KARTA PRZEDMIOTU

I. Dane podstawowe

Nazwa przedmiotu	**Bezpieczeństwo teleinformatyczne**
Nazwa przedmiotu w języku angielskim	IT security
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**	**letni**	**2**
konwersatorium	—	—	
ćwiczenia	—	—	
laboratorium	—	—	
warsztaty	—	—	
seminarium	—	—	
proseminarium	—	—	
lektorat	—	—	
praktyki	—	—	
zajęcia terenowe	—	—	
pracownia dyplomowa	—	—	
translatorium	—	—	
wizyta studyjna	—	—	

Wymagania wstępne	Znajomość regulacji prawa konstytucyjnego, administracyjnego oraz prawa cywilnego. Umiejętność interpretacji przepisów prawa.

II. Cele kształcenia dla przedmiotu

Przedstawienie zagadnień z zakresu szeroko pojętego bezpieczeństwa teleinformatycznego (cyberbezpieczeństwa) w ujęciu interdyscyplinarnym, poznanie definicji, najważniejszych regulacji prawnych i zawartych w nich normach dotyczących przedmiotowej ochrony informacji w różnych aspektach. Analiza rozwoju i funkcjonowania bezpieczeństwa teleinformatycznego w ujęciu publicznoprawnym i prywatnoprawnym.

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

Symbol	Opis efektu przedmiotowego	Odniesienie do efektu kierunkowego
WIEDZA		
W_01	Zna na poziomie podstawowym pojęcia i normy dotyczące bezpieczeństwa teleinformatycznego, które potrafi scharakteryzować.	K_W02
W_02	Definiuje podstawowe pojęcia bezpieczeństwa informacyjnego, terminologię oraz ma wiedzę z zakresu ochrony informacji. Potrafi wymienić źródła prawa dotyczące bezpieczeństwa teleinformatycznego.	K_W01
W_03	Zna zasady tworzenia, stosowania i oddziaływania norm prawa dotyczących cyberbezpieczeństwa mających wpływ na bezpieczeństwo informacji państwa.	K_W03
W_04	Ma wiedzę o tendencjach i kierunkach rozwoju systemów teleinformatycznych.	K_W04
W_05	Zna i rozumie funkcjonowanie oraz kompetencje właściwych organów państwa mających na celu ochronę przetwarzanej informacji.	K_W07
W_06	Potrafi wymienić rodzaje naruszeń w systemach teleinformatycznych mających wpływ na bezpieczeństwo informacji.	K_W08
W_07	Zna i rozumie zasady funkcjonowania państwa w obszarze cyberbezpieczeństwa.	K_W13
W_08	Zna i określa prawa i obowiązki właściwych podmiotów zobowiązanych do ochrony informacji niejawnych w systemach i sieciach teleinformatycznych.	K_W11
UMIEJĘTNOŚCI		
U_01	Potrafi wyszukiwać, selekcjonować, analizować, oceniać praktyczne dane na temat bezpieczeństwa teleinformatycznego.	K_U01
U_02	Potrafi umiejętnie wykorzystać zdobyte informacje dla celów prawnych, społecznych i gospodarczych. Ocenia bezpieczeństwo informacyjne organizacji.	K_U02
U_03	Posiada umiejętność merytorycznego argumentowania, stawiania tez, formułowania wniosków oraz omawiania zagadnień kluczowych z zakresu przedmiotowej problematyki.	K_U09
U_04	Potrafi dokonać wykładni przepisów prawa dotyczących bezpieczeństwa teleinformatycznego w aspekcie publicznym i prywatnym w konkretnym stanie faktycznym.	K_U08
KOMPETENCJE SPOŁECZNE		
K_01	Ma świadomość rangi różnych przepisów systemu prawa regulujących bezpieczeństwo teleinformatyczne. Analizuje podstawowe zasady bezpiecznego przetwarzania informacji.	K_K01
K_02	Docenia rolę cyberbezpieczeństwa państwa oraz znaczenie różnych sposobów zabezpieczeń informacji.	K_K02
K_03	Zna prawa i obowiązki podmiotów przetwarzających informacje w systemach teleinformatycznych.	K_K03
K_04	Dostrzega wieloaspektowość czynników wpływających na	K_K05

	rozwój bezpieczeństwa teleinformatycznego.	
K_05	Jest świadom odpowiedzialności jaka spoczywa na podmiotach przetwarzających informacje w systemach teleinformatycznych.	K_K08

IV. Opis przedmiotu/ treści programowe

1. Pojęcie i znaczenie informacji w dobie społeczeństwa informacyjnego.
2. Zasady bezpieczeństwa informacji przetwarzanej elektronicznie.
3. Bezpieczeństwo informacyjne i bezpieczeństwo informacji przetwarzanej w systemach teleinformatycznych.
4. Państwo jako podmiot polityki bezpieczeństwa w cyberprzestrzeni.
5. Cyberbezpieczeństwo państwa - uwarunkowania prawne.
6. Współczesne systemy teleinformatyczne przetwarzające informacje.
7. Ochrona informacji niejawnych przetwarzanej w sieciach i systemach teleinformatycznych.
8. Zagrożenia informacji przez cyberprzestępczość.

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	Praca z tekstem	Praca pisemna	Sprawdzian pisemny
W_04	Wykład konwencjonalny	Egzamin	Protokół
W_05	Studium przypadku	Obserwacja	Karta oceny
W_06	Wykład konwersatoryjny	Zaliczenie ustne	Protokół
W_07	Wykład konwencjonalny	Egzamin	Protokół
W_08	Wykład konwersatoryjny	Zaliczenie ustne	Protokół
UMIEJĘTNOŚCI			
U_01	Analiza tekstu	Sprawdzenie umiejętności praktycznych	Test
U_02	Praca zespołowa	Zaliczenie ustne	Protokół
U_03	Giełda pomysłów	Wykonanie projektu	Karta oceny
U_04	Rozmowa sokratyczna	Referat	Wydruk
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 treści z wykładowych wraz ze sprawdzeniem umiejętności samodzielnej interpretacji przepisów dotyczących bezpieczeństwa teleinformatycznego, cyberbezpieczeństwa i ochrony informacji.

VII. Obciążenie pracą studenta

Forma aktywności studenta	Liczba godzin
Liczba godzin kontaktowych z nauczycielem	30
Liczba godzin indywidualnej pracy studenta	60

VIII. Literatura

Literatura podstawowa
1. C. Banasiński, M. Rojszczak, Cyberbezpieczeństwo, Wolters Kluwer, Warszawa 2020. 2. W. Kitler, K. Taczkowska-Olszewska, F. Radoniewicz, Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz. C.H. Beck, Warszawa 2019. 3. M. Rojszczak, Ochrona prywatności w cyberprzestrzeni z uwzględnieniem zagrożeń wynikających z nowych technik przetwarzania informacji. Wolters Kluwer, Warszawa 2019. 4. K. Czaplicki, A. Gryszczyńska, G. Szpor, Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz. Wolters Kluwer, Warszawa 2019. 5. J. Krawiec, Cyberbezpieczeństwo. Podejście systemowe. Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa 2019. 6. J. Kowalewski, M. Kowalewski, Ochrona informacji i systemów teleinformatycznych w cyberprzestrzeni. Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa 2017.
Literatura uzupełniająca
1. C. Banasiński, Cyberbezpieczeństwo. Zarys wykładu. Wolters Kluwer, Warszawa 2018. 2. K. Liderman, Bezpieczeństwo informacyjne, Warszawa 2016. 3. M. Lakomy, Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw, Katowice 2015. 4. M. Górka, Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku, Difin, Warszawa 2014. 5. M. Siwicki, Cyberprzestępczość, Warszawa 2013. 6. J. Depo, J. Piwowarski, Bezpieczeństwo informacyjne, Kraków 2012. 7. S. Hoc, Ustawa o ochronie informacji niejawnych. Komentarz. Wydawnictwo Prawnicze LexisNexis. Warszawa 2010. 8. M. Madej, M.Terlikowski, (red.), Bezpieczeństwo teleinformatyczne państwa, Warszawa 2009.