Załącznik nr 1.5 do Zarządzenia Rektora UR nr 12/2019

SYLABUS

DOTYCZY CYKLU KSZTAŁCENIA 2020/2021 – 2021/2022

(skrajne daty)

Rok akademicki 2021/2022

1. PODSTAWOWE INFORMACJE O PRZEDMIOCIE

Nazwa przedmiotu	**Bezpieczeństwo systemów mechatronicznych i informatycznych**
Kod przedmiotu*	
Nazwa jednostki prowadzącej kierunek	Kolegium Nauk Przyrodniczych
Nazwa jednostki realizującej przedmiot	Kolegium Nauk Przyrodniczych
Kierunek studiów	Mechatronika
Poziom studiów	Studia II-go stopnia
Profil	Ogólnoakademicki
Forma studiów	Studia stacjonarne
Rok i semestr/y studiów	Rok II, semestr 3
Rodzaj przedmiotu	Przedmiot kierunkowy
Język wykładowy	Polski
Koordynator	prof. dr hab. Yaroslav Bobytskyy
Imię i nazwisko osoby prowadzącej / osób prowadzących	prof. dr hab. Yaroslav Bobytskyy

***** *-opcjonalnie, zgodnie z ustaleniami w Jednostce*

1.1.Formy zajęć dydaktycznych, wymiar godzin i punktów ECTS

Semestr (nr)	Wykł.	Ćw.	Konw.	Lab.	Sem.	ZP	Prakt.	Inne (jakie?)	**Liczba pkt. ECTS**
3	15			15					2

1.2. Sposób realizacji zajęć

☒ zajęcia w formie tradycyjnej

☐ zajęcia realizowane z wykorzystaniem metod i technik kształcenia na odległość

1.3 Forma zaliczenia przedmiotu (z toku) (egzamin, zaliczenie z oceną, zaliczenie bez oceny)

Wykład – zaliczenie bez oceny

Ćwiczenia laboratoryjne – zaliczenie z oceną

2.WYMAGANIA WSTĘPNE

Sieci komunikacyjne i systemy telemetryczne, projektowanie układów mechatronicznych, normalizacja w automatyce, sterowniki programowalne.

3. CELE, EFEKTY UCZENIA SIĘ, TREŚCI PROGRAMOWE I STOSOWANE METODY DYDAKTYCZNE

3.1 Cele przedmiotu

C1	Poznanie pojęć z zakresu podstawowych zjawisk fizycznych zachodzących podczas zakłóceń w pracy systemów zasilania, podstawowe awarie, nabranie umiejętności projektowania bezpiecznego systemu mechatronicznego w kontekście polityki bezpieczeństwa.
C2	Zapoznanie z mechanizmami działania podstawowych protokołów sieciowych wykorzystywanych w systemach mechatronicznych oraz urządzeń sieciowych w kontekście bezpieczeństwa na różnych poziomach warstw sieciowych.
C3	Przyswojenie umiejętności w zakresie analizy podstawowych problemów jakości energii elektrycznej, normy, standardy i dyrektywy bezpieczeństwa, przyczyny złej jakości energii elektrycznej, analiza metod poprawy jakości energii, ocena wskaźników jakościowych.

3.2 Efekty uczenia się dla przedmiotu

EK (efekt uczenia się)	Treść efektu uczenia się zdefiniowanego dla przedmiotu Student:	Odniesienie do efektów kierunkowych [1]
EK_01	zna podstawy na temat pracy sieci i instalacji elektrycznych, potrafi dobrać odpowiednie systemy zabezpieczeń, ocenia niezawodność maszyn i urządzeń w kontekście bezpieczeństwa systemów mechatronicznych oraz zasad ich projektowania.	K_W07
EK_02	potrafi określić zagrożenia pracy sieci i systemów informatycznych sterujących systemami mechatronicznymi, a także wymagania stawiane współczesnym systemom mechatronicznym w kontekście bezpieczeństwa.	K_U04
EK_03	ma świadomość wagi współczesnych systemów mechatronicznych oraz zagrożeń wynikających z jego pracy, jest otwarty na nowości techniczne z obszaru IT.	K_K01

3.3 Treści programowe

A. Problematyka wykładu

Treści merytoryczne
Omówienie tematyki przedmiotu, literatury, form i zasad zaliczenia.
Integracja inżynierii bezpieczeństwa w systemach mechatronicznych.
Podstawowe zagadnienia związane z ochroną systemów mechatronicznych, podstawowe akty prawne, normy i dyrektywy dotyczące bezpieczeństwa systemów mechatronicznych.
Rozumienie hierarchię kontroli dla skutecznego zapobiegania zagrożeniom.

[1] W przypadku ścieżki kształcenia prowadzącej do uzyskania kwalifikacji nauczycielskich uwzględnić również efekty uczenia się ze standardów kształcenia przygotowującego do wykonywania zawodu nauczyciela.

Projektowanie i budowa systemów zabezpieczających maszyn i urządzeń, ocena ryzyka. Bezpieczeństwo zasilania systemów informatycznych i mechatronicznych.
Podział zakłóceń, rodzaje zagrożeń występujących w systemach zasilających, budowa urządzeń zabezpieczających. Monitorowanie parametrów systemów zasilających. Zasady pomiarów parametrów i urządzenia pomiarowe.
Niezawodność układów zasilania w kontekście systemów mechatronicznych.
Bezpieczeństwo podstawowych protokołów i urządzeń sieciowych stosowanych w systemach IT, filozofia działania podstawowych ataków sieciowych - ataki na dostępność, poufność i integralność danych, skanowanie, podsłuch, podszywanie.
Podsumowanie, utrwalenie poznanych wiadomości.

B. Problematyka ćwiczeń laboratoryjnych

Treści merytoryczne
Omówienie tematyki przedmiotu, literatury, form i zasad zaliczenia.
Planowanie i zapewnienie niezawodności w nadzorowanych procesach eksploatacji urządzeń mechatronicznych z uwzględnieniem podstawowych wskaźników eksploatacji urządzeń w cyklu ich życia.
Badania diagnostyczne w urządzeniach mechatronicznych. Klasyfikacja symptomów diagnostycznych stanu technicznego urządzeń. Pomiary termowizyjne i szybkozmienne.
Limitowanie dostępu do systemów komputerowych i do danych; sterowanie uprawnieniami użytkownika; identyfikacja, autentykacja i autoryzacja, rozwiązania dla identyfikacji i autentykacji użytkowników.
Typowe zagrożenia, ataki na sieci i ich wykrywanie, metody unikania i przeciwdziałania; reagowanie na naruszenia bezpieczeństwa i poprawności funkcjonowania sieci.
Podpis elektroniczny i certyfikacja, autentykacja usługodawców, certyfikacja serwerów, bezpieczna poczta elektroniczna; infrastruktura PKI i środki techniczne, niezbędne dla jej budowy, właściwości sprzętowych modułów kryptograficznych.
Podsumowanie, utrwalenie poznanych wiadomości. Zaliczenie.

3.4 Metody dydaktyczne

Wykład: wykład z prezentacją multimedialną, analiza przypadków, dyskusja.
Ćwiczenia laboratoryjne ukierunkowane na samodzielne rozwiązywanie problemów dotyczących zabezpieczeń systemów sterowania i automatyki z wykorzystaniem dostępnych stanowisk sterowników przemysłowych.

4. METODY I KRYTERIA OCENY

4.1 Sposoby weryfikacji efektów uczenia się

Symbol efektu	Metody oceny efektów uczenia się (np.: kolokwium, egzamin ustny, egzamin pisemny, projekt, sprawozdanie, obserwacja w trakcie zajęć)	Forma zajęć dydaktycznych (w, ćw, ...)
EK_ 01	Rozmowa oceniająca	wykład
EK_ 02	Odpytywanie, obserwacja w trakcie zajęć, sprawozdanie	lab.
EK_ 03	Obserwacja w trakcie zajęć	wykład, lab.

4.2 Warunki zaliczenia przedmiotu (kryteria oceniania)

Wykład (zaliczenie bez oceny): rozmowa oceniająca. Warunkiem dopuszczenia do rozmowy oceniającej jest uzyskanie pozytywnej oceny z ćwiczeń laboratoryjnych. Student w trakcie rozmowy oceniającej powinien wykazać się znajomością problematyki poruszanej na wykładzie w stopniu co najmniej podstawowym, aby uzyskać zaliczenie przedmiotu. **Laboratorium** (zaliczenie z oceną): Ocena końcowa stanowi średnią ocen z odpytywania studentów podczas realizacji określonych zadań problemowych oraz oceny ze sprawozdania obrazującego poziom zrealizowanych ćwiczeń.

5. CAŁKOWITY NAKŁAD PRACY STUDENTA POTRZEBNY DO OSIĄGNIĘCIA ZAŁOŻONYCH EFEKTÓW W GODZINACH ORAZ PUNKTACH ECTS

Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe wynikające z harmonogramu studiów	30
Inne z udziałem nauczyciela akademickiego (udział w konsultacjach, egzaminie)	4
Godziny nie kontaktowe – praca własna studenta (przygotowanie do zajęć, egzaminu, napisanie referatu itp.)	18
SUMA GODZIN	52
SUMARYCZNA LICZBA PUNKTÓW ECTS	**2**

** Należy uwzględnić, że 1 pkt ECTS odpowiada 25-30 godzin całkowitego nakładu pracy studenta.*

6. PRAKTYKI ZAWODOWE W RAMACH PRZEDMIOTU

wymiar godzinowy	---
zasady i formy odbywania praktyk	---

7. LITERATURA

Literatura podstawowa:

[1] Markowski A. (red): Zapobieganie stratom w przemyśle. Cz. II i III – Zarządzanie bezpieczeństwem procesowym. Wyd. Politechniki Łódzkiej, Łódź 1999.

[2] Pikowicz W.: Inżynieria bezpieczeństwa technicznego. Problematyka Podstawowa. WNT 2009.

[3] William Stallings, Lawrie Brown. Bezpieczeństwo systemów informatycznych. Zasady i praktyka. Wydanie IV. Tom 1, (ebook), HELION s.a.,2019.

[4] William Stallings, Lawrie Brown. Bezpieczeństwo systemów informatycznych. Zasady i praktyka. Wydanie IV. Tom 2, (ebook), HELION s.a. 2019.

[5] William Stallings: Kryptografia i bezpieczeństwo sieci komputerowych: koncepcje i metody bezpiecznej komunikacji. Gliwice: Wydawnictwo Helion, 2012.

[6] Bodo Heimann, Wilfried Gerth, Karl Popp: Mechatronika: komponenty, metody, przykłady. Przekł. Z niem. Marek Gawrysiak. Warszawa, Wydaw. Naukowe PWN, 2001.

[7] Kacejko P., Machowski J.: Zwarcia w systemach elektroenergetycznych. WNT, Warszawa, 2002.

[8] R. Kowalik, M. Januszewski, A Smolarczyk: Cyfrowa elektroenergetyczna automatyka zabezpieczeniowa. Oficyna Wydawnicza Politechniki Warszawskiej. Warszawa, 2006.

Literatura uzupełniająca:

[1] Niziński S.: Eksploatacja obiektów technicznych. ITE, Radom 2002.

[2] Wendell Odom, Tom Knott: Przekładnie Z ang. Stanisław piech. - Warszawa: Wydaw. Naukowe PWN, 2007.

[3] Jerzy Tchórzewski: Badanie prawidłowości rozwoju systemów elektroenergetycznych: sztuczne życie elektroenergetycznej sieci przesyłowej. Siedlce, Wydawnictwo AP, 2000.

[4] Cyberprzestępczość: jak walczyć z łamaniem prawa w sieci: przygotuj się do walki z cyberprzestępczością / DEBRA LITTLEJOHN SHINDER, ED TITTEL RED. TECHNICZNY - GLIWICE: "HELION", 2004.

[5] Joel Scambray, Stuart Mcclure, George Kurtz: Hakerzy - cała prawda: sekrety zabezpieczeń sieci komputerowych. - WARSZAWA: "TRANSLATOR", 2001.

[6] Poradnik mechatronika / oprac. Merytoryczne wersji polskiej - Joachim Potrykus. Warszawa, Wydawnictwo Rea, 2013.

Akceptacja Kierownika Jednostki lub osoby upoważnionej