KARTA MODUŁU KSZTAŁCENIA
ROK AKADEMICKI 2018/2019
BEZPIECZEŃSTWO NARODOWE

Informacje ogólne

1. Nazwa modułu kształcenia

CYBERZAGROŻENIA BEZPIECZEŃSTWA PAŃSTWA

2. Nazwa jednostki prowadzącej moduł

Wydział Nauk Ekonomicznych i Technicznych
Katedra Ekonomii i Zarządzania
Zakład Bezpieczeństwa Narodowego

3. Kod modułu *(Wypełnia koordynator ECTS)*	**4. Grupa treści kształcenia** *kierunkowego*	**5. Typ modułu** *obowiązkowy*
6. Poziom studiów *II stopnia*	**7. Liczba punktów ECTS** 2	**8. Poziom przedmiotu** *zaawansowany*

9. Rok studiów *II rok - semestr III - zimowy*	**10. Liczba godzin w semestrze**					**11. Liczba godzin w tygodniu**				
	Wyk.	Ćw.	Lab	Sem.	Proj.	Wyk.	Ćw.	Lab	Sem.	Proj.
Studia stacjonarne	15	30	-	-	-	1	2	-	-	-
Studia niestacjonarne	-	-	-	-	-	-	-	-	-	-

12. Język wykładowy: polski

13. Wykładowca (Wykładowcy): dr Katarzyna Chomicz, e-mail: k.chomicz@dydaktyka.pswbp.pl

Informacje szczegółowe

14. Wymagania wstępne

1. brak

15. Cele przedmiotu

C1. WIEDZA: Przekazanie studentom wiedzy nt. cyberzagrożeń bezpieczeństwa państwa
C2. UMIEJĘTNOŚCI: Przekazanie studentom uwarunkowań, zasad działania w zakresie cyberzagrożeń bezpieczeństwa państwa
C3. KOMPETENCJE: Przygotowanie studentów do wykorzystania zdobytej wiedzy w samodzielnych studiach, wiedzy i umiejętności w praktyce zawodowej, weryfikacji pozyskiwanych wiadomości, krytycznego ich odbioru i osądu

16. Efekty kształcenia w zakresie wiedzy, umiejętności i kompetencji społecznych

nr	Student, który zaliczył przedmiot potrafi:	Odniesienie do celów przedmiotu
EK01	Definiować podstawowe pojęcia m.in.: cyberzagrożenie, cyberprzestępczość, cyberbezpieczeństwo, cyberprzestrzeń	C1
EK02	Rozróżniać i charakteryzować cyberzagrożenia bezpieczeństwa państwa oraz instytucje z nimi związane	C2
EK03	Wskazywać i analizować cyberzagrożenie bezpieczeństwa państwa oraz instytucje z nimi związane	C3

17. Treści programowe

	Forma zajęć - WYKŁADY	Liczba godzin S	Liczba godzin NS	Odniesienie do efektów kształcenia dla

				przedmiotu
W1	Powstanie, rozwój i istota cyberprzestrzeni	2	-	EK01
W2	Technologia cyberprzestrzeni	2	-	EK01,03
W3	Zagrożenia w cyberprzestrzeni	4	-	EK01,03
W4	Geneza powstania podmiotów cyberbezpieczeństwa	2	-	EK01
W5	Bezpieczeństwo państwa w cyberprzestrzeni	2	-	EK01,02
W6	System reagowania na incydenty komputerowe – wybrane aspekty	1	-	EK01,02,03
W7	Rozwiązania prawno-instytucjonalne w zakresie bezpieczeństwa państwa w cyberprzestrzeni	2	-	EK02,03
	SUMA GODZIN	**15**	-	-

	Forma zajęć - ĆWICZENIA	Liczba godzin S	Liczba godzin NS	Odniesienie do efektów kształcenia dla przedmiotu
ĆW1	Ewolucja cyberprzestrzeni; Społeczeństwo informacyjne	4	-	EK01,02
ĆW2	Cyberprzestrzeń i jej istota; Wyzwania i zagrożenia w cyberprzestrzeni	4	-	EK01,02,03
ĆW3	Analiza dokumentu „Strategia Cyberbezpieczeństwa RP na lata 2017-2022”	2	-	EK03
ĆW4	Analiza wybranych cyberzagrożeń	5	-	EK01,02
ĆW5	Cyberterroryzm i jego zwalczanie	3	-	EK01,02
ĆW6	Systematyka oraz kwalifikacja prawna wybranych cyberprzestępstw	5	-	EK01,02
ĆW7	Bezpieczeństwo cyberprzestrzeni w wymiarze instytucjonalnym; Współpraca międzysektorowa w zakresie cyberbezpieczeństwa	6	-	EK01,02,03
ĆW8	Propozycje zmian systemowych dla poprawy cyberbezpieczeństwa RP	1	-	EK03
	SUMA GODZIN	**30**	-	-

18. Narzędzia/metody dydaktyczne	
1.	Obserwacja aktywności studenta na zajęciach z wykorzystaniem metod aktywizujących
2.	Case study – prace w grupach
3.	Wykład+prezentacja multimedialna+Metoda Flipped Learning
19. Sposoby oceny (F – formująca, P - podsumowująca)	
F1	Obecność i aktywność na zajęciach
F2	Przygotowywanie prezentacji
P1	Zaliczenie przedmiotu

20. Literatura podstawowa i uzupełniająca

Literatura podstawowa:

1. P. Borek, Z. Ciekanowski (red.), *Determinanty bezpieczeństwa państwa wobec współczesnych zagrożeń*, Biała Podlaska 2017
2. M. Sawicki, *Cyberprzestępczość*, Warszawa 2013
3. K. Michalski, I. Oleksiewicz, E. Sienkiewicz, *Bezpieczeństwo w społeczeństwie informacyjnym. Zagadnienia w wymiarze online i offline*, Warszawa 2017
4. W. Kitler, *Bezpieczeństwo narodowe RP. Podstawowe kategorie. Uwarunkowania. System*, Warszawa 2011
5. J. Janczak, A. Nowak, *Bezpieczeństwo informacyjne. Wybrane problemy*, Warszawa 2013

Literatura uzupełniająca:

1. Strategia cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022, Ministerstwo Cyfryzacji, Warszawa 2017

21. Obciążenie pracą studenta

Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności	
	S	**NS**
Godziny kontaktowe z nauczycielem	45	-
Zapoznanie się ze wskazaną literaturą	2	-
Przygotowanie do zajęć	1	-
Przygotowanie do zaliczenia zajęć	2	-
SUMA	**50**	-
SUMARYCZNA LICZBA PUNKTÓW ECTS DLA PRZEDMIOTU	**2**	-

22. Kryteria oceny

	ndst. (2)	dst. (3)	db. (4)	bdb. (5)
EK01	Student nie potrafi definiować żadnych podstawowych pojęć m.in.:	Student potrafi definiować część podstawowych pojęć m.in.: cyberprzestrzeń,	Student potrafi definiować większość podstawowych pojęć m.in.:	Student potrafi definiować podstawowe pojęcia m.in.:

	cyberprzestrzeń, cyberbezpieczeństwo, cyberzagrożenie, cyberprzestępczość	cyberbezpieczeństwo, cyberzagrożenie, cyberprzestępczość	cyberprzestrzeń, cyberbezpieczeństwo, cyberzagrożenie, cyberprzestępczość	cyberprzestrzeń, cyberbezpieczeństwo, cyberzagrożenie, cyberprzestępczość
EK02	Student nie potrafi rozróżniać i charakteryzować cyberzagrożenia bezpieczeństwa państwa oraz instytucje z nimi związane	Student potrafi w podstawowym stopniu rozróżniać i charakteryzować cyberzagrożenia bezpieczeństwa państwa oraz instytucje z nimi związane	Student zasadniczo potrafi rozróżniać i charakteryzować cyberzagrożenia bezpieczeństwa państwa oraz instytucje z nimi związane	Student potrafi rozróżniać i charakteryzować cyberzagrożenia bezpieczeństwa państwa oraz instytucje z nimi związane
EK03	Student nie potrafi wskazywać i analizować cyberzagrożenia bezpieczeństwa państwa oraz instytucje z nimi związane	Student potrafi wskazać część wskazywać i analizować cyberzagrożenia bezpieczeństwa państwa oraz instytucje z nimi związane	Student potrafi wskazać większość wskazywać i analizować cyberzagrożenia bezpieczeństwa państwa oraz instytucje z nimi związane	Student potrafi wskazać wskazywać i analizować cyberzagrożenia bezpieczeństwa państwa oraz instytucje z nimi związane

Inne przydatne informacje
Informacja, gdzie można zapoznać się z prezentacjami do zajęć, instrukcjami do laboratorium, itp. – www.pswbp.pl
Informacje na temat miejsca odbywania zajęć – zajęcia będą się odbywały w miejscach wskazanych w planie zajęć
Informacja na temat terminu zajęć (dzień tygodnia/godzina) – zajęcia będą się odbywały według planu zajęć
Informacja na temat konsultacji (godziny+miejsce) – www.pswbp.pl

Tabela podsumowująca

Efekt kształcenia	**Odniesienie danego efektu do efektów zdefiniowanych dla całego programu**	**Cele przedmiotu**	**Treści programowe**	**Narzędzia/ metody dydaktyczne**	**Sposób oceny**
EK01	K_W02,	C1	W1-7, ĆW1-8	1,2,3	F1,F2 i P1
EK02	K_U03, K_U21, K_K04, K_K13	C2	W1-W7, ĆW1-8	1,2,3	F1,F2 i P1
EK03	K_W15	C3	W1-W7, ĆW1-8	1,2,3	F1,F2 i P1