Tabela opisu efektów uczenia się studiów podyplomowych

Politechnika Krakowska im. Tadeusza Kościuszki w Krakowie

Nazwa jednostki/jednostek organizacyjnych prowadzących studia wraz z symbolem jednostki/jednostek: Wydział Inżynierii Elektrycznej i Komputerowej E-0
Nazwa jednostki wiodącej Wydział Inżynierii Elektrycznej i Komputerowej E-0
Nazwa studiów podyplomowych Bezpieczeństwo infrastruktury krytycznej i kluczowej w zakresie systemów przemysłowych Operational Technology (OT)

Dziedzina lub dziedziny nauki/~~sztuki~~[1]: Dziedzina nauk inżynieryjno-technicznych (100%)

Poziom Polskiej Ramy Kwalifikacji[2] 6 PRK

Symbole efektów uczenia się	KIERUNKOWE EFEKTY UCZENIA SIĘ STUDIÓW PODYPLOMOWYCH	Odniesienie do		
		uniwersalnych charakterystyk pierwszego stopnia PRK[3]	charakterystyk drugiego stopnia efektów uczenia się dla kwalifikacji na poziomach 6-8 PRK typowych dla kwalifikacji uzyskiwanych w ramach systemu szkolnictwa wyższego i nauki po uzyskaniu kwalifikacji pełnej na poziomie 4[4]	charakterystyk drugiego stopnia PRK typowych dla kwalifikacji o charakterze zawodowym – poziomy 6-8[5]
1	2	3	4	5
	WIEDZA: ABSOLWENT ZNA I ROZUMIE	**Kod składnika opisu**	**Kod składnika opisu**	**Kod składnika opisu**
COT_W01	pojęcia dotyczące bezpieczeństwa informacji (danych) oraz sieci komputerowych	P6U_W	P6S_WG	P6Z_WT
COT_W02	zaawansowane mechanizmy oraz algorytmy zabezpieczania informacji cyfrowych	P6U_W	P6S_WG	P6Z_WT
COT_W03	problemy bezpiecznej komunikacji poprzez publiczne kanały wymiany informacji	P6U_W	P6S_WG	P6Z_WO
COT_W04	wybrane typy zagrożeń i ataków na systemy i sieci	P6U_W	P6S_WG	P6Z_WZ
COT_W05	protokoły transmisji w sieciach oraz tworzenie prywatnych sieci VPN	P6U_W	P6S_WG	P6Z_WT
COT_W06	zaawansowane mechanizmy zabezpieczeń wybranych systemów	P6U_W	P6S_WG	P6Z_WT
COT_W07	metodyki, techniki i narzędzia niezbędne do implementacji skryptów	P6U_W	P6S_WG	P6Z_WZ
COT_W08	zasady tworzenia i wykorzystania polityki bezpieczeństwa	P6U_W	P6S_WG	P6Z_WO

COT_W09	wybrane metody przeprowadzania testów penetracyjnych	P6U_W	P6S_WG	P6Z_WZ
COT_W10	wybrane narzędzia administratora systemów i sieci SIEM, SOAR, SOC	P6U_W	P6S_WG	P6Z_WN
	UMIEJĘTNOŚCI: ABSOLWENT POTRAFI	**Kod składnika opisu**	**Kod składnika opisu**	**Kod składnika opisu**
COT_U01	wybrać oraz wykorzystać odpowiednie mechanizmy ochrony informacji cyfrowych w kontekście określonego problemu	P6U_U	P6S_UW	P6Z_UO
COT_U02	skonfigurować i zabezpieczyć system operacyjny pod kątem prywatnych sieci VPN	P6U_U	P6S_UW	P6Z_UU
COT_U03	przeprowadzić analizę ruchu w sieciach przemysłowych OT	P6U_U	P6S_UW	P6Z_UI
COT_U04	skonfigurować wybrane usługi w systemach i sieciach OT	P6U_U	P6S_UW	P6Z_UU
COT_U05	implementować skrypty powłoki systemów operacyjnych	P6U_U	P6S_UW	P6Z_UI
COT_U06	przygotować dokumentację techniczną zrealizowanych rozwiązań	P6U_U	P6S_UW	P6Z_UO
COT_U07	wykonać analizę bezpieczeństwa środowiska OT	P6U_U	P6S_UW	P6Z_UI
COT_U08	wykrywać popularne ataki na systemy i sieci oraz odpowiednio zareagować na zaistniały incydent	P6U_U	P6S_UW	P6Z_UO
COT_U09	używać wybranych narzędzi administratora systemów i sieci IPS/IDS	P6U_U	P6S_UW	P6Z_UN
COT_U10	przeprowadzać testy penetracyjne	P6U_U	P6S_UW	P6Z_UN
	KOMPETENCJE SPOŁECZNE: ABSOLWENT JEST GOTÓW DO	**Kod składnika opisu**	**Kod składnika opisu**	**Kod składnika opisu**
COT_K01	kierowania się w swojej pracy profesjonalizmem i etyką zawodową	P6U_K	P6S_KK	P6Z_KO P6Z_KP
COT_K02	realizacji swoich działań z uwzględnieniem aspektów ekonomicznych	P6U_K	P6S_KK	P6Z_KW P6Z_KP

Objaśnienia używanych symboli:

SP = symbol studiów podyplomowych
01, 02, 03 i kolejne = numer efektu uczenia się
W = wiedza
U = umiejętności
K = kompetencje społeczne
Przykłady: **SP_W01**, **SP_U01**, **SP_K01**

1. Uniwersalne charakterystyki poziomów 6-8 PRK pierwszego stopnia:

P = poziom PRK (6, 7, 8)
U = charakterystyka uniwersalna
W = wiedza
U = umiejętności

K = kompetencje społeczne
Przykłady: **P6U_W**, **P7U_W**

2. Charakterystyki drugiego stopnia efektów uczenia się dla kwalifikacji na poziomach 6-8 PRK typowe dla kwalifikacji uzyskiwanych w ramach szkolnictwa wyższego i nauki po uzyskaniu kwalifikacji pełnej na poziomie 4:

P = poziom PRK (6, 7, 8)
S = charakterystyka typowa dla kwalifikacji uzyskiwanych w ramach szkolnictwa wyższego

W = wiedza	**U = umiejętności**	**K = kompetencje społeczne**
G = głębia i zakres	W = wykorzystanie wiedzy	K = krytyczna ocena
K = kontekst	K = komunikowanie się	O = odpowiedzialność
	O = organizacja pracy	R = rola zawodowa
	U = uczenie się	

Przykłady: **P6S_WG**, **P7S_WG**

3. Charakterystyki drugiego stopnia PRK typowe dla kwalifikacji o charakterze zawodowym – poziomy 6-8:

P = poziom PRK (6, 7, 8)
Z = charakterystyka typowa dla kwalifikacji uzyskiwanych w ramach kształcenia i szkolenia zawodowego

W = wiedza	**U = umiejętności**	**K = kompetencje społeczne**
T = teorie i zasady	I = informacje	P = przestrzeganie reguł
Z = zjawiska i procesy	O = organizacja pracy	W = współpraca
O = organizacja pracy	N = narzędzia i materiały	O = odpowiedzialność
N = narzędzia i materiały	U = uczenie się i rozwój zawodowy	

Przykłady:
P6Z_UO,
P7Z_K

---

[1] W przypadku więcej niż jednej dziedziny nauki/sztuki należy wpisać wszystkie, zgodnie z rozporządzeniem Ministra Nauki i Szkolnictwa Wyższego z dnia 20 września 2018 r. w sprawie dziedzin nauki i dyscyplin naukowych oraz dyscyplin artystycznych (Dz.U. 2018 r. poz. 1818).
[2] Należy podać właściwy poziom Polskiej Ramy Kwalifikacji, zgodnie z ustawą z dnia 22 grudnia 2015 r. o Zintegrowanym Systemie Kwalifikacji (Dz.U. z.2020 r. poz. 226).
[3] Opis zakładanych efektów uczenia się dla kierunku studiów wyższych, poziomu i profilu kształcenia uwzględnia wszystkie uniwersalne charakterystyki pierwszego stopnia określone w ustawie z dnia 22 grudnia 2015 r. o Zintegrowanym Systemie Kwalifikacji, właściwe dla danego poziomu Polskiej Ramy Kwalifikacji.
[4] Charakterystyki drugiego stopnia efektów uczenia się dla kwalifikacji na poziomie 6-8 PRK typowe dla kwalifikacji uzyskiwanych w ramach szkolnictwa wyższego i nauki po uzyskaniu kwalifikacji pełnej na poziomie 4, określone w rozporządzeniu Ministra Nauki i Szkolnictwa Wyższego z dnia 14 listopada 2018 r. w sprawie charakterystyk drugiego stopnia efektów uczenia się dla kwalifikacji na poziomach 6-8 Polskiej Ramy Kwalifikacji (Dz.U. 2018 r. poz. 2218).
[5] Charakterystyki drugiego stopnia Polskiej Ramy Kwalifikacji typowych dla kwalifikacji o charakterze zawodowym – poziomy 6-8 określone w rozporządzeniu Ministra Edukacji Narodowej z dnia 13 kwietnia 2016 r. w sprawie charakterystyk drugiego stopnia Polskiej Ramy Kwalifikacji typowych dla kwalifikacji o charakterze zawodowym – poziomy 1-8 (Dz.U. 2016 r. poz. 537).

PLAN STUDIÓW PODYPLOMOWYCH
Bezpieczeństwo infrastruktury krytycznej i kluczowej w zakresie systemów przemysłowych Operational Technology (OT)
Wydział Inżynierii Elektrycznej i Komputerowej E-0
0688 - Interdyscyplinarne programy i kwalifikacje obejmujące technologie informacyjno-komunikacyjne

Obowiązuje od roku akademickiego 2023/2024

Lp.	Nazwa przedmiotu	RAZEM									semestry															
											I								II							
		Liczba godzin RAZEM	W	C	L	K	P	S	ECTS	E/Z	W	C	L	K	P	S	ECTS	E/Z	W	C	L	K	P	S	ECTS	E/Z
1	Bezpieczeństwo infrastruktury krytycznej i kluczowej	15	15			0			2	Z	15			0			2	Z								
2	Systemy energetyczne, systemy ppoż oraz ochrona pporażeniowa w systemach OT	20	15			5			2	Z	15			5			2	Z								
3	Systemy i układy sterowania procesowego - dobór, konfiguracja i administracja	15				15			2	Z				15			2	Z								
4	Zagrożenia w obszarze cyberbezpieczeństwa sieci i systemów OT	15	15						2	Z	15						2	Z								
5	Zarządzanie bezpieczeństwem informacji - SZBI	20	15			5			3	E	15			5			3	E								
6	Projektowanie, budowa, konfiguracja i administrowanie przemysłowych sieci OT	40	10			30			5	Z	5			15					5			15			5	Z
7	Tworzenie, administracja i konfiguracja wirtualnych prywatnych sieci VPN	10	5			5			2	Z									5			5			2	Z
8	SIEM, SOAR, SOC - dobór, konfiguracja i administracja. Audyt systemów OT	30	10			20			4	Z									10			20			4	Z
9	Przemysłowe systemy IPS/IDS – dobór, konfiguracja i administracja	30	10			20			4	Z									10			20			4	Z
10	Platforma softwerowo-sprzętowa systemów przemysłowych OT - egzamin końcowy*	30				30			4	E												30			4	E
	Ogółem	225	95	0	0	130	0	0	30		65	0	0	40	0	0	11		30	0	0	90	0	0	19	
	Liczba egzaminów/zaliczeń	2/8																								

Legenda: W - wykłady, C - ćwiczenia, L - laboratoria, K - laboratoria komputerowe, P - projekty, S - seminaria, E - egzamin, Z - zaliczenie przedmiotu

* Platforma softwerowo-sprzetowa systemów przemysłowych OT - zajęcia z egzaminem końcowym sprawdzającym zagadnienia omawiane również podczas pozostałych zajęć.
Egzamin kończący się uzyskaniem certyfikatu cyberbezpieczeństwa, wymagane 70% poprawnych rozwiązań zadań praktycznych

.....
kierownik studiów podyplomowych

.....
kierownik jednostki organizacyjnej PK/
przewodniczący rady programowej studiów

.....
Pełnomocnik Rektora Politechniki Krakowskiej
ds. Kształcenia

Politechnika Krakowska im. Tadeusza Kościuszki

Karta przedmiotu

Obowiązuje uczestników rozpoczynających studia podyplomowe w roku akademickim 2023/2024
Nazwa studiów podyplomowych: Bezpieczeństwo infrastruktury krytycznej i kluczowej w zakresie systemów przemysłowych Operational Technology (OT)
Nazwa jednostki/jednostek organizacyjnych prowadzących studia wraz z symbolem jednostki/jednostek: Wydział Inżynierii Elektrycznej i Komputerowej E-0
Nazwa jednostki wiodącej Wydział Inżynierii Elektrycznej i Komputerowej E-0
Kod i nazwa studiów podyplomowych według klasyfikacji ISCED 0688 - Interdyscyplinarne programy i kwalifikacje obejmujące technologie informacyjno-komunikacyjne

Nazwa przedmiotu w języku polskim	Bezpieczeństwo infrastruktury krytycznej i kluczowej
Nazwa przedmiotu w języku angielskim	Critical infrastructure and cyber security
Kategoria przedmiotu	specjalnościowy
Liczba punktów ECTS	2
Semestry	I
Język wykładowy	Polski

Wymagania wstępne: Znajomość podstawowa systemów sieciowych i infrastruktury systemów sterowania,
Zagrożenia w obszarze cyberbezpieczeństwa i bezpieczeństwa infrastruktury krytycznej,

Cele przedmiotu: Celem przedmiotu jest nabycie wiedzy i umiejętności w zakresie podstawowych zasad obowiązujących w Polsce oraz UE w zakresie bezpieczeństwa infrastruktury krytycznej i kluczowej.

Efekty uczenia się:
EU1: zna systemy i infrastrukturę na, na które są narażone (COT_W01, COT_W02, COT_W03, COT_W04, COT_W5, COT_W6, COT_W7, COT_W8, COT_W9).
EU2: potrafi identyfikować zagrożenia (COT_U02, COT_U09).
EU3: potrafi wykrywać i analizować zagrożenia poprzez wprowadzenie zabezpieczeń zapobiegających atakom (COT_U02, COT_U04, COT_U08, COT_U09).
EU4: potrafi dobrać rodzaj i zakres działań naprawczych (COT_U05).
EU5: jest przygotowany do zarządzania i administrowania takimi systemami (COT_K02).

Forma zajęć, semestralna liczba godzin

Semestr	Forma zaliczenia (E/Z)	Wykłady	Ćwiczenia	Laboratorium	Laboratorium komputerowe	Projekt	Seminarium
I	Z	15					

Treści programowe (oddzielnie dla każdej formy zajęć):

Forma zajęć	Tematyka zajęć	Liczba godzin
W	1. Zagadnienia związane z Infrastrukturą krytyczną. 2. Zagadnienia związane z Infrastrukturą kluczową. 3. Krajowy system cyberbezpieczeństwa 4. Omówienie i analiza Ustawy o Krajowym systemie cyberbezpieczeństwa 5. NIS 1 i NIS 2 – omówienie dyrektyw UE w zakresie Cyberbezpieczeństwa. 6. Zasady projektowania i budowy odpornych systemów informatycznych zgodnych z KSC 7. Analiza i obsługa incydentów i podatności.	15

Metody dydaktyczne: wykład problemowy

Sposoby weryfikacji i oceny efektów uczenia się: Wykład: zaliczenie pisemne.

Kryteria oceny: odpowiedzieć poprawnie na minimum 70% pytań na kolokwium z wiadomości przekazywanych na wykładach.

Dodatkowe informacje ustalane przez osobę odpowiedzialną za przedmiot:
Wykaz literatury:
1. Materiały dostarczone przez prowadzącego w formie elektronicznej.
2. Dokumentacja dostępna na stronach Rządowego Centrum Bezpieczeństwa oraz Ministerstwa Cyfryzacji.

Zatwierdzenie karty przedmiotu:

…….	……	……..……
miejscowość, data	osoba odpowiedzialna za przedmiot	kierownik jednostki organizacyjnej PK/ przewodniczący rady programowej studiów

Politechnika Krakowska im. Tadeusza Kościuszki

Karta przedmiotu

Obowiązuje uczestników rozpoczynających studia podyplomowe w roku akademickim 2023/2024
Nazwa studiów podyplomowych: Bezpieczeństwo infrastruktury krytycznej i kluczowej w zakresie systemów przemysłowych Operational Technology (OT)
Nazwa jednostki/jednostek organizacyjnych prowadzących studia wraz z symbolem jednostki/jednostek: Wydział Inżynierii Elektrycznej i Komputerowej E-0
Nazwa jednostki wiodącej Wydział Inżynierii Elektrycznej i Komputerowej E-0
Kod i nazwa studiów podyplomowych według klasyfikacji ISCED 0688 - Interdyscyplinarne programy i kwalifikacje obejmujące technologie informacyjno-komunikacyjne

Nazwa przedmiotu w języku polskim	Systemy energetyczne, systemy ppoż oraz ochrona przeciwporażeniowa w systemach OT
Nazwa przedmiotu w języku angielskim	Energy systems, fire protection systems and electric shock protection in OT systems
Kategoria przedmiotu	specjalnościowy
Liczba punktów ECTS	2
Semestry	I
Język wykładowy	Polski

Wymagania wstępne: Znajomość podstawowa systemów energetycznych, przeciwporażeniowych i przeciwpożarowych,
Zagrożenia systemów energetycznych i ppoż. w obszarze cyberbezpieczeństwa i bezpieczeństwa infrastruktury krytycznej,

Cele przedmiotu: Celem przedmiotu jest nabycie wiedzy i umiejętności w zakresie podstawowych zasad obowiązujących w Polsce oraz UE w zakresie bezpieczeństwa infrastruktury krytycznej i kluczowej.

Efekty uczenia się:
EU1: zna systemy i infrastrukturę energetyczną zasilającą IK, na które są narażone (COT_W01, COT_W02, COT_W03, COT_W04, COT_W5, COT_W6, COT_W7, COT_W8, COT_W9).
EU2: potrafi identyfikować zagrożenia (COT_U02, COT_U09).
EU3: potrafi wykrywać i analizować zagrożenia poprzez wprowadzenie zabezpieczeń zapobiegających atakom na systemy energetyczne i ppoż. (COT_U02, COT_U04, COT_U08, COT_U09).
EU4: potrafi dobrać rodzaj i zakres działań naprawczych (COT_U05).
EU5: jest przygotowany do projektowania, budowy, obsługi i administrowania takimi systemami (COT_K02).

Forma zajęć, semestralna liczba godzin

Semestr	Forma zaliczenia (E/Z)	Wykłady	Ćwiczenia	Laboratorium	Laboratorium komputerowe	Projekt	Seminarium
I	Z	15			5		

Treści programowe (oddzielnie dla każdej formy zajęć):

Forma zajęć	Tematyka zajęć	Liczba godzin
W	1. Zagadnienia związane z systemami energetycznymi stosownymi w zasilaniu Infrastruktury Krytycznej i Kluczowej oraz systemów OT 2. Ochrona przeciwporażeniowa i odgromowa stosowana w zabezpieczeniu systemów przemysłowych OT. 3. Systemy ochrony i zapewnienia ciągłości działania i niezawodności systemów energetycznych. 4. UPS-y, zasilacze buforowe, agregaty prądotwórcze i inne systemu zapewniające ciągłość zasilania systemów OT. 5.Systemy przeciwpożarowe chroniące systemy infrastruktury krytycznej i kluczowej oraz systemy przemysłowe OT.	15

K	1.Projekt oraz budowa modelowego systemu energetycznego zasilającego infrastrukturę krytyczną, kluczową oraz systemy OT. 2. Weryfikacja numeryczna wraz z analizą otrzymanych wyników symulacyjnych. 3. Projekt systemu przeciwpożarowego obiektów technologicznych wyposażonych w systemy przemysłowe OT.	5

Metody dydaktyczne: wykład problemowy, ćwiczenia laboratoryjne

Sposoby weryfikacji i oceny efektów uczenia się: Wykład: zaliczenie pisemne.
Laboratorium komputerowe: ocena wykonywanych zadań praktycznych.

Kryteria oceny: odpowiedzieć poprawnie na minimum 70% pytań na kolokwium z wiadomości przekazywanych na wykładach. Poprawne wykonanie minimum 70% zadań praktycznych

---

Dodatkowe informacje ustalane przez osobę odpowiedzialną za przedmiot:
Wykaz literatury:
1. Materiały dostarczone przez prowadzącego w formie elektronicznej.
2. Dokumentacja dostępna na stronach producentów systemów energetycznych i ppoż.

Zatwierdzenie karty przedmiotu:

…….	……	……..……
miejscowość, data	osoba odpowiedzialna za przedmiot	kierownik jednostki organizacyjnej PK/ przewodniczący rady programowej studiów

Politechnika Krakowska im. Tadeusza Kościuszki

Karta przedmiotu

Obowiązuje uczestników rozpoczynających studia podyplomowe w roku akademickim 2023/2024
Nazwa studiów podyplomowych: Bezpieczeństwo infrastruktury krytycznej i kluczowej w zakresie systemów przemysłowych Operational Technology (OT)
Nazwa jednostki/jednostek organizacyjnych prowadzących studia wraz z symbolem jednostki/jednostek: Wydział Inżynierii Elektrycznej i Komputerowej E-0
Nazwa jednostki wiodącej Wydział Inżynierii Elektrycznej i Komputerowej E-0
Kod i nazwa studiów podyplomowych według klasyfikacji ISCED 0688 - Interdyscyplinarne programy i kwalifikacje obejmujące technologie informacyjno-komunikacyjne

Nazwa przedmiotu w języku polskim	Systemy i układy sterowania procesowego - dobór, konfiguracja i administracja
Nazwa przedmiotu w języku angielskim	Control systems - selection, configuration and administration
Kategoria przedmiotu	specjalnościowy
Liczba punktów ECTS	2
Semestry	I
Język wykładowy	Polski

Wymagania wstępne: Znajomość podstawowa systemów sterowania, wizualizacji procesów technologicznych,
Zagrożenia systemów sterowania i wizualizacji w obszarze cyberbezpieczeństwa i bezpieczeństwa infrastruktury krytycznej,

Cele przedmiotu: Celem przedmiotu jest nabycie wiedzy i umiejętności w zakresie podstawowych zasad obowiązujących w Polsce oraz UE w zakresie bezpieczeństwa infrastruktury krytycznej i kluczowej.

Efekty uczenia się:
EU1: zna systemy i układy sterowania procesowego, systemy SCADA stosowane w IK i systemach OT (COT_W01, COT_W02, COT_W03, COT_W04, COT_W5, COT_W6, COT_W7, COT_W8, COT_W9).
EU2: potrafi identyfikować zagrożenia systemów i układów sterowania. (COT_U02, COT_U09).
EU3: potrafi wykrywać i analizować zagrożenia poprzez wprowadzenie zabezpieczeń zapobiegających atakom na systemy i układy sterowania i systemy Wizualizacyjne (COT_U02, COT_U04, COT_U08, COT_U09).
EU4: potrafi dobrać rodzaj i zakres działań naprawczych (COT_U05).
EU5: jest przygotowany do projektowania, budowy, obsługi i administrowania systemów wirtualnych (COT_K02).

Forma zajęć, semestralna liczba godzin

Semestr	Forma zaliczenia (E/Z)	Wykłady	Ćwiczenia	Laboratorium	Laboratorium komputerowe	Projekt	Seminarium
I	Z				15		

Treści programowe (oddzielnie dla każdej formy zajęć):

Forma zajęć	Tematyka zajęć	Liczba godzin
K	1. Budowa i konfiguracja w systemie symulacyjnym układu sterowania procesem technologicznym. 2. Tworzenie, administracja i zarządzanie systemami wirtualnymi. 3. Budowa i konfiguracja systemu wizualizacyjnego wraz z komunikacją do w/w systemu sterującego. 4. Parametryzacja systemów sterowania i wizualizacji pod kątem ochrony przed cyber zagrożeniami i atakami.	15

Metody dydaktyczne: ćwiczenia laboratoryjne

Laboratorium komputerowe: ocena wykonywanych zadań praktycznych.

Kryteria oceny: Poprawne wykonanie minimum 70% zadań praktycznych

---

Dodatkowe informacje ustalane przez osobę odpowiedzialną za przedmiot:
Wykaz literatury:
1. Materiały dostarczone przez prowadzącego w formie elektronicznej.
2. Dokumentacja programów symulacyjnych użytych w prowadzonych ćwiczeniach.

Zatwierdzenie karty przedmiotu:

…….	……	……..……
miejscowość, data	osoba odpowiedzialna za przedmiot	kierownik jednostki organizacyjnej PK/ przewodniczący rady programowej studiów

Politechnika Krakowska im. Tadeusza Kościuszki

Karta przedmiotu

Obowiązuje uczestników rozpoczynających studia podyplomowe w roku akademickim 2023/2024
Nazwa studiów podyplomowych: Bezpieczeństwo infrastruktury krytycznej i kluczowej w zakresie systemów przemysłowych Operational Technology (OT)
Nazwa jednostki/jednostek organizacyjnych prowadzących studia wraz z symbolem jednostki/jednostek: Wydział Inżynierii Elektrycznej i Komputerowej E-0
Nazwa jednostki wiodącej Wydział Inżynierii Elektrycznej i Komputerowej E-0
Kod i nazwa studiów podyplomowych według klasyfikacji ISCED 0688 - Interdyscyplinarne programy i kwalifikacje obejmujące technologie informacyjno-komunikacyjne

Nazwa przedmiotu w języku polskim	Zagrożenia w obszarze cyberbezpieczeństwa sieci i systemów OT
Nazwa przedmiotu w języku angielskim	Threats in the area of cybersecurity of OT networks and systems
Kategoria przedmiotu	specjalnościowy
Liczba punktów ECTS	2
Semestry	I
Język wykładowy	Polski

Wymagania wstępne: Znajomość zgadnie związanych z cyberzagrożeniami i cyberbezpieczestwem, Zagrożenia systemów sterowania i wizualizacji w obszarze cyberbezpieczeństwa i bezpieczeństwa infrastruktury krytycznej,

Cele przedmiotu: Celem przedmiotu jest nabycie wiedzy i umiejętności w zakresie podstawowych zasad obowiązujących w Polsce oraz UE w zakresie bezpieczeństwa infrastruktury krytycznej i kluczowej.

Efekty uczenia się:
EU1: zna rodzaje cyberzagrożen (COT_W01, COT_W02, COT_W03, COT_W04, COT_W5, COT_W6, COT_W7, COT_W8, COT_W9).
EU2: potrafi identyfikować zagrożenia spowodowane cyberatakami. (COT_U02, COT_U09).
EU3: potrafi wykrywać i analizować zagrożenia oraz identyfikować ich skutki (COT_U02, COT_U04, COT_U08, COT_U09).
EU4: potrafi dobrać rodzaj i zakres działań naprawczych (COT_U05).
EU5: jest przygotowany do projektowania, budowy, obsługi i administrowania systemów wirtualnych (COT_K02).

Forma zajęć, semestralna liczba godzin

Semestr	Forma zaliczenia (E/Z)	Wykłady	Ćwiczenia	Laboratorium	Laboratorium komputerowe	Projekt	Seminarium
I	Z	15					

Treści programowe (oddzielnie dla każdej formy zajęć):

Forma zajęć	Tematyka zajęć	Liczba godzin
W	1. Rodzaje cyberzagrożeń. 2. Metodologia wykrywania i identyfikacji cyberzagrożen. 3. Analiza przypadku na przykładzie zagrożeń typu DDoS, dezinformacja, złośliwe oprogramowanie. 4. Analiza przypadku ataków socjotechnicznych 5. Różnice w wyzwaniach cyberbezpieczeństwa w IT i OT 6. Przykałdy ataków skierowanych na infrastrukturę OT	15

Metody dydaktyczne: wykład problemowy

Sposoby weryfikacji i oceny efektów uczenia się: Wykład: zaliczenie pisemne.

Kryteria oceny: odpowiedzieć poprawnie na minimum 70% pytań na kolokwium z wiadomości przekazywanych na wykładach.

Dodatkowe informacje ustalane przez osobę odpowiedzialną za przedmiot:
Wykaz literatury:
1. Materiały dostarczone przez prowadzącego w formie elektronicznej.
2. Materiały dydaktyczne dostępne na dedykowanych serwisach internetowych.

Zatwierdzenie karty przedmiotu:

……..	……	……..……
miejscowość, data	osoba odpowiedzialna za przedmiot	kierownik jednostki organizacyjnej PK/ przewodniczący rady programowej studiów

Politechnika Krakowska im. Tadeusza Kościuszki

Karta przedmiotu

Obowiązuje uczestników rozpoczynających studia podyplomowe w roku akademickim 2023/2024
Nazwa studiów podyplomowych: Bezpieczeństwo infrastruktury krytycznej i kluczowej w zakresie systemów przemysłowych Operational Technology (OT)
Nazwa jednostki/jednostek organizacyjnych prowadzących studia wraz z symbolem jednostki/jednostek: Wydział Inżynierii Elektrycznej i Komputerowej E-0
Nazwa jednostki wiodącej Wydział Inżynierii Elektrycznej i Komputerowej E-0
Kod i nazwa studiów podyplomowych według klasyfikacji ISCED 0688 - Interdyscyplinarne programy i kwalifikacje obejmujące technologie informacyjno-komunikacyjne

Nazwa przedmiotu w języku polskim	Zarządzanie bezpieczeństwem informacji - SZBI
Nazwa przedmiotu w języku angielskim	Information Security Management System - SZBI
Kategoria przedmiotu	specjalnościowy
Liczba punktów ECTS	3
Semestry	I
Język wykładowy	Polski

Wymagania wstępne: Znajomość zgadnie związanych z cyberzagrożeniami i cyberbezpieczestwem, Podstawowa znajomość systemów i norm związanych z zarządzaniem informacji,

Cele przedmiotu: Celem przedmiotu jest nabycie wiedzy i umiejętności w zakresie podstawowych zasad obowiązujących w Polsce oraz UE w zakresie bezpieczeństwa infrastruktury krytycznej i kluczowej.

Efekty uczenia się:
EU1: zna systemy i normy związane z budową, nadzorowaniem i działaniem infrastruktury zagrożobej cyberatakami (COT_W01, COT_W02, COT_W03, COT_W04, COT_W5, COT_W6, COT_W7, COT_W8, COT_W9).
EU2: potrafi tworzyć i nadzorować dokumentację SZBI (COT_U02, COT_U09).
EU3: potrafi wykrywać i analizować prawidłowość działania systemu SZBI (COT_U02, COT_U04, COT_U08, COT_U09).
EU4: potrafi dobrać rodzaj i zakres działań naprawczych (COT_U05).

Forma zajęć, semestralna liczba godzin

Semestr	Forma zaliczenia (E/Z)	Wykłady	Ćwiczenia	Laboratorium	Laboratorium komputerowe	Projekt	Seminarium
I	E	15			5		

Treści programowe (oddzielnie dla każdej formy zajęć):

Forma zajęć	Tematyka zajęć	Liczba godzin
W	1. Podstawy bezpieczeństwa informacji, Norma ISO/IEC 27001 - wstęp i analiza przypadku. 2. Tworzenie systemu zarządzania bezpieczeństwem informacji –SZBI – road map w budowaniu cyberbezpieczeństwa 3. Zasady nadzoru, rozwoju, monitorowania i doskonalenia systemu 4. Zasady przeprowadzania audytów wewnętrznych i certyfikujących	15
K	1.Budowa, tworzenie i weryfikacja przykładowego systemu SZBI – możliwość wykorzystania przykładów własnych	5

Metody dydaktyczne: wykład problemowy, ćwiczenia laboratoryjne

Sposoby weryfikacji i oceny efektów uczenia się: Wykład: zaliczenie pisemne.
Laboratorium komputerowe: ocena wykonywanych zadań praktycznych.

Kryteria oceny: odpowiedzieć poprawnie na minimum 70% pytań na kolokwium z wiadomości przekazywanych na wykładach. Poprawne wykonanie minimum 70% zadań praktycznych

---

Dodatkowe informacje ustalane przez osobę odpowiedzialną za przedmiot:
Wykaz literatury:
1. Materiały dostarczone przez prowadzącego w formie elektronicznej.
2. Norma ISO/IEC 27001
2. Materiały dydaktyczne dostępne na dedykowanych serwisach internetowych.

Zatwierdzenie karty przedmiotu:

……..	……	……..……
miejscowość, data	osoba odpowiedzialna za przedmiot	kierownik jednostki organizacyjnej PK/ przewodniczący rady programowej studiów

Politechnika Krakowska im. Tadeusza Kościuszki

Karta przedmiotu

Obowiązuje uczestników rozpoczynających studia podyplomowe w roku akademickim 2023/2024
Nazwa studiów podyplomowych: Bezpieczeństwo infrastruktury krytycznej i kluczowej w zakresie systemów przemysłowych Operational Technology (OT)
Nazwa jednostki/jednostek organizacyjnych prowadzących studia wraz z symbolem jednostki/jednostek: Wydział Inżynierii Elektrycznej i Komputerowej E-0
Nazwa jednostki wiodącej Wydział Inżynierii Elektrycznej i Komputerowej E-0
Kod i nazwa studiów podyplomowych według klasyfikacji ISCED 0688 - Interdyscyplinarne programy i kwalifikacje obejmujące technologie informacyjno-komunikacyjne

Nazwa przedmiotu w języku polskim	Projektowanie, budowa, konfiguracja i administrowanie przemysłowych sieci OT
Nazwa przedmiotu w języku angielskim	Design, construction, configuration and administration of industrial OT networks
Kategoria przedmiotu	specjalnościowy
Liczba punktów ECTS	5
Semestry	I i II
Język wykładowy	Polski

Wymagania wstępne: Znajomość zagadnień związanych z sieciami informatycznymi i przemysłowymi, Podstawowa znajomość systemów sieciowych i infrastruktury sieciowej,

Cele przedmiotu: Celem przedmiotu jest nabycie wiedzy i umiejętności w zakresie podstawowych zasad obowiązujących w Polsce oraz UE w zakresie bezpieczeństwa infrastruktury krytycznej i kluczowej.

Efekty uczenia się:
EU1: zna systemy i normy związane z projektowaniem, budową, konfiguracją i administrowaniem sieci OT (COT_W01, COT_W02, COT_W03, COT_W04, COT_W5, COT_W6, COT_W7, COT_W8, COT_W9).
EU2: potrafi zarządzać i administrować adresacją sieci, tworzyć i zarządzać VLAN (COT_U02, COT_U09).
EU3: potrafi wykrywać i analizować ruch w sieci OT, zarządzać politykami i konfigurować spamporty (COT_U02, COT_U04, COT_U08, COT_U09).
EU4: potrafi dobrać rodzaj i zakres działań naprawczych (COT_U05).

Forma zajęć, semestralna liczba godzin

Semestr	Forma zaliczenia (E/Z)	Wykłady	Ćwiczenia	Laboratorium	Laboratorium komputerowe	Projekt	Seminarium
I	E	10			30		

Treści programowe (oddzielnie dla każdej formy zajęć):

Forma zajęć	Tematyka zajęć	Liczba godzin
W	1. Budowa sieci informatycznych 2. Konfiguracja i administracji adresacją sieciową. 3. Zasady budowy redundantnych sieci przemysłowych OT 4. Polityki bezpieczeństwa i zasady bezpieczeństwa sieci OT 5. Zarządzanie uprawnieniami i polityka dostępowa 6. Analiza i raportowanie	10
K	1.Projekt i budowa przemysłowej sieci OT opartej o rozwiązania redundantne. 2. Projekt wraz z analizą cyberbezpieczeństwa sieci OT	30

	3. Tworzenie i zarzadzanie politykami bezpieczeństwa sieci OT 4. Analiza pracy sieci z wykorzystaniem narzędzi raportujących.	

Metody dydaktyczne: wykład problemowy, ćwiczenia laboratoryjne

Sposoby weryfikacji i oceny efektów uczenia się: Wykład: zaliczenie pisemne.
Laboratorium komputerowe: ocena wykonywanych zadań praktycznych.

Kryteria oceny: odpowiedzieć poprawnie na minimum 70% pytań na kolokwium z wiadomości przekazywanych na wykładach. Poprawne wykonanie minimum 70% zadań praktycznych

---

Dodatkowe informacje ustalane przez osobę odpowiedzialną za przedmiot:
Wykaz literatury:
1. Materiały dostarczone przez prowadzącego w formie elektronicznej.
2. Materiały dydaktyczne dostępne na dedykowanych serwisach internetowych.

Zatwierdzenie karty przedmiotu:

…….	……	……..……
miejscowość, data	osoba odpowiedzialna za przedmiot	kierownik jednostki organizacyjnej PK/ przewodniczący rady programowej studiów

Politechnika Krakowska im. Tadeusza Kościuszki

Karta przedmiotu

Obowiązuje uczestników rozpoczynających studia podyplomowe w roku akademickim 2023/2024
Nazwa studiów podyplomowych: Bezpieczeństwo infrastruktury krytycznej i kluczowej w zakresie systemów przemysłowych Operational Technology (OT)
Nazwa jednostki/jednostek organizacyjnych prowadzących studia wraz z symbolem jednostki/jednostek: Wydział Inżynierii Elektrycznej i Komputerowej E-0
Nazwa jednostki wiodącej Wydział Inżynierii Elektrycznej i Komputerowej E-0
Kod i nazwa studiów podyplomowych według klasyfikacji ISCED 0688 - Interdyscyplinarne programy i kwalifikacje obejmujące technologie informacyjno-komunikacyjne

Nazwa przedmiotu w języku polskim	Tworzenie, administracja i konfiguracja wirtualnych prywatnych sieci VPN.
Nazwa przedmiotu w języku angielskim	Creation, administration and configuration of virtual private VPN networks
Kategoria przedmiotu	specjalnościowy
Liczba punktów ECTS	2
Semestry	II
Język wykładowy	Polski

Wymagania wstępne: Znajomość zagadnień związanych z sieciami informatycznymi i przemysłowymi, Podstawowa znajomość systemów szyfrowania i zabezpieczania połączeń komunikacyjnych,

Cele przedmiotu: Celem przedmiotu jest nabycie wiedzy i umiejętności w zakresie podstawowych zasad obowiązujących w Polsce oraz UE w zakresie bezpieczeństwa infrastruktury krytycznej i kluczowej.

Efekty uczenia się:
EU1: zna systemy i normy związane z projektowaniem, budową, konfiguracją i administrowaniem sieci OT (COT_W01, COT_W02, COT_W03, COT_W04, COT_W5, COT_W6, COT_W7, COT_W8, COT_W9).
EU2: potrafi tworzyć i administrować wirtualne sieci VPN (COT_U02, COT_U09).
EU3: potrafi analizować ruch sieciowy i zarządzać tym ruchem (COT_U02, COT_U04, COT_U08, COT_U09).
EU4: potrafi dobrać rodzaj i zakres działań naprawczych (COT_U05).

Forma zajęć, semestralna liczba godzin

Semestr	Forma zaliczenia (E/Z)	Wykłady	Ćwiczenia	Laboratorium	Laboratorium komputerowe	Projekt	Seminarium
I	E	5			5		

Treści programowe (oddzielnie dla każdej formy zajęć):

Forma zajęć	Tematyka zajęć	Liczba godzin
W	1. Budowa i konfiguracja wirtualnych prywatnych sieci VPN 2. Zarządzanie poświadczeniami. 3. Szyfrowanie połączeń wraz z doborem optymalnych poziomów zabezpieczeń. 4. Analiza i raportowanie	5
K	1.Projekt i budowa wirtualnych szyfrowanych prywatnych sieci VPN 2.Praktyczne wykonanie i skonfigurowanie VPN dla środowiska badawczego.	5

Metody dydaktyczne: wykład problemowy, ćwiczenia laboratoryjne

Sposoby weryfikacji i oceny efektów uczenia się: Wykład: zaliczenie pisemne.
Laboratorium komputerowe: ocena wykonywanych zadań praktycznych.

Kryteria oceny: odpowiedzieć poprawnie na minimum 70% pytań na kolokwium z wiadomości przekazywanych na wykładach. Poprawne wykonanie minimum 70% zadań praktycznych

---

Dodatkowe informacje ustalane przez osobę odpowiedzialną za przedmiot:
Wykaz literatury:
1. Materiały dostarczone przez prowadzącego w formie elektronicznej.
2. Materiały dydaktyczne dostępne na dedykowanych serwisach internetowych.

Zatwierdzenie karty przedmiotu:

…….	……	……..……
miejscowość, data	osoba odpowiedzialna za przedmiot	kierownik jednostki organizacyjnej PK/ przewodniczący rady programowej studiów

Politechnika Krakowska im. Tadeusza Kościuszki

Karta przedmiotu

Obowiązuje uczestników rozpoczynających studia podyplomowe w roku akademickim 2023/2024
Nazwa studiów podyplomowych: Bezpieczeństwo infrastruktury krytycznej i kluczowej w zakresie systemów przemysłowych Operational Technology (OT)
Nazwa jednostki/jednostek organizacyjnych prowadzących studia wraz z symbolem jednostki/jednostek: Wydział Inżynierii Elektrycznej i Komputerowej E-0
Nazwa jednostki wiodącej Wydział Inżynierii Elektrycznej i Komputerowej E-0
Kod i nazwa studiów podyplomowych według klasyfikacji ISCED 0688 - Interdyscyplinarne programy i kwalifikacje obejmujące technologie informacyjno-komunikacyjne

Nazwa przedmiotu w języku polskim	SIEM, SOAR, SOC - dobór, konfiguracja i administracja. Audyt systemów OT
Nazwa przedmiotu w języku angielskim	SIEM, SOAR, SOC - selection, configuration and administration. Audit of OT systems
Kategoria przedmiotu	specjalnościowy
Liczba punktów ECTS	4
Semestry	II
Język wykładowy	Polski

Wymagania wstępne: Znajomość zagadnień związanych z sieciami informatycznymi i przemysłowymi, Podstawowa znajomość systemów szyfrowania i zabezpieczania połączeń komunikacyjnych,

Cele przedmiotu: Celem przedmiotu jest nabycie wiedzy i umiejętności w zakresie podstawowych zasad obowiązujących w Polsce oraz UE w zakresie bezpieczeństwa infrastruktury krytycznej i kluczowej.

Efekty uczenia się:
EU1: zna systemy i normy związane z projektowaniem, budową, konfiguracją i administrowaniem sieci OT (COT_W01, COT_W02, COT_W03, COT_W04, COT_W5, COT_W6, COT_W7, COT_W8, COT_W9).
EU2: potrafi tworzyć i administrować wirtualne sieci VPN (COT_U02, COT_U09).
EU3: potrafi analizować ruch sieciowy i zarządzać tym ruchem (COT_U02, COT_U04, COT_U08, COT_U09).
EU4: potrafi dobrać rodzaj i zakres działań naprawczych (COT_U05).

Forma zajęć, semestralna liczba godzin

Semestr	Forma zaliczenia (E/Z)	Wykłady	Ćwiczenia	Laboratorium	Laboratorium komputerowe	Projekt	Seminarium
I	E	10			20		

Treści programowe (oddzielnie dla każdej formy zajęć):

Forma zajęć	Tematyka zajęć	Liczba godzin
W	1. Monitorowanie, reagowanie, zgłaszanie incydentu 2. SOC/SIEM/SOAR - definicje, różnice, przykłady, dobór 3. Narzędzie wspierające monitorowanie 4. Budowanie scenariuszy dla zespołów SOC 5. Audyt infrastruktury IT oraz OT - określanie granic 6. Audyt bezpieczeństwa sieci OT - na czym powinien bazować 7. Określenie wektorów ataku 8. Testy penetracyjne a skanowanie podatności 9. Przykład projektowania raportu	10

K	1. Instalacja przykładowego oprogramowania typu SIEM 2. Przykład analizy zdarzenia/incydentu 3. Poznanie narzędzi do wykonywania testów penetracyjnych / skanów podatności 4. Symulacja testu penetracyjnego / skanu podatności na przykładzie aplikacji webowej 5. Tworzenie przykładowego raportu	20

Metody dydaktyczne: wykład problemowy, ćwiczenia laboratoryjne

Sposoby weryfikacji i oceny efektów uczenia się: Wykład: zaliczenie pisemne.
Laboratorium komputerowe: ocena wykonywanych zadań praktycznych.

Kryteria oceny: odpowiedzieć poprawnie na minimum 70% pytań na kolokwium z wiadomości przekazywanych na wykładach. Poprawne wykonanie minimum 70% zadań praktycznych

---

Dodatkowe informacje ustalane przez osobę odpowiedzialną za przedmiot:
Wykaz literatury:
1. Materiały dostarczone przez prowadzącego w formie elektronicznej.
2. Materiały dydaktyczne dostępne na dedykowanych serwisach internetowych.

Zatwierdzenie karty przedmiotu:

…….	……	……..……
miejscowość, data	osoba odpowiedzialna za przedmiot	kierownik jednostki organizacyjnej PK/ przewodniczący rady programowej studiów

Politechnika Krakowska im. Tadeusza Kościuszki

Karta przedmiotu

Obowiązuje uczestników rozpoczynających studia podyplomowe w roku akademickim 2023/2024
Nazwa studiów podyplomowych: Bezpieczeństwo infrastruktury krytycznej i kluczowej w zakresie systemów przemysłowych Operational Technology (OT)
Nazwa jednostki/jednostek organizacyjnych prowadzących studia wraz z symbolem jednostki/jednostek: Wydział Inżynierii Elektrycznej i Komputerowej E-0
Nazwa jednostki wiodącej Wydział Inżynierii Elektrycznej i Komputerowej E-0
Kod i nazwa studiów podyplomowych według klasyfikacji ISCED 0688 - Interdyscyplinarne programy i kwalifikacje obejmujące technologie informacyjno-komunikacyjne

Nazwa przedmiotu w języku polskim	Przemysłowe systemy IPS/IDS – dobór, konfiguracja i administracja
Nazwa przedmiotu w języku angielskim	Industrial IPS/IDS systems – selection, configuration and administration
Kategoria przedmiotu	specjalnościowy
Liczba punktów ECTS	4
Semestry	II
Język wykładowy	Polski

Wymagania wstępne: Znajomość zagadnień związanych z sieciami informatycznymi i przemysłowymi, Podstawowa znajomość systemów monitorowania i diagnostyki sieci OT,

Cele przedmiotu: Celem przedmiotu jest nabycie wiedzy i umiejętności w zakresie podstawowych zasad obowiązujących w Polsce oraz UE w zakresie bezpieczeństwa infrastruktury krytycznej i kluczowej.

Efekty uczenia się:
EU1: zna systemy i normy związane z projektowaniem, budową, konfiguracją i administrowaniem sieci OT (COT_W01, COT_W02, COT_W03, COT_W04, COT_W5, COT_W6, COT_W7, COT_W8, COT_W9).
EU2: potrafi tworzyć i administrować systemy monitorujące sieci przemysłowe OT (COT_U02, COT_U09).
EU3: potrafi analizować ruch sieciowy i identyfikować zagrożenia (COT_U02, COT_U04, COT_U08, COT_U09).
EU4: potrafi dobrać rodzaj i zakres działań naprawczych (COT_U05).

Forma zajęć, semestralna liczba godzin

Semestr	Forma zaliczenia (E/Z)	Wykłady	Ćwiczenia	Laboratorium	Laboratorium komputerowe	Projekt	Seminarium
I	E	10			20		

Treści programowe (oddzielnie dla każdej formy zajęć):

Forma zajęć	Tematyka zajęć	Liczba godzin
W	1. Monitorowanie, reagowanie, zgłaszanie incydentu do systemu nadrzędnego klasy SIEM 2. IDS/IPS- definicje, różnice, przykłady, dobór 3. Narzędzie wspierające monitorowanie 4. Określenie wektorów ataku 5. Testy penetracyjne a skanowanie podatności w sieci OT 6. Przykład projektowania raportu systemu monitorującego sieć OT	10

K	1. Instalacja przykładowego oprogramowania typu IDS/IPS 2. Przykład analizy zdarzeń i możliwych incydentów 3. Symulacja testu penetracyjnego / skanu podatności na przykładzie aplikacji klasy IDS. 4. Budowanie i monitorowanie struktury systemu sieci OT 5. Tworzenie połączenia komunikacyjnego z nadrzędnym systemem klasy SIEM - syslog 6. Tworzenie przykładowego raportu	20

Metody dydaktyczne: wykład problemowy, ćwiczenia laboratoryjne

Sposoby weryfikacji i oceny efektów uczenia się: Wykład: zaliczenie pisemne.
Laboratorium komputerowe: ocena wykonywanych zadań praktycznych.

Kryteria oceny: odpowiedzieć poprawnie na minimum 70% pytań na kolokwium z wiadomości przekazywanych na wykładach. Poprawne wykonanie minimum 70% zadań praktycznych

---

Dodatkowe informacje ustalane przez osobę odpowiedzialną za przedmiot:
Wykaz literatury:
1. Materiały dostarczone przez prowadzącego w formie elektronicznej.
2. Materiały dydaktyczne dostępne na dedykowanych serwisach internetowych.

Zatwierdzenie karty przedmiotu:

…….	……	……..……
miejscowość, data	osoba odpowiedzialna za przedmiot	kierownik jednostki organizacyjnej PK/ przewodniczący rady programowej studiów

Politechnika Krakowska im. Tadeusza Kościuszki

Karta przedmiotu

Obowiązuje uczestników rozpoczynających studia podyplomowe w roku akademickim 2023/2024
Nazwa studiów podyplomowych: Bezpieczeństwo infrastruktury krytycznej i kluczowej w zakresie systemów przemysłowych Operational Technology (OT)
Nazwa jednostki/jednostek organizacyjnych prowadzących studia wraz z symbolem jednostki/jednostek: Wydział Inżynierii Elektrycznej i Komputerowej E-0
Nazwa jednostki wiodącej Wydział Inżynierii Elektrycznej i Komputerowej E-0
Kod i nazwa studiów podyplomowych według klasyfikacji ISCED 0688 - Interdyscyplinarne programy i kwalifikacje obejmujące technologie informacyjno-komunikacyjne

Nazwa przedmiotu w języku polskim	Platforma softwerowo-sprzętowa systemów przemysłowych OT
Nazwa przedmiotu w języku angielskim	Software and hardware platform for industrial OT systems
Kategoria przedmiotu	specjalnościowy
Liczba punktów ECTS	4
Semestry	II
Język wykładowy	Polski

Wymagania wstępne: Znajomość zagadnień związanych z sieciami informatycznymi i przemysłowymi poznanymi w toku studiów podyplomowych,
Znajomość systemów monitorowania i diagnostyki sieci OT,

Cele przedmiotu: Celem przedmiotu jest budowa systemu bezpieczeństwa systemów OT zgodnie z zasadami obowiązującymi w Polsce oraz UE w zakresie bezpieczeństwa infrastruktury krytycznej i kluczowej.

Efekty uczenia się:
EU1: zna systemy i normy związane z projektowaniem, budową, konfiguracją i administrowaniem sieci OT (COT_W01, COT_W02, COT_W03, COT_W04, COT_W5, COT_W6, COT_W7, COT_W8, COT_W9).
EU2: potrafi tworzyć i administrować systemy bezpieczeństwa przemysłowych systemów OT (COT_U02, COT_U09).
EU3: potrafi analizować ruch sieciowy i identyfikować zagrożenia (COT_U02, COT_U04, COT_U08, COT_U09).
EU4: potrafi dobrać rodzaj i zakres działań naprawczych (COT_U05).

Forma zajęć, semestralna liczba godzin

Semestr	Forma zaliczenia (E/Z)	Wykłady	Ćwiczenia	Laboratorium	Laboratorium komputerowe	Projekt	Seminarium
I	E				30		

Treści programowe (oddzielnie dla każdej formy zajęć):

Forma zajęć	Tematyka zajęć	Liczba godzin
K	1. Budowa systemu OT wraz z implementacją oprogramowania typu IDS/IPS - każdy słuchacz studiów 2. Analizy występujących zdarzenia/incydentu 3. Analiza i opis przykładowego raportu bezpieczeństwa - zaliczenie zadania	30

Metody dydaktyczne: wykład problemowy, ćwiczenia laboratoryjne

Sposoby weryfikacji i oceny efektów uczenia się: Wykład: zaliczenie pisemne.
Laboratorium komputerowe: ocena wykonywanych zadań praktycznych.

Kryteria oceny: odpowiedzieć poprawnie na minimum 70% pytań na kolokwium z wiadomości przekazywanych na wykładach. Poprawne wykonanie minimum 70% zadań praktycznych

---

Dodatkowe informacje ustalane przez osobę odpowiedzialną za przedmiot:
Wykaz literatury:
1. Materiały dostarczone przez prowadzącego w formie elektronicznej.
2. Materiały dydaktyczne dostępne na dedykowanych serwisach internetowych.

Zatwierdzenie karty przedmiotu:

…….	……	……..……
miejscowość, data	osoba odpowiedzialna za przedmiot	kierownik jednostki organizacyjnej PK/ przewodniczący rady programowej studiów