



Karta przedmiotu  
Bezpieczeństwo systemów informacyjnych

**1. Informacje podstawowe**

<b>Kierunek studiów</b> elektronika i telekomunikacja	<b>Cykl kształcenia (nabór)</b> 2024/25	
<b>Specjalność</b> -	<b>Kod przedmiotu</b> 05EITS.DI3C.0356.24	
<b>Jednostka zarządzająca kierunkiem studiów</b> Wydział Telekomunikacji, Informatyki i Elektrotechniki	<b>Języki wykładowe</b> polski	
<b>Poziom studiów</b> drugiego stopnia (mgr inż.)	<b>Obligatoryjność</b> Obowiązkowy	
<b>Profil studiów</b> Profil ogólnoakademicki	<b>Blok zajęciowy</b> Przedmioty kierunkowe	
<b>Forma studiów</b> studia stacjonarne		
<b>Wymagania wstępne</b>	Podstawowa wiedza z zakresu sieci komputerowych i systemów operacyjnych.	
<b>Przedmioty wprowadzające</b>	matematyka	
<b>Koordinator</b>	Jacek Majewski	
<b>Okres</b> Semestr 1	<b>Forma i godziny zajęć</b> • Wykład: 15, Zaliczenie na ocenę	<b>Liczba punktów ECTS</b> 1
<b>Okres</b> Semestr 2	<b>Forma i godziny zajęć</b> • Ćwiczenia projektowe: 30, Zaliczenie na ocenę	<b>Liczba punktów ECTS</b> 2

**2. Efekty uczenia się dla przedmiotu**

Kod	Opis efektów uczenia się	Odniesienie do kierunkowych efektów uczenia się	Odniesienie do charakterystyk PRK
<b>Wiedza:</b>			
W1	ma pogłębioną wiedzę w zakresie budowy systemu zarządzania bezpieczeństwem informacji w procesach przetwarzania danych w firmowych systemach informatycznych	EIT_O2_K_W05, EIT_O2_K_W20	P7S_WK, P7S_WG P7S_WG_inż
W2	posiada wiedzę o trendach technologii ICT i ich wpływ na politykę bezpieczeństwa informacyjnego	EIT_O2_K_W07	P7S_WG
<b>Umiejętności:</b>			
U1	potrafi przeprowadzić proces weryfikacji bezpieczeństwa wskazanego elementu w zadaniu projektowym	EIT_O2_K_U09, EIT_O2_K_U32, EIT_O2_K_U33, EIT_O2_K_U34	P7S_UO, P7S_UW, P7S_UW_inż, P7S_UW, P7S_UW_inż, P7S_UW P7S_UW_inż
U2	potrafi zaproponować ulepszenia poprawiające poziom bezpieczeństwa wskazanego elementu w zadaniu projektowym	EIT_O2_K_U11, EIT_O2_K_U25, EIT_O2_K_U28	P7S_UW, P7S_UW_inż, P7S_UW, P7S_UW_inż, P7S_UW P7S_UW_inż
<b>Kompetencje społeczne:</b>			
K1	rozumie potrzebę współpracy w grupie projektowej i konieczność efektywnej komunikacji	EIT_O2_K_K05	P7S_KO

### 3. Treści programowe

Lp.	Treści programowe	Formy zajęć	Efekty uczenia się dla przedmiotu
1.	<p>1. Bezpieczeństwo - definicje pojęć podstawowych (informacja, dezinformacja, entropia, środki bezpieczeństwa, poufność, integralność, dostępność, tajność, nienaruszalność danych itd..).</p> <p>2. Bezpieczeństwo jako proces realizowany w czasie obejmujący różne dziedziny i obszary funkcjonowania firmy.</p> <p>3. Dobre praktyki bezpieczeństwa dla systemów teleinformatycznych.</p> <p>4. Model ISO OSI RM (ang. ISO Open Systems Interconnection Reference Model ) i TCP/IP - funkcjonalność.</p> <p>5. Usługi z zakresu bezpieczeństwa - analiza na modelu funkcjonalnym ISO OSI RM.</p> <p>6. Rola czynnika ludzkiego w budowaniu polityki zabezpieczeń - socjotechnika.</p> <p>7. Rola procesu analizy ryzyka w efektywnym budowaniu polityki bezpieczeństwa.</p> <p>8. Systemy monitorowania aktywności oraz wykrywanie i przeciwdziałanie incydentom bezpieczeństwa (IPS, IDS ang. Intrusion Detection System, Intrusion Prevention System).</p> <p>9. Sieci operacyjne OT i ich podatności.</p> <p>10. Porównanie sieci operacyjnych OT i sieci IT.</p> <p>11. Charakterystyka modelu "Zero Trust Security".</p> <p>12. Specyfika kryptografii klucza publicznego na przykładzie specyfikacji FIDO2.</p> <p>13. Środowisko zintegrowanego zarządzania bezpieczeństwem - SIEM</p> <p>14. Systemy identyfikacji zdarzeń (konsekwencje i zagrożenia) - wg. RFC 4949</p> <p>W trakcie wykładu będą analizowane na bieżąco wybrane incydenty z zakresu bezpieczeństwa.</p>	Wykład	W1, W2
2.	<p>Tematy są wybierane przez zespoły (2-3 osobowe). Obszar tematu obejmuje opracowanie (lub analizę) metod zabezpieczeń danych w procesach systemu zarządzania bezpieczeństwem informacji.</p> <p>Wykorzystanie środków programowych, sprzętowych oraz proceduralnych w celu określenia optymalnego systemu zabezpieczeń dotyczących atrybutów (ISO 27001): poufności, integralności i dostępności danych.</p>	Ćwiczenia projektowe	U1, U2, K1

#### 4. Metody prowadzenia zajęć, weryfikacji efektów uczenia się i warunki zaliczenia

##### Semestr 1

Forma zajęć	
-------------	--

Wykład	<b>Metody prowadzenia zajęć:</b>	
	Wykład	
	<b>Metody (sposoby) weryfikacji:</b>	<b>Udział:</b>
	Test	100%
	<b>Warunki zaliczenia przedmiotu:</b>	
	<p>Test (wielokrotnego wyboru z dodatnimi i ujemnymi punktami) zawiera zagadnienia z zakresu W1 i W2 efektów uczenia się. Każdorazowo w przypadku zestawu pytań i odpowiedzi jest określana wartość minimalna punktów do uzyskania pozytywnej oceny (osiągnięcia powyżej 51 % efektów uczenia się). Pozostała skala ocen jest zgodna z:</p> <ul style="list-style-type: none"> <li>• poniżej 51% - niedostateczny (2,0)</li> <li>• od 51 % - dostateczny (3,0)</li> <li>• od 61 % - dostateczny plus (3,5)</li> <li>• od 71 % - dobry (4,0)</li> <li>• od 81 % - dobry plus (4,5)</li> <li>• od 91% - bardzo dobry (5,0)</li> </ul>	

## Semestr 2

Forma zajęć		
Ćwiczenia projektowe	<b>Metody prowadzenia zajęć:</b>	
	Dyskusja, Projekt, Case study, Praca w grupie	
	<b>Metody (sposoby) weryfikacji:</b>	<b>Udział:</b>
	Projekt	70%
	Udział w dyskusji	20%
	Aktywność	10%
	<b>Warunki zaliczenia przedmiotu:</b>	
Ocena projektu, rozwiązania postawionego problemu, aktywność w jego realizacji, planowość w realizacji etapów, współpraca w grupie, udział w dyskusji.		

Efekt uczenia się dla przedmiotu	Metody (sposoby) weryfikacji			
	Test	Projekt	Aktywność	Udział w dyskusji
W1	x			
W2	x			
U1		x		x
U2		x		x
K1		x	x	x

## 5. Literatura

### Literatura podstawowa

1. Białas A., 2018, Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie, Wydawnictwo Naukowe PWN
2. Fry Ch., Nystrom M., 2010, Monitoring i bezpieczeństwo sieci, Helion
3. Normy dotyczące bezpieczeństwa informacji ISO/IEC, PN
4. Liderman K., 2008, Analiza ryzyka i ochrona informacji w systemach komputerowych, Wydawnictwo Naukowe PWN
5. Karpiński M., 2012, Bezpieczeństwo informacji: praca zbiorowa, Wydawnictwo PAK
6. M. Liyanage, A. Braeken, P. Kumar, M. Ylianttila, "IoT Security: Advances in Authentication", J. Wiley & Sons, 2019

### Literatura uzupełniająca

1. Analiza incydentów (raporty) - naruszeń bezpieczeństwa technologii, procedur
2. Trejderowski T., 2016, Socjotechnika. Podstawy manipulacji w praktyce, Wydawnictwo Naukowe PWN
3. Stokłosa J., Bilski T., Pankowski T., 2001, Bezpieczeństwo danych w systemach informatycznych, Wydawnictwo Naukowe PWN
4. Raporty European Union Agency for Network and Information Security (<https://www.enisa.europa.eu>)

## 6. Nakład pracy studenta - bilans godzin i punktów ECTS

Aktywność studenta		Obciążenie studenta Liczba godzin
Zajęcia prowadzone z bezpośrednim udziałem nauczyciela akademickiego lub innych osób prowadzących zajęcia	Wykład	15
	Ćwiczenia projektowe	30
Praca własna studenta	Konsultacje	10
	Zbieranie informacji do zadanej pracy	5
	Przygotowanie do zajęć	10
	Przygotowanie projektu	20
<b>Łączny nakład pracy studenta</b>		90
<b>Liczba punktów ECTS</b>		3

\* Godzina (dydaktyczna) oznacza 45 minut