AKADEMIA WSB						
Kierunek studiów: Bezpieczeństwo Narodowe						
Przedmiot: Bezpieczeństwo w cyberprzestrzeni						
Profil kształcenia: praktyczny						
Poziom kształcenia: studia I stopnia						
Liczba godzin w semestrze	1		2		3	
	I	II	III	IV	V	**VI**
Studia stacjonarne (w/ćw/lab/pr/e)*						**12ćw**
Studia niestacjonarne (w/ćw/lab/pr/e)						**12ćw**
JĘZYK PROWADZENIA ZAJĘĆ	Polski					
WYKŁADOWCA	dr inż. Krystian Mączka, dr Tomasz Pączkowski					
FORMA ZAJĘĆ	Ćwiczenia					
CELE PRZEDMIOTU	Zapoznanie studenta z obowiązującymi przepisami prawa w zakresie ochrony danych w sieci Internet oraz w zakresie ochrony cyberprzestrzeni RP jak również zdobycie umiejętności w zakresie umiejętności pracy z tekstami przepisów prawa.					

Odniesienie do efektów uczenia się		**Opis efektów uczenia się**	**Sposób weryfikacji efektu uczenia się**
Efekt kierunkowy	**PRK**		
WIEDZA			
BN_W01	P6U_W	Zna przepisy prawa w zakresie ochrony danych osobowych oraz gromadzenia i przesyłania danych cyfrowych oraz ich bezpieczeństwa;	Test/kolokwium;
UMIEJĘTNOŚCI			
BN_U01	P6U_U	Potrafi pracować z tekstami ustaw, rozporządzeń, norm dotyczących cyberbezpieczeństwa;	Test/kolokwium;
BN_U03	P6U_U	Potrafi opracować regulamin, politykę, wytyczne dotyczące bezpieczeństwa danych cyfrowych;	Sprawdzenie opracowanego tekstu;
KOMPETENCJE SPOŁECZNE			
BN_K06	P6U_K	Jest gotów do profesjonalnych działań w zakresie opracowywania regulaminów i polityk bezpieczeństwa danych cyfrowych;	Sprawdzenie opracowanego tekstu;

Nakład pracy studenta (w godzinach dydaktycznych 1h dyd.=45 minut)**

Stacjonarne	**Niestacjonarne**
udział w wykładach =	udział w wykładach =
udział w ćwiczeniach = 12	udział w ćwiczeniach = 12
przygotowanie do ćwiczeń =	przygotowanie do ćwiczeń = 5
przygotowanie do wykładu = 5	przygotowanie do wykładu =
przygotowanie do zaliczenia/egzaminu = 6	przygotowanie do zaliczenia/egzaminu = 6
realizacja zadań projektowych =	realizacja zadań projektowych =
e-learning =	e-learning =
zaliczenie/egzamin =1	zaliczenie/egzamin =1
inne (konsultacje) = 2	inne (konsultacje) = 2
RAZEM:26	**RAZEM:26**
Liczba punktów ECTS:1	**Liczba punktów ECTS:1**
w tym w ramach zajęć praktycznych:	**w tym w ramach zajęć praktycznych:**

WARUNKI WSTĘPNE	Student posiada podstawową wiedzę z zakresu działania sieci Internet i obsługi komputera.

TREŚCI PRZEDMIOTU	Treści realizowane w formie bezpośredniej: • Omówienie założeń Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych • Omówienie założeń Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych RODO) • Omówienie założeń Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa • Omówienie założeń Strategii Cyberbezpieczenstwa Rzeczypospolitej Polskiej na lata 2017-2022 • Praca z tekstem ustaw i rozporządzeń • Tworzenie regulaminów instytucji w oparci o przepisy prawne z uwzględnieniem technologii gromadzenia i przesyłania danych w formie cyfrowej • Tworzenie polityki bezpieczeństwa • Tworzenie klauzuli poufności • Identyfikacja uprawnień SOC i CERT • Identyfikacja incydentu do zgłoszenia obligatoryjnego i fakultatywnego • Opracowanie regulaminu zgłaszania incydentów do SOC i CERT • Opracowanie zgłoszeń do Głównego Inspektora Danych Osobowych • Omówienie incydentów bezpieczeństwa wg ISO 27000 • Omówienie i weryfikacja założeń o dyrektywach NIST • Praca z tekstem – wskazanie w tekście na błędy i zaniechania pracownika w zakresie zgłoszenia incydentu Treści realizowane w formie e-learning:
LITERATURA OBOWIĄZKOWA	• Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych • Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych RODO) • Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa • Strategia Cyberbezpieczenstwa Rzeczypospolitej Polskiej na lata 2017-2022
LITERATURA UZUPEŁNIAJĄCA	• Wasilewski, Janusz. "Zarys definicyjny cyberprzestrzeni." Przegląd Bezpieczeństwa Wewnętrznego 5.9 (2013): 225-234. • Pala, Mariusz. "Wybrane aspekty bezpieczeństwa w cyberprzestrzeni." De Securitate et Defensione. O Bezpieczeństwie i Obronności 1.1 (2015): 113-130 • Stevens, Tim. Cyber security and the politics of time. Cambridge University Press, 2016. • Probst, Christian W., et al., eds. Insider threats in cyber security. Vol. 49. Springer Science & Business Media, 2010.
METODY NAUCZANIA	W formie bezpośredniej: Wykład multimedialny, dyskusja, burza mózgów W formie e-learning: nie dotyczy
POMOCE NAUKOWE	Rzutnik multimedialny, tablica
PROJEKT	Cel projektu: Temat projektu: Forma projektu:
FORMA I WARUNKI ZALICZENIA	W formie bezpośredniej: Kolokwium

** W-wykład, ćw- ćwiczenia, lab- laboratorium, pro- projekt, e- e-learning*