Politechnika Krakowska im. Tadeusza Kościuszki w Krakowie
Nazwa jednostki/jednostek organizacyjnych prowadzących studia wraz z symbolem jednostki/jednostek i wydziału:
Wydział Inżynierii Elektrycznej i Komputerowej
Nazwa jednostki wiodącej: **Wydział Inżynierii Elektrycznej i Komputerowej E-0**
Nazwa studiów podyplomowych: **Cyberbezpieczeństwo infrastruktury transportu szynowego**

Poziom Polskiej Ramy Kwalifikacji **6 PRK**
Dziedzina lub dziedziny nauki/sztuki: **Dziedzina nauk inżynieryjno-technicznych (100%)**

PLAN STUDIÓW PODYPLOMOWYCH

Obowiązuje dla cykli kształcenia rozpoczynających się od: rok akademicki 2025/26, semestr letni

Lp.	Nazwa przedmiotu	RAZEM									semestry															
											I								II							
		Liczba godzin RAZEM	W	C	L	LK	P	S	ECTS	Egz	W	C	L	LK	P	S	ECTS	Egz	W	C	L	LK	P	S	ECTS	Egz
1	Bezpieczeństwo łańcucha dostaw i zgodność systemów kolejowych z regulacjami UE	15	10	5					3	Z	10	5					3	Z								
2	Budowa Systemu Zarządzania Bezpieczeństwem Informacji w transporcie szynowym	15	10	5					4	E	10	5					4	E								
3	Podstawy bezpieczeństwa infrastruktury automatyki przemysłowej	40	20	20					6	E	15	10					3	Z	5	10					3	E
4	Projektowanie, budowa, konfiguracja i administrowanie przemysłowych sieci OT	35	10			25			5	E	10			10			2	Z				15			3	E
5	Systemy i układy sterowania procesowego - dobór, konfiguracja i administracja	15				15			2	Z				15			2	Z								
6	Systemy i urządzenia sterowania ruchem kolejowym	30	25			5			5	Z	10						1	Z	15			5			4	Z
7	Zapewnienie zgodności systemów transportu szynowego z normą IEC 62443, TS 50701 oraz IEC 63452	30	15	15					5	E									15	15					5	E
Ogółem		**180**	**90**	**45**	**0**	**45**	**0**	**0**	**30**	**4**	**55**	**20**	**0**	**25**	**0**	**0**	**15**	**1**	**35**	**25**	**0**	**20**	**0**	**0**	**15**	**3**

Litera "E" w kolumnach Egz (w poszczególnych semestrach) oznacza egzamin. Liczba zawarta w kolumnie Egz - w podsumowaniu RAZEM - oznacza liczbę egzaminów.

Legenda: W - wykłady, C - ćwiczenia, L - laboratoria, LK - laboratoria komputerowe, P - projekty, S - seminaria

Określenie trybu i warunków przeprowadzania egzaminu końcowego, w tym formę egzaminu (ustny lub pisemny), obowiązek przygotowania pracy końcowej, wagi służące do ustalenia ostatecznego wyniku studiów: Problemy współczesnej trakcji elektrycznej - egzamin końcowy - zajęcia z ustnym egzaminem końcowym sprawdzającym zagadnienia omawiane również podczas pozostałych zajęć. Warunkiem dopuszczenia do egzaminu końcowego jest zaliczenie wszystkich semestrów studiów podyplomowych, spełnienie wymogów formalnych. Termin egzaminu określa kierownik studiów i podaje do wiadomości uczestnikom nie później niż w dniu rozpoczęcia drugiego semestru. Egzamin końcowy ma formę ustną i stanowi weryfikację osiągniętych efektów uczenia się ujętych w programie studiów podyplomowych. Egzamin końcowy przeprowadzany jest przez komisję egzaminacyjną składającą się z kierownika studiów podyplomowych oraz dwóch osób prowadzących zajęcia dydaktyczne na studiach podyplomowych. Egzamin ustny polega na odpowiedzi na trzy pytania związane z przedmiotami na studiach podyplomowych. Po zakończeniu egzaminu komisja sporządza protokół egzaminu końcowego i podaje wynik. Egzamin końcowy jest zdany, jeżeli ocena z egzaminu jest większa lub równa 3,0. Ostateczny wynik studiów podyplomowych jest średnią ważoną następujących ocen: średnia arytmetyczna ocen z pytań zadanych przez komisję podczas egzaminu końcowego z wagą 0,4 i ocena z toku studiów z wagą 0,6.

Wymiar, zasady i forma odbywania praktyk zawodowych: W ramach studiów podyplomowych nie przewiduje się odbywania praktyk zawodowych.

Politechnika Krakowska im. Tadeusza Kościuszki

Karta przedmiotu

Obowiązuje uczestników rozpoczynających studia podyplomowe w roku akademickim 2026/2027

Nazwa studiów podyplomowych: Cyberbezpieczeństwo infrastruktury transportu szynowego
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 łańcucha dostaw i zgodność systemów kolejowych z regulacjami UE
Nazwa przedmiotu w języku angielskim	Supply chain security and compliance of railway systems with EU regulations
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:
EU01: zna szczegółowe wymagania Dyrektywy NIS2 oraz Rozporządzenia Cyber Resilience Act (CRA) w odniesieniu do cyklu życia produktów kolejowych. (CITS-W10)
EU02: rozumie relacje między normami IEC 62443, CLC/TS 50701 oraz IEC 63452 w procesie budowy bezpiecznej architektury systemów sterowania ruchem. (CITS-W13, CITS-W07)
EU03: zna modele zarządzania ryzykiem w łańcuchu dostaw oraz mechanizmy odpowiedzialności zarządu za naruszenia regulacji unijnych. (CITS-W07, CITS-W10)
EU04: zna metody integracji wymogów bezpieczeństwa funkcjonalnego (Safety) z cyberbezpieczeństwem (Security) w systemach klasy ETCS/ERTMS. (CITS-W11, CITS-W13)
EU05: potrafi dokonać oceny bezpieczeństwa łańcucha dostaw oraz sformułować wymagania dla dostawców urządzeń z elementami cyfrowymi zgodnie z CRA. (CITS-U17)
EU06: potrafi zweryfikować dokumentację techniczną i procesową wymaganą do certyfikacji komponentów taborowych na terenie UE. (CITS-U06, CITS-U13)
EU07: potrafi analizować zapisy w umowach SLA pod kątem zapewnienia ciągłości działania i cyberodporności podwykonawców. (CITS-U17, CITS-U07)
EU08: prezentuje profesjonalną postawy w procesach audytowych i kierowania się etyką zawodową w zarządzaniu bezpieczeństwem krytycznym. (CITS-K01)

Forma zajęć, semestralna liczba godzin

Semestr	Forma zaliczenia (E/Z)	Wykłady	Ćwiczenia	Laboratorium	Laboratorium komputerowe	Projekt	Seminarium
I	Z	10	5				
II							

Treści programowe (oddzielnie dla każdej formy zajęć):

Forma zajęć	Tematyka zajęć	Liczba godzin
W	1. Charakterystyka systemów IT i OT w transporcie szynowym jako elementu infrastruktury krytycznej państwa. 2. Analiza struktury łańcucha dostaw dla producentów taboru oraz dostawców systemów sterowania ruchem 3. Identyfikacja cyfrowych i fizycznych zagrożeń wynikających z zależności od zewnętrznych dostawców komponentów. 4. Wymagania Dyrektywy NIS2 w zakresie zarządzania ryzykiem i raportowania incydentów w sektorze transportu. 5. Rola Cyber Resilience Act (CRA) w zapewnieniu bezpieczeństwa produktów z elementami cyfrowymi w całym cyklu ich życia. 6. Obowiązki producentów i dystrybutorów dotyczące certyfikacji oraz oznakowania zgodnie z wymogami Rozporządzenia Cyber Resilience Act (CRA). 7. Wdrażanie koncepcji "security-by-design" i "security-by-default" w procesach produkcji urządzeń kolejowych. 8. Zasady odporności podmiotów krytycznych na podstawie unijnej Dyrektywy CER. 9. Zastosowanie normy CLC/TS 50701 oraz IEC 63452 jako fundamentu cyberbezpieczeństwa w systemach kolejowych. 10. Zarządzanie podatnościami w oprogramowaniu przy wykorzystaniu zestawień Software Bill of Materials (SBOM). 11. Praktyczne aspekty konstruowania umów SLA oraz audytowania poziomu zabezpieczeń u podwykonawców. 12. Integracja wymogów bezpieczeństwa funkcjonalnego (Safety) z ochroną przed cyberatakami (Security). 13. Procedury oceny zgodności i certyfikacji komponentów taborowych z regulacjami unijnymi. 14. Analiza odpowiedzialności prawnej i finansowej zarządów spółek za brak zgodności z NIS2 i CRA.	10
	1. Przygotowanie oceny zgodnie z CRA dla wybranego komponentu 2. Analiza umowy z dostawcą pod kątem zgodności z wymaganiami prawnymi 3. Analiza źródeł danych o podatnościach komponentów	5

Praca własna uczestnika:

	Opis pracy własnej	Liczba godzin
PW	Studiowanie zalecanej literatury i przygotowanie do dyskusji	60

Metody dydaktyczne:

wykład problemowy oraz ćwiczenia

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.

Wykaz literatury:

1. Materiały dostarczone przez prowadzącego w formie elektronicznej.
2. Rozporządzenie CRA w formie elektronicznej
3. Dyrektywa NIS2 oraz Ustawa o Krajowym Systemie Cyberbezpieczeństwa w formie elektronicznej

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 2026/2027

Nazwa studiów podyplomowych: Cyberbezpieczeństwo infrastruktury transportu szynowego
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	Budowa Systemu Zarządzania Bezpieczeństwem Informacji w transporcie szynowym
Nazwa przedmiotu w języku angielskim	Designing Information Security Management System in the railways transport
Kategoria przedmiotu	specjalnościowy
Liczba punktów ECTS	4
Semestry	I
Język wykładowy	Polski

Wymagania wstępne: Znajomość zgadnie związanych z cyberzagrożeniami i cyberbezpieczeństwem, 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:
EU01: Wyjaśnia zasady i wymagania normy ISO/IEC 27001 oraz jej rolę w budowaniu odporności cybernetycznej organizacji (CITS_W01, CITS_W08).
EU02: Opisuje etapy tworzenia SZBI (road map) oraz mechanizmy nadzoru i doskonalenia systemu zgodnie z cyklem PDCA (CITS_W08, CITS_W13).
EU03: Zna metodykę przeprowadzania audytów wewnętrznych oraz proces certyfikacji systemu zarządzania bezpieczeństwem (CITS_W08, CITS_W14).
EU04: Potrafi opracować szkielet dokumentacji SZBI oraz zaprojektować politykę bezpieczeństwa dla wybranej organizacji (CITS_U06, CITS_U17).
EU05: Przeprowadza weryfikację (audyt) przykładowego systemu SZBI, identyfikując niezgodności i obszary do poprawy (CITS_U07, CITS_U14).
EU06: Potrafi dobrać adekwatne zabezpieczenia organizacyjne i techniczne w ramach systemu zarządzania, uwzględniając specyfikę transportu szynowego (CITS_U18).
EU07: Student jest gotów do profesjonalnego i etycznego podejścia do audytu SZBI [CITS-K01]

Forma zajęć, semestralna liczba godzin

Semestr	Forma zaliczenia (E/Z)	Wykłady	Ćwiczenia	Laboratorium	Laboratorium komputerowe	Projekt	Seminarium
I	E	10	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	10
C	1.Budowa, tworzenie i weryfikacja przykładowego systemu SZBI – możliwość wykorzystania przykładów własnych	5

Praca własna uczestnika:

	Opis pracy własnej	Liczba godzin
PW	Studiowanie zalecanej literatury i przygotowanie do dyskusji	85

Metody dydaktyczne:

wykład problemowy oraz ćwiczenia

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

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 2026/2027

Nazwa studiów podyplomowych: Cyberbezpieczeństwo infrastruktury transportu szynowego
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	Podstawy bezpieczeństwa infrastruktury automatyki przemysłowej
Nazwa przedmiotu w języku angielskim	Introduction to the automation systems cyber security
Kategoria przedmiotu	specjalnościowy
Liczba punktów ECTS	6
Semestry	I oraz II
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 w zakresie bezpieczeństwa infrastruktury krytycznej i kluczowej.

Efekty uczenia się:
EU1: zna pojęcia związane z infrastrukturą krytyczną, kluczową oraz systemami automatyki przemysłowej oraz zna niezbędne podstawy prawne. [CITS-W01, CITS-W05, CITS-W06, CITS-W10, CITS-W11]
EU2: zna podstawowe standardy zarządzania ryzykiem oraz potrafi wykonać analizę ryzyka wybranego systemu. [CITS-W07, CITS-W13, CITS-U07, CITS-U15]
EU3: potrafi zaprojektować niezbędne procedury oraz wykonać dokumentację dla wypełnienia wymagań prawnych. [CITS-W08, CITS-W10, CITS-U06, CITS-U17]
EU4: potrafi identyfikować i analizować zagrożenia oraz potrafi dobrać rodzaj i zakres działań naprawczych. [CITS-U03, CITS-U07, CITS-U08, CITS-U09, CITS-U18]

Forma zajęć, semestralna liczba godzin

Semestr	Forma zaliczenia (E/Z)	Wykłady	Ćwiczenia	Laboratorium	Laboratorium komputerowe	Projekt	Seminarium
I		15	10				
II	E	5	10				

Treści programowe (oddzielnie dla każdej formy zajęć):

Forma zajęć	Tematyka zajęć	Liczba godzin
W	1. Zagadnienia związane z Infrastrukturą Krytyczną i Kluczową 2. Różnice charakterystyk systemów IT oraz OT 3. Przykłady ataków na systemy automatyki przemysłowej, szczegółowa analiza wybranych ataków 4. Omówienie i analiza Ustawy o Krajowym Systemie Cyberbezpieczeństwa 5. Omówienie i analiza Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2024/2847 6. Analiza charakterystyki systemów OT i ich porównanie z systemami IT w oparciu o NIST SP 800-82 7. Analiza NIST Cyber Security Framework 8. Analiza standardów zarządzania ryzykiem dla systemów informatycznych	20
C	1. Udokumentowanie przykładowego systemu zgodnie z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2024/2847 2. Przygotowanie procedury zarządzania incydentami dla przykładowego przedsiębiorstwa zgodnie z Ustawą o Krajowym Systemie Cyberbezpieczeństwa 3. Analiza wybranych cyberataków na systemy automatyki przemysłowej	20

Praca własna uczestnika:

	Opis pracy własnej	Liczba godzin
PW	Studiowanie zalecanej literatury i przygotowanie do dyskusji	110

Metody dydaktyczne:

wykład problemowy oraz ćwiczenia

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.

Wykaz literatury:

1. Materiały dostarczone przez prowadzącego w formie elektronicznej.
2. Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2024/2847
3. Ustawa o Krajowym Systemie Cyberbezpieczeństwa
4. Dokumentacja NIST Cyber Security Framework
5. Dokument NIST SP 800-82 v3
6. 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 2026/2027

Nazwa studiów podyplomowych: Cyberbezpieczeństwo infrastruktury transportu szynowego
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:
EU01: zna zasady budowy sieci IT oraz specyfikę redundantnych sieci przemysłowych OT wraz z metodami ich adresacji. [CITS-W05]
EU02: zna mechanizmy zabezpieczania systemów operacyjnych oraz metody automatyzacji administracji przy użyciu skryptów powłoki. [CITS-W06]
EU03: zna architekturę i funkcje systemów IDS/IPS, SIEM oraz technologie VPN wykorzystywane do zabezpieczania transmisji danych. [CITS-W06]
EU04: zna metodykę identyfikacji wektorów ataku oraz zasady przeprowadzania testów penetracyjnych w specyficznych środowiskach OT. [CITS-W09, CITS-W04]
EU05: zna zaawansowane mechanizmy i algorytmy zabezpieczania informacji cyfrowych, obejmujące podstawy kryptografii postkwantowej oraz systemy kwantowej dystrybucji klucza (QKD) [CITS-W02]
EU06: potrafi skonfigurować, zabezpieczyć i administrować systemem operacyjnym oraz wybranymi usługami w sieciach OT. [CITS-U02, CITS-U04]
EU07: potrafi implementować skrypty powłoki w celu automatyzacji zarządzania bezpieczeństwem i zadaniami systemowymi. [CITS-U05]
EU08: potrafi przeprowadzić analizę ruchu sieciowego w systemach OT oraz wykrywać anomalie i incydenty przy użyciu narzędzi klasy IDS/IPS. [CITS-U03, CITS-U08]
EU09: potrafi zaprojektować i zbudować redundantną sieć przemysłową oraz skonfigurować bezpieczne połączenia VPN. [CITS-U15, CITS-U09]
EU10: potrafi skonfigurować raportowanie zdarzeń do systemu SIEM i przygotować profesjonalną dokumentację z analizy bezpieczeństwa sieci. [CITS-U09, CITS-U06]
EU11: potrafi przeprowadzić skanowanie podatności oraz symulowane testy penetracyjne w infrastrukturze transportu szynowego. [CITS-U10, CITS-U07]

EU12: Student jest gotów do profesjonalnego i etycznego podejścia do zarządzania infrastrukturą krytyczną oraz odpowiedzialnego reagowania na incydenty. [CITS-K01]

Forma zajęć, semestralna liczba godzin

Semestr	Forma zaliczenia (E/Z)	Wykłady	Ćwiczenia	Laboratorium	Laboratorium komputerowe	Projekt	Seminarium
I		10			10		
II	E				15		

Treści programowe (oddzielnie dla każdej formy zajęć):

Forma zajęć	Tematyka zajęć	Liczba godzin
W	1. Zasady budowy sieci informatycznych oraz konfiguracja i administracja adresacją sieciową. 2. Projektowanie redundantnych sieci przemysłowych OT wraz z wdrażaniem dedykowanych polityk bezpieczeństwa. 3. Zarządzanie uprawnieniami, poświadczeniami i polityką dostępową w systemach transportowych. 4. Metody konfiguracji i zabezpieczania systemów operacyjnych pracujących w infrastrukturze krytycznej. 5. Budowa wirtualnych sieci prywatnych VPN oraz dobór metod szyfrowania dla bezpiecznych połączeń. 6. Charakterystyka systemów IDS/IPS oraz mechanizmy monitorowania i zgłaszania incydentów do systemów nadrzędnych klasy SIEM. 7. Metodyka określania wektorów ataku oraz przeprowadzania testów penetracyjnych i skanowania podatności w sieciach OT. 8. Zasady analizy danych sieciowych oraz projektowanie raportów z systemów monitorujących bezpieczeństwo. 9. Zaawansowane mechanizmy i algorytmy zabezpieczania informacji cyfrowych, obejmujące podstawy kryptografii postkwantowej oraz systemy kwantowej dystrybucji klucza (QKD)	10
K	1. Praktyczny projekt i budowa przemysłowej sieci OT opartej o rozwiązania redundantne. 2. Analiza cyberbezpieczeństwa sieci OT wraz z tworzeniem i zarządzaniem politykami bezpieczeństwa. 3. Praktyczna konfiguracja i zabezpieczanie usług systemowych w sieciach przemysłowych OT. 4. Implementacja skryptów powłoki systemów operacyjnych do automatyzacji zadań administracyjnych i bezpieczeństwa. 5. Projektowanie i konfiguracja wirtualnych szyfrowanych sieci VPN dla środowiska badawczego. 6. Instalacja oprogramowania typu IDS/IPS oraz praktyczna analiza ruchu w sieciach przemysłowych OT. 7. Przeprowadzanie testów penetracyjnych i skanowania podatności na przykładzie aplikacji klasy IDS. 8. Budowanie struktury sieci OT i konfiguracja przesyłania zdarzeń do systemu SIEM za pomocą protokołu syslog. 9. Monitorowanie pracy sieci oraz automatyczne generowanie raportów bezpieczeństwa.	25

Praca własna uczestnika:

	Opis pracy własnej	Liczba godzin

PW	Studiowanie zalecanej literatury i przygotowanie do dyskusji	90

Metody dydaktyczne:

wykład problemowy oraz ćwiczenia

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.

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 2026/2027

Nazwa studiów podyplomowych: Cyberbezpieczeństwo infrastruktury transportu szynowego
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 systemów i układów sterowania procesowego

Efekty uczenia się:
EU1: Zna budowę i zasady konfiguracji układów sterowania procesowego, systemów SCADA oraz zaawansowane mechanizmy zabezpieczania informacji cyfrowej w systemach IT/OT (CITS_W01, CITS_W03, CITS_W05, CITS_W06).
EU2: Potrafi identyfikować i analizować zagrożenia oraz typowe wektory ataków na systemy i sieci sterowania (CITS_W04, CITS_U07).
EU3: Potrafi dobrać i zaimplementować adekwatne zabezpieczenia oraz mechanizmy ochrony dla systemów sterowania i wizualizacji (CITS_U01, CITS_U09, CITS_U18).
EU4: Potrafi wykrywać incydenty w systemach sterowania oraz dobrać odpowiedni rodzaj i zakres działań naprawczych (CITS_U08).
EU5: Jest przygotowany do projektowania, bezpiecznej konfiguracji, administrowania oraz dokumentowania systemów wirtualnych i usług w sieciach OT (CITS_U02, CITS_U04, CITS_U06).

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
LK	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

Praca własna uczestnika:

	Opis pracy własnej	Liczba godzin
PW	Studiowanie zalecanej literatury i przygotowanie do dyskusji	35

Metody dydaktyczne:

wykład problemowy oraz ćwiczenia

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.

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 2026/2027

Nazwa studiów podyplomowych: Cyberbezpieczeństwo infrastruktury transportu szynowego
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 urządzenia sterowania ruchem kolejowym
Nazwa przedmiotu w języku angielskim	Railway Traffic Control Systems and Devices
Kategoria przedmiotu	specjalnościowy
Liczba punktów ECTS	5
Semestry	I i II
Język wykładowy	Polski

Wymagania wstępne: Wiedza z podstaw teorii trakcji. Znajomość podstaw elektroniki i telekomunikacji.

Cele przedmiotu: Uzyskanie wiedzy z zakresu budowy i funkcjonowania układów systemów automatycznej kontroli jazdy pociągu. Poznanie zasad projektowania systemów automatycznej kontroli jazdy pociągów.

Forma zajęć, semestralna liczba godzin:

Semestr	Forma zaliczenia (E/Z)	Wykłady	Ćwiczenia	Laboratorium	Laboratorium komputerowe	Projekt	Seminarium
I		10					
II	Z	15			5		

E – egzamin; Z – zaliczenie

Efekty uczenia się:
EU1: Zna zasadę bezpiecznej jazdy pociągu oraz ogólną budowę i działanie systemów samoczynnego hamowania, automatycznego prowadzenia i automatycznej jazdy pociągu (CITS_W11).
EU2: Zna budowę i działanie systemu sterowania ETCS oraz zasady interoperacyjności i certyfikacji urządzeń infrastruktury kolejowej (CITS_W11, CITS_W12).
EU3: Potrafi przedstawić koncepcję projektową podstawowych układów automatycznej kontroli jazdy pociągu (CITS_U11).
EU4: Potrafi przedstawić koncepcję podstawowego systemu sterowania ruchem dla linii kolejowej dużych prędkości oraz wskazać podmioty odpowiedzialne za certyfikację (CITS_U12, CITS_U13).
EU5: Jest gotów do kierowania się w swojej pracy profesjonalizmem i etyką zawodową oraz realizacji działań z uwzględnieniem aspektów ekonomicznych (CITS_K01, CITS_K02).

Treści programowe (oddzielnie dla każdej formy zajęć):

Forma zajęć	Tematyka zajęć	Liczba godzin
W	Systemy samoczynnego hamowania pociągu SHP, PZB. System automatycznego prowadzenia pociągu ATC w tym podsystem ochrony pociągu ATP i podsystem automatycznej jazdy pociągu ATO. Metody transmisji informacji pomiędzy pojazdem a urządzeniami sterowania ruchem. Wybrane systemy sterowania pociągami na wydzielonych liniach kolejowych dużych prędkości. Europejski System Sterowania Pociągiem (ETCS).	25
LK	Systemy samoczynnego hamowania pociągu SHP, PZB. System automatycznego prowadzenia pociągu ATC. Europejski System Sterowania Pociągiem (ETCS).	5

Praca własna uczestnika:

	Opis pracy własnej	Liczba godzin
PW	Studiowanie zalecanej literatury i przygotowanie do dyskusji	95

Metody dydaktyczne:

wykład problemowy oraz ćwiczenia

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.

Wykaz literatury:

1. Dyduch J., Kornaszewski M. - Systemy sterowania ruchem kolejowym, Radom, 2003, WPR.
2. Dyduch J., Pawlik M - Systemy automatycznej kontroli jazdy pociągu., Radom, 2002, WPR.
3. Narkiewicz J - GPS i inne satelitarne systemy nawigacyjne, Warszawa, 2007, WKiŁ.
4. Andrzej Kochan, Paweł Wontorski - Komputerowe systemy kierowania i sterowania ruchem kolejowym. Część 1: Funkcje, elementy i układy, 2020, Oficyna Wydawnicza PW.
5. Materiały dostarczone przez prowadzącego w formie elektronicznej.
6. 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 2026/2027

Nazwa studiów podyplomowych: Cyberbezpieczeństwo infrastruktury transportu szynowego
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	Zapewnienie zgodności systemów transportu szynowego z normą IEC 62443, TS 50701 oraz IEC 63452
Nazwa przedmiotu w języku angielskim	Ensuring compliance of rail transport systems with IEC 62443, TS 50701, and IEC 63443 standards.
Kategoria przedmiotu	specjalnościowy
Liczba punktów ECTS	5
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:
EU01: zna i rozumie wymagania norm oraz standardów cyberbezpieczeństwa (IEC 62443, TS 50701, IEC 63452) oraz ich relacje z wytycznymi NIST w kontekście systemów transportu szynowego. [CITS-W13]
EU02: potrafi przeprowadzić audyt systemu pod kątem zgodności z normami oraz określić dla stref i kanałów wektory poziomów bezpieczeństwa SL-C, SL-A i SL-T. [CITS-U16, CITS-U14]
EU03: potrafi samodzielnie wykonać podział systemu na strefy i kanały oraz przeprowadzić analizę ryzyka systemu zgodnie z wymogami SuC. [CITS-U15, CITS-U07, CITS-U06]
EU04: potrafi przeprowadzić ocenę poziomu bezpieczeństwa komponentów systemu zgodnie z normą IEC 62443-4-2 oraz wyznaczyć dla nich wektory SL. [CITS-U14, CITS-U07, CITS-U06]
EU05: potrafi dobrać adekwatne techniczne i organizacyjne zabezpieczenia dedykowane dla systemów transportu szynowego. [CITS-U18, CITS-U01, CITS-U06, CITS-U07]
EU06: Student jest gotów do profesjonalnego i etycznego podejścia do oceny zgodności z normami IEC 62443, TS 50701, IEC 63452 systemów informatycznych [CITS-K01]

Forma zajęć, semestralna liczba godzin

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

Treści programowe (oddzielnie dla każdej formy zajęć):

Forma zajęć	Tematyka zajęć	Liczba godzin
W	1. Podstawy rodziny norm IEC 62443 (IEC 62443, TS 50701 oraz IEC 63452). 2. Dostosowanie normy IEC 62443 dla rynku kolejowego w postaci norm TS 50701 oraz IEC 63452. 3. Różnice między cyberbezpieczeństwem systemów IT a systemów automatyki przemysłowej (OT) i sterowania ruchem kolejowym. 4. Porównanie IEC 62443 z rodziną norm NIST (w szczególności NIST SP 800-82 oraz NIST Cybersecurity Framework). 5. Kluczowe różnice w podejściu: procesowe i horyzontalne podejście NIST vs. techniczne i certyfikowalne podejście IEC 62443 (Component-System-Process). 6. Konstrukcja normy IEC 62443 i jej cztery poziomy (General, Policies & Procedures, System, Component). 7. Zawartość dokumentu IEC 62443-1-1, który definiuje podstawową terminologię, koncepcje oraz modele dla bezpieczeństwa systemów automatyki i sterowania przemysłowego. 8. Zawartość dokumentu IEC 62443-2-1, który określa wymagania dotyczące ustanowienia i utrzymania Systemu Zarządzania Cyberbezpieczeństwem (CSMS) dla właścicieli obiektów. 9. Zawartość dokumentu IEC 62443-2-3, który skupia się na wymaganiach dotyczących procesów zarządzania poprawkami (patch management) w środowisku przemysłowym. 10. Zawartość dokumentu IEC 62443-2-4, który definiuje wymagania wobec dostawców usług i integratorów w zakresie procesów bezpieczeństwa przy wdrażaniu systemów. 11. Zawartość dokumentu IEC 62443-3-1, który dokonuje przeglądu dostępnych technologii bezpieczeństwa oraz ich przydatności dla systemów sterowania i automatyki. 12. Zawartość dokumentu IEC 62443-3-2, który ustala zasady podziału systemów na strefy oraz kanały komunikacyjne, a także opisuje metodykę oceny ryzyka. 13. Zawartość dokumentu IEC 62443-3-3, który określa techniczne wymagania bezpieczeństwa dla całego systemu oraz definiuje poziomy zapewnienia bezpieczeństwa (Security Levels). 14. Zawartość dokumentu IEC 62443-4-1, który definiuje wymagania dla producentów sprzętu i oprogramowania dotyczące bezpiecznego cyklu życia rozwoju produktu. 15. Zawartość dokumentu IEC 62443-4-2, który zawiera szczegółowe techniczne wymagania bezpieczeństwa dla poszczególnych komponentów systemu, takich jak sterowniki PLC czy urządzenia sieciowe. 16. Definicja SuC (System under Consideration) w architekturze kolejowej – co wchodzi w skład systemu taborowego, a co przytorowego. 17. Podział na strefy (Zones) i kanały (Conduits) na przykładzie komunikacji pociąg-ziemia (Train-to-Ground). 18. Typowy podział na strefy w taborze i infrastrukturze zgodnie z TS 50701/IEC 63452: strefa sterowania ruchem (TCMS/Signalling), strefa systemów bezpieczeństwa (Safety), strefa pasażerska (PIS/Wi-Fi) oraz strefa operatorska (Maintenance). 19. Metodyka oceny stref i kanałów: definiowanie granic bezpieczeństwa, inwentaryzacja przepływów danych oraz identyfikacja punktów styku (Conduit Mapping). 20. Sposoby przeprowadzania szacowania ryzyka zgodnie z TS 50701 oraz IEC 62443 (High-level vs Detailed Risk Assessment). 21. Ocena bezpieczeństwa komponentów (Component Security Assessment) – weryfikacja technicznych wymagań (FR) dla urządzeń końcowych, sieciowych i aplikacji zgodnie z normą 4-2. 22. Typologia poziomów bezpieczeństwa: różnica między poziomem docelowym (SL-T), osiągniętym (SL-A) a zdolnością systemu (SL-C). 23. Poziomy SL-1 do SL-4: charakterystyka zagrożeń od przypadkowych błędów po ataki sponsorowane przez państwa. 24. Relacja między cyberbezpieczeństwem (Security) a bezpieczeństwem funkcjonalnym (Safety/SIL) w transporcie szynowym.	15

	25. Odpowiedzialność w łańcuchu dostaw: rola Asset Owner (Przewoźnik/Zarządca), System Integrator oraz Product Supplier. 26. Proces certyfikacji urządzeń i systemów na zgodność z IEC 62443 w kontekście dopuszczenia taboru do ruchu.	
Ć	15. Zdefiniowanie SuC dla wybranego systemu 16. Wykonanie oceny ryzyka dla wybranego SuC 17. Wykonanie podziału wybranego SuC na strefy i kanały 18. Wykonanie oceny poziomów bezpieczeństwa SL-C dla wybranego systemu 19. Zaproponowanie zabezpieczeń kompensacyjnych	15

Praca własna uczestnika:

	Opis pracy własnej	Liczba godzin
PW	Studiowanie zalecanej literatury i przygotowanie do dyskusji	95

Metody dydaktyczne:

wykład problemowy oraz ćwiczenia; opcjonalnie dodatkowa wizyta studyjna u producenta systemu monitorowania cyberbezpieczeństwa onboard dla pojazdów szynowych, lub równoważna

Sposoby weryfikacji i oceny efektów uczenia się:

Wykład: zaliczenie pisemne.

Kryteria oceny:

Odpowiedzieć poprawnie na minimum 70% pytań na egzaminie

Wykaz literatury:

4. Materiały dostarczone przez prowadzącego w formie elektronicznej.
5. Normy IEC 62443 oraz TS 50701
6. Normy NIST serii 800
7. Przykładowe „IEC 62443-4-2 Conformity document” dostarczone przez prowadzącego.
8. Materiały dydaktyczne dostępne na dedykowanych serwisach internetowych.

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 Cyberbezpieczeństwo infrastruktury transportu szynowego **(CITS)**

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**
CITS-W01	zagadnienia dotyczące bezpieczeństwa informacji (danych) oraz sieci komputerowych	P6U_W	P6S_WG	P6Z_WT
CITS-W02	zaawansowane mechanizmy i algorytmy zabezpieczania informacji cyfrowych, obejmujące podstawy kryptografii postkwantowej oraz systemy kwantowej dystrybucji klucza (QKD)	P6U_W	P6S_WG	P6Z_WT
CITS-W03	zagadnienia bezpiecznej komunikacji za pośrednictwem publicznych kanałów wymiany informacji	P6U_W	P6S_WG	P6Z_WO
CITS-W04	wybrane typy zagrożeń i ataków na systemy i sieci komputerowe	P6U_W	P6S_WG	P6Z_WZ
CITS-W05	protokoły transmisji w sieciach IT oraz sieciach przemysłowych (OT)	P6U_W	P6S_WG	P6Z_WT

CITS-W06	zaawansowane mechanizmy zabezpieczeń systemów IT oraz systemów automatyki przemysłowej (OT), w tym rozwiązania IPS/IDS, SIEM, SOAR, VPN	P6U_W	P6S_WG	P6Z_WT
CITS-W07	podstawy procesu zarządzania ryzykiem dla systemów automatyki przemysłowej w oparciu o normą IEC 62443, IEC 63452 oraz NIST SP 800-37 (Risk Management Framework - RMF)	P6U_W	P6S_WG	P6Z_WZ
CITS-W08	zasady tworzenia i wykorzystania systemu zarządzania bezpieczeństwem informacji (SZBI) przedsiębiorstwie	P6U_W	P6S_WG	P6Z_WO
CITS-W09	wybrane metody przeprowadzania testów penetracyjnych, z uwzględnieniem specyfiki obszaru automatyki przemysłowej	P6U_W	P6S_WG	P6Z_WZ
CITS-W10	wymagania Dyrektywy Parlamentu Europejskiego i Rady UE 2022/2555, Ustawy o Krajowym Systemie Cyberbezpieczeństwa oraz wymagania względem dostawcy urządzeń z elementami cyfrowymi zgodnie z Rozporządzenie Parlamentu Europejskiego i Rady UE 2024/2847	P6U_W	P6S_WG	P6Z_WN
CITS-W11	zasadę bezpiecznej jazdy pociągu oraz ogólną budowę i działanie systemów samoczynnego hamowania, automatycznego prowadzenia i automatycznej jazdy pociągu, budowę i działanie systemu sterowania ETCS	P6U_W	P6S_WG	P6Z_WN
CITS-W12	zasady interoperacyjności, systemy Dyrektyw Nowego i Globalnego Podejścia, dyrektywy o interoperacyjności kolei oraz istotę Technicznych Specyfikacji Interoperacyjności a także Certyfikację taboru kolejowego i urządzeń infrastruktury	P6U_W	P6S_WG	P6Z_WN
CITS-W13	wymagania norm IEC 62443, TS 50701 oraz IEC 63452, definicję SuC, podział systemu na strefy i kanały, poziomy bezpieczeństwa, wektory bezpieczeństwa, sposoby przeprowadzania oceny systemu i komponentów zgodnie z normą IEC 62443, wzajemne relacje pomiędzy normami IEC a standardami NIST oraz ISO serii 27000	P6U_W	P6S_WG	P6Z_WN
	UMIEJĘTNOŚCI: ABSOLWENT POTRAFI	**Kod składnika opisu**	**Kod składnika opisu**	**Kod składnika opisu**
CITS-U01	wybrać oraz wykorzystać odpowiednie mechanizmy ochrony informacji cyfrowych w kontekście określonego problemu	P6U_U	P6S_UW	P6Z_UO
CITS-U02	skonfigurować i zabezpieczyć system operacyjny	P6U_U	P6S_UW	P6Z_UU
CITS-U03	przeprowadzić analizę ruchu w sieciach przemysłowych OT	P6U_U	P6S_UW	P6Z_UI
CITS-U04	skonfigurować wybrane usługi w systemach i sieciach OT	P6U_U	P6S_UW	P6Z_UU
CITS-U05	implementować skrypty powłoki systemów operacyjnych	P6U_U	P6S_UW	P6Z_UI
CITS-U06	przygotować dokumentację techniczną realizowanych rozwiązań lub projektów	P6U_U	P6S_UW	P6Z_UO

CITS-U07	wykonać analizę bezpieczeństwa środowiska IT oraz OT	P6U_U	P6S_UW	P6Z_UI
CITS-U08	wykrywać typowe ataki na systemy IT/OT oraz odpowiednio zareagować na zaistniały incydent	P6U_U	P6S_UW	P6Z_UO
CITS-U09	używać wybranych narzędzi bezpieczeństwa jak IPS/IDS, SIEM, SOAR, VPN z uwzględnieniem specyfiki systemów transportu	P6U_U	P6S_UW	P6Z_UN
CITS-U10	przeprowadzać testy penetracyjne z uwzględnieniem specyfiki systemów transportu szynowego	P6U_U	P6S_UW	P6Z_UN
CITS-U11	przedstawić koncepcję projektową podstawowych układów automatycznej	P6U_U	P6S_UW	P6Z_UN
CITS-U12	przedstawić koncepcję podstawowego systemu sterowania ruchem dla linii kolejowej dużych prędkości	P6U_U	P6S_UW	P6Z_UN
CITS-U13	przedstawić koncepcję procesu certyfikacji taboru kolejowego i urządzeń infrastruktury na terenie Unii Europejskiej oraz wybrać podmioty odpowiedzialne za certyfikację	P6U_U	P6S_UW	P6Z_UN
CITS-U14	przeprowadzić ocenę poziomu bezpieczeństwa komponentów systemu zgodnie z normą IEC 62443-4-2, określić wektory SL-C, SL-A, SL-T dla stref i kanałów	P6U_U	P6S_UW	P6Z_UN
CITS-U15	wykonać podział systemu na strefy i kanały oraz przeprowadzić analizę ryzyka systemu zgodnie z normą IEC 62443 oraz IEC 63452	P6U_U	P6S_UW	P6Z_UN
CITS-U16	przeprowadzić audyt systemu pod kątem zgodności z normą IEC 62443 oraz IEC 63452	P6U_U	P6S_UW	P6Z_UN
CITS-U17	dokonać oceny bezpieczeństwa łańcucha dostaw zgodnie z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2024/2847, Ustawy o Krajowym Systemie Cyberbezpieczeństwa oraz opisać niezbędne wymagania względem dostawcy urządzeń z elementami cyfrowymi oraz zaprojektować dokumentacje systemu zgodnie z Rozporzadzenie Parlamentu	P6U_U	P6S_UW	P6Z_UN
CITS-U18	dobrać adekwatne zabezpieczenia dla systemów transportu szynowego w oparciu o wyniki analizy ryzyka	P6U_U	P6S_UW	P6Z_UN
	KOMPETENCJE SPOŁECZNE: ABSOLWENT JEST GOTÓW DO	**Kod składnika opisu**	**Kod składnika opisu**	**Kod składnika opisu**
CITS-K01	kierowania się w swojej pracy profesjonalizmem i etyką zawodową	P6U_K	P6S_KK	P6Z_KO P6Z_KP
CITS-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
G = głębia i zakres
K = kontekst

U = umiejętności
W = wykorzystanie wiedzy
K = komunikowanie się
O = organizacja pracy
U = uczenie się

K = kompetencje społeczne
K = krytyczna ocena
O = odpowiedzialność
R = rola zawodowa

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
T = teorie i zasady
Z = zjawiska i procesy
O = organizacja pracy
N = narzędzia i materiały

U = umiejętności
I = informacje
O = organizacja pracy
N = narzędzia i materiały
U = uczenie się i rozwój zawodowy

K = kompetencje społeczne
P = przestrzeganie reguł
W = współpraca
O = odpowiedzialność

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).