KARTA PRZEDMIOTU

I. Dane podstawowe

Nazwa przedmiotu	**Cyberbezpieczeństwo**
Nazwa przedmiotu w języku angielskim	Cybersecurity
Kierunek studiów	prawo
Poziom studiów (I, II, jednolite magisterskie)	jednolite magisterskie
Forma studiów (stacjonarne, niestacjonarne)	stacjonarne
Dyscyplina	prawo
Język wykładowy	polski

Koordynator przedmiotu/osoba odpowiedzialna	**dr Dariusz Żak**

Forma zajęć *(katalog zamknięty ze słownika)*	Liczba godzin	semestr	Punkty ECTS
wykład	**30**	**zimowy**	**6**
konwersatorium	—	—	
ćwiczenia	**15**	**zimowy**	
laboratorium	—	—	
warsztaty	—	—	
seminarium	—	—	
proseminarium	—	—	
lektorat	—	—	
praktyki	—	—	
zajęcia terenowe	—	—	
pracownia dyplomowa	—	—	
translatorium	—	—	
wizyta studyjna	—	—	

Wymagania wstępne	Znajomość prawa konstytucyjnego i prawa administracyjnego.

II. Cele kształcenia dla przedmiotu

Założeniami przedmiotu (wykładów i ćwiczeń) jest: analiza regulacji prawnych dotyczących systemu cyberbezpieczeństwa w kraju i Unii Europejskiej, poznanie kluczowych pojęć, przedstawienie zagadnień z przedmiotowego zakresu, właściwych organów, charakterystyka poszczególnych regulacji prawnych. Inferencja wybranych orzeczeń sądów powstałych w wyniku stosowania unormowań odnoszących się do cyberbezpieczeństwa.

III. Efekty uczenia się dla przedmiotu wraz z odniesieniem do efektów kierunkowych

Symbol	Opis efektu przedmiotowego	Odniesienie do efektu kierunkowego
WIEDZA		
W_01	Zna miejsce cyberbezpieczeństwa w systemie norm, powiązania podstawowych pojęć i ich cechy z przedmiotowego zakresu, które potrafi opisać.	K_W01
W_02	Definiuje podstawowe pojęcia, terminologię oraz ma pogłębioną wiedzę z obszaru cyberbezpieczeństwa.	K_W02
W_03	Potrafi wymienić źródła prawne dotyczące cyberbezpieczeństwa, najważniejsze akty prawne i zawarte w nich przepisy. Zna zasady tworzenia, stosowania i oddziaływania norm z zakresu cyberbezpieczeństwa i ma wiedzę o tendencjach i kierunkach ewolucji tych przepisów.	K_W03
W_04	Zna i rozumie formy funkcjonowania poszczególnych uczestników w ramach cyberbezpieczeństwa, ich kompetencje oraz akty prawne na podstawie których działają.	K_W07
W_05	Zna cele i zasady funkcjonowania poszczególnych form ochrony cyberprzestrzeni.	K_W08
W_06	Potrafi wymienić rodzaje i scharakteryzować obowiązki operatorów usług kluczowych, dostawców usług cyfrowych i podmiotów publicznych w obszarze cyberbezpieczeństwa.	K_W13
W_07	Zna i rozumie zasady udostępniania informacji i przetwarzania danych osobowych.	K_W11
UMIEJĘTNOŚCI		
U_01	Potrafi wyszukiwać, selekcjonować, analizować i oceniać działanie poszczególnych stron systemu cyberbezpieczeństwa .	K_U01
U_02	Potrafi umiejętnie wykorzystać zdobyte informacje dla celów ochrony przez zagrożeniami cyberprzestępczością.	K_U02
U_03	Posiada umiejętność merytorycznego argumentowania (z wykorzystaniem poglądów innych autorów), stawiania tez, formułowania wniosków praktycznych i prawnych.	K_U09
U_04	Potrafi dokonać wykładni przepisów prawa dotyczących cyberbezpieczeństwa w określonym stanie faktycznym.	K_U08
KOMPETENCJE SPOŁECZNE		
K_01	Otwiera się na zagadnienia publiczno - gospodarcze, dyskutuje o nich i potrafi się krytycznie odnieść do działań podmiotów publicznych związanych z cyberbezpieczeństwem.	K_K01
K_02	Docenia rolę systemu ochrony cyberbezpieczeństwa.	K_K02
K_03	Zna prawa i obowiązki właściwych organów publicznych prowadzących działalność w zakresie cyberbezpieczeństwa. Ma teoretyczne przygotowanie do podjęcia działań i zastosowaniu odpowiednich środków w celu ochrony cyberprzestrzeni.	K_K03
K_04	Może uczestniczyć w przygotowaniu i realizacji przedsięwzięć prawnych w przedmiotowym obszarze cyberbezpieczeństwa.	K_K05
K_05	Jest świadom odpowiedzialności jaką generuje prowadzenie	K_K08

	działalności on-line w systemach i sieciach teleinformatycznych.	

IV. Opis przedmiotu/ treści programowe

1. Geneza regulacji prawnych cyberbezpieczeństwa.
2. Pojęcia ogólne cyberbezpieczeństwa.
3. Regulacje prawne Unii Europejskiej ds. cyberbezpieczeństwa.
4. Identyfikacja i rejestracja operatorów usług kluczowych.
5. Obowiązki operatorów usług kluczowych.
6. Obowiązki dostawców usług cyfrowych.
7. Obowiązki podmiotów publicznych.
8. Zadania zespołów ds. Reagowania na Incydenty Bezpieczeństwa Komputerowego.
9. Zasady udostępniania informacji i przetwarzania danych osobowych.
10. Organy właściwe do spraw cyberbezpieczeństwa.
11. Zadania ministra właściwego do spraw informatyzacji.
12. Zadania Ministra Obrony Narodowej.
13. Nadzór i kontrola operatorów usług kluczowych, dostawców usług cyfrowych i podmiotów świadczących usługi w zakresie cyberbezpieczeństwa.
14. Pełnomocnik i Kolegium ds. cyberbezpieczeństwa.
15. Strategia RP ds. cyberbezpieczeństwa.
16. Odpowiedzialność karna.

V. Metody realizacji i weryfikacji efektów uczenia się

Symbol efektu	Metody dydaktyczne *(lista wyboru)*	Metody weryfikacji *(lista wyboru)*	Sposoby dokumentacji *(lista wyboru)*
WIEDZA			
W_01	Dyskusja	Obserwacja	Karta oceny
W_02	Analiza laboratoryjna	Obserwacja	Test
W_03	Studium przypadku	Obserwacja	Karta oceny
W_04	Wykład konwencjonalny	Egzamin	Protokół
W_05	Wykład konwersatoryjny	Zaliczenie ustne	Protokół
W_06	Wykład konwencjonalny	Egzamin	Protokół
W_07	Wykład konwersatoryjny	Zaliczenie ustne	Protokół

UMIEJĘTNOŚCI			
U_01	Analiza tekstu	Sprawdzenie umiejętności praktycznych	Test
U_02	Ćwiczenia praktyczne	Zaliczenie pisemne	Karta oceny
U_03	Praca zespołowa	Zaliczenie ustne	Protokół
U_04	Metoda projektu	Prezentacja	Karta oceny
KOMPETENCJE SPOŁECZNE			
K_01	Dyskusja	Obserwacja	Karta oceny
K_02	Dyskusja	Obserwacja	Karta oceny
K_03	Dyskusja	Obserwacja	Karta oceny
K_04	Metoda problemowa	Zaliczenie ustne	Karta egzaminacyjna
K_05	Metoda projektu	Egzamin	Protokół

VI. Kryteria oceny, wagi

Ocena udzielana jest na podstawie znajomości materiału prezentowanego na wykładzie oraz ćwiczeniach, umiejętności samodzielnej interpretacji regulacji dotyczących cyberbezpieczeństwa oraz rozwiązania kazusów z przedmiotowej problematyki.

VII. Obciążenie pracą studenta

Forma aktywności studenta	Liczba godzin
Liczba godzin kontaktowych z nauczycielem	45
Liczba godzin indywidualnej pracy studenta	210

VIII. Literatura

Literatura podstawowa

1. K. Czaplicki (red.), A. Gryszczyńska (red.), G. Szpor (red.), *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*. Wolters Kluwer, Warszawa 2019.
2. C. Banasiński, M. Rojszczak, *Cyberbezpieczeństwo*, Wolters Kluwer, Warszawa 2020.
3. W. Kitler, Joanna Taczkowska-Olszewska, F. Radoniewicz (red.), *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*. C.H. Beck, Warszawa 2019.

Literatura uzupełniająca

1. J. Krawiec, *Cyberbezpieczeństwo. Podejście systemowe*, Warszawa 2019.
2. A. Besiekierska, (red.), *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*. C.H. Beck,, Warszawa 2019.