Nazwa zajęć:					
Cyberbezpieczeństwo			Cybersecurity		
Kierunek:					***Obowiązuje od roku ak.***
Bezpieczeństwo narodowe					2020/2021
Poziom:		***Profil:***		***Grupa zajęć:***	
I st. licencjacki		Praktyczny			Kierunkowe
Semestr:	***Forma zaliczenia:***	***Punkty ECTS:***		***Zajęcia do wyboru:***	***Język zajęć:***
3	Z - zaliczenie na ocenę	3		Nie	Polski

Forma zajęć i liczba godzin na studiach stacjonarnych i niestacjonarnych:

Wykład	***Ćwiczenia***		***Suma godzin:***
15 / 8	30 / 16		45 / 24

Specjalność:

Nazwiska osób odpowiedzialnych za zajęcia:

dr inż.Grzegorz Świdzikowski

Opis zajęć:

Przedmiot "Cyberbezpieczeństwo" przeznaczony jest dla studentów kierunku bezpieczeństwo narodowe, którzy posiadają podstawową wiedzę w zakresie roli i znaczenia informacji we współczesnym świecie oraz jej miejsca w strukturach i organach bezpieczeństwa państwa. Podstawowym celem w ramach realizowanego przedmiotu jest przedstawienie możliwości wykorzystania nowoczesnych technologii teleinformatycznych w zakresie przetwarzania informacji ze szczególnym uwzględnieniem aspektów negatywnie wpływających (zagrożeń) dla pojedyńczych osób, grup, społeczeństw czy też państwa. Po ukończeniu przedmiotu studenci będą posiadac wiedzę oraz świadomość możliwości wystąpienia potencjalnych zagrożeń w zakresie utraty poufności, integralności czy dotępności do przetwarzanych w systemach teleinformatycznych informacji. Pozwoli to rozwinąć umiejętność samodzielnej identyfikacji zagrożeń w cybeprzestrzeni oraz zrozumienia możliwych konsekwencji w procesie wymiany informacji przy użyciu nowoczesnych środków teleinformatycznych.

Cele dydaktyczne:

Ukształtowanie wiedzy oraz świadomości w zakresie możliwości wystąpienia zagrożeń związanych z przetwarzaniem informacji w cyberprzestrzeni - dla jednostki oraz dla państwa.

Przedstawienie różnego rodzaju zagrożeń w obszarze cyberprzestrzeni związanych z systemem bezpieczeństwa państwa.

Rozwinięcie umiejętności rozróżniania zagrożeń występujących w cyberprzestrzeni oraz szacowania ewentualnych konsekwencji ich wystąpienia.

Kształtowanie kompetencji niezbędnych do samodzielnego wykonywania podstawowych czynności realizowanych w procesie reakcji na stwierdzone zagrożenia w sieciach i systemach teleinformatycznych.

Metody dydaktyczne:				***Metody oceniania:***	
MP1	wykład informacyjny			MO1	kolokwium pisemne
MP2	praca ze źródłem elektronicznym			MO2	sprawozdanie z ćwiczeń
MC1	ćwiczenie praktyczne				
MS1	dyskusja dydaktyczna				

MS2	metoda sytuacyjna				

Wykład

W1	Zarys historii rozwoju sieci i systemów teleinformatycznych
W2	Topologia współczesnej cyberprzestrzeni
W3	Pojęcia i definicje z obszaru cyberprzestrzeni
W4	Zalety cyberprzestrzeni - społeczeństwo informacyjne
W5	Zagrożenia w cyberprzestrzeni - wybrane przykłady
W6	Pojęcie i istota walki informacyjnej - dezinformacja
W7	Rozwój cyberprzestępczości i cyberterroryzmu - wybrane przykłady
W8	Podstawowe sposoby i metody przeciwdziałania zagrożeniom w cyberprzestrzeni

Ćwiczenia

C1	Analiza i ocena podstawowych zagrożeń stanowiska komputerowego.
C2	Analiza i ocena podstawowych zagrożeń sieci komputerowej.
C3	Charakterystyka poszczególnych grup, rodzajów zagrożeń w sieci komputerowej
C4	Metody i sposoby, organizacyjne oraz techniczne przeciwdziałania zagrożeniom.
C5	Wybrane przykłady działań hakerów.
C6	Wybrane przykłady działań cyberprzestępców.
C7	Sposoby i metody działań przestępczych w sieci - metody ataków.

Literatura podstawowa

1	Bezpieczeństwo w cyberprzestrzeni. Wybrane zagadnienia. (red.) Magdalena Molendowska, Rafał Miernik, wyd. Marszałek, ISBN 9788381804158
2	Wybrane aspekty cyberbezpieczeństwa w Polsce. Tomasz Hoffman, wyd. FNCE
3	Zagrożenia cyberprzestrzeni i świata wirtualnego, Józef Bednarek, Anna Andrzejewska, wyd. DIFIN, ISBN 978-83-793-0228-4

Literatura uzupełniająca

1	Zagrożenia cywilizacyjne XXI wieku, Anna Moniuszko-Malinowska, wyd. Alfa Medica Press
2	USTAWA z dnia 5 lipca 2018 r.o krajowym systemie cyberbezpieczeństwa
3	Doktryna cyberbezpieczeństwa RP - Biuro Bezpieczeństwa Narodowego

Warunki zaliczenia

Warunkiem uzyskania pozytywnej oceny i zaliczenia przedmiotu jest przyswojenie podstawowej wiedzy i umiejętności w zakresie znajomości i rozpoznawania podstawowych zagrożeń występujących w cyberprzestrzeni

Przykłady pytań zaliczeniowych

Jak należy rozumieć pojęcie cyberprzestrzeni
Jak należy rozumieć pojęcie bezpieczeństwo cyberprzestrzeni
Podaj trzy znane zagrożenia dla systemów teleinformatycznych i krótko je scharakteryzuj

Zdefiniuj pojęcie cybeprzestępstwa

Obciążenie pracą studenta

Studia stacjonarne/niestacjonarne

Forma pracy studenta	Wykład		Ćwiczenia				Suma	
Zajęcia z bezpośrednim udziałem nauczyciela	15 g	8 g	30 g	16 g			45 g	24 g
Zapozanie się z literaturą przedmiotu	9 g	15 g	4 g	10 g			13 g	25 g
Przygotowanie się do zajęć	2 g	4 g	2 g	4 g			4 g	8 g
Przygotowanie się do kolokwiów	4 g	5 g					4 g	5 g
Realizacja zadanych ćwiczeń i zadań			6 g	9 g			6 g	9 g
Przygotowanie sprawozdania z ćwiczeń			3 g	4 g			3 g	4 g
Przygotowanie projektu / pracy								
Przygotowanie się i udział w egzaminie								
	30 g	32 g	45 g	43 g			75 g	75 g

Efekty uczenia się	KEK	Treści kształcenia	Metody dydaktyczne	M. oceniania
Posiada wiedzę dotyczącą możliwości wystąpienia zagrożeń związanych z przetwarzaniem informacji w cyberprzestrzeni - dla jednostki, dla państwa i dla relacji międzynarodowych.	K_W02	W1-W5, W7-W8 C1-C6	MP1,MP2, MC1, MS1, MS2	MO1, MO2
Posiada wiedzę z zakresu oddziaływania na społeczność międzynarodową i krajową oraz relacje wewnętrzne i zewnętrzne w kontekście działań informacyjnych	K_W04	W6 C7	MP1,MP2, MC1, MS1, MS2	MO1, MO2
Rozróżnia zagrożenia występujące w cyberprzestrzeni oraz szacuje ewentualne konsekwencje ich wystąpienia.	U_W09	W1-W8 C1-C7	MP1,MP2, MC1, MS1, MS2	MO1, MO2
Umieć reagować i postępować w sytuacjach stwierdzenia zagrożenia w sieci teleinformatycznej	K_U01	W5,W8 C1-C4	MP1,MP2, MC1, MS1, MS2	MO1, MO2
Potrafi zidentyfikować różnego rodzaju zagrożenia w obszarze cyberprzestrzeni, związane z systemem bezpieczeństwa państwa.	K_U03	W1-W8 C1-C6	MP1,MP2, MC1, MS1, MS2	MO1, MO2

Potrafi samodzielnie wykonywać podstawowe czynności realizowane w procesie reakcji na stwierdzone zagrożenia w sieciach i systemach teleinformatycznych.	K_U07	W1-W8 C1-C7	MP1,MP2, MC1, MS1, MS2	MO1, MO2
Rozumie następstwa rozwoju nowoczesnych technologii i wynikających z niej dobrodziejstw oraz pojawiających się nowych zagrożeń w sieciach i systemach teleinformatycznych	K_K02	W-4-W5 C4-C7	MP1,MP2, MC1, MS1, MS2	MO1, MO2