

Szczegółowe informacje o seminarium		
<b>Temat przedmiotu:</b>	Bezpieczeństwo informacji w erze cyfryzacji	
<b>Grupa Kierunków:</b>	<b>Stopień studiów:</b>	<b>Tryb studiów:</b>
	I	stacjonarne
<b>Nazwa Kierunku:</b>	Cyfryzacja i zarządzanie danymi w biznesie	
<b>Specjalność:</b>	-	
<b>Promotor:</b>	dr Grzegorz Podgórski	
<b>Opis tematyki seminarium:</b>		
<p>Tematyka seminarium dotyczy:</p> <p>Seminarium skierowane jest dla osób zainteresowanych tematyką bezpieczeństwa informacji i usług w nowoczesnej instytucji i organizacji. Poruszane zagadnienia będą się odnosić do organizacji wykorzystujących między innymi nowoczesne technologie takie jak: chmura obliczeniowa, IoT, BlockChain, BYOD, BYOT. Organizacji i instytucji wykorzystujących model pracy stacjonarnej, zdalnej i mieszanej chcących zapewnić odpowiedni poziom bezpieczeństwa informacji i usług.</p> <p>Poruszane będą takie zagadnienia jak bezpieczeństwo sieci i systemów teleinformatycznych, jak również bezpieczeństwo nowych technologii oraz wpływ nowych trendów na bezpieczeństwo sieci, systemów informatycznych oraz usług. Omówione zostaną także zagadnienia związane z wartością informacji w dzisiejszym świecie, zagrożeniami bezpieczeństwa informacji oraz sposoby zabezpieczeń.</p>		
<b>Wymagania/preferencje wstępne dla seminarium</b>		<b>Liczba miejsc:</b>
brak		6-12
<b>Szczegółowy opis przedmiotu:</b>		
<b>Treści programowe (tematy/problemy zajęć):</b>		<b>L.g. dydaktycznych</b>
<ol style="list-style-type: none"> <li>1. Cel, zakres i przedmiot seminarium. Wymogi formalne i organizacyjne.</li> <li>2. Omówienie podstawowych pojęć związanych z pracą dyplomową (formułowanie tezy pracy, celów pracy, narzędzia badawcze, struktura pracy, literatura, pozyskiwanie danych).</li> <li>3. Rola informacji we współczesnym świecie (rodzaje, klasyfikacja, czas życia informacji, atrybuty informacji).</li> <li>4. Omówienie problematyki dotyczącej bezpieczeństwa informacji i danych w organizacjach wykorzystujących nowoczesne technologie.</li> <li>5. Nowoczesne technologie a bezpieczeństwo informacji – chmura obliczeniowa, IoT, blockchain, BYOD.</li> <li>6. Wybór i dyskusja tematyki prac.</li> <li>7. Konsultacje nad proponowanymi metodykami badań.</li> <li>8. Dyskusja nad harmonogramami prac.</li> </ol>		66

- |  |  |
|--|--|
| 9. Dyskusja nad wybranymi źródłami i literaturą. |  |
| 10. Dyskusja nad wynikami prowadzonych badań.    |  |
| 11. Prezentacja rozdziałów prac i wyników badań. |  |

#### Literatura:

##### Obowiązkowa:

- 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, 2018
- A. Białas: „Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie”, PWN, Warszawa 2018.

##### 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.
- Liderman K.: Podręcznik administratora bezpieczeństwa teleinformatycznego. Mikom, Warszawa, grudzień 2003

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

##### Semestr 4:

Obecność na spotkaniach – 10%

Wybór tematyki pracy – 80%

Wygłoszenie referatu na temat pracy – 10%

##### Semestr 5:

Obecność na spotkaniach – 10%

Koncepcja pracy – 30%

Spis treści – 10%

Plan badań – 20%

Rozdziały teoretyczne – 40%

##### Semestr 6:

Prezentacja wyników badań – 50%

Złożenie całej pracy – 50%