KARTA KURSU

Nazwa	**Teoria organizacji i zarządzania**
Nazwa w j. ang.	Organisation and Management Theory

Koordynator	prof. dr hab. inż. Mikołaj Karpiński	Zespół dydaktyczny
		prof. dr hab. inż. Mikołaj Karpiński
Punktacja ECTS*	Studia stacjonarne:2 Studia niestacjonarne: 2	

Opis kursu (cele kształcenia)

Celem kursu jest wprowadzenie studenta we współczesne problemy organizacji i zarządzania, ze szczególnym uwzględnieniem zagadnień cyberbezpieczeństwa. Student poznaje wytyczne zawarte w narodowych dokumentach, także w międzynarodowych normach i standardach.

Warunki wstępne

Wiedza	Wiedza w zakresie powszechnym, na poziomie szkoły średniej; znajomość wybranych zagadnień matematyki wyższej, aplikacji internetowych i technologii sieciowych.
Umiejętności	-
Kursy	-

Efekty uczenia się

	Efekt uczenia się dla kursu	Odniesienie do efektów kierunkowych
Wiedza	W01: zna teoretyczne podstawy organizacji i zarządzania z naciskiem na cyberbezpieczeństwo.	K_W02, K_W06
	W02: ma wiedzę w zakresie wymagań stawianych przez normy i standardy do zarządzania cyberbezpieczeństwem.	K_W07
	W03: zna politykę cyberbezpieczeństwa informacji.	K_W08, K_W09
	W04: ma wiedzę w zakresie w zakresie budowy systemów zarządzania bezpieczeństwem informacji.	K_W06, K_W10

	Efekt uczenia się dla kursu	Odniesienie do efektów kierunkowych
Umiejętności	U01: student potrafi swobodnie operować pojęciami nabytymi w trakcie trwania kursu.	K_U05
	U02: student swobodnie potrafi ułożyć zdobyte informacje w ciąg przyczynowo-skutkowy.	K_U09
	U03: student na podstawie nabytych informacji potrafi wskazać mechanizmy istniejące w omawianej na kursie dziedzinie wiedzy.	K_U11
	U04: potrafi korzystać z źródeł dotyczących omawianej tematyki.	K_U13

	Efekt uczenia się dla kursu	Odniesienie do efektów kierunkowych
Kompetencje społeczne	K01: student potrafi w zrozumiały sposób przekazywać nabytą na kursie wiedzę.	K_K01
	K02: student w trakcie dyskusji uczy argumentacji i obrony własnego stanowiska.	K_K02
	K03: student potrafi samodzielnie uzupełniać nabytą w trakcie kursu wiedzę, korzystając zarówno z literatury, jak i źródeł internetowych.	K_K02, K_K03

Studia stacjonarne

Organizacja											
Forma zajęć	Wykład (W)	Ćwiczenia w grupach									
		A		K		L		S		P		E	
Liczba godzin	15	15											

Studia niestacjonarne

Organizacja											
Forma zajęć	Wykład (W)	Ćwiczenia w grupach									
		A		K		L		S		P		E	
Liczba godzin	10	10											

Opis metod prowadzenia zajęć

studia stacjonarne (dopuszcza się realizację zajęć z zastosowaniem i technik kształcenia na odległość) Wykład prowadzony w sposób klasyczny, wspomagany metodami audiowizualnymi (w tym filmami dokumentalnymi) i multimedialnymi. Ćwiczenia: - dyskusja dydaktyczna, prezentacje poszczególnych tematów przez studentów - słowne objaśnienie - prezentacja przygotowana przez studentów studia niestacjonarne (dopuszcza się realizację zajęć z zastosowaniem metod i technik kształcenia na odległość) Wykład prowadzony w sposób klasyczny, wspomagany metodami audiowizualnymi (np. filmami dokumentalnymi) i multimedialnymi. Ćwiczenia: - dyskusja dydaktyczna, prezentacje poszczególnych tematów przez studentów - słowne objaśnienie - prezentacja przygotowana przez studentów

Formy sprawdzania efektów uczenia się

	E – learning	Gry dydaktyczne	Ćwiczenia w szkole	Zajęcia terenowe	Praca laboratoryjna	Projekt indywidualny	Projekt grupowy	Udział w dyskusji	Referat	Praca pisemna (esej)	Egzamin ustny	Egzamin pisemny	Inne
W01								X					
W02								X					
W03							X	X					
W04							X	X					
U01							X	X					
U02							X	X					
U03							X	X					
U04							X						
K01							X	X					
K02							X	X					
K03							X						

Kryteria oceny	Dopuszcza się przeprowadzenie zaliczenia z zastosowaniem metod i technik kształcenia na odległość. Obecność na zajęciach, aktywność (zadawanie pytań/udzielanie odpowiedzi ustnej w trakcie wykładu i podczas dyskusji dydaktycznej kierowanej na omawiany temat), systematyczność w wykonaniu ćwiczeń udokumentowane sprawozdaniem oraz uzyskanie pozytywnej oceny końcowej – średniej ocen formujących.

Uwagi	

Treści merytoryczne (wykaz tematów)

1. Teoretyczne podstawy organizacji i zarządzania pod kątem cyberbezpieczeństwa oraz odpowiednich standardów.
2. Zarządzanie incydentami związanymi z bezpieczeństwem informacji.
3. Koncepcja typu ITIL (Information Technology Infrastructure Library).
4. Reagowanie na incydenty na przykładzie CERT / CSIRT
5. Zasady gromadzenia informacji dla systemu wykrywania i blokowania ataków.
6. Polityka cyberbezpieczeństwa informacji.
7. Systemy zarządzania bezpieczeństwem informacji.

Wykaz literatury podstawowej

1. Banasiński Cezary. Cyberbezpieczeństwo. Zarys wykładu. Wydanie 2. – Warszawa: Wolters Kluwer, 2023. – 588 s.
2. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii.
3. Lachiewicz Stefan, Matejun Marek. Ewolucja nauk o zarządzaniu. [w:] Zakrzewska-Bielawska A. (red.), Podstawy zarządzania. – Warszawa: Oficyna a Wolters Kluwer business, 2012. – S. 85-141. [Online]. Dostęp: https://www.matejun.com/pubs-pl/2012_Lachiewicz_Matejun_Ewolucja_nauk_o_zarzadzaniu.pdf ; www.matejun.pl
4. Podstawy organizacji i zarządzania. Adam Stabryła (red.). Kraków: Wydawnictwo Uniwersytetu Ekonomicznego, 2012. – 508 s.
5. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

Wykaz literatury uzupełniającej

1. Center for Internet Security: CIS Critical Security Controls. [Online]. Dostęp: https://www.cisecurity.org/controls
2. Gus Khawaja. Kali Linux i testy penetracyjne. Biblia. – Gliwice: Helion, 2022. – 472 s.
3. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection: Information security management systems – Requirements. [Online]. Dostęp: https://www.iso.org/standard/27001
4. ITIL® 4: the framework for the management of IT-enabled services. [Online]. Dostęp: https://www.axelos.com/certifications/itil-service-management
5. Karpiński Mikołaj. Bezpieczeństwo informacji. – Warszawa: Wydawnictwo Pomiary Automatyka Kontrola. – 2012. – 280 s. – ISBN 978-83-930505-3-6.
6. NIST Cybersecurity Framework. [Online]. Dostęp: https://www.nist.gov/cyberframework ; https://stinet.pl/nist-cybersecurity-framework-przedstawienie-postaci/
7. Petrov O., Borowik B., Karpinskyy M., Korchenko O., Lakhno V. Immune and defensive corporate systems with intellectual identification of threats. – Pszczyna: Śląska Oficyna Drukarska. – 2016. – 222 p.
8. Vijay Kumar Velu. Kali Linux i zaawansowane testy penetracyjne. Zostań ekspertem cyberbezpieczeństwa za pomocą Metasploit, Nmap, Wireshark i Burp Suite. Wydanie IV. – Gliwice: Helion, 2023. – 520 s.
9. Zarządzanie ryzykiem - przegląd wybranych metodyk. Praca zbiorowa pod redakcją bryg. dr. inż. Dariusza Wróblewskiego. – Józefów: CNBOP-PIB, 2015. – 480 s.

Bilans godzinowy zgodny z CNPS (Całkowity Nakład Pracy Studenta) **studia stacjonarne**

liczba godzin w kontakcie z prowadzącymi	Wykład	15
	Konwersatorium (ćwiczenia, laboratorium itd.)	15
	Pozostałe godziny kontaktu studenta z prowadzącym	5
liczba godzin pracy studenta bez kontaktu z prowadzącymi	Lektura w ramach przygotowania do zajęć	5
	Opracowanie zadań domowych (problemowych) po zapoznaniu się z niezbędną literaturą przedmiotu	5
	Przygotowanie projektu (praca indywidualna lub w grupie)	5
	Przygotowanie do egzaminu/zaliczenia	
Ogółem bilans czasu pracy		50
Liczba punktów ECTS w zależności od przyjętego przelicznika		2

Bilans godzinowy zgodny z CNPS (Całkowity Nakład Pracy Studenta) **studia niestacjonarne**

liczba godzin w kontakcie z prowadzącymi	Wykład	10
	Konwersatorium (ćwiczenia, laboratorium itd.)	10
	Pozostałe godziny kontaktu studenta z prowadzącym	5
liczba godzin pracy studenta bez kontaktu z prowadzącymi	Lektura w ramach przygotowania do zajęć	10
	Opracowanie zadań domowych (problemowych) po zapoznaniu się z niezbędną literaturą przedmiotu	10
	Przygotowanie projektu (praca indywidualna lub w grupie)	5
	Przygotowanie do egzaminu/zaliczenia	
Ogółem bilans czasu pracy		50
Liczba punktów ECTS w zależności od przyjętego przelicznika		2