Politechnika Opolska
Wydział Elektrotechniki, Automatyki i Informatyki

Karta Opisu Przedmiotu

Studia podyplomowe	**INFORMATYKA W PRAWIE I ADMINISTRACJI**		
Nazwa przedmiotu	**Cyberbezpieczeństwo**		
Subject Title	**Cybersecurity**		
Semestr	**ECTS (pkt,)**	**Tryb zaliczenia przedmiotu**	**Kod przedmiotu**
2	**2**	**Zaliczenie**	

Wymagania wstępne w zakresie przedmiotu	**Wiedza**	1. Podstawowa wiedza z zakresu technologii informacyjnej
	Umiejętności	1. Potrafi obsługiwać komputer i system operacyjny
	Kompetencje społeczne	1. Przestrzega zasad etyki zawodowej

Cele przedmiotu: Nabycie umiejętności dostrzegania problemów z zakresu cyberbezpieczeństwa

Program przedmiotu

Forma zajęć	**Liczba godzin zajęć w semestrze**	**Prowadzący zajęcia (tytuł/stopień naukowy, imię i nazwisko)**
Wykład	**8**	dr hab. inż. Michał Podpora
Ćwiczenia		
Laboratorium	**10**	dr hab. inż. Michał Podpora
Projekt		
Seminarium		

Treści kształcenia

Wykład	**Sposób realizacji**	**Wykład z dyskusją**

Lp.	**Tematyka zajęć**	**Liczba godzin**
1.	Zakres tematyki cyklu przedmiotów, warunki zaliczenia, literatura, wprowadzenie. Prywatność; anonimowość; ciasteczka; aktywność.	1
2.	Bezpieczeństwo danych i systemów w świetle prawa. RODO, GIODO, KC, KK.	1
3.	Bezpieczeństwo, podatności, zagrożenia, incydenty, pentesty. Phishing, malware, socjotechnika.	1
4.	Biały wywiad — wprowadzenie, przegląd technik i narzędzi, dobre praktyki.	1
5.	Biały wywiad — wielość podejść; Biały wywiad gospodarczy. Biały wywiad w domenie cyberbezpieczeństwa kraju.	1
6.	Dyski, macierze dyskowe, dyski sieciowe, przechowywanie w chmurze. Różne rzeczywistości definicji pliku skasowane o/utracone o/uszkodzonego.	1
7.	USB, BYOD i inni wrogowie bezpieczeństwa w firmie. Dlaczego hasła mają być bezpieczne (haveibeenpwned, inne). Higiena haseł. Skanery użytkowników i haseł, socjotechnika.	1
8.	Testy penetracyjne jako metoda weryfikacji bezpieczeństwa systemów i sieci. Pojęcie wycieku danych i typy wycieków danych. Konsekwencje wycieków danych i postępowanie w sytuacji wycieku. Metody ujawniania wycieków oraz zapobiegania.	1
Liczba godzin zajęć w semestrze		**8**

Laboratorium	**Sposób realizacji**	**Zajęcia praktyczne z komputerem**

Lp.	**Tematyka zajęć**	**Liczba godzin**
1.	Zakres tematyki, BHP, przedmiotowy system oceniania, organizacja zajęć. Instrukcja/dyskusja nt. przygotowania warsztatu do pracy własnej. Podstawowa ochrona własne o komputera oraz własnych danych sensytywnych.	2
2.	Podstawowa ochrona domowej sieci komputerowej. Podstawowa ochrona małej firmowej sieci komputerowej. Podstawowa ochrona danych w małej firmie. Ochrona danych osobowych.	2

3.	Biały wywiad w zastosowaniach wywiadu gospodarczego. Biały wywiad w zastosowaniach do analiz zależności ekonomicznych dużych działań cyberagresji zorganizowanej.	2
4.	Narzędzia programowe i sprzętowe przydatne przy odzyskiwaniu (i pozyskiwaniu) informacji Warsztat informatyka śledczego.	2
5.	Bezpieczeństwo sieci lokalnej — warsztaty z użyciem programu przechwytującego — analiza działania protokołów warstwy transportowej modelu OSI: TCP i UDP.	2
Liczba godzin zajęć w semestrze		**10**

Efekty uczenia się dla przedmiotu - po zakończonym cyklu studiów			**Odniesienie do kierunkowych efektów uczenia się**	**Formy realizacji (W, C, L, P, S)**	**Formy weryfikacji efektów uczenia się**
Wiedza	1.	Zna definicję Białego Wywiadu oraz działania w obszarze sieci komputerowych i systemów operacyjnych, które mieszczą się w niej, potrafi jasno odróżnić od nich działania będące włamaniem /nieautoryzowanym dostępem.	P_W01	W	C F G
	2.	Zna podstawowe portale, metody, techniki i narzędzia wykorzystywane przy pozyskiwaniu informacji w ramach białego wywiadu, granice białego wywiadu.	P_W04	W	C F G
Umiejętności	1.	Potrafi rozpoznawać i właściwie reagować na zagrożenia bezpieczeństwa informacji związane z nieautoryzowanym dostępem do danych.	P_U03	L	F N O R
	2.	Potrafi wybrać i zastosować odpowiednią strategię i technologię magazynowania danych, jak również odpowiednią metodę i narzędzie odzyskiwania danych.	P_U05	L	F N O R
Kompetencje społeczne	1 .	Potrafi zastosować posiadane kompetencje miękkie, współpracować w grupie, a także rozpoznać atak socjotechniczny wykorzystujący kompetencje miękkie.	P_K03	L	F N O R

Formy weryfikacji efektów uczenia się:

A-egzamin pisemny, B-egzamin ustny, C-zaliczenie pisemne, D-zaliczenie ustne, E-na podstawie ocen cząstkowych z odpowiedzi ustnych, F-na podstawie ocen cząstkowych z odpowiedzi pisemnych, G-praca kontrolna, H-ocena ze sprawozdań, I-ocena z przebiegu ćwiczeń, J-ocena z przygotowania do ćwiczeń, K-ocena z przebiegu realizacji projektu, L-ocena pisemnej realizacji projektu, M-ocena z obrony projektu, N-ocena formy prezentacji, O-ocena treści prezentacji, P-obserwacja aktywności na zajęciach, R-obserwacja systematyczności.

Metody dydaktyczne:

Wykład: Wykład z dyskusją

Laboratorium: Zajęcia praktyczne z komputerem

Zajęcia mogą być prowadzone z wykorzystaniem metod i technik kształcenia na odległość.

Forma i warunki zaliczenia przedmiotu:

Wykład — zaliczenie pisemne na ocenę. Próg zaliczenia 50% punktów. Progi ocen co 10%.

Ćwiczenia — ocena na podstawie ocen cząstkowych z ćwiczeń + prezentacji + aktywności. Próg zaliczenia 50% punktów. Progi ocen co 10%.

Literatura podstawowa:

1. Liedel K., Serafin T., Otwarte źródła informacji w działalności wywiadowczej, ISBN: 978-83-7641-406-5, Difin, 2011
2. Filipkowski W., Mądrzejowski W. red., Biały wywiad. Otwarte źródła informacji wokół teorii i praktyki, ISBN: 978-83- 255-3425-7, C.H. Beck, 2011
3. Hadnagy C., Socjotechnika: sztuka zdobywania władzy nad umysłami, ISBN: 978-83-283-6319-9, Helion, 2020
4. Sanger DE, Cyberbroń - broń doskonała. Wojny, akty terroryzmu i zarządzanie strachem w epoce komputerów, ISBN: 978-83-283-7152-1, Helion, 2021
5. Preston W.C., Archiwizacja i odzyskiwanie danych, ISBN: 978-83-246-1182-9, Helion 2008
6. Kalinowski A., Metody Inwigilacji i Elementy Informatyki Śledczej., ISBN: 978-83-923745-4-1, CSH, 2011

Literatura uzupełniająca:

1. Ahearn F.M., Wyrażenia regularne„ ISBN: 978-83-246-6868-7, Helion, 2013
2. Long J., Google Hacking for Penetration Testers, ISBN: 9781931836364, Syngress Media Inc., 2001
3. Fitzgerald M., How to disappear, ISBN: 9784-1-59921-977-6, Lyons Press, 2010
4. M., Hiding from the Internet, ISBN: 978-1478277293, CCI Publishing, 2013
5. Calishain T., Dornfest R., Google hacks. Tips & tools for smarter searching, ISBN: 0-596-00857-0, O'Reilly, 2005