KARTA PRZEDMIOTU NA ROK AKADEMICKI 2020/2021

INFORMACJE OGÓLNE

1. Nazwa przedmiotu kształcenia

Cyberzagrożenia bezpieczeństwa państwa

2. Nazwa jednostki prowadzącej moduł

Wydział Nauk Ekonomicznych

3. Grupa treści kształcenia

nauki kierunkowe

4. Typ przedmiotu

obowiązkowy

5. Poziom studiów

studia drugiego stopnia

6. Liczba punktów ECTS

3

7. Poziom przedmiotu

średniozaawansowany

8. Rok studiów, semestr

II rok, III semestr

9. Liczba godzin w semestrze

Wyk.	Ćw.	L*	Prj. Pbn.	Zp.	Pr.
15	30				

10. Język wykładowy:

polski

11. Wykładowca (wykładowcy)

mgr Artur Artecki – ćwiczenia
dr Aneta Chrząszcz – wykład

INFORMACJE SZCZEGÓŁOWE

12. Wymagania wstępne

Wiedza z zakresu nauk społecznych zdobyta na wcześniejszych etapach studiów (studia I stopnia, I rok studiów II stopnia).

13. Cele przedmiotu

C1 Zaprezentowanie studentom wiedzy z zakresu cyberbezpieczeństwa, jego kluczowych zagrożeń oraz sposobów ich zwalczania.

C2 Rozwój umiejętności analizy i syntezy oraz oceny i krytyki zjawisk związanych ze sferą cyberzagrożeń bezpieczeństwa państwa.

14. Efekty uczenia się w zakresie wiedzy, umiejętności i kompetencji społecznych

Student, który zaliczył przedmiot:	odniesienie do kierunkowych efektów uczenia się
WIEDZA	
EU01 Zna pojęcie cyberbezpieczeństwa oraz potrafi podać przykłady zagrożeń odnoszących się do bezpieczeństwa kulturowego i metody zapobiegania tymże zagrożeniom.	KW_02, KW_06
EU02 Zna podstawy prawne cyberbezpieczeństwa państwa.	KW_04, KW_09
UMIEJĘTNOŚCI	
EU03 Potrafi poddać analizie uwarunkowania bezpieczeństwa cybernetycznego państwa w aspekcie wewnętrznym i aspekcie zewnętrznym, ilustrując swoją wypowiedź przykładami.	KU_01, KU_04, KU_06, KU_19

EU04 Potrafi krytycznie omówić relacje pomiędzy bezpieczeństwem kulturowym jako jednym z rodzajów bezpieczeństwa państwa a innymi rodzajami bezpieczeństwa.	KU_01, KU_04, KU_06, KU_19
KOMPETENCJE SPOŁECZNE	
EU05 Potrafi formułować krytyczne oceny zjawisk z zakresu bezpieczeństwa cybernetycznego państwa.	KK_07

15. Treści programowe

Forma zajęć - wykłady

Społeczeństwo informacyjne
Cyberprzestrzeń i jej istota
Technologia cyberprzestrzeni
Zagrożenia w cyberprzestrzeni
Podmioty cyberbezpieczeństwa
Bezpieczeństwo państwa w cyberprzestrzeni – główne zagadnienia
Rozwiązania prawno-instytucjonalne w zakresie bezpieczeństwa państwa w cyberprzestrzeni

Forma zajęć - ćwiczenia

Cyberprzestrzeń i jej ewolucja
Wyzwania i zagrożenia w cyberprzestrzeni
„Strategia Cyberbezpieczeństwa RP na lata 2017-2022" – analiza dokumentu
Wybrane cyberzagrożenia oraz ich zwalczania
Cyberterroryzm i jego zwalczanie
System reagowania na incydenty komputerowe – wybrane aspekty
Cyberprzestępczość
Bezpieczeństwo cyberprzestrzeni w wymiarze instytucjonalnym
Współpraca międzysektorowa w zakresie cyberbezpieczeństwa

16. Narzędzia/metody dydaktyczne

1. wykład z elementami konwersatoryjnymi
2. analiza materiału źródłowego (akty normatywne)
3. rozmowa nauczająca
4. prezentacja multimedialna

17. Sposoby oceny (F – formująca; P – podsumowująca)

F1. obecność na zajęciach
F2. prezentacja multimedialna
P1. kolokwium
P2. zaliczenie na ocenę

18. Obciążenia pracą studenta

forma aktywności	średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z nauczycielem**	35
Przygotowanie się do zajęć, w tym analiza literatury przedmiotu	10
Przygotowanie prezentacji multimedialnej	5
Przygotowanie się do kolokwium	10
Przygotowanie się do zaliczenia na ocenę	15
SUMA	75
SUMARYCZNA LICZBA PUNKTÓW ECTS	

DLA PRZEDMIOTU 3

19. Literatura podstawowa i uzupełniająca

Literatura podstawowa:

1. Borek P., Ciekanowski Z., *Determinanty bezpieczeństwa państwa wobec współczesnych zagrożeń*, Biała Podlaska 2017.
2. Wojciechowska-Filipek S., Ciekanowski Z., *Bezpieczeństwo funkcjonowania w cyberprzestrzeni: jednostki, organizacji, państwa,* Warszawa 2015.
3. Bąk T., Ciekanowski Z., Nowicka J., *Współczesne zagrożenia bezpieczeństwa państwa*, Warszawa 2015.

Literatura uzupełniająca:

1. Sawicki M., *Cyberprzestępczość*, Warszawa 2013.
2. Michalski K., Oleksiewicz I., Sienkiewicz E., *Bezpieczeństwo w społeczeństwie informacyjnym. Zagadnienia w wymiarze online i offline*, Warszawa 2017.
3. Kitler W., *Bezpieczeństwo narodowe RP. Podstawowe kategorie. Uwarunkowania. System*, Warszawa 2011.
4. Janczak J., Nowak A., Bezpieczeństwo informacyjne. Wybrane problemy, Warszawa 2013.

20. Formy oceny - szczegóły

1. Obecność na zajęciach – zgodnie z regulaminem studiów.
2. Wykład: kolokwium w formie testu jednokrotnego wyboru.
3. Ćwiczenia: kolokwium oraz prezentacja multimedialna

Wskaźniki końcowej oceny studenta - wykład

Ocena	Algorytm oceny końcowej
2	do 50%
3*	powyżej 50%, ale nie więcej niż 60%
3,5	powyżej 60%, ale nie więcej niż 70%
4	powyżej 70%, ale nie więcej niż 80%
4,5	powyżej 80%, ale nie więcej niż 90%
5	powyżej 90%

* Student opanował wszystkie efekty kształcenia ujęte w karcie przedmiotu.

21. Inne przydatne informacje o przedmiocie

1. Informacja, gdzie można zapoznać się z prezentacjami do zajęć, instrukcjami do laboratorium, itp.
   www.pswbp.pl
2. Informacje na temat miejsca odbywania zajęć
   www.pswbp.pl
3. Informacja na temat terminu zajęć (dzień tygodnia/godzina)
   www.pswbp.pl
4. Informacja na temat konsultacji (godziny + miejsce)
   www.pswbp.pl

*L – laboratorium (w przypadku zajęć z języka obcego oznacza lektorat)

** Zajęcia prowadzone z bezpośrednim udziałem nauczyciela akademickiego lub innej osoby prowadzącej zajęcia **oraz konsultacje**