POLITECHNIKA BYDGOSKA
Wydział Telekomunikacji, Informatyki i Elektrotechniki

Karta przedmiotu

Bezpieczeństwo systemów informacyjnych

1. Informacje podstawowe

Kierunek studiów elektronika i telekomunikacja	**Cykl kształcenia (nabór)** 2024/25
Specjalność -	**Kod przedmiotu** 05EITN.DI3C.0356.24
Jednostka zarządzająca kierunkiem studiów Wydział Telekomunikacji, Informatyki i Elektrotechniki	**Języki wykładowe** polski
Poziom studiów drugiego stopnia (mgr inż.)	**Obligatoryjność** Obowiązkowy
Profil studiów Profil ogólnoakademicki	**Blok zajęciowy** Przedmioty kierunkowe
Forma studiów studia niestacjonarne	

Wymagania wstępne	Podstawowa wiedza z zakresu sieci komputerowych i systemów operacyjnych.
Przedmioty wprowadzające	matematyka
Koordynator	Jacek Majewski

Okres	**Forma i godziny zajęć**	**Liczba punktów ECTS**
Semestr 1	• Wykład: 9, Zaliczenie na ocenę	1

Okres	**Forma i godziny zajęć**	**Liczba punktów ECTS**
Semestr 2	• Ćwiczenia projektowe: 18, Zaliczenie na ocenę	2

2. Efekty uczenia się dla przedmiotu

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

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

Semestr 1

Forma zajęć	

Wykład	**Metody prowadzenia zajęć:**	
	Wykład	
	Metody (sposoby) weryfikacji:	**Udział:**
	Test	100%
	Warunki zaliczenia przedmiotu:	
	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 (osiagnięcia powyżej 51 % efektów uczenia się). Pozostała skala ocen jest zgodna z: • poniżej 51% - niedostateczny (2,0) • od 51 % - dostateczny (3,0) • od 61 % - dostateczny plus (3,5) • od 71 % - dobry (4,0) • od 81 % - dobry plus (4,5) • od 91% - bardzo dobry (5,0)	

Semestr 2

Forma zajęć		
Ćwiczenia projektowe	**Metody prowadzenia zajęć:**	
	Dyskusja, Projekt, Case study, Praca w grupie	
	Metody (sposoby) weryfikacji:	**Udział:**
	Projekt	70%
	Udział w dyskusji	20%
	Aktywność	10%
	Warunki zaliczenia przedmiotu:	
	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	9
	Ćwiczenia projektowe	18
Praca własna studenta	Konsultacje	10
	Zbieranie informacji do zadanej pracy	5
	Przygotowanie do zajęć	15
	Przygotowanie projektu	20
Łączny nakład pracy studenta		77
Liczba punktów ECTS		3

* Godzina (dydaktyczna) oznacza 45 minut