UNIWERSYTET IM. ADAMA MICKIEWICZA W POZNANIU

Cyberochrona w instytucjach

Sylabus zajęć

Informacje podstawowe

Kierunek studiów Bezpieczeństwo narodowe	**Cykl dydaktyczny** 2024/25
Specjalność Cyberbezpieczeństwo	**Kod zajęć** 14BENCBPS.22S.10116.24
Jednostka organizacyjna Wydział Nauk Politycznych i Dziennikarstwa	**Języki wykładowe** polski
Poziom studiów studia drugiego stopnia	**Obligatoryjność** Obowiązkowy specjalnościowy
Forma studiów studia stacjonarne	**Blok zajęciowy** Przedmioty specjalnościowe
Profil studiów profil praktyczny	

Koordynator zajęć	Jacek Raubo
Prowadzący zajęcia	Jacek Raubo

Okres	**Forma zajęć / liczba godzin / forma zaliczenia**	**Liczba punktów ECTS**
Semestr 2	• Ćwiczenia: 10, Zaliczenie z oceną	2

Cele kształcenia dla zajęć

Kod	Cel
C1	Celem przedmiotu „Cyberochrona w instytucjach” ma być w pierwszej kolejności zbudowanie świadomości absolwenta, niezbędnych do uchwycenia korelacji w zakresie sprawnego oraz efektywnego funkcjonowania zróżnicowanych podmiotów publicznych (jak również prywatnych, np. związanych z infrastrukturą krytyczną państwa) i niezbędnego ciągłego inwestowania w rosnące potrzeby cyberbezpieczeństwa. Stwarzając okazję do uwypuklenia obrazu domeny cyber, jako przestrzeni rozwijającej się i trudnej do zobrazowania konwencjonalnym zasobem definicyjnym oraz podejść naukowych, które są tradycyjnie wykorzystywane do opisu kwestii klasycznych dylematów bezpieczeństwa.
C2	Celem ma być ukazanie z jakimi wyzwaniami w domenie cyber, obecnie i w przyszłości, może mierzyć się instytucja publiczna/samorządowa (lub podmiot prywatny) jeśli chodzi o ochronę własnych zasobów w domenie cyber, jak również mapować rolę domeny cyber, jako przestrzeni wymagającej ochrony. Tym samym, twórcy przedmiotu dążą do nakreślenia niezbędnej wiedzy z zakresu prawnego (obowiązki, prawa, itp.), ale przede wszystkim praktycznego. Chodzi o stworzenie niezbędnej odpowiedzialności w zakresie projektowania podejścia do nowoczesnego cyberbezpieczeństwa.
C3	Celem jest, zarówno w oparciu o własne zasoby techniczne i kadrowe – budowanie dobrych praktyk wśród liderów bezpieczeństwa, w tym cyber, kończących kierunek bezpieczeństwo narodowe, ale też zdolność do współpracy z osobami o mniejszej świadomości wyzwań w sferze cyberbezpieczeństwa. Absolwenci mają, także uzyskać zdolność do samodzielnego poszukiwania niezbędnej współpracy technicznej z podmiotami prywatnymi – kluczowe firmy zapewniające usługi oraz rozwiązania z zakresu cyberbezpieczeństwa, ale również z odpowiednimi partnerami ze strony państwa, struktur naukowych, wojska oraz służb specjalnych. Tworząc tym samym komplementarne podejście do ciągłego doskonalenia się i przede wszystkim strategicznego pozycjonowania cyberbezpieczeństwa w planach funkcjonowania danej instytucji.

Wymagania wstępne

Student musi dysponować niezbędnym instrumentarium w zakresie pojęć podstawowych, odnoszących się do różnych kategorii bezpieczeństwa oraz cyberbezpieczeństwa. Chodzi przede wszystkim o wcześniejsze zdefiniowanie najważniejszych zagadnień z zakresu technologii informacyjnych. Istotne jest również umiejętne osadzenie kluczowych polskich instytucji odpowiedzialnych za bezpieczeństwo – MON, MSWiA, ABW, SKW, etc. w całościowym obrazie bezpieczeństwa państwa. Student winien charakteryzować się również podstawami w zakresie wiedzy odnoszącej się do systemu prawnego RP.

Efekty uczenia się dla zajęć

Kod	Efekty uczenia się dla zajęć w zakresie	Efekty uczenia się dla kierunku	Metody weryfikacji osiągnięcia efektów uczenia się dla zajęć
Wiedzy – Student/ka:			
W1	Potrafi zdefiniować zależność pomiędzy bezpieczeństwem pracy i funkcjonowania danej instytucji a cyberbezpieczeństwem.	BEN_K2_W01, BEN_K2_W02, BEN_K2_W03, BEN_K2_W04, BEN_K2_W05, BEN_K2_W08, BEN_K2_W10, BEN_K2_W11	Kolokwium pisemne
W2	Jest w stanie rozpoznawać i definiować kluczowe zagrożenia wynikające z rozwoju cyberprzestrzeni dla funkcjonowania wybranych instytucji w państwie.	BEN_K2_W01, BEN_K2_W02, BEN_K2_W03, BEN_K2_W04, BEN_K2_W05, BEN_K2_W08, BEN_K2_W09, BEN_K2_W10, BEN_K2_W11	Kolokwium pisemne

Kod	Efekty uczenia się dla zajęć w zakresie	Efekty uczenia się dla kierunku	Metody weryfikacji osiągnięcia efektów uczenia się dla zajęć
W3	Potrafi wskazywać kluczowe narzędzia techniczne oraz rozwiązania systemowe, dostępne na polskim i europejskim rynku mogące zwiększać poziom cyberbezpieczeństwa w pracy instytucji w Polsce.	BEN_K2_W01, BEN_K2_W02, BEN_K2_W03, BEN_K2_W04, BEN_K2_W05, BEN_K2_W08, BEN_K2_W09, BEN_K2_W10, BEN_K2_W11	Kolokwium pisemne
Umiejętności – Student/ka:			
U1	Zabiera głos w zakresie udoskonalania systemu cyberbezpieczeństwa w danej instytucji, dążąc do zrozumienia potrzeb technicznych oraz z zakresu zarządzania zasobami – kadrowymi, technicznymi i finansowymi.	BEN_K2_U01, BEN_K2_U02, BEN_K2_U03, BEN_K2_U04, BEN_K2_U05, BEN_K2_U06, BEN_K2_U08	Kolokwium pisemne
U2	Uczestniczy w ciągłym doskonaleniu systemu cyberbezpieczeństwa.	BEN_K2_U01, BEN_K2_U02, BEN_K2_U03, BEN_K2_U04, BEN_K2_U05, BEN_K2_U06, BEN_K2_U07, BEN_K2_U08	Kolokwium pisemne
Kompetencji społecznych – Student/ka:			
K1	Potrafi uzyskiwać wiedzę z różnych zasobów danych dotyczących cyberbezpieczeństwa, wykorzystując je w toku swojej pracy zawodowej lub służby.	BEN_K2_K01, BEN_K2_K02, BEN_K2_K03, BEN_K2_K04, BEN_K2_K05	Kolokwium pisemne

Treści programowe dla zajęć

Lp.	Treści programowe dla zajęć	Efekty uczenia się dla zajęć	Formy zajęć
1.	Nakreślenie obszaru zależności funkcjonowania bezpieczeństwa całościowego instytucji (struktury centralne, samorządowe, etc.) od ich poziomu cyberbezpieczeństwa w warunkach XXI w. – ukazanie rosnącej wrażliwości w holistycznym ujęciu funkcjonowania danej struktury.	W1, W2, W3, U1, U2, K1	Ćwiczenia
2.	Budowanie świadomości rosnących potrzeb cyberbezpieczeństwa w środowisku danej instytucji – problemy w odbiorze kwestii praktycznych przez osoby na różnych szczeblach zarządzania instytucją.	W1, W2, W3, U1, U2, K1	Ćwiczenia
3.	Współpraca w obrębie państwa, jako niezbędna odpowiedź na kolejne wyzwania w sferze cyberbezpieczeństwa.	W1, W2, W3, U1, U2, K1	Ćwiczenia

Lp.	Treści programowe dla zajęć	Efekty uczenia się dla zajęć	Formy zajęć
4.	Kluczowe wyzwania z jakimi może spotkać się instytucja publiczna oraz prywatna w przypadku cyberprzestrzeni. Od problemów technicznych po zaawansowane możliwości oddziaływania ze strony podmiotów państwowych oraz całego spektrum aktorów niepaństwowych.	W1, W2, W3, U1, U2, K1	Ćwiczenia
5.	Mapowanie kluczowych aktorów w sferze cyberbezpieczeństwa po stronie sektora prywatnego. Gdzie szukać rozwiązań sektorowych, kto oferuje rozwiązania całościowe w sferze cyberbezpieczeństwa.	W1, W2, W3, U1, U2, K1	Ćwiczenia
6.	Analiza kluczowych źródeł wiedzy w zakresie niezbędnych praktyk budowania odpowiedniego poziomu cyberbezpieczeństwa – jak tworzyć i monitorować zasoby informacji w dynamicznie zmieniającej się architekturze domeny cyber.	W1, W2, W3, U1, U2, K1	Ćwiczenia

Informacje dodatkowe

Forma zajęć	Metody i formy prowadzenia zajęć
Ćwiczenia	Wykład z prezentacją multimedialną wybranych zagadnień, Wykład konwersatoryjny, Wykład problemowy, Dyskusja, Metoda analizy przypadków, Uczenie problemowe (Problem-based learning), Metoda ćwiczeniowa

Forma zajęć	Warunki zaliczenia zajęć
Ćwiczenia	bardzo dobry (bdb; 5,0): wiedza, bardzo dobrze opanowane umiejętności oraz wykształcone kompetencje personalne i społeczne dobry plus (+db; 4,5): pogłębiona wiedza, dobrze wyuczone umiejętności oraz wykształcone kompetencje personalne i społeczne dobry (db; 4,0): dobra wiedza, dobrze wyuczone umiejętności oraz wykształcone kompetencje personalne i społeczne dostateczny plus (+dst; 3,5): zadawalająca wiedza, wyuczone umiejętności oraz kompetencje personalne i społeczne dostateczny (dst; 3,0): podstawowa wiedza, opanowane najważniejsze umiejętności oraz wykształcone podstawowe kompetencje personalne i społeczne niedostateczny (ndst; 2,0): niezadawalająca wiedza, nieopanowane umiejętności oraz niewykształcone kompetencje personalne i społeczne

Literatura

Obowiązkowa

1. Bezpieczeństwo informacyjne, Krzysztof Liderman, Wydawnictwo Naukowe EUN, 2017.
2. Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku, Marek Górka, Difin, 2014.
3. Cyberbezpieczeństwo, red. Cezary Banasiński i Marcin Rojszczak, Wolters Kluwer, 2020.
4. Cyberodpowiedzialność, Katarzyna Chałubińska-Jentkiewicz , Wydawnictwo Adam Marszałek 2019.

Nakład pracy studenta i punkty ECTS

Rodzaje zajęć studenta	Średnia liczba godzin* przeznaczonych na zrealizowane rodzaje zajęć

Ćwiczenia	10
Czytanie wskazanej literatury	40
Przygotowanie do egzaminu	10
Łączny nakład pracy studenta	**Liczba godzin** 60
Liczba punktów ECTS	**ECTS** 2

* godzina (lekcyjna) oznacza 45 minut

Efekty uczenia się dla kierunku

Kod	Treść
BEN_K2_K01	Absolwent/ka jest gotów/gotowa do poszerzania i aktualizowania oraz krytycznej oceny posiadanej wiedzy, w szczególności tej z obszaru nauki o bezpieczeństwie
BEN_K2_K02	Absolwent/ka jest gotów/gotowa do odpowiedzialnego pełnienia ról zawodowych, z uwzględnieniem zmieniających się potrzeb społecznych, oraz zachowywania się w sposób profesjonalny i etyczny w pracy zawodowej oraz działalności publicznej typowej dla specjalisty odpowiadającego za bezpieczeństwo lokalne, narodowe i międzynarodowe
BEN_K2_K03	Absolwent/ka jest gotów/gotowa do uznawania znaczenia wiedzy w rozwiązywaniu problemów poznawczych i praktycznych w naukach o bezpieczeństwie oraz zasięgania opinii ekspertów w przypadku trudności z samodzielnym rozwiązaniem problemu
BEN_K2_K04	Absolwent/ka jest gotów/gotowa do inicjowania działań na rzecz interesu publicznego oraz wypełniania zobowiązań społecznych, inspirowania i organizowania działalności na rzecz środowiska społecznego (w tym systemu bezpieczeństwa)
BEN_K2_K05	Absolwent/ka jest gotów/gotowa do rozwijania dorobku i podtrzymywania etosu zawodu specjalisty odpowiedzialnego za bezpieczeństwo lokalne, narodowe i międzynarodowe
BEN_K2_U01	Absolwent/ka potrafi właściwie dobierać źródła i informacje z nich pochodzące, dokonywać oceny, krytycznej analizy, syntezy, twórczej interpretacji i prezentacji tych informacji w celu formułowania i rozwiązywania złożonych i nietypowych problemów w zakresie nauki o bezpieczeństwie
BEN_K2_U02	Absolwent/ka potrafi innowacyjnie wykonywać zadania w nieprzewidywalnych warunkach przez odpowiedni dobór oraz stosowanie właściwych metod i narzędzi, w tym zaawansowanych technik typowych dla nauki o bezpieczeństwie
BEN_K2_U03	Absolwent/ka potrafi wykorzystywać posiadaną wiedzę do przystosowania istniejących lub opracowania nowych metod i narzędzi służących do rozwiązywania problemów w zakresie nauki o bezpieczeństwie
BEN_K2_U04	Absolwent/ka potrafi wykorzystywać posiadaną wiedzę do formułowania i rozwiązywania problemów oraz wykonywania zadań typowych dla działalności zawodowej specjalisty odpowiadającego za bezpieczeństwo lokalne, narodowe i międzynarodowe
BEN_K2_U05	Absolwent/ka potrafi formułować i testować hipotezy związane z prostymi problemami wdrożeniowymi charakterystycznymi dla nauki o bezpieczeństwie
BEN_K2_U06	Absolwent/ka potrafi umiejętnie wykorzystywać zdobytą wiedzę z zakresu nauki o bezpieczeństwie w komunikowaniu społecznym oraz politycznym i prowadzeniu debaty, rozszerzoną o krytyczną analizę skuteczności i przydatności stosowanej wiedzy
BEN_K2_U07	Absolwent/ka potrafi kierować pracą zespołu, w tym organizacji lub instytucji zajmującej się bezpieczeństwem oraz współdziałać z innymi osobami w ramach tych prac i przyjmować w nich wiodącą rolę
BEN_K2_U08	Absolwent/ka potrafi samodzielnie planować i realizować własne uczenie się przez całe życie i ukierunkowywać innych w tym zakresie
BEN_K2_W01	Absolwent/ka zna i rozumie w pogłębionym stopniu fakty, obiekty i zjawiska stanowiące zaawansowaną wiedzę ogólną z zakresu nauki o bezpieczeństwie
BEN_K2_W02	Absolwent/ka zna i rozumie w pogłębionym stopniu metody i narzędzia opisu, w tym techniki pozyskiwania i analizy danych oraz teorie dotyczące bezpieczeństwa, wyjaśniające złożone zależności między elementami systemów bezpieczeństwa
BEN_K2_W03	Absolwent/ka zna i rozumie wybrane zagadnienia z zakresu zaawansowanej wiedzy szczegółowej, właściwe dla kierunku bezpieczeństwo narodowe oraz zastosowania praktyczne tej wiedzy w działalności zawodowej specjalisty odpowiadającego za bezpieczeństwo lokalne, narodowe oraz międzynarodowe
BEN_K2_W04	Absolwent/ka zna i rozumie fundamentalne dylematy współczesnej cywilizacji, związane z rozwojem i rolą systemów bezpieczeństwa oraz ich wpływem na społeczeństwo
BEN_K2_W05	Absolwent/ka zna i rozumie ekonomiczne, prawne, etyczne i inne uwarunkowania działalności zawodowej typowej dla specjalisty odpowiadającego za bezpieczeństwo lokalne, narodowe i międzynarodowe

Kod	Treść
BEN_K2_W08	Absolwent/ka zna i rozumie w sposób pogłębiony wybrane metody i narzędzia opisu, w tym techniki pozyskiwania danych oraz modelowania systemu bezpieczeństwa i procesów w nim zachodzących, a także identyfikowania rządzących nim prawidłowości
BEN_K2_W09	Absolwent/ka zna i rozumie rolę systemu bezpieczeństwa w funkcjonowaniu grupy społecznej, państwa i wspólnoty międzynarodowej oraz ich historycznej ewolucji
BEN_K2_W10	Absolwent/ka zna i rozumie w sposób pogłębiony metody diagnozowania potrzeb i oceny jakości usług podmiotów odpowiedzialnych za bezpieczeństwo lokalne, narodowe i międzynarodowe
BEN_K2_W11	Absolwent/ka zna i rozumie funkcjonowanie organizacji i sposoby pracy w obszarze typowym dla specjalisty odpowiadającego za bezpieczeństwo lokalne, narodowe i międzynarodowe