Bezpieczeństwo informacji w pracy prawnika

Karta opisu przedmiotu

Informacje podstawowe

Kierunek studiów prawo	**Cykl kształcenia** 2024/25
Ścieżka	**Kod przedmiotu**
Jednostka organizacyjna Wydział Prawa i Administracji	**Języki wykładowe** Polski
Poziom kształcenia jednolite magisterskie	**Dyscypliny** Nauki prawne
Forma studiów studia stacjonarne	**Klasyfikacja ISCED** 0421Prawo
Profil studiów ogólnoakademicki	
Obligatoryjność fakultatywny	

Okres	**Forma weryfikacji uzyskanych efektów uczenia się** egzamin **Sposób realizacji i godziny zajęć** wykład: 30	**Liczba punktów ECTS** 3.0
Semestr 3, Semestr 4 Semestr 5, Semestr 6 Semestr 7, Semestr 8 Semestr 9, Semestr 10		

Cele kształcenia dla przedmiotu

C1	Przekazanie wiedzy i umiejętności z bezpieczeństwa informacji i podstaw cyberbezpieczeństwa we współczesnym świecie, oraz praktyczna nauka poprawnej konfiguracji narzędzi informatycznych wykorzystywanych w pracy prawnika.
C2	Uświadomienie studentom, że w dobie cyfryzacji kancelarie prawnicze przechowują duże ilości danych osobowych i wrażliwych informacji, które są atrakcyjnym celem dla cyberprzestępców. Przedmiot stawia za cel przedstawienie, jakie są potencjalne zagrożenia związane z niewłaściwym zabezpieczaniem takich danych i jak należy właściwie skonfigurować środowisko pracy i jakich narzędzi używać aby czynić zadość wymogom nakładanym przez przepisy powszechnie obowiązującego prawa i standardy ochrony informacji.
C3	Zajęcia mają na celu zarówno umożliwić uzyskanie wiedzy teoretycznej, jak i praktycznych umiejętności reagowania na ataki sieciowe, oraz nauczyć właściwego zapewnienia bezpieczeństwa urządzeń z których w przyszłości studenci korzystać będą tak służbowo, jak prywatnie.

Efekty uczenia się dla przedmiotu

Kod	Efekty w zakresie	Kierunkowe efekty uczenia się	Metody weryfikacji
Wiedzy - Student zna i rozumie:			
W1	Student zna i rozumie normy prawne regulujące kwestie cyberbezpieczeństwa w Polsce i UE.	PRA_K3_W05 PRA_K3_W06	egzamin
W2	Student zna i rozumie znaczenie niebezpieczeństw związanych z nieprawidłową konfiguracją narzędzi informatycznych i potencjalnym wyciekiem danych osobowych.	PRA_K3_W08	egzamin
W3	Student zna i rozumie działanie narzędzi służących do zabezpieczania systemów informatycznych i danych w nich przechowywanych.	PRA_K3_W08	egzamin
Umiejętności - Student potrafi:			
U1	Student potrafi samodzielnie skonfigurować i wykorzystywać narzędzia do szyfrowania danych, czy bezpiecznego ich przechowywania, zgodnie z wymogami nakładanymi przez przepisy powszechnie obowiązującego prawa.	PRA_K3_U07	egzamin
U2	Student potrafi prawidłowo posługiwać się terminologią z zakresu cyberbezpieczeństwa i ochrony informacji.	PRA_K3_U03	egzamin
U3	Student potrafi zidentyfikować różne typy zagrożeń cybernetycznych, takich jak phishing, ransomware czy ataki DDoS. Powinien również znać podstawowe metody obrony przed nimi i umieć stosować najlepsze praktyki w zakresie bezpieczeństwa informacji.	PRA_K3_U02	egzamin
Kompetencji społecznych - Student jest gotów do:			
K1	Student jest gotów do doskonalenia oraz uzupełniania nabytej wiedzy i umiejętności a także rozumie potrzebę stałego dokształcania się.	PRA_K3_K04 PRA_K3_K06	egzamin
K2	Student jest gotów do dalszego kształcenia.	PRA_K3_K04	egzamin

Bilans punktów ECTS

Forma aktywności studenta	Średnia liczba godzin* przeznaczonych na zrealizowane rodzaje zajęć
wykład	30
analiza aktów normatywnych	10
analiza orzecznictwa	5
samodzielna nauka dotycząca treści poruszanych na zajęciach	30

Łączny nakład pracy studenta	**Liczba godzin** 75	**ECTS** 3.0
Liczba godzin kontaktowych	**Liczba godzin** 30	**ECTS** 1.0

* godzina (lekcyjna) oznacza 45 minut

Treści programowe

Lp.	Treści programowe	Efekty uczenia się dla przedmiotu
1.	Pojęcie informacji i danych, jak przetwarzane są dane w systemach informatycznych. Pojęcie bezpieczeństwa i integralności danych, znaczenie informacji, niebezpieczeństwa związane z niewłaściwym przechowywaniem informacji.	W1, W2, W3, U1, U2, U3, K1, K2
2.	CIA triad - poufność (confidentiality), integralność (integrity) i dostępność do informacji (availability). Systemy zarządzania bezpieczeństwem informacji, Ustawa z dnia 5 lipca 2018r. o krajowym systemie cyberbezpieczeństwa, NIS2.	W1, W2, W3, U1, U2, U3, K1, K2
3.	Dlaczego i jak należy zabezpieczać nośniki danych. Szyfrowanie danych i połączeń, - wady, zalety, przypadki użycia, bezpieczeństwo, kryptografia klucza publicznego, 2FA i U2F i FIDO2. Bezpieczeństwo haseł i ich łamanie. Jakie hasła są bezpieczne i jak je przechowywać.	W1, W2, W3, U1, U2, U3, K1, K2
4.	Praktyczne aspekty pracy w kancelarii – organizacja środowiska pracy. Szyfrowanie nośników informacji, TrueCrypt VeraCrypt, BitLocker, tworzenie kontenerów, przechowywanie kluczy.	W1, W2, W3, U1, U2, U3, K1, K2
5.	Organizacja środowiska pracy. Bezpieczne przesyłanie wiadomości, dokumentów i załączników, PGP, 7Zip.	W1, W2, W3, U1, U2, U3, K1, K2
6.	Praktyczne aspekty pracy w kancelarii. Bezpieczeństwo kopii zapasowych z danymi osobowymi, zasady tworzenia kopii zapasowych, Dropbox, OneDrive, Google Drive a RODO (zajęcia praktyczne).	W1, W2, W3, U1, U2, U3, K1, K2
7.	Praktyczne aspekty pracy kancelarii – organizacja środowiska pracy. Bezpieczna praca zdalna, korzystanie z VPN.	W1, W2, W3, U1, U2, U3, K1, K2
8.	Praktyczne aspekty pracy w kancelarii – zasoby sieciowe, kontrola dostępu, reakcja na wypadek ataku ransomware, bezpieczeństwo systemów informatycznych, pojęcie luk systemowych.	W1, W2, W3, U1, U2, U3, K1, K2
9.	Praktyczne aspekty pracy w kancelarii – rozporządzenie eIDAS i podpisy elektroniczne, Kwalifikowany podpis elektroniczny, Zaawansowany podpis elektroniczny, Zwykły podpis elektroniczny, różnice i wykorzystanie w pracy prawnika, Ustawa o usługach zaufania i identyfikacji elektronicznej.	W1, W2, W3, U1, U2, U3, K1, K2
10.	Rodzaje ataków na informacje, bezpieczeństwo sieciowe i ochrona przed atakami. Ataki ransomware. Odpowiedzialność za niewłaściwe zabezpieczenie systemu informatycznego.	W1, W2, W3, U1, U2, U3, K1, K2

11.	Ataki Phishingowe i ich rodzaje jako model uzyskania dostępu do systemu informatycznego. Odpowiedzialność za niewłaściwe zabezpieczenie systemu informatycznego.	W1, W2, W3, U1, U2, U3, K1, K2
12.	Chmura obliczeniowa a narzędzia informatyczne wykorzystywane przez prawników. Oprogramowanie wykorzystujące Mechanizmy wykorzystujące sztuczną inteligencję oraz narzędzia pozwalające na automatyzację procesów w kancelarii.	W1, W2, W3, U1, U2, U3, K1, K2

Informacje rozszerzone

Metody nauczania:

wykład konwencjonalny, wykład z prezentacją multimedialną, konsultacje, rozwiązywanie zadań, analiza przypadków, dyskusja, burza mózgów, analiza tekstów.

Rodzaj zajęć	Formy zaliczenia	Warunki zaliczenia przedmiotu
wykład	egzamin	Egzamin pisemny (pytania problemowe i testowe) 4 pytań testowe - 1 krotnego wyboru po 1 pkt. 4 pytania opisowe z puli podanych 20 pytań. Odpowiedź na każde pytanie - pół strony po 4 punkty. Studenci sami opracowują odpowiedzi na pytania (na podstawie zajęć i własnego researchu) - mogą ze mną skonsultować poprawność odpowiedzi.

Wymagania wstępne i dodatkowe

Brak

Literatura

Kryminologia. Teoria i praktyka, red. P. Chomczyński, P. Frąckowiak, D. Woźniakowska, Warszawa 2024 - Rozdział 21
dla chętnych i dla rozwinięcia wiedzy Książka: Wprowadzenie do bezpieczeństwa IT - Tom 1, ed.MICHAŁ SAJDAK, 2024, Kraków