W, P7S_WG, P7S_WK
W04	Ois_W01, Ois_W02, Ois_W03, Ois_W04	SIB2_W01, SIB2_W04	P7U_W, P7S_WG, P7S_WK
W05	Ois_W01, Ois_W02, Ois_W03, Ois_W04	SIB2_W01, SIB2_W04	P7U_W, P7S_WG, P7S_WK
W06	Ois_W01, Ois_W02, Ois_W03, Ois_W04	SIB2_W01, SIB2_W04	P7U_W, P7S_WG, P7S_WK
W07	Ois_W01, Ois_W02, Ois_W03, Ois_W04	SIB2_W01, SIB2_W04	P7U_W, P7S_WG, P7S_WK
W08	Ois_W01, Ois_W02, Ois_W03, Ois_W04	SIB2_W01, SIB2_W04	P7U_W, P7S_WG, P7S_WK
W09	Ois_W01, Ois_W02, Ois_W03, Ois_W04	SIB2_W01, SIB2_W04	P7U_W, P7S_WG, P7S_WK
W10	Ois_W01, Ois_W02, Ois_W03, Ois_W04	SIB2_W01, SIB2_W04	P7U_W, P7S_WG, P7S_WK
W11	Ois_W01, Ois_W02, Ois_W03, Ois_W04	SIB2_W01, SIB2_W04	P7U_W, P7S_WG, P7S_WK
W12	Ois_W01, Ois_W02, Ois_W03, Ois_W04	SIB2_W01, SIB2_W04	P7U_W, P7S_WG, P7S_WK
C01	Ois_U01, Ois_U02, Ois_U03, Ois_U04, Ois_K01, Ois_K02	SIB2_U01, SIB2_U02, SIB2_U04, SIB2_U06, SIB2_U07, SIB2_K01, SIB2_K02, SIB2_K03, SIB2_K05	P7U_U, P7S_UW, P7S_UK, P7S_UO, P7U_K, P7S_KK, P7S_KO, P7S_KR
C02	Ois_U01, Ois_U02, Ois_U03, Ois_U04, Ois_K01, Ois_K02	SIB2_U01, SIB2_U02, SIB2_U04, SIB2_U06, SIB2_U07, SIB2_K01, SIB2_K02, SIB2_K03, SIB2_K05	P7U_U, P7S_UW, P7S_UK, P7S_UO, P7U_K, P7S_KK, P7S_KO, P7S_KR
C03	Ois_U01, Ois_U02, Ois_U03, Ois_U04, Ois_K01, Ois_K02	SIB2_U01, SIB2_U02, SIB2_U04, SIB2_U06, SIB2_U07, SIB2_K01, SIB2_K02, SIB2_K03, SIB2_K05	P7U_U, P7S_UW, P7S_UK, P7S_UO, P7U_K, P7S_KK, P7S_KO, P7S_KR

C04	Ois_U01, Ois_U02, Ois_U03, Ois_U04, Ois_K01, Ois_K02	SIB2_U01, SIB2_U02, SIB2_U04, SIB2_U06, SIB2_U07, SIB2_K01, SIB2_K02, SIB2_K03, SIB2_K05	P7U_U, P7S_UW, P7S_UK, P7S_UO, P7U_K, P7S_KK, P7S_KO, P7S_KR
C05	Ois_U01, Ois_U02, Ois_U03, Ois_U04, Ois_K01, Ois_K02	SIB2_U01, SIB2_U02, SIB2_U04, SIB2_U06, SIB2_U07, SIB2_K01, SIB2_K02, SIB2_K03, SIB2_K05	P7U_U, P7S_UW, P7S_UK, P7S_UO, P7U_K, P7S_KK, P7S_KO, P7S_KR
C06	Ois_U01, Ois_U02, Ois_U03, Ois_U04, Ois_K01, Ois_K02	SIB2_U01, SIB2_U02, SIB2_U04, SIB2_U06, SIB2_U07, SIB2_K01, SIB2_K02, SIB2_K03, SIB2_K05	P7U_U, P7S_UW, P7S_UK, P7S_UO, P7U_K, P7S_KK, P7S_KO, P7S_KR
C07	Ois_U01, Ois_U02, Ois_U03, Ois_U04, Ois_K01, Ois_K02	SIB2_U01, SIB2_U02, SIB2_U04, SIB2_U06, SIB2_U07, SIB2_K01, SIB2_K02, SIB2_K03, SIB2_K05	P7U_U, P7S_UW, P7S_UK, P7S_UO, P7U_K, P7S_KK, P7S_KO, P7S_KR
C08	Ois_U01, Ois_U02, Ois_U03, Ois_U04, Ois_K01, Ois_K02	SIB2_U01, SIB2_U02, SIB2_U04, SIB2_U06, SIB2_U07, SIB2_K01, SIB2_K02, SIB2_K03, SIB2_K05	P7U_U, P7S_UW, P7S_UK, P7S_UO, P7U_K, P7S_KK, P7S_KO, P7S_KR
C09	Ois_U01, Ois_U02, Ois_U03, Ois_U04, Ois_K01, Ois_K02	SIB2_U01, SIB2_U02, SIB2_U04, SIB2_U06, SIB2_U07, SIB2_K01, SIB2_K02, SIB2_K03, SIB2_K05	P7U_U, P7S_UW, P7S_UK, 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	**15**		**125**	**5**
Ćwiczenia	**20**			
Seminaria				
Konwersatoria				
Konsultacje	**5**			
Rozliczenie rygorów przedmiotu				
Przygotowanie do ćwiczeń	**X**	**30**		
Opanowanie informacji		**30**		
Przygotowanie do rozliczenia rygorów		**15**		
RAZEM	**40**	**85**		

VI. METODY DYDAKTYCZNE

1.	Prezentacje multimedialne
2.	Ćwiczenia laboratoryjne

VII. FORMA ZALICZENIA PRZEDMIOTU

Rygor	*Kryteria składowe*	*Waga*
Zaliczenie	Kolokwium	0,5
	Wykonanie projektów	0,5
Egzamin		

VIII. LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

OBOWIĄZKOWA

1. C. Cempel, *Teoria i inżynieria systemów. Zasady i zastosowania myślenia systemowego*, ITE Radom 2008

2.	W. Findeisen (red.), *Analiza systemowa. Podstawy i metodologia*, PWN, 1985
3.	P. Sienkiewicz, *Analiza systemowa. Podstawy i zastosowania*, Bellona, 1994
4.	W. Bojarski, *Podstawy analizy i inżynierii systemów*, WNT, 1983
5.	E. Skrzypek, M. Hofman, *Zarządzanie procesami w przedsiębiorstwie*, Wolters Kluwer Polska, 2010
6.	A. Bitkowska, *Zarządzanie procesami biznesowymi w przedsiębiorstwie*, Vizja Press & IT, Warszawa 2009.
UZUPEŁNIAJĄCA	
1.	J. Konieczny, *Inżynieria systemów działania*, WNT, 1983
2.	P. Sienkiewicz, *Inżynieria systemów kierowania*, PWE, 1988
3.	P. Sienkiewicz, *Inżynieria systemów*, Wydawnictwo, MON, 1983
4.	E. Yourdon, *Współczesna analiza strukturalna*, WNT, 1996
IX.	**PROWADZĄCY PRZEDMIOT**
Stopień, imię i nazwisko	dr hab. Grzegorz Krasnodębski
adres e-mail	g.krasnodebski@amw.gdynia.pl

KARTA PRZEDMIOTU	AKADEMIA MARYNARKI WOJENNEJ WYDZIAŁ DOWODZENIA I OPERACJI MORSKICH	

I.	CHARAKTERYSTYKA PRZEDMIOTU			
Nazwa przedmiotu:		**Audyt i certyfikacja systemów informatycznych**	*Kod*:	**Oes**
Kierunek studiów:		Systemy informacyjne w bezpieczeństwie		
Poziom studiów:		Studia II stopnia		
Forma studiów:		Niestacjonarne		
Kształcenie w zakresie:		Cyberbezpieczeństwo, Analiza danych i informatyka śledcza		
Profil:		Ogólnoakademicki		
Liczba ECTS:		5		
Semestr:		1		
Wymagania wstępne:		Podstawowa wiedza nt. zasad organizacji systemów zarządzania bezpieczeństwem informacyjnym.		
Język wykładowy:		Polski		
Cel przedmiotu:	**C01**	Zapoznanie z uwarunkowaniami charakterystycznymi dla tworzenia systemów zarządzania bezpieczeństwem informacyjnym oraz organizacji ochrony informacji jako szczególnie ważnego elementu zasobów instytucji.		
	C02	Zapoznanie z zasadami inwentaryzacji, klasyfikacji oraz oceny zasobów informacyjnych przetwarzanych w systemach teleinformatycznych w aspekcie zagrożeń oraz podatności ocenianych systemów.		
	C03	Zapoznanie z zasadami realizacji audytów bezpieczeństwa teleinformatycznego, oceny i zarządzania ryzykiem oraz metodami i standardami testowania i audytowania systemów bezpieczeństwa informacyjnego.		
	C04	Ukształtowanie prawidłowych wzorców sumienności, transparentności i niezawisłości w działaniu		

II.	Kierunkowe efekty uczenia się		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Oes_W01**	student ma wiedzę w zakresie podstawowych pojęć i definicji dotyczących audytu, kontroli, certyfikacji i akredytacji	wypowiedź ustna, praca pisemna lub sprawdzian
	Oes_W02	student ma wiedzę w zakresie regulacji formalno-prawnych w obszarze audytu i certyfikacji osób, systemów zarządzania oraz produktów	wypowiedź ustna, praca pisemna lub sprawdzian
	Oes_W03	student rozumie cele certyfikacji oraz audytu oraz zna zasady ich przeprowadzania	wypowiedź ustna, praca pisemna lub sprawdzian
	Oes_W04	student ma wiedzę w zakresie zarządzania ryzykiem	wypowiedź ustna, praca pisemna lub sprawdzian
	Oes_W05	student ma wiedzę w zakresie mechanizmów kontrolnych	wypowiedź ustna/sprawdzian/kolokwium

		wymaganych normami bezpieczeństwa	
Umiejętości:	**Oes_U01**	student rozumie i potrafi oceniać skuteczność systemu zarządzania bezpieczeństwem informacji	wypowiedź ustna, praca pisemna lub sprawdzian
	Oes_U02	student potrafi identyfikować główne zagrożenia w obszarze bezpieczeństwa informacji oraz proponować adekwatne mechanizmy kontrolne	wypowiedź ustna, praca pisemna lub sprawdzian
	Oes_U03	student potrafi przygotować program audytu, oraz zidentyfikować i udokumentować niezgodności, a także analizować ich ewentualny wpływ na bezpieczeństwo przetwarzanych informacji	wypowiedź ustna, praca pisemna lub sprawdzian
	Oes_U04	student potrafi nazwać i sklasyfikować zidentyfikowane ryzyko	wypowiedź ustna, praca pisemna lub sprawdzian
Kompetencje społeczne:	**Oes_K01**	Krytycznie ocenia posiadaną wiedzę i odbierane treści z zakresu audytu i certyfikacja systemów informatycznych	Obserwacja
	Oes_K02	Inicjuje i uczestniczy konstruktywnie w przygotowaniu zadań z zakresu audytu i certyfikacja systemów informatycznych	praca pisemna

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
W01	Audyt i certyfikacja systemów informatycznych - wprowadzenie	1
W02	Podstawy audytowania	1
W03	Rosnąca rola cyberbezpieczeństwa	1
W04	Cyberbezpieczeństwo w pigułce	1
W05	SZBI zgodny z ISO 27001	1
W06	Mechanizmy kontrolne ISO 27001	1
W07	Zarządzanie ryzykiem	1
W08	Kluczowe akty prawne i normalizacyjne	1
W09	Taksonomia cyberzagrożeń	1
W10	Ład korporacyjny w zakresie IT	1
W11	Podstawowe procesy bezpieczeństwa informacji	1
W12	Podstawowe zasady bezpieczeństwa	1
W13	Wdrażanie SZBI	1
W14	Certyfikacja osób, systemów zarządzania i produktów	1
W15	Sprawdzian	1

C01	Charakterystyka krajowych i międzynarodowych aktów prawnych i normatywnych regulujących proces audytowania i certyfikacji systemów zarządzania bezpieczeństwem informacyjnym. Referat studenta.	4
C02	Charakterystyka zasad inwentaryzacji, klasyfikacji i oceny wartości zasobów informacyjnych. Pomiary bezpieczeństw teleinformatycznego. Referat studenta.	3
C03	Charakterystyka procesu zarządzania ryzykiem. Analiza ryzyka w zakresie identyfikacji zagrożeń, podatności i środowiska. Dobór adekwatnych środków ochrony. Studium przypadku. Referat studenta.	3
C04	Zarządzanie projektowaniem i budową systemu bezpieczeństwa teleinformatycznego. Dokumentowanie prac projektowych. Referat studenta.	4
C05	Audyt bezpieczeństwa teleinformatycznego. Referat studenta.	3
C06	Audyt i certyfikowanie systemu zarządzania bezpieczeństwem informacyjnym.	3

IV.	**KORELACJA EFEKTÓW KSZTAŁCENIA**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod efektu obszarowego*
W01	-	-	-
W02	Oes_W01, Oes_W02, Oes_W03, Oes_U01, Oes_U03	SIB2_W01, SIB2_W02, SIB2_W03	P7U_W, P7S_WG, P7S_WK
W03	Oes_W04, Oes_U02, Oes_U04	SIB2_W01, SIB2_W02, SIB2_W03	P7U_W, P7S_WG, P7S_WK
W04	Oes_W03, Oes_W04, Oes_W05, Oes_U01, Oes_U02, Oes_U04	SIB2_W01, SIB2_W02, SIB2_W03	P7U_W, P7S_WG, P7S_WK
W05	Oes_W01, Oes_W02, Oes_W03, Oes_W04, Oes_U01, Oes_U02, Oes_U03	SIB2_W01, SIB2_W02, SIB2_W03	P7U_W, P7S_WG, P7S_WK
W06	Oes_W01, Oes_W03, Oes_W05, Oes_U03	SIB2_W01, SIB2_W02, SIB2_W03	P7U_W, P7S_WG, P7S_WK
W07	Oes_W01, Oes_W03, Oes_W04, Oes_W05, Oes_U01, Oes_U02, Oes_U04	SIB2_W01, SIB2_W02, SIB2_W03	P7U_W, P7S_WG, P7S_WK
W08	Oes_W01, Oes_W02, Oes_W04	SIB2_W01, SIB2_W02, SIB2_W03	P7U_W, P7S_WG, P7S_WK
W09	Oes_W04, Oes_U02, Oes_U04	SIB2_W01, SIB2_W02, SIB2_W03	P7U_W, P7S_WG, P7S_WK
W10	Oes_W01, Oes_W02, Oes_W04, Oes_U01	SIB2_W01, SIB2_W02, SIB2_W03	P7U_W, P7S_WG, P7S_WK
W11	Oes_W03, Oes_W05, Oes_U02	SIB2_W01, SIB2_W02, SIB2_W03	P7U_W, P7S_WG, P7S_WK
W12	Oes_W03, Oes_W05, Oes_U02	SIB2_W01, SIB2_W02, SIB2_W03	P7U_W, P7S_WG, P7S_WK
W13	Oes_W01, Oes_W03, Oes_U01	SIB2_W01, SIB2_W02, SIB2_W03	P7U_W, P7S_WG, P7S_WK
W14	Oes_W01, Oes_W02, Oes_W03, Oes_U02	SIB2_W01, SIB2_W02, SIB2_W03	P7U_W, P7S_WG, P7S_WK

W15			
C01	Oes_W01, Oes_W03, Oes_K01, Oes_K02	-	-
C02	Oes_W02, Oes_W04, Oes_W05, Oes_U01, Oes_U02, Oes_K01, Oes_K02	SIB2_U01, SIB2_U04, SIB2_U06, SIB2_K02, SIB2_K04	P7U_U, P7S_UW, P7S_UK, P7S_UO, P7U_K, P7S_KK, P7S_KR
C03	Oes_W01, Oes_W04, Oes_W05, Oes_U01, Oes_U02, Oes_U03, Oes_U04, Oes_K01, Oes_K02	SIB2_U01, SIB2_U04, SIB2_U06, SIB2_K02, SIB2_K04	P7U_U, P7S_UW, P7S_UK, P7S_UO, P7U_K, P7S_KK, P7S_KR
C04	Oes_W05, Oes_U03, Oes_K01, Oes_K02	SIB2_U01, SIB2_U04, SIB2_U06, SIB2_K02, SIB2_K04	P7U_U, P7S_UW, P7S_UK, P7S_UO, P7U_K, P7S_KK, P7S_KR
C05	Oes_W01, Oes_W03, Oes_W04, Oes_U01, Oes_U03, Oes_U04, Oes_K01, Oes_K02	SIB2_U01, SIB2_U04, SIB2_U06, SIB2_K02, SIB2_K04	P7U_U, P7S_UW, P7S_UK, P7S_UO, P7U_K, P7S_KK, P7S_KR
C06	Oes_W01, Oes_W02, Oes_W03, Oes_W04, Oes_U01, Oes_U03, Oes_U04, Oes_K01, Oes_K02	-	-

V. NAKŁAD PRACY STUDENTA

Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**15**		**125**	**5**
Ćwiczenia	**20**			
Seminaria				
Konwersatoria				
Konsultacje	**5**			
Rozliczenie rygorów przedmiotu				
Przygotowanie do ćwiczeń		**30**		
Opanowanie informacji		**30**		
Przygotowanie do rozliczenia rygorów		**15**		
RAZEM	**40**	**85**		

VI. METODY DYDAKTYCZNE

1.	Wykład z prezentacją multimedialną/dyskusja
2.	Ćwiczenia audytoryjne: projekt praktyczny
3.	Ćwiczenia audytoryjne: praca w grupach

VII. FORMA ZALICZENIA PRZEDMIOTU

Rygor	*Kryteria składowe*	*Waga*
Zaliczenie	ocena ze sprawdzianu	0,4
	aktywność podczas wykładów	0,1
	praca zaliczeniowa	0,2
	ocena z przygotowania i aktywności na ćwiczeniach	0,1
	ocena z projektu	0,2
	obecność na ćwiczeniach obowiązkowa (w przypadku nieobecności pow. 50% - student nieklasyfikowany)	

VIII. LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

OBOWIĄZKOWA	
1.	K. Lidermann, *Bezpieczeństwo informacyjne. Nowe wyzwania*, PWN Warszawa 2017
2.	T. Polaczek, *Audyt bezpieczeństwa informacji w praktyce : praktyczny przewodnik po zagadnieniach ochrony informacji*, Gliwice, Helion, 2006
3.	K. Jajuga (red. naukowa);, *Zarządzanie ryzykiem* autorzy: Krzysztof Jajuga, Wanda Ronka-Chmielowiec, Andrzej Stopczyński, Agnieszka Wojtasik-Terech. Wydanie II. – Warszawa, Wydawnictwo Naukowe PWN SA, 2019.
4.	*Polska norma PN-EN ISO/IEC 27001:2017-06 - wersja polska*, PKN; Warszawa 2017
UZUPEŁNIAJĄCA	
1.	B. Noga, M. Noga, *Zarządzanie ryzykiem w procesie podejmowania decyzji ekonomicznych przez organizacje*, Wydanie I, - Warszawa, CeDeWu, 2019.
2.	*Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 roku w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego*, Dz.U.2011.159.948
3.	*Decyzja nr 7/MON Ministra Obrony Narodowej z dnia 20 stycznia 2012 roku w sprawie organizacji ochrony systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych w resorcie obrony narodowej*, Dz.Urz.MON.2012.8
4.	*Polska norma PN-EN ISO/IEC 27002:2017-06 - wersja polska*, PKN; Warszawa 2017
IX.	**PROWADZĄCY PRZEDMIOT**
Stopień, Imię i nazwisko	dr inż. Jakub Syta, kmdr por. mgr inż. Piotr KATA
adres e-mail	j.syta@amw.gdynia.pl, p.kata@amw.gdynia.pl

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:	**Ocena ryzyka i prognozowanie w bezpieczeństwie**	*Kod*:	**Zpa**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Niestacjonarne		
Kształcenie w zakresie:	Cyberbezpieczeństwo, Analiza danych i informatyka śledcza		
Profil:	Ogólnoakademicki		
Liczba ECTS:	5		
Semestr:	1		
Wymagania wstępne:	Podstawy matematyki, statystyki		
Język wykładowy:	Polski		
Cel przedmiotu:	**C01**	Przedstawienie teorii oraz metod oceny ryzyka w bezpieczeństwie	
	C02	Przedstawienie metod prognozowania w bezpieczeństwie	
	C03	Zaprezentowanie nowoczesnych technologii do oceny ryzyka oraz prognozowania	

II.	**EFEKTY UCZENIA SIĘ**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Zpa_W01**	Posiada wiedzę z zakresu oceny ryzyka	Kolokwium
	Zpa_W02	Posiada wiedzę z zakresu prognozowania	Kolokwium
Umiejętności:	**Zpa_U01**	Potrafi oceniać ryzyko w bezpieczeństwie	Zadanie
	Zpa_U02	Potrafi opracowywać prognozy w bezpieczeństwie	Projektowe
	Zpa_U03	Potrafi wykorzystywać nowoczesne technologie do oceny ryzyka i prognozowania	Zadanie
	Zpa_U04	Posiada umiejętność rozwijania swojej wiedzy dotyczącej oceny ryzyka i prognozowania	Projektowe
Kompetencje społeczne:	**Zpa_K01**	Potrafi współdziałać i pracować w grupie	Zadanie

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
W01	Geneza, pojęcie, definicje ryzyka	1
W02	(geneza i historia ryzyka, etymologia pojęcia ryzyka, definicje i mechanizm ryzyka, dualność pojęcia ryzyka, ryzyko w teorii decyzji, rodzaje ryzyka, gotowość podejmowania ryzyka)	2
W03	Taksonomia ryzyka	2
W04	(ryzyko ekonomiczne, ryzyko prawno-organizacyjne, ryzyko polityczne, ryzyko ekologiczne, ryzyko medyczne, ryzyko społeczne, ryzyko medialne, ryzyko kulturowo-religijne)	2
W05	Miary ryzyka	3
W06	(szacowanie prawdopodobieństwo wystąpienia określonego rodzaju zagrożenia lub straty, a także zysku i korzyści)	2
W07	Symulacja komputerowa do oceny ryzyka i prognozowania	3

	(pojęcie symulacji, technika symulacji, symulacja komputerowa, obiekty symulacji, zalety symulacji)	
C01	Ocena ryzyka (realizacja projektu)	9
C02	Ocena ryzyka - kolokwium	1
C03	Opracowania prognozy (realizacja projektu)	9
C04	Prognozowanie - kolokwium	1

IV.	**KORELACJA EFEKTÓW UCZENIA SIĘ**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyki PRK*
W01	Zpa_W01, Zpa_W02	SIB2_W01, SIB2_W02	P7U_W, P7S_WG, P7S_WK
W02	Zpa_W01, Zpa_W02	SIB2_W01, SIB2_W02	P7U_W, P7S_WG, P7S_WK
W03	Zpa_W01, Zpa_W02	SIB2_W01, SIB2_W02	P7U_W, P7S_WG, P7S_WK
W04	Zpa_W01, Zpa_W02	SIB2_W01, SIB2_W02	P7U_W, P7S_WG, P7S_WK
W05	Zpa_W01, Zpa_W02	SIB2_W01, SIB2_W02	P7U_W, P7S_WG, P7S_WK
W06	Zpa_W01, Zpa_W02	SIB2_W01, SIB2_W02	P7U_W, P7S_WG, P7S_WK
W07	Zpa_W01, Zpa_W02	SIB2_W01, SIB2_W02	P7U_W, P7S_WG, P7S_WK
C01	Zpa_U01, Zpa_U02, Zpa_U03, Zpa_U04, Zpa_K01	SIB2_U01, SIB2_U02, SIB2_U04, SIB2_U06, SIB2_U07, SIB2_K01, SIB2_K02, SIB2_K03	P7U_U, P7S_UW, P7S_UK, P7S_UO, P7U_K, P7S_KK, P7S_KO
C02	Zpa_U01, Zpa_U02, Zpa_U03, Zpa_U04, Zpa_K01	SIB2_U01, SIB2_U02, SIB2_U04, SIB2_U06, SIB2_U07, SIB2_K01, SIB2_K02, SIB2_K03	P7U_U, P7S_UW, P7S_UK, P7S_UO, P7U_K, P7S_KK, P7S_KO
C03	Zpa_U01, Zpa_U02, Zpa_U03, Zpa_U04, Zpa_K01	SIB2_U01, SIB2_U02, SIB2_U04, SIB2_U06, SIB2_U07, SIB2_K01, SIB2_K02, SIB2_K03	P7U_U, P7S_UW, P7S_UK, P7S_UO, P7U_K, P7S_KK, P7S_KO
C04	Zpa_U01, Zpa_U02, Zpa_U03, Zpa_U04, Zpa_K01	SIB2_U01, SIB2_U02, SIB2_U04, SIB2_U06, SIB2_U07, SIB2_K01, SIB2_K02, SIB2_K03	P7U_U, P7S_UW, P7S_UK, P7S_UO, P7U_K, P7S_KK, P7S_KO

V.	**NAKŁAD PRACY STUDENTA**			
Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**15**	**X**	**126**	**5**
Ćwiczenia	**20**			
Seminaria				
Konwersatoria				
Konsultacje (zaliczenie nieobecności, rozliczenie rygorów, poprawy)	**6**			
Przygotowanie do ćwiczeń	**X**	**30**		
Opanowanie informacji		**30**		
Przygotowanie do rozliczenia rygorów		**25**		
RAZEM	**41**	**85**		

VI.	**METODY DYDAKTYCZNE**
1.	Wykład
2.	Ćwiczenia
3.	Laboratorium
4.	Praca w grupach

VII.	**FORMA ZALICZENIA PRZEDMIOTU**	
Rygor	*Kryteria składowe*	*Waga*
Zaliczenie	Ocena z ćwiczeń - sprawozdania	0,4
	Ocena z kolokwium (materiał z wykładów)	0,6

Egzamin	Ocena z egzaminu	1,0
VIII.	**LITERATURA**	
	OBOWIĄZKOWA	
1.	J. Bizon-Górecka, *Ryzyko. Zarządzanie ryzykiem w przedsiębiorstwie. Modelowanie systemu zarządzania ryzykiem w przedsiębiorstwie - ujęcie holistyczne*, Towarzystwo Naukowe Organizacji i Kierownictwa, Bydgoszcz 2007	
2.	M. Cieślik, *Prognozowanie gospodarcze*, 2004	
3.	T. T. Kaczmarek, *Ryzyko i zarządzanie ryzykiem. Ujęcie interdyscyplinarne*, Warszawa 2005	
	UZUPEŁNIAJĄCA	
1.	W. Kasperek, K. Pelc, *Wyzwania technologiczne - Prognozy i strategie*, 2002	
2.	P. Matkowski, *Zarządzanie ryzykiem operacyjnym*, Oficyna Ekonomiczna, Kraków 2006	
3.	S. Strzelczak, *Operational Risk Management*, Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa 2008	
IX.	**PROWADZĄCY PRZEDMIOT**	
Stopień, Imię i nazwisko	Prof. dr hab. Krzysztof FICOŃ, mgr Martyna BARTKOWSKA	
adres e-mail	k.ficon@amw.gdynia.pl m.bartkowska@amw.gdynia.pl	

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 projektem**	***Kod*:**	**Za**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Niestacjonarne		
Kształcenie w zakresie:	Cyberbezpieczeństwo, Analiza danych i informatyka śledcza		
Profil:	Ogólnoakademicki		
Liczba ECTS:	5		
Semestr:	2		
Wymagania wstępne:	Podstawowa wiedza z zarządzania i organizacji oraz ekonomii		
Język wykładowy:	Polski		
Cel przedmiotu:	**C01**	Zapoznanie studentów z zasadami zarządzania projektami w organizacji.	

II.	**EFEKTY UCZENIA SIĘ**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Za_W01**	Student rozumie powody i potrzeby wprowadzenia zasad zarządzania projektami w organizacjach.	Kolokwium
	Za_W02	Student zna ogólne zasady metody planowania oraz realizowania projektów, tworzenia harmonogramów i planów projektu, budowania zespołu, zarządzania ryzykiem i zmianami w projekcie.	Kolokwium
Umiejętności:	**Za_U01**	Student umie wybierać i proponować sposób planowania i realizacji projektu.	Praca projektowa
	Za_U02	Student umie wykorzystywać podstawowe narzędzia organizatorskie w zakresie planowania i realizacji projektów.	Praca projektowa
Kompetencje społeczne:	**Za_K01**	Student potrafi współdziałać i pracować w zespole projektowym, przyjmując w nim różne role.	Praca projektowa
	Za_K02	Student potrafi odpowiednio określić priorytety projektowe służące realizacji określonego przez siebie celu projektowego.	Praca projektowa
	Za_K03	Student potrafi przewidywać wielokierunkowe skutki społeczne wdrażanych projektów.	Praca projektowa

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
W01	**Podstawy zarządzania projektami:** definicja projektu, najważniejsze cechy projektów, rodzaje projektów, zarządzanie projektem, cykl życia	2

	projektu, procesy zarządzania projektem(inicjowanie projektu, planowanie projektu, realizowanie projektu, kontrolowanie projektu, zamykanie projektu), środowisko projektu, Interesariusze projektu, źródła sukcesu projektu, przyczyny niepowodzeń, rola i znaczenie projektów w funkcjonowaniu organizacji.	
W02	**Kontekst projektu:** strategia zarządzania projektem, struktury projektowe, kierownik projektu, przywództwo, zespół projektowy, umiejętności zespołu projektowego, miejsce i rola pracownika w projekcie.	2
W03	**Obszary Wiedzy Zarządzania Projektami:** zarządzanie integracją projektu, zarządzanie zakresem projektu, zarządzanie czasem projektu, zarządzanie kosztami projektu, zarządzanie jakością projektu, zarządzanie zasobami ludzkimi projektu, zarządzanie komunikacją projektu, zarządzanie ryzykiem projektu, zarządzanie zaopatrzeniem projektu.	2
W04	**Inicjowanie projektu:**analizy przedprojektowe (analiza udziałowców projektu, analiza potencjalnych problemów projektowych, analiza produktów projektu, Karta Projektu, czynniki powodzenia projektu, metody oceny rentowności projektów – kryteria wyboru projektu.	3
W05	**Planowanie projektu:** zakres projektu, struktura podziału pracy (WBS), zależności między nimi i dodatkowe, ograniczenia zadań w czasie, szacowanie czasu zadania, określenie i przydział zasobów, rozwiązywanie problemu przeciążenia zasobów, harmonogram projektu (harmonogram projektu w postaci sieci CPM, metody PERT, Łańcuch Krytyczny, Harmonogram Gntta), budżet projektu, metody budżetowania projektu, planowanie organizacji projektu (macierz odpowiedzialności oraz schemat organizacyjny projektu), zasady pracy w projekcie - procedury i standardy projektowe, plan projektu i jego elementy (plan komunikacji, plan zarządzania jakością, plan zarządzania zmianami, plan zarządzania zasobami ludzkimi).	2
W06	**Realizacja i controlling projektu:** procesy realizacji projektu, Controlling projektu - podstawowe zasady, kontrola przebiegu projektu: spotkania przeglądowe i dokumenty, kontrola projektu: raportowanie i eskalowanie problemów, kontrola zmian w projekcie.	2
W07	**Zamknięcie projektu:** procesy zamknięcia projektu, procedury akceptacji i zamknięcia projektu, dokumentacja projektu.	2
C01	**Planowanie projektu za pomocą MS Project – środowisko programu**	4
C02	**Planowanie projektu organizacyjnego dla dowolnej inicjatywy w obszarze bezpieczeństwa państwa za pomocą programu MS Project:**ustalanie celów projektowych, planowanie zakresu, doprecyzowywanie zakresu, określenie działań, określenie kolejności działań, planowanie zasobów, szacowanie czasu trwania działań, opracowanie harmonogramu, oszacowanie kosztów, budżetowanie kosztów, analiza opłacalności projektu, analiza ryzyka projektu, opracowanie planu projektu.	12
C03	**Zaliczenie przedmiotu.**	4

IV.	**KORELACJA EFEKTÓW UCZENIA SIĘ**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyki PRK*
W01	Za_W01, Za_W02	SIB2_W01, SIB2_W04	P7U_W, P7S_WG, P7S_WK

W02	Za_W01, Za_W02	SIB2_W01, SIB2_W04	P7U_W, P7S_WG, P7S_WK
W03	Za_W01, Za_W02	SIB2_W01, SIB2_W04	P7U_W, P7S_WG, P7S_WK
W04	Za_W01, Za_W02	SIB2_W01, SIB2_W04	P7U_W, P7S_WG, P7S_WK
W05	Za_W01, Za_W02	SIB2_W01, SIB2_W04	P7U_W, P7S_WG, P7S_WK
W06	Za_W01, Za_W02	SIB2_W01, SIB2_W04	P7U_W, P7S_WG, P7S_WK
W07	Za_W01, Za_W02	SIB2_W01, SIB2_W04	P7U_W, P7S_WG, P7S_WK
C01	Za_U01, Za_U02, Za_K01, Za_K02, Za_K03	SIB2_U01, SIB2_U02, SIB2_U04, SIB2_U06, SIB2_K03, SIB2_K04, SIB2_K05	P7U_U, P7S_UW, P7S_UK, P7S_UO, P7U_K, P7S_KO, P7S_KR
C02	Za_U01, Za_U02, Za_K01, Za_K02, Za_K03	SIB2_U01, SIB2_U02, SIB2_U04, SIB2_U06, SIB2_K03, SIB2_K04, SIB2_K05	P7U_U, P7S_UW, P7S_UK, P7S_UO, P7U_K, P7S_KO, P7S_KR
C03	Za_U01, Za_U02, Za_K01, Za_K02, Za_K03	SIB2_U01, SIB2_U02, SIB2_U04, SIB2_U06, SIB2_K03, SIB2_K04, SIB2_K05	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 Nie kontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**15**	**X**	**125**	**5**
Ćwiczenia	**20**			
Seminaria	**0**			
Konwersatoria	**0**			
Konsultacje (zaliczenie nieobecności, rozliczenie rygorów, poprawy)	**5**			
Przygotowanie do ćwiczeń	**X**	**25**		
Opanowanie informacji		**25**		
Przygotowanie do rozliczenia rygorów		**35**		
RAZEM	**40**	**85**		

VI. METODY DYDAKTYCZNE

- wykład; - prezentacja multimedialna;	- ćwiczenia – obsługa programu MS Project - praca projektowa indywidualna – z wykorzystaniem programu MS Project;

VII. FORMA ZALICZENIA PRZEDMIOTU

Rygor	*Kryteria składowe*	*Waga*
Zaliczenie	Ocena z kolokwium	0,5
	Ocena z ćwiczeń	0,5
	Razem	1,0

VIII. LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

OBOWIĄZKOWA

1. M. Trocki, *Zarządzanie projektami*, Wydawnictwo Naukowe PWN, 2012 r.
2. M. Pawlak, *Zarządzanie projektami*, Wydawnictwo Naukowe PWN, 2011 r.
3. J. Kisielnicki, *Zarządzanie projektami udzie, procedury, wyniki*, Wolter Kluwer, 2011

UZUPEŁNIAJĄCA

1. A. Kozarkiewicz, M. Łada, *Zarządzanie wartością projektów. Instrumenty rachunkowości zarządczej i controllingu*, C.H. Beck, 2010 r.
2. A. Koszlajda, *Zarządzanie projektami IT. Przewodnik po metodykach*, Helion 2010 r.
3. Zajączkowska A., *Koordynator projektu - instruktaż skutecznego zarządzania projektami unijnymi z suplementem elektronicznym do monitoringu zadań*, Ośrodek Doradztwa i Doskonalenia Kadr, 2010 r.
4. M. Flasiński, *Zarządzanie projektami informatycznymi*, Wydawnictwo Naukowe PWN, 2009 r.
5. S. Barker, R. Cole, *Zarządzanie projektem*, Wydawnictwo Naukowe PWN, 2010 r.

IX.	PROWADZĄCY PRZEDMIOT
Stopień, imię i nazwisko	dr. Jerzy KUPIŃSKI, dr Anna MILER
adres e-mai	j.kupiński@amw.gdynia.pl a.miler@amw.gdynia.pl

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:	**Komunikacja społeczna**	*Kod*:	**Iq**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Niestacjonarne		
Kształcenie w zakresie:	Cyberbezpieczeństwo, Analiza danych i informatyka śledcza		
Profil:	Akademicki		
Liczba ECTS:	3		
Semestr:	2		
Wymagania wstępne:	Poszerzona wiedza z zakresu komunikacji		
Język wykładowy:	Polski		
Cel przedmiotu:	**C01**	Przybliżenie wiedzy pozwalającej zrozumieć istotę zagadnień dotyczących komunikacji społecznej.	
	C02	Zdobycie umiejętności w zakresie umiejętności miękkich.	

II.	**EFEKTY UCZENIA SIĘ**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Iq_W01**	Ma podstawową wiedzę o rożnych rodzajach struktur społecznych oraz rządzące nimi prawidłowości	Kolokwium ustne, praca na ćwiczeniach
	Iq_W02	Posiada elementarną wiedzę na temat efektywnego porozumiewania się w różnorodnych sytuacjach życia zawodowego oraz w kontaktach z cudzoziemcami	Kolokwium ustne, praca na ćwiczeniach
	Iq_W03	Posiada podstawową wiedzę o człowieku, jako podmiocie tworzącym struktury społecznie i działającym w ramach tych struktur	Kolokwium ustne, praca na ćwiczeniach
Umiejętności:	**Iq_U01**	Wykorzystuje zdobytą wiedzę do rozstrzygania dylematów pojawiających się w pracy zawodowej	Kolokwium ustne, praca na ćwiczeniach
	Iq_U02	Potrafi wykorzystać elementarna wiedzę teoretyczną, i pozyskiwać dane do analizowania procesów i zjawisk zachodzących w stosunkach międzyludzkich	Kolokwium ustne, praca na ćwiczeniach
	Iq_U03	Posiada umiejętność przygotowania wystąpień ustnych w języku polskim i obcym, z wykorzystaniem podstawowych ujęć teoretycznych oraz źródeł, związanej ze szczegółowymi kwestiami dotyczącymi stosunków międzyludzkich	Kolokwium ustne, praca na ćwiczeniach
Kompetencje społeczne	**Iq_K01**	Dysponuje umiejętnościami interdyscyplinarnymi, komunikacyjnymi, społecznymi, interpersonalnymi i interkulturowymi, które umożliwiają mu podjęcie pracy w biznesie, instytucjach	Kolokwium ustne, praca na ćwiczeniach

		samorządowych, instytucjach rządowych, mediach i instytucjach międzynarodowych	

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
W01	Istota i funkcje komunikacji społecznej	2
W02	Negocjacje i mediacje	2
W03	Bariery w komunikacji	2
W04	Manipulacja a perswazja – wywieranie wpływu na innych	2
W05	Stres i trema	2
C01	Przygotowanie wystąpień publicznych	2
C02	Komunikacja werbalna i niewerbalna w praktyce	2
C03	Mobbing i molestowanie w pracy zawodowej	2
C04	Jak zostać dobrym liderem	2
C05	Asertywność	2

IV.	**KORELACJA EFEKTÓW UCZENIA SIĘ**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod efektu obszarowego*
W01	Iq_W01, Iq_W03	SIB2_W01, SIB2_W02	P7U_W, P7S_WG, P7S_WK
W02	Iq_W02, Iq_W03	SIB2_W01, SIB2_W02	P7U_W, P7S_WG, P7S_WK
W03	Iq_W02	SIB2_W01, SIB2_W02	P7U_W, P7S_WG, P7S_WK
W04	Iq_W01, Iq_W02, Iq_W03	SIB2_W01, SIB2_W02	P7U_W, P7S_WG, P7S_WK
W05	Iq_W01, Iq_W02, Iq_W03	SIB2_W01, SIB2_W02	P7U_W, P7S_WG, P7S_WK
C01	Iq_W01, Iq_U01, Iq_K01	SIB2_U01, SIB2_U03, SIB2_U04, SIB2_K01	P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK
C02	Iq_W02, Iq_U02, Iq_K01	SIB2_U01, SIB2_U03, SIB2_U04, SIB2_K01	P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK
C03	Iq_W03, Iq_U02, Iq_K01	SIB2_U01, SIB2_U03, SIB2_U04, SIB2_K01	P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK
C04	Iq_W01, Iq_U03, Iq_K01	SIB2_U01, SIB2_U03, SIB2_U04, SIB2_K01	P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK
C05	Iq_W01, Iq_U01, Iq_K01	SIB2_U01, SIB2_U03, SIB2_U04, SIB2_K01	P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK

V.	**NAKŁAD PRACY STUDENTA**			
Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**10**	**X**	**75**	**3**
Ćwiczenia	**10**			
Seminaria				
Konwersatoria				
Konsultacje (zaliczenie nieobecności, rozliczenie rygorów, poprawy)	**5**			
Przygotowanie do ćwiczeń	**X**	**15**		
Opanowanie informacji		**20**		
Przygotowanie do rozliczenia rygorów		**15**		
RAZEM	**25**	**50**		

VI.	**METODY DYDAKTYCZNE**
1.	Wykład z prezentacją multimedialną
2.	Ćwiczenia audytoryjne: dyskusja
3.	Ćwiczenia audytoryjne: praca indywidualna i w grupach

VII.	**FORMA ZALICZENIA PRZEDMIOTU**	
Rygor	*Kryteria składowe*	*Waga*
Zaliczenie	Kolokwium ustne	1,0

VIII.	**LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA**

OBOWIĄZKOWA	
1.	E. Griffin (przekł. O. i W. Kubińscy), *Podstawy komunikacji społecznej*, Gdańskie Wydawnictwo Psychologiczne, Gdańsk 2003
2.	Ht Rückle (tł. T. Soróbka), *Mowa ciała dla menedżerów*, ASTRUM, Wrocław, 2001
UZUPEŁNIAJĄCA	
1.	M. Leary, *Wywieranie wrażenia na innych. O sztuce Autoprezentacji*, Gdańskie Wydawnictwo Psychologiczne, Gdańsk 2010
2.	S. Bębas, J. Plis, J, Bednarek (red. nauk.,), *Komunikacja w cyberświecie*, Wyższa Szkoła Handlowa w Radomiu, Wyższa Szkoła Handlowa, Radom, 2012
3,	L. Gracz, K. Słupińska (red. naukowa), *Negocjacje i komunikacja: wybrane aspekty*, autorzy U. Chrąchol-Barczyk, L. Gracz, I. Ostrowska, G. Rosa, K. Słupińska. Wydanie I, Legionowo: Wydawnictwo edu-Libri, Kraków, 2018
IX.	**PROWADZĄCY PRZEDMIOT**
Stopień, Imię i nazwisko	dr Karol Słowi
adres e-mail	k.slowi@amw.gdynia.pl

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:	**Certyfikacja Systemu Zarządzania ISO/IEC 27001**	*Kod*:	**Csz**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Niestacjonarne		
Kształcenie w zakresie:	Cyberbezpieczeństwo, Analiza danych i informatyka śledcza		
Profil:	Ogólnoakademicki		
Liczba ECTS:	6		
Semestr:	2		
Wymagania wstępne:	Podstawowa znajomość systemu zarządzania bezpieczeństwem informacyjnym w organizacji		
Język wykładowy:	Polski		
Cel przedmiotu:	**C01**	Zapoznanie studentów z wymaganiami Normy ISO 27001.	
	C02	Zapoznanie studentów z procesami realizowanymi w przedsiębiorstwie raz zarządzaniem informacjami stanowiącymi tajemnicę służbową	
	C03	Zapoznanie studentów z wdrożeniem, utrzymanie i doskonaleniem systemu zarządzania bezpieczeństwem informacji według wymagań Normy ISO 27001.	
	C04	Nauczenie studentów przygotowania podstawowych dokumentacji wymaganych do wdrożenia systemu zarzadzania bezpieczeństwem informacji według normy ISO 27001	

II.	**EFEKTY UCZENIA SIĘ**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Csz_W01**	Student rozumie zapisy związane z wymaganiami Normy ISO 27001	egzamin
	Csz_W02	Student zna procesy realizowane w organizacji	egzamin
	Csz_W03	Student potrafi wskazać wymagania jakie należy spełnić aby wdrożyć, utrzymać i doskonalić system bezpieczeństwa informacji według Normy ISO 27001.	egzamin
	Csz_W04	Student zna zasady wyboru jednostki certyfikującej celem certyfikacji wdrożonego systemu zarzadzania bezpieczeństwem informacji.	egzamin
Umiejętności:	**Csz_U01**	Student potrafi badać i oceniać stan systemu ochrony informacji	projekt
	Csz_U02	Student potrafi przeprowadzić analizę ryzyka i ocenę poziomu zagrożeń	projekt
	Csz_U03	Student potrafi od podstaw przygotować dokumentację niezbędną do wdrożenia i certyfikowania systemu bezpieczeństwa informacji	projekt
	Csz_U04	Student potrafi przygotować plan ciągłości działania	projekt

Kompetencje Społeczne:	**Csz_K01**	Student rozumie potrzebę ciągłego dokształcania się zawodowego i rozwoju osobistego. Dokonuje samooceny własnych kompetencji, wyznacza kierunki własnego rozwoju i kształcenia. Samodzielnie podejmuje refleksje dotyczące etyki w odniesieniu do wykonywanej pracy.	obserwacja na zajęciach
	Csz_K02	Potrafi prezentować swoje poglądy oraz umiejętnie argumentować ich słuszność, a także uznawać argumentację innych	obserwacja na zajęciach

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
W01	Wprowadzenie do przedmiotu. Struktura i podział zajęć. Zasady zaliczenia przedmiotu.	1
W02	Ogólne informacje dotyczące Normy ISO 27001	1
W03	Polityki bezpieczeństwa informacji	1
W04	Organizacja bezpieczeństwa informacji	1
W05	Urządzenia mobilne i telepraca	1
W06	Bezpieczeństwo zasobów ludzkich	2
W07	Zarzadzanie aktywami	2
W08	Kontrola dostępu do informacji i zasobu danych. Kryptografia oraz bezpieczeństwo fizyczne i środowiskowe	2
W09	Sprzęt i bezpieczna eksploatacja, ochrona przed szkodliwym oprogramowaniem	1
W10	Pozyskiwanie, rozwój i utrzymanie systemów	1
W11	Relacje z dostawcami, zarzadzanie incydentami, ciągłość bezpieczeństwa informacji oraz zgodność z wymogami prawnymi	1
W12	Egzamin zaliczeniowe.	1
C01	Wdrożenie, utrzymanie systemu Bezpieczeństwa informacji. Zapoznanie z obowiązującymi zasadami certyfikacji organizacji przez niezależne jednostki certyfikujące. Przydział projektów.	2
C02	Opracowywanie dokumentacji/ informacji związanych z kontekstem organizacji	3
C03	Opracowywanie dokumentacji/ informacji związanych z przywództwem w organizacji	3
C04	Opracowywanie dokumentacji/ informacji związanych z planowaniem w organizacji	3
C05	Opracowywanie dokumentacji/ informacji związanych ze wsparciem	3
C06	Opracowywanie dokumentacji/ informacji związanych z działaniami operacyjnymi	3
C07	Opracowywanie dokumentacji/ informacji związanych z oceną wyników	2
C08	Opracowywanie dokumentacji/ informacji związanych z doskonaleniem systemu	2
C09	Realizacja projektów indywidualnych.	3
C10	Oddawanie indywidualnych projektów przez studentów. Uwagi prowadzącego, poprawki studentów. Wystawianie ocen końcowych.	1

IV.	**KORELACJA EFEKTÓW KSZTAŁCENIA**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyki PRK*
W01	Csz_W01	-	

W02	Csz_W01, Csz_W02	SIB2_W01, SIB2_W03	P7U_W, P7S_WG, P7S_WK
W03	Csz_W01, Csz_W03	SIB2_W01, SIB2_W03	P7U_W, P7S_WG, P7S_WK
W04	Csz_W01, Csz_W03	SIB2_W01, SIB2_W03	P7U_W, P7S_WG, P7S_WK
W05	Csz_W01, Csz_W02	SIB2_W01, SIB2_W03	P7U_W, P7S_WG, P7S_WK
W06	Csz_W01, Csz_W03	SIB2_W01, SIB2_W03	P7U_W, P7S_WG, P7S_WK
W07	Csz_W01, Csz_W02	SIB2_W01, SIB2_W03	P7U_W, P7S_WG, P7S_WK
W08	Csz_W01, Csz_W04	SIB2_W01, SIB2_W03	P7U_W, P7S_WG, P7S_WK
W09	Csz_W01, Csz_W03	SIB2_W01, SIB2_W03	P7U_W, P7S_WG, P7S_WK
W10	Csz_W01, Csz_W04	SIB2_W01, SIB2_W03	P7U_W, P7S_WG, P7S_WK
W11	Csz_W01, Csz_W03	SIB2_W01, SIB2_W03	P7U_W, P7S_WG, P7S_WK
W12	Csz_W01, Csz_W04	SIB2_W01, SIB2_W03	P7U_W, P7S_WG, P7S_WK
C01	Csz_W01,Csz_U01	SIB2_U01, SIB2_U04, SIB2_U06, SIB2_K02, SIB2_K03, SIB2_K05	P7U_U, P7S_UW, P7S_UK, P7S_UO, P7U_K, P7S_KK, P7S_KO, P7S_KR
C02	Csz_U01, Csz_U02, Csz_U04	SIB2_U01, SIB2_U04, SIB2_U06, SIB2_K02, SIB2_K03, SIB2_K05	P7U_U, P7S_UW, P7S_UK, P7S_UO, P7U_K, P7S_KK, P7S_KO, P7S_KR
C03	Csz_U01, Csz_U03	SIB2_U01, SIB2_U04, SIB2_U06, SIB2_K02, SIB2_K03, SIB2_K05	P7U_U, P7S_UW, P7S_UK, P7S_UO, P7U_K, P7S_KK, P7S_KO, P7S_KR
C04	Csz_U01, Csz_U03	SIB2_U01, SIB2_U04, SIB2_U06, SIB2_K02, SIB2_K03, SIB2_K05	P7U_U, P7S_UW, P7S_UK, P7S_UO, P7U_K, P7S_KK, P7S_KO, P7S_KR
C05	Csz_U01, Csz_U02, Csz_U04	SIB2_U01, SIB2_U04, SIB2_U06, SIB2_K02, SIB2_K03, SIB2_K05	P7U_U, P7S_UW, P7S_UK, P7S_UO, P7U_K, P7S_KK, P7S_KO, P7S_KR
C06	Csz_U01, Csz_U03	SIB2_U01, SIB2_U04, SIB2_U06, SIB2_K02, SIB2_K03, SIB2_K05	P7U_U, P7S_UW, P7S_UK, P7S_UO, P7U_K, P7S_KK, P7S_KO, P7S_KR
C07	Csz_U01, Csz_U04	SIB2_U01, SIB2_U04, SIB2_U06, SIB2_K02, SIB2_K03, SIB2_K05	P7U_U, P7S_UW, P7S_UK, P7S_UO, P7U_K, P7S_KK, P7S_KO, P7S_KR
C08	Csz_U01, Csz_U02	SIB2_U01, SIB2_U04, SIB2_U06, SIB2_K02, SIB2_K03, SIB2_K05	P7U_U, P7S_UW, P7S_UK, P7S_UO, P7U_K, P7S_KK, P7S_KO, P7S_KR
C09	Csz_U01, Csz_K01, Csz_K02	SIB2_U01, SIB2_U04, SIB2_U06, SIB2_K02, SIB2_K03, SIB2_K05	P7U_U, P7S_UW, P7S_UK, P7S_UO, P7U_K, P7S_KK, P7S_KO, P7S_KR
C10	Csz_U01, Csz_K01, Csz_K02	SIB2_U01, SIB2_U04, SIB2_U06, SIB2_K02, SIB2_K03, SIB2_K05	P7U_U, P7S_UW, P7S_UK, 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	**15**		**151**	**6**
Ćwiczenia	**25**			
Seminaria				
Konwersatoria				
Konsultacje				
Rozliczenie rygorów przedmiotu	**6**			
Przygotowanie do ćwiczeń		**50**		
Opanowanie informacji		**25**		
Przygotowanie do rozliczenia rygorów		**30**		
RAZEM	**46**	**105**		

VI. METODY DYDAKTYCZNE

1.	Wykład z prezentacją multimedialną

2.	Praktyczne ćwiczenia z zakresu tworzenia dokumentacji, audytu oraz wdrażania procedur bezpieczeństwa	
VII.	**FORMA ZALICZENIA PRZEDMIOTU**	
Rygor	*Kryteria składowe*	*Waga*
Egzamin	ocena z ćwiczeń - sprawozdania	0,25
	ocena z egzaminu (materiał z wykładów)	0,75
VIII.	**LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA**	
	OBOWIĄZKOWA	
3.	*„PN-EN ISO/IEC 27001 Technika informacyjna Techniki bezpieczeństwa Systemy zarządzania bezpieczeństwem informacji Wymagania”* PKN 2017	
4.	„*Bezpieczeństwo Informacyjne nowe wyzwania”* K. Liderman PWN 2017	
	UZUPEŁNIAJĄCA	
2.	Dariusz Wróblewski, Zarządzanie ryzykiem – przegląd wybranych metodyk, Wydawnictwo CNBOP-PIB, 2015	
IX.	**PROWADZĄCY PRZEDMIOT**	
Stopień, Imię i nazwisko		
adres e-mail		

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:	**Sztuczna inteligencja**	*Kod*:	**Osi**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Studia niestacjonarne		
Specjalność:	Cyberbezpieczeństwo, Analiza danych i informatyka śledcza		
Profil:	Ogólnoakademicki		
Liczba ECTS:	5		
Semestr:	2		
Wymagania wstępne:	-		
Język wykładowy:	Polski		
Cel przedmiotu:	**C01**	zapoznanie z założeniami sztucznej inteligencji oraz jej rozwoju na przestrzeni lat	
	C02	wykształcenie umiejętność projektowania prostych programów przy pomocy języka C/C++	
	C03	wykształcenie umiejętność projektowania prostych programów przy pomocy języka drabinkowego do realizacji zagadnień związanych z automatyką procesów technologicznych	
	C04	wykształcenie umiejętność projektowania zależności w ramach systemów ekspertowych do wspomagania podejmowania decyzji przez sztuczną inteligencję	

II.	**EFEKTY KSZTAŁCENIA**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Osi_W01**	Student zna i potrafi określić genezę sztucznej inteligencji oraz etapy jej rozwoju	kolokwium
	Osi_W02	Student zna i rozumie podstawy programowania będące podstawą do projektowania systemów bazujących na sprzężeniach zwrotnych	kolokwium
	Osi_W03	Student zna kluczowe techniki realizacji zagadnień związanych z automatyką procesów oraz rozumie stojącą za nimi logiką	kolokwium
	Osi_W04	Student potrafi zdefiniować logikę systemu ekspertowego będącego elementem systemu wspomagania podejmowania decyzji opartego na sztucznej inteligencji	kolokwium
	Osi_W05	Student jest świadomy konsekwencji poddawania się procesom oceny przez sztuczną inteligencję w ramach m.in. kampanii marketingowych	kolokwium
Umiejętności:	**Osi_U01**	Student potrafi obsługiwać skrypty uczenia maszynowego w środowisku Python 3	kolokwium
	Osi_U02	Student zna i potrafi zdefiniować rodzaje sieci neurowych wraz z ich zastosowaniem	kolokwium
Kompetencje społeczne	**Osi_K01**	Potrafi efektywnie pracować i współdziałać w różnych grupach eksperckich i strukturach roboczych.	obserwacja

	Osi_K02	W oparciu o uzyskaną teoretyczną wiedzę programową potrafi samodzielnie aktualizować i doskonalić swoją wiedzę i umiejętności praktyczne w zakresie wykorzystania sztucznej inteligencji w bezpieczeństwie	obserwacja

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
W01	Charakterystyka przedmiotu. Struktura i podział zajęć. Rygory i ustalenia organizacyjne	3
W02	Rozwój technologii komputerowych – od assemblera do sieci neuronowych	3
W03	Pojęcie sztucznej inteligencji oraz jej potencjał w realizacji powierzonych zadań	3
W04	Definiowanie logiki systemów ekspertowych	3
W05	Realizacja zadań wspomagania podejmowania decyzji przez systemy ekspertowe oraz mechanizmy uczenia maszynowego	3
L01	Realizacja zadań w ramach programowania C/C++	1
L02	Realizacja zadań w ramach projektowania systemów automatycznych	4
L03	Projektowanie logiki systemów ekspertowych	5
L04	Projektowanie skrytpów uczenia maszynowego	7
L05	Otwarta analiza sprawozdań z ćwiczeń	3

IV.	**KORELACJA EFEKTÓW KSZTAŁCENIA**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyki PRK*
W01	-	-	-
W02	Osi_W01, Osi_W02, Osi_W03, Osi_W04, Osi_W05	SIB2_W01, SIB2_W02, SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W03	Osi_W01, Osi_W02, Osi_W03, Osi_W04, Osi_W05	SIB2_W01, SIB2_W02, SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W04	Osi_W01, Osi_W02, Osi_W03, Osi_W04, Osi_W05	SIB2_W01, SIB2_W02, SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W05	Osi_W01, Osi_W02, Osi_W03, Osi_W04, Osi_W05	SIB2_W01, SIB2_W02, SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W06	Osi_W01, Osi_W02, Osi_W03, Osi_W04, Osi_W05	SIB2_W01, SIB2_W02, SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK

W07	Osi_W01, Osi_W02, Osi_W03, Osi_W04, Osi_W05	SIB2_W01, SIB2_W02, SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W08	Osi_W01, Osi_W02, Osi_W03, Osi_W04, Osi_W05	SIB2_W01, SIB2_W02, SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W09	Osi_W01, Osi_W02, Osi_W03, Osi_W04, Osi_W05	SIB2_W01, SIB2_W02, SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
L01	-		
L02	Osi_U01, Osi_U02, Osi_K01, Osi_K02	SIB2_U01, SIB2_U03, SIB2_U05, SIB2_U06, SIB2_K01, SIB2_K02	P7U_U, P7S_UW, P7S_UK, P7S_UO, P7U_K, P7S_KK
L03	Osi_U01, Osi_U02, Osi_K01, Osi_K02	SIB2_U01, SIB2_U03, SIB2_U05, SIB2_U06, SIB2_K01, SIB2_K02	P7U_U, P7S_UW, P7S_UK, P7S_UO, P7U_K, P7S_KK
L04	Osi_U01, Osi_U02, Osi_K01, Osi_K02	SIB2_U01, SIB2_U03, SIB2_U05, SIB2_U06, SIB2_K01, SIB2_K02	P7U_U, P7S_UW, P7S_UK, P7S_UO, P7U_K, P7S_KK
L05	Osi_U01, Osi_U02, Osi_K01, Osi_K02	SIB2_U01, SIB2_U03, SIB2_U05, SIB2_U06, SIB2_K01, SIB2_K02	P7U_U, P7S_UW, P7S_UK, P7S_UO, P7U_K, P7S_KK

V.	**NAKŁAD PRACY STUDENTA**			
Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**15**		**126**	**5**
Ćwiczenia	**0**			
Seminaria				
Laboratoria	**20**			
Konsultacje (zaliczenie nieobecności, rozliczenie rygorów, poprawy)	**6**			
Przygotowanie do ćwiczeń		**28**		
Opanowanie informacji		**28**		
Przygotowanie do rozliczenia rygorów		**29**		
RAZEM	**41**	**85**		

VI.	**METODY DYDAKTYCZNE**

1.	Wykład z prezentacją multimedialną		
2.	Ćwiczenia na stanowiskach komputerowych		
VII.	**FORMA ZALICZENIA PRZEDMIOTU**		
Rygor	*Kryteria składowe*		*Waga*
Egzamin	ocena z ćwiczeń - test		0,3
	egzamin (materiał z wykładów)		0,7
VIII.	**LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA**		
OBOWIĄZKOWA			
6.	K. Ficoń, *Sztuczna inteligencja nie tylko dla humanistów*, BelStudio, Warszawa 2013		
7.	J. Arabas*, Wykłady z algorytmów ewolucyjnych*, Wydawnictwa Naukowo-Techniczne, Warszawa 2001		
8.	D. E. Goldberg, *Algorytmy genetyczne i ich zastosowania*, Wydawnictwa NaukowoTechniczne, Warszawa 1995		
UZUPEŁNIAJĄCA			
9.	T. Masters, *Sieci neuronowe w praktyce*, WNT 1996		
10.	J. Korbicz, A, Obuchowicz, D. Uciński, *Sztuczne sieci neuronowe*, PLJ 1994		
IX.	**PROWADZĄCY PRZEDMIOT**		
Stopień, Imię i nazwisko	mgr inż. Karol Gazda, por. mar. mgr Łukasz Grzyb (ćwiczenia)		
adres e-mail	k.gazda@amw.gdynia.pl, l.grzyb@amw.gdynia.pl		

3.8. Karty przedmiotów modułu kształceniastudiów studiów niestacjonarnych w zakresie Cyberbezpieczeństwo – C

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 projektami informatycznymi**	*Kod*:	**Ozo**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Niestacjonarne		
Kształcenie w zakresie:	Cyberbezpieczeństwo		
Profil:	Ogólnoakademicki		
Liczba ECTS:	5		
Semestr:	3		
Wymagania wstępne:	-----		
Język wykładowy:	Polski z terminologią angielską		
Cel przedmiotu:	**C01**	Zademonstrowanie istotności precyzyjnego przygotowywania wymagań i elastycznego podejścia do ich wdrażania	
	C02	Pokazanie istotności procesów komunikacyjnych w trakcie projektów IT	
	C05	Zademonstrowanie przydatności różnych narzędzi informatycznych w osiąganiu różnych celów	

II.	**EFEKTY UCZENIA SIĘ**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Ozo_W01**	Zna i rozumie w pogłębiony sposób wybrane fakty, teorie, metody oraz złożone zależności między nimi, także w powiązaniu z innymi dziedzinami różnorodne, złożone uwarunkowania i aksjologiczny kontekst prowadzonej działalności z zakresu teorii bezpieczeństwa, systemów informatycznych, systemów administracji publicznej, cyberbezpieczeństwa, analizy danych oraz zarządzania projektami	Sprawdzian
	Ozo_W02	Zna i rozumie podstawowe procesy zachodzące w cyklu życia projektów dotyczących systemów teleinformatycznych	Sprawdzian
	Ozo_W03	Zna i rozumie w pogłębiony sposób podstawowe zasady tworzenia różnych form przedsiębiorczości związane z wykorzystaniem systemów informacyjnych w bezpieczeństwie	Sprawdzian, Wykonanie projektu
Umiejętności:	**Ozo_U01**	Wykorzystuje posiadaną wiedzę z zakresu bezpieczeństwa, systemów informatycznych, systemów administracji publicznej, cyberbezpieczeństwa oraz analizy danych oraz formułować i rozwiązywać złożone i nietypowe problemy oraz innowacyjnie wykonywać zadania w warunkach nieprzewidywalnych poprzez:	Wykonanie projektu

		- 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; - przystosowanie istniejących lub opracowanie nowych metod i narzędzi	
	Ozo_U02	Komunikuje się z otoczeniem z użyciem specjalistycznej technologii	Wykonanie projektu
	Ozo_U03	Potrafi brać udział w debacie z zakresu wykorzystania systemów informacyjnych w bezpieczeństwie - przedstawia i ocenia różne opinie i stanowiska oraz dyskutuje o nich	Prezentacja projektu, Wykonanie projektu
	Ozo_U04	Planuje i organizuje pracę indywidualną oraz kieruje pracą zespołu w ramach realizacji zadań	Wykorzystywanie narzędzi, Wykonanie projektu
Kompetencje społeczne:	**Ozo_K01**	Krytycznie ocenia posiadaną wiedzę i odbierane treści z zakresu teorii bezpieczeństwa, systemów informatycznych, systemów administracji publicznej, cyberbezpieczeństwa, analizy danych oraz zarządzania projektami	Wykonanie projektu, Sprawdzian
	Ozo_K02	Uznaje znaczenie wiedzy w rozwiązywaniu problemów badawczych i praktycznych oraz zasięga opinii ekspertów w przypadku trudności z samodzielnym rozwiązywaniem problemów dotyczących wykorzystania systemów informacyjnych w bezpieczeństwie	Wykonanie projektu, Praca grupowa
	Ozo_K03	Inicjuje i uczestniczy konstruktywnie w przygotowaniu projektów społecznych (politycznych, gospodarczych, obywatelskich), uwzględniając ich różne aspekty, planując i zarządzając przy tym czasem własnym oraz czasem w przedsięwzięciach zespołowych	Wykonanie projektu
	Ozo_K04	Planuje przedsięwzięcia własne i zespołów, z uwzględnieniem zmieniających się potrzeb społecznych, rozwiązuje problemy organizacyjne i inne o różnym poziomie złożoności	Wykonanie projektu, Wykorzystywanie narzędzi
	Ozo_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	Praca grupowa, Wykonanie projektu

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
W01	Organizacja zajęć	1
W02	Cele zarządzania projektami	1
W03	Procesy zarządzania projektami	2
W04	Tematy w ramach zarządzania projektami	1

W05	Zasady w zarządzaniu projektami	2
W06	Role w zarządzaniu projektami	1
W07	Wymagania dla projektów IT	1
W08	Metody prowadzenia projektów	1
W09	Wspieranie zarządzania projektami narzędziami IT	1
W10	Kończenie projektu	2
W11	Sprawdzian	2
C01	Organizacja zajęć	1
C02	Instalacja środowisk, rozpoznanie narzędzi	1
C03	Zarządzanie przebiegiem ćwiczeń (Kanban)	1
C04	Generowanie wymagań funkcjonalnych i bezpieczeństwa	2
C05	Identyfikacja ról	1
C06	Definiowanie wartości biznesowej	2
C07	2 Prezentacje śród-semestralne	2
C08	Rozpisanie kamieni milowych i zadań	2
C09	Opis artefaktów projektu	1
C10	Identyfikacja ryzyk projektowych	1
C11	Identyfikacja ryzyk produktowych	1
C12	Opis produktu (wymagań biznesowych)	1
C13	Przygotowanie makiety interface użytkownika	1
C14	Schemat logiczny architektury rozwiązania	1
C15	Plakat reklamowy	1
C16	Prezentacje zaliczeniowe	1

IV.	**KORELACJA EFEKTÓW UCZENIA SIĘ**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyk PRK*
W01	Ozo_W01, Ozo_W02, Ozo_W03, Ozo_K03, Ozo_K04, Ozo_K05	SIB2_W01, SIB2_W02, SIB2_W04, SIB2_K04, SIB2_K05	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KR
W02	Ozo_W01, Ozo_W02, Ozo_W03, Ozo_K05	SIB2_W01, SIB2_W02, SIB2_W04, SIB2_K04, SIB2_K05	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KR
W03	Ozo_W01, Ozo_W02	SIB2_W01, SIB2_W02	P7U_W, P7S_WG, P7S_WK,
W04	Ozo_W01, Ozo_W02, Ozo_W03, Ozo_U04, Ozo_K02	SIB2_W01, SIB2_W02, SIB2_W04, SIB2_U06, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UO, P7U_K, P7S_KK
W05	Ozo_W01, Ozo_W02, Ozo_W03, Ozo_U04, Ozo_K02, Ozo_K05	SIB2_W01, SIB2_W02, SIB2_W04, SIB2_U06, SIB2_K02, SIB2_K05	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UO, P7U_K, P7S_KK, P7S_KR
W06	Ozo_W01, Ozo_W02, Ozo_U04, Ozo_K02, Ozo_K05	SIB2_W01, SIB2_W02, SIB2_U06, SIB2_K02, SIB2_K05	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UO, P7U_K, P7S_KK, P7S_KR
W07	Ozo_W01, Ozo_W02, Ozo_W03	SIB2_W01, SIB2_W02, SIB2_W04	P7U_W, P7S_WG, P7S_WK
W08	Ozo_W01, Ozo_W02, Ozo_W03, Ozo_U04, Ozo_K05	SIB2_W01, SIB2_W02, SIB2_U06, SIB2_K05	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UO, P7U_K, P7S_KR
W09	Ozo_W01, Ozo_W02, Ozo_U02, Ozo_U04, Ozo_K05	SIB2_W01, SIB2_W02, SIB2_U03, SIB2_U06, SIB2_K05	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UK, P7S_UO, P7U_K, P7S_KR
W10	Ozo_W01, Ozo_W02, Ozo_W03, Ozo_K03, Ozo_K04, Ozo_K05	SIB2_W01, SIB2_W02, SIB2_W04, SIB2_K03, SIB2_K04, SIB2_K05	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KO, P7S_KR

W11	Ozo_W01, Ozo_W02, Ozo_W03, Ozo_U01, Ozo_K05	SIB2_W01, SIB2_W02, SIB2_W04, SIB2_U01, SIB2_K05	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7U_K, P7S_KR
C01	Ozo_W01, Ozo_W02, Ozo_U01, Ozo_U02, Ozo_K03, Ozo_K04	SIB2_W01, SIB2_W02, SIB2_U01, SIB2_U03, SIB2_K03, SIB2_K04	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KO, P7S_KR
C02	Ozo_W01, Ozo_W02, Ozo_U01, Ozo_U02	SIB2_W01, SIB2_W02, SIB2_U01, SIB2_U03	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7S_UK
C03	Ozo_W01, Ozo_W02, Ozo_W03, Ozo_U01, Ozo_U02, Ozo_U04, Ozo_K03, Ozo_K04, Ozo_K05	SIB2_W01, SIB2_W02, SIB2_W04, SIB2_U01, SIB2_U03, SIB2_U06, SIB2_K04, SIB2_K05	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7S_UK, P7S_UO, P7U_K, P7S_KR
C04	Ozo_W01, Ozo_W02, Ozo_W03, Ozo_U01, Ozo_U02, Ozo_U03, Ozo_K01	SIB2_W01, SIB2_W02, SIB2_W04, SIB2_U01, SIB2_U03, SIB2_U04, SIB2_K01	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK
C05	Ozo_W01, Ozo_W02, Ozo_U01, Ozo_U02, Ozo_U04, Ozo_K02, Ozo_K05	SIB2_W01, SIB2_W02, SIB2_U01, SIB2_U03, SIB2_U06, SIB2_K02, SIB2_K05	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7S_UK, P7S_UO, P7U_K, P7S_KK, P7S_KR
C06	Ozo_W01, Ozo_W02, Ozo_W03, Ozo_U01, Ozo_U02, Ozo_U03, Ozo_K01, Ozo_K05	SIB2_W01, SIB2_W02, SIB2_W04, SIB2_U01, SIB2_U03, SIB2_U04, SIB2_K01, SIB2_K05	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK, P7S_KR
C07	Ozo_W01, Ozo_W02, Ozo_W03, Ozo_U02, Ozo_U03, Ozo_U04, Ozo_K01	SIB2_W01, SIB2_W02, SIB2_W04, SIB2_U03, SIB2_U04, SIB2_U06, SIB2_K01	P7U_W, P7S_WG, P7S_WK, P7U_U P7S_UK, P7S_UO, P7U_K, P7S_KK
C08	Ozo_W01, Ozo_W02, Ozo_W03, Ozo_U01, Ozo_U02, Ozo_U03, Ozo_U04, Ozo_K02	SIB2_W01, SIB2_W02, SIB2_W04, SIB2_U01, SIB2_U03, SIB2_U04, SIB2_U06, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7S_UK, P7S_UO, P7U_K P7S_KK
C09	Ozo_W01, Ozo_W02, Ozo_W03, Ozo_U01, Ozo_U02, Ozo_U03	SIB2_W01, SIB2_W02, SIB2_W04, SIB2_U01, SIB2_U03, SIB2_U04,	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7S_UK,
C10	Ozo_W01, Ozo_W02, Ozo_W03, Ozo_U01, Ozo_U02, Ozo_U03, Ozo_K01	SIB2_W01, SIB2_W02, SIB2_W04, SIB2_U01, SIB2_U03, SIB2_U04, SIB2_K01	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK
C11	Ozo_W01, Ozo_W02, Ozo_W03, Ozo_U01, Ozo_U02, Ozo_U03, Ozo_K01, Ozo_K02, Ozo_K05	SIB2_W01, SIB2_W02, SIB2_W04, SIB2_U01, SIB2_U03, SIB2_U04, SIB2_K01, SIB2_K02, SIB2_K05	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK, P7S_KR
C12	Ozo_W01, Ozo_W02, Ozo_W03, Ozo_U01, Ozo_U02, Ozo_U03, Ozo_K05	SIB2_W01, SIB2_W02, SIB2_W04, SIB2_U01, SIB2_U03, SIB2_U04, SIB2_K05	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KR
C13	Ozo_W01, Ozo_W02, Ozo_W03, Ozo_U01, Ozo_U02	SIB2_W01, SIB2_W02, SIB2_W04, SIB2_U01, SIB2_U03,	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7S_UK,
C14	Ozo_W01, Ozo_W02, Ozo_W03, Ozo_U01, Ozo_U02, Ozo_U03	SIB2_W01, SIB2_W02, SIB2_W04, SIB2_U01, SIB2_U03, SIB2_U04,	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7S_UK,
C15	Ozo_W01, Ozo_W02, Ozo_W03, Ozo_U01, Ozo_U02	SIB2_W01, SIB2_W02, SIB2_W04, SIB2_U01, SIB2_U03,	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7S_UK,
C16	Ozo_W01, Ozo_W02, Ozo_W03, Ozo_U01, Ozo_U02, Ozo_U03, Ozo_K01, Ozo_K03, Ozo_K04	SIB2_W01, SIB2_W02, SIB2_W04, SIB2_U01, SIB2_U03, SIB2_U04, SIB2_K01, SIB2_K03, SIB2_K04	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7S_UK, 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	**15**	**X**	**126**	**5**
Ćwiczenia	**20**			
Seminaria	**0**			
Konwersatoria	**0**			
Konsultacje (zaliczenie nieobecności, rozliczenie rygorów)	**6**			
Przygotowanie do ćwiczeń	**X**	**35**		
Opanowanie informacji		**30**		
Przygotowanie do rozliczenia rygorów		**20**		
RAZEM	**41**	**85**		

VI.	**METODY DYDAKTYCZNE**
1.	Wykład z prezentacją multimedialną
2.	Ćwiczenia z wykorzystywaniem narzędzi online
3.	Ćwiczenia z wykorzystywaniem narzędzi offline
4.	Praca w grupach
5.	Prezentacje

VII.	**FORMA ZALICZENIA PRZEDMIOTU**	
Rygor	*Kryteria składowe*	*Waga*
Egzamin	Egzamin	0,4
	Ocena z ćwiczeń	0,4
	Praca zaliczeniowa	0.2

VIII.	**LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA**
	OBOWIĄZKOWA
1.	Flasiński M.; Zarządzanie projektami informatycznymi
2.	Jasińska K., Szapiro T., Zarządzanie procesami realizacji projektów w sektorze ICT
	UZUPEŁNIAJĄCA
1.	Managing Successful Projects with PRINCE2® 2017 Edition
2.	K. Gene Projekt Jednorożec. Powieść o szansie w epoce przewrotów cyfrowych
3.	K. Gene Projekt Fenix. Powieść o IT, modelu DevOps

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

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:	**Akredytacja bezpieczeństwa teleinformatycznego**	*Kod*:	**Ljb**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Niestacjonarne		
Kształcenie w zakresie:	Cyberbezpieczeństwo		
Profil:	Ogólnoakademicki		
Liczba ECTS:	5		
Semestr:	3		
Wymagania wstępne:	Brak		
Język wykładowy:	Polski		
Cel przedmiotu:	**C01**	Zapoznanie z celami i przeznaczeniem akredytacji bezpieczeństwa teleinformatycznego.	
	C02	Zapoznanie z przepisami definiującymi zasady akredytacji bezpieczeństwa.	
	C03	Przybliżenie sposobów realizacji procesu akredytacji bezpieczeństwa teleinformatycznego.	

II.	**EFEKTY UCZENIA SIĘ**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Ljb_W01**	Student zna i rozumie zasady wykonywania dokumentacji bezpieczeństwa teleinformatycznego	Egzamin
	Ljb_W02	Student zna mechanizmy bezpieczeństwa wykorzystywane w systemach teleinformatycznych	Egzamin
	Ljb_W03	Student zna zasady akredytacji bezpieczeństwa teleinformatycznego oraz szacowania ryzyka.	Egzamin
Umiejętności:	**Ljb_U01**	Student potrafi wykorzystać znajomość języka angielskiego w zakresie słownictwa specjalistycznego na poziomie gwarantującym poprawne posługiwanie się dokumentacją techniczną.	Egzamin; zadania
	Ljb_U02	Student potrafi wykonać szacowanie ryzyka dla systemów teleinformatycznych oraz zna podstawy akredytacji bezpieczeństwa.	Egzamin; zadania
Kompetencje społeczne:	**Ljb_K01**	Student dostrzega znaczenie wiedzy w zakresie rozwiązywania problemów zabezpieczenia technicznego i wprowadzania nowych rozwiązań oraz docenia znaczenie samodzielnego poszerzania wiedzy i umiejętności	Praca w grupach

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
W01	Wprowadzenie do akredytacji bezpieczeństwa teleinformatycznego	1
W02	Zarządzanie ryzykiem	1
W03	Szczególne Wymagania Bezpieczeństwa	2
W04	Procedury Bezpiecznej Eksploatacji	1
W05	Analiza Ryzyka	1
W06	Zasady akredytacji niejawnych systemów teleinformatycznych	1

W07	Rola i funkcje krajowej władzy bezpieczeństwa	1
W08	Zadania i zakres obowiązków poszczególnych osób funkcyjnych w procesie akredytacji bezpieczeństwa teleinformatycznego.	2
C01	Metodyka CRAMM	1
C02	Charakterystyka Systemu Teleinformatycznego	1
C03	Zarządzanie Systemem Teleinformatycznym	1
C04	Bezpieczeństwo osobowe	1
C05	Bezpieczeństwo urządzeń	1
C06	Bezpieczeństwo oprogramowania	1
C07	Ciągłość działania	1
C08	Monitorowanie i audyt	1
C09	Zarządzanie nośnikami danych	1
C10	Plany awaryjne	1

IV.	**KORELACJA EFEKTÓW UCZENIA SIĘ**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyk PRK*
W01	Ljb_W01, Ljb_W02, Ljb_W03, Ljb_K01	SIB2_W01, SIB2_W02, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W02	Ljb_W01, Ljb_W02, Ljb_W03, Ljb_K01	SIB2_W01, SIB2_W02, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W03	Ljb_W01, Ljb_W02, Ljb_W03, Ljb_K01	SIB2_W01, SIB2_W02, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W04	Ljb_W01, Ljb_W02, Ljb_W03, Ljb_K01	SIB2_W01, SIB2_W02, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W05	Ljb_W01, Ljb_W02, Ljb_W03, Ljb_K01	SIB2_W01, SIB2_W02, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W06	Ljb_W01, Ljb_W02, Ljb_W03, Ljb_K01	SIB2_W01, SIB2_W02, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W07	Ljb_W01, Ljb_W02, Ljb_W03, Ljb_K01	SIB2_W01, SIB2_W02, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W08	Ljb_W01, Ljb_W02, Ljb_W03, Ljb_K01	SIB2_W01, SIB2_W02, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
C01	Ljb_W03, Ljb_U01, Ljb_U02, Ljb_K01	SIB2_W01, SIB2_U01, SIB2_U05, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK
C02	Ljb_W03, Ljb_U01, Ljb_U02, Ljb_K01	SIB2_W01, SIB2_U01, SIB2_U05, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK
C03	Ljb_W03, Ljb_U01, Ljb_U02, Ljb_K01	SIB2_W01, SIB2_U01, SIB2_U05, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK
C04	Ljb_W03, Ljb_U01, Ljb_U02, Ljb_K01	SIB2_W01, SIB2_U01, SIB2_U05, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK
C05	Ljb_W03, Ljb_U01, Ljb_U02, Ljb_K01	SIB2_W01, SIB2_U01, SIB2_U05, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK
C06	Ljb_W03, Ljb_U01, Ljb_U02, Ljb_K01	SIB2_W01, SIB2_U01, SIB2_U05, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK
C07	Ljb_W03, Ljb_U01, Ljb_U02, Ljb_K01	SIB2_W01, SIB2_U01, SIB2_U05, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK
C08	Ljb_W03, Ljb_U01, Ljb_U02, Ljb_K01	SIB2_W01, SIB2_U01, SIB2_U05, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK

C09	Ljb_W03, Ljb_U01, Ljb_U02, Ljb_K01	SIB2_W01, SIB2_U01, SIB2_U05, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK
C10	Ljb_W03, Ljb_U01, Ljb_U02, Ljb_K01	SIB2_W01, SIB2_U01, SIB2_U05, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK

V. NAKŁAD PRACY STUDENTA

Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**10**		**80**	**3**
Ćwiczenia	**10**			
Seminaria				
Konwersatoria				
Konsultacje	**5**			
Rozliczenie rygorów przedmiotu				
Przygotowanie do ćwiczeń		**20**		
Wykonanie zadań domowych		**20**		
Przygotowanie do rozliczenia rygorów		**15**		
RAZEM	**25**	**55**		

VI. METODY DYDAKTYCZNE

1. Wykłady z prezentacjami multimedialnymi
2. Ćwiczenia na stanowiskach komputerowych

VII. FORMA ZALICZENIA PRZEDMIOTU

Rygor	*Kryteria składowe*	*Waga*
Zaliczenie	Egzamin	0,8
	Ocena z ćwiczeń	0,2

VIII. LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

OBOWIĄZKOWA

1. Krzysztof Liderman, Bezpieczeństwo teleinformatyczne Polityka bezpieczeństwa i ochrony informacji, WSISiZ, 2003.
2. Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. 2010 nr 182 poz. 1228)
3. Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz.U.2011.159.948)
4. Marek Anzel "Szacowanie ryzyka oraz zarządzanie ryzykiem w świetle nowej ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych - przykład metody analizy ryzyka opartej na gotowych macierzach"

UZUPEŁNIAJĄCA

1. Liderman Krzysztof, Bezpieczeństwo informacyjne, PWN , Warszawa 2012.

IX. PROWADZĄCY PRZEDMIOT

Stopień, Imię i nazwisko	mgr Krzysztof GAWIOR
adres e-mail	k.gawior@amw.gdynia.pl

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:	**Testy penetracyjne**	*Kod*:	**Mte**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Niestacjonarne		
Specjalność:	Cyberbezpieczeństwo		
Profil:	Ogólnoakademicki		
Liczba ECTS:	4		
Semestr:	3		
Wymagania wstępne:	brak		
Język wykładowy:	Polski z terminologią angielską		
Cel przedmiotu:	**C01**	Zapoznanie studentów z metodyką prowadzenia testów penetracyjnych systemów i usług informatycznych.	
	C02	Pozyskanie umiejętności związanych z wykrywaniem podatności w systemach teleinformatycznych.	
	C03	Pozyskanie umiejętności przygotowania oraz przeprowadzenia testu penetracyjnego w systemie Windows oraz systemie Linux.	

II.	**EFEKTY KSZTAŁCENIA**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Mte_ W01**	Zna i rozumie w pogłębiony sposób wybrane fakty, teorie, metody oraz złożone zależności między nimi, także w powiązaniu z innymi dziedzinami różnorodne, złożone uwarunkowania i aksjologiczny kontekst prowadzonej działalności z zakresu teorii bezpieczeństwa, cyberbezpieczeństwa oraz analizy danych i informatyki śledczej. Zna zasady i metody prowadzenia testów penetracyjnych w sieciach komputerowych.	Pytania sprawdzające podczas zajęć. Kolokwium.
	Mte_ W02	Zna i rozumie w pogłębiony sposób zagadnienia związane z bezpieczeństwem informacji oraz wykorzystaniem technologii informacyjnych. Zna zasady i metody prowadzenia testów pod kątem wyszukiwania podatności w systemach i sieciach teleinformatycznych	Rozwiązanie zadań problemowych
Umiejętności:	**Mte_ U01**	Potrafi wykorzystać posiadaną wiedzę z zakresu bezpieczeństwa, cyberbezpieczeństwa oraz formułować i rozwiązywać złożone i nietypowe problemy. Potrafi przygotować oraz przeprowadzić testy penetracyjne w sieciach komputerowych.	Przygotowanie sprawozdania. Kolokwium.
	Mte U02	Potrafi brać udział w debacie z zakresu wykorzystania systemów informacyjnych w bezpieczeństwie - przedstawiać i oceniać różne opinie i stanowiska oraz dyskutować o nich. Potrafi przeprowadzić testy penetracyjne w systemach i sieciach teleinformatycznych pod kątem wyszukiwania podatności z uwzględnieniem właściwej metody ich realizacji.	Przygotowanie sprawozdania. Kolokwium.

	Mte_U03	Potrafi posługiwać się językiem obcym na poziomie B2 Europejskiego Systemu Opisu Kształcenia Językowego ze szczególnym uwzględnienie specjalistycznej terminologii z zakresu wykorzystania systemów informacyjnych w bezpieczeństwie.	Wykonanie ćwiczenia
	Mte_U04	Potrafi samodzielnie planować i realizować własne uczenie się przez całe życie i ukierunkowywać innych w tym zakresie.	Przygotowanie sprawozdania. Kolokwium.
Kompetencje społeczne:	**Mte_K01**	Krytycznie ocenia posiadaną wiedzę i odbierane treści z zakresu teorii bezpieczeństwa, cyberbezpieczeństw oraz analizy danych i informatyki śledczej.	Przygotowanie do zajęć
	Mte_K02	Uznaje znaczenie wiedzy w rozwiązywaniu problemów badawczych i praktycznych oraz zasięga opinii ekspertów w przypadku trudności z samodzielnych rozwiazywaniem problemów dotyczących wykorzystania systemów informacyjnych w bezpieczeństwie	Przygotowanie do zajęć

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
W01	Zajęcia organizacyjne. Wprowadzenie do przedmiotu. Sprawy organizacyjne.	10 min
W02	System teleinformatyczny: Podstawowe definicje; Atrybuty bezpieczeństwa; Bezpieczeństwo systemu teleinformatycznego.	2
W03	Polityka bezpieczeństwa: Podstawowe definicje; Elementy bezpieczeństwa; Zarządzanie bezpieczeństwem; Przykładowa polityka bezpieczeństwa.	2
W04	Metodyka testów penetracyjnych: Definicja testów penetracyjnych; Rodzaje i opis metodyk (OSSTMM, PTES, NIST800-115, Metasploit, Core Impact, OWASP Web Security Testing Guide, Testy penetracyjne ukierunkowane na cel).	4
W05	Etapy testów penetracyjnych: Czynności wstępne; Rozpoznanie pasywne.	2
W06	Etapy testów penetracyjnych: Aspekty prawne; Rozpoznanie aktywne.	4
W07	Etapy testów penetracyjnych: Faza penetracji / ataku;	2
W08	Etapy testów penetracyjnych: Uzyskanie dostępu – eksploracja środowiska.	2
W09	Etapy testów penetracyjnych: Przygotowanie raportu.	2
L01	Realizacja etapów testów penetracyjnych: Czynności wstępne; Rozpoznanie pasywne.	4
L02	Realizacja etapów testów penetracyjnych: Aspekty prawne; Rozpoznanie aktywne.	4
L03	Realizacja etapów testów penetracyjnych: Faza penetracji / ataku;	4
L04	Realizacja etapów testów penetracyjnych: Uzyskanie dostępu – eksploracja środowiska.	4
L05	Realizacja etapów testów penetracyjnych: Przygotowanie raportu.	4
C01	Analiza pakietów ruchu sieciowego z wykorzystaniem programu WireShark – analizy przypadków	15

IV.	**KORELACJA EFEKTÓW KSZTAŁCENIA**		
Forma	*Kod efektu przedmiotu*	*Kod symbolu*	*Kod charakterystyk PRK*
W01	Mte_W01, Mte_W02	SIB2_W01, SIB2_W02,	P7U_W, P7S_WG, P7S_WK,

	Mte_K01, Mte_K02	SIB2_K01, SIB2_K02	P7U_K, P7S_KK
W02	Mte_W01, Mte_W02 Mte_K01, Mte_K02	SIB2_W01, SIB2_W02, SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W03	Mte_W01, Mte_W02 Mte_K01, Mte_K02	SIB2_W01, SIB2_W02, SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W04	Mte_W01, Mte_W02 Mte_K01, Mte_K02	SIB2_W01, SIB2_W02, SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W05	Mte_W01, Mte_W02 Mte_K01, Mte_K02	SIB2_W01, SIB2_W02, SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W06	Mte_W01, Mte_W02 Mte_K01, Mte_K02	SIB2_W01, SIB2_W02, SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W07	Mte_W01, Mte_W02 Mte_K01, Mte_K02	SIB2_W01, SIB2_W02, SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W08	Mte_W01, Mte_W02 Mte_K01, Mte_K02	SIB2_W01, SIB2_W02, SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W09	Mte_W01, Mte_W02 Mte_K01, Mte_K02	SIB2_W01, SIB2_W02, SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
L01	Mte_W01, Mte_W02 Mte_U01, Mte_U02, Mte_U04, Mte_U04, Mte_K01, Mte_K02	SIB2_W01, SIB2_W02, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07, SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK P7U_U, P7S_UW, P7S_UK, P7S_UU P7U_K P7S_KK
L02	Mte_W01, Mte_W02 Mte_U01, Mte_U02, Mte_U04, Mte_U04, Mte_K01, Mte_K02	SIB2_W01, SIB2_W02, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07, SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK P7U_U, P7S_UW, P7S_UK, P7S_UU P7U_K P7S_KK
L03	Mte_W01, Mte_W02 Mte_U01, Mte_U02, Mte_U04, Mte_U04, Mte_K01, Mte_K02	SIB2_W01, SIB2_W02, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07, SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK P7U_U, P7S_UW, P7S_UK, P7S_UU P7U_K P7S_KK
L04	Mte_W01, Mte_W02 Mte_U01, Mte_U02, Mte_U04, Mte_U04, Mte_K01, Mte_K02	SIB2_W01, SIB2_W02, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07, SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK P7U_U, P7S_UW, P7S_UK, P7S_UU P7U_K P7S_KK
L05	Mte_W01, Mte_W02 Mte_U01, Mte_U02, Mte_U04, Mte_U04, Mte_K01, Mte_K02	SIB2_W01, SIB2_W02, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07, SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK P7U_U, P7S_UW, P7S_UK, P7S_UU P7U_K P7S_KK
C01	Mte_W01, Mte_W02 Mte_U01, Mte_U02, Mte_U04, Mte_U04, Mte_K01, Mte_K02	SIB2_W01, SIB2_W02, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07, SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK P7U_U, P7S_UW, P7S_UK, P7S_UU P7U_K P7S_KK

V.	**NAKŁAD PRACY STUDENTA**			
Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**10**		**110**	**4**
Laboratorium	**10**			
Ćwiczenia	**10**			
Konwersatoria				
Konsultacje	**3**			
Rozliczenie rygorów przedmiotu	**2**			
Przygotowanie do ćwiczeń i laboratorium	**x**	**25**		
Opanowanie informacji		**25**		
Przygotowanie do rozliczenia rygorów		**25**		
RAZEM	**35**	**75**		

VI.	METODY DYDAKTYCZNE
1.	Wykład z prezentacją multimedialną
2.	Praca przy stanowisku komputerowym
3.	Rozwiązywanie zadań problemowych
4.	Studiowanie literatury

VII. FORMA ZALICZENIA PRZEDMIOTU		
Rygor	*Kryteria składowe*	*Waga*
Zaliczenie	Ocena za aktywność na zajęciach	0,2
	Ocena z kolokwium	0,8
Zaliczenie	Aktywność na zajęciach laboratoryjnych	0,2
	Sprawozdania z laboratorium	0,8

VIII.	LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA
	OBOWIĄZKOWA
1.	Białas A., Bezpieczeństwo informacji i usług, Wydawnictwo Naukowo-Techniczne, Warszawa 2007;
2.	Khawaja G. Kali Linux i testy penetracyjne. Biblia. Wydawnictwo Helion, Gliwice 2022;
3.	Velu V. K., Kali Linux i zaawansowane testy penetracyjne. Zostań ekspertem cyberbezpieczeństwa za pomocą Metasploit, Nmap, Wireshark i Burp Suite. Wydanie IV., Wydawnictwo Helion, Gliwice 2023;
4.	Georgia W., Bezpieczny system w praktyce, Wyższa szkoła hackingu i testy penetracyjne, Wydawnictwo Helion, 2015;
5.	Kim P., Podręcznik pentestera. Bezpieczeństwo systemów informatycznych, Wydawnictwo Helion, Gliwice 2014;
6.	Tanner N. H., Blue Team i cyberbezpieczeństwo. Zestaw narzędzi dla specjalistów od zabezpieczenia sieci. Wydawnictwo Helion, Gliwice 2021;
	UZUPEŁNIAJĄCA
1.	Ustawa z dnia 16 lipca 2004r. Prawo telekomunikacyjne (Dz.U. 2004 Nr 171 poz. 1800, tekst ujednolicony);
2.	Ustawa z dnia 18 lipca 2002r. o świadczeniu usług drogą elektroniczną (Dz.U. 2002 Nr 144 poz. 1204, z późn. zm.);
3.	Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2018 r. poz. 1560, z 2019 r. poz. 2020, 2248);
4.	Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (Dz.U. 2020 poz. 1444, tekst jednolity);
5.	Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2017 poz. 2247, tekst jednolity);
6.	Rozporządzenie Rady Ministrów z dnia 11 września 2018 r. w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych;
7.	PN-13335-1, Technika informatyczna - Wytyczne do zarządzania bezpieczeństwem systemów informatycznych - Pojęcia i modele bezpieczeństwa systemów informatycznych, 1999;
8.	NIST National Institute of Standard and Technology - Special Publication 800-37, Revision 2. Risk Management Framework for Information Systems and Organizations, grudzień 2018;
9.	OSSTMM 3 The Open Source Security Testing Methodology Manual. Contemporary Security Testing and Analysis, Pete Herzog, ISECOM, grudzień 2010;

10.	Technical Guide to Information Security Testing and Assessment (SP 800-115). Recommendations of the National Institute of Standards and Technology, wrzesień 2008;	
11.	PTES Penetration Testing Execution Standard, http://www.pentest-standard.org;	
12.	OWASP The Open Web Application Security Project, https://owasp.org/;	
IX.	**PROWADZĄCY PRZEDMIOT**	
Stopień, Imię i nazwisko		kmdr por. dr inż. Adam Stojałowski
adres e-mail		a.stojalowski@amw.gdynia.pl

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:	**Bezpieczeństwo sieci komputerowych i bezprzewodowych**	*Kod*:	**Oxk**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Niestacjonarne		
Kształcenie w zakresie:	Cyberbezpieczeństwo		
Profil:	Ogólnoakademicki		
Liczba ECTS:	5		
Semestr:	3		
Wymagania wstępne:	Brak		
Język wykładowy:	Polski		
Cel przedmiotu:	**C01**	Zapoznanie studentów z zasadami działania sieci komputerowych, ich klasyfikacją i charakterystyką oraz urządzeniami sieciowymi i wykorzystywanymi mediami transmisyjnymi.	
	C02	Zapoznanie studentów z warstwową architekturą sieci oraz protokołami sieciowymi wykorzystywanymi do komunikacji hostów na poziomie poszczególnych warstw.	
	C03	Wykształcenie umiejętności podstawowej konfiguracji urządzeń sieciowych dla realizacji komunikacji z wykorzystaniem sieci komputerowej, obserwacji i analizy działania sieci oraz ruchu sieciowego, diagnozowania podstawowych nieprawidłowości w działaniu sieci komputerowych	

II.	**EFEKTY UCZENIA SIĘ**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Oxk_W01**	Student zna podstawowe urządzenia i standardy sieciowe oraz ich rolę w transmisji danych w sieciach lokalnych i rozległych o różnych topologiach.	Egzamin
	Oxk_W02	Student zna podstawowe modele warstwowe sieci oraz role poszczególne warstwy w procesie transmisji danych między hostami sieci.	Egzamin
	Oxk_W03	Student zna podstawowe protokoły transmisyjne i ich przyporządkowanie do warstwy na poziomie której są wykorzystywane.	Egzamin
Umiejętności:	**Oxk_U01**	Student potrafi zbudować i skonfigurować prostą sieć lokalną.	Egzamin, rozwiązywanie zadań
	Oxk_U02	Student potrafi analizować ruch sieciowy na podstawie danych sterujących poszczególnych warstw sieciowych	Egzamin, rozwiązywanie zadań
	Oxk_U03	Student potrafi łączyć sieci lokalne i konfigurować parametry routingu.	Egzamin, rozwiązywanie zadań
	Oxk_U04	Student potrafi zarządzać przychodzącym do sieci ruchem oraz podejmować działania zwiększające bezpieczeństwo sieci.	Egzamin, rozwiązywanie zadań

Kompetencje społeczne:	**Oxk_K01**	Student w oparciu o uzyskaną podstawową wiedzę z zakresu sieci teleinformatycznych potrafi doskonalić swoją wiedzę i umiejętności z tego obszaru.	Praca w grupach

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
W01	Klasyfikacja i ogólna charakterystyka sieci komputerowych.	2
W02	Warstwowe architektury sieciowe.	1
W03	Warstwa łącza danych, adresacja MAC, standard Ethernet.	1
W04	Protokoły warstwy sieciowej, adresacja IPv4 i IPv6	2
W05	Protokoły warstwy transportowej vs protokoły aplikacji.	1
W06	Zasady i rodzaje routingu.	1
W07	Bezpieczeństwo sieci bezprzewodowych. Ataki na sieci bezprzewodowe WLAN.	2
L01	Wyznaczanie adresu sieci i rozgłoszeniowego sieci na podstawie różnych klas adresów IP hostów, zapoznanie z programem Cisco Packet Tracer – budowa sieci LAN z serwerem DHCP.	3
L02	Protokół TCP, analiza faz zestawiania i rozłączania sesji w warstwie transportowej. Analiza nagłówka protokołu TCP i UDP	3
L03	Routing statyczny i dynamiczny, konfiguracja routerów, podgląd i analiza tablicy routingu, porównanie metryk trasowania oraz dystansu administracyjnego protokołów routingu	3
L04	Konfiguracja usługi NAT oraz analiza tablicy NAT w ustawieniach routera, analiza przesyłanych pakietów IP pod kątem tłumaczenia adresów i portów.	3
L05	Podstawy bezpieczeństwa w sieciach komputerowych. Konfiguracja reguł zapory sieciowej na serwerze oraz weryfikacja ich działania. Konfigurowanie sieci VPN – tunelowanie GRE i IPsec. Tworzenie sieci VLAN oraz zapewnienie transmisji danych między nimi (metoda „router na patyku”, wykorzystanie podinterfejsów routera).	3
L06	Podstawy bezpieczeństwa w sieciach bezprzewodowych. Konfiguracja i zarządzanie AP. Mechanizmy bezpieczeństwa wykorzystywane w sieciach bezprzewodowych.	5

IV.	**KORELACJA EFEKTÓW UCZENIA SIĘ**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyk PRK*
W01	Oxk_W01, Oxk_W02, Oxk_W03, Oxk_K01	SIB2_W01, SIB2_W02, SIB2_K01	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W02	Oxk_W01, Oxk_W02, Oxk_W03, Oxk_K01	SIB2_W01, SIB2_W02, SIB2_K01	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W03	Oxk_W01, Oxk_W02, Oxk_W03, Oxk_K01	SIB2_W01, SIB2_W02, SIB2_K01	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W04	Oxk_W01, Oxk_W02, Oxk_W03, Oxk_K01	SIB2_W01, SIB2_W02, SIB2_K01	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W05	Oxk_W01, Oxk_W02, Oxk_W03, Oxk_K01	SIB2_W01, SIB2_W02, SIB2_K01	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W06	Oxk_W01, Oxk_W02, Oxk_W03, Oxk_K01	SIB2_W01, SIB2_W02, SIB2_K01	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W07	Oxk_W01, Oxk_W02, Oxk_W03, Oxk_K01	SIB2_W01, SIB2_W02, SIB2_K01	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
L01	Oxk_W01, Oxk_U01, Oxk_U02, Oxk_U03, Oxk_U04, Oxk_K01	SIB2_W01, SIB2_U01 SIB2_U02, SIB2_K01	P7U_W, P7S_WG, P7U_U, P7S_UW, P7U_K, P7S_KK

L02	Oxk_W01, Oxk_U01, Oxk_U02, Oxk_U03, Oxk_U04, Oxk_K01	SIB2_W01, SIB2_U01 SIB2_U02, SIB2_K01	P7U_W, P7S_WG, P7U_U, P7S_UW P7U_K, P7S_KK
L03	Oxk_W01, Oxk_U01, Oxk_U02, Oxk_U03, Oxk_U04, Oxk_K01	SIB2_W01, SIB2_U01 SIB2_U02, SIB2_K01	P7U_W, P7S_WG, P7U_U, P7S_UW P7U_K, P7S_KK
L04	Oxk_W01, Oxk_U01, Oxk_U02, Oxk_U03, Oxk_U04, Oxk_K01	SIB2_W01, SIB2_U01 SIB2_U02, SIB2_K01	P7U_W, P7S_WG, P7U_U, P7S_UW P7U_K, P7S_KK
L05	Oxk_W01, Oxk_U01, Oxk_U02, Oxk_U03, Oxk_U04, Oxk_K01	SIB2_W01, SIB2_U01 SIB2_U02, SIB2_K01	P7U_W, P7S_WG, P7U_U, P7S_UW P7U_K, P7S_KK
L06	Oxk_W01, Oxk_U01, Oxk_U02, Oxk_U03, Oxk_U04, Oxk_K01	SIB2_W01, SIB2_U01 SIB2_U02, SIB2_K01	P7U_W, P7S_WG, P7U_U, P7S_UW P7U_K, P7S_KK

V. NAKŁAD PRACY STUDENTA

Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**10**		**126**	**5**
Ćwiczenia				
Seminaria				
Laboratoria	**20**			
Konsultacje	**5**			
Rozliczenie rygorów przedmiotu	**1**			
Przygotowanie do ćwiczeń		**30**		
Wykonanie zadań domowych		**30**		
Przygotowanie do rozliczenia rygorów		**30**		
RAZEM	**36**	**90**		

VI. METODY DYDAKTYCZNE

1. Metody podające: Wykłady z prezentacjami multimedialnymi
2. Metody aktywizujące: pogadanka, obserwacja, praca z dokumentacją, praca w grupach, case study.
3. Ćwiczenia na stanowiskach komputerowych

VII. FORMA ZALICZENIA PRZEDMIOTU

Rygor	*Kryteria składowe*	*Waga*
Zaliczenie	Ocena z kolokwium (materiał z wykładów)	0,4
	Ocena z ćwiczeń	0,6

VIII. LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

OBOWIĄZKOWA

1. Józefiok A., *Budowa sieci komputerowych na przełącznikach i routerach Cisco*, Helion, Gliwice 2013
2. Wrotek W., *Sieci komputerowe*, Helion, Gliwice 2016

UZUPEŁNIAJĄCA

1. Tanenbaum, Wetherall, Sieci komputerowe, Helion, Gliwice 2012
2. Kluczewski J., Bezpieczeństwo sieci komputerowych (ebook), Itstart, Piekary Śląskie 2019
3. Sportack M., Sieci komputerowe. Księga eksperta, Helion, Gliwice 2004

IX. PROWADZĄCY PRZEDMIOT

Stopień, Imię i nazwisko	mgr Grzegorz PIOTROWSKI
adres e-mail	grzegorz.piotrowski@c2o.eu

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:	**Elementy kryptologii**	*Kod*:	**Mkr**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Niestacjonarne		
Kształcenie w zakresie:	Cyberbezpieczeństwo		
Profil:	Ogólnoakademicki		
Liczba ECTS:	5		
Semestr:	4		
Wymagania wstępne:	Podstawowa wiedza na temat technologii komputerowych oraz systemów liczbowych.		
Język wykładowy:	Polski		
Cel przedmiotu:	**C01**	Zapoznanie studentów z podstawowymi pojęciami z zakresu kryptologii, w tym kryptografii i kryptoanalizy.	
	C02	Zapoznanie studentów z algorytmami i protokołami kryptograficznymi	
	C03	Wykształcenie umiejętności szyfrowania i deszyfrowania wiadomości używając współczesnych oraz historycznych algorytmów, a także podstawowych umiejętności z zakresu ich kryptoanalizy	

II.	**EFEKTY UCZENIA SIĘ**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Mkr_W01**	Student zna i rozumie istotę oraz potrzebę szyfrowania danych.	Egzamin
	Mkr_W02	Student zna i wie jak rozpoznać oraz wykorzystać mechanizmy szyfrów historycznych.	Egzamin
	Mkr_W03	Student zna współczesne algorytmy symetryczne oraz obowiązujący standard szyfrowania blokowego.	Egzamin
	Mkr_W04	Student zna i rozumie sposób działania współczesnych algorytmów asymetrycznych oraz protokołów kryptograficznych.	Egzamin
	Mkr_W05	Student zna i rozumie mechanizmy kryptoanalizy współczesnych algorytmów.	Egzamin
Umiejętności:	**Mkr_U01**	Student potrafi użyć mechanizmów wykorzystywanych w kryptologii klasycznej.	Zadania na ćwiczeniach
	Mkr_U02	Student potrafi szyfrować i deszyfrować wiadomości wykorzystując współczesne algorytmy symetryczne. Potrafi generować klucze prywatne i publiczne oparte o kryptografię asymetryczną oraz potrafi szyfrować i deszyfrować wiadomości przy ich wykorzystaniu.	Zadania na laboratorium, egzamin
	Mkr_U03	Student potrafi posługiwać się protokołami uzgadniania wspólnego klucza sesyjnego i wykorzystywać je w praktyce. Potrafi podpisywać przekazywane wiadomości wykorzystując współczesne algorytmu podpisu cyfrowego	Zadania na laboratorium

	Mkr_U04	Student potrafi ocenić bezpieczeństwo badanego algorytmu wykorzystując poznane mechanizmy kryptoanalizy.	Zadania na ćwiczeniach, egzamin
	Mkr_U05	Student potrafi przeprowadzić ataki kryptoanalityczne na proste szyfry symetryczne i asymetryczne	Zadania na laboratorium
Kompetencje społeczne:	**Mkr_K01**	Student krytycznie ocenia posiadaną wiedzę i odbierane treści z zakresu kryptologii oraz potrafi doskonalić swoją wiedzę i umiejętności z tego obszaru.	Praca w grupach

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
W01	Kryptografia klasyczna. Metody szyfrowania i deszyfrowania.	1
W02	Metody kryptoanalizy szyfrów historycznych.	1
W03	Kryptografia symetryczna. Szyfry blokowe.	1
W04	Kryptografia symetryczna. Szyfry strumieniowe.	1
W05	Kryptografia asymetryczna. Algorytm RSA	1
W06	Algorytmy oparte na teorii krzywych eliptycznych.	1
W07	Protokoły kryptograficzne – protokoły wymiany klucza.	1
W08	Protokoły podpisu elektronicznego.	1
W09	Metody kryptoanalizy szyfrów symetrycznych.	1
W10	Metody kryptoanalizy szyfrów asymetrycznych.	1
C01	Szyfrowanie wiadomości algorytmami klasycznymi	1
C02	Deszyfrowanie wiadomości algorytmami klasycznymi	2
C03	Metody kryptoanalizy algorytmów klasycznych	2
L01	Współczesne standardy szyfrowania blokowego	1
L02	Metody kryptoanalizy szyfrów blokowych. Kryptoanaliza różnicowa.	1
L03	Współczesne standardy szyfrowania strumieniowego.	2
L04	Metody kryptoanalizy szyfrów strumieniowych. Ataki algebraiczne.	2
L05	Kryptografia asymetryczna. Algorytm RSA.	1
L06	Algorytmy oparte na krzywych eliptycznych.	2
L07	Protokoły kryptograficzne – protokół Diffiego-Hellmana.	2
L08	Współczesne algorytmy podpisów cyfrowych.	2
L09	Metody kryptoanalizy algorytmów asymetrycznych.	2

IV.	**KORELACJA EFEKTÓW UCZENIA SIĘ**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyk PRK*
W01	Mkr_W01, Mkr_W02, Mkr_W03, Mkr_W04, Mkr_W05, Mkr_K01	SIB2_W01, SIB2_W02, SIB2_K01	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W02	Mkr_W01, Mkr_W02, Mkr_W03, Mkr_W04, Mkr_W05, Mkr_K01	SIB2_W01, SIB2_W02, SIB2_K01	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W03	Mkr_W01, Mkr_W02, Mkr_W03, Mkr_W04, Mkr_W05, Mkr_K01	SIB2_W01, SIB2_W02, SIB2_K01	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W04	Mkr_W01, Mkr_W02, Mkr_W03, Mkr_W04, Mkr_W05, Mkr_K01	SIB2_W01, SIB2_W02, SIB2_K01	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W05	Mkr_W01, Mkr_W02, Mkr_W03, Mkr_W04, Mkr_W05, Mkr_K01	SIB2_W01, SIB2_W02, SIB2_K01	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK

W06	Mkr_W01, Mkr_W02, Mkr_W03, Mkr_W04, Mkr_W05, Mkr_K01	SIB2_W01, SIB2_W02, SIB2_K01	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W07	Mkr_W01, Mkr_W02, Mkr_W03, Mkr_W04, Mkr_W05, Mkr_K01	SIB2_W01, SIB2_W02, SIB2_K01	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W08	Mkr_W01, Mkr_W02, Mkr_W03, Mkr_W04, Mkr_W05, Mkr_K01	SIB2_W01, SIB2_W02, SIB2_K01	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W09	Mkr_W01, Mkr_W02, Mkr_W03, Mkr_W04, Mkr_W05, Mkr_K01	SIB2_W01, SIB2_W02, SIB2_K01	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W10	Mkr_W01, Mkr_W02, Mkr_W03, Mkr_W04, Mkr_W05, Mkr_K01	SIB2_W01, SIB2_W02, SIB2_K01	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
C01	Mkr_W01, Mkr_W02 Mkr_U01, Mkr_U05, Mkr_K01	SIB2_W01, SIB2_U01, SIB2_K01	P7U_W, P7S_WG, P7U_U, P7S_UW, P7U_K, P7S_KK
C02	Mkr_W01, Mkr_W02 Mkr_U01, Mkr_U05, Mkr_K01	SIB2_W01, SIB2_U01, SIB2_K01	P7U_W, P7S_WG, P7U_U, P7S_UW, P7U_K, P7S_KK
C03	Mkr_W01, Mkr_W02 Mkr_U01, Mkr_U05, Mkr_K01	SIB2_W01, SIB2_U01, SIB2_K01	P7U_W, P7S_WG, P7U_U, P7S_UW, P7U_K, P7S_KK
L01	Mkr_W03, Mkr_W04, Mkr_U01, Mkr_U02, Mkr_U03, Mkr_U04, Mkr_U05, Mkr_K01	SIB2_W01, SIB2_U01, SIB2_U02, SIB2_K01	P7U_W, P7S_WG, P7U_U, P7S_UW, P7U_K, P7S_KK
L02	Mkr_W03, Mkr_W04, Mkr_U01, Mkr_U02, Mkr_U03, Mkr_U04, Mkr_U05, Mkr_K01	SIB2_W01, SIB2_U01, SIB2_U02, SIB2_K01	P7U_W, P7S_WG, P7U_U, P7S_UW, P7U_K, P7S_KK
L03	Mkr_W03, Mkr_W04, Mkr_U01, Mkr_U02, Mkr_U03, Mkr_U04, Mkr_U05, Mkr_K01	SIB2_W01, SIB2_U01, SIB2_U02, SIB2_K01	P7U_W, P7S_WG, P7U_U, P7S_UW, P7U_K, P7S_KK
L04	Mkr_W03, Mkr_W04, Mkr_U01, Mkr_U02, Mkr_U03, Mkr_U04, Mkr_U05, Mkr_K01	SIB2_W01, SIB2_U01, SIB2_U02, SIB2_K01	P7U_W, P7S_WG, P7U_U, P7S_UW, P7U_K, P7S_KK
L05	Mkr_W03, Mkr_W04, Mkr_U01, Mkr_U02, Mkr_U03, Mkr_U04, Mkr_U05, Mkr_K01	SIB2_W01, SIB2_U01, SIB2_U02, SIB2_K01	P7U_W, P7S_WG, P7U_U, P7S_UW, P7U_K, P7S_KK
L06	Mkr_W03, Mkr_W04, Mkr_U01, Mkr_U02, Mkr_U03, Mkr_U04, Mkr_U05, Mkr_K01	SIB2_W01, SIB2_U01, SIB2_U02, SIB2_K01	P7U_W, P7S_WG, P7U_U, P7S_UW, P7U_K, P7S_KK
L07	Mkr_W03, Mkr_W04, Mkr_U01, Mkr_U02, Mkr_U03, Mkr_U04, Mkr_U05, Mkr_K01	SIB2_W01, SIB2_U01, SIB2_U02, SIB2_K01	P7U_W, P7S_WG, P7U_U, P7S_UW, P7U_K, P7S_KK
L08	Mkr_W03, Mkr_W04, Mkr_U01, Mkr_U02, Mkr_U03, Mkr_U04, Mkr_U05, Mkr_K01	SIB2_W01, SIB2_U01, SIB2_U02, SIB2_K01	P7U_W, P7S_WG, P7U_U, P7S_UW, P7U_K, P7S_KK
L09	Mkr_W03, Mkr_W04, Mkr_U01, Mkr_U02, Mkr_U03, Mkr_U04, Mkr_U05, Mkr_K01	SIB2_W01, SIB2_U01, SIB2_U02, SIB2_K01	P7U_W, P7S_WG, P7U_U, P7S_UW, P7U_K, P7S_KK

V.	NAKŁAD PRACY STUDENTA			
Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**10**		**126**	**5**
Ćwiczenia	**5**			
Laboratorium	**15**			
Konwersatoria				
Konsultacje	**5**			
Rozliczenie rygorów przedmiotu	**1**			
Przygotowanie do ćwiczeń		**30**		
Wykonanie zadań domowych		**30**		
Przygotowanie do rozliczenia rygorów		**30**		
RAZEM	**36**	**90**		

VI.	METODY DYDAKTYCZNE
1.	Wykłady z prezentacjami multimedialnymi
2.	Ćwiczenia na stanowiskach komputerowych

VII.	FORMA ZALICZENIA PRZEDMIOTU	
Rygor	*Kryteria składowe*	*Waga*
Egzamin	Egzamin pisemny	0,8
	Ocena z ćwiczeń i laboratorium	0,2

VIII.	LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA
	OBOWIĄZKOWA
1.	J.Buchmann, Wprowadzenie do kryptografii, PWN 2006
2.	B.Schneier, Kryptografia dla praktyków. Protokoły, algorytmy i programy źródłowe w języku C, WNT 1995
	UZUPEŁNIAJĄCA
1.	Marcin Karbowski, Podstawy kryptografii. Wydanie III, Helion, Gliwice 2014
2.	A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, Kryptografia stosowana, WNT, Warszawa 2005

IX.	PROWADZĄCY PRZEDMIOT
Stopień, Imię i nazwisko	dr hab. Jerzy KOSIŃSKI, prof. AMW, mgr inż. Kamil SZCZEPANIUK
adres e-mail	j.kosinski@amw.gdynia.pl, k.szczepaniuk@amw.gdynia.pl

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:	**Administrowanie systemem Linux**	*Kod*:	**Oxl**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Niestacjonarne		
Kształcenie w zakresie:	Cyberbezpieczeństwo		
Profil:	Ogólnoakademicki		
Liczba ECTS:	4		
Semestr:	4		
Wymagania wstępne:	Brak		
Język wykładowy:	Polski		
Cel przedmiotu:	**C01**	Zapoznanie studentów z procesem administrowania systemem operacyjnym Linux	
	C03	Zapoznanie studentów z metodami zabezpieczania usług w systemie operacyjnym Linux	

II.	**EFEKTY UCZENIA SIĘ**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Oxl_W01**	Zna i rozumie w pogłębiony sposób wybrane fakty, teorie, metody oraz zależności między nimi z zakresu systemów informatycznych.	Pytania sprawdzające podczas zajęć. Kolokwium.
Umiejętności:	**Oxl_U01**	Potrafi wykorzystać posiadaną wiedzę z zakresu systemów informatycznych oraz rozwiązywać złożone i nietypowe problemy poprzez dobór oraz zastosowanie właściwych metod i narzędzi.	Rozwiązanie zadań problemowych
	Oxl_U02	Potrafi brać udział w debacie z zakresu wykorzystania systemów informacyjnych w bezpieczeństwie - przedstawiać i oceniać różne opinie i stanowiska oraz dyskutować o nich.	Rozwiązanie zadań problemowych Wypowiedzi ustne, aktywność w ramach dyskusji.
	Oxl_U03	Potrafi posługiwać się językiem obcym ze szczególnym uwzględnienie specjalistycznej terminologii z zakresu wykorzystania systemów informacyjnych w bezpieczeństwie.	Rozwiązanie zadań problemowych
	Oxl_U04	Potrafi samodzielnie planować i realizować własne uczenie się przez całe życie i ukierunkowywać innych w tym zakresie.	Przygotowanie do zajęć
Kompetencje społeczne:	**Oxl_K01**	Krytycznie ocenia posiadaną wiedzę i odbierane treści z zakresu systemów informatycznych .	Sprawozdanie /

			przygotowanie do zajęć
	Oxl_K02	Uznaje znaczenie wiedzy w rozwiązywaniu problemów praktycznych oraz zasięga opinii ekspertów w przypadku trudności z samodzielnym rozwiazywaniem problemów dotyczących wykorzystania systemów informacyjnych w bezpieczeństwie.	Rozwiązanie zadań problemowych

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
W01	Wprowadzenie do przedmiotu. Sprawy organizacyjne. Zapoznanie z warunkami zaliczenia. Kontakt. Literatura. Wprowadzenie systemu Linux.	1
W02	Uzyskanie dostępu do systemu Linux. - Wprowadzenie do Bash Shell; - Sposoby logowania się do systemu.	1
W03	System plików. - Organizacja systemu plików; - Kontrola dostępu do plików; - Dowiązania.	2
W04	Zarządzanie kontami użytkowników i grupami systemu Linux. - Konta użytkowników systemu Linux; - Konta grup systemu Linux; - Zarządzanie kontami użytkowników.	2
W05	Operacje na plikach i katalogach - Tworzenie, kopiowanie, przenoszenie i usuwanie plików i katalogów; - Edycja i zapisywanie plików.	2
W06	Monitorowanie procesów - Proces i jego charakterystyka; - Operacje na procesach; - Monitorowanie procesów.	2
W07	Secure Shell (SSH) - Wprowadzenie do SSH; - Klient – serwer; - Zabezpieczenie usługi SSH.	2
W08	Konfiguracja sieci TCP/IP - Model TCP/IP i protokoły sieciowe; - Routing; - Analiza ruchu oraz troubleshooting; - Konfiguracja sieci.	2
W09	Logi i zdarzenia w systemie - Rejestrowanie zdarzeń; - Przegląd i monitorowanie logów.	2
W10	Zarządzanie oprogramowaniem i kontrola usług - zarządzenie oprogramowaniem; - zarządzenie usługami.	2
W11	Zarządzanie bezpieczeństwem systemu operacyjnego - zarządzanie bezpieczeństwem SELinux;	2

	- zarządzenie bezpieczeństwem sieci.	
L01	Uzyskanie dostępu do systemu Linux - Uzyskanie dostępu do systemu; - Korzystanie z powłoki Bash Shell.	2
L02	Konta użytkowników i grup - Zarządzanie kontami lokalnych użytkowników; - Zarządzanie grupami lokalnymi; - Zarządzanie hasłami.	3
L03	Operacje na plikach i katalogach - Tworzenie, kopiowanie, przenoszenie i usuwanie plików i katalogów; - Wyszukiwanie, edycja i zapisywanie plików.	3
L04	Monitorowanie procesów - Operacje na procesach; - Monitorowanie procesów.	2
L05	Secure Shell (SSH) - Komunikacja klient – serwer; - Zabezpieczenie usługi SSH.	2
L06	Konfiguracja sieci TCP/IP - Analiza ruchu sieciowego; - Przegląd konfiguracji sieci.	3
L07	Logi i zdarzenia w systemie - Rejestrowanie zdarzeń; - Przegląd i monitorowanie logów	2
L08	Zarządzanie oprogramowaniem i kontrola usług - zarządzenie oprogramowaniem; - zarządzenie usługami.	2
L09	Zarządzanie bezpieczeństwem - zarządzanie bezpieczeństwem SELinux; - zarządzenie bezpieczeństwem sieci.	2
L10	Wprowadzenie do kontenerów - Wprowadzenie do technologii kontenerowej; - Uruchamianie podstawowego kontenera.	4

IV.	**KORELACJA EFEKTÓW UCZENIA SIĘ**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyk PRK*
W01	Oxl_W01, Oxl_U02, Oxl_U03, Oxl_U04 Oxl_K01, Oxl_K02	SIB2_W01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UK, P7S_UU P7U_K, P7S_KK
W02	Oxl_W01, Oxl_U02, Oxl_U03, Oxl_U04 Oxl_K01, Oxl_K02	SIB2_W01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UK, P7S_UU P7U_K, P7S_KK
W03	Oxl_W01, Oxl_U02, Oxl_U03, Oxl_U04 Oxl_K01, Oxl_K02	SIB2_W01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K01	P7U_W, P7S_WG, P7U_U, P7S_UK, P7S_UU P7U_K, P7S_KK
W04	Oxl_W01, Oxl_U02, Oxl_U03, Oxl_U04 Oxl_K01, Oxl_K02	SIB2_W01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UK, P7S_UU P7U_K, P7S_KK
W05	Oxl_W01, Oxl_U02, Oxl_U03, Oxl_U04 Oxl_K01, Oxl_K02	SIB2_W01, SIB2_U04, SIB2_U05, SIB2_U07	P7U_W, P7S_WG, P7U_U, P7S_UK, P7S_UU P7U_K, P7S_KK

		SIB2_K01, SIB2_K02	
W06	Oxl_W01, Oxl_U02, Oxl_U03, Oxl_U04 Oxl_K01, Oxl_K02	SIB2_W01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UK, P7S_UU P7U_K, P7S_KK
W07	Oxl_W01, Oxl_U02, Oxl_U03, Oxl_U04 Oxl_K01, Oxl_K02	SIB2_W01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UK, P7S_UU P7U_K, P7S_KK
W08	Oxl_W01, Oxl_U02, Oxl_U03, Oxl_U04 Oxl_K01, Oxl_K02	SIB2_W01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UK, P7S_UU P7U_K, P7S_KK
W09	Oxl_W01, Oxl_ Oxl_U02, Oxl_U03, Oxl_U04 Oxl_K01, Oxl_K02	SIB2_W01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UK, P7S_UU P7U_K, P7S_KK
W10	Oxl_W01, Oxl_U02, Oxl_U03, Oxl_U04 Oxl_K01, Oxl_K02	SIB2_W01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UK, P7S_UU P7U_K, P7S_KK
L01	Oxl_W01, Oxl_U01, Oxl_U03, Oxl_K02	SIB2_W01, SIB2_U01, SIB2_U05, SIB2_K02	P7U_W, P7S_WG P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK
L02	Oxl_W01, Oxl_U01, Oxl_U03, Oxl_K02	SIB2_W01, SIB2_U01, SIB2_U05, SIB2_K02	P7U_W, P7S_WG P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK
L03	Oxl_W01, Oxl_U01, Oxl_U03, Oxl_K02	SIB2_W01, SIB2_U01, SIB2_U05, SIB2_K02	P7U_W, P7S_WG P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK
L04	Oxl_W01, Oxl_U01, Oxl_U03, Oxl_K02	SIB2_W01, SIB2_U01, SIB2_U05, SIB2_K02	P7U_W, P7S_WG P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK
L05	Oxl_W01, Oxl_U01, Oxl_U03, Oxl_K02	SIB2_W01, SIB2_U01, SIB2_U05, SIB2_K02	P7U_W, P7S_WG P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK
L06	Oxl_W01, Oxl_U01, Oxl_U03, Oxl_K02	SIB2_W01, SIB2_U01, SIB2_U05, SIB2_K02	P7U_W, P7S_WG P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK
L07	Oxl_W01, Oxl_U01, Oxl_U03, Oxl_K02	SIB2_W01, SIB2_U01, SIB2_U05, SIB2_K02	P7U_W, P7S_WG P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK
L08	Oxl_W01, Oxl_U01, Oxl_U03, Oxl_K02	SIB2_W01, SIB2_U01, SIB2_U05, SIB2_K02	P7U_W, P7S_WG P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK
L09	Oxl_W01, Oxl_U01, Oxl_U03, Oxl_K02	SIB2_W01, SIB2_U01, SIB2_U05, SIB2_K02	P7U_W, P7S_WG P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK
L10	Oxl_W01, Oxl_U01, Oxl_U03, Oxl_K02	SIB2_W01, SIB2_U01, SIB2_U05, SIB2_K02	P7U_W, P7S_WG P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK

V.	**NAKŁAD PRACY STUDENTA**			
Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**10**		**100**	**4**
Ćwiczenia	**0**			
Seminaria	**0**			
Laboratorium	**10**			
Konsultacje	**5**			

Rozliczenie rygorów przedmiotu				
Przygotowanie do ćwiczeń		**25**		
Wykonanie zadań domowych		**25**		
Przygotowanie do rozliczenia rygorów		**25**		
RAZEM	**25**	**75**		

VI.	**METODY DYDAKTYCZNE**
1.	Wykład z prezentacją multimedialną
2.	Praca przy stanowisku komputerowym
3.	Rozwiązywanie zadań problemowych
4.	Studiowanie literatury

VII.	**FORMA ZALICZENIA PRZEDMIOTU**	
Rygor	*Kryteria składowe*	*Waga*
Zaliczenie	Aktywność na zajęciach laboratoryjnych	0,2
	Sprawozdania z laboratorium	0,8
Zaliczenie	Ocena za aktywność na zajęciach	0,2
	Ocena z kolokwium	0,8

VIII.	**LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA**
	OBOWIĄZKOWA
1.	E. Nemeth, G. Snyder, T. R. Hein, B. Whaley, D. Mackin, Unix i Linux. Przewodnik administratora systemów. Wydanie V, Helion, 2018
2.	B. Ward, Jak działa Linux: podręcznik administratora, Helion, 2015
3.	Ł. Sosna, Linux. Komendy i polecenia. Wydanie VI, Wydawnictwo Helion 2022
	UZUPEŁNIAJĄCA
1.	M. Ebrahim, A. Mallett, Skrypty powłoki systemu Linux. Zagadnienia zaawansowane. Wydanie II, Helion, Gliwice 2019
2.	Pablo Iranzo Gómez, Pedro Ibánez Requena, Miguel Pérez Colino, Scott McCarty, Red Hat Enterprise Linux 9 Administration. A comprehensive Linux system administration guide for RHCSA certification exam candidates - Second Edition, Wydawnictwo Packt Publishing 2022
3.	Eric McLeroy, Red Hat Certified Specialist in Services Management and Automation EX358 Exam Guide, Wydawnictwo Packt Publishing 2022

IX.	**PROWADZĄCY PRZEDMIOT**
Stopień, Imię i nazwisko	kmdr por. dr inż. Adam Stojałowski
adres e-mail	a.stojalowski@amw.gdynia.pl

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:	**Cyberbezpieczeństwo**	*Kod*:	**Lxc**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Niestacjonarne		
Kształcenie w zakresie:	Cyberbezpieczeństwo		
Profil:	Ogólnoakademicki		
Liczba ECTS:	4		
Semestr:	IV		
Wymagania wstępne:			
Język wykładowy:	Polski		
Cel przedmiotu:	**C01**	zwiększenie świadomości użytkowników cyberprzestrzeni w zakresie metod i środków bezpieczeństwa w cyberprzestrzeni.	
	C02	propagowanie powszechnej oraz specjalistycznej edukacji społecznej w zakresie bezpieczeństwa cyberprzestrzeni RP	
	C03	uwrażliwienie na zagrożenia płynące z cyberprzestrzeni	

II.	**EFEKTY UCZENIA SIĘ**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Lxc_W01**	Zna podstawową terminologię związaną z problematyką zajęć. Posiada wiedzę o podstawowych regulacjach prawnych (polskich i międzynarodowych) w zakresie bezpieczeństwa w cyberprzestrzeni	kolokwium
	Lxc_W02	Posiada wiedzę na temat standardów i norm obowiązujących w jednostkach sektora publicznego i prywatnego w zakresie bezpieczeństwa w cyberprzestrzeni	Test sprawdzający podczas zajęć, praca domowa
	Lxc_W03	Posiada wiedzę na temat znaczenia, roli i kompetencji instytucji odpowiadających za bezpieczeństwo w cyberprzestrzeni, ich wzajemnych zależności w strukturach państwowych i międzynarodowych	praca pisemna podczas zajęć
	Lxc_W04	Posiada wiedzę na temat znaczenia, roli i kompetencji osób administrujących bezpieczeństwem w cyberprzestrzeni	Test sprawdzający podczas zajęć, praca domowa
Umiejętności:	**Lxc_U01**	Potrafi identyfikować zagrożenia dla bezpieczeństwa w cyberprzestrzeni	kolokwium
	Lxc_U02	Posiada umiejętność określenia, analizowania i proponowania rozwiązań dla konkretnych zagadnień związanych z obszarem ochrony bezpieczeństwa w cyberprzestrzeni w instytucjach państwowych i prywatnych	praca pisemna podczas zajęć
	Lxc_U03	Potrafi prognozować zagrożenia cyberprzestrzeni	praca pisemna podczas zajęć

Kompetencje społeczne:	**Lxc_K01**	Potrafi dokonać prawidłowej oceny systemu norm i reguł porządkujących system zarządzania bezpieczeństwem w cyberprzestrzeni.	wykonanie projektu
	Lxc_K02	Rozumie potrzebę uczenia się przez całe życie	odpowiedź tablicowa

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
W01	Wprowadzenie do problematyki zajęć (zakres, terminologia, akty prawne). Organizacja i funkcjonowanie systemu ochrony bezpieczeństwa w cyberprzestrzeni w RP, UE, NATO.	1
W02	Modele cyberprzestrzeni: określenie obszaru cyberprzestrzeni człowieka i państwa	1
W03	Prawne aspekty definiowania cyberprzestrzeni i zagrożeń w cyberprzestrzeni	1
W04	Źródła zagrożeń w cyberprzestrzeni. Charakterystyka cyberprzestępczości. Prognozy cyberprzestępczości	1
W05	Środki i metody ataków w cyberprzestrzeni	2
W06	Zagrożenia płatności i bankowości elektronicznych	2
W07	Organizacja „systemu" zwalczania cyberprzestępczości	2
L01	Ustalanie powiązań oraz tożsamości w Internecie	10
L02	Zabezpieczanie i analiza pozyskanego materiału	5
C01	Zasady i metody wyszukiwania informacji o zagrożeniach w Internecie	5

IV.	**KORELACJA EFEKTÓW UCZENIA SIĘ**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyk PRK*
W01	Lxc_W01, Lxc_W02, Lxc_W03, Lxc_W04	SIB2_W01, SIB2_W02	P7U_W, P7S_WG, P7S_WK
W02	Lxc_W01, Lxc_W02, Lxc_W03, Lxc_W04	SIB2_W01, SIB2_W02	P7U_W, P7S_WG, P7S_WK
W03	Lxc_W01, Lxc_W02, Lxc_W03, Lxc_W04	SIB2_W01, SIB2_W02	P7U_W, P7S_WG, P7S_WK
W04	Lxc_W01, Lxc_W02, Lxc_W03, Lxc_W04	SIB2_W01, SIB2_W02	P7U_W, P7S_WG, P7S_WK
W05	Lxc_W01, Lxc_W02, Lxc_W03, Lxc_W04	SIB2_W01, SIB2_W02	P7U_W, P7S_WG, P7S_WK
C01	Lxc_U01, Lxc_U02, Lxc_U03, Lxc_K01, Lxc_K02	SIB2_U01, SIB2_U02, SIB2_U04, SIB2_U07, SIB2_K01, SIB2_K02, SIB2_K04	P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK, P7S_KR
L01	Lxc_U01, Lxc_U02, Lxc_U03, Lxc_K01, Lxc_K02	SIB2_U01, SIB2_U02, SIB2_U04, SIB2_U07, SIB2_K01, SIB2_K02, SIB2_K04	P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK, P7S_KR
L02	Lxc_U01, Lxc_U02, Lxc_U03, Lxc_K01, Lxc_K02	SIB2_U01, SIB2_U02, SIB2_U04, SIB2_U07, SIB2_K01, SIB2_K02, SIB2_K04	P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK, P7S_KR
L03	Lxc_U01, Lxc_U02, Lxc_U03, Lxc_K01, Lxc_K02	SIB2_U01, SIB2_U02, SIB2_U04, SIB2_U07, SIB2_K01, SIB2_K02, SIB2_K04	P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK, P7S_KR

V.	**NAKŁAD PRACY STUDENTA**			
Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**10**	**X**	**105**	**4**

Ćwiczenia	**5**			
Seminaria				
Laboratoria	**15**			
Konsultacje (zaliczenie nieobecności, rozliczenie rygorów, poprawy)	**5**			
Przygotowanie do ćwiczeń	**X**	**20**		
Opanowanie informacji		**25**		
Przygotowanie do rozliczenia rygorów		**25**		
RAZEM	**35**	**70**		

VI.	**METODY DYDAKTYCZNE**
1.	Wykład interaktywny z prezentacją multimedialną
2	Ćwiczenia audytoryjne: symulacja zagrożeń, projekt praktyczny
3	Ćwiczenia audytoryjne: praca w grupach

VII.	**FORMA ZALICZENIA PRZEDMIOTU**	
Rygor	*Kryteria składowe*	*Waga*
Zaliczenie	Kolokwium - Test nabytej wiedzy	0,5
	Projekt	0,25
	Rozwiązanie zadań	0,25

VIII.	**LITERATURA**
	OBOWIĄZKOWA
1.	B. Hołyst, J. Pomykała, *Cyberprzestępczość i ochrona informacji*, Wydawnictwo WSM, 2012 r.
2.	J. Kosiński, *Paradygmaty cyberprzestępczości*, Warszawa 2015
3.	*Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa*, Dz.U. 2018 poz. 1560
4.	*Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii*, 32016L1148
5.	K. Liedel, *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*, Toruń 2005
	UZUPEŁNIAJĄCA
1.	*Strategia Rozwoju Systemu Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2022*, BBN 2013
2.	*Informacja o wynikach kontroli. Realizacja przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni RP*, NIK 2015
3.	G. Szpor, CH Beck, *Ochrona wolności, własności i bezpieczeństwa*, 2011 r.

IX.	**PROWADZĄCY PRZEDMIOT**
Stopień, Imię i nazwisko	dr hab. Jerzy KOSIŃSKI, prof. AMW
adres e-mail	j.kosinski@amw.gdynia.pl

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:	**Prognozowanie cyberzagrożeń**	*Kod*:	**Lcp**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Nietacjonarne		
Kształcenie w zakresie:	Cyberbezpieczeństwo		
Profil:	Ogólnoakademicki		
Liczba ECTS:	4		
Semestr:	4		
Wymagania wstępne:	Podstawowa znajomość wektorów ataków oraz technik mitygacji, utwardzania i audytowania systemów IT		
Język wykładowy:	Polski		
Cel przedmiotu:	**C01**	Zapoznanie z teorią oraz metodą oceny ryzyka w cyberprzestrzeni.	
	C02	Zapoznanie z metodami prognozowania zagrożeń w cyberprzestrzeni.	
	C03	Zaprezentowanie nowoczesnych technologii do oceny ryzyka oraz prognozowania.	

II.	**EFEKTY UCZENIA SIĘ**	
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Lcp_W01**	Zna problematykę cyberbezpieczeństwa, metod oceny ryzyka w cyberprzestrzeni oraz zna podstawowe zagrożenia bezpieczeństwa informacji.	Egzamin
	Lcp_W02	Zna podstawy bezpieczeństwa systemów teleinformatycznych, mechanizmy bezpieczeństwa wykorzystywane w systemach teleinformatycznych.	Egzamin
	Lcp_W03	Zna podstawowe techniki kryptografii oraz ma wiedzę z zakresu bezpieczeństwa wirtualizacji.	Egzamin
	Lcp_W04	Posiada wiedzę z zakresu ocena ryzyka i prognozowanie cyberzagrożeń.	Egzamin
	Lcp_W05	Posiada wiedzę z zakresu inżynierii systemów i analiza systemowej.	Egzamin
	Lcp_W06	Posiada wiedzę z zakresu planowania operacji w cyberprzestrzeni.	Egzamin
Umiejętności:	**Lcp_U01**	Potrafi przeprowadzić ocenę ryzyka w cyberprzestrzeni oraz wskazać zagrożenia bezpieczeństwa informacji.	Zadania laboratoryjne
	Lcp_U02	Potrafi wykorzystywać metody i techniki zabezpieczenia informacji w systemach i sieciach teleinformatycznych.	Zadania laboratoryjne
	Lcp_U03	Potrafi analizować dane z zakresu bezpieczeństwa i obronności.	Zadania laboratoryjne
	Lcp_U04	Potrafi oceniać ryzyko i prognozować cyberzagrożenia w systemach i sieciach teleinformatycznych	Zadania laboratoryjne

	Lcp_U05	Zna język angielski w zakresie słownictwa specjalistycznego na poziomie gwarantującym poprawne posługiwanie się dokumentacją techniczną oraz komunikatywność.	Zadania laboratoryjne
Kompetencje społeczne:	**Lcp_K01**	Posiada umiejętność w dążeniu do opanowania nawyków w sprawnym wykonywaniu obowiązków i czynności służbowych podczas realizacji zadań w różnorodnych warunkach w czasie pokoju, kryzysu i wojny	Praca w grupach
	Lcp_K02	Ma świadomość odpowiedzialnego pełnienia ról zawodowych w ramach zadań realizowanych przez SZ RP, z uwzględnieniem zmieniających się potrzeb społecznych, a w szczególności w zakresie rozwijania dorobku kryptologii i cyberbezpieczeństwa.	Praca w grupach
	Lcp_K03	Dostrzega znaczenie wiedzy w zakresie rozwiązywania problemów zabezpieczenia technicznego i wprowadzania nowych rozwiązań oraz docenia znaczenie samodzielnego poszerzania wiedzy i umiejętności	Praca w grupach

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
W01	Charakterystyka Cyberzagrożeń	1
W02	Teoretyczne aspekty prognozowania	1
W03	Klasyfikacja prognoz	1
W04	Etapy prognozowania	1
W05	Reguły prognozowania	1
W06	Prognozowanie strukturalne	1
W07	Prognozowanie niestrukturalne	1
W08	Prognozy ex post i ex ante	1
W09	Metody prognozowania przyczynowo-skutkowego	1
W10	Ocena trafności prognozy	1
C01	Sformułowanie zadania prognostycznego	1
C02	Określenie przesłanek prognostycznych	1
C03	Wybór danych gromadzonych na potrzeby budowy prognoz	1
C04	Zebranie danych prognostycznych	1
C05	Statystyczna obróbka danych prognostycznych	1
C06	Analiza danych prognostycznych	1
C07	Transformacja danych	1
C08	Agregacja danych	1
C09	Uzupełnianie brakujących danych	1
C10	Wybór metody prognozowania	1
C11	Budowa modelu prognostycznego	2
C12	Scenariusze	1
C13	Gra decyzyjna wykorzystywana w prognozowaniu	2
C14	Burza mózgów	1
C15	Ocena dokładności prognozy	1
C16	Ocena trafności prognozy	2

C17	Zaliczenie		1
IV.	**KORELACJA EFEKTÓW UCZENIA SIĘ**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyk PRK*
W01	Lcp_W01, Lcp_W02, Lcp_W03, Lcp_K01	SIB2_W01, SIB2_W02, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W02	Lcp_W01, Lcp_W02, Lcp_W03, Lcp_K01	SIB2_W01, SIB2_W02, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W03	Lcp_W01, Lcp_W02, Lcp_W03, Lcp_K01	SIB2_W01, SIB2_W02, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W04	Lcp_W01, Lcp_W02, Lcp_W04, Lcp_K01	SIB2_W01, SIB2_W02, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W05	Lcp_W01, Lcp_W04, Lcp_W05, Lcp_K01	SIB2_W01, SIB2_W02, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W06	Lcp_W01, Lcp_W02, Lcp_W03, Lcp_K01	SIB2_W01, SIB2_W02, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W07	Lcp_W01, Lcp_W02, Lcp_W03, Lcp_K01	SIB2_W01, SIB2_W02, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W08	Lcp_W01, Lcp_W02, Lcp_W04, Lcp_K01	SIB2_W01, SIB2_W02, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W09	Lcp_W01, Lcp_W05, Lcp_W06, Lcp_K01	SIB2_W01, SIB2_W02, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W10	Lcp_W01, Lcp_W02, Lcp_W06, Lcp_K01	SIB2_W01, SIB2_W02, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
C01	Lcp_W03, Lcp_U01, Lcp_U02, Lcp_K01	SIB2_W01, SIB2_U01, SIB2_U05, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK
C02	Lcp_W03, Lcp_U01, Lcp_U02, Lcp_K01	SIB2_W01, SIB2_U01, SIB2_U05, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK
C03	Lcp_W03, Lcp_U01, Lcp_U02, Lcp_K01	SIB2_W01, SIB2_U01, SIB2_U05, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK
C04	Lcp_W03, Lcp_U01, Lcp_U02, Lcp_K01	SIB2_W01, SIB2_U01, SIB2_U05, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK
C05	Lcp_W03, Lcp_U01, Lcp_U03, Lcp_K01	SIB2_W01, SIB2_U01, SIB2_U05, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK
C06	Lcp_W03, Lcp_U01, Lcp_U03, Lcp_K01	SIB2_W01, SIB2_U01, SIB2_U05, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK
C07	Lcp_W03, Lcp_U01, Lcp_U04, Lcp_K01	SIB2_W01, SIB2_U01, SIB2_U05, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK
C08	Lcp_W03, Lcp_U01, Lcp_U02, Lcp_U05, Lcp_K01	SIB2_W01, SIB2_U01, SIB2_U05, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK
C09	Lcp_W03, Lcp_U01, Lcp_U02, Lcp_U05, Lcp_K01	SIB2_W01, SIB2_U01, SIB2_U05, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK
C10	Lcp_W03, Lcp_U01, Lcp_U02, Lcp_U05, Lcp_K01	SIB2_W01, SIB2_U01, SIB2_U05, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK
C11	Lcp_W05, Lcp_U01, Lcp_U05, Lcp_K01	SIB2_W01, SIB2_U01, SIB2_U05, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK
C12	Lcp_W05, Lcp_U01, Lcp_U04, Lcp_K01	SIB2_W01, SIB2_U01, SIB2_U05, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK

C13	Lcp_W04, Lcp_U01, Lcp_U05, Lcp_U05, Lcp_K01	SIB2_W01, SIB2_U01, SIB2_U05, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK
C14	Lcp_W03, Lcp_U01, Lcp_U02, Lcp_U05, Lcp_K01	SIB2_W01, SIB2_U01, SIB2_U05, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK
C15	Lcp_W03, Lcp_U01, Lcp_U02, Lcp_U05, Lcp_K01	SIB2_W01, SIB2_U01, SIB2_U05, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK
C15	Lcp_W03, Lcp_U01, Lcp_U02, Lcp_K01	SIB2_W01, SIB2_U01, SIB2_U05, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK
C16	Lcp_W03, Lcp_U01, Lcp_U04, Lcp_K01	SIB2_W01, SIB2_U01, SIB2_U05, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7U_K, P7S_KK

V. NAKŁAD PRACY STUDENTA

Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**10**		**105**	**4**
Ćwiczenia	**20**			
Seminaria				
Konwersatoria				
Konsultacje	**5**			
Rozliczenie rygorów przedmiotu	**1**			
Przygotowanie do ćwiczeń		**20**		
Wykonanie zadań domowych		**25**		
Przygotowanie do rozliczenia rygorów		**25**		
RAZEM	**36**	**70**		

VI. METODY DYDAKTYCZNE

1. Wykłady z prezentacjami multimedialnymi
2. Ćwiczenia na stanowiskach komputerowych

VII. FORMA ZALICZENIA PRZEDMIOTU

Rygor	*Kryteria składowe*	*Waga*
Egzamin	Egzamin	0,8
	Ocena z ćwiczeń	0,2

VIII. LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

OBOWIĄZKOWA

1. B. Guzik, D. Appenzeller, W. Jurek: Prognozowanie i symulacje. Wybrane zagadnienia. MD 153 lub 168, AE Poznań
2. M. Cieślak (red.): Prognozowanie gospodarcze. Metody i zastosowania. PWN, Warszawa 2001
3. M. Anholcer, H. Gaspars, A. Owczarkowski: Przykłady i zadania z badań operacyjnych i ekonometrii, MD 163, AE Poznań
4. Tetlock Philip E., Gardner Dan, Superprognozowanie. Sztuka i nauka prognozowania, CeDeWu Sp. z o.o., Warszawa 2016

UZUPEŁNIAJĄCA

1. Maciąg A., Pietroń R., Kukla S., Prognozowanie i symulacja w Przedsiębiorstwie, PWE, Warszawa 2013
2. Gajda B., Prognozowanie i symulacje w ekonomii i zarządzaniu, C.H. Beck, Warszawa 2017
3. Dittmann P., Dittmann I., A. Szpulak, E. Szabela - Pasierbińska, Prognozowanie w zarządzaniu przedsiębiorstwem, Wolters Kluwer Polska, Warszawa 2012
4. Dittmann P., Prognozowanie w przedsiębiorstwie. Metody i ich zastosowania, Oficyna Ekonomiczna, Kraków 2004
5. Cieślak M. (red.), Nieklasyczne Metody Prognozowania, PWN, Warszawa1983
6. Sułek M., Prognozowanie i symulacje międzynarodowe, PWN, Warszawa 2010
7. Świeboda H., Prognozowanie zagrożeń bezpieczeństwa narodowego Rzeczpospolitej Polskiej, ASzWoj, Warszawa 2017

IX. PROWADZĄCY PRZEDMIOT

Stopień, Imię i nazwisko	dr Robert Janczewski
adres e-mail	r.janczewski@amw.gdynia.pl

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:	**Symulacja komputerowa**	*Kod*:	**Oku**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Niestacjonarne		
Kształcenie w zakresie:	Cyberbezpieczeństwo		
Profil:	Ogólnoakademicki		
Liczba ECTS:	4		
Semestr:	4		
Wymagania wstępne:	Technologia informacyjna, Podstawy statystyki, Architektura systemów i sieci komputerowych		
Język wykładowy:	Polski		
Cel przedmiotu:	**C01**	Zapoznanie studentów z narzędziami, metodami, technikami symulacyjnymi.	
	C02	Ćwiczenie elementów projektowania, modelowania i symulacji.	
	C03	Prezentacja wybranych symulatorów jako przykładów praktycznego zastosowania symulacji komputerowej.	

II.	**EFEKTY UCZENIA SIĘ**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Oku_W01**	Zna podstawowe zagadnienia związane z projektowaniem, modelowaniem i symulacją, w tym rodzaje zespołów projektowych, otoczenie bliższe i dalsze projektów cele modelowania, rodzaje i zmienne modeli, cele, rodzaje, warunki, wady i zalety symulacji.	test
	Oku_W02	Zna poszczególne etapy analizy symulacyjnej.	test
	Oku_W03	Ma podstawową wiedzę w zakresie wybranych symulacji.	test
Umiejętności:	**Oku_U01**	Potrafi omówić poszczególne etapy analizy symulacyjnej.	test
	Oku_U02	Posiada umiejętność zbierania i analizy danych wejściowych.	test
	Oku_U03	Potrafi omówić i wskazać przykłady praktycznego zastosowania symulacji komputerowych.	praca na symulatorach
Kompetencje społeczne:	**Oku_K01**	Posiada umiejętność praktycznego wykorzystania wybranych symulatorów.	praca na symulatorach
	Oku_K02	Potrafi efektywnie pracować i współdziałać w różnych grupach eksperckich i strukturach roboczych.	praca pisemna
	Oku_K03	W oparciu o uzyskaną teoretyczną wiedzę programową potrafi samodzielnie aktualizować i doskonalić swoją wiedzę i umiejętności praktyczne w zakresie symulacji komputerowej.	test

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

W01	**Wprowadzenie do symulacji i modelowania** (pojęcie projektu, modelu, symulacji, zmienne modeli, rodzaje zespołów projektowych, modeli symulacji, cele, wady, zalety i błędy symulacji, wybrane zastosowania symulacji).	2
W02	**Analiza symulacyjna** (sformułowanie problemu, zebranie i analiza danych, budowa modelu matematycznego, opracowanie programu komputerowego, walidacja i weryfikacja modelu, projektowanie układu eksperymentów, analiza wyników).	2
W03	**Zbieranie i analiza danych wejściowych** (sztuka zbierania danych, metoda reprezentacyjna, w tym etapy stosowania, podstawowe schematy losowania, parametryzacja podstawowych rozkładów ciągłych i dyskretnych).	2
W04	**Weryfikacja i walidacja modelu** (podstawowe definicje, zasady procesu weryfikacji i walidacji modelu, techniki walidacji i weryfikacji).	2
W05	**Planowanie eksperymentów symulacyjnych i analiza wyników** (aspekty planowania eksperymentów, metody redukcji wariancji, merytoryczne projektowanie układu eksperymentów, analiza statystyczna wyników).	2
L01	Symulator zdarzeń kryzysowych.	4
L02	Symulacje open-source w środowisku komputerowym	4
L03	Symulator mostka nawigacyjnego.	4
L04	Symulator strzelecki ŚNIEŻNIK.	4
L05	Symulatory i trenażery uzbrojenia okrętowego.	4

IV.	**KORELACJA EFEKTÓW UCZENIA SIĘ**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyk PRK*
W01	Oku_W01, Oku_W02, Oku_W03	SIB2_W01	P7U_W, P7S_WG
W02	Oku_W01, Oku_W02, Oku_W03	SIB2_W01	P7U_W, P7S_WG
W03	Oku_W01, Oku_W02, Oku_W03	SIB2_W01	P7U_W, P7S_WG
W04	Oku_W01, Oku_W02, Oku_W03	SIB2_W01	P7U_W, P7S_WG
W05	Oku_W01, Oku_W02, Oku_W03	SIB2_W01	P7U_W, P7S_WG
L01	Oku_U01, Oku_U02, Oku_U03, Oku_K01, Oku_K02, Oku_K03	SIB2_U01, SIB2_U06, SIB2_K01, SIB2_K05	P7U_U, P7S_UW, P7S_UO, P7U_K, P7S_KK, P7S_KR
L02	Oku_U01, Oku_U02, Oku_U03, Oku_K01, Oku_K02, Oku_K03	SIB2_U01, SIB2_U06, SIB2_K01, SIB2_K05	P7U_U, P7S_UW, P7S_UO, P7U_K, P7S_KK, P7S_KR
L03	Oku_U01, Oku_U02, Oku_U03, Oku_K01, Oku_K02, Oku_K03	SIB2_U01, SIB2_U06, SIB2_K01, SIB2_K05	P7U_U, P7S_UW, P7S_UO, P7U_K, P7S_KK, P7S_KR
L04	Oku_U01, Oku_U02, Oku_U03, Oku_K01, Oku_K02, Oku_K03	SIB2_U01, SIB2_U06, SIB2_K01, SIB2_K05	P7U_U, P7S_UW, P7S_UO, P7U_K, P7S_KK, P7S_KR
L05	Oku_U01, Oku_U02, Oku_U03, Oku_K01, Oku_K02, Oku_K03	SIB2_U01, SIB2_U06, SIB2_K01, SIB2_K05	P7U_U, P7S_UW, P7S_UO, P7U_K, P7S_KK, P7S_KR

V.	**NAKŁAD PRACY STUDENTA**			
Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**10**	**X**	**105**	**4**
Ćwiczenia	**0**			
Seminaria	**0**			
Laboratoria	**20**			
Konsultacje (zaliczenie nieobecności, rozliczenie rygorów, poprawy)	**5**			
Przygotowanie do ćwiczeń	**X**	**25**		
Opanowanie informacji		**20**		
Przygotowanie do rozliczenia rygorów		**25**		

RAZEM		35	70		
VI.	**METODY DYDAKTYCZNE**				
1.	prezentacja multimedialna				
2	wybrane symulatory				
3	praca w grupach i inne formy aktywizujące				
VII.	**FORMA ZALICZENIA PRZEDMIOTU**				
Rygor	*Kryteria składowe*			*Waga*	
Zaliczenie	wykonanie określonych ćwiczeń na symulatorach			0,4	
	test komputerowy			0,6	
VIII.	**LITERATURA**				
OBOWIĄZKOWA					
1.	G.S. Fishman, *Symulacja komputerowa. Pojęcia i metody*, PWE Warszawa 1981.				
2.	J. B. Gajda, *Prognozowanie i symulacja a decyzje gospodarcze*, C.H.Beck Warszawa, 2001.				
3.	B. Mielczarek, *Modelowanie symulacyjne w zarządzaniu,* Wyd. Politechniki Wrocławskiej, Wrocław 2009.				
UZUPEŁNIAJĄCA					
1.	K. Krupa, *Modelowanie symulacja i prognozowanie. Systemy ciągłe*, WNT Warszawa, 2008.				
2.	M. Nowak, *Symulacja komputerowa w problemach decyzyjnych*, AE Katowice, 2007.				
3.	R. F. Barton, *Wprowadzenie do symulacji i gier*, WNT, Warszawa 1974.				
4.	*Instrukcje poszczególnych symulatorów.*				
IX.	**PROWADZĄCY PRZEDMIOT**				
Stopień, Imię i nazwisko	mgr inż. Karol Gazda, mgr inż. Łukasz Grzyb				
adres e-mail	k.gazda@amw.gdynia.pl, l.grzyb@amw.gdynia.pl				

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:	**Podstawy prawne cyberbezpieczeństwa**	*Kod*:	**Ccq**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Niestacjonarne		
Kształcenie w zakresie:	Cyberbezpieczeństwo		
Profil:	Ogólnoakademicki		
Liczba ECTS:	4		
Semestr:	4		
Wymagania wstępne:	Podstawowa wiedza z zakresu państwa i prawa		
Język wykładowy:	Polski		
Cel przedmiotu:	**C01**	Zapoznanie słuchaczy z najważniejszymi aktami prawnymi regulującymi problematykę cyberbezpieczeństwa w wymiarze krajowym.	
	C02	Zapoznanie słuchaczy z najważniejszymi aktami prawnymi regulującymi problematykę cyberbezpieczeństwa w wymiarze międzynarodowym.	

II.	**EFEKTY UCZENIA SIĘ**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Ccq_W01**	Posiada wiedzez zakresu prawa krajowego i międzynarodowego oraz norm postępowania w cyberprzestrzeni, wpływających na prawa i obowiązki państw na płaszczyźnie międzynarodowej	Kolowium/ dyskusja
Umiejętności:	**Oku_U01**	Umiejętność analizy krajowych i międzynarodowych aktów prawnych oraz norm z zakresu cyberbezpieczeństwa.	Kolowium/ dyskusja
	Oku_U02	Potrafi znaleźć legitymację do działań państw w cyberprzestrzeni	Kolowium/ dyskusja
Kompetencje społeczne:	**Oku_K01**	Potrafi dokonać subsumpcji normy prawnej w konkretnym stanie faktycznym	Obserwacja podczas zajęć
	Oku_K02	Przestrzega unormowań materialnych i proceduralnych krajowych oraz międzynarodowych dotyczących prowadzenia działań w cyberprzestrzeni	Obserwacja podczas zajęć
	Oku_K03	W oparciu o uzyskaną teoretyczną wiedzę programową potrafi samodzielnie aktualizować i doskonalić swoją wiedzę i umiejętności.	Obserwacja podczas zajęć

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
W01	Zasady poszanowania suwerenności terytorialnej.	3
W02	Zakaz interwencji w sprawy wewnętrzne; zakaz użycia siły.	3

W03	Zakaz przeciwdziałania wykorzystaniu własnego terytorium do czynności szkodliwych dla drugiego państwa (zasada dobrego sąsiedztwa); zasady przypisania cyberoperacji państwu.	3
W04	Naruszenie bezpieczeństwa informacyjnego systemów komputerowych w świetle konkretnych norm prawa międzynarodowego.	3
W05	Przepisy regulujące odpowiedzialność międzynarodową państwa za działania indywidualnych hakerów i grup hakerskich; prawne ramy operacji odwetowych; prawo do samoobrony przed napaścią zbrojną.	3
C01	Problemy z prawnym zdefiniowaniem pojęcia cyberprzestrzeń. Przegląd ustawodawstwa wybranych państw. Status prawny cyberprzestrzeni.	3
C02	Status prawny państw w cyberprzestrzeni. Prawa i obowiązki państw w cyberprzestrzeni.	3
C03	Regulacje międzynarodowe działań w cyberprzestrzeni	3
C04	Krajowa regulacja z zakresu cyberbezpieczeństwa.	3
C05	Unormowania dot. Przestępstw komputerowych	3

IV. KORELACJA EFEKTÓW UCZENIA SIĘ

Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyk PRK*
W01	Ccq_W01,	SIB2_W01	P7U_W, P7S_WG
W02	Ccq_W01,	SIB2_W01	P7U_W, P7S_WG
W03	Ccq_W01,	SIB2_W01	P7U_W, P7S_WG
W04	Ccq_W01,	SIB2_W01	P7U_W, P7S_WG
W05	Ccq_W01,	SIB2_W01	P7U_W, P7S_WG
C01	Ccq_U01, Ccq_U02, , Ccq_K01, Ccq_K02, Ccq_K03	SIB2_U01, SIB2_U06, SIB2_K01, SIB2_K05	P7U_U, P7S_UW, P7S_UO, P7U_K, P7S_KK, P7S_KR
C02	Ccq_U01, Ccq_U02, , Ccq_K01, Ccq_K02, Ccq_K03	SIB2_U01, SIB2_U06, SIB2_K01, SIB2_K05	P7U_U, P7S_UW, P7S_UO, P7U_K, P7S_KK, P7S_KR
C03	Ccq_U01, Ccq_U02, , Ccq_K01, Ccq_K02, Ccq_K03	SIB2_U01, SIB2_U06, SIB2_K01, SIB2_K05	P7U_U, P7S_UW, P7S_UO, P7U_K, P7S_KK, P7S_KR
C04	Ccq_U01, Ccq_U02, , Ccq_K01, Ccq_K02, Ccq_K03	SIB2_U01, SIB2_U06, SIB2_K01, SIB2_K05	P7U_U, P7S_UW, P7S_UO, P7U_K, P7S_KK, P7S_KR
C05	Ccq_U01, Ccq_U02, , Ccq_K01, Ccq_K02, Ccq_K03	SIB2_U01, SIB2_U06, SIB2_K01, SIB2_K05	P7U_U, P7S_UW, P7S_UO, P7U_K, P7S_KK, P7S_KR

V. NAKŁAD PRACY STUDENTA

Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**15**	**X**	**105**	**4**
Ćwiczenia	**15**			
Seminaria	**0**			
Laboratoria				
Konsultacje (zaliczenie nieobecności, rozliczenie rygorów, poprawy)	**5**			
Przygotowanie do ćwiczeń	**X**	**25**		
Opanowanie informacji		**25**		
Przygotowanie do rozliczenia rygorów		**20**		
RAZEM	**35**	**70**		

VI. METODY DYDAKTYCZNE

1.	prezentacja multimedialna
2	wybrane symulatory
3	praca w grupach i inne formy aktywizujące

VII. FORMA ZALICZENIA PRZEDMIOTU

Rygor	*Kryteria składowe*	*Waga*
Zaliczenie	wykonanie określonych zadań podczas ćwiczeń	0,4
	test	0,6

VIII.	LITERATURA
	OBOWIĄZKOWA
1.	Schmitt M.N., Tallinn Manual on the International law applicable to the cyber warfare, Cambridge 2013.
2.	Adamski A., Prawo karne komputerowe, Warszawa 2000..
	UZUPEŁNIAJĄCA
1.	Adamski A., Przestępczość w cyberprzestrzeni. Prawne środki przeciwdziałania zjawisku w Polsce na tle projektu Konwencji Rady Europy, Toruń 2001.
2.	Banasiński C., Rojszczak M. (red.), Cyberbezpieczeństwo, Warszawa 2020.
3.	Klimburg A., National Cyber Security. Framework Manual, NATO Cooperative Cyber Defence Centre of Excellence Tallin, Estonia 2012.

IX.	PROWADZĄCY PRZEDMIOT
Stopień, Imię i nazwisko	dr Alicja Żukowska
adres e-mail	a.zukowska@amw.gdynia.pl

3.9. Karty przedmiotów modułu kształcenia studiów niestacjonarnych w zakresie Analiza danych i informatyka śledcza – C

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:	**Pozyskiwanie i analiza danych z technologii bezzałogowych**	*Kod*:	**Wyn**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Niestacjonarne		
Kształcenie w zakresie:	Analiza danych i informatyka śledcza		
Profil:	Ogólnoakademicki		
Liczba ECTS:	5		
Semestr:	3		
Wymagania wstępne:	Brak		
Język wykładowy:	Polski z terminologią angielską		
Cel przedmiotu:	**C01**	Zapoznanie studentów z konstrukcjami, technikami budowy, komputerami, aparaturami i kontrolerami technologii bezzałogowych	
	C02	Zapoznanie studentów z metodami, technikami i narzędziami informatyki śledczej do pozyskiwania danych z technologii bezzałogowych	
	C03	Wykształcenie umiejętności analizy danych pozyskiwanych z technologii bezzałogowych.	

II.	**EFEKTY UCZENIA SIĘ**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Wyn_W01**	Student zna i rozumie budowę i zasadę działania bezzałogowych statków powietrznych, pojazdów lądowych i morskich.	Kolokwium
	Wyn_W02	Student zna metody, techniki i narzędzia do pozyskiwania danych z technologii bezzałogowych.	Kolokwium
	Wyn_W03	Student zna techniki i zasady analizowania pozyskanego materiału z technologii bezzałogowych	Kolokwium
Umiejętności:	**Wyn_U01**	Student potrafi pozyskiwać dane z urządzeń bezzałogowych zgodnie z etyką informatyki śledczej	Zadania na laboratorium / Kolokwium
	Wyn_U02	Student potrafi analizować i korelować pozyskane dane z urządzeń bezzałogowych	Zadania na laboratorium / Kolokwium
Kompetencje społeczne:	**Wyn_K01**	Student krytycznie ocenia posiadaną wiedzę i umiejętności z zakresu pozyskiwania danych z technologii bezzałogowych oraz potrafi je doskonalić	Zadania na laboratorium

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
W01	Budowa i zasada działania pojazdów bezzałogowych	4

W02	Komputery, aparatury, kontrolery i systemy telemetryczne technologii bezzałogowych	4
W03	Komunikacja pojazdów bezzałogowych	4
W04	Techniki pozyskiwania danych z urządzeń bezzałogowych	4
W05	Techniki analizy danych z pozyskanych urządzeń technologii bezzałogowych	4
C01	Analiza budowa i testowanie działania pojazdów bezzałogowych	4
C02	Analiza kontrolerów i komponentów zapisujących dane na pokładzie urządzeń bezzałogowych	4
C03	Testowanie komunikacji urządzeń bezzałogowych i analiza widma radiowego	4
C04	Pozyskiwanie danych z urządzeń bezzałogowych	4
C05	Analiza danych z pozyskanych urządzeń technologii bezzałogowych	4
L01	Analiza struktur i systemów plików na nośnikach pojazdów bezzałogowych	4
L02	Proces pozyskiwania danych z uszkodzonych urządzeń bezzałogowych	4
L03	Klasyfikacja danych	4
L04	Analiza narzędzi do informatyki śledczej pojazdów bezzałogowych	4
L05	Analiza LOGów odzyskanych z kontrolerów pojazdów bezzałogowych	4

IV.	**KORELACJA EFEKTÓW UCZENIA SIĘ**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyk PRK*
W01	Wyn_W01, Wyn _W02	SIB2_W01	P7U_W, P7S_WG
W02	Wyn_W01, Wyn _W02	SIB2_W01	P7U_W, P7S_WG
W03	Wyn_W01, Wyn _W02	SIB2_W01	P7U_W, P7S_WG
W04	Wyn_W01, Wyn _W02	SIB2_W01	P7U_W, P7S_WG
W05	Wyn_W01, Wyn _W02, Wyn_W03	SIB2_W01	P7U_W, P7S_WG
C01	Wyn_U01, Wyn_U02, Wyn_K01	SIB2_U01, SIB2_U06, K01	P7U_U, P7S_UW, P7S_UO, P7U_K, P7S_KK
C02	Wyn_U01, Wyn_U02, Wyn_K01	SIB2_U01, SIB2_U06, K01	P7U_U, P7S_UW, P7S_UO, P7U_K, P7S_KK
C03	Wyn_U01, Wyn_U02, Wyn_K01	SIB2_U01, SIB2_U06, K01	P7U_U, P7S_UW, P7S_UO, P7U_K, P7S_KK
C04	Wyn_U01, Wyn_U02, Wyn_K01	SIB2_U01, SIB2_U06, K01	P7U_U, P7S_UW, P7S_UO, P7U_K, P7S_KK
C05	Wyn_U01, Wyn_U02, Wyn_K01	SIB2_U01, SIB2_U06, K01	P7U_U, P7S_UW, P7S_UO, P7U_K, P7S_KK

V.	**NAKŁAD PRACY STUDENTA**			
Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**10**	**X**	**126**	**5**
Ćwiczenia	**20**			
Seminaria	**0**			
Laboratorium	**0**			
Konsultacje (zaliczenie nieobecności, rozliczenie rygorów, pOzoawy)	**6**			
Przygotowanie do ćwiczeń	**X**	**30**		
Opanowanie informacji		**30**		
Przygotowanie do rozliczenia rygorów		**30**		
RAZEM	**36**	**90**		

VI.	**METODY DYDAKTYCZNE**

1.	Wykład z prezentacjami multimedialnymi
2.	Praca z dokumentacją
3.	Laboratorium na stanowiskach komputerowych – praca indywidualna, praca w grupach

VII.	**FORMA ZALICZENIA PRZEDMIOTU**	
Rygor	*Kryteria składowe*	*Waga*
Egzamin	Kolokwium	0,5
	Ocena z laboratorium	0,5

VIII.	LITERATURA **PODSTAWOWA I UZUPEŁNIAJĄCA**
	OBOWIĄZKOWA
1.	Wiktor Wyszywacz, Drony Budowa, Loty, Przepisy
2.	William Oettinger, Informatyka śledcza. Gromadzenie, analiza i zabezpieczanie dowodów elektronicznych dla początkujących
	UZUPEŁNIAJĄCA
1.	

IX.	**PROWADZĄCY PRZEDMIOT**
Stopień, Imię i nazwisko	por. mgr Łukasz GRZYB
adres e-mail	l.grzyb@amw.gdynia.pl

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:	**Zastosowanie kryptologii w informatyce śledczej**	*Kod*:	
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Niestacjonarne		
Kształcenie w zakresie:	Analiza danych i informatyka śledcza		
Profil:	Ogólnoakademicki		
Liczba ECTS:	3		
Semestr:	3		
Wymagania wstępne:	Brak		
Język wykładowy:	Polski		
Cel przedmiotu:	**C01**	Zapoznanie studentów z podstawowymi technikami kryptologii wykorzystywanymi w informatyce śledczej.	
	C02	Zapoznanie studentów z praktycznym zastosowaniem metod kryptologicznych do analizy danych cyfrowych.	
	C03	Wykształcenie umiejętności rozwiązywania problemów kryptograficznych w kontekście śledztw informatycznych	

II.	**EFEKTY UCZENIA SIĘ**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Lju_W01**	Student zna i rozumie techniki kryptologii stosowane w informatyce śledczej.	Kolokwium
	Lju_W02	Student zna standardy i protokoły kryptograficzne wykorzystywane w analizie danych cyfrowych.	Kolokwium
	Lju_W03	Student rozumie zasady działania narzędzi kryptograficznych stosowanych w śledztwach cyfrowych.	Kolokwium
Umiejętności:	**Lju_U01**	Student potrafi zastosować techniki kryptologiczne do analizy danych zebranych podczas śledztwa.	Zadania na laboratorium
	Lju_U02	Student potrafi wykorzystywać narzędzia kryptograficzne do szyfrowania i deszyfrowania danych śledczych.	Zadania na laboratorium, kolokwium
Kompetencje społeczne:	**Lju_K01**	Student krytycznie ocenia posiadaną wiedzę i umiejętności z zakresu kryptologii oraz potrafi je doskonalić w kontekście śledztw informatycznych.	Zadania na laboratorium

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
W01	Wprowadzenie do kryptologii w informatyce śledczej	2
W02	Standardy i protokoły kryptograficzne	2
W03	Techniki szyfrowania i deszyfrowania danych	2
W04	Narzędzia kryptograficzne w śledztwach cyfrowych	2
W05	Praktyczne zastosowania kryptologii w analizie danych	2
L01	Szyfrowanie danych	2
L02	Deszyfrowanie danych	2
L03	Wykorzystanie narzędzi kryptograficznych	2

L04	Analiza danych śledczych	2
L05	Praktyczne studium przypadków	2

IV.	**KORELACJA EFEKTÓW UCZENIA SIĘ**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyk PRK*
W01	Lju_W01, Lju_W02, Lju _W03	SIB2_W01, SIB2_W02	P7U_W, P7S_WG, P7S_WK
W02	Lju_W01, Lju_W02, Lju _W03	SIB2_W01, SIB2_W02	P7U_W, P7S_WG, P7S_WK
W03	Lju_W01, Lju_W02, Lju _W03	SIB2_W01, SIB2_W02	P7U_W, P7S_WG, P7S_WK
W04	Lju_W01, Lju_W02, Lju _W03	SIB2_W01, SIB2_W02	P7U_W, P7S_WG, P7S_WK
W05	Lju_W01, Lju_W02, Lju _W03	SIB2_W01, SIB2_W02	P7U_W, P7S_WG, P7S_WK
L01	Lju_U01, Lju_U02, Lju_K01	SIB2_U01, SIB2_U02, SIB2_K01	P7U_U, P7S_UW, P7U_K, P7S_KK
L02	Lju_U01, Lju_U02, Lju_K01	SIB2_U01, SIB2_U02, SIB2_K01	P7U_U, P7S_UW, P7U_K, P7S_KK
L03	Lju_U01, Lju_U02, Lju_K01	SIB2_U01, SIB2_U02, SIB2_K01	P7U_U, P7S_UW, P7U_K, P7S_KK
L04	Lju_U01, Lju_U02, Lju_K01	SIB2_U01, SIB2_U02, SIB2_K01	P7U_U, P7S_UW, P7U_K, P7S_KK
L05	Lju_U01, Lju_U02, Lju_K01	SIB2_U01, SIB2_U02, SIB2_K01	P7U_U, P7S_UW, P7U_K, P7S_KK

V.	**NAKŁAD PRACY STUDENTA**			
Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**10**		**80**	**3**
Ćwiczenia	**10**			
Seminaria				
Konwersatoria				
Konsultacje	**5**			
Rozliczenie rygorów przedmiotu				
Przygotowanie do ćwiczeń		**20**		
Wykonanie zadań domowych		**20**		
Przygotowanie do rozliczenia rygorów		**15**		
RAZEM	**25**	**55**		

VI.	**METODY DYDAKTYCZNE**
1.	Wykład z prezentacjami multimedialnymi
2.	Praca z dokumentacją
3.	Laboratorium na stanowiskach komputerowych – praca indywidualna, praca w grupach

VII.	**FORMA ZALICZENIA PRZEDMIOTU**	
Rygor	*Kryteria składowe*	*Waga*
Zaliczenie	Kolokwium	0,5
	Ocena z laboratorium	0,5

VIII.	**LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA**
	OBOWIĄZKOWA
1.	Marcin Karbowski, Podstawy kryptografii. Wydanie III, Helion, Gliwice 2014
2.	Harlan Carvey, "Windows Forensic Analysis Toolkit", Syngress 2018
	UZUPEŁNIAJĄCA
1.	Christopher L.T. Brown, "Computer Evidence: Collection and Preservation", Charles River Media 2012
2.	Eoghan Casey, "Handbook of Digital Forensics and Investigation", Academic Press 2010

IX.	**PROWADZĄCY PRZEDMIOT**

Stopień, Imię i nazwisko	mgr inż. Kamil Szczepaniuk
adres e-mail	k.szczepaniuk@amw.gdynia.pl

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:	**Testy penetracyjne**	*Kod*:	**Mte**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Niestacjonarne		
Specjalność:	Analiza danych i informatyka śledcza		
Profil:	Ogólnoakademicki		
Liczba ECTS:	4		
Semestr:	3		
Wymagania wstępne:	brak		
Język wykładowy:	Polski z terminologią angielską		
Cel przedmiotu:	**C01**	Zapoznanie studentów z metodyką prowadzenia testów penetracyjnych systemów i usług informatycznych.	
	C02	Pozyskanie umiejętności związanych z wykrywaniem podatności w systemach teleinformatycznych.	
	C03	Pozyskanie umiejętności przygotowania oraz przeprowadzenia testu penetracyjnego w systemie Windows oraz systemie Linux.	

II.	**EFEKTY KSZTAŁCENIA**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Mte_ W01**	Zna i rozumie w pogłębiony sposób wybrane fakty, teorie, metody oraz złożone zależności między nimi, także w powiązaniu z innymi dziedzinami różnorodne, złożone uwarunkowania i aksjologiczny kontekst prowadzonej działalności z zakresu teorii bezpieczeństwa, cyberbezpieczeństwa oraz analizy danych i informatyki śledczej. Zna zasady i metody prowadzenia testów penetracyjnych w sieciach komputerowych.	Pytania sprawdzające podczas zajęć. Kolokwium.
	Mte_ W02	Zna i rozumie w pogłębiony sposób zagadnienia związane z bezpieczeństwem informacji oraz wykorzystaniem technologii informacyjnych. Zna zasady i metody prowadzenia testów pod kątem wyszukiwania podatności w systemach i sieciach teleinformatycznych	Rozwiązanie zadań problemowych
Umiejętności:	**Mte_ U01**	Potrafi wykorzystać posiadaną wiedzę z zakresu bezpieczeństwa, cyberbezpieczeństwa oraz formułować i rozwiązywać złożone i nietypowe problemy. Potrafi przygotować oraz przeprowadzić testy penetracyjne w sieciach komputerowych.	Przygotowanie sprawozdania. Kolokwium.
	Mte U02	Potrafi brać udział w debacie z zakresu wykorzystania systemów informacyjnych w bezpieczeństwie - przedstawiać i oceniać różne opinie i stanowiska oraz dyskutować o nich. Potrafi przeprowadzić testy penetracyjne w systemach i sieciach teleinformatycznych pod kątem wyszukiwania podatności z uwzględnieniem właściwej metody ich realizacji.	Przygotowanie sprawozdania. Kolokwium.

	Mte_U03	Potrafi posługiwać się językiem obcym na poziomie B2 Europejskiego Systemu Opisu Kształcenia Językowego ze szczególnym uwzględnienie specjalistycznej terminologii z zakresu wykorzystania systemów informacyjnych w bezpieczeństwie.	Wykonanie ćwiczenia
	Mte_U04	Potrafi samodzielnie planować i realizować własne uczenie się przez całe życie i ukierunkowywać innych w tym zakresie.	Przygotowanie sprawozdania. Kolokwium.
Kompetencje społeczne:	**Mte_K01**	Krytycznie ocenia posiadaną wiedzę i odbierane treści z zakresu teorii bezpieczeństwa, cyberbezpieczeństw oraz analizy danych i informatyki śledczej.	Przygotowanie do zajęć
	Mte_K02	Uznaje znaczenie wiedzy w rozwiązywaniu problemów badawczych i praktycznych oraz zasięga opinii ekspertów w przypadku trudności z samodzielnych rozwiazywaniem problemów dotyczących wykorzystania systemów informacyjnych w bezpieczeństwie	Przygotowanie do zajęć

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
W01	Zajęcia organizacyjne. Wprowadzenie do przedmiotu. Sprawy organizacyjne.	10 min
W02	System teleinformatyczny: Podstawowe definicje; Atrybuty bezpieczeństwa; Bezpieczeństwo systemu teleinformatycznego.	2
W03	Polityka bezpieczeństwa: Podstawowe definicje; Elementy bezpieczeństwa; Zarządzanie bezpieczeństwem; Przykładowa polityka bezpieczeństwa.	2
W04	Metodyka testów penetracyjnych: Definicja testów penetracyjnych; Rodzaje i opis metodyk (OSSTMM, PTES, NIST800-115, Metasploit, Core Impact, OWASP Web Security Testing Guide, Testy penetracyjne ukierunkowane na cel).	4
W05	Etapy testów penetracyjnych: Czynności wstępne; Rozpoznanie pasywne.	2
W06	Etapy testów penetracyjnych: Aspekty prawne; Rozpoznanie aktywne.	4
W07	Etapy testów penetracyjnych: Faza penetracji / ataku;	2
W08	Etapy testów penetracyjnych: Uzyskanie dostępu – eksploracja środowiska.	2
W09	Etapy testów penetracyjnych: Przygotowanie raportu.	2
L01	Realizacja etapów testów penetracyjnych: Czynności wstępne; Rozpoznanie pasywne.	4
L02	Realizacja etapów testów penetracyjnych: Aspekty prawne; Rozpoznanie aktywne.	4
L03	Realizacja etapów testów penetracyjnych: Faza penetracji / ataku;	4
L04	Realizacja etapów testów penetracyjnych: Uzyskanie dostępu – eksploracja środowiska.	4
L05	Realizacja etapów testów penetracyjnych: Przygotowanie raportu.	4
C01	Analiza pakietów ruchu sieciowego z wykorzystaniem programu WireShark – analizy przypadków	15

IV.	**KORELACJA EFEKTÓW KSZTAŁCENIA**		
Forma	*Kod efektu przedmiotu*	*Kod symbolu*	*Kod charakterystyk PRK*
W01	Mte_W01, Mte_W02	SIB2_W01, SIB2_W02,	P7U_W, P7S_WG, P7S_WK,

	Mte_K01, Mte_K02	SIB2_K01, SIB2_K02	P7U_K, P7S_KK
W02	Mte_W01, Mte_W02 Mte_K01, Mte_K02	SIB2_W01, SIB2_W02, SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W03	Mte_W01, Mte_W02 Mte_K01, Mte_K02	SIB2_W01, SIB2_W02, SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W04	Mte_W01, Mte_W02 Mte_K01, Mte_K02	SIB2_W01, SIB2_W02, SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W05	Mte_W01, Mte_W02 Mte_K01, Mte_K02	SIB2_W01, SIB2_W02, SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W06	Mte_W01, Mte_W02 Mte_K01, Mte_K02	SIB2_W01, SIB2_W02, SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W07	Mte_W01, Mte_W02 Mte_K01, Mte_K02	SIB2_W01, SIB2_W02, SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W08	Mte_W01, Mte_W02 Mte_K01, Mte_K02	SIB2_W01, SIB2_W02, SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W09	Mte_W01, Mte_W02 Mte_K01, Mte_K02	SIB2_W01, SIB2_W02, SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
L01	Mte_W01, Mte_W02 Mte_U01, Mte_U02, Mte_U04, Mte_U04, Mte_K01, Mte_K02	SIB2_W01, SIB2_W02, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07, SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK P7U_U, P7S_UW, P7S_UK, P7S_UU P7U_K P7S_KK
L02	Mte_W01, Mte_W02 Mte_U01, Mte_U02, Mte_U04, Mte_U04, Mte_K01, Mte_K02	SIB2_W01, SIB2_W02, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07, SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK P7U_U, P7S_UW, P7S_UK, P7S_UU P7U_K P7S_KK
L03	Mte_W01, Mte_W02 Mte_U01, Mte_U02, Mte_U04, Mte_U04, Mte_K01, Mte_K02	SIB2_W01, SIB2_W02, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07, SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK P7U_U, P7S_UW, P7S_UK, P7S_UU P7U_K P7S_KK
L04	Mte_W01, Mte_W02 Mte_U01, Mte_U02, Mte_U04, Mte_U04, Mte_K01, Mte_K02	SIB2_W01, SIB2_W02, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07, SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK P7U_U, P7S_UW, P7S_UK, P7S_UU P7U_K P7S_KK
L05	Mte_W01, Mte_W02 Mte_U01, Mte_U02, Mte_U04, Mte_U04, Mte_K01, Mte_K02	SIB2_W01, SIB2_W02, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07, SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK P7U_U, P7S_UW, P7S_UK, P7S_UU P7U_K P7S_KK
C01	Mte_W01, Mte_W02 Mte_U01, Mte_U02, Mte_U04, Mte_U04, Mte_K01, Mte_K02	SIB2_W01, SIB2_W02, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07, SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK P7U_U, P7S_UW, P7S_UK, P7S_UU P7U_K P7S_KK

V.	**NAKŁAD PRACY STUDENTA**			
Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**10**		**110**	**4**
Laboratorium	**10**			
Ćwiczenia	**10**			
Konwersatoria				
Konsultacje	**3**			
Rozliczenie rygorów przedmiotu	**2**			
Przygotowanie do ćwiczeń i laboratorium	**x**	**25**		
Opanowanie informacji		**25**		
Przygotowanie do rozliczenia rygorów		**25**		
RAZEM	**35**	**75**		

VI.	METODY DYDAKTYCZNE
1.	Wykład z prezentacją multimedialną
2.	Praca przy stanowisku komputerowym
3.	Rozwiązywanie zadań problemowych
4.	Studiowanie literatury

VII. FORMA ZALICZENIA PRZEDMIOTU		
Rygor	*Kryteria składowe*	*Waga*
Zaliczenie	Ocena za aktywność na zajęciach	0,2
	Ocena z kolokwium	0,8
Zaliczenie	Aktywność na zajęciach laboratoryjnych	0,2
	Sprawozdania z laboratorium	0,8

VIII.	LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA
	OBOWIĄZKOWA
1.	Białas A., Bezpieczeństwo informacji i usług, Wydawnictwo Naukowo-Techniczne, Warszawa 2007;
2.	Khawaja G. Kali Linux i testy penetracyjne. Biblia. Wydawnictwo Helion, Gliwice 2022;
3.	Velu V. K., Kali Linux i zaawansowane testy penetracyjne. Zostań ekspertem cyberbezpieczeństwa za pomocą Metasploit, Nmap, Wireshark i Burp Suite. Wydanie IV., Wydawnictwo Helion, Gliwice 2023;
4.	Georgia W., Bezpieczny system w praktyce, Wyższa szkoła hackingu i testy penetracyjne, Wydawnictwo Helion, 2015;
5.	Kim P., Podręcznik pentestera. Bezpieczeństwo systemów informatycznych, Wydawnictwo Helion, Gliwice 2014;
6.	Tanner N. H., Blue Team i cyberbezpieczeństwo. Zestaw narzędzi dla specjalistów od zabezpieczenia sieci. Wydawnictwo Helion, Gliwice 2021;
	UZUPEŁNIAJĄCA
1.	Ustawa z dnia 16 lipca 2004r. Prawo telekomunikacyjne (Dz.U. 2004 Nr 171 poz. 1800, tekst ujednolicony);
2.	Ustawa z dnia 18 lipca 2002r. o świadczeniu usług drogą elektroniczną (Dz.U. 2002 Nr 144 poz. 1204, z późn. zm.);
3.	Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2018 r. poz. 1560, z 2019 r. poz. 2020, 2248);
4.	Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (Dz.U. 2020 poz. 1444, tekst jednolity);
5.	Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2017 poz. 2247, tekst jednolity);
6.	Rozporządzenie Rady Ministrów z dnia 11 września 2018 r. w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych;
7.	PN-13335-1, Technika informatyczna - Wytyczne do zarządzania bezpieczeństwem systemów informatycznych - Pojęcia i modele bezpieczeństwa systemów informatycznych, 1999;
8.	NIST National Institute of Standard and Technology - Special Publication 800-37, Revision 2. Risk Management Framework for Information Systems and Organizations, grudzień 2018;
9.	OSSTMM 3 The Open Source Security Testing Methodology Manual. Contemporary Security Testing and Analysis, Pete Herzog, ISECOM, grudzień 2010;

10.	Technical Guide to Information Security Testing and Assessment (SP 800-115). Recommendations of the National Institute of Standards and Technology, wrzesień 2008;	
11.	PTES Penetration Testing Execution Standard, http://www.pentest-standard.org;	
12.	OWASP The Open Web Application Security Project, https://owasp.org/;	
IX.	**PROWADZĄCY PRZEDMIOT**	
Stopień, Imię i nazwisko		kmdr por. dr inż. Adam Stojałowski
adres e-mail		a.stojalowski@amw.gdynia.pl

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:	**Bezpieczeństwo sieci komputerowych i bezprzewodowych**	*Kod*:	**Oxk**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Niestacjonarne		
Kształcenie w zakresie:	Analiza danych i informatyka śledcza		
Profil:	Ogólnoakademicki		
Liczba ECTS:	5		
Semestr:	3		
Wymagania wstępne:	Brak		
Język wykładowy:	Polski		
Cel przedmiotu:	**C01**	Zapoznanie studentów z zasadami działania sieci komputerowych, ich klasyfikacją i charakterystyką oraz urządzeniami sieciowymi i wykorzystywanymi mediami transmisyjnymi.	
	C02	Zapoznanie studentów z warstwową architekturą sieci oraz protokołami sieciowymi wykorzystywanymi do komunikacji hostów na poziomie poszczególnych warstw.	
	C03	Wykształcenie umiejętności podstawowej konfiguracji urządzeń sieciowych dla realizacji komunikacji z wykorzystaniem sieci komputerowej, obserwacji i analizy działania sieci oraz ruchu sieciowego, diagnozowania podstawowych nieprawidłowości w działaniu sieci komputerowych	

II.	**EFEKTY UCZENIA SIĘ**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Oxk_W01**	Student zna podstawowe urządzenia i standardy sieciowe oraz ich rolę w transmisji danych w sieciach lokalnych i rozległych o różnych topologiach.	Egzamin
	Oxk_W02	Student zna podstawowe modele warstwowe sieci oraz role poszczególne warstwy w procesie transmisji danych między hostami sieci.	Egzamin
	Oxk_W03	Student zna podstawowe protokoły transmisyjne i ich przyporządkowanie do warstwy na poziomie której są wykorzystywane.	Egzamin
Umiejętności:	**Oxk_U01**	Student potrafi zbudować i skonfigurować prostą sieć lokalną.	Egzamin, rozwiązywanie zadań
	Oxk_U02	Student potrafi analizować ruch sieciowy na podstawie danych sterujących poszczególnych warstw sieciowych	Egzamin, rozwiązywanie zadań
	Oxk_U03	Student potrafi łączyć sieci lokalne i konfigurować parametry routingu.	Egzamin, rozwiązywanie zadań
	Oxk_U04	Student potrafi zarządzać przychodzącym do sieci ruchem oraz podejmować działania zwiększające bezpieczeństwo sieci.	Egzamin, rozwiązywanie zadań

Kompetencje społeczne:	**Oxk_K01**	Student w oparciu o uzyskaną podstawową wiedzę z zakresu sieci teleinformatycznych potrafi doskonalić swoją wiedzę i umiejętności z tego obszaru.	Praca w grupach

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
W01	Klasyfikacja i ogólna charakterystyka sieci komputerowych.	2
W02	Warstwowe architektury sieciowe.	1
W03	Warstwa łącza danych, adresacja MAC, standard Ethernet.	1
W04	Protokoły warstwy sieciowej, adresacja IPv4 i IPv6	2
W05	Protokoły warstwy transportowej vs protokoły aplikacji.	1
W06	Zasady i rodzaje routingu.	1
W07	Bezpieczeństwo sieci bezprzewodowych. Ataki na sieci bezprzewodowe WLAN.	2
L01	Wyznaczanie adresu sieci i rozgłoszeniowego sieci na podstawie różnych klas adresów IP hostów, zapoznanie z programem Cisco Packet Tracer – budowa sieci LAN z serwerem DHCP.	3
L02	Protokół TCP, analiza faz zestawiania i rozłączania sesji w warstwie transportowej. Analiza nagłówka protokołu TCP i UDP	3
L03	Routing statyczny i dynamiczny, konfiguracja routerów, podgląd i analiza tablicy routingu, porównanie metryk trasowania oraz dystansu administracyjnego protokołów routingu	3
L04	Konfiguracja usługi NAT oraz analiza tablicy NAT w ustawieniach routera, analiza przesyłanych pakietów IP pod kątem tłumaczenia adresów i portów.	3
L05	Podstawy bezpieczeństwa w sieciach komputerowych. Konfiguracja reguł zapory sieciowej na serwerze oraz weryfikacja ich działania. Konfigurowanie sieci VPN – tunelowanie GRE i IPsec. Tworzenie sieci VLAN oraz zapewnienie transmisji danych między nimi (metoda „router na patyku”, wykorzystanie podinterfejsów routera).	3
L06	Podstawy bezpieczeństwa w sieciach bezprzewodowych. Konfiguracja i zarządzanie AP. Mechanizmy bezpieczeństwa wykorzystywane w sieciach bezprzewodowych.	5

IV.	**KORELACJA EFEKTÓW UCZENIA SIĘ**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyk PRK*
W01	Oxk_W01, Oxk_W02, Oxk_W03, Oxk_K01	SIB2_W01, SIB2_W02, SIB2_K01	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W02	Oxk_W01, Oxk_W02, Oxk_W03, Oxk_K01	SIB2_W01, SIB2_W02, SIB2_K01	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W03	Oxk_W01, Oxk_W02, Oxk_W03, Oxk_K01	SIB2_W01, SIB2_W02, SIB2_K01	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W04	Oxk_W01, Oxk_W02, Oxk_W03, Oxk_K01	SIB2_W01, SIB2_W02, SIB2_K01	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W05	Oxk_W01, Oxk_W02, Oxk_W03, Oxk_K01	SIB2_W01, SIB2_W02, SIB2_K01	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W06	Oxk_W01, Oxk_W02, Oxk_W03, Oxk_K01	SIB2_W01, SIB2_W02, SIB2_K01	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W07	Oxk_W01, Oxk_W02, Oxk_W03, Oxk_K01	SIB2_W01, SIB2_W02, SIB2_K01	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
L01	Oxk_W01, Oxk_U01, Oxk_U02, Oxk_U03, Oxk_U04, Oxk_K01	SIB2_W01, SIB2_U01 SIB2_U02, SIB2_K01	P7U_W, P7S_WG, P7U_U, P7S_UW, P7U_K, P7S_KK

L02	Oxk_W01, Oxk_U01, Oxk_U02, Oxk_U03, Oxk_U04, Oxk_K01	SIB2_W01, SIB2_U01 SIB2_U02, SIB2_K01	P7U_W, P7S_WG, P7U_U, P7S_UW P7U_K, P7S_KK
L03	Oxk_W01, Oxk_U01, Oxk_U02, Oxk_U03, Oxk_U04, Oxk_K01	SIB2_W01, SIB2_U01 SIB2_U02, SIB2_K01	P7U_W, P7S_WG, P7U_U, P7S_UW P7U_K, P7S_KK
L04	Oxk_W01, Oxk_U01, Oxk_U02, Oxk_U03, Oxk_U04, Oxk_K01	SIB2_W01, SIB2_U01 SIB2_U02, SIB2_K01	P7U_W, P7S_WG, P7U_U, P7S_UW P7U_K, P7S_KK
L05	Oxk_W01, Oxk_U01, Oxk_U02, Oxk_U03, Oxk_U04, Oxk_K01	SIB2_W01, SIB2_U01 SIB2_U02, SIB2_K01	P7U_W, P7S_WG, P7U_U, P7S_UW P7U_K, P7S_KK
L06	Oxk_W01, Oxk_U01, Oxk_U02, Oxk_U03, Oxk_U04, Oxk_K01	SIB2_W01, SIB2_U01 SIB2_U02, SIB2_K01	P7U_W, P7S_WG, P7U_U, P7S_UW P7U_K, P7S_KK

V. NAKŁAD PRACY STUDENTA

Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**10**		**126**	**5**
Ćwiczenia				
Seminaria				
Laboratoria	**20**			
Konsultacje	**5**			
Rozliczenie rygorów przedmiotu	**1**			
Przygotowanie do ćwiczeń		**30**		
Wykonanie zadań domowych		**30**		
Przygotowanie do rozliczenia rygorów		**30**		
RAZEM	**36**	**90**		

VI. METODY DYDAKTYCZNE

1. Metody podające: Wykłady z prezentacjami multimedialnymi
2. Metody aktywizujące: pogadanka, obserwacja, praca z dokumentacją, praca w grupach, case study.
3. Ćwiczenia na stanowiskach komputerowych

VII. FORMA ZALICZENIA PRZEDMIOTU

Rygor	*Kryteria składowe*	*Waga*
Zaliczenie	Ocena z kolokwium (materiał z wykładów)	0,4
	Ocena z ćwiczeń	0,6

VIII. LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

OBOWIĄZKOWA

1. Józefiok A., *Budowa sieci komputerowych na przełącznikach i routerach Cisco*, Helion, Gliwice 2013
2. Wrotek W., *Sieci komputerowe*, Helion, Gliwice 2016

UZUPEŁNIAJĄCA

1. Tanenbaum, Wetherall, Sieci komputerowe, Helion, Gliwice 2012
2. Kluczewski J., Bezpieczeństwo sieci komputerowych (ebook), Itstart, Piekary Śląskie 2019
3. Sportack M., Sieci komputerowe. Księga eksperta, Helion, Gliwice 2004

IX. PROWADZĄCY PRZEDMIOT

Stopień, Imię i nazwisko	mgr Grzegorz PIOTROWSKI
adres e-mail	grzegorz.piotrowski@c2o.eu

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:	**Techniki pozyskiwania cyfrowego materiału dowodowego**	*Kod*:	**Lkh**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Niestacjonarne		
Kształcenie w zakresie:	Analiza danych i informatyka śledcza		
Profil:	Ogólnoakademicki		
Liczba ECTS:	5		
Semestr:	4		
Wymagania wstępne:	Brak		
Język wykładowy:	Polski		
Cel przedmiotu:	**C01**	Zapoznanie studentów z zasadami zachowania łańcucha dowodowego.	
	C02	Zapoznanie studentów z technikami pozyskiwania cyfrowego materiału dowodowego z wykorzstaniem specjalistycznych narzędzi oraz oprogramowania.	
	C03	Wykształcenie umiejętności dopasowania właściwych technik pozyskiwania cyfrowego materiału dowodowego względem badanych urządzeń.	

II.	**EFEKTY UCZENIA SIĘ**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Lkh_W01**	Student zna podstawowe urządzenia i oprogramowanie oraz ich rolę w zapewnieniu integralności danych łańcucha dowodowego.	Egzamin
	Lkh_W02	Student zna podstawowe techiniki pozyskiwania cyfrowego materiału dowodowego.	Egzamin
	Lkh_W03	Student zna etapy akwizycji danych w odniesieniu do badanych urządzeń.	Egzamin
Umiejętności:	**Lkh_U01**	Student potrafi przygotować urządzenie do zabezpieczenia danych.	Egzamin, rozwiązywanie zadań
	Lkh_U02	Student potrafi dopasować narzędzia i techniki do badanego urządzenia.	Rozwiązywanie zadań
	Lkh_U03	Student potrafi przeprowadzić proces akwizycji danych.	Rozwiązywanie zadań
	Lkh_U04	Student potrafi zapewnić integralność danych na potrzeby zachowania łańcucha dowodowego.	Rozwiązywanie zadań
Kompetencje społeczne:	**Lkh_K01**	Student w oparciu o uzyskaną podstawową wiedzę z zakresu pozyskiwania cyfrowego materiału dowodowego potrafi doskonalić swoją wiedzę i umiejętności z tego obszaru.	Praca w grupach

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

W01	Klasyfikacja i ogólna charakterystyka urządzeń poddawanych badaniom śledczym.	2
W02	Narzędzia sprzętowe oraz oprogramowania do informatyki śledczej.	3
W03	Zasady zachowania łańcucha dowodowego.	3
W04	Klasyczne techniki pozyskiwania cyfrowego materiału dowodowego	3
W05	Alternatywen techniki pozyskiwania cyfrowego materiału dowodowego	3
W06	Analiza zgromadzonego materiału dowodowego	3
W07	Raportowanie wyników badań	3
L01	Przegląd i analiza typów urządzeń mogących przechowywać cyfrowy materiał dowodowy	8
L02	Narzędzia do pozyskiwania cyfrowego materiału dowodowego	5
L03	Oprogramowanie do pozyskiwania cyfrowego materiału dowodowego	5
L04	Techiniki do pozyskiwania cyfrowego materiału dowodowego z systemów Windows, Linux, MacOS	5
L05	Narzędzia do pozyskiwania cyfrowego materiału dowodowego z urządzeń mobilnych	7
L06	Analiza oraz raportowanie ujawnionego materiału dowodowego.	10

IV.	**KORELACJA EFEKTÓW UCZENIA SIĘ**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyk PRK*
W01	Lkh_W01, Lkh_W02, Lkh_W03, Lkh_K01	SIB2_W01, SIB2_W02, SIB2_K01	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W02	Lkh_W01, Lkh_W02, Lkh_W03, Lkh_K01	SIB2_W01, SIB2_W02, SIB2_K01	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W03	Lkh_W01, Lkh_W02, Lkh_W03, Lkh_K01	SIB2_W01, SIB2_W02, SIB2_K01	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W04	Lkh_W01, Lkh_W02, Lkh_W03, Lkh_K01	SIB2_W01, SIB2_W02, SIB2_K01	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W05	Lkh_W01, Lkh_W02, Lkh_W03, Lkh_K01	SIB2_W01, SIB2_W02, SIB2_K01	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W06	Lkh_W01, Lkh_W02, Lkh_W03, Lkh_K01	SIB2_W01, SIB2_W02, SIB2_K01	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W07	Lkh_W01, Lkh_W02, Lkh_W03, Lkh_K01	SIB2_W01, SIB2_W02, SIB2_K01	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
L01	Lkh_W01, Lkh_U01, Lkh_U02, Lkh_U03, Lkh_U04, Lkh_K01	SIB2_W01, SIB2_U01 SIB2_U02, SIB2_K01	P7U_W, P7S_WG, P7U_U, P7S_UW, P7U_K, P7S_KK
L02	Lkh_W01, Lkh_U01, Lkh_U02, Lkh_U03, Lkh_U04, Lkh_K01	SIB2_W01, SIB2_U01 SIB2_U02, SIB2_K01	P7U_W, P7S_WG, P7U_U, P7S_UW P7U_K, P7S_KK
L03	Lkh_W01, Lkh_U01, Lkh_U02, Lkh_U03, Lkh_U04, Lkh_K01	SIB2_W01, SIB2_U01 SIB2_U02, SIB2_K01	P7U_W, P7S_WG, P7U_U, P7S_UW P7U_K, P7S_KK
L04	Lkh_W01, Lkh_U01, Lkh_U02, Lkh_U03, Lkh_U04, Lkh_K01	SIB2_W01, SIB2_U01 SIB2_U02, SIB2_K01	P7U_W, P7S_WG, P7U_U, P7S_UW P7U_K, P7S_KK
L05	Lkh_W01, Lkh_U01, Lkh_U02, Lkh_U03, Lkh_U04, Lkh_K01	SIB2_W01, SIB2_U01 SIB2_U02, SIB2_K01	P7U_W, P7S_WG, P7U_U, P7S_UW P7U_K, P7S_KK
L06	Lkh_W01, Lkh_U01, Lkh_U02, Lkh_U03, Lkh_U04, Lkh_K01	SIB2_W01, SIB2_U01 SIB2_U02, SIB2_K01	P7U_W, P7S_WG, P7U_U, P7S_UW P7U_K, P7S_KK

V.	**NAKŁAD PRACY STUDENTA**			
Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**10**		**126**	**5**

Ćwiczenia	**5**			
Seminaria				
Laboratoria	**15**			
Konsultacje	**5**			
Rozliczenie rygorów przedmiotu	**1**			
Przygotowanie do ćwiczeń		**30**		
Wykonanie zadań domowych		**30**		
Przygotowanie do rozliczenia rygorów		**30**		
RAZEM	**36**	**90**		

VI.	**METODY DYDAKTYCZNE**
1.	Metody podające: Wykłady z prezentacjami multimedialnymi
2.	Metody aktywizujące: obserwacja, praca z dokumentacją, praca w grupach, case study.
3.	Ćwiczenia na stanowiskach komputerowych

VII.	**FORMA ZALICZENIA PRZEDMIOTU**	
Rygor	*Kryteria składowe*	*Waga*
Zaliczenie	Ocena z egzaminu (materiał z wykładów)	0,4
	Ocena z ćwiczeń	0,6

VIII.	**LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA**
	OBOWIĄZKOWA
1.	Kasprzak W.A. (2015), Ślady cyfrowe. Studium prawno-kryminalistyczne, Difin, Warszawa.
2.	Kosiński J. (2015), Paradygmaty cyberprzestępczości, Difin, Warszawa.
	UZUPEŁNIAJĄCA
1.	ISO/IEC 27041:2015, Information Technology – Security Techniques – Guidance on Assuring Suitability and Adequacy of Incident Investigative Method.
2.	ISO/IEC 27042:2015, Information Technology – Security Techniques – Guidelines for the Analysis and Interpretation of Digital Evidence.
3.	ISO/IEC 27043:2015, Information Technology – Security Techniques – Incident Investigation Principles and Processes.

IX.	**PROWADZĄCY PRZEDMIOT**
Stopień, Imię i nazwisko	mgr Karol GAZDA
adres e-mail	k.gazda@amw.gdynia.pl

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:	**Biały wywiad – techniki zaawansowane**	*Kod*:	**Tbx**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Niestacjonarne		
Kształcenie w zakresie:	Analiza danych i informatyka śledcza		
Profil:	Ogólnoakademicki		
Liczba ECTS:	4		
Semestr:	4		
Wymagania wstępne:	Brak		
Język wykładowy:	Polski		
Cel przedmiotu:	**C01**	Zapoznanie studentów z bezpiecznymi zasadami pozyskiwania informacji oraz pojęciami białego wywiadu i odróżnienie go od pozostałych technik wywiadowczych.	
	C02	Zapoznanie studentów z metodami i narzędziami do pozyskiwania informacji.	
	C03	Wykształcenie umiejętności analizy danych pozyskiwanych z otwartych źródeł.	

II.	**EFEKTY UCZENIA SIĘ**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Tbx_W01**	Student zna i rozumie różnicę pomiędzy białym wywiadem, a innymi formami wywiadu.	Kolokwium
	Tbx_W02	Student zna metody i narzędzia do pozyskiwania informacji z otwartych źródeł.	Kolokwium
	Tbx_W03	Student zna techniki i zasady analizowania pozyskanego materiału z otwartych źródeł.	Kolokwium
Umiejętności:	**Tbx_U01**	Student potrafi pozyskiwać informacje z otwartych źródeł zgodnie z etyką białego wywiadu.	Zadania na laboratorium / Kolokwium
	Tbx_U02	Student potrafi korzystać z metod, technik i narzędzi służących do pozyskiwania danych z otwartych źródeł narzędzi.	Zadania na laboratorium / Kolokwium
	Tbx_U03	Student potrafi analizować i korelować dane pozyskane z otwartych źródeł.	Zadania na laboratorium / Kolokwium
Kompetencje społeczne:	**Tbx_K01**	Student krytycznie ocenia posiadaną wiedzę i umiejętności z zakresu białego wywiadu oraz potrafi je doskonalić.	Zadania na laboratorium

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
W01	Definicje i pojęcia dotyczące białego wywiadu	2
W02	Źródła informacji	2

W03	Techniki wyszukiwania informacji	2
W04	Narzędzia i oprogramowanie	2
W05	Analiza i weryfikacja informacji	2
L01	Analiza otwartych źródeł informacji	2
L02	Pozyskiwanie danych z otwartych źródeł informacji	2
L03	Zastosowanie technik w procesie pozyskiwania danych	2
L04	Pozyskiwanie danych przy wykorzystaniu narzędzi i oprogramowania do białego wywiadu	2
L05	Weryfikacja autentyczności pozyskanych danych	1
L06	Praktyczne zastosowania białego wywiadu	1

IV. KORELACJA EFEKTÓW UCZENIA SIĘ

Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyk PRK*
W01	Tbx_W01, Tbx_W02	SIB2_W01	P7U_W, P7S_WG
W02	Tbx_W01, Tbx_W02	SIB2_W01	P7U_W, P7S_WG
W03	Tbx_W01, Tbx_W02	SIB2_W01	P7U_W, P7S_WG
W04	Tbx_W01, Tbx_W02	SIB2_W01	P7U_W, P7S_WG
W05	Tbx_W01, Tbx_W02, Tbx_W03	SIB2_W01	P7U_W, P7S_WG
L01	Tbx_U01, Tbx_U02, Tbx_U03 Tbx_K01	SIB2_U01, SIB2_U06, K01	P7U_U, P7S_UW, P7S_UO, P7U_K, P7S_KK
L02	Tbx_U01, Tbx_U02, Tbx_U03 Tbx_K01	SIB2_U01, SIB2_U06, K01	P7U_U, P7S_UW, P7S_UO, P7U_K, P7S_KK
L03	Tbx_U01, Tbx_U02, Tbx_U03 Tbx_K01	SIB2_U01, SIB2_U06, K01	P7U_U, P7S_UW, P7S_UO, P7U_K, P7S_KK
L04	Tbx_U01, Tbx_U02, Tbx_U03 Tbx_K01	SIB2_U01, SIB2_U06, K01	P7U_U, P7S_UW, P7S_UO, P7U_K, P7S_KK
L05	Tbx_U01, Tbx_U02, Tbx_U03 Tbx_K01	SIB2_U01, SIB2_U06, K01	P7U_U, P7S_UW, P7S_UO, P7U_K, P7S_KK
L06	Tbx_U01, Tbx_U02, Tbx_U03 Tbx_K01	SIB2_U01, SIB2_U06, K01	P7U_U, P7S_UW, P7S_UO, P7U_K, P7S_KK

V. NAKŁAD PRACY STUDENTA

Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**10**		**100**	**4**
Ćwiczenia	**0**			
Seminaria	**0**			
Laboratoria	**10**			
Konsultacje	**5**			
Rozliczenie rygorów przedmiotu				
Przygotowanie do ćwiczeń		**25**		
Wykonanie zadań domowych		**25**		
Przygotowanie do rozliczenia rygorów		**25**		
RAZEM	**25**	**75**		

VI. METODY DYDAKTYCZNE

1. Wykład z prezentacjami multimedialnymi
2. Praca z dokumentacją
3. Laboratorium na stanowiskach komputerowych – praca indywidualna, praca w grupach

VII. FORMA ZALICZENIA PRZEDMIOTU

Rygor	*Kryteria składowe*	*Waga*
Zaliczenie	Kolokwium	0,5
	Ocena z laboratorium	0,5

VIII. LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

OBOWIĄZKOWA

1. Krzysztof Wosiński, Bezpieczeństwo osób i systemów IT z wykorzystaniem białego wywiadu

2.	Dawid Kuciel, OSINT – Sztuka zdobywania informacji
UZUPEŁNIAJĄCA	
1.	Wojciech Filipkowski, Wiesław Mądrzejowski, Biały wywiad: otwarte źródła informacji – wokół teorii i praktyki
IX.	**PROWADZĄCY PRZEDMIOT**
Stopień, Imię i nazwisko	por. mgr Łukasz Grzyb
adres e-mail	l.grzyb@amw.gdynia.pl

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:	**Zarzadzanie ryzykiem bezpieczeństwa systemów**	*Kod*:	**Ojb**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Niestacjonarne		
Kształcenie w zakresie:	Analiza danych i informatyka śledcza		
Profil:	Ogólnoakademicki		
Liczba ECTS:	4		
Semestr:	4		
Wymagania wstępne:			
Język wykładowy:	Polski		
Cel przedmiotu: **C01**	Zapoznanie studentów z współczesnymi sposobami zarządzania ryzykiem w kontekście bezpieczeństwa systemów IT		
C02	Zapoznanie studentów z metodologią przeprowadzania analizy ryzyka dla bezpieczeństwa systemów IT		

II.	**EFEKTY UCZENIA SIĘ**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Ojb_W01**	Zrozumienie teoretycznych podstaw zarządzania ryzykiem: Znajomość kluczowych koncepcji, metodologii i standardów związanych z identyfikacją, analizą oraz zarządzaniem ryzykiem w bezpieczeństwie systemów informatycznych.	Pytania sprawdzające podczas zajęć. Kolokwium.
	Ojb_W02	Znajomość narzędzi i technik oceny ryzyka: Umiejętność identyfikacji narzędzi i stosowania technik służących do oceny ryzyka, w tym analizy ilościowej i jakościowej.	Rozwiązanie zadań problemowych
	Ojb_W03	Wiedza o strategiach minimalizacji ryzyka: Zrozumienie metod redukcji, transferu, akceptacji i unikania ryzyka w kontekście bezpieczeństwa informacji.	Rozwiązanie zadań problemowych
	Ojb_W04	Zrozumienie prawnych i regulacyjnych aspektów zarządzania ryzykiem: Znajomość przepisów prawnych oraz standardów branżowych mających wpływ na procesy zarządzania ryzykiem w organizacji.	Pytania sprawdzające podczas zajęć. Kolokwium.
Umiejętności:	**Ojb_U01**	Umiejętność przeprowadzania analizy ryzyka: Zdolność do samodzielnego przeprowadzenia kompleksowej analizy ryzyka, w tym identyfikacji zagrożeń, oceny podatności i estymacji potencjalnych skutków.	Rozwiązanie zadań problemowych Wypowiedzi ustne, aktywność w ramach dyskusji.
	Ojb_U02	Projektowanie i implementacja strategii zarządzania ryzykiem: Umiejętność opracowywania efektywnych planów zarządzania ryzykiem oraz implementacji odpowiednich środków bezpieczeństwa.	Sprawozdanie
	Ojb_U03	Monitorowanie i aktualizacja planów zarządzania ryzykiem: Zdolność do ciągłego monitorowania efektywności stosowanych rozwiązań oraz dostosowywania strategii zarządzania ryzykiem do zmieniającego się środowiska.	Rozwiązanie zadań problemowych Wypowiedzi ustne, aktywność w ramach dyskusji.
Kompetencje społeczne:	**Ojb_K01**	Umiejętność pracy zespołowej w zarządzaniu ryzykiem: Zdolność do efektywnej współpracy z różnymi grupami interesariuszy przy analizie i zarządzaniu ryzykiem.	Sprawozdanie

	Ojb_K02	Komunikacja wyników analizy ryzyka: Umiejętność jasnego i przekonującego prezentowania wyników analizy ryzyka, strategii zarządzania i rekomendacji zarówno specjalistom, jak i niespecjalistom.	Rozwiązanie zadań problemowych Wypowiedzi ustne, aktywność w ramach dyskusji.

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
W01	Wprowadzenie do zarządzania ryzykiem w bezpieczeństwie informacji: Podstawy teoretyczne i kluczowe definicje.	4
W02	Metodologie oceny ryzyka: Przegląd popularnych metodologii, takich jak OCTAVE, EBIOS i CRAMM.	4
W03	Identyfikacja i analiza zagrożeń: Techniki identyfikacji zagrożeń i ocena ich potencjalnych skutków.	4
W04	Analiza podatności i ocena wpływu: Metody oceny podatności systemów na zagrożenia i metodologie estymacji wpływu.	4
W05	Strategie minimalizacji ryzyka: Omówienie różnych strategii, takich jak unikanie ryzyka, jego transfer, akceptacja i redukcja.	4
W06	Zarządzanie ryzykiem a przepisy prawne i standardy: Wpływ regulacji prawnych i standardów branżowych na procesy zarządzania ryzykiem.	2
W07	Przyszłość zarządzania ryzykiem w bezpieczeństwie IT: Najnowsze trendy i przewidywane zmiany w obszarze zarządzania ryzykiem.	3
C01	Przeprowadzenie analizy ryzyka krok po kroku: Ćwiczenie praktyczne wykorzystujące wybraną metodologię.	3
C02	Tworzenie macierzy ryzyka: Praktyczne ćwiczenia w budowaniu i analizie macierzy ryzyka.	3
C03	Case study: Analiza rzeczywistego incydentu bezpieczeństwa: Grupowe rozwiązanie studium przypadku.	4
C04	Zarządzanie kryzysowe i planowanie odpowiedzi na incydenty: Opracowywanie planów reagowania na incydenty.	4
C05	Warsztaty z narzędzi do zarządzania ryzykiem: Praktyczne ćwiczenia z użyciem oprogramowania wspomagającego zarządzanie ryzykiem.	3
C06	Negocjacje i komunikacja w zarządzaniu ryzykiem: Symulacje negocjacji z interesariuszami i efektywnej komunikacji wyników analizy ryzyka.	3
C07	Etyczne aspekty zarządzania ryzykiem: Dyskusje na temat dylematów etycznych w zarządzaniu ryzykiem.	3
C08	Projektowanie i ocena polityk bezpieczeństwa: Ćwiczenia związane z opracowywaniem i oceną polityk bezpieczeństwa, które pomagają w zarządzaniu ryzykiem.	2

IV.	**KORELACJA EFEKTÓW UCZENIA SIĘ**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyk PRK*
W01	Ojb_W01, Ojb_W02, Ojb_W03, Ojb_W04, Ojb_U01, Ojb_U02, Ojb_U03 Ojb_K01, Ojb_K02	SIB2_W01, SIB2_W03, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7S_UK P7S_UU, P7U_K, P7S_KK
W02	Ojb_W01, Ojb_W02, Ojb_W03, Ojb_W04, Ojb_U01, Ojb_U02, Ojb_U03 Ojb_K01, Ojb_K02	SIB2_W01, SIB2_W03, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7S_UK P7S_UU, P7U_K, P7S_KK
W03	Ojb_W01, Ojb_W02,	SIB2_W01, SIB2_W03,	P7U_W, P7S_WG, P7S_WK,

	Ojb_W03, Ojb_W04, Ojb_U01, Ojb_U02, Ojb_U03 Ojb_K01, Ojb_K02	SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_U, P7S_UW, P7S_UK P7S_UU, P7U_K, P7S_KK
W04	Ojb_W01, Ojb_W02, Ojb_W03, Ojb_W04, Ojb_U01, Ojb_U02, Ojb_U03 Ojb_K01, Ojb_K02	SIB2_W01, SIB2_W03, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7S_UK P7S_UU, P7U_K, P7S_KK
W05	Ojb_W01, Ojb_W02, Ojb_W03, Ojb_W04, Ojb_U01, Ojb_U02, Ojb_U03 Ojb_K01, Ojb_K02	SIB2_W01, SIB2_W03, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7S_UK P7S_UU, P7U_K, P7S_KK
W06	Ojb_W01, Ojb_W02, Ojb_W03, Ojb_W04, Ojb_U01, Ojb_U02, Ojb_U03 Ojb_K01, Ojb_K02	SIB2_W01, SIB2_W03, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7S_UK P7S_UU, P7U_K, P7S_KK
W07	Ojb_W01, Ojb_W02, Ojb_W03, Ojb_W04, Ojb_U01, Ojb_U02, Ojb_U03 Ojb_K01, Ojb_K02	SIB2_W01, SIB2_W03, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7S_UK P7S_UU, P7U_K, P7S_KK
C01	Ojb_W01, Ojb_W02, Ojb_W03, Ojb_W04, Ojb_U01, Ojb_U02, Ojb_U03 Ojb_K01, Ojb_K02	SIB2_W01, SIB2_W03, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7S_UK P7S_UU, P7U_K, P7S_KK
C02	Ojb_W01, Ojb_W02, Ojb_W03, Ojb_W04, Ojb_U01, Ojb_U02, Ojb_U03 Ojb_K01, Ojb_K02	SIB2_W01, SIB2_W03, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7S_UK P7S_UU, P7U_K, P7S_KK
C03	Ojb_W01, Ojb_W02, Ojb_W03, Ojb_W04, Ojb_U01, Ojb_U02, Ojb_U03 Ojb_K01, Ojb_K02	SIB2_W01, SIB2_W03, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7S_UK P7S_UU, P7U_K, P7S_KK
C04	Ojb_W01, Ojb_W02, Ojb_W03, Ojb_W04, Ojb_U01, Ojb_U02, Ojb_U03 Ojb_K01, Ojb_K02	SIB2_W01, SIB2_W03, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7S_UK P7S_UU, P7U_K, P7S_KK
C05	Ojb_W01, Ojb_W02, Ojb_W03, Ojb_W04, Ojb_U01, Ojb_U02, Ojb_U03 Ojb_K01, Ojb_K02	SIB2_W01, SIB2_W03, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7S_UK P7S_UU, P7U_K, P7S_KK
C06	Ojb_W01, Ojb_W02, Ojb_W03, Ojb_W04, Ojb_U01, Ojb_U02, Ojb_U03 Ojb_K01, Ojb_K02	SIB2_W01, SIB2_W03, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7S_UK P7S_UU, P7U_K, P7S_KK
C07	Ojb_W01, Ojb_W02, Ojb_W03, Ojb_W04, Ojb_U01, Ojb_U02, Ojb_U03 Ojb_K01, Ojb_K02	SIB2_W01, SIB2_W03, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7S_UK P7S_UU, P7U_K, P7S_KK
C08	Ojb_W01, Ojb_W02, Ojb_W03, Ojb_W04, Ojb_U01, Ojb_U02, Ojb_U03 Ojb_K01, Ojb_K02	SIB2_W01, SIB2_W03, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_U, P7S_UW, P7S_UK P7S_UU, P7U_K, P7S_KK

V.	**NAKŁAD PRACY STUDENTA**			
Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**10**	**X**	**105**	**4**
Ćwiczenia	**5**			
Seminaria				
Laboratoria	**15**			

Konsultacje (zaliczenie nieobecności, rozliczenie rygorów, poprawy)	**5**			
Przygotowanie do ćwiczeń	**X**	**20**		
Opanowanie informacji		**25**		
Przygotowanie do rozliczenia rygorów		**25**		
RAZEM	**35**	**70**		

VI.	**METODY DYDAKTYCZNE**
1.	Wykład z prezentacją multimedialną
2.	Praca przy stanowisku komputerowym
3.	Rozwiązywanie zadań problemowych

VII.	**FORMA ZALICZENIA PRZEDMIOTU**	
Rygor	*Kryteria składowe*	*Waga*
Zaliczenie	Ocena za aktywność na zajęciach	0,2
	Ocena z kolokwium	0,4
	Sprawozdania z laboratorium	0,4

VIII.	**LITERATURA**
	OBOWIĄZKOWA
1.	John Stoneburner, Alice Goguen, and Alexis Feringa, "Risk Management Guide for Information Technology Systems"
2.	Douglas Hubbard, "The Failure of Risk Management: Why It's Broken and How to Fix It".
3.	Bruce Schneier, "Beyond Fear: Thinking Sensibly About Security in an Uncertain World".
4.	Chris Chapman and Stephen Ward, "Managing Project Risk and Uncertainty: A Constructively Simple Approach to Decision Making".
5.	Paul Hopkin, "Fundamentals of Risk Management: Understanding, Evaluating and Implementing Effective Risk Management".
	UZUPEŁNIAJĄCA
1.	Norman Marks, "World-Class Risk Management".
2.	David Vose, "Risk Analysis: A Quantitative Guide".
3.	Timothy J. Leech, "Implementing Enterprise Risk Management: From Methods to Applications".

IX.	
Stopień, Imię i nazwisko	mgr Tomasz Janczewski
adres e-mail	t.janczewski@amw.gdynia.pl

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:	**Zagrożenia bezpieczeństwa aplikacji i systemów**	*Kod*:	**Ojc**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Niestacjonarne		
Kształcenie w zakresie:	Analiza danych i informatyka śledcza		
Profil:	Ogólnoakademicki		
Liczba ECTS:	4		
Semestr:	4		
Wymagania wstępne:	Brak		
Język wykładowy:	Polski		
Cel przedmiotu:	**C01**	Zapoznanie studentów z aktualnymi zagrożeniami związanymi z bezpieczeństwem aplikacji i systemów	
	C02	Zapoznanie studentów z aktualnymi sposobami, technikami zabezpieczania aplikacji oraz systemów	
	C03	Zaprezentowanie sposobów, technik i działań cyberprzestępców w kontekście aplikacji i systemów pracujących w sieci internet	

II.	**EFEKTY UCZENIA SIĘ**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Ojc_W01**	Zrozumienie podstawowych koncepcji związanych z bezpieczeństwem aplikacji i systemów, w tym zagrożeń, podatności oraz metod ich wykrywania i zapobiegania.	Pytania sprawdzające podczas zajęć. Kolokwium.
	Ojc_W02	Znajomość najnowszych technologii i narzędzi wykorzystywanych do ochrony aplikacji i systemów przed atakami zewnętrznymi i wewnętrznymi.	Pytania sprawdzające podczas zajęć. Kolokwium.
	Ojc_W03	Analiza przypadków zastosowania różnych metod ochrony w realnych scenariuszach, w celu identyfikacji ich efektywności i ograniczeń.	Pytania sprawdzające podczas zajęć. Kolokwium.
	Ojc_W04	Zdolność do identyfikacji i interpretacji przepisów prawnych oraz standardów bezpieczeństwa mających zastosowanie w różnych sektorach technologicznych.	Pytania sprawdzające podczas zajęć. Kolokwium.
Umiejętności:	**Ojc_U01**	**Projektowanie i implementacja zabezpieczeń w aplikacjach i systemach**, w celu minimalizacji ryzyka i zapewnienia zgodności z normami.	Rozwiązanie zadań problemowych Wypowiedzi ustne, aktywność w ramach dyskusji.
	Ojc_U02	**Umiejętność analizy i oceny bezpieczeństwa aplikacji i systemów** przy użyciu zaawansowanych technik testowania penetracyjnego i audytów.	Sprawozdanie
	Ojc_U03	**Praktyczne umiejętności w zakresie stosowania narzędzi bezpieczeństwa** do monitorowania, wykrywania i reagowania na incydenty bezpieczeństwa.	Rozwiązanie zadań problemowych
	Ojc_U04	**Zdolność do szybkiego identyfikowania i reagowania na nowo odkryte podatności** oraz aktualizacja systemów	Dyskusja

		zabezpieczeń w odpowiedzi na dynamicznie zmieniające się zagrożenia.	
Kompetencje społeczne:	**Ojc_K01**	Rozwój umiejętności pracy zespołowej poprzez współpracę przy projektach związanych z bezpieczeństwem, w tym dzielenie się wiedzą i odpowiedzialnością za projekty zabezpieczeń.	Rozwiązanie zadań problemowych
	Ojc_K02	Efektywna komunikacja zagrożeń i strategii bezpieczeństwa z różnymi grupami interesariuszy, w tym zarządem, pracownikami technicznymi i użytkownikami końcowymi.	Praca pisemna
	Ojc_K03	Podejmowanie etycznych decyzji w kontekście bezpieczeństwa informacji, z uwzględnieniem wpływu tych decyzji na użytkowników i organizację.	Sprawozdanie połączone z dyskusją w trakcie zajęć

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
W01	Podstawy bezpieczeństwa cybernetycznego: Wprowadzenie do kluczowych koncepcji, terminologii.	2
W02	Metody identyfikacji zagrożeń i podatności w systemach IT: Narzędzia i techniki używane do oceny bezpieczeństwa.	2
W03	Zarządzanie ryzykiem w bezpieczeństwie informacji: Procesy i metodyki stosowane w planowaniu i reagowaniu na ryzyko.	2
W04	Szyfrowanie i zarządzanie kluczami: Zasady i praktyki stosowania szyfrowania do ochrony danych.	2
W05	Bezpieczeństwo aplikacji webowych: Specyficzne zagrożenia, podatności i strategie obronne w aplikacjach internetowych.	2
W06	Inżynieria społeczna i phishing: Rozpoznawanie i przeciwdziałanie manipulacji psychologicznej.	2
W07	Zabezpieczanie infrastruktury krytycznej i chmurowej: Techniki ochrony zasobów wrażliwych i rozproszonych.	2
W08	Zarządzanie incydentami bezpieczeństwa: Procedury i narzędzia do wykrywania, reagowania i odzyskiwania po incydentach bezpieczeństwa.	2
W09	Przegląd regulacji i standardów w bezpieczeństwie IT: Międzynarodowe i krajowe regulacje wpływające na strategie bezpieczeństwa.	2
W10	Najnowsze trendy i przyszłość w bezpieczeństwie cybernetycznym: Analiza rozwijających się technologii i metod, takich jak sztuczna inteligencja i uczenie maszynowe w bezpieczeństwie.	2
C01	Analiza przypadków naruszeń bezpieczeństwa: Praktyczne studium przypadków znanych ataków i ich skutków.	2
C02	Scenariusze zarządzania ryzykiem: Symulacje oceny i zarządzania ryzykiem w różnych środowiskach IT.	2
C03	Warsztaty z szyfrowania danych: Ćwiczenia praktyczne z zastosowaniem różnych metod szyfrowania i zarządzania kluczami.	2
C04	Rozwiązywanie problemów związanych z bezpieczeństwem aplikacji webowych: Interaktywne zadania dotyczące wykrywania i naprawiania podatności.	2
C05	Ćwiczenia z inżynierii społecznej: Symulacje ataków phishingowych i obrony przed manipulacjami.	2
C06	Planowanie reakcji na incydenty: Tworzenie i ocena planów reakcji na incydenty bezpieczeństwa.	2

C07	Przegląd i analiza regulacji w bezpieczeństwie IT: Dyskusje grupowe na temat wpływu i implementacji różnych regulacji prawnych.	3
L01	Testowanie penetracyjne systemów: Praktyczne ćwiczenia w zakresie wykonywania testów penetracyjnych na przykładowych systemach.	2
L02	Implementacja zabezpieczeń w aplikacjach webowych: Laboratorium z zakresu stosowania technik obronnych do ochrony aplikacji webowych.	2
L03	Konfiguracja firewalli i systemów wykrywania intruzów: Praktyczne zajęcia z konfiguracji i testowania zapór sieciowych i IDS.	2
L04	Symulacja zarządzania incydentami bezpieczeństwa: Praktyczne ćwiczenia z reagowania na symulowane incydenty bezpieczeństwa.	2
L05	Zarządzanie kluczami i szyfrowanie w praktyce: Laboratorium z zakresu implementacji systemów zarządzania kluczami.	2
L06	Ochrona infrastruktury krytycznej i chmurowej: Ćwiczenia z zabezpieczania specyficznych środowisk IT, takich jak chmura.	2
L07	Wykorzystanie narzędzi do monitorowania bezpieczeństwa: Praktyczne zajęcia z wykorzystaniem nowoczesnych narzędzi do monitorowania i alarmowania w realnym czasie.	3
K1	Ocena i poprawa projektów zabezpieczeń: Konsultacje skupiają się na indywidualnych lub grupowych projektach studentów.	2
K2	Przygotowanie do egzaminów i ocena wiedzy: Konsultacje poświęcone przeglądowi i pogłębieniu wiedzy studentów przed kolokwium zaliczeniowym.	3

IV.	**KORELACJA EFEKTÓW UCZENIA SIĘ**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyk PRK*
W01	Ojc_W01, Ojc_W02, Ojc_W03, Ojc_W04, Ojc_U02, Ojc_U03, Ojc_U04 Ojc_K01, Ojc_K02, Ojc_K03	SIB2_W01, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7S_UU P7U_K, P7S_KK
W02	Ojc_W01, Ojc_W02, Ojc_W03, Ojc_W04, Ojc_U02, Ojc_U03, Ojc_U04 Ojc_K01, Ojc_K02, Ojc_K03	SIB2_W01, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7S_UU P7U_K, P7S_KK
W03	Ojc_W01, Ojc_W02, Ojc_W03, Ojc_W04, Ojc_U02, Ojc_U03, Ojc_U04 Ojc_K01, Ojc_K02, Ojc_K03	SIB2_W01, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7S_UU P7U_K, P7S_KK
W04	Ojc_W01, Ojc_W02, Ojc_W03, Ojc_W04, Ojc_U02, Ojc_U03, Ojc_U04 Ojc_K01, Ojc_K02, Ojc_K03	SIB2_W01, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7S_UU P7U_K, P7S_KK
W05	Ojc_W01, Ojc_W02, Ojc_W03, Ojc_W04, Ojc_U02, Ojc_U03, Ojc_U04 Ojc_K01, Ojc_K02, Ojc_K03	SIB2_W01, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7S_UU P7U_K, P7S_KK
W06	Ojc_W01, Ojc_W02, Ojc_W03, Ojc_W04, Ojc_U02, Ojc_U03, Ojc_U04 Ojc_K01, Ojc_K02, Ojc_K03	SIB2_W01, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7S_UU P7U_K, P7S_KK
W07	Ojc_W01, Ojc_W02, Ojc_W03, Ojc_W04, Ojc_U02, Ojc_U03, Ojc_U04 Ojc_K01, Ojc_K02, Ojc_K03	SIB2_W01, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7S_UU P7U_K, P7S_KK
W08	Ojc_W01, Ojc_W02, Ojc_W03, Ojc_W04, Ojc_U02, Ojc_U03, Ojc_U04	SIB2_W01, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7S_UU

	Ojc_K01, Ojc_K02, Ojc_K03	SIB2_K01, SIB2_K02	P7U_K, P7S_KK
W09	Ojc_W01, Ojc_W02, Ojc_W03, Ojc_W04, Ojc_U02, Ojc_U03, Ojc_U04 Ojc_K01, Ojc_K02, Ojc_K03	SIB2_W01, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7S_UU P7U_K, P7S_KK
W10	Ojc_W01, Ojc_W02, Ojc_W03, Ojc_W04, Ojc_U02, Ojc_U03, Ojc_U04 Ojc_K01, Ojc_K02, Ojc_K03	SIB2_W01, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7S_UU P7U_K, P7S_KK
C01	Ojc_W01, Ojc_W02, Ojc_W03, Ojc_W04, Ojc_U02, Ojc_U03, Ojc_U04 Ojc_K01, Ojc_K02, Ojc_K03	SIB2_W01, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7S_UU P7U_K, P7S_KK
C02	Ojc_W01, Ojc_W02, Ojc_W03, Ojc_W04, Ojc_U02, Ojc_U03, Ojc_U04 Ojc_K01, Ojc_K02, Ojc_K03	SIB2_W01, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7S_UU P7U_K, P7S_KK
C03	Ojc_W01, Ojc_W02, Ojc_W03, Ojc_W04, Ojc_U02, Ojc_U03, Ojc_U04 Ojc_K01, Ojc_K02, Ojc_K03	SIB2_W01, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7S_UU P7U_K, P7S_KK
C04	Ojc_W01, Ojc_W02, Ojc_W03, Ojc_W04, Ojc_U02, Ojc_U03, Ojc_U04 Ojc_K01, Ojc_K02, Ojc_K03	SIB2_W01, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7S_UU P7U_K, P7S_KK
C05	Ojc_W01, Ojc_W02, Ojc_W03, Ojc_W04, Ojc_U02, Ojc_U03, Ojc_U04 Ojc_K01, Ojc_K02, Ojc_K03	SIB2_W01, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7S_UU P7U_K, P7S_KK
C06	Ojc_W01, Ojc_W02, Ojc_W03, Ojc_W04, Ojc_U02, Ojc_U03, Ojc_U04 Ojc_K01, Ojc_K02, Ojc_K03	SIB2_W01, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7S_UU P7U_K, P7S_KK
C07	Ojc_W01, Ojc_W02, Ojc_W03, Ojc_W04, Ojc_U02, Ojc_U03, Ojc_U04 Ojc_K01, Ojc_K02, Ojc_K03	SIB2_W01, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7S_UU P7U_K, P7S_KK
L01	Ojc_W01, Ojc_W02, Ojc_W03, Ojc_W04, Ojc_U02, Ojc_U03, Ojc_U04 Ojc_K01, Ojc_K02, Ojc_K03	SIB2_W01, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7S_UU P7U_K, P7S_KK
L02	Ojc_W01, Ojc_W02, Ojc_W03, Ojc_W04, Ojc_U02, Ojc_U03, Ojc_U04 Ojc_K01, Ojc_K02, Ojc_K03	SIB2_W01, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7S_UU P7U_K, P7S_KK
L03	Ojc_W01, Ojc_W02, Ojc_W03, Ojc_W04, Ojc_U02, Ojc_U03, Ojc_U04 Ojc_K01, Ojc_K02, Ojc_K03	SIB2_W01, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7S_UU P7U_K, P7S_KK
L04	Ojc_W01, Ojc_W02, Ojc_W03, Ojc_W04, Ojc_U02, Ojc_U03, Ojc_U04 Ojc_K01, Ojc_K02, Ojc_K03	SIB2_W01, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7S_UU P7U_K, P7S_KK
L05	Ojc_W01, Ojc_W02, Ojc_W03, Ojc_W04, Ojc_U02, Ojc_U03, Ojc_U04 Ojc_K01, Ojc_K02, Ojc_K03	SIB2_W01, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7S_UU P7U_K, P7S_KK
L06	Ojc_W01, Ojc_W02, Ojc_W03, Ojc_W04, Ojc_U02, Ojc_U03, Ojc_U04	SIB2_W01, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7S_UU

	Ojc_K01, Ojc_K02, Ojc_K03	SIB2_K01, SIB2_K02	P7U_K, P7S_KK
L07	Ojc_W01, Ojc_W02, Ojc_W03, Ojc_W04, Ojc_U02, Ojc_U03, Ojc_U04 Ojc_K01, Ojc_K02, Ojc_K03	SIB2_W01, SIB2_U01, SIB2_U04, SIB2_U05, SIB2_U07 SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7U_U, P7S_UW, P7S_UK, P7S_UU P7U_K, P7S_KK

V.

Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**10**		**105**	**4**
Ćwiczenia				
Seminaria				
Laboratorium	**20**			
Konsultacje	**5**			
Rozliczenie rygorów przedmiotu				
Przygotowanie do ćwiczeń		**20**		
Wykonanie zadań domowych		**25**		
Przygotowanie do rozliczenia rygorów		**25**		
RAZEM	**35**	**70**		

VI. METODY DYDAKTYCZNE

1.	Wykład z prezentacją multimedialną
2.	Praca przy stanowisku komputerowym
3.	Rozwiązywanie zadań problemowych

VII. FORMA ZALICZENIA PRZEDMIOTU

Rygor	*Kryteria składowe*	*Waga*
Zaliczenie	Aktywność na zajęciach laboratoryjnych	0,2
	Sprawozdania z laboratorium	0,8
Zaliczenie	Ocena za aktywność na zajęciach	0,2
	Ocena z kolokwium	0,8

VIII. LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

OBOWIĄZKOWA

1.	Charles P. Pfleeger, Shari Lawrence Pfleeger, "Security in Computing", 5th Edition
2.	Ross J. Anderson, "Security Engineering: A Guide to Building Dependable Distributed Systems", 3rd Edition.
3.	Michael Howard, David LeBlanc, "Writing Secure Code", 2nd Edition.
4.	Bruce Schneier, "Applied Cryptography: Protocols, Algorithms and Source Code in C", 2nd Edition.

UZUPEŁNIAJĄCA

1.	Stewart James, Mike Chapple, Darril Gibson, "CISSP: Certified Information Systems Security Professional Study Guide", 8th Edition.
2.	Kevin Mitnick, William L. Simon, "The Art of Deception: Controlling the Human Element of Security".
3.	Nina Godbole, Sunit Belapure, "Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives"
4.	Brian Carrier, "File System Forensic Analysis".

IX. PROWADZĄCY PRZEDMIOT

Stopień, Imię i nazwisko	mgr Tomasz Janczewski
adres e-mail	t.janczewski@amw.gdynia.pl

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:	**Metody ataku i obrony w cyberprzestrzeni**	*Kod*:	**Lxi**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Niestacjonarne		
Kształcenie w zakresie:	Analiza danych i informatyka śledcza		
Profil:	Ogólnoakademicki		
Liczba ECTS:	4		
Semestr:	4		
Wymagania wstępne:			
Język wykładowy:	Polski		
Cel przedmiotu:	**C01**	Zapoznanie studentów z metodycznym podejściem do projektowania ataków w cyberprzestrzeni w celu zrozumienia doboru sposobu obrony.	
	C02	Zapoznanie słuchaczy z zasadami doboru narzędzi ataku i obrony w sieciach komputerowych, z uwzględnieniem specyfiki ruchu w warstwie aplikacyjnej.	
	C03	Zapoznanie studentów z metodami zabezpieczania usług przed potencjalnym atakiem.	

II.	**EFEKTY UCZENIA SIĘ**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Lxi_W01**	Zna i rozumie wybrane fakty, teorie, metody oraz zależności między nimi z zakresu ataku w cyberprzestrzeni.	Kolokwium
	Lxi_W02	Student zna sposoby zabezpieczania usług sieciowych przed typowymi atakami w sieciach teleinformatycznych	Kolokwium
Umiejętności:	**Lxi_U01**	Student potrafi zaprojektować wektor ataku i zgodnie z założeniami przeprowadzić akcję ofensywną	Kolokwium, rozwiązywanie zadań
	Lxi_U02	Słuchacz posiada umiejętności pozwalające mu na zabezpieczenie podstawowych usług w cyberprzestrzeni	Kolokwium, rozwiązywanie zadań
	Lxi_U03	Potrafi łączyć kilka technik obrony jak i ataku w celu otrzymania jak najbardziej kompleksowego rozwiązania w realizacji postawionych zadań	Kolokwium, rozwiązywanie zadań
Kompetencje społeczne:	**Lxi_K01**	Student w oparciu o uzyskaną podstawową wiedzę z zakresu sieci teleinformatycznych potrafi doskonalić swoją wiedzę i umiejętności z tego obszaru	Praca w grupach
	Lxi_K02	Uznaje znaczenie wiedzy w rozwiązywaniu problemów praktycznych oraz zasięga opinii ekspertów w przypadku trudności z samodzielnym rozwiazywaniem problemów dotyczących wykorzystania systemów informacyjnych w bezpieczeństwie.	Rozwiązanie zadań problemowych

	Lxi_K03	Krytycznie ocenia posiadaną wiedzę i odbierane treści z zakresu systemów informatycznych	Sprawozdanie / przygotowanie do zajęć

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
W01	Zrozumieć Cybersecurity Kill Chain	6
W02	Informacje o zagrożeniach	4
W03	Zarządzanie lukami w zabezpieczeniach	4
W04	DeepFake oraz narzędzia AI/ML Cyberbezpieczeństwie	4
W05	Innowacje w strategiach bezpieczeństwa	2
C01	Analizy przypadku ataków w cyberprzestrzeni (kluczowe obiekty dla państw)	4
C02	Dobór sił i środków do realizacji zadań w cyberprzestrzeni	4
C03	Wykorzystanie analizy zagrożeń do badania podejrzanych działań	2
L01	Rekonesans	4
L02	Przejmowanie sieci teleinformatycznych	4
L03	Naruszenie bezpieczeństwa systemu	4
L04	Przechwytywanie tożsamości użytkownika	4
L05	Urządzenia wbudowane i hakowanie RFID/Mifare	4

IV.	**KORELACJA EFEKTÓW UCZENIA SIĘ**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyk PRK*
W01	Lxi_W01, Lxi_W02, Lxi_K01, Lxi_K02, Lxi_K03	SIB2_W01, SIB2_W02, SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W02	Lxi_W01, Lxi_W02, Lxi_K01, Lxi_K02, Lxi_K03	SIB2_W01, SIB2_W02, SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W03	Lxi_W01, Lxi_W02, Lxi_K01, Lxi_K02, Lxi_K03	SIB2_W01, SIB2_W02, SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W04	Lxi_W01, Lxi_W02, Lxi_K01, Lxi_K02, Lxi_K03	SIB2_W01, SIB2_W02, SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
W05	Lxi_W01, Lxi_W02, Lxi_K01, Lxi_K02, Lxi_K03	SIB2_W01, SIB2_W02, SIB2_K01, SIB2_K02	P7U_W, P7S_WG, P7S_WK, P7U_K, P7S_KK
C01	Lxi_W01, Lxi_U01, Lxi_U02, Lxi_U03, Lxi_K01, Lxi_K02, Lxi_K03	SIB2_W01, SIB2_U01, SIB2_U02, SIB2_K01, SIB2_K02, SIB2_K04	P7U_W, P7S_WG, P7U_U, P7S_UW P7U_K, P7S_KK, P7S_KR
C02	Lxi_W01, Lxi_U01, Lxi_U02, Lxi_U03, Lxi_K01, Lxi_K02, Lxi_K03	SIB2_W01, SIB2_U01, SIB2_U02, SIB2_K01, SIB2_K02, SIB2_K04	P7U_W, P7S_WG, P7U_U, P7S_UW P7U_K, P7S_KK, P7S_KR
C03	Lxi_W01, Lxi_U01, Lxi_U02, Lxi_U03, Lxi_K01, Lxi_K02, Lxi_K03	SIB2_W01, SIB2_U01, SIB2_U02, SIB2_K01, SIB2_K02, SIB2_K04	P7U_W, P7S_WG, P7U_U, P7S_UW P7U_K, P7S_KK, P7S_KR
L01	Lxi_W01, Lxi_U01, Lxi_U02, Lxi_U03, Lxi_K01, Lxi_K02, Lxi_K03	SIB2_W01, SIB2_U01, SIB2_U02, SIB2_K01, SIB2_K02, SIB2_K04	P7U_W, P7S_WG, P7U_U, P7S_UW P7U_K, P7S_KK, P7S_KR
L02	Lxi_W01, Lxi_U01, Lxi_U02, Lxi_U03, Lxi_K01, Lxi_K02, Lxi_K03	SIB2_W01, SIB2_U01, SIB2_U02, SIB2_K01, SIB2_K02, SIB2_K04	P7U_W, P7S_WG, P7U_U, P7S_UW P7U_K, P7S_KK, P7S_KR
L03	Lxi_W01, Lxi_U01, Lxi_U02, Lxi_U03, Lxi_K01, Lxi_K02, Lxi_K03	SIB2_W01, SIB2_U01, SIB2_U02,	P7U_W, P7S_WG, P7U_U, P7S_UW P7U_K, P7S_KK, P7S_KR

		SIB2_K01, SIB2_K02, SIB2_K04	
L04	Lxi_W01, Lxi_U01, Lxi_U02, Lxi_U03, Lxi_K01, Lxi_K02, Lxi_K03	SIB2_W01, SIB2_U01, SIB2_U02, SIB2_K01, SIB2_K02, SIB2_K04	P7U_W, P7S_WG, P7U_U, P7S_UW P7U_K, P7S_KK, P7S_KR
L05	Lxi_W01, Lxi_U01, Lxi_U02, Lxi_U03, Lxi_K01, Lxi_K02, Lxi_K03	SIB2_W01, SIB2_U01, SIB2_U02, SIB2_K01, SIB2_K02, SIB2_K04	P7U_W, P7S_WG, P7U_U, P7S_UW P7U_K, P7S_KK, P7S_KR

V. NAKŁAD PRACY STUDENTA

Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**10**	**X**	**105**	**4**
Ćwiczenia	**0**			
Seminaria	**0**			
Laboratoria	**20**			
Konsultacje (zaliczenie nieobecności, rozliczenie rygorów, poprawy)	**5**			
Przygotowanie do ćwiczeń	**X**	**20**		
Opanowanie informacji		**30**		
Przygotowanie do rozliczenia rygorów		**20**		
RAZEM	**35**	**70**		

VI. METODY DYDAKTYCZNE

1.	Metody podające: wykład problemowy / wykład konwersatoryjny / wykład z prezentacją multimedialną.
2.	Metody aktywizujące: pogadanka, obserwacja, praca z dokumentacją, praca w grupach, case study.
3.	Ćwiczenia/Laboratorium: praca w grupach / praca indywidualna z wykorzystaniem stanowisk komputerowych

VII. FORMA ZALICZENIA PRZEDMIOTU

Rygor	*Kryteria składowe*	*Waga*
Zaliczenie	Ocena z kolokwium (materiał z wykładów)	0,4
	Ocena z laboratoriów i ćwiczeń	0,6

VIII. LITERATURA

OBOWIĄZKOWA

1.	Dan Borges, Adversarial Tradecraft in Cybersecurity, ISBN 978-1-80107-620-3, 2021 Packt Publishing
2.	Yuri Diogenes, Erdal Ozkaya, Cybersecurity – Attack and Defense Strategies, ISBN 978-1-83882-779-3, 2019 Packt Publishing

UZUPEŁNIAJĄCA

1.	Maxie Reynolds, The Art of Attack, ISBN: 978-1-119-80546-5, 2021 Wiley
2.	Ben McCarty, Cyberjutsu : cybersecurity for the modern ninja, ISBN-13: 978-1-7185-0054-9, 2021 No Starch Press

IX. PROWADZĄCY PRZEDMIOT

Stopień, Imię i nazwisko	mgr Grzegorz Piotrowski
adres e-mail	grzegorz.piotrowski@c2o.eu

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:	**Podstawy prawne cyberbezpieczeństwa**	*Kod*:	**Ccq**
Kierunek studiów:	Systemy informacyjne w bezpieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Niestacjonarne		
Kształcenie w zakresie:	Analiza danych i informatyka śledcza		
Profil:	Ogólnoakademicki		
Liczba ECTS:	4		
Semestr:	4		
Wymagania wstępne:	Podstawowa wiedza z zakresu państwa i prawa		
Język wykładowy:	Polski		
Cel przedmiotu:	**C01**	Zapoznanie słuchaczy z najważniejszymi aktami prawnymi regulującymi problematykę cyberbezpieczeństwa w wymiarze krajowym.	
	C02	Zapoznanie słuchaczy z najważniejszymi aktami prawnymi regulującymi problematykę cyberbezpieczeństwa w wymiarze międzynarodowym.	

II.	**EFEKTY UCZENIA SIĘ**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Ccq_W01**	Posiada wiedzez zakresu prawa krajowego i międzynarodowego oraz norm postępowania w cyberprzestrzeni, wpływających na prawa i obowiązki państw na płaszczyźnie międzynarodowej	Kolowium/ dyskusja
Umiejętności:	**Oku_U01**	Umiejętność analizy krajowych i międzynarodowych aktów prawnych oraz norm z zakresu cyberbezpieczeństwa.	Kolowium/ dyskusja
	Oku_U02	Potrafi znaleźć legitymację do działań państw w cyberprzestrzeni	Kolowium/ dyskusja
Kompetencje społeczne:	**Oku_K01**	Potrafi dokonać subsumpcji normy prawnej w konkretnym stanie faktycznym	Obserwacja podczas zajęć
	Oku_K02	Przestrzega unormowań materialnych i proceduralnych krajowych oraz międzynarodowych dotyczących prowadzenia działań w cyberprzestrzeni	Obserwacja podczas zajęć
	Oku_K03	W oparciu o uzyskaną teoretyczną wiedzę programową potrafi samodzielnie aktualizować i doskonalić swoją wiedzę i umiejętności.	Obserwacja podczas zajęć

III.	**TREŚCI PROGRAMOWE**	
Forma	*Tematyka*	*Liczba godzin*
W01	Zasady poszanowania suwerenności terytorialnej.	5
W02	Zakaz interwencji w sprawy wewnętrzne; zakaz użycia siły.	5

W03	Zakaz przeciwdziałania wykorzystaniu własnego terytorium do czynności szkodliwych dla drugiego państwa (zasada dobrego sąsiedztwa); zasady przypisania cyberoperacji państwu.	5
W04	Naruszenie bezpieczeństwa informacyjnego systemów komputerowych w świetle konkretnych norm prawa międzynarodowego.	5
W05	Przepisy regulujące odpowiedzialność międzynarodową państwa za działania indywidualnych hakerów i grup hakerskich; prawne ramy operacji odwetowych; prawo do samoobrony przed napaścią zbrojną.	5
C01	Problemy z prawnym zdefiniowaniem pojęcia cyberprzestrzeń. Przegląd ustawodawstwa wybranych państw. Status prawny cyberprzestrzeni.	5
C02	Status prawny państw w cyberprzestrzeni. Prawa i obowiązki państw w cyberprzestrzeni.	5
C03	Regulacje międzynarodowe działań w cyberprzestrzeni	5
C04	Krajowa regulacja z zakresu cyberbezpieczeństwa.	5
C05	Unormowania dot. Przestępstw komputerowych	5

IV.	**KORELACJA EFEKTÓW UCZENIA SIĘ**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyk PRK*
W01	Ccq_W01,	SIB2_W01	P7U_W, P7S_WG
W02	Ccq_W01,	SIB2_W01	P7U_W, P7S_WG
W03	Ccq_W01,	SIB2_W01	P7U_W, P7S_WG
W04	Ccq_W01,	SIB2_W01	P7U_W, P7S_WG
W05	Ccq_W01,	SIB2_W01	P7U_W, P7S_WG
L01	Ccq_U01, Ccq_U02, , Ccq_K01, Ccq_K02, Ccq_K03	SIB2_U01, SIB2_U06, SIB2_K01, SIB2_K05	P7U_U, P7S_UW, P7S_UO, P7U_K, P7S_KK, P7S_KR
L02	Ccq_U01, Ccq_U02, , Ccq_K01, Ccq_K02, Ccq_K03	SIB2_U01, SIB2_U06, SIB2_K01, SIB2_K05	P7U_U, P7S_UW, P7S_UO, P7U_K, P7S_KK, P7S_KR
L03	Ccq_U01, Ccq_U02, , Ccq_K01, Ccq_K02, Ccq_K03	SIB2_U01, SIB2_U06, SIB2_K01, SIB2_K05	P7U_U, P7S_UW, P7S_UO, P7U_K, P7S_KK, P7S_KR
L04	Ccq_U01, Ccq_U02, , Ccq_K01, Ccq_K02, Ccq_K03	SIB2_U01, SIB2_U06, SIB2_K01, SIB2_K05	P7U_U, P7S_UW, P7S_UO, P7U_K, P7S_KK, P7S_KR
L05	Ccq_U01, Ccq_U02, , Ccq_K01, Ccq_K02, Ccq_K03	SIB2_U01, SIB2_U06, SIB2_K01, SIB2_K05	P7U_U, P7S_UW, P7S_UO, P7U_K, P7S_KK, P7S_KR

V.	**NAKŁAD PRACY STUDENTA**			
Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**15**	**X**	**105**	**4**
Ćwiczenia	**15**			
Seminaria	**0**			
Laboratoria	**0**			
Konsultacje (zaliczenie nieobecności, rozliczenie rygorów, poprawy)	**5**			
Przygotowanie do ćwiczeń	**X**	**25**		
Opanowanie informacji		**25**		
Przygotowanie do rozliczenia rygorów		**20**		
RAZEM	**35**	**70**		

VI.	**METODY DYDAKTYCZNE**
1.	Metody podające: wykład /wykład problemowy / wykład konwersatoryjny / wykład z prezentacją multimedialną.
2.	Metody aktywizujące: pogadanka, obserwacja, praca z dokumentacją, praca w grupach, case study.
3.	Ćwiczenia/Laboratorium: praca w grupach / praca indywidualna.

VII.	**FORMA ZALICZENIA PRZEDMIOTU**	
Rygor	*Kryteria składowe*	*Waga*
Zaliczenie	wykonanie określonych zadań podczas ćwiczeń	0,4

	test	0,6
VIII.	**LITERATURA**	
	OBOWIĄZKOWA	
1.	Schmitt M.N., Tallinn Manual on the International law applicable to the cyber warfare, Cambridge 2013.	
2.	Adamski A., Prawo karne komputerowe, Warszawa 2000..	
	UZUPEŁNIAJĄCA	
1.	Adamski A., Przestępczość w cyberprzestrzeni. Prawne środki przeciwdziałania zjawisku w Polsce na tle projektu Konwencji Rady Europy, Toruń 2001.	
2.	Banasiński C., Rojszczak M. (red.), Cyberbezpieczeństwo, Warszawa 2020.	
3.	Klimburg A., National Cyber Security. Framework Manual, NATO Cooperative Cyber Defence Centre of Excellence Tallin, Estonia 2012.	
IX.	**PROWADZĄCY PRZEDMIOT**	
Stopień, Imię i nazwisko	dr Alicja Żukowska	
adres e-mail	a.zukowska@amw.gdynia.pl	

3.10. Karta przedmiotu modułu dyplomowego studiów niestacjonarnych – D

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 i prawa autorskie, praca dyplomowa**	*Kod*:	**Axp**
Kierunek studiów:	Systemy informacyjne w bezieczeństwie		
Poziom studiów:	Studia II stopnia		
Forma studiów:	Niestacjonarne		
Specjalność:	Cyberbezpieczeństwo, Analiza danych i informatyka śledcza		
Profil:	Ogólnokademicki		
Liczba ECTS:	11		
Semestr:	3,4		
Wymagania wstępne:	Wiedza merytoryczna z przedmiotu metodologia badań nad bezpieczeństwem		
Język wykładowy:	polski		
Cel przedmiotu:	**C01**	Zapoznać z procesem prowadzenia badań naukowych w zakresie bezpieczeństwa	
	C02	Nauczyć technik i narzędzi wykorzystywanych do prowadzenia badan naukowych	
	C03	Przygotować do opracowania pracy magisterskiej odpowiadającej regułom pracy naukowej	

II.	**EFEKTY UCZENIA**		
Zakres	*Kod*	*Opis efektu*	*Sposób oceny*
Wiedza:	**Axp_W01**	Wiedza o podstawowych technikach i narzędziach badawczych stosowanych w badaniach nad bezpieczeństwem	Odpowiedź ustna
	Axp_W02	Zrozumienie istoty procesu badań naukowych i możliwości zastosowania go w badaniach nad bezpieczeństwem	Odpowiedź ustna
	Axp_W03	Znajomość podstawowych zasadach prawa autorskiego	Odpowiedź ustna
Umiejętności:	**Axp_U01**	Wybór i sporządzanie adekwatnych narzędzi badawczych do określonych metod badawczych	Odpowiedź ustna
	Axp_U02	Przeprowadzanie badań teoretycznych i empirycznych	Odpowiedź ustna
Kompetencje społeczne:	**Axp_K01**	Zrozumienie istoty i potrzeb pogłębiania wiedzy	Odpowiedź ustna
	Axp_K02	Dostrzeganie zagrożeń bezpieczeństwa i poszukiwanie środków zaradczych	Opracowanie pisemne

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

W01	**Zasady prowadzenia badań empirycznych** - pojęcie metod badawczych i technik badawczych; podstawowe – empiryczne metody badawcze; proste i złożone; schematy opracowania narzędzi badawczych	1
W02	**Pozyskiwanie materiału badawczego** – metodami empirycznymi, narzędzia badawcze w badaniach ilościowych i jakościowych	1
W03	**Wywiad i jego narzędzia badawcze** – zasady opracowywania kwestionariuszy wywiadu	2
W04	**Ankietowanie i narzędzia badawcze** – zasady opracowywania kwestionariuszy ankiety	2
W05	**Obserwacja i jej narzędzia badawcze** – zasady opracowywania dziennika obserwacji	1
W06	**Prawo autorskie** – zasady pisemnego sporządzania sprawozdań z procesu badawczych	2
W07	Sprawdzian pisemny – zaliczenie przedmiotu	1

IV.	**KORELACJA EFEKTÓW UCZENIA**		
Forma	*Kod efektu przedmiotu*	*Kod efektu kierunkowego*	*Kod charakterystyki PRK*
W01	Axp_W01, Axp_K01	SIB2_W01, SIB2_K04	P7U_W P7S_WG P7U_K P7S_KR
W02	Axp_W01, Axp_W02, Axp_K02	SIB2_W01, SIB2_K02	P7U_W P7S_WG P7U_K P7S_KK
W03	Axp_W01, Axp_W02, Axp_W03	SIB2_W01	P7U_W P7S_WG
W04	Axp_W01, Axp_U02	SIB2_W01, SIB2_U01, SIB2_K03,	P7U_W P7S_WG P7U K P7S_KO P7U_U P7S_UW
W05	Axp_W01, Axp_U01	SIB2_W01, SIB2_U01,	P7U_W P7S_WG P7U_U P7S_UW
W06	Axp_W03 Axp_K01	SIB2_W01, SIB2_K02	P7U_W P7S_WG P7U_K P7S_KK
W07	Axp_K01	SIB2_K01, SIB2_K02	P7U_K P7S_KK

V.	**NAKŁAD PRACY STUDENTA**			
Forma aktywności	*Liczba godzin kontaktowych*	*Liczba godzin niekontaktowych*	*Razem liczba godzin*	*Pkt. ECTS*
Wykład	**10**	**X**	**275**	**11**
Ćwiczenia	**60**			
Seminaria	**-**			
Konwersatoria	**-**			
Konsultacje (zaliczenie nieobecności, rozliczenie rygorów, poprawy)	**15**			
Przygotowanie do ćwiczeń	**X**	**60**		
Opanowanie informacji		**30**		
Przygotowanie do rozliczenia rygorów		**100**		
RAZEM	**85**	**190**		

VI.	**METODY I NARZĘDZIA DYDAKTYCZNE**
1.	Wykłady – oddziaływanie słowne i prezentacje multimedialne.
2.	Zadania do dyskusji
3.	Wykaz literatury do samodzielnego studiowania

VII.	FORMA ZALICZENIA PRZEDMIOTU	
Rygor	*Kryteria składowe*	*Waga*
Zaliczenie	Ocena za znajomość teoretyczną przedmiotu.	1,0

VIII.	LITERATURA
	OBOWIĄZKOWA
1.	S. Nowak, *Metodologia badań społecznych*, PWN, Warszawa 2010.
2.	K. Pawlik, R. Zenderowski, *Dyplom z Internetu. Jak korzystać z Internetu pisząc prace dyplomowe*, Wydawnictwa Fachowe, Warszawa 2010.
3.	W. Zaczyński, *Praca badawcza nauczyciela*, Wydawnictwa Szkolne i Pedagogiczne, Warszawa 1995.
4.	R. Zenderowski, *Praca magisterska*, licencjat, Wyd. CeDeWu.pl, Warszawa
5.	Ch. Frankfort-Nachmias, *Metody badawcze w naukach społecznych*, wyd. Zysk i Ska, Poznań 2001.
	UZUPEŁNIAJĄCA
1.	E. Babbie, *Podstawy nauk społecznych*, PWN, Warszawa 2009.
2.	J. Apanowicz, *Metodologia nauk*, Dom Organizatora, Toruń 2003.
3.	A. Chalmers, *Czym jest to co zwiemy nauką?*, wyd. Siedmiogród, Wrocław 1977.
4.	J. Sztumski, *Wstęp do metod i technik badań społecznych*, wyd. „Śląsk", Katowice 2010

IX.	PROWADZĄCY PRZEDMIOT
Stopień, Imię i nazwisko	dr Stefan KOWALSKI,
adres e-mail, tel.	s.kowalski@amw.gdynia.pl 261 262 893

3.11. Matryca efektów uczenia się w zakresie Cyberbezpieczeństwo studiów stacjonarnych i niestacjonarnych

Symbol EU	Przedmioty	A. Grupa treści podstawowych	Język angielski	Geografia bezpieczeństwa	Historia bezpieczeństwa	Strategia bezpieczeństwa wewnętrznego	Metodologia badań nad bezpieczeństwem	Podstawy ekonomii	Podstawy prawa	Wprowadzenie do psychologii społecznej	Podstawy socjologii	Podstawy stosunków międzynarodowych	Podstawy bezpieczenstwa narodowego (pol./ang.)	Podstawy zarządzania i organizacji	Podstawy filozofii i logiki	Podstawy pedagogiki	Historia techniki	Ochrona ludności i obrona cywilna	B. Grupa treści kierunkowych	Zarządzanie systemami bezpieczeństwa wewnętrznego	Inżynieria systemów i projektowanie procesów	Audyt i certyfikacja systemów informatycznych	Ocena ryzyka i prognozowanie w bezpieczeństwie	Zarządzanie projektem	Komunikacja społeczna	Certyfikacja Systemu Zarządzania ISO/IEC 27001	Sztuczna inteligencja	C.Grupa treści szkolenia specjalistycznego	Zarządzanie projektami informatycznymi	Akredytacja bezpieczeństwa teleinformatycznego	Testy penetracyjne	Bezpieczeństwo sieci komputerowych i bezprzewodowych	Elementy kryptologii	Administrowanie systemem Linux	Cyberbezpieczeństwo	Prognozowanie cyberzagrożeń	Symulacja komputerowa	Podstawy prawne cyberbezpieczeństwa	D. Praca dyplomowa	Seminarium dyplomowe i prawa autorskie	Praca dyplomowa	Podsumowanie
WIEDZA																																											
SIB2_W01				X	X	X	X	X	X	X	X	X	X	X	X	X	X			X	X	X	X	X	X	X	X		X	X	X	X	X	X	X	X	X	X	X	X	X	X	**34**
SIB2_W02				X			X			X			X					X				X	X		X		X		X	X	X	X	X		X	X						**16**
SIB2_W03				X		X			X			X	X					X		X		X				X			X	X	X	X	X									**9**
SIB2_W04													X					X		X	X			X					X														**5**
SIB2_U01				X			X		X	X		X	X	X	X	X	X	X		X	X	X	X	X	X	X	X		X	X	X	X	X	X	X	X	X	X	X	X	X	**31**
SIB2_U02				X	X	X	X	X			X			X	X	X				X	X		X	X								X	X		X							**16**
SIB2_U03													X		X										X		X		X														**5**
SIB2_U04				X	X	X					X	X								X	X	X	X	X	X	X			X		X				X	X							**16**
SIB2_U05			X																								X		X	X	X				X		X						**7**
SIB2_U06															X						X	X	X	X		X	X		X									X	X					**10**
SIB2_U07			X			X	X		X	X	X		X	X		X		X			X	X		X						X				X	X								**16**
SIB2_K01						X		X		X		X		X	X						X	X		X		X		X		X		X	X	X	X	X		X	X				**21**
SIB2_K02			X		X	X	X	X			X	X	X		X	X					X	X	X	X			X	X		X	X	X			X	X	X						**23**
SIB2_K03			X	X	X		X	X			X			X		X		X			X		X	X		X			X	X	X											**16**
SIB2_K04				X		X	X		X				X		X					X		X		X					X							X								**13**
SIB2_K05				X									X								X			X		X			X															**8**

3.12. Matryca efektów uczenia się w zakresie Analiza danych i informatyka śledczastudiów stacjonarnych i niestacjonarnych

Symbol EU	Przedmioty	A. Grupa treści podstawowych	Język angielski	Geografia bezpieczeństwa	Historia bezpieczeństwa	Strategia bezpieczeństwa wewnętrznego	Metodologia badań nad bezpieczeństwem	Podstawy ekonomii	Podstawy prawa	Wprowadzenie do psychologii społecznej	Podstawy socjologii	Podstawy stosunków międzynarodowych	Podstawy bezpieczenstwa narodowego (pol./ang.)	Podstawy zarządzania i organizacji	Podstawy filozofii i logiki	Podstawy pedagogiki	Historia techniki	Ochrona ludności i obrona cywilna	B. Grupa treści kierunkowych	Zarządzanie systemami bezpieczeństwa wewnętrznego	Inżynieria systemów i projektowanie procesów	Audyt i certyfikacja systemów informatycznych	Ocena ryzyka i prognozowanie w bezpieczeństwie	Zarządzanie projektem	Komunikacja społeczna	Certyfikacja Systemu Zarządzania ISO/IEC 27001	Sztuczna inteligencja	C.Grupa treści szkolenia specjalistycznego	Pozyskiwanie i analiza danych z technologii bezzałogowych	Zastosowanie kryptologii w informatyce śledczej	Testy penetracyjne	Bezpieczeństwo sieci komputerowych i bezprzewodowych	Techniki pozyskiwania cyfrowego materiału dowodowego	Biały wywiad – techniki zaawansowane	Zarzadzanie ryzykiem bezpieczeństwa systemów	Zagrożenia bezpieczeństwa aplikacji i systemów	Metody ataku i obrony w cyberprzestrzeni	Podstawy prawne cyberbezpieczeństwa	D. Praca dyplomowa	Seminarium dyplomowe i prawa autorskie	Praca dyplomowa	Podsumowanie
WIEDZA																																												
SIB2_W01				X	X	X	X	X	X	X	X	X	X	X	X	X	X			X	X	X	X	X	X	X	X		X	X	X	X	X	X	X	X	X	X	X	X	X	X	**34**
SIB2_W02				X			X			X			X					X				X	X		X		X			X	X	X	X				X					**14**
SIB2_W03				X		X			X				X	X				X		X		X				X													X					**10**
SIB2_W04														X						X	X			X																				**4**
SIB2_U01				X			X		X	X		X	X	X	X	X	X	X		X	X	X	X	X	X	X	X		X	X	X	X	X	X	X	X	X	X	X	X	X	X	**31**
SIB2_U02				X	X	X	X	X			X			X	X	X				X	X		X	X						X		X	X				X					**17**
SIB2_U03														X		X									X		X																	**4**
SIB2_U04				X	X	X						X	X							X	X	X	X	X	X	X					X						X	X					**15**
SIB2_U05		X																									X				X						X	X					**5**
SIB2_U06															X						X	X	X	X		X	X		X						X					X				**10**
SIB2_U07		X			X	X		X	X	X		X	X		X		X			X	X		X								X						X	X					**16**
SIB2_K01					X		X		X		X		X	X						X	X		X		X		X		X	X	X	X	X	X	X	X	X	X	X	X	X	X	**23**
SIB2_K02		X		X	X	X	X			X	X	X	X		X	X					X	X	X			X	X				X						X	X	X			X	X	**21**
SIB2_K03		X	X	X		X	X			X			X		X		X				X		X	X		X					X											X	X	**15**
SIB2_K04			X		X	X		X					X		X					X		X		X																X			X	X	**12**
SIB2_K05			X										X								X			X		X																X			**6**

4. SPOSOBY WERYFIKACJI I OCENY EFEKTÓW UCZENIA SIĘ OSIĄGANYCH PRZEZ STUDENTA W TRAKCIE CAŁEGO CYKLU KSZTAŁCENIA

Osiągnięcie efektów uczenia się dla kierunku Systemy informacyjne w bezpieczeństwie weryfikowane jest na różnych etapach kształcenia: poprzez rozliczanie wszystkich przedmiotów/modułów, w tym seminarium dyplomowego i przygotowania do pracy dyplomowej oraz w trakcie egzaminu dyplomowego.

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:

- egzaminy pisemne i ustne,
- prace pisemne przygotowywane samodzielnie,
- rozwiązywanie zadań problemowych,
- kolokwia,
- projekty,
- prezentacje multimedialne prowadzone i przygotowywane indywidualnie lub grupowo,
- 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 (kazusy),
- egzamin dyplomowy / obrona pracy.

Z kolei najważniejszymi źródłami weryfikacji osiągnięcia zakładanych efektów uczenia są:

- analiza pracy studenta w trakcie i po zakończeniu kształcenia w ramach danego przedmiotu/modułu,
- przygotowanie i analiza pracy dyplomowej,

Uwadze poddano również 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.

Znajdujące się w programie studiów matryce efektów uczenia się przedstawiają pokrycie kierunkowych efektów uczenia się dla poszczególnych przedmiotów i modułów.

5. HARMONOGRAM REALIZACJI PROGRAMU STUDIÓW (PLAN STUDIÓW)

Dla każdego zakresu kształcenia opracowano oddzielny plan studiów. Ujęto w nich informacje dotyczące podziału treści kształcenia na poszczególne grupy: podstawowe, kierunkowe, kształcenie w zakresie i pracę dyplomową. Zawierają one także łączną liczbę godzin zajęć programowych z podziałem na rodzaj zajęć, przypisanymi punktami ECTS oraz formą zaliczenia w poszczególnych semestrach.

Ogólna liczba punktów ECTS dla każdego z przedmiotów/modułów została szczegółowo podzielona na punkty ECTS, które student musi uzyskać w ramach zajęć prowadzonych z bezpośrednim udziałem nauczycieli akademickich lub innych osób prowadzących zajęcia, tzw. kontaktowych, w ramach pracy własnej oraz w ramach zajęć związanych z prowadzoną na uczelni działalnością naukową w dyscyplinie nauk o bezpieczeństwie.

5.1. Plan studiów stacjonarnych dla zakresu Cyberbezpieczeństwo

PLAN STUDIÓW II STOPNIA

Kierunek studiów: Systemy informacyjne w bezpieczeństwie **Profil:** **ogólnoakademicki**

Specjalność: Cyberbezpieczeństwo **Forma:** **studia stacjonarne**

Indeks	Moduły, grupy przedmiotów, przedmioty	Kod przedmiotu	Razem godz.	Godziny kontaktowe (W, Ćw.,K)	Godz. praca własna	Punkty ECTS	Punkty ECTS kontaktowe	Punkty ECTS praca własna	W tym ECTS w dyscyplinie nauk.nauki o bezp.	Status przedm. [O/W]	Godz. zajęć razem	Liczba godzin według formy zajęć						Liczba godzin/rygor/pkt ECTS w semestrze:											
																		I			II			III			IV		
												wykłady	ćwiczenia	laboratoria	konsultacje, rozliczenie	zajęcia warsztatowe	projekt	Godz. kontaktowe	Rygor	Punkty ECTS	Godz. kontaktowe	Rygor	Punkty ECTS	Godz. kontaktowe	Rygor	Punkty ECTS	Godz. kontaktowe	Rygor	Punkty ECTS
A. Grupa treści podstawowych			**706**	**363**	**343**	**28**	**14,4**	**13,6**	**21,0**		**560**	**435**	**125**	**0**	**83**	**0**	**0**	**136**		**10**	**136**		**11**	**91**		**7**	**0**		**0**
A.1	Język angielski	Ja	50	35	15	2	1,4	0,6	0,0	O	30	0	30	0	5			35	Zo	2									
A.2	Geografia bezpieczeństwa	Dj	125	66	59	5	2,6	2,4	5,0	O	60	30	30	0	6			66	E	5									
A.3	Historia bezpieczeństwa	Yt	75	35	40	3	1,4	1,6	3,0	O	30	30	0	0	5			35	Zo	3									
A.4	Strategia bezpieczeństwa wewnętrznego	Ig	150	66	84	6	2,6	3,4	3,0	O	60	40	20	0	6						66	E	6						
A.5	Metodologia badań nad bezpieczeństwem	Cxm	75	35	40	3	1,4	1,6	3,0	O	30	15	15	0	5						35	Zo	3						
A.6	Podstawy ekonomii**	Cea	50	35	15	2	1,4	0,6	0,0	W	30	30	0	0	5						35	Zo	2						
A.7	Podstawy prawa**	Cap	50	35	15	2	1,4	0,6	0,0	W	30	30	0	0	5						35	Zo	2						
A.8	Wprowadzenie do psychologii społecznej**	Pps	50	35	15	2	1,4	0,6	0,0	W	30	30	0	0	5						35	Zo	2						
A.9	Podstawy socjologii**	Isx	50	35	15	2	1,4	0,6	0,0	W	30	30	0	0	5						35	Zo	2						
A.10	Podstawy stosunków międzynarodowych**	Ysq	50	35	15	2	1,4	0,6	0,0	W	30	30	0	0	5						35	Zo	2						
A.11	Podstawy bezpieczenstwa narodowego (pol./ang.)**	Ybc	75	35	40	3	1,4	1,6	3,0	W	30	30	0	0	5									35	Zo	3			
A.12	Podstawy zarządzania i organizacji**	Pko	75	35	40	3	1,4	1,6	0,0	W	30	30	0	0	5									35	Zo	3			
A.13	Podstawy filozofii i logiki**	Itn	75	35	40	3	1,4	1,6	0,0	W	30	30	0	0	5									35	Zo	3			
A.14	Podstawy pedagogiki**	Ppy	75	35	40	3	1,4	1,6	0,0	W	30	30	0	0	5									35	Zo	3			
A.15	Historia techniki**	Hta	75	35	40	3	1,4	1,6	0,0	W	30	30	0	0	5									35	Zo	3			
A.16	Ochrona ludności i obrona cywilna	Fc	106	56	50	4	2,1	1,9	4,0	O	50	20	30	0	6									56	E	4			
B. Grupa treści kierunkowych			**978**	**508**	**470**	**39**	**20,3**	**18,7**	**25,0**		**465**	**195**	**160**	**110**	**43**	**0**	**0**	**261**		**20**	**247**		**19**	**0**		**0**	**0**		**0**
B.1	Zarządzanie systemami bezpieczeństwa wewnętrznego	Zog	125	65	60	5	2,6	2,4	3,0	O	60	30	30	0	5			65	Zo	5									
B.2	Inżynieria systemów i projektowanie procesów	Zpa	125	65	60	5	2,6	2,4	4,0	O	60	20	0	40	5			65	Zo	5									
B.3	Audyt i certyfikacja systemów informatycznych	Oes	125	65	60	5	2,6	2,4	3,0	O	60	30	30	0	5			65	Zo	5									
B.4	Ocena ryzyka i prognozowanie w bezpieczeństwie	Zpa	126	66	60	5	2,6	2,4	3,0	O	60	20	40	0	6			66	E	5									
B.5	Zarządzanie projektem	Za	125	65	60	5	2,6	2,4	4,0	O	60	20	0	40	5						65	Zo	5						
B.6	Komunikacja społeczna	Iq	75	40	35	3	1,6	1,4	2,0	O	35	15	20	0	5						40	Zo	3						
B.7	Certyfikacja Systemu Zarządzania ISO/IEC 27001	Csz	151	76	75	6	3,0	3,0	4,0	O	70	30	40	0	6						76	E	6						
B.8	Sztuczna inteligencja	Osi	126	66	60	5	2,6	2,4	2,0	O	60	30	0	30	6						66	E	5						
C.Grupa treści szkolenia specjalistycznego			**1088**	**578**	**510**	**42**	**22,3**	**19,7**	**32,0**		**525**	**200**	**150**	**175**	**53**	**0**	**0**	**0**		**0**	**0**		**0**	**242**		**17**	**336**		**25**

C.1	Zarządzanie projektami informatycznymi	Ozo	126	66	60	5	2,6	2,4	3,0	W	60	25	35	0	6									66	E	5			
C.2	Akredytacja bezpieczeństwa teleinformatycznego	Ljb	80	50	30	3	1,9	1,1	4,0	W	45	20	25	0	5									50	Zo	3			
C.3	Testy penetracyjne	Mte	110	60	50	4	2,2	1,8	2,0	W	55	20	15	20	5									60	Zo	4			
C.4	Bezpieczeństwo sieci komputerowych i bezprzewodowych	Oxk	126	66	60	5	2,6	2,4	3,0	W	60	20	0	40	6									66	E	5			
C.5	Elementy kryptologii	Mkr	126	66	60	5	2,6	2,4	4,0	W	60	20	10	30	6												66	E	5
C.6	Administrowanie systemem Linux	Oxl	100	50	50	4	2,0	2,0	3,0	W	45	20	0	25	5												50	Zo	4
C.7	Cyberbezpieczeństwo	Lxc	105	55	50	4	2,1	1,9	3,0	W	50	10	10	30	5												55	Zo	4
C.8	Prognozowanie cyberzagrożeń	Lcp	105	55	50	4	2,1	1,9	5,0	W	50	20	30	0	5												55	Zo	4
C.9	Symulacja komputerowa	Oku	105	55	50	4	2,1	1,9	3,0	W	50	20	0	30	5												55	Zo	4
C.10	Podstawy prawne cyberbezpieczeństwa	Ccq	105	55	50	4	2,1	1,9	2,0	W	50	25	25	0	5												55	Zo	4
D. Praca dyplomowa			**275**	**85**	**190**	**11**	**3,4**	**7,6**	**11,0**		**70**	**10**	**60**	**0**	**15**	**0**	**0**	**0**		**0**	**0**		**0**	**50**		**6**	**35**		**5**
D.1	Seminarium dyplomowe i prawa autorskie	Axp	25	15	10	1	0,6	0,4	1,0	W	10	10	0	0	5									15	Zo	1			
D.2	Praca dyplomowa	Add	250	70	180	10	2,8	7,2	10,0	W	60	0	60	0	10									35	Z	5	35	Z	5
	ogółem godzin / pkt. ECTS		**3047**	**1534**	**1513**	**120**	**60,3**	**59,7**	**89,0**		**1620**	**840**	**495**	**285**	**194**	**0**	**0**	**397**		**30**	**383**		**30**	**383**		**30**	**371**		**30**
														egzamin - E				**2**			**3**			**3**			**1**	
													Rodzaje i liczba rygorów w semestrze:	**zaliczenie - Z**				**0**			**0**			**1**			**1**	
														projekt - P				**0**			**0**			**0**			**0**	

Wskaźniki		
Łączna liczba punktów ECTS, którą student musi uzyskać na zajęciach prowadzonych z bezpośrednim udziałem nauczycieli akademickich lub innych osób prowadzących zajęcia (co najmniej 50%)	**60,3**	**50,3%**
Łączna liczba punktów ECTS w ramach zajęć do wyboru, nie mniej niż 30% liczby punktów ECTS (A5-A14+C+D)	**78,0**	**65,0%**
Łączna liczba punktów ECTS w ramach zajęć związanych z prowadzoną w uczelni działalnością naukową w dyscyplinie nauki o bezpieczeństwie (więcej niż 50% punktów ECTS)	**89,0**	**74,2%**

5.2. Plan studiów stacjonarnych dla zakresu Analiza danych i informatyka śledcza

PLAN STUDIÓW II STOPNIA

Kierunek studiów: Systemy informacyjne w bezpieczeństwie **Profil:** **ogólnoakademicki**

Specjalność: Analiza danych i informatyka śledcza **Forma:** **studia stacjonarne**

Indeks	Moduły, grupy przedmiotów, przedmioty	Kod przedmiotu	Razem godz.	Godziny kontaktowe (W, Ćw.,K)	Godz. praca własna	Punkty ECTS	Punkty ECTS kontaktowe	Punkty ECTS praca własna	W tym ECTS w dyscyplinie nauk.nauki o bezp.	Status przedm. [O/W]	Godz. zajęć razem	Liczba godzin według formy zajęć						Liczba godzin/rygor/pkt ECTS w semestrze:											
																		I			II			III			IV		
												wykłady	ćwiczenia	laboratoria	konsultacje, rozliczenie	zajęcia warsztatowe	projekt	Godz. kontaktowe	Rygor	Punkty ECTS	Godz. kontaktowe	Rygor	Punkty ECTS	Godz. kontaktowe	Rygor	Punkty ECTS	Godz. kontaktowe	Rygor	Punkty ECTS
A. Grupa treści podstawowych			**706**	**363**	**343**	**28**	**14,4**	**13,6**	**21,0**		**560**	**435**	**125**	**0**	**83**	**0**	**0**	**136**		**10**	**136**		**11**	**91**		**7**	**0**		**0**
A.1	Język angielski	Ja	50	35	15	2	1,4	0,6	0,0	O	30	0	30	0	5			35	Zo	2									
A.2	Geografia bezpieczeństwa	Dj	125	66	59	5	2,6	2,4	5,0	O	60	30	30	0	6			66	E	5									
A.3	Historia bezpieczeństwa	Yt	75	35	40	3	1,4	1,6	3,0	O	30	30	0	0	5			35	Zo	3									
A.4	Strategia bezpieczeństwa wewnętrznego	Ig	150	66	84	6	2,6	3,4	3,0	O	60	40	20	0	6						66	E	6						
A.5	Metodologia badań nad bezpieczeństwem	Cxm	75	35	40	3	1,4	1,6	3,0	O	30	15	15	0	5						35	Zo	3						
A.6	Podstawy ekonomii**	Cea	50	35	15	2	1,4	0,6	0,0	W	30	30	0	0	5						35	Zo	2						
A.7	Podstawy prawa**	Cap	50	35	15	2	1,4	0,6	0,0	W	30	30	0	0	5						35	Zo	2						
A.8	Wprowadzenie do psychologii społecznej**	Pps	50	35	15	2	1,4	0,6	0,0	W	30	30	0	0	5						35	Zo	2						
A.9	Podstawy socjologii**	Isx	50	35	15	2	1,4	0,6	0,0	W	30	30	0	0	5						35	Zo	2						
A.10	Podstawy stosunków międzynarodowych**	Ysq	50	35	15	2	1,4	0,6	0,0	W	30	30	0	0	5						35	Zo	2						
A.11	Podstawy bezpieczenstwa narodowego (pol./ang.)**	Ybc	75	35	40	3	1,4	1,6	3,0	W	30	30	0	0	5									35	Zo	3			
A.12	Podstawy zarządzania i organizacji**	Pko	75	35	40	3	1,4	1,6	0,0	W	30	30	0	0	5									35	Zo	3			
A.13	Podstawy filozofii i logiki**	Itn	75	35	40	3	1,4	1,6	0,0	W	30	30	0	0	5									35	Zo	3			
A.14	Podstawy pedagogiki**	Ppy	75	35	40	3	1,4	1,6	0,0	W	30	30	0	0	5									35	Zo	3			
A.15	Historia techniki**	Hta	75	35	40	3	1,4	1,6	0,0	W	30	30	0	0	5									35	Zo	3			
A.16	Ochrona ludności i obrona cywilna	Fc	106	56	50	4	2,1	1,9	4,0	O	50	20	30	0	6									56	E	4			
B. Grupa treści kierunkowych			**978**	**508**	**470**	**39**	**20,3**	**18,7**	**25,0**		**465**	**195**	**160**	**110**	**43**	**0**	**0**	**261**		**20**	**247**		**19**	**0**		**0**	**0**		**0**
B.1	Zarządzanie systemami bezpieczeństwa wewnętrznego	Zog	125	65	60	5	2,6	2,4	3,0	O	60	30	30	0	5			65	Zo	5									
B.2	Inżynieria systemów i projektowanie procesów	Zpa	125	65	60	5	2,6	2,4	4,0	O	60	20	0	40	5			65	Zo	5									
B.3	Audyt i certyfikacja systemów informatycznych	Oes	125	65	60	5	2,6	2,4	3,0	O	60	30	30	0	5			65	Zo	5									
B.4	Ocena ryzyka i prognozowanie w bezpieczeństwie	Zpa	126	66	60	5	2,6	2,4	3,0	O	60	20	40	0	6			66	E	5									
B.5	Zarządzanie projektem	Za	125	65	60	5	2,6	2,4	4,0	O	60	20	0	40	5						65	Zo	5						
B.6	Komunikacja społeczna	Iq	75	40	35	3	1,6	1,4	2,0	O	35	15	20	0	5						40	Zo	3						
B.7	Certyfikacja Systemu Zarządzania ISO/IEC 27001	Csz	151	76	75	6	3,0	3,0	4,0	O	70	30	40	0	6						76	E	6						
B.8	Sztuczna inteligencja	Osi	126	66	60	5	2,6	2,4	2,0	O	60	30	0	30	6						66	E	5						
C.Grupa treści szkolenia specjalistycznego			**1088**	**578**	**510**	**42**	**22,3**	**19,7**	**23,0**		**525**	**210**	**135**	**180**	**53**	**0**	**0**	**0**		**0**	**0**		**0**	**242**		**17**	**336**		**25**
C.1	Pozyskiwanie i analiza danych z technologii bezzałogowych	Wyn	126	66	60	5	2,6	2,4	3,0	W	60	20	20	20	6									66	E	5			

C.2	Zastosowanie kryptologii w informatyce śledczej	Lju	80	50	30	3	1,9	1,1	2,0	W	45	20	0	25	5									50	Zo	3			
C.3	Testy penetracyjne	Mte	110	60	50	4	2,2	1,8	2,0	W	55	20	15	20	5									60	Zo	4			
C.4	Bezpieczeństwo sieci komputerowych i bezprzewodowych	Oxk	126	66	60	5	2,6	2,4	3,0	W	60	20	0	40	6									66	E	5			
C.5	Techniki pozyskiwania cyfrowego materiału dowodowego	Lkh	126	66	60	5	2,6	2,4	3,0	W	60	20	0	40	6												66	E	5
C.6	Biały wywiad – techniki zaawansowane	Tbx	100	50	50	4	2,0	2,0	2,0	W	45	20	25	0	5												50	Zo	4
C.7	Zarzadzanie ryzykiem bezpieczeństwa systemów	Ojb	105	55	50	4	2,1	1,9	2,0	W	50	25	25	0	5												55	Zo	4
C.8	Zagrożenia bezpieczeństwa aplikacji i systemów	Ojc	105	55	50	4	2,1	1,9	2,0	W	50	20	15	15	5												55	Zo	4
C.9	Metody ataku i obrony w cyberprzestrzeni	Lxi	105	55	50	4	2,1	1,9	2,0	W	50	20	10	20	5												55	Zo	4
C.10	Podstawy prawne cyberbezpieczeństwa	Ccq	105	55	50	4	2,1	1,9	2,0	W	50	25	25	0	5												55	Zo	4
D. Praca dyplomowa			**275**	**85**	**190**	**11**	**3,4**	**7,6**	**11,0**		**70**	**10**	**60**	**0**	**15**	**0**	**0**	**0**		**0**	**0**		**0**	**50**		**6**	**35**		**5**
D.1	Seminarium dyplomowe i prawa autorskie	Axp	25	15	10	1	0,6	0,4	1,0	W	10	10	0	0	5									15	Zo	1			
D.2	Praca dyplomowa	Add	250	70	180	10	2,8	7,2	10,0	W	60	0	60	0	10									35	Z	5	35	Z	5
	ogółem godzin / pkt. ECTS		**3047**	**1534**	**1513**	**120**	**60,3**	**59,7**	**80,0**		**1620**	**850**	**480**	**290**	**194**	**0**	**0**	**397**		**30**	**383**		**30**	**383**		**30**	**371**		**30**
														egzamin - E			**2**			**3**			**3**			**1**	
											Rodzaje i liczba rygorów w semestrze:			**zaliczenie - Z**			**0**			**0**			**1**			**1**	
														projekt - P			**0**			**0**			**0**			**0**	

Wskaźniki		
Łączna liczba punktów ECTS, którą student musi uzyskać na zajęciach prowadzonych z bezpośrednim udziałem nauczycieli akademickich lub innych osób prowadzących zajęcia (co najmniej 50%)	**60,3**	**50,3%**
Łączna liczba punktów ECTS w ramach zajęć do wyboru, nie mniej niż 30% liczby punktów ECTS (A5-A14+C+D)	**78,0**	**65,0%**
Łączna liczba punktów ECTS w ramach zajęć związanych z prowadzoną w uczelni działalnością naukową w dyscyplinie nauki o bezpieczeństwie (więcej niż 50% punktów ECTS)	**80,0**	**66,7%**

5.3. Plan studiów niestacjonarnych dla zakresu Cyberbezpieczeństwo

PLAN STUDIÓW II STOPNIA

Kierunek studiów: Systemy informacyjne w bezpieczeństwie

Profil: ogólnoakademicki

Specjalność: Cyberbezpieczeństwo

Forma: studia niestacjonarne

Indeks	Moduły, grupy przedmiotów, przedmioty	Kod przedm.	Razem godz.	Godziny kontaktowe (W, Ćw.,K)	Godz. praca własna	Punkty ECTS	Punkty ECTS kontaktowe	Punkty ECTS praca własna	W tym ECTS w dyscyplinie nauk.nauki o bezp.	Status przedm. [O/W]	Godz. zajęć razem	Liczba godzin według formy zajęć						Liczba godzin/rygor/pkt ECTS w semestrze:											
																		I			II			III			IV		
												wykłady	ćwiczenia	laboratoria	konsultacje, rozliczenie	zajęcia warsztatowe	projekt	Godz. kontaktowe	Rygor	Punkty ECTS	Godz. kontaktowe	Rygor	Punkty ECTS	Godz. kontaktowe	Rygor	Punkty ECTS	Godz. kontaktowe	Rygor	Punkty ECTS
A. Grupa treści podstawowych			**706**	**230**	**476**	**28**	**9,1**	**18,9**	**21,0**		**315**	**235**	**80**	**0**	**83**	**0**	**0**	**96**		**10**	**82**		**11**	**52**		**7**	**0**		**0**
A.1	Język angielski	Ja	50	35	15	2	1,4	0,6	0,0	O	30	0	30	0	5			35	Zo	2									
A.2	Geografia bezpieczeństwa	Dj	125	36	89	5	1,4	3,6	5,0	O	30	15	15	0	6			36	E	5									
A.3	Historia bezpieczeństwa	Yt	75	25	50	3	1,0	2,0	3,0	O	20	20	0	0	5			25	Zo	3									
A.4	Strategia bezpieczeństwa wewnętrznego	Ig	150	36	114	6	1,4	4,6	3,0	O	30	20	10	0	6						36	E	6						
A.5	Metodologia badań nad bezpieczeństwem	Cxm	75	25	50	3	1,0	2,0	3,0	O	20	10	10	0	5						25	Zo	3						
A.6	Podstawy ekonomii**	Cea	50	21	29	2	0,8	1,2	0,0	W	16	16	0	0	5						21	Zo	2						
A.7	Podstawy prawa**	Cap	50	21	29	2	0,8	1,2	0,0	W	16	16	0	0	5						21	Zo	2						
A.8	Wprowadzenie do psychologii społecznej**	Pps	50	21	29	2	0,8	1,2	0,0	W	16	16	0	0	5						21	Zo	2						
A.9	Podstawy socjologii**	Isx	50	21	29	2	0,8	1,2	0,0	W	16	16	0	0	5						21	Zo	2						
A.10	Podstawy stosunków międzynarodowych**	Ysq	50	21	29	2	0,8	1,2	0,0	W	16	16	0	0	5						21	Zo	2						
A.11	Podstawy bezpieczenstwa narodowego (pol./ang.)**	Ybc	75	21	54	3	0,8	2,2	3,0	W	16	16	0	0	5									21	Zo	3			
A.12	Podstawy zarządzania i organizacji**	Pko	75	21	54	3	0,8	2,2	0,0	W	16	16	0	0	5									21	Zo	3			
A.13	Podstawy filozofii i logiki**	Itn	75	21	54	3	0,8	2,2	0,0	W	16	16	0	0	5									21	Zo	3			
A.14	Podstawy pedagogiki**	Ppy	75	21	54	3	0,8	2,2	0,0	W	16	16	0	0	5									21	Zo	3			
A.15	Historia techniki**	Hta	75	21	54	3	0,8	2,2	0,0	W	16	16	0	0	5									21	Zo	3			
A.16	Ochrona ludności i obrona cywilna	Fc	106	31	75	4	1,2	2,8	4,0	O	25	10	15	0	6									31	E	4			
B. Grupa treści kierunkowych			**978**	**313**	**665**	**39**	**12,5**	**26,5**	**26,0**		**270**	**115**	**95**	**60**	**43**	**0**	**0**	**161**		**20**	**152**		**19**	**0**		**0**	**0**		**0**
B.1	Zarządzanie systemami bezpieczeństwa wewnętrznego	Zog	125	40	85	5	1,6	3,4	3,0	O	35	15	20	0	5			40	Zo	5									
B.2	Inżynieria systemów i projektowanie procesów	Zpa	125	40	85	5	1,6	3,4	4,0	O	35	15	0	20	5			40	Zo	5									
B.3	Audyt i certyfikacja systemów informatycznych	Oes	125	40	85	5	1,6	3,4	3,0	O	35	15	20	0	5			40	Zo	5									
B.4	Ocena ryzyka i prognozowanie w bezpieczeństwie	Zpa	126	41	85	5	1,6	3,4	3,0	O	35	15	20	0	6			41	E	5									
B.5	Zarządzanie projektem	Za	125	40	85	5	1,6	3,4	4,0	O	35	15	0	20	5						40	Zo	5						
B.6	Komunikacja społeczna	Iq	75	25	50	3	1,0	2,0	2,0	O	20	10	10	0	5						25	Zo	3						
B.7	Certyfikacja Systemu Zarządzania ISO/IEC 27001	Csz	151	46	105	6	1,8	4,2	4,0	O	40	15	25	0	6						46	E	6						
B.8	Sztuczna inteligencja	Osi	126	41	85	5	1,6	3,4	3,0	O	35	15	0	20	6						41	E	5						
C.Grupa treści szkolenia specjalistycznego			**1088**	**338**	**750**	**42**	**13,0**	**29,0**	**31,0**		**285**	**110**	**65**	**110**	**53**	**0**	**0**	**0**		**0**	**0**		**0**	**137**		**17**	**201**		**25**

C.1	Zarządzanie projektami informatycznymi	Ozo	126	41	85	5	1,6	3,4	2,0	W	35	15	20	0	6								41	E	5					
C.2	Akredytacja bezpieczeństwa teleinformatycznego	Ljb	80	25	55	3	0,9	2,1	3,0	W	20	10	10	0	5								25	Zo	3					
C.3	Testy penetracyjne	Mte	110	35	75	4	1,3	2,7	3,0	W	30	10	10	10	5								35	Zo	4					
C.4	Bezpieczeństwo sieci komputerowych i bezprzewodowych	Oxk	126	36	90	5	1,4	3,6	4,0	W	30	10	0	20	6								36	E	5					
C.5	Elementy kryptologii	Mkr	126	36	90	5	1,4	3,6	2,0	W	30	10	5	15	6											36	E	5		
C.6	Administrowanie systemem Linux	Oxl	100	25	75	4	1,0	3,0	4,0	W	20	10	0	10	5											25	Zo	4		
C.7	Cyberbezpieczeństwo	Lxc	105	35	70	4	1,3	2,7	3,0	W	30	10	5	15	5											35	Zo	4		
C.8	Prognozowanie cyberzagrożeń	Lcp	105	35	70	4	1,3	2,7	5,0	W	30	10	0	20	5											35	Zo	4		
C.9	Symulacja komputerowa	Oku	105	35	70	4	1,3	2,7	3,0	W	30	10	0	20	5											35	Zo	4		
C.10	Podstawy prawne cyberbezpieczeństwa	Ccq	105	35	70	4	1,3	2,7	2,0	W	30	15	15	0	5											35	Zo	4		
D. Praca dyplomowa			**275**	**85**	**190**	**11**	**3,4**	**7,6**	**11,0**		**70**	**10**	**60**	**0**	**15**	**0**	**0**	**0**		**0**	**0**		**0**	**50**		**6**	**35**		**5**
D.1	Seminarium dyplomowe i prawa autorskie	Axp	25	15	10	1	0,6	0,4	1,0	W	10	10	0	0	5								15	Zo	1					
D.2	Praca dyplomowa	Add	250	70	180	10	2,8	7,2	10,0	W	60	0	60	0	10								35	Z	5	35	Z	5		
	ogółem godzin / pkt. ECTS		**3047**	**966**	**2081**	**120**	**38,0**	**82,0**	**89,0**		**940**	**470**	**300**	**170**	**194**	**0**	**0**	**257**		**30**	**234**		**30**	**239**		**30**	**236**		**30**
														egzamin - E				**2**			**3**			**3**			**1**		
														zaliczenie - Z				**0**			**0**			**1**			**1**		
														projekt - P				**0**			**0**			**0**			**0**		

Rodzaje i liczba rygorów w semestrze:

Wskaźniki		
Łączna liczba punktów ECTS, którą student musi uzyskać na zajęciach prowadzonych z bezpośrednim udziałem nauczycieli akademickich lub innych osób prowadzących zajęcia (co najmniej 30%)	**38,0**	**31,7%**
Łączna liczba punktów ECTS w ramach zajęć do wyboru, nie mniej niż 30% liczby punktów ECTS (A5-A14+C+D)	**78,0**	**65,0%**
Łączna liczba punktów ECTS w ramach zajęć związanych z prowadzoną w uczelni działalnością naukową w dyscyplinie nauki o bezpieczeństwie (więcej niż 50% punktów ECTS)	**89,0**	**74,2%**

5.4. Plan studiów niestacjonarnych dla zakresu Analiza danych i informatyka śledcza

PLAN STUDIÓW II STOPNIA

Kierunek studiów: Systemy informacyjne w bezpieczeństwie

Profil: ogólnoakademicki

Specjalność: Analiza danych i informatyka śledcza

Forma: studia niestacjonarne

Indeks	Moduły, grupy przedmiotów, przedmioty	Kod przedm.	Razem godz.	Godziny kontaktowe (W, Ćw.,K)	Godz. praca własna	Punkty ECTS	Punkty ECTS kontaktowe	Punkty ECTS praca własna	W tym ECTS w dyscyplinie nauk.nauki o bezp.	Status przedm. [O/W]	Godz. zajęć razem	Liczba godzin według formy zajęć						Liczba godzin/rygor/pkt ECTS w semestrze:											
																		I			II			III			IV		
												wykłady	ćwiczenia	laboratoria	konsultacje, rozliczenie	zajęcia warsztatowe	projekt	Godz. kontaktowe	Rygor	Punkty ECTS	Godz. kontaktowe	Rygor	Punkty ECTS	Godz. kontaktowe	Rygor	Punkty ECTS	Godz. kontaktowe	Rygor	Punkty ECTS
A. Grupa treści podstawowych			**706**	**230**	**476**	**28**	**9,1**	**18,9**	**21,0**		**315**	**235**	**80**	**0**	**83**	**0**	**0**	**96**		**10**	**82**		**11**	**52**		**7**	**0**		**0**
A.1	Język angielski	Ja	50	35	15	2	1,4	0,6	0,0	O	30	0	30	0	5			35	Zo	2									
A.2	Geografia bezpieczeństwa	Dj	125	36	89	5	1,4	3,6	5,0	O	30	15	15	0	6			36	E	5									
A.3	Historia bezpieczeństwa	Yt	75	25	50	3	1,0	2,0	3,0	O	20	20	0	0	5			25	Zo	3									
A.4	Strategia bezpieczeństwa wewnętrznego	Ig	150	36	114	6	1,4	4,6	3,0	O	30	20	10	0	6						36	E	6						
A.5	Metodologia badań nad bezpieczeństwem	Cxm	75	25	50	3	1,0	2,0	3,0	O	20	10	10	0	5						25	Zo	3						
A.6	Podstawy ekonomii**	Cea	50	21	29	2	0,8	1,2	0,0	W	16	16	0	0	5						21	Zo	2						
A.7	Podstawy prawa**	Cap	50	21	29	2	0,8	1,2	0,0	W	16	16	0	0	5						21	Zo	2						
A.8	Wprowadzenie do psychologii społecznej**	Pps	50	21	29	2	0,8	1,2	0,0	W	16	16	0	0	5						21	Zo	2						
A.9	Podstawy socjologii**	Isx	50	21	29	2	0,8	1,2	0,0	W	16	16	0	0	5						21	Zo	2						
A.10	Podstawy stosunków międzynarodowych**	Ysq	50	21	29	2	0,8	1,2	0,0	W	16	16	0	0	5						21	Zo	2						
A.11	Podstawy bezpieczenstwa narodowego (pol./ang.)**	Ybc	75	21	54	3	0,8	2,2	3,0	W	16	16	0	0	5									21	Zo	3			
A.12	Podstawy zarządzania i organizacji**	Pko	75	21	54	3	0,8	2,2	0,0	W	16	16	0	0	5									21	Zo	3			
A.13	Podstawy filozofii i logiki**	Itn	75	21	54	3	0,8	2,2	0,0	W	16	16	0	0	5									21	Zo	3			
A.14	Podstawy pedagogiki**	Ppy	75	21	54	3	0,8	2,2	0,0	W	16	16	0	0	5									21	Zo	3			
A.15	Historia techniki**	Hta	75	21	54	3	0,8	2,2	0,0	W	16	16	0	0	5									21	Zo	3			
A.16	Ochrona ludności i obrona cywilna	Fc	106	31	75	4	1,2	2,8	4,0	O	25	10	15	0	6									31	E	4			
B. Grupa treści kierunkowych			**978**	**313**	**665**	**39**	**12,5**	**26,5**	**26,0**		**270**	**115**	**95**	**60**	**43**	**0**	**0**	**161**		**20**	**152**		**19**	**0**		**0**	**0**		**0**
B.1	Zarządzanie systemami bezpieczeństwa wewnętrznego	Zog	125	40	85	5	1,6	3,4	3,0	O	35	15	20	0	5			40	Zo	5									
B.2	Inżynieria systemów i projektowanie procesów	Zpa	125	40	85	5	1,6	3,4	4,0	O	35	15	0	20	5			40	Zo	5									
B.3	Audyt i certyfikacja systemów informatycznych	Oes	125	40	85	5	1,6	3,4	3,0	O	35	15	20	0	5			40	Zo	5									
B.4	Ocena ryzyka i prognozowanie w bezpieczeństwie	Zpa	126	41	85	5	1,6	3,4	3,0	O	35	15	20	0	6			41	E	5									
B.5	Zarządzanie projektem	Za	125	40	85	5	1,6	3,4	4,0	O	35	15	0	20	5						40	Zo	5						
B.6	Komunikacja społeczna	Iq	75	25	50	3	1,0	2,0	2,0	O	20	10	10	0	5						25	Zo	3						
B.7	Certyfikacja Systemu Zarządzania ISO/IEC 27001	Csz	151	46	105	6	1,8	4,2	4,0	O	40	15	25	0	6						46	E	6						
B.8	Sztuczna inteligencja	Osi	126	41	85	5	1,6	3,4	3,0	O	35	15	0	20	6						41	E	5						
C.Grupa treści szkolenia specjalistycznego			**1088**	**333**	**755**	**42**	**12,8**	**29,2**	**31,0**		**280**	**105**	**65**	**110**	**53**	**0**	**0**	**0**		**0**	**0**		**0**	**132**		**17**	**201**		**25**

C.1	Pozyskiwanie i analiza danych z technologii bezzałogowych	Wyn	126	36	90	5	1,4	3,6	2,0	W	30	10	20	0	6									36	E	5			
C.2	Zastosowanie kryptologii w informatyce śledczej	Lju	80	25	55	3	0,9	2,1	3,0	W	20	10	10	0	5									25	Zo	3			
C.3	Testy penetracyjne	Mte	110	35	75	4	1,3	2,7	3,0	W	30	10	10	10	5									35	Zo	4			
C.4	Bezpieczeństwo sieci komputerowych i bezprzewodowych	Oxk	126	36	90	5	1,4	3,6	4,0	W	30	10	0	20	6									36	E	5			
C.5	Techniki pozyskiwania cyfrowego materiału dowodowego	Lkh	126	36	90	5	1,4	3,6	2,0	W	30	10	5	15	6												36	E	5
C.6	Biały wywiad – techniki zaawansowane	Tbx	100	25	75	4	1,0	3,0	4,0	W	20	10	0	10	5												25	Zo	4
C.7	Zarzadzanie ryzykiem bezpieczeństwa systemów	Ojb	105	35	70	4	1,3	2,7	3,0	W	30	10	5	15	5												35	Zo	4
C.8	Zagrożenia bezpieczeństwa aplikacji i systemów	Ojc	105	35	70	4	1,3	2,7	5,0	W	30	10	0	20	5												35	Zo	4
C.9	Metody ataku i obrony w cyberprzestrzeni	Lxi	105	35	70	4	1,3	2,7	3,0	W	30	10	0	20	5												35	Zo	4
C.10	Podstawy prawne cyberbezpieczeństwa	Ccq	105	35	70	4	1,3	2,7	2,0	W	30	15	15	0	5												35	Zo	4
D. Praca dyplomowa			**275**	**85**	**190**	**11**	**3,4**	**7,6**	**11,0**		**70**	**10**	**60**	**0**	**15**	**0**	**0**	**0**		**0**	**0**		**0**	**50**		**6**	**35**		**5**
D.1	Seminarium dyplomowe i prawa autorskie	Axp	25	15	10	1	0,6	0,4	1,0	W	10	10	0	0	5									15	Zo	1			
D.2	Praca dyplomowa	Add	250	70	180	10	2,8	7,2	10,0	W	60	0	60	0	10									35	Z	5	35	Z	5
	ogółem godzin / pkt. ECTS		**3047**	**961**	**2086**	**120**	**37,8**	**82,2**	**89,0**		**935**	**465**	**300**	**170**	**194**	**0**	**0**	**257**		**30**	**234**		**30**	**234**		**30**	**236**		**30**
														egzamin - E		**2**			**3**			**3**			**1**		
													Rodzaje i liczba rygorów w semestrze:	**zaliczenie - Z**		**0**			**0**			**1**			**1**		
														projekt - P		**0**			**0**			**0**			**0**		

Wskaźniki		
Łączna liczba punktów ECTS, którą student musi uzyskać na zajęciach prowadzonych z bezpośrednim udziałem nauczycieli akademickich lub innych osób prowadzących zajęcia (co najmniej 30%)	**37,8**	**31,5%**
Łączna liczba punktów ECTS w ramach zajęć do wyboru, nie mniej niż 30% liczby punktów ECTS (A5-A14+C+D)	**78,0**	**65,0%**
Łączna liczba punktów ECTS w ramach zajęć związanych z prowadzoną w uczelni działalnością naukową w dyscyplinie nauki o bezpieczeństwie (więcej niż 50% punktów ECTS)	**89,0**	**74,2%**

6. BILANS PUNKTÓW ECTS

6.1. Wskaźniki łączne dotyczące programu studiów stacjonarnych II stopnia – zakres Cyberbezpieczeństwo

Kategoria	Liczba punktów ECTS
Wskaźniki dotyczące programu studiów na kierunku Systemy informacyjne w bezpieczeństwie, poziomie i profilu kształcenia	
Liczba punktów ECTS konieczna do uzyskania kwalifikacji odpowiadających poziomowi kształcenia	**120**
Łączna liczba punktów ECTS jaką student musi uzyskać w ramach zajęć prowadzonych z bezpośrednim udziałem nauczycieli akademickich lub innych osób prowadzących zajęcia	**60,3**
Łączna liczba punktów ECTS, jaką student musi uzyskać w ramach zajęć z dziedziny nauk humanistycznych.	**>5***
Łączna liczba punktów ECTS w ramach zajęć związanych z prowadzoną w uczelni działalnością naukową w dyscyplinie nauki o bezpieczeństwie	**89**
Liczba punktów ECTS przyporządkowana zajęciom do wyboru	**78**
Liczba punktów ECTS przyporządkowana praktykom zawodowym oraz liczba godzin praktyk zawodowych	**X**

* kierunek studiów przypisany do dziedziny nauk społecznych

6.1.1. Łączna liczba punktów ECTS jaką student musi uzyskać w ramach zajęć prowadzonych z bezpośrednim udziałem nauczycieli akademickich lub innych osób prowadzących zajęcia

Moduły zajęć związane z bezpośrednim udziałem nauczycieli akademickich lub innych osób prowadzących zajęcia			
Nazwa modułu zajęć	**Forma/formy zajęć**	**Łączna liczba godzin**	**Liczba punktów ECTS**
A. Grupa treści podstawowych	wykład, ćwiczenia	363	14,4
B. Grupa treści kierunkowych	wykład, ćwiczenia	508	20,3
C. Grupa treści kształcenia w zakresie **Cyberbezpieczeństwo**	wykład, ćwiczenia	578	22,3
D. Praca dyplomowa	wykład, ćwiczenia	85	3,4
Razem pkt. ECTS:			**60,3**
Wskaźnik % do ogółu pkt. ECTS			**50,3%**

6.1.2. Łączna liczba punktów ECTS w ramach zajęć związanych z prowadzoną w uczelni działalnością naukową w dyscyplinie nauki o bezpieczeństwie (więcej niż 50% punktów ECTS)

Moduły zajęć związanych z prowadzoną w uczelni działalnością naukową w dyscyplinie nauki o bezpieczeństwie		
Nazwa modułu zajęć	**Forma/formy zajęć**	**Liczba punktów ECTS**
A. Grupa treści podstawowych	wykład, ćwiczenia	21,0
B. Grupa treści kierunkowych	wykład, ćwiczenia	25,0
C. Grupa treści kształcenia w zakresie **Cyberbezpieczeństwo**	wykład, ćwiczenia	32,0
D. Praca dyplomowa	wykład, ćwiczenia	11,00
Razem pkt. ECTS:		**89,0**
Wskaźnik % do ogółu pkt. ECTS		**74,2%**

6.1.3. Łączna liczba punktów ECTS w ramach zajęć do wyboru, nie mniej niż 30% liczby punktów ECTS

Kod i nazwa przedmiotu/modułu do wyboru			
Kod i nazwa przedmiotu/modułu	**Forma/formy zajęć**	**Łączna liczba godzin**	**Liczba punktów ECTS**
A6. Podstawy ekonomii*	wykład	50	2
A7. Podstawy prawa*	wykład	50	2
A8. Wprowadzenie do psychologii społecznej**	wykład	50	2
A9. Podstawy socjologii*	wykład	50	2
A10. Podstawy stosunków międzynarodowych*	wykład	50	2
A11. Podstawy bezpieczenstwa narodowego (pol./ang.)*	wykład	75	3
A12. Podstawy zarządzania i organizacji*	wykład	75	3
A13. Podstawy filozofii i logiki*	wykład	75	3
A14. Podstawy pedagogiki*	wykład	75	3
A15. Historia techniki*	wykład	75	3
C. Grupa treści kształcenia w zakresie **Cyberbezpieczeństwo**	wykład/ćwiczenia	1088	42
D. Praca dyplomowa	wykład/ćwiczenia	275	11
Razem pkt. ECTS:			**78**
Wskaźnik % do ogółu pkt. ECTS			**65,0%**

* Spośród tych przedmiotów student wybiera co najmniej po jednym przedmiocie w semestrze II i III, tak by uzyskać w sumie co najmniej 5 pkt ECTS.

6.2. Wskaźniki łączne dotyczące programu studiów stacjonarnych II stopnia – zakres Analiza danych i informatyka śledcza

Kategoria **Wskaźniki dotyczące programu studiów na kierunku Systemy informacyjne w bezpieczeństwie, poziomie i profilu kształcenia**	**Liczba punktów ECTS**
Liczba punktów ECTS konieczna do uzyskania kwalifikacji odpowiadających poziomowi kształcenia	**120**
Łączna liczba punktów ECTS jaką student musi uzyskać w ramach zajęć prowadzonych z bezpośrednim udziałem nauczycieli akademickich lub innych osób prowadzących zajęcia	**60,3**
Łączna liczba punktów ECTS, jaką student musi uzyskać w ramach zajęć z dziedziny nauk humanistycznych.	**>5***
Łączna liczba punktów ECTS w ramach zajęć związanych z prowadzoną w uczelni działalnością naukową w dyscyplinie nauki o bezpieczeństwie	**80**
Liczba punktów ECTS przyporządkowana zajęciom do wyboru	**78**
Liczba punktów ECTS przyporządkowana praktykom zawodowym oraz liczba godzin praktyk zawodowych	**X**

* kierunek studiów przypisany do dziedziny nauk społecznych

6.2.1. Łączna liczba punktów ECTS jaką student musi uzyskać w ramach zajęć prowadzonych z bezpośrednim udziałem nauczycieli akademickich lub innych osób prowadzących zajęcia

Moduły zajęć związane z bezpośrednim udziałem nauczycieli akademickich lub innych osób prowadzących zajęcia			
Nazwa modułu zajęć	**Forma/formy zajęć**	**Łączna liczba godzin**	**Liczba punktów ECTS**
A. Grupa treści podstawowych	wykład, ćwiczenia	363	14,4
B. Grupa treści kierunkowych	wykład, ćwiczenia	508	20,3
C. Grupa treści kształcenia w zakresie **Analiza danych i informatyka śledcza**	wykład, ćwiczenia	578	22,3
D. Praca dyplomowa	wykład, ćwiczenia	85	3,4
Razem pkt. ECTS:			**60,3**
Wskaźnik % do ogółu pkt. ECTS			**50,3%**

6.2.2. Łączna liczba punktów ECTS w ramach zajęć związanych z prowadzoną w uczelni działalnością naukową w dyscyplinie nauki o bezpieczeństwie (więcej niż 50% punktów ECTS)

Moduły zajęć związanych z prowadzoną w uczelni działalnością naukową w dyscyplinie nauki o bezpieczeństwie		
Nazwa modułu zajęć	**Forma/formy zajęć**	**Liczba punktów ECTS**
A. Grupa treści podstawowych	wykład, ćwiczenia	21,0
B. Grupa treści kierunkowych	wykład, ćwiczenia	25,0
C. Grupa treści kształcenia w zakresie **Analiza danych i informatyka śledcza**	wykład, ćwiczenia	23,0
D. Praca dyplomowa	wykład, ćwiczenia	11,00
Razem pkt. ECTS:		**80,0**
Wskaźnik % do ogółu pkt. ECTS		**66,7%**

6.2.3. Łączna liczba punktów ECTS w ramach zajęć do wyboru, nie mniej niż 30% liczby punktów ECTS

Kod i nazwa przedmiotu/modułu do wyboru			
Kod i nazwa przedmiotu/modułu	**Forma/formy zajęć**	**Łączna liczba godzin**	**Liczba punktów ECTS**
A6. Podstawy ekonomii*	wykład	50	2
A7. Podstawy prawa*	wykład	50	2
A8. Wprowadzenie do psychologii społecznej**	wykład	50	2
A9. Podstawy socjologii*	wykład	50	2
A10. Podstawy stosunków międzynarodowych*	wykład	50	2
A11. Podstawy bezpieczenstwa narodowego (pol./ang.)*	wykład	75	3
A12. Podstawy zarządzania i organizacji*	wykład	75	3
A13. Podstawy filozofii i logiki*	wykład	75	3
A14. Podstawy pedagogiki*	wykład	75	3
A15. Historia techniki*	wykład	75	3
C. Grupa treści kształcenia w zakresie **Analiza danych i informatyka śledcza**	wykład/ćwiczenia	1088	42
D. Praca dyplomowa	wykład/ćwiczenia	275	11
Razem pkt. ECTS:			**78**
Wskaźnik % do ogółu pkt. ECTS			**65,0%**

* Spośród tych przedmiotów student wybiera co najmniej po jednym przedmiocie w semestrze II i III, tak by uzyskać w sumie co najmniej 5 pkt ECTS.

6.3. Wskaźniki łączne dotyczące programu studiów niestacjonarnych II stopnia – zakres Cyberbezpieczeństwo

Kategoria **Wskaźniki dotyczące programu studiów na kierunku Systemy informacyjne w bezpieczeństwie, poziomie i profilu kształcenia**	**Liczba punktów ECTS**
Liczba punktów ECTS konieczna do uzyskania kwalifikacji odpowiadających poziomowi kształcenia	**120**
Łączna liczba punktów ECTS jaką student musi uzyskać w ramach zajęć prowadzonych z bezpośrednim udziałem nauczycieli akademickich lub innych osób prowadzących zajęcia	**38,0**
Łączna liczba punktów ECTS, jaką student musi uzyskać w ramach zajęć z dziedziny nauk humanistycznych.	**>5***
Łączna liczba punktów ECTS w ramach zajęć związanych z prowadzoną w uczelni działalnością naukową w dyscyplinie nauki o bezpieczeństwie	**89**
Liczba punktów ECTS przyporządkowana zajęciom do wyboru	**78**
Liczba punktów ECTS przyporządkowana praktykom zawodowym oraz liczba godzin praktyk zawodowych	**X**

* kierunek studiów przypisany do dziedziny nauk społecznych

6.3.1. Łączna liczba punktów ECTS jaką student musi uzyskać w ramach zajęć prowadzonych z bezpośrednim udziałem nauczycieli akademickich lub innych osób prowadzących zajęcia

Moduły zajęć związane z bezpośrednim udziałem nauczycieli akademickich lub innych osób prowadzących zajęcia			
Nazwa modułu zajęć	**Forma/formy zajęć**	**Łączna liczba godzin**	**Liczba punktów ECTS**
A. Grupa treści podstawowych	wykład, ćwiczenia	230	9,1
B. Grupa treści kierunkowych	wykład, ćwiczenia	313	12,5
C. Grupa treści kształcenia w zakresie **Cyberbezpieczeństwo**	wykład, ćwiczenia	338	13,0
D. Praca dyplomowa	wykład, ćwiczenia	85	3,4
Razem pkt. ECTS:			**38,0**
Wskaźnik % do ogółu pkt. ECTS			**31,7%**

6.3.2. Łączna liczba punktów ECTS w ramach zajęć związanych z prowadzoną w uczelni działalnością naukową w dyscyplinie nauki o bezpieczeństwie (więcej niż 50% punktów ECTS)

Moduły zajęć związanych z prowadzoną w uczelni działalnością naukową w dyscyplinie nauki o bezpieczeństwie		
Nazwa modułu zajęć	**Forma/formy zajęć**	**Liczba punktów ECTS**
A. Grupa treści podstawowych	wykład, ćwiczenia	21,0
B. Grupa treści kierunkowych	wykład, ćwiczenia	26,0
C. Grupa treści kształcenia w zakresie **Cyberbezpieczeństwo**	wykład, ćwiczenia	31,0
D. Praca dyplomowa	wykład, ćwiczenia	11,00
Razem pkt. ECTS:		**89,0**
Wskaźnik % do ogółu pkt. ECTS		**74,2%**

6.3.3. Łączna liczba punktów ECTS w ramach zajęć do wyboru, nie mniej niż 30% liczby punktów ECTS

Kod i nazwa przedmiotu/modułu do wyboru			
Kod i nazwa przedmiotu/modułu	**Forma/formy zajęć**	**Łączna liczba godzin**	**Liczba punktów ECTS**
A6. Podstawy ekonomii*	wykład	50	2
A7. Podstawy prawa*	wykład	50	2
A8. Wprowadzenie do psychologii społecznej*	wykład	50	2
A9. Podstawy socjologii*	wykład	50	2
A10. Podstawy stosunków międzynarodowych*	wykład	50	2
A11. Podstawy bezpieczenstwa narodowego (pol./ang.)*	wykład	75	3
A12. Podstawy zarządzania i organizacji*	wykład	75	3
A13. Podstawy filozofii i logiki*	wykład	75	3
A14. Podstawy pedagogiki*	wykład	75	3
A15. Historia techniki*	wykład	75	3
C. Grupa treści kształcenia w zakresie **Cyberbezpieczeństwo**	wykład/ćwiczenia	1088	42
D. Praca dyplomowa	wykład/ćwiczenia	275	11
Razem pkt. ECTS:			**78**
Wskaźnik % do ogółu pkt. ECTS			**65,0%**

* Spośród tych przedmiotów student wybiera co najmniej po jednym przedmiocie w semestrze II i III, tak by uzyskać w sumie co najmniej 5 pkt ECTS.

6.4. Wskaźniki łączne dotyczące programu studiów niestacjonarnych II stopnia – zakres Analiza danych i informatyka śledcza

Kategoria **Wskaźniki dotyczące programu studiów na kierunku Systemy informacyjne w bezpieczeństwie, poziomie i profilu kształcenia**	**Liczba punktów ECTS**
Liczba punktów ECTS konieczna do uzyskania kwalifikacji odpowiadających poziomowi kształcenia	**120**
Łączna liczba punktów ECTS jaką student musi uzyskać w ramach zajęć prowadzonych z bezpośrednim udziałem nauczycieli akademickich lub innych osób prowadzących zajęcia	**37,8**
Łączna liczba punktów ECTS, jaką student musi uzyskać w ramach zajęć z dziedziny nauk humanistycznych.	**>5***
Łączna liczba punktów ECTS w ramach zajęć związanych z prowadzoną w uczelni działalnością naukową w dyscyplinie nauki o bezpieczeństwie	**89**
Liczba punktów ECTS przyporządkowana zajęciom do wyboru	**78**
Liczba punktów ECTS przyporządkowana praktykom zawodowym oraz liczba godzin praktyk zawodowych	**X**

* kierunek studiów przypisany do dziedziny nauk społecznych

6.4.1. Łączna liczba punktów ECTS jaką student musi uzyskać w ramach zajęć prowadzonych z bezpośrednim udziałem nauczycieli akademickich lub innych osób prowadzących zajęcia

Moduły zajęć związane z bezpośrednim udziałem nauczycieli akademickich lub innych osób prowadzących zajęcia			
Nazwa modułu zajęć	**Forma/formy zajęć**	**Łączna liczba godzin**	**Liczba punktów ECTS**
A. Grupa treści podstawowych	wykład, ćwiczenia	230	9,1
B. Grupa treści kierunkowych	wykład, ćwiczenia	313	12,5
C. Grupa treści kształcenia w zakresie **Analiza danych i informatyka śledcza**	wykład, ćwiczenia	333	12,8
D. Praca dyplomowa	wykład, ćwiczenia	85	3,4
Razem pkt. ECTS:			**37,8**
Wskaźnik % do ogółu pkt. ECTS			**31,5%**

6.4.2. Łączna liczba punktów ECTS w ramach zajęć związanych z prowadzoną w uczelni działalnością naukową w dyscyplinie nauki o bezpieczeństwie (więcej niż 50% punktów ECTS)

Moduły zajęć związanych z prowadzoną w uczelni działalnością naukową w dyscyplinie nauki o bezpieczeństwie		
Nazwa modułu zajęć	**Forma/formy zajęć**	**Liczba punktów ECTS**
A. Grupa treści podstawowych	wykład, ćwiczenia	21,0
B. Grupa treści kierunkowych	wykład, ćwiczenia	26,0
C. Grupa treści kształcenia w zakresie **Analiza danych i informatyka śledcza**	wykład, ćwiczenia	31,0
D. Praca dyplomowa	wykład, ćwiczenia	11,00
Razem pkt. ECTS:		**89,0**
Wskaźnik % do ogółu pkt. ECTS		**74,2%**

6.4.3. Łączna liczba punktów ECTS w ramach zajęć do wyboru, nie mniej niż 30% liczby punktów ECTS

Kod i nazwa przedmiotu/modułu do wyboru			
Kod i nazwa przedmiotu/modułu	**Forma/formy zajęć**	**Łączna liczba godzin**	**Liczba punktów ECTS**
A6. Podstawy ekonomii*	wykład	50	2
A7. Podstawy prawa*	wykład	50	2
A8. Wprowadzenie do psychologii społecznej*	wykład	50	2
A9. Podstawy socjologii*	wykład	50	2
A10. Podstawy stosunków międzynarodowych*	wykład	50	2
A11. Podstawy bezpieczenstwa narodowego (pol./ang.)*	wykład	75	3
A12. Podstawy zarządzania i organizacji*	wykład	75	3
A13. Podstawy filozofii i logiki*	wykład	75	3
A14. Podstawy pedagogiki*	wykład	75	3
A15. Historia techniki*	wykład	75	3
C. Grupa treści kształcenia w zakresie **Analiza danych i informatyka śledcza**	wykład/ćwiczenia	1088	42
D. Praca dyplomowa	wykład/ćwiczenia	275	11
Razem pkt. ECTS:			**78**
Wskaźnik % do ogółu pkt. ECTS			**65,0%**

* Spośród tych przedmiotów student wybiera co najmniej po jednym przedmiocie w semestrze II i III, tak by uzyskać w sumie co najmniej 5 pkt ECTS.