Szczegółowe informacje o seminarium		
Temat przedmiotu:	Bezpieczeństwo informacji i ochrona danych	
Grupa Kierunków:	**Stopień studiów:**	**Tryb studiów:**
	II	niestacjonarne
Nazwa Kierunku:	Zarządzanie biznesem	
Specjalność:	Zarządzanie zasobami IT	
Promotor:	dr Grzegorz Podgórski	

Opis tematyki seminarium:

Seminarium skierowane jest dla osób zainteresowanych tematyką bezpieczeństwa informacji, usług i zasobów IT w nowoczesnej instytucji i organizacji. Poruszane zagadnienia będą się odnosić do organizacji wykorzystujących między innymi nowoczesne technologie takie jakie: chmura obliczeniowa, IoT, BlockChain, BYOD, BYOT. Organizacji i instytucji wykorzystujących model pracy stacjonarnej, zdalnej i mieszanej chcących zapewnić odpowiedni poziom bezpieczeństwa informacji i usług.

Na seminarium poruszane będą takie zagadnienia jak: zapewnienie i zarządzanie bezpieczeństwem zasobów IT w organizacji przy wykorzystaniu nowych technologii oraz wpływ nowych trendów na bezpieczeństwo sieci, systemów informatycznych oraz ciągłości działania usług. Dyskutowane i analizowane będą m.in. zagadnienia związane z wartością informacji, zagrożeniami bezpieczeństwa informacji oraz sposoby zabezpieczeń.

Wymagania/preferencje wstępne dla seminarium	Liczba miejsc:
brak	6-12

Szczegółowy opis przedmiotu:

Treści programowe (tematy/problemy zajęć):	L.g. dydaktycznych
1. Cel, zakres i przedmiot seminarium. Wymogi formalne i organizacyjne. 2. Omówienie podstawowych pojęć związanych z pracą magisterską (formułowanie tezy pracy, celów pracy, narzędzia badawcze, struktura pracy, literatura, pozyskiwanie danych). 3. Rola informacji we współczesnym świecie oraz dla organizacji (rodzaje, klasyfikacja, czas życia informacji, atrybuty informacji). 4. Omówienie problematyki dotyczącej bezpieczeństwa zasobów i usług IT w organizacjach wykorzystujących nowoczesne technologie. 5. Nowoczesne technologie a bezpieczeństwo informacji – chmura obliczeniowa, IoT, blockchain, BYOD. 6. Wybór i dyskusja tematyki prac. 7. Konsultacje nad proponowanymi metodykami badań. 8. Dyskusja nad harmonogramami prac. 9. Dyskusja nad wybranymi źródłami i literaturą. 10. Dyskusja nad wynikami prowadzonych badań. 11. Prezentacja rozdziałów prac i wyników badań.	25

Literatura:

Obowiązkowa:

- A. Białas: „Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie”, PWN, Warszawa 2022
- W. Stallings, L. Brown "Bezpieczeństwo systemów informatycznych. Zasady i praktyka. Wydanie IV. Tom 1", Helion 2019
- W. Stallings, L. Brown "Bezpieczeństwo systemów informatycznych. Zasady i praktyka. Wydanie IV. Tom 2", Helion 2019
- K.Liderman "Bezpieczeństwo informacyjne. Nowe wyzwania", PWN, 2017

Zalecana:

- Y. Diogenes, E. Ozkaya "Cybersecurity Attack and Defense Strategies", Packt Publishing, 2018
- A. Barczuk, T. Sydoruk: „Bezpieczeństwo systemów informatycznych zarządzania”, Dom Wydawniczy Bellona, Warszawa 2003.

Sposób obliczania oceny semestralnej / końcowej z przedmiotu (algorytm)**:**

Semestr 2:

Obecność na spotkaniach – 10%

Wybór tematyki pracy – 80%

Wygłoszenie referatu na temat pracy – 10%

Semestr 3:

Obecność na spotkaniach – 10%

Koncepcja pracy – 30%

Spis treści – 10%

Plan badań – 20%

Rozdziały teoretyczne – 40%

Semestr 4:

Prezentacja wyników badań – 50%

Złożenie całej pracy – 50%