

KARTA PRZEDMIOTU

Kod przedmiotu	0714.8.ME1.D17.BPDC	
Nazwa przedmiotu w języku	polskim	Bezpieczeństwo przetwarzania danych cyfrowych Safety of digital data processing
	angielskim	

1. USYTUOWANIE PRZEDMIOTU W SYSTEMIE STUDIÓW

1.1. Kierunek studiów	Mechatronika
1.2. Forma studiów	Studia stacjonarne / studia niestacjonarne
1.3. Poziom studiów	Studia pierwszego stopnia inżynierskie
1.4. Profil studiów*	Praktyczny
1.5. Osoba przygotowująca kartę przedmiotu	dr inż. Zbigniew Nagórny
1.6. Kontakt	znagorny@ujk.edu.pl

2. OGÓLNA CHARAKTERYSTYKA PRZEDMIOTU

2.1. Język wykładowy	Polski
2.2. Wymagania wstępne*	Podstawowa wiedza z zakresu podstawy informatyki i sieci komputerowe

3. SZCZEGÓŁOWA CHARAKTERYSTYKA PRZEDMIOTU

3.1. Forma zajęć	Wykład 30h (w tym 10h e-learning), ćwiczenia 60h	
3.2. Miejsce realizacji zajęć	Zajęcia w pomieszczeniach Filii w Sandomierzu oraz zdalnie przy użyciu platform dostępnych w Uczelni	
3.3. Forma zaliczenia zajęć	Wykład: egzamin, ćwiczenia: zaliczenie z oceną	
3.4. Metody dydaktyczne	Wykład informacyjny z użyciem komputera, metoda przypadków, opis, ćwiczenia przedmiotowe	
3.5. Wykaz literatury	podstawowa	<ol style="list-style-type: none"> Liderman K.: Bezpieczeństwo informacyjne. PWN, Warszawa, 2012. Stokłosa J., Bilski T., Pankowski T.: Bezpieczeństwo danych w systemach informatycznych. PWN, Warszawa, 2001.
	uzupełniająca	<ol style="list-style-type: none"> Strebe M.: Bezpieczeństwo sieci. Wyd. MIKOM, Warszawa, 2005. Schneier B.: Kryptografia dla praktyków. WNT, Warszawa, 2002. Adams C., Lloyd S.: Podpis elektroniczny: klucz publiczny. Wydawnictwo Robomatic, Wrocław, 2002.

4. CELE, TREŚCI I EFEKTY UCZENIA SIĘ

<p>4.1. Cele przedmiotu</p> <p>Wykład</p> <p>C1. Przedstawienie studentom wiedzy z zakresu bezpieczeństwa gromadzenia, przechowywania i przesyłania danych cyfrowych</p> <p>Ćwiczenia</p> <p>C2. Kształtowanie u studentów umiejętności stosowania zasady zapewniające bezpieczeństwo gromadzenia, przechowywania i przesyłania danych cyfrowych</p>	<p>4.2. Treści programowe</p> <p>Wykład (30h)</p> <ol style="list-style-type: none"> Zagrożenia bezpieczeństwa systemów komputerowych. Rodzaje ataków na systemy komputerowe. Podstawowe zasady zapewniające bezpieczeństwo systemów komputerowych. Inżynieria społeczna a bezpieczeństwo systemów komputerowych. Szyfrowanie, szyfry symetryczne, szyfry asymetryczne. Techniczne podstawy podpisu elektronicznego. Funkcje realizowane przez podpis elektroniczny. Zastosowanie podpisu elektronicznego w administracji i gospodarce. Platforma ePUAP, Profil Zaufany. Metody uwierzytelniania, autoryzacji i kontroli dostępu. <p>(w tym 10h e-learning)</p> <ol style="list-style-type: none"> Bezpieczeństwo systemów operacyjnych. Bezpieczeństwo sieci komputerowych. Bezpieczne protokoły sieciowe, zastosowanie. Bezpieczeństwo fizyczne. Polityka bezpieczeństwa. <p>Ćwiczenia (30h)</p> <ol style="list-style-type: none"> Urząd certyfikacji, certyfikat klucza publicznego, rodzaje certyfikatów.
---	--

2. Funkcje skrótu, zastosowanie.
3. Proces składania i weryfikacji podpisu elektronicznego.
4. Tworzenie i wysyłanie pism urzędowych poprzez platformę ePUAP.
5. Zasady tworzenia silnych haseł.
6. Ochrona przed wirusami komputerowymi i złośliwym oprogramowaniem.
7. Archiwizacja i ochrona danych.
8. Bezpieczeństwo usług katalogowych.
9. Bezpieczeństwo sieci Wi-Fi.
10. Bezpieczeństwo aplikacji sieciowych.
11. Zapora ogniowa, zasada działania, konfiguracja, zastosowanie.
12. Strefa zdemilitaryzowana, zastosowanie.
13. Sieci VPN, konfiguracja, zastosowanie.
14. Monitorowanie zabezpieczeń w systemach komputerowych.
15. Podsumowanie ćwiczeń i zaliczenie.

4.3. Przedmiotowe efekty uczenia się

Efekt	Student, który zaliczył przedmiot	Odniesienie do kierunkowych efektów uczenia się
w zakresie WIEDZY:		
W01	Zna zagrożenia dla bezpieczeństwa systemów komputerowych.	M1P_W02
W02	Ma uporządkowaną wiedzę na temat sposobów zapewnienia bezpieczeństwa gromadzenia, przechowywania i przesyłania danych w systemach komputerowych.	M1P_W02
w zakresie UMIEJĘTNOŚCI:		
U01	Potrafi konfigurować i zarządzać systemami komputerowymi, z uwzględnieniem zasad bezpieczeństwa.	M1P_U02 M1P_U06
U02	Potrafi monitorować zabezpieczenia w systemach komputerowych.	M1P_U02 M1P_U06
U03	Potrafi pozyskiwać informacje z zakresu bezpieczeństwa przetwarzania danych cyfrowych z literatury, baz danych i innych źródeł, także w języku angielskim lub innym języku obcym; potrafi łączyć i interpretować uzyskane informacje, jak również wyciągać wnioski i uzasadniać opinie.	M1P_U01 M1P_U08
U04	Ma umiejętność samokształcenia się z zakresu bezpieczeństwa przetwarzania danych cyfrowych.	M1P_U09 M1P_U10 M1P_U13
w zakresie KOMPETENCJI SPOŁECZNYCH:		
K01	Ma świadomość potrzeby uzupełniania wiedzy z zakresu bezpieczeństwa przetwarzania danych cyfrowych przez całe życie i potrafi dobrać właściwe metody uczenia.	M1P_K01
K02	Rozumie pozatechniczne aspekty działalności inżyniera-mechatronika w zakresie bezpieczeństwa przetwarzania danych cyfrowych, między innymi jej konsekwencje społeczne oraz wpływ na stan środowiska.	M1P_K02
K03	Rozumie społeczną rolę inżyniera oraz bierze udział w przekazywaniu społeczeństwu wiarygodnych informacji i opinii dotyczących osiągnięć techniki i innych jej aspektów, szczególnie w zakresie bezpieczeństwa przetwarzania danych cyfrowych.	M1P_K02 M1P_K03

4.4. Sposoby weryfikacji osiągnięcia przedmiotowych efektów uczenia się

Efekty przedmiotowe (symbol)	Sposób weryfikacji (+/-)																				
	Egzamin ustny/pisemny*			Kolokwium*			Projekt*			Aktywność na zajęciach*			Praca własna*			Praca w grupie*			Inne Test e-learning		
	Forma zajęć			Forma zajęć			Forma zajęć			Forma zajęć			Forma zajęć			Forma zajęć			Forma zajęć		
	W	C	...	W	C	...	W	C	...	W	C	...	W	C	...	W	C	...	W	C	E
W01-W02	+	-	-	-	+	-	-	-	-	+	-	-	+	-	-	-	-	-	-	-	+
U01-U04	+	-	-	-	+	-	-	-	-	+	-	-	+	-	-	+	-	-	-	-	+
K01-K03	-	-	-	-	-	-	-	-	-	+	-	-	-	-	-	+	-	-	-	-	-

*niepotrzebne usunąć

4.5. Kryteria oceny stopnia osiągnięcia efektów uczenia się

Forma zajęć	Ocena	Kryterium oceny
(W) * (w tym e-learning)	3	50-65% ogólnej liczby punktów do zdobycia z egzaminu i testu e-learningowego pod warunkiem uzyskania zaliczenia z ćwiczeń
	3,5	66-70% ogólnej liczby punktów do zdobycia z egzaminu i testu e-learningowego pod warunkiem uzyskania zaliczenia z ćwiczeń
	4	71-80% ogólnej liczby punktów do zdobycia z egzaminu i testu e-learningowego pod warunkiem uzyskania

		zaliczenia z ćwiczeń
	4,5	81-85% ogólnej liczby punktów do zdobycia z egzaminu i testu e-learningowego pod warunkiem uzyskania zaliczenia z ćwiczeń
	5	Powyżej 85% ogólnej liczby punktów do zdobycia z egzaminu i testu e-learningowego pod warunkiem uzyskania zaliczenia z ćwiczeń
Ćwiczenia (C) *	3	50-65% ogólnej liczby punktów do zdobycia za kolokwium zaliczeniowe oraz aktywność studenta na 50-65% zajęć
	3,5	66-70% ogólnej liczby punktów do zdobycia za kolokwium zaliczeniowe oraz aktywność studenta na 66-70% zajęć
	4	71-80% ogólnej liczby punktów do zdobycia za kolokwium zaliczeniowe oraz aktywność studenta na 71-80% zajęć
	4,5	81-85% ogólnej liczby punktów do zdobycia za kolokwium zaliczeniowe oraz aktywność studenta na 81-85% zajęć
	5	Powyżej 85% ogólnej liczby punktów do zdobycia za kolokwium zaliczeniowe oraz aktywność studenta na więcej niż 85% zajęć

5. BILANS PUNKTÓW ECTS – NAKŁAD PRACY STUDENTA

Kategoria	Obciążenie studenta	
	Studia stacjonarne	Studia niestacjonarne
LICZBA GODZIN REALIZOWANYCH PRZY BEZPOŚREDNIM UDZIALE NAUCZYCIELA /GODZINY KONTAKTOWE/	60	40
Udział w wykładach	20	20
Udział w ćwiczeniach	28	18
Udział w egzaminie/kolokwium zaliczeniowym*	2	2
Inne (udział w zajęciach e-learningu) *	10	-
SAMODZIELNA PRACA STUDENTA /GODZINY NIEKONTAKTOWE/	90	110
Przygotowanie do wykładu	20	20
Przygotowanie do ćwiczeń	50	70
Przygotowanie do egzaminu/kolokwium*	20	20
ŁĄCZNA LICZBA GODZIN	150	150
PUNKTY ECTS za przedmiot	6	6

*niepotrzebne usunąć

Przyjmuję do realizacji (data i czytelne podpisy osób prowadzących przedmiot w danym roku akademickim)

.....