Politechnika Warszawska

Załącznik nr 1
do uchwały nr 66/2019
Prezydium Polskiej Komisji Akredytacyjnej
z dnia 28 lutego 2019 r. z późn. zm.

Ocena programowa

Profil ogólnoakademicki

Raport samooceny

Nazwa i siedziba uczelni prowadzącej oceniany kierunek studiów:

Politechnika Warszawska,

Pl. Politechniki 1, 00-661 Warszawa

Nazwa ocenianego kierunku studiów: **Cyberbezpieczeństwo**

1. Poziomy studiów: **pierwszy, drugi stopień**
2. Forma studiów: **stacjonarne (oba stopnie)**
3. Nazwa dyscypliny, do której został przyporządkowany kierunek[1]
   Informatyka techniczna i telekomunikacja (100%)

W przypadku przyporządkowania kierunku studiów do więcej niż 1 dyscypliny:

Nazwa dyscypliny wiodącej, w ramach której uzyskiwana jest ponad połowa efektów uczenia się wraz z określeniem procentowego udziału liczby punktów ECTS dla dyscypliny wiodącej w ogólnej liczbie punktów ECTS wymaganej do ukończenia studiów na kierunku.

Nazwa dyscypliny wiodącej	Punkty ECTS	
	liczba	%
Informatyka techniczna i telekomunikacja (studia pierwszego stopnia)	210	100
Informatyka techniczna i telekomunikacja (studia drugiego stopnia)	90	100

Na studiach prowadzone jest kształcenie przygotowujące do wykonywania zawodu nauczyciela
☐ TAK ☒ NIE

[1]Nazwy dyscyplin należy podać zgodnie z rozporządzeniem MNiSW z dnia 20 września 2018 r. w sprawie dziedzin nauki i dyscyplin naukowych oraz dyscyplin artystycznych (Dz. U. 2018 poz. 1818).

Efekty uczenia się zakładane dla ocenianego kierunku, poziomu i profilu studiów

[1] „Odniesienie – symbol I/III" oznacza odniesienie do charakterystyk drugiego stopnia efektów uczenia się Polskiej Ramy Kwalifikacji dla profilu ogólnoakademickiego (symbol I) lub odniesienie dla kwalifikacji obejmujących kompetencje inżynierskie (symbol III) określonych Rozporządzeniem 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. z 2018r., poz. 2218) i uwzględnia odpowiednio Kod składnika charakterystyk drugiego stopnia Polskiej Ramy Kwalifikacji i określony w uchwale Senatu PW w sprawie przyjęcia przez Politechnikę Warszawską kodu składnika charakterystyk drugiego stopnia Polskiej Ramy Kwalifikacji dla kwalifikacji uzyskiwanych w ramach szkolnictwa wyższego

[2] „Odniesienie-symbol" oznacza odniesienie do uniwersalnych charakterystyk pierwszego stopnia Polskiej Ramy Kwalifikacji, określonych w załączniku do Ustawy z dnia 22 grudnia 2015 r. o Zintegrowanym Systemie Kwalifikacji (t.j. Dz. U. z 2018 r. poz. 2153, z późn. zm.)

Cyberbezpieczeństwo - Studia stacjonarne pierwszego stopnia w języku polskim

Lp.	Symbol efektu uczenia się	Efekt uczenia się	[1]Odniesienie – symbol I/III	[2]Odniesienie – symbol
[1]	*[2]*	*[3]*	*[4]*	*[5]*
		Wiedza		
		Absolwent		
1.	W01	ma wiedzę w zakresie matematyki, obejmującą logikę, teorię mnogości, analizę, algebrę, rachunek prawdopodobieństwa i statystykę matematyczną, tworzącą podstawy teoretyczne do: - opisu i analizy działania systemów przesyłania, przetwarzania i gromadzenia informacji, - opisu i analizy algorytmów przetwarzania sygnałów, w tym sygnałów dźwięku i obrazu, - opisu i analizy działania podstawowych komponentów systemów i sieci teleinformatycznych, a także podstawowych zjawisk fizycznych w nich występujących, - opisu i projektowania rozwiązań związanych z zapewnieniem cyberbezpieczeństwa systemów informacyjnych i sieci teleinformatycznych	I.P6S_WG	P6U_W.1
2.	W02	ma wiedzę w zakresie fizyki, obejmującą mechanikę klasyczną i kwantową, elektryczność i magnetyzm, optykę, fotonikę oraz elementy fizyki statystycznej i dynamiki nieliniowej, a w szczególności wiedzę: - umożliwiającą zrozumienie zjawisk fizycznych występujących w komponentach systemów i sieci teleinformatycznych,	I.P6S_WG	P6U_W.1

Lp.	Symbol efektu uczenia się	Efekt uczenia się	[1]Odniesienie – symbol I/III	[2]Odniesienie – symbol
[1]	*[2]*	*[3]*	*[4]*	*[5]*
		- umożliwiającą zrozumienie mechanizmów ataków na warstwę fizyczną systemów i sieci teleinformatycznych oraz metod ochrony przed nimi - stanowiącą podstawę do analizy i projektowania nowych metod ochrony informacji (kryptografia kwantowa) - umożliwiającą rozumienie roli i wagi generatorów zmiennej pseudolosowej dla współczesnych technik bezpieczeństwa, metod wytwarzania i oceny ciągów losowych i pseudolosowych z generatorów fizycznych i logicznych		
3.	W03	ma wiedzę w zakresie elektroniki i telekomunikacji, a także teorii systemów, obejmującą m.in.: - zasadę działania i sposób użycia podstawowych elementów i układów elektronicznych, - podstawy transmisji przewodowej, radiowej i optycznej, - podstawowe metody przetwarzania sygnałów, - własności i zastosowania podstawowych systemów liniowych i nieliniowych, tworzącą podstawy teoretyczne i metodyczne do identyfikowania problemów i formułowania specyfikacji złożonych zadań inżynierskich i problemów badawczych, związanych w szczególności z zapewnieniem cyberbezpieczeństwa oraz ich rozwiązywania	I.P6S_WG	P6U_W.1
4.	W04	ma wiedzę w zakresie techniki cyfrowej i sprzętowych komponentów systemów komputerowych i sieci teleinformatycznych, obejmującą m.in.: - podstawy techniki cyfrowej, - metody projektowania układów i systemów cyfrowych z wykorzystaniem różnych typów komponentów, - architekturę i organizację systemów komputerowych, tworzącą podstawy do projektowania warstwy sprzętowej systemów teleinformatycznych, w szczególności rozwiązań związanych z zapewnieniem cyberbezpieczeństwa tych systemów	I.P6S_WG	P6U_W.1

Lp.	Symbol efektu uczenia się	Efekt uczenia się	[1]Odniesienie – symbol I/III	[2]Odniesienie – symbol
[1]	*[2]*	*[3]*	*[4]*	*[5]*
5.	W05	ma wiedzę w zakresie oprogramowania systemów komputerowych i sieci teleinformatycznych, obejmującą m.in.: - algorytmy i techniki programowania, - metody projektowania i programowania baz danych, - usługi i aplikacje internetowe i mobilne, - komputerowe i sieciowe systemy operacyjne, tworzącą podstawy do projektowania warstwy programowej systemów teleinformatycznych, w szczególności rozwiązań związanych z zapewnieniem cyberbezpieczeństwa tych systemów	I.P6S_WG	P6U_W.1
6.	W06	ma wiedzę w zakresie teleinformatyki, obejmującą m.in.: - usługi i aplikacje, - sieci i chmury, - komutacja i routing, - sieci bezprzewodowe komórkowe, lokalne i sensorowe - sieci lokalne i sieci centrów tworzącą podstawy do projektowania komponentów sieci teleinformatycznych, w szczególności rozwiązań związanych z zapewnieniem cyberbezpieczeństwa tych sieci	I.P6S_WG	P6U_W.1
7.	W07	ma wiedzę w zakresie cyberbezpieczeństwa, obejmującą m.in. następujące zagadnienia: - bezpieczeństwo danych, - bezpieczeństwo systemów i oprogramowania, - bezpieczeństwo komunikacji, - kryminalistyka cyfrowa, - bezpieczeństwo organizacyjne, społeczne i zarządzanie cyberbepieczeństwem, tworzącą podstawy do projektowania rozwiązań związanych z zapewnieniem bezpieczeństwa systemów informacyjnych i sieci teleinformatycznych	I.P6S_WG	P6U_W.1
8.	W08	ma elementarną wiedzę na temat procesów zachodzących w cyklu życia komponentów systemu informacyjnego lub sieci teleinformatycznej oraz tych systemów i sieci	I.P6S_WG III.P6S_WG	P6U_W.1
9.	W09	ma podstawową wiedzę niezbędną do rozumienia pozatechnicznych (prawnych, ekonomicznych, etycznych i innych) uwarunkowań działalności	I.P6S_WK.2	P6U_W.2

Lp.	Symbol efektu uczenia się	Efekt uczenia się	[1]Odniesienie – symbol I/III	[2]Odniesienie – symbol
[1]	*[2]*	*[3]*	*[4]*	*[5]*
		inżynierskiej w zakresie bezpośrednio lub pośrednio związanym z cyberbezpieczeństwem		
10.	W10	ma podstawową wiedzę w zakresie ochrony własności intelektualnej, w tym ochrony własności przemysłowej i prawa autorskiego	I.P6S_WK.2	P6U_W.2
11.	W11	ma podstawową wiedzę w zakresie zarządzania i prowadzenia działalności gospodarczej; zna ogólne zasady tworzenia i rozwoju form indywidualnej przedsiębiorczości	I.P6S_WK.3 III.P6S_WK	P6U_W.2
12.	W12	rozumie fundamentalne dylematy współczesnej cywilizacji, związane zwłaszcza z rozwojem techniki	I.P6S_WK.1	P6U_W.2
Umiejętności				
		Absolwent		
1.	U01	potrafi – przy identyfikowaniu problemów i formułowaniu specyfikacji zadań inżynierskich oraz problemów badawczych, w tym zadań i problemów złożonych i nietypowych, związanych z zapewnieniem cyberbezpieczeństwa oraz ich rozwiązywaniu: - wykorzystywać posiadaną wiedzę z zakresu nauk podstawowych oraz nauk technicznych, - pozyskiwać uzupełniające tę wiedzę informacje z literatury, baz danych i innych źródeł; dokonywać ich selekcji, interpretacji i krytycznej oceny, integrować uzyskane informacje, a także wyciągać wnioski oraz formułować i uzasadniać opinie	I.P6S_UW.1 III.P6S_UW.2	P6U_U.1
2.	U02	potrafi dokonać krytycznej analizy i oceny istniejących rozwiązań w zakresie cyberbezpieczeństwa	I.P6S_UW.1 III.P6S_UW.3	P6U_U.1
3.	U03	potrafi planować i przeprowadzać eksperymenty, w tym pomiary i symulacje komputerowe, analizować i interpretować uzyskane wyniki oraz wyciągać wnioski	I.P6S_UW.1 III.P6S_UW.1	P6U_U.1
4.	U04	potrafi – przy identyfikowaniu problemów i formułowaniu specyfikacji zadań inżynierskich oraz problemów badawczych, w tym zadań i problemów złożonych i nietypowych, związanych z zapewnieniem cyberbezpieczeństwa oraz ich rozwiązywaniu – wykorzystać, również w sposób innowacyjny, metody analityczne, symulacyjne i eksperymentalne oraz odpowiednie narzędzia, dokonując właściwego wyboru tych metod i narzędzi	I.P6S_UW.1 III.P6S_UW.4	P6U_U.1

Lp.	Symbol efektu uczenia się	Efekt uczenia się	[1]Odniesienie – symbol I/III	[2]Odniesienie – symbol
[1]	*[2]*	*[3]*	*[4]*	*[5]*
5.	U05	potrafi – przy identyfikowaniu problemów i formułowaniu specyfikacji zadań inżynierskich oraz problemów badawczych związanych z zapewnieniem cyberbezpieczeństwa oraz rozwiązywaniu tych zadań – dostrzec i uwzględnić ich aspekty systemowe i pozatechniczne (ekonomiczne, społeczne, etyczne, czynnik ludzki i inne) oraz dokonać wstępnej oceny ekonomicznej proponowanych rozwiązań	I.P6S_UW.1 III.P6S_UW.2	P6U_U.1
6.	U06	potrafi wykorzystać informacje pochodzące z różnych źródeł do identyfikowania i analizy podatności i zagrożeń dla bezpieczeństwa danych, oprogramowania, poszczególnych komponentów oraz całości systemów informacyjnych i sieci teleinformatycznych	I.P6S_UW.1 III.P6S_UW.3	P6U_U.1
7.	U07	potrafi ocenić możliwości funkcjonowania systemu lub sieci w warunkach wystąpienia zagrożeń; potrafi przewidzieć skutki (techniczne, ekonomiczne, społeczne i inne) ataków stwarzających zagrożenie dla bezpieczeństwa systemów informacyjnych i sieci teleinformatycznych oraz zaproponować działania minimalizujące te skutki	I.P6S_UW.1 III.P6S_UW.3	P6U_U.1
8.	U08	potrafi – zgodnie z zadaną specyfikacją – zaprojektować, zrealizować (przynajmniej częściowo), przetestować i ocenić – ze względu na właściwie dobrany zestaw kryteriów, uwzględniający także aspekty pozatechniczne – fragment infrastruktury (sprzęt i oprogramowanie) służącej zapewnieniu bezpieczeństwa systemu informacyjnego lub sieci teleinformatycznej, używając właściwie dobranych metod i narzędzi	I.P6S_UW.1 III.P6S_UW.4	P6U_U.1
9.	U09	potrafi pracować indywidualnie i w zespole, także w zespole interdyscyplinarnym; potrafi opracować i zrealizować harmonogram prac zapewniający dotrzymanie terminów	I.P6S_UO.1 I.P6S_UO.2	P6U_U.3
10.	U10	potrafi opracować dokumentację dotyczącą realizacji zadania inżynierskiego, przygotować tekst zawierający m.in. omówienie uzyskanych wyników oraz przedstawić prezentację i uczestniczyć w dyskusji na ten temat, rzetelnie przedstawiając zalety i wady proponowanego rozwiązania	I.P6S_UK.1 I.P6S_UK.2	P6U_U.3
11.	U11	potrafi uczestniczyć w dyskusji na tematy techniczne, zwłaszcza związane bezpośrednio lub pośrednio z cyberbezpieczeństwem, dokonywać ocen przedstawianych rozwiązań i opinii	I.P6S_UK.2 III.P6S_UW.3	P6U_U.3

Lp.	Symbol efektu uczenia się	Efekt uczenia się	[1]Odniesienie – symbol I/III	[2]Odniesienie – symbol
[1]	*[2]*	*[3]*	*[4]*	*[5]*
12.	U12	posługuje się językiem angielskim w stopniu wystarczającym do porozumiewania się (poziom B2), a także czytania ze zrozumieniem dokumentacji i instrukcji obsługi narzędzi informatycznych, urządzeń sieciowych oraz podobnych dokumentów	I.P6S_UK.1 I.P6S_UK.3	P6U_U.3
13.	U13	ma umiejętność samokształcenia się, m.in. w celu podnoszenia kompetencji zawodowych	I.P6S_UU	P6U_U.2
Kompetencje Społeczne				
		Absolwent		
1.	K01	rozumie potrzebę stałego aktualizowania i wzbogacania posiadanej wiedzy – podnoszenia kompetencji zawodowych, osobistych i społecznych	I.P6S_KK.1	
2.	K02	ma świadomość ważności i zrozumienie ekonomicznych, społecznych i innych pozatechnicznych aspektów i skutków działalności inżyniera oraz związanej z tym odpowiedzialności za podejmowane decyzje i realizowane zadania; jest gotów do podejmowania decyzji i przyjmowania odpowiedzialności za skutki tych decyzji i podejmowanych działań		P6U_K.2
3.	K03	ma świadomość ważności zachowania w sposób profesjonalny, podkreślania znaczenia wiedzy w rozwiązywaniu problemów inżynierskich, przestrzegania i propagowania zasad etyki zawodowej, kształtowania etosu zawodu inżyniera	I.P6S_KK.2 I.P6S_KR	P6U_K.1
4.	K04	potrafi myśleć i działać w sposób przedsiębiorczy	I.P6S_KO.3	P6U_K.2
5.	K05	ma świadomość roli społecznej absolwenta uczelni technicznej, działania na rzecz interesu publicznego, a zwłaszcza formułowania i przekazywania społeczeństwu – m.in. poprzez środki masowego przekazu – informacji i opinii dotyczących osiągnięć techniki i innych aspektów działalności inżyniera-specjalisty w zakresie cyberbezpieczeństwa; podejmuje starania, aby przekazać takie informacje i opinie w sposób powszechnie zrozumiały	I.P6S_KO.1 I.P6S_KO.2	P6U_K.1

Cyberbezpieczeństwo - Studia stacjonarne drugiego stopnia w języku polskim

Lp.	Symbol efektu uczenia się dla programu studiów	Efekt uczenia się	[1] Odniesienie – symbol I/III	[2] Odniesienie – symbol
[1]	[2]	[3]	[4]	[5]
		Wiedza		
		Absolwent		
1.	W_01	Zna i rozumie główne tendencje rozwojowe informatyki technicznej i telekomunikacji, także w szerszym, społecznym kontekście.	I.P7S_WG.o	P7U_W
2.	W_02	Zna i rozumie podstawowe procesy zachodzące w systemach teleinformatycznych, istotne dla zapewnienia bezpiecznego funkcjonowania takich systemów.	I.P7S_WG.o III.P7S_WG	P7U_W
3.	W_03	Zna metodologiczne podstawy prowadzenia badań naukowych; ma wiedzę dotyczącą metodyki prowadzenia prac o charakterze badawczym w dziedzinie nauk inżynieryjno-technicznych, w szczególności związanych z badaniami z zakresu cyberbezpieczeństwa.	I.P7S_WG.o	P7U_W
4.	W_04	Zna zaawansowane narzędzia informatyczne niezbędne do analizy wyników badań.	I.P7S_WG.o	P7U_W
5.	W_05	Ma zaawansowaną wiedzę z zakresu matematyki, obejmującą m.in.: - metody i algorytmy algebry liniowej, - podstawy logiki temporalnej, - algorytmy kodowania i dekodowania dla liniowych kodów korekcyjnych, - podstawy teorii krat, - podstawy teoretyczne rozpoznawania wzorców, tworzącą podstawy do identyfikowania problemów i formułowania specyfikacji złożonych i nietypowych zadań inżynierskich oraz problemów badawczych, związanych z zapewnieniem cyberbezpieczeństwa oraz ich innowacyjnego rozwiązywania, dotyczących w szczególności analizy danych, weryfikacji formalnej i kryptografii postkwantowej.	I.P7S_WG.o	P7U_W
6.	W_06	W pogłębionym stopniu zna i rozumie wybrane fakty, teorie i metody, stanowiące zaawansowaną wiedzę z zakresu analizy danych w kontekście jej zastosowań w rozwiązywaniu problemów dotyczących cyberbezpieczeństwa.	I.P7S_WG.o	P7U_W
7.	W_07	W pogłębionym stopniu zna i rozumie wybrane fakty, teorie i metody, stanowiące zaawansowaną wiedzę z zakresu zapewniania bezpieczeństwa systemów Internetu Rzeczy.	I.P7S_WG.o	P7U_W

8.	W_08	W pogłębionym stopniu zna i rozumie wybrane fakty, teorie i metody, stanowiące zaawansowaną wiedzę z zakresu wybranych aspektów cyberbezpieczeństwa, w tym: - bezpieczeństwa rozwiązań sprzętowych, - bezpieczeństwa komunikacji opartej na najnowszych standardach sieci bezprzewodowych.	I.P7S_WG.o	P7U_W
9.	W_09	Zna i rozumie procesy zachodzące w cyklu życia systemów teleinformatycznych, zwłaszcza związane z zapewnieniem bezpieczeństwa tych systemów.	I.P7S_WG.o	P7U_W
10.	W_10	Rozumie fundamentalne dylematy współczesnej cywilizacji, związane z rozwojem nauk inżynieryjnotechnicznych, a zwłaszcza informatyki technicznej i telekomunikacji, oraz wykorzystaniem najnowszych osiągnięć nauki i techniki i wynikającymi z tego zagrożeniami, w szczególności osobiste i społeczne dylematy będące następstwem działań zagrażających bezpieczeństwu systemów teleinformatycznych.	I.P7S_WK	P7U_W
11.	W_11	ma podstawową wiedzę niezbędną do rozumienia pozatechnicznych (prawnych, ekonomicznych, etycznych i innych) uwarunkowań działalności zawodowej w zakresie bezpośrednio lub pośrednio związanym z cyberbezpieczeństwem.	I.P7S_WK	P7U_W
12.	W_12	ma podstawową wiedzę w zakresie ochrony własności intelektualnej, w tym ochrony własności przemysłowej i prawa autorskiego, zwłaszcza w zakresie bezpośrednio lub pośrednio związanym z cyberbezpieczeństwem.	I.P7S_WK	P7U_W
13.	W_13	zna i rozumie podstawowe zasady tworzenia i rozwoju różnych form indywidualnej przedsiębiorczości, w tym związane przedsiębiorczością startupową.	I.P7S_WK III.P7S_WK	P7U_W
Umiejętności				
		Absolwent		
1.	U_01	Potrafi pozyskiwać informacje z właściwie dobranych źródeł, dokonywać ich krytycznej oceny, analizy, syntezy i twórczej interpretacji, wyciągać wnioski i wyczerpująco je uzasadniać.	I.P7S_UW.o	P7U_U
2.	U_02	Potrafi przeprowadzić krytyczną analizę sposobu funkcjonowania istniejących rozwiązań technicznych z zakresu bezpieczeństwa systemów teleinformatycznych i oceniać te rozwiązania.	I.P7S_UW.o III.P7S_UW.o	P7U_U
3.	U_03	Potrafi planować i przeprowadzać eksperymenty / badania, w tym symulacje komputerowe dotyczące bezpieczeństwa systemów teleinformatycznych, oraz interpretować uzyskane wyniki.	I.P7S_UW.o III.P7S_UW.o	P7U_U
4.	U_04	Potrafi wykorzystać zaawansowane narzędzia informatyczne niezbędne do przeprowadzenia eksperymentów/badań związanych z zagadnieniami cyberbezpieczeństwa i analizy ich wyników.	I.P7S_UW.o	P7U_U

5.	U_05	Potrafi formułować i testować hipotezy związane z prostymi problemami badawczymi dotyczącymi m.in. zapewnienia bezpieczeństwa systemów teleinformatycznych.	I.P7S_UW.o	P7U_U
6.	U_06	Potrafi dokonać identyfikacji i sformułować specyfikację złożonych zadań dotyczących cyberbezpieczeństwa, a w szczególności: - analizy danych w kontekście jej zastosowań w rozwiązywaniu problemów związanych z zapewnieniem bezpieczeństwa systemów teleinformatycznych, - zapewniania bezpieczeństwa sieci bezprzewodowych najnowszych generacji i systemów Internetu Rzeczy.	I.P7S_UW.o	P7U_U
7.	U_07	Potrafi zaprojektować – zgodnie z zadaną specyfikacją, używając właściwie dobranych metod i narzędzi – rozwiązanie zawierające elementy innowacyjności, związane z zapewnieniem bezpieczeństwa systemów teleinformatycznych, a także zweryfikować jego poprawność.	I.P7S_UW.o III.P7S_UW.o	P7U_U
8.	U_08	Potrafi przy identyfikacji i formułowaniu specyfikacji złożonych zadań dotyczących bezpieczeństwa systemów teleinformatycznych oraz ich rozwiązywaniu: - dostrzegać ich aspekty systemowe i pozatechniczne, w tym aspekty etyczne, - oceniać aspekty ekonomiczne proponowanych rozwiązań i podejmowanych działań; Potrafi wnieść wkład w opracowanie strategii zarządzania bezpieczeństwem na poziomie instytucjonalnym.	I.P7S_UW.o III.P7S_UW.o	P7U_U
9.	U_09	Potrafi – w pracach badawczych oraz przy rozwiązywaniu zadań dotyczących zapewnienia bezpieczeństwa systemów teleinformatycznych: - wykorzystywać metody analityczne, symulacyjne i eksperymentalne, - dokonać wyboru oraz zastosować właściwe metody, techniki i narzędzia, w tym zaawansowane techniki informacyjno-komunikacyjne, - przystosować istniejące lub opracować nowe metody i narzędzia.	I.P7S_UW.o III.P7S_UW.o	P7U_U
10.	U_10	Potrafi przygotować opracowanie i przedstawić prezentację ustną, dotyczącą w szczególności zagadnień z zakresu cyberbezpieczeństwa, potrafi przygotować krótkie doniesienie naukowe.	I.P7S_UK	P7U_U
11.	U_11	Potrafi komunikować się przy użyciu różnych technik w środowisku zawodowym oraz w innych środowiskach; potrafi prowadzić debatę.	I.P7S_UK	P7U_U
12.	U_12	Potrafi posługiwać się językiem angielskim na poziomie B2+ Europejskiego Systemu Opisu Kształcenia Językowego.	I.P7S_UK	P7U_U

13.	U_13	Potrafi pracować indywidualnie oraz współdziałać z innymi osobami w ramach prac zespołowych; potrafi kierować pracą zespołu.	I.P7S_UO	P7U_U
14.	U_14	Potrafi określić kierunki dalszego uczenia się, zaplanować i zrealizować proces samokształcenia, a także ukierunkowywać innych w tym zakresie.	I.P7S_UU	P7U_U
Kompetencje społeczne				
		Absolwent		
1.	K_01	Jest gotów do krytycznej oceny posiadanej wiedzy i odbieranych treści oraz do uznawania znaczenia wiedzy w rozwiązywaniu problemów poznawczych i praktycznych oraz zasięgania opinii ekspertów w przypadku trudności z samodzielnym rozwiązaniem problemu; jest gotów do stałego aktualizowania i wzbogacania posiadanej wiedzy.	I.P7S_KK	P7U_K
2.	K_02	Jest gotów do wypełniania zobowiązań społecznych, inspirowania i organizowania działalności na rzecz środowiska społecznego oraz interesu publicznego, a zwłaszcza formułowania i przekazywania społeczeństwu – m.in. poprzez środki masowego przekazu – informacji i opinii dotyczących zagrożeń związanych z cyberbezpieczeństwem i sposobów przeciwdziałania tym zagrożeniom; podejmuje starania, aby przekazać takie informacje i opinie w sposób powszechnie zrozumiały.	I.P7S_KO	P7U_K
3.	K_03	Jest gotów do myślenia i działania w sposób przedsiębiorczy, przewodzenia grupie i ponoszenia odpowiedzialności za nią.	I.P7S_KO	P7U_K
4.	K_04	Jest gotów do odpowiedzialnego pełnienia ról zawodowych, z uwzględnieniem zmieniających się potrzeb społecznych, w tym: - rozwijania dorobku zawodu, - podtrzymywanie etosu zawodu, - przestrzegania etyki zawodowej oraz działania na rzecz przestrzegania tych zasad.	I.P7S_KR	P7U_K

Skład zespołu przygotowującego raport samooceny

Imię i nazwisko	Tytuł lub stopień naukowy/stanowisko/funkcja pełniona w uczelni
Tomasz Starecki	prof. dr hab. inż., Dziekan Wydziału Elektroniki i Technik Informacyjnych (WEiTI)
Piotr Firek	dr inż., prodziekan WEiTI ds. nauczania
Danuta Ojrzeńska-Wójter	mgr inż., zastępca dyrektora Instytutu Telekomunikacji PW ds. nauczania
Katarzyna Kamińska	dr, kierownik kierunku Cyberbezpieczeństwo
Dariusz Turlej	dr inż., Pełnomocnik Dziekana ds. międzynarodowej wymiany studentów
Andrzej Pfitzner	dr hab. inż., prof. uczelni, Pełnomocnik ds. Zapewnienia Jakości Kształcenia

Spis treści

Prezentacja uczelni

Politechnika Warszawska **(PW, https://www.pw.edu.pl/**) jest najstarszą i jedną z największych uczelni technicznych w Polsce, założoną w 1826 roku jako Szkoła Przygotowawcza, a pod obecną nazwą działa od 1915 roku, kiedy to rozpoczęła kształcenie z polskim językiem wykładowym. Po wojnie włączono do niej Szkołę Inżynierską im. H. Wawelberga i St. Rotwanda.

PW posiada status Uczelni Badawczej, a jednym z jej priorytetowych obszarów działalności naukowej jest **cyberbezpieczeństwo**. Uczelnia od lat zajmuje wysokie pozycje w rankingach uczelni technicznych w Polsce, od kilku lat zajmuje miejsce w najlepszej trójce w Rankingu Uczelni Akademickich Perspektyw. Obecnie na PW studiuje ponad 22 tysiące studentów, około tysiąca doktorantów, a kadra liczy ponad pięć tysięcy pracowników. Uczelnia oferuje kształcenie na 20 wydziałach i 50 kierunkach, w tym na studiach związanych z cyberbezpieczeństwem prowadzonych m.in. na Wydziale Elektroniki i Technik Informacyjnych, Wydziale Elektrycznym, Wydziale Mechatroniki oraz Wydziale Fizyki.

Wydział Elektroniki i Technik Informacyjnych (WEiTI, https://www.elka.pw.edu.pl/), powstały w 1951 roku i wyodrębniony z Wydziału Elektrycznego, jest największym wydziałem PW pod względem liczby studentów i pracowników. Zatrudnia ponad 350 nauczycieli akademickich, a studiuje na nim około 3000 studentów. Na Wydziale prowadzone są **studia pierwszego, drugiego a także studia podyplomowe związane z kierunkiem Cyberbezpieczeństwo.** Prowadzone jest też kształcenie doktorantów w tym zakresie. Od początku swego istnienia (studia na pierwszym stopniu rozpoczęły się w październiku 2019 r.), kierunek **Cyberbezpieczeństwo** jest jednym z najpopularniejszych kierunków studiów pod względem liczby aplikacji na jedno miejsce oraz biorąc pod uwagę liczbę aplikacji:

Rok naboru	Rekrutacja na kierunek Cyberbezpieczeństwo	
2019	31 aplikacji na miejsce	II miejsce na PW
2020	20 aplikacji na miejsce	II miejsce na PW
2021	22 aplikacje na miejsce	I miejsce na PW
2022	25 aplikacji na miejsce	I miejsce na PW
2023	21 aplikacji na miejsce	I miejsce na PW [źródło]
2024	19 aplikacji na miejsce	I miejsce na PW [źródło]

W skład Wydziału wchodzi sześć instytutów, pięć z nich jest związanych z nauczaniem na kierunku **Cyberbezpieczeństwo**: Instytut Informatyki, Automatyki i Informatyki Stosowanej, Radioelektroniki i Technik Multimedialnych, Telekomunikacji oraz Mikroelektroniki i Optoelektroniki. Instytuty funkcjonują w dwóch obiektach zlokalizowanych na terenie kampusu głównego Politechniki Warszawskiej - w Gmachu Elektroniki oraz Gmachu Elektrotechniki.

Wydział współpracuje z ponad 200 podmiotami naukowymi i komercyjnymi, zarówno krajowymi, jak i zagranicznymi.

Część I. Samoocena uczelni w zakresie spełniania szczegółowych kryteriów oceny programowej na kierunku studiów o profilu ogólnoakademickim

Kryterium 1. Konstrukcja programu studiów: koncepcja, cele kształcenia i efekty uczenia się

1.1. Powiązania koncepcji kształcenia z misją i głównymi celami strategicznymi uczelni (przy uwzględnieniu każdego z ocenianych poziomów studiów), oczekiwań formułowanych wobec kandydatów, oferowanych specjalności/specjalizacji

Koncepcja kształcenia na kierunku **Cyberbezpieczeństwo** jest zgodna z misją i wizją rozwoju **Politechniki Warszawskiej**, zawartą w Strategii Rozwoju do roku 2030 [Załącznik do uchwały nr 159/L/2021 Senatu PW z dnia 22 grudnia 2021 r., załącznik ***PW.Strategia2030***] Strategia ta koncentruje się na dążeniu, aby budować pozycję Politechniki Warszawskiej jako wiodącego ośrodka badawczo-dydaktycznego w tej części Europy. Zakłada rozwój nowoczesnych metod kształcenia, umiędzynarodowienie oferty edukacyjnej oraz silną współpracę z otoczeniem społeczno-gospodarczym. Priorytetem jest integracja dydaktyki z badaniami naukowymi, promowanie innowacji oraz dostosowanie programów kształcenia do dynamicznych potrzeb rynku pracy. Uczelnia dąży do kształcenia specjalistów gotowych sprostać globalnym wyzwaniom technologicznym i społecznym, wspierając rozwój kompetencji kluczowych dla przyszłości gospodarki opartej na wiedzy. Elementem tej wizji jest dążenie, aby Politechnika Warszawska była uczelnią, która jest krajowym liderem wprowadzania innowacji programowych i metodycznych w procesie kształcenia. Kierunek studiów w Strategii jako „kształcenie służące przygotowaniu wysoko wykwalifikowanej kadry o kompetencjach/umiejętnościach odpowiadających aktualnym i przewidywanym w przyszłości potrzebom społecznym i gospodarczym", poprzez:

– poprawę stopnia dopasowania kompetencji absolwentów do potrzeb gospodarczych i społecznych oraz kształtowanie tych potrzeb (Strategia PW do roku 2030, K1: Kształcenie uwzględniające potrzeby otoczenia społeczno-gospodarczego),

– dostosowanie wymagań programowych do standardów międzynarodowych (Strategia PW do roku 2030, K2: Nowoczesne metody nauczania),

– stworzenie studentom możliwie najlepszych warunków do studiowania, w wyniku m.in. zwiększenia wkładu studentów w kształtowanie programu i procesu dydaktycznego oraz stosowania nowoczesnych, efektywnych metod, technik i narzędzi kształcenia, a w szczególności zastępowania tradycyjnych form nauczania, opartych na przekazywaniu wiedzy (wykłady), bardziej efektywnymi metodami, kładącymi nacisk na aktywność studenta, takimi jak nauczanie zorientowane na rozwiązywanie problemów i realizację projektów (Strategia PW do roku 2030, K3: Efektywne mechanizmy projakościowe w dydaktyce).

Politechnika Warszawska dąży do uzyskania statusu europejskiego centrum kształcenia, otwartego na studentów z całego świata. Uczelnia stawia na nowoczesne i efektywne nauczanie, z dużym udziałem zajęć projektowych oraz silnym powiązaniem kształcenia z badaniami. Strategia Rozwoju PW przewiduje rozwijanie współpracy z czołowymi technicznymi uczelniami europejskimi w ramach inicjatywy Uniwersytety Europejskie jako członek konsorcjum ENHANCE, a także z najlepszymi uczelniami z innych regionów świata. Planowane jest również rozszerzenie oferty kształcenia w języku angielskim, aby przyciągnąć więcej zagranicznych studentów i umożliwić polskim studentom realizację części programu studiów na renomowanych uczelniach zagranicznych (Strategia PW 2030 K4: Integracja z europejskim systemem kształcenia akademickiego).

Zapewnienie bezpieczeństwa teleinformatycznego – bezpieczeństwa działania systemów komputerowych i sieci teleinformatycznych w warunkach różnego typu zagrożeń, których skala rośnie wraz z upowszechnieniem m.in. urządzeń mobilnych, ma obecnie krytyczne znaczenie dla

funkcjonowania różnych gałęzi gospodarki i administracji państwa, a także dla zapewnienia bezpieczeństwa użytkowników sieci publicznych.

Na rodzimym rynku pracy odczuwany jest wyraźny brak specjalistów w zakresie cyberbezpieczeństwa (bezpieczeństwa teleinformatycznego), artykułowany przez przedstawicieli różnych instytucji publicznych i podmiotów gospodarczych. Między innymi w odpowiedzi na to zapotrzebowanie, Politechnika Warszawska wskazała gospodarkę cyfrową, **cyberbezpieczeństwo**, sztuczną inteligencję, w tym uczenie maszynowe oraz Internet rzeczy (ang. Internet of Things, IoT) jako kluczowe elementy transformacji cyfrowej. Uczestnicząc w niej jako aktywny partner zmian, PW projektuje, testuje i wdraża nowe rozwiązania oraz kształci kolejne pokolenia cyfrowych innowatorów (Strategia PW do roku 2030, Strategiczne pola oddziaływania: Fundamenty naukowe: natura i aparat jej opisu). **Cyberbezpieczeństwo** wpisuje się również w jeden z siedmiu **Priorytetowych Obszarów Badawczych (POB)**, które Politechnika Warszawska zdefiniowała w ramach projektu „Inicjatywa Doskonałości – Uczelnia Badawcza" (IDUB) jako:

1. Technologie fotoniczne,
2. Sztuczna inteligencja i robotyka,
3. **Cyberbezpieczeństwo i analiza danych**,
4. Biotechnologia i inżynieria biomedyczna,
5. Technologie materiałowe,
6. Fizyka wysokich energii i technika eksperymentu,
7. Konwersja i magazynowanie energii.

Dzięki działaniom IDUB, Politechnika Warszawska prowadzi reorientację celów i metod kształcenia, aby stymulować innowacyjne i przedsiębiorcze postawy studentów oraz przygotować ich do zespołowego rozwiązywania interdyscyplinarnych problemów i prowadzenia badań. Elementy tej reorientacji obejmują upowszechnianie dobrych praktyk w zakresie innowacyjnych form i metod kształcenia, które motywują i aktywizują studentów, w tym metod opartych na realizacji projektów powiązanych z badaniami (Strategia PW do roku 2030, Nauka – cele strategiczne i operacyjne, działania, N1: Doskonałość naukowa).

1.2. Związek kształcenia z prowadzoną w uczelni działalnością naukową, w tym z głównymi kierunkami działalności naukowej prowadzonej w uczelni w dyscyplinie, do której kierunek jest przyporządkowany. Najważniejsze osiągnięcia naukowe uczelni w tym zakresie z ostatnich 5 lat będących wynikiem tej działalności, a także sposoby wykorzystania wyników działalności naukowej w opracowaniu i doskonaleniu programu studiów, jak również w procesie jego realizacji, ze szczególnym uwzględnieniem możliwości zdobywania przez studentów kompetencji badawczych i udziału w badaniach

Kształcenie na kierunku **Cyberbezpieczeństwo** na Wydziale Elektroniki i Technik Informacyjnych Politechniki Warszawskiej jest ściśle powiązane z rozwijającą się działalnością naukową uczelni w dyscyplinie informatyka techniczna i telekomunikacja **(ITT)**. O jakości prac naukowych prowadzonych przez pracowników Wydziału EITI kształcących na kierunku **Cyberbezpieczeństwo** świadczą liczne osiągnięcia naukowe, do których zaliczyć można uzyskanie tytułów profesora, stopni naukowych doktora habilitowanego oraz stopni doktora nauk technicznych.

Do osiągnięć naukowych pracowników WEiTI, które powiązane są z dyscypliną ITT, należą m.in.:

1. W obszarze rozwoju metod optymalizacji:

- Opracowanie metod optymalizacji dla bezprzewodowych sieci wieloskokowych,

- Opracowanie metod orkiestracji dla aplikacji i usług oferowanych w zrytualizowanych infrastrukturach sieciowych bazujących na technikach NFV/SDN. Projekt realizowany we współpracy z Orange i AT&T,
- Opracowanie modelu zarządzania ruchem dla Federacji Chmur Obliczeniowych: opracowanie metody strategii konstruowania Federacji oraz Metody projektowania sieci dla Federacji. Prace realizowana w ramach projektu europejskiego COST ACROSS.

2. W obszarze systemów transmisyjnych i przetwarzania sygnałów:

- Uzyskanie rekordowych szybkości transmisji z wykorzystaniem laserów 850 nm VCSEL: 54 Gbit/s na dystansie 1 km jak i 107 Gbit/s na dystansie do 100 m zakończone publikacją postdeadline,
- Opracowanie efektywnych widmowo unipolarnych impulsów do przenoszenia informacji w łączach optycznych z modulacją natężeniową światła,
- Realizacja projektu “NMKM+: Nanostrukturalne światłowody fotoniczne do kilkumodowej propagacji nowej generacji”, Program Strategiczny NCBiR "Nowoczesne technologie materiałowe" TECHMATSTRATEG,
- Opracowanie światłowodowego czujnika wibracji i deformacji bazującego na technologii światłowodów wielordzeniowych oraz macierzy VCSEL.

3. W obszarze metod uczenia maszynowego:

- Opracowanie autorskich algorytmów bazujących na metodach sztucznej inteligencji wykrywających źródła ataków, w ramach projektu “Platforma detekcji anomalii sieciowych” współfinansowanego przez NCBR (akronim PDAS, CYBERSECIDENT/369532/I/NCBR/2017),
- Opracowanie zintegrowanego systemu informatycznego wykorzystującego metody sztucznej inteligencji do automatycznej optymalizacji kandydatów na nowe leki, w ramach projektu LIDER IX finansowanego przez NCBR (akronim LEADOMISE, LIDER/36/0128/L-9/17/NCBR/2018)
- Opracowanie algorytmów rozpoznawania emocji człowieka na podstawie analizy obrazów twarzy i głosu, przedstawionych w pracy doktorskiej dr Xin Chang “Human emotion recognition from image and speech using deep neural networks” oraz związanych z nią publikacjach naukowych,
- Opracowanie algorytmów wykrywania zachowań niepożądanych na podstawie analizy sekwencji wizyjnych z systemu obserwacji i nadzoru (CCTV) zrealizowanych w wyniku realizacji projektu badawczego: “Inteligentny system wspomagania decyzji oparty na algorytmicznej analizie obrazu w działaniach służb wymiaru sprawiedliwości” finansowanego przez NCBiR.

4. W obszarze sieci nowych generacji i nowych technik sieciowych:

- Opracowanie rozwiązania P4rt-OVS - programowalnego przełącznika SDN pozwalającego programowo definiować i rekonfigurować warstwę przekazu danych programowych przełączników działających w centrum danych lub chmurach telekomunikacyjnych. Projekt wykonany został we współpracy z Orange Labs,
- Opracowanie rozwiązań w obszarze mobilnych sieci piątej generacji (5G), w tym obejmujących zagadnienia dotyczące zapewnienia bezpieczeństwa. W szczególności opracowanie: 1) planu oszacowania zagrożeń występujących w sieci 5G w Polsce i w Europie, 2) specyfikacji testów rdzenia sieci 5G oraz rozwiązań wertykalnych. Wyniki testów prac były prezentowane na

konferencji Mobile World Congress'21 (45 tys. uczestników), oraz 3) schematów certyfikacji sieci 5G dla Europejskiej Agencji Cyberbezpieczeństwa (ENISA). Wyniki tych prac były podstawą nawiązania współpracy międzynarodowej (w ramach projektów z US oraz EU), a także opublikowanie ~15 prac w renomowanych czasopismach i konferencjach,

- Opracowanie sondy ruchu zbiorczego do wykrywania ataków typu DDoS kierowanych do dostarczycieli usług przyłączonych do sieci. Prace realizowano w ramach projektu pt. „TAMA: Skalowalne i wydajne rozwiązanie programistyczne chroniące sieci operatorskie przed atakami typu DDoS (Distributed Denial of Service)" realizowanego wspólnie z firma Exatel S.A., współfinansowanego przez NCBiR w ramach programu "CyberSecIdent – Cyberbezpieczeństwo i e-Tożsamość" (2018-2019),
- Opracowanie systemu MEC (Multi-access Edge Computing) umożliwiającego migrację aplikacji na brzeg sieci w otoczenie użytkownika, obejmujące architekturę, algorytmy orkiestracji i zarządzania rozproszoną, wirtualną infrastruktura obliczeniową. Rozwiązanie zostało opracowane we współpracy z Instytutem Łączności, Poznańskim Centrum Superkomputerowo-Sieciowym, Politechniką Gdańską i DGT.

5. W obszarze cyberbezpieczeństwa:

- Kompleksowa analiza potencjalnych ukrytych kanałów w modelu publikowania subskrybentów w protokole telemetrycznego transportu kolejkowania wiadomości (MQTT), szeroko stosowanym w środowiskach Internetu rzeczy (IoT).
- Opracowanie zaawansowanego laboratorium kryminalistyki śledczej we współpracy z NASK, w ramach projektu współfinansowanego przez NCBR (akronim FORENSICS, CyberSecIdent 369234/I/NCBR/2017)
- Opracowanie laboratorium badania podatności stacjonarnych i mobilnych urządzeń informatycznych oraz algorytmów i oprogramowania we współpracy z NASK, w ramach projektu współfinansowanego przez NCBR (akronim LaVa, CyberSecIdent 488240/IV/NCBR/2021)
- Opracowanie systemu wspomagania detekcji i obrazowania ataków APT (Advanced Persistent Threat) we współpracy z ComCERT S.A. i Cryptomage S.A., w ramach projektu współfinansowanego przez NCBR (akronim DAPT, CYBERSECIDENT/488393/IV/NCBR/2021)
- Opracowanie biblioteki algorytmów detekcji anomalii i cyberzagrożeń w sieciach IoT w podziemnych zakładach górniczych (DetIoT) w ramach projektu Centrum monitorowania instalacji przemysłowych w podziemnych zakładach górniczych i wykrywania cyberzagrożeń (Program Operacyjny Inteligentny Rozwój 2014-2020, współfinansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego oraz NCBR (POIR.01.01.01-00-0180/22-00)

W aspekcie tematyki cyberbezpieczeństwa, badania prowadzone na Wydziale, koncentrują się takich zagadnieniach jak analiza/wykrywanie cyberzagrożeń, zarządzanie incydentami, zastosowanie sztucznej inteligencji w detekcji anomalii i reagowaniu na incydenty bezpieczeństwa; kryminalistyka cyfrowa, informatyka śledcza; systemy zdecentralizowane i agentowe; zagadnienia CTI (ang. Cyber Threat Intelligence), metody proaktywnej identyfikacji cyberzagrożeń (TH, ang. Threat Hunting), budowa i optymalizacja systemów cyberbezpieczeństwa oraz zarządzanie cyberbezpieczeństwem; rozwiązania chmurowe, w tym zabezpieczenie infrastruktury, bezpieczeństwo danych, projektowanie rozwiązań chmurowych; bezpieczeństwo sieci 5G+/6G, bezpieczeństwo chmury obliczeniowej oraz bezpieczeństwo sztucznej inteligencji w aspektach sieciach mobilnych następnej generacji;

projektowanie, prototypowanie i realizacja programowo-sprzętowych systemów przetwarzania informacji w obszarach cyberbezpieczeństwa, kryptografii/kryptoanalizy, radia definiowanego programowo (SDR, ang. Software-Defined Radio), wysokowydajnego przetwarzania (HPC, ang. High-Performance Computing), zastosowanie technik MTD (ang. Moving Target Defence), NFV (ang. Network Functions Virtualisation) i SDN (ang. Software Defined Networking) w obszarze cyberbezpieczeństwa; zastosowanie nowoczesnych koncepcji TEE (ang. Trusted Execution Environment) oraz HRoT (ang. Hardware Root of Trust) do realizacji mechanizmów cyberbezpieczeństwa w rozwiązaniach IoT, SmartCity, Industry 4.0, cyberbezpieczeństwo systemów i sieci IT/OT/IoT; analiza, wykrywanie, zwalczanie, zapobieganie i ograniczanie skutków dezinformacji. Ludzki wymiar cyberbezpieczeństwa – manipulacja, inżynieria społeczna, biały wywiad (OSInt), bezpieczeństwo operacyjne (OpSec); aspekty bezpieczeństwa sieci 5G i 5G MEC, metody detekcji i ochrony aplikacji webowych, cyberbezpieczeństwo ofensywne, w tym wykorzystanie metod sztucznej inteligencji w cyberbezpieczeństwie ofensywnym. Wraz z rosnącym znaczeniem badań o charakterze interdyscyplinarnym prowadzone są też badania w obszarze cyberbiobezpieczeństwa, w tym opracowywanie metod bio-inspirowanych w identyfikacji cyberzagrożeń, bezpieczeństwo informacji biologicznej oraz metody sztucznej inteligencji w aplikacjach cyberbiobezpiczeństwa. Pozyskiwane projekty badawcze związane z cyberbezpieczeństwem stanowią gwarancję odpowiedniej tematyki i jakości projektów prac dyplomowych realizowanych przez studentów. Równocześnie, badania obejmują zarówno teoretyczne podstawy, jak i ich praktyczne wdrożenia, co pozwala studentom na zdobywanie kompleksowej wiedzy i umiejętności.

Pracownicy WEiTI kształcący na kierunku **Cyberbezpieczeństwo** prowadzą wysokiej jakości prace badawcze i badawczo-rozwojowe, w ramach których, w analizowanym okresie:

– powstało łącznie 3820 publikacji (książek, monografii, artykułów w czasopismach recenzowanych) i 330 materiałów konferencyjnych; wśród publikacji znalazły się pozycje w najbardziej prestiżowych czasopismach (za 200 pkt wg punktacji ministerialnej), m.in. Nature, IEEE Transactions on Industrial Electronics, IEEE Transactions on Power Electronics, Physical Review Letters, Measurement, Sensors and Actuators B – Chemical, IEEE Robotics and Automation Letters,

– uzyskano 142870 punktów ministerialnych w ramach dyscypliny **informatyka techniczna i telekomunikacja**,

– realizowane są (lub były) 432 projekty badawczo-rozwojowe, z czego rozpoczęto 350 nowych grantów naukowo-badawczych i zewnętrznych prac zleconych, w tym:

- 50 grantów finansowanych przez NCBiR,
- 55 grantów finansowanych przez Ministerstwo Edukacji i Nauki,
- 35 grantów w ramach projektów Unii Europejskiej,
- 25 grantów w ramach funduszy strukturalnych,
- 4 granty w ramach Krajowego Planu Odbudowy,
- 65 grantów NCN,

– zgłoszono lub uzyskano prawa ochronne (patent) dla 160 wynalazków, w tym patenty krajowe, patenty zagraniczne (USA, europejskie PCT, oraz o jednolitym skutku prawnym), oraz topografie,

– realizowana jest międzynarodowa współpraca z ośrodkami takimi jak m.in.: European Organization for Nuclear Research (CERN), Foundation for Fundamental Research on Matter, Istituto Nazionale di Fisica Nucleare, GSI Helmholtz Centre for Heavy Ion Research GmbH, Université Clermont Auvergne, DESY Deutsches Elektronen – Synchrotron, ESA European Space Agency, European Spallation Source ERIC, Fraunhofer Institute, Lund University, University of Cambridge, University of Tokyo, National Taiwan University of Science and Technology, Oxford University, Rice University, Houston, Texas, Xi'an

Jiaotong University, University of Western Australia, Politecnico di Bari, Electronics and Telecommunications Research Institute.

1.3. Zgodność koncepcji kształcenia z potrzebami otoczenia społeczno-gospodarczego oraz rynku pracy, roli i znaczenia interesariuszy wewnętrznych i zewnętrznych w procesie opracowania koncepcji kształcenia i jej doskonalenia

Do badań identyfikujących potrzeby otoczenia społeczno-gospodarczego i rynku pracy oraz opisujących sylwetki absolwenta, zrealizowanych w okresie 2020-2024, zaliczyć należy:

- Czym jest sukces dla absolwentów Politechniki Warszawskiej? Analiza wyników badania (2020.20)
- Jak osiągnąć sukces? Diagnoza czynników sukcesu absolwentów Politechniki Warszawskiej (2020.21)
- Kariera w 4 zdaniach. Analiza wypowiedzi absolwentów Politechniki Warszawskiej (2020.22)
- Przypadek czy ciężka praca – co wpłynęło na sukces absolwentów PW? (2020.23)
- Wpływ środowiska rodzinnego na wybory edukacyjne absolwenta PW (do czasu podjęcia studiów) oraz odniesiony przez niego sukces (2020.24)
- Sylwetki zawodowe absolwentów PW (2020.25)
- Sylwetki zawodowe absolwentek PW (2020.27)
- Rynek pracy na Mazowszu w kontekście kształcenia na uczelni technicznej 2021 (2021.81)
- Rynek pracy na Mazowszu w kontekście kształcenia na uczelni technicznej 2019-2022 (2022.45)
- Rynek pracy na Mazowszu w kontekście kształcenia na uczelni technicznej 2022 (2022.46)
- Monitoring trendów edukacyjnych – Jak kształcić na potrzeby gospodarki opartej na innowacjach (2021.59)
- Diagnoza bieżących i perspektywicznych kierunków prac badawczo-rozwojowych. Analiza zagadnienia w kontekście modyfikacji programów kształcenia (2022.44)
- Monitoring Karier Zawodowych Absolwentów Politechniki Warszawskiej (2020.01)
- Absolwenci Wydziału Elektroniki i Technik Informacyjnych Politechniki Warszawskiej (2020.05)
- Pracodawca dla inżyniera 2021 (2021.18)
- Pracodawca dla inżyniera 2023 (2023.16)

Szczegółowe założenia badań społecznych realizowanych na Politechnice Warszawskiej na potrzeby identyfikacji potrzeb otoczenia społeczno-gospodarczego przedstawione zostały w publikacji Potrzeby otoczenia społeczno-gospodarczego Uczelni – czym są i jak je badać? (2022.55)

Najnowszy raport Global Cybersecurity Outlook (Joshi et al., 2025) zwraca uwagę, że aż 67% organizacji wskazuje na istotne braki kadrowe w obszarze cyberbezpieczeństwa (ang. moderate-to-critical skills gap). Tylko 14% deklaruje zabezpieczenie kadrowe obszarów związanych z cyberbezpieczeństwem. Co ważne, między pomiarem z 2024 a 2025 roku zanotowano wzrost deklarowanej przez firmy luki kompetencyjnej w obszarze cyberbezpieczeństwa o 8%.

W ramach inicjatywy World Economic Forum Bridging the Cyber Skills Gap opracowano osobny raport definiujący braki kadrowe w obszarze cyberbezpieczeństwa (Strategic Cybersecurity Talent Framework) (Esi Alorvor et al., 2024). Wśród obszarów technicznych, w których swobodnie powinni poruszać się zatrudniani kandydaci, wskazano na zabezpieczenia sieci, szyfrowanie, testy penetracyjne oraz reagowanie na incydenty. Kompetencje i umiejętności cenione na rynku pracy obejmują też rozwiązania chmurowe (zabezpieczenie infrastruktury, bezpieczeństwo danych, projektowanie rozwiązań chmurowych). Badanie wyróżnia obszary, które będą w najbliższym czasie najbardziej pożądane przy zatrudnianiu, są to m.in. ocena ryzyka i zarządzanie ryzykiem, inżynieria bezpieczeństwa, kompetencje z obszaru GRC (ang. governance, risk management and compliance) oraz uczenie maszynowe i sztuczna inteligencja (ML/AI). Wskazano także obszar kompetencji

nietechnicznych, gdzie poza umiejętnościami komunikacji, pracy w grupie i zarządzaniem ryzykiem, pojawiły się też: przywiązywanie uwagi do detali oraz umiejętność wyjaśniania złożonych problemów. Wśród doświadczeń praktycznych, na które mogą zwracać uwagę pracownicy działów rekrutacji są m.in. bezpośrednie doświadczenia w rozwiązywaniu rzeczywistych problemów z cyberbezpieczeństwem, ale też np. udział w konkursach technicznych w tym obszarze. Nie bez znaczenia jest motywacja i chęć do rozwoju (w tym adaptacja do nowych zagrożeń).

Badania 2024 ISC2 Cybersecurity Workforce Study potwierdzają lukę kompetencyjną. Mimo wzrostu zapotrzebowania na wzmocnienie zabezpieczeń, pracodawcy ograniczają zatrudnienie i rozwój zespołów ds. cyberbezpieczeństwa. Aż 60% badanych wskazuje, że luki utrudniają zapewnienie bezpieczeństwa organizacji. W Stanach Zjednoczonych luki kadrowe w obszarze cyberbezpieczeństwa są tak duże, że powstała mapa zapotrzebowania na ekspertów Cyberseek, w której dane można filtrować po sektorze, kategorii pracy i certyfikatach, w podziale na stany, z informacją o liczebności otwartych stanowisk.

Przy opracowaniu programu studiów I stopnia wykorzystano opinie zebrane z kilkunastu instytucji z otoczenia społeczno-gospodarczego, zainteresowanych zatrudnieniem absolwentów tych studiów (badanie przeprowadzono w 2018 r.): Asseco, Centralne Laboratorium Kryminalistyczne Policji, CERT Polska, Cryptomage, IBM, KPMG, Narodowe Centrum Kryptologii, Orange, PKO BP, Play, T-Mobile, VT Cyber, WB Electronics. Przykładowe wyniki tych badań, dotyczące oczekiwanych kompetencji absolwenta, przedstawiono w Tabeli 1.1 i 1.2. Kompetencje zostały uszeregowane według istotności dla potencjalnego pracodawcy.

Tabela 1.1. Zestawienie oczekiwanych kompetencji absolwenta w kategorii "Wiedza"

WIEDZA	Średnia	Mediana	Odchylenie standardowe
Sieci teleinformatyczne	8,6	8,0	1,0
Logika	8,1	8,0	1,8
Architektura systemów informatycznych	7,9	8,0	1,5
Protokoły komunikacyjne	7,7	8,0	1,9
Sieci telekomunikacyjne	7,1	7,5	1,7
Sztuczna inteligencja	6,9	7,0	1,3
IoT, embedded devices	6,8	7,0	1,3
Programowanie C/C++/C#/Java	6,7	7,0	2,0
Bazy danych	6,3	6,0	1,6
Zarządzanie projektami	5,3	5,0	1,5
Etyka	5,2	5,5	2,8
Układy cyfrowe	5,1	5,5	2,2
Technika mikroprocesorowa	5,1	5,0	2,1

Tabela 1.2. Zestawienie oczekiwanych kompetencji absolwenta w kategorii "Kompetencje miękkie"

KOMPETENCJE MIĘKKIE	Średnia	Mediana	Odchylenie standardowe
Uczciwość	9,8	10,0	0,6
Uczenie się	9,3	10,0	1,0
Zaangażowanie	9,1	10,0	1,2
Inicjatywa	8,6	9,0	1,4
Troska o jakość	8,6	8,5	1,6
Współpraca	8,4	8,0	1,2
Innowacyjność	8,1	8,0	1,3

Organizowanie pracy własnej	8,0	8,0	0,6
Adaptacja	8,0	8,0	2,0
Orientacja na cele	7,8	7,5	1,6
Radzenie sobie ze stresem	7,7	8,0	1,7
Komunikacja ustna	7,2	8,0	1,6
Orientacja na klienta	7,0	7,0	1,9
Komunikacja pisemna	7,0	6,5	1,8
Wpływ na innych	5,7	5,5	2,2
Wrażliwość międzykulturowa	4,4	4,0	2,5

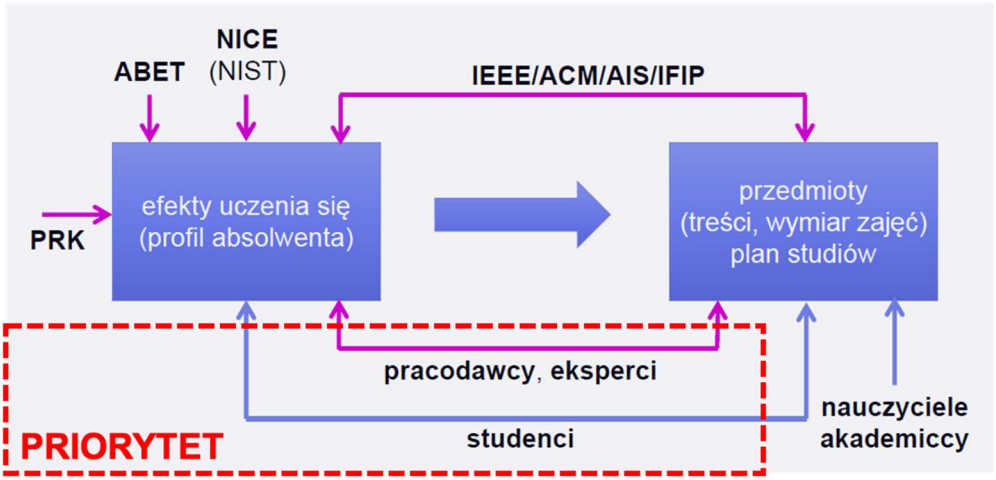
Bezpośredni udział w pracach programowych wzięła ponadto grupa najwyższej klasy ekspertów z zakresu cyberbezpieczeństwa (podane afiliacje dotyczą okresu prac nad programem):

- dr inż. Andrzej Bartosiewicz: Dyrektor dr. infrastruktury krytycznej i cyberbezpieczeństwa, Thales Polska,
- Robert Kośla: Dyrektor Departamentu Cyberbezpieczeństwa w Ministerstwie Cyfryzacji (poprzednio dyrektor sektora bezpieczeństwa narodowego i obronności na region Europy Środkowej i Wschodniej w Microsoft Europe),
- Mirosław Maj: prezes Fundacji Bezpieczna Cyberprzestrzeń, wiceprezes zarządu ComCERT SA,
- prof. Ewa Niewiadomska-Szynkiewicz: Zastępca Dyrektora NASK do Spraw Naukowych.

W pracach programowych – w całym 10-miesięcznym okresie ich trwania – uczestniczyli studenci delegowani przez Wydziałową Radę Samorządu. Ich udział w tych pracach nie ograniczał się do opiniowania propozycji przedstawianych przez kadrę akademicką – opierając się na doświadczeniach wynikających z pracy zawodowej oraz uczestnictwa w programach międzynarodowej wymiany studentów (ERASMUS+, ATHENS) studenci przedstawiali konkretne propozycje dotyczące pożądanych treści programowych, wykorzystywanych narzędzi (w tym języków programowania i narzędzi programistycznych) oraz form realizacji zajęć. Przekazywali opinie dotyczące m.in. mankamentów obecnie prowadzonych programów studiów i postulaty dotyczące pożądanych (i – co równie ważne – niepożądanych) treści i form kształcenia. Propozycje te wpłynęły w znacznym stopniu na ostateczny kształt programu, co stanowiło przykład skutecznego wdrożenia szeroko opisywanej w literaturze koncepcji współdziałania kadry akademickiej i studentów w procesie kształtowania oferty edukacyjnej, stanowiącej jedną z najlepszych metod doskonalenia jakości kształcenia.

W procesie projektowania zespół koordynujący (pracownicy + studenci) odbywał regularne spotkania (co ok. 2 tygodnie przez ok. 10 miesięcy) – z każdego spotkania sporządzano notatkę. Repozytorium prac zespołu (z wykorzystaniem chmury) zawierające pełną dokumentację tych prac, było w znacznej części otwarte dla społeczności Wydziału.

Można stwierdzić, że program powstał we współpracy ze wszystkimi istotnymi interesariuszami, przy czym jako podstawową zasadę w pracach programowych przyjęto, że opracowany program ma odpowiadać przede wszystkim potrzebom i interesom odbiorców (studentów i pracodawców), a w mniejszym stopniu – interesom kadry nauczającej. To podejście do projektowania programu studiów I stopnia zilustrowano na Rys. 1.1



Rys. 1.1 Schemat podejścia do projektowania programu studiów pierwszego stopnia na kierunku **Cyberbezpieczeństwo**

1.4. Sylwetka absolwenta, przewidywanych miejsc zatrudnienia absolwentów

Absolwent studiów na kierunku **Cyberbezpieczeństwo** ma ogólną wiedzę i umiejętności, m.in. z zakresu matematyki, informatyki, telekomunikacji i elektroniki, niezbędne do kształtowania specjalistycznych kompetencji w zakresie cyberbezpieczeństwa oraz umożliwiające pogłębianie i uzupełnianie tych kompetencji wraz z rozwojem technologii i innymi zmianami zachodzącymi w sferze gospodarczo-społecznej.

Potrafi wykorzystać nabyte kompetencje do rozwiązywania problemów z zakresu cyberbezpieczeństwa, a w szczególności zadań dotyczących:

- wykorzystywania informacji pochodzących z różnych źródeł do identyfikowania i analizowania podatności i zagrożeń dla bezpieczeństwa danych, systemów informacyjnych i sieci teleinformatycznych,

- projektowania, realizowania, testowania i utrzymania infrastruktury (sprzętu i oprogramowania) służącej zapewnieniu bezpieczeństwa systemów i sieci teleinformatycznych,

- reagowania na sytuacje wymagające interwencji w celu przeciwdziałania zaistniałym lub spodziewanym atakom, stwarzającym zagrożenie dla bezpieczeństwa systemów i sieci teleinformatycznych, w sposób minimalizujący skutki tych ataków.

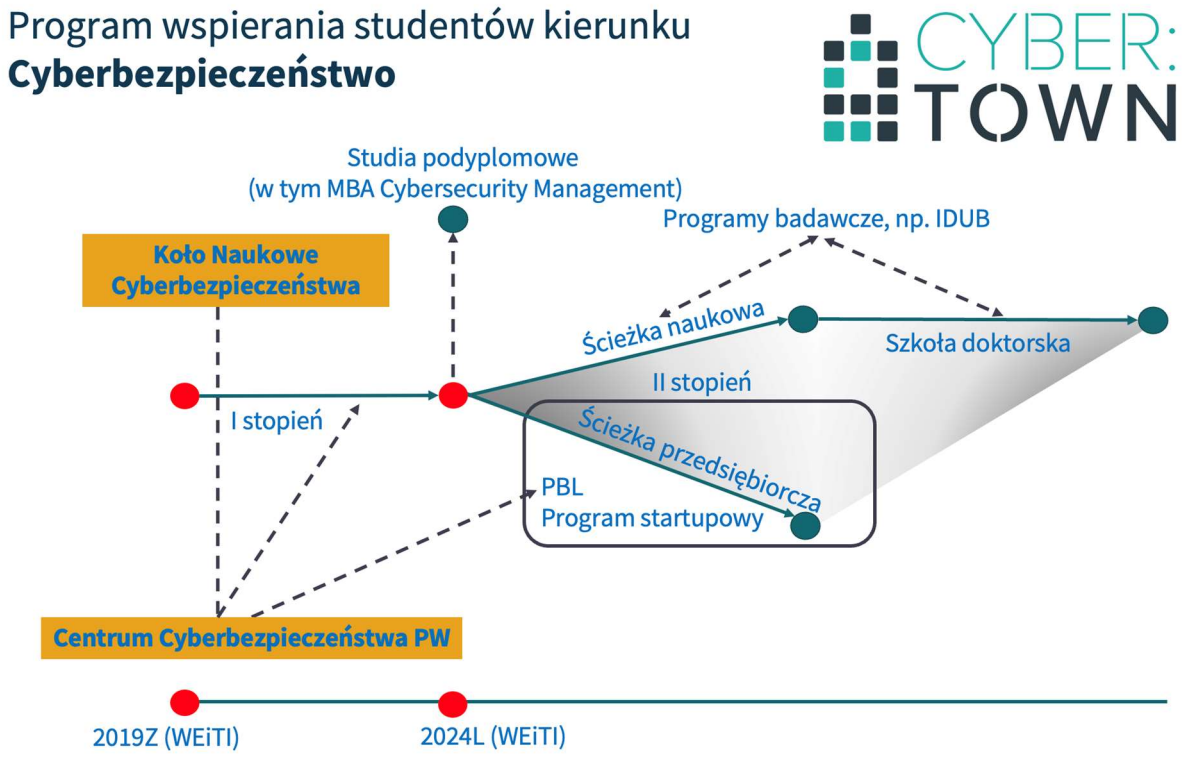
Posiadając także wiedzę z zakresu zagadnień ogólnospołecznych (m.in. prawa, zarządzania, socjologii, etyki) oraz umiejętności interpersonalne, potrafi pracować w zespole interdyscyplinarnym i współpracować z osobami odpowiedzialnymi za bezpieczeństwo funkcjonowania dużych instytucji/organizacji oraz infrastruktury krytycznej państwa.

Jest przygotowany do pracy w firmach tworzących rozwiązania informatyczne (sprzęt i oprogramowanie) o odpowiednim poziomie bezpieczeństwa oraz specjalistyczne rozwiązania służące zapewnieniu bezpieczeństwa systemów i sieci teleinformatycznych. Może też pracować w firmach/instytucjach o różnym profilu działalności, wykorzystujących nowoczesne rozwiązania informatyczne, w szczególności – w instytucjach sektora finansowego, administracji publicznej, a także w instytucjach zajmujących się różnymi aspektami bezpieczeństwa państwa.

Ma świadomość roli społecznej absolwenta uczelni technicznej, a zwłaszcza rozumie potrzebę formułowania i przekazywania społeczeństwu, w szczególności poprzez środki masowego przekazu, informacji i opinii dotyczących osiągnięć techniki i innych aspektów działalności technicznej.

1.5. Cechy wyróżniające koncepcję kształcenia oraz wykorzystanych wzorców krajowych lub międzynarodowych

Wzorem uczelni zagranicznych, rozpoczynając studia na kierunku **Cyberbezpieczeństwo**, student zostaje włączony w spójny ekosystem naukowo-dydaktyczny **Cyber:Town** (Rys. 1.2), którego celem jest wspieranie kształtowania ścieżki naukowej i przedsiębiorczej przyszłych specjalistów w dziedzinie cyberbezpieczeństwa.



Rys. 1.2. Program wspierania studentów kierunku **Cyberbezpieczeństwo** w ramach spójnego otoczenia naukowo-dydaktyczny **Cyber:Town**

Cyber:Town obejmuje:

- studia I stopnia na kierunku **Cyberbezpieczeństwo**,
- studia II stopnia na kierunku **Cyberbezpieczeństwo**,
- studia podyplomowe **Inżynieria Cyberbezpieczeństwa**,
- studia podyplomowe **MBA Cybersecurity Management**

i zakłada współpracę z otoczeniem społeczno-gospodarczym.
W ekosystemie **Cyber:Town** istotne role pełnią:

- **Koło Naukowe Cyberbezpieczeństwa** będące pierwszym polem doświadczeń dla osób wykazujących zainteresowania badaniami w zakresie cyberbezpieczeństwa **oraz**
- **uczelniane Centrum Cyberbezpieczeństwa,** w którym studenci mogą realizować staże zajmując się bezpieczeństwem teleinformatycznym PW.

Modelowy plan studiów dla kierunku **Cyberbezpieczeństwo** na pierwszym i drugim stopniu zamieszczono w załącznikach ***2.1.PlanMod1***, ***2.1.PlanMod2***. Każdy student – w ramach indywidualizacji toku studiów – może realizować ten plan w wybrany przez siebie sposób, zapewniający spełnienie wymagań programowych i rejestracyjnych, m.in. przez wybór przedmiotów obieralnych oraz regulowanie tempa studiowania (liczby i zestawu przedmiotów realizowanych na poszczególnych semestrach).

Studia realizowane są wg jednolitego programu (bez specjalności), ale bogata oferta przedmiotów obieralnych (możliwość korzystania z pełnego zestawu przedmiotów prowadzonych na Wydziale), możliwość korzystania z oferty innych wydziałów i innych uczelni, możliwość wyboru tematyki pracy dyplomowej oraz możliwość wyboru miejsca odbywania praktyki umożliwiają studentom konstruowanie indywidualnych ścieżek kształcenia ukierunkowanych na wybraną grupę zagadnień z zakresu cyberbezpieczeństwa, przykładowo:

- bezpieczeństwo danych,
- bezpieczeństwo sprzętowych komponentów systemów komputerowych i sieci teleinformatycznych,
- bezpieczeństwo oprogramowania,
- bezpieczeństwo komunikacji,
- kryminalistyka cyfrowa,
- zarządzanie cyberbepieczeństwem.

Zestaw kompetencji absolwenta (efektów uczenia się) oraz zestaw zasadniczych treści zawartych w programie studiów prowadzącym do uzyskania tych kompetencji opracowano korzystając m.in. z następujących materiałów wyznaczających światowe standardy w tym zakresie:

– raportu National Initiative for Cybersecurity Education (NICE): Cybersecurity Workforce Framework, opracowanego przez National Institute of Standards and Technology, August 2017. Raport ten zawiera szczegółową charakterystykę pełnego spektrum zróżnicowanych profili/ról zawodowych i związanych z nimi kompetencji (wiedzy i umiejętności) osób kształconych w tym zakresie,

– raportu Cybersecurity Curricula 2017, opracowanego przez Joint Task Force on Cybersecurity Education: Association for Computing Machinery (ACM), IEEE Computer Society (IEEE-CS), Association for Information Systems Special Interest Group on Information Security and Privacy (AIS SIGSEC), International Federation for Information Processing Technical Committee on Information Security Education (IFIP WG 11.8), December 2017.

Wzięto również pod uwagę efekty uczenia się (ang. student outcomes), określone w kryteriach akredytacji przyjętych przez *Accreditation Board for Engineering and Technology* (USA). W procesie przygotowywania się do opracowania programu studiów dokonano analizy literatury dotyczącej kształcenia w zakresie cyberbezpieczeństwa (głównie materiałów o charakterze przeglądowym) oraz kilku programów oferowanych przez uczelnie zagraniczne. W szczególności wykorzystano pełną dokumentację programu studiów „Cyber Security Engineering", prowadzonego od roku 2014 w Volgenau School of Engineering, George Mason University, USA.

Międzynarodowe doświadczenia dydaktyczne w zakresie cyberbezpieczeństwa związane są także z udziałem pracowników Wydziału w realizacji projektu PaRIS (Partnership in Information Security) finansowanego z programu Erasmus+, w którym partnerami PW są University of Luxembourg - Faculty of Sciences, University of Lisbon oraz National Technical University of Ukraine "Kyiv Polytechnic Institute". W ramach tego projektu przygotowywane zostały: *International Joint Master's Programme in Information Security* oraz 5-dniowy *Intensive Study Programme in Information Security*.

Jeszcze przed rekrutacją na studia, **Cyber:Town** zaprasza przyszłych studentów do pierwszego zetknięcia z uczelnią, rekonesansu tematyki studiów, poznania kadry dydaktycznej, członków Koła Naukowego Cyberbezpieczeństwa oraz reprezentantów studentów kierunku (na poziomie różnych semestrów), w ramach wydarzenia **Drzwi Otwarte PW [https://cyber.elka.pw.edu.pl]**. Zgodnie z wynikami ankiet przeprowadzonych wśród studentów pierwszego semestru kierunku **Cyberbezpieczeństwo** (w semestrze 24Z), ponad 20% z nich wzięło udział we wspomnianym wydarzeniu.

Po rozpoczęciu pierwszego semestru studenci wprowadzani są w zasady funkcjonowania Uczelni, Wydziału oraz specyfikę studiowania w ramach serii spotkań prowadzonych przez **przedstawicieli Wydziałowej Rady Samorządu WEiTI** (**Samorząd Studentów Politechniki Warszawskiej**). W trakcie początkowej orientacji na Uczelni studenci uzyskują również dostęp do przewodnika online **StarterPW**, który pomaga lepiej poznać Politechnikę Warszawską, studenckie prawa i obowiązki oraz wykorzystywane w toku nauczania systemy informatyczne. Przewodnik podzielony jest na część interaktywną i opisową, a dostępny jest poprzez uczelnianą platformę dydaktyczną **LeON PW**. W nawigacji wewnątrz uczelnianych budynków wspiera studentów dedykowana aplikacja **PW Navi** (dostępna w Google Play i Apple Store), która pomaga w lokalizacji w pięciu wybranych budynkach PW (Gmach Główny, Gmach Elektroniki, Gmach Fizyki, Budynek Rektorska 4, budynek Centrum Analiz Geoprzestrzennych i Satelitarnych). Cechą szczególną aplikacji nawigacyjnej PW Navi jest możliwość dostosowywania jej pracy do potrzeb osób z niepełnosprawnościami. Może się to odbywać poprzez dobór odpowiednich opcji konfiguracyjnych, uwzględniających problemy w poruszaniu się, widzeniu i słuchu. Po wyborze odpowiedniej opcji nawigacja poprowadzi osobę na wózku trasą uwzględniającą specyfikę takiego ruchu. Z kolei w celu wsparcia osób niewidomych zainstalowano zestaw aktuatorów dźwiękowych, których zadaniem jest wskazywanie głosowe konkretnych pomieszczeń. Pozostałe narzędzia dedykowane studentom, w tym studentom z niepełnosprawnościami, które ułatwiają korzystanie z budynków i zasobów PW, opisano w Kryterium 2.4.

Znamienna dla programu studiów drugiego stopnia na kierunku **Cyberbezpieczeństwo** jest jego elastyczność, przejawiająca się w możliwości realizacji przez studenta zindywidualizowanego programu, łączącego w różnym stopniu dwie uzupełniające się wizje ścieżki kształcenia: **naukową i przedsiębiorczą**. **Ścieżka naukowa** jest ściśle ukierunkowana na perspektywę kontynuowania kształcenia w szkole doktorskiej, z silnym naciskiem na aktywne zaangażowanie studentów w badania naukowe. **Ścieżka przedsiębiorcza** jest zorientowana na praktyczne zastosowania cyberbezpieczeństwa i skoordynowana z realizacją projektów badawczych mających zastosowanie w otoczeniu społeczno-gospodarczym (Rys. 1.3).

Program ten wpisuje się w strategię rozwoju PW, związaną m.in. z uzyskaniem statusu uczelni badawczej. **Cyberbezpieczeństwo i analiza danych** stanowi jeden z siedmiu wyodrębnionych przez PW **Priorytetowych Obszarów Badawczych (POB)** (szerzej w Kryterium 1.1). W celu wsparcia studentów realizujących najciekawsze pomysły badawcze w ścieżce naukowej oraz aby umożliwić zdobycie pierwszych doświadczeń w aspekcie aplikowania o środki finansowe na prowadzoną działalność naukową, w ramach **Centrum Badawczego POB Cyberbezpieczeństwo i analiza danych (Projekt IDUB)**, uruchomiony został konkurs **CyberSummer@WUT** organizowany corocznie w okresie letniej przerwy wakacyjnej. Konkurs cieszy się dużym zainteresowaniem wśród studentów, przynosząc równocześnie **wymierne** efekty w postaci publikacji naukowych.

Na każdym etapie studiów studenci zapraszani są do uczestnictwa w działającym w ramach ekosystemu **Cyber:Town Kole Naukowym Cyberbezpieczeństwa (KN Cyber) [https://kncyber.pl/]**, (Rys. 1.3), gdzie można rozwijać własne projekty wykraczające poza podstawowy program studiów. **KN Cyber** funkcjonuje w formie wirtualnego hackerspace dając tym samym przestrzeń do zderzania pomysłów i kreatywności. Drugim wymiarem aktywności są otwarte sieci zainteresowań wokół różnych obszarów cyberbezpieczeństwa np. badań podatności aplikacji i systemów, bezpieczeństwa niskopoziomowego systemów operacyjnych i procesorów, detekcji cyberzagrożeń czy cyberpsychologii.

Rys.1.3. Logotyp **Koła Naukowego Cyberbezpieczeństwa**

KN Cyber organizuje także regularne spotkania ze specjalistami cyberbezpieczeństwa, prowadzi własne serie warsztatów dla zainteresowanych (np. cyberbezpieczeństwo aplikacji webowych) czy grupy mentoringowe m.in. z metod uczenia maszynowego - łącząc rozrywkę z cyberbezpieczeństwem. Średnia liczba uczestników w semestrze 24Z oscylowała w okolicach 50 osób, zarówno podczas półtoragodzinnych wykładów, jak i czterogodzinnych warsztatów. Koło prowadzi także ścieżkę rozwojową dla zainteresowanych zadaniami i konkursami typu CTF (ang. Capture-The-Flag). Działalność Koła jest aktywnie wspierana przez kadrę dydaktyczną.

Koło Naukowe Cyberbezpieczeństwa KN Cyber od początku swojej działalności w skuteczny sposób angażuje się w aktualne problemy sektorowe, koncentrując się również na wspieraniu działań ogólnokrajowych, stymulowanych przez regulacje prawne, w tym Ustawę o Krajowym Systemie Cyberbezpieczeństwa (UoKSC).

Jednym w istotniejszych sukcesów **KN Cyber** jest **Projekt Artemis**, czyli rozbudowany i modułowy skaner podatności, który opracowany został przez studentów Koła, a następnie rozbudowany przez **CERT Polska**. Początkowo, skaner podatności wykorzystywany był przez **NASK** (Naukowa i Akademicka Sieć Komputerowa) do badania bezpieczeństwa stron internetowych podmiotów oraz instytucji podległych pod **CSIRT NASK.** W dniu 12 lutego 2025 r. **Ministerstwo Cyfryzacji** wraz z **CERT Polska** ogłosiło udostępnienie serwisu **moje.cert.pl** mającego na celu poprawę odporności cyfrowej polskich usług. Serwis **moje.cert.pl** dostępny jest dla każdego właściciela domeny (tj. od osoby prywatnej przez małe firmy po instytucje publiczne), umożliwiając bezpłatne korzystanie z usług takich jak:

- skanowanie bezpieczeństwa własnych domen (błędy w konfiguracji usług webowych, niezaktualizowane oprogramowanie, znane podatności),
- otrzymywanie alertów o wykrytych wyciekach z serwisów pod tymi domenami,
- weryfikacja czy dana sieć jest chroniona Listą Ostrzeżeń,
- otrzymywanie alertów o infekcjach szkodliwym oprogramowaniem (wykrycie ruchu do serwera C&C czy oznaki infekcji botnetem).

Ponadto, studenci są zapraszani do udziału **w wielu cyklicznych wydarzeniach naukowych, również we współpracy z otoczeniem społeczno-gospodarczym**, które organizowane są na terenie Uczelni i Wydziału, należą do nich np. wykłady zaproszonych specjalistów z branży oraz spotkania ISSA Polska - Stowarzyszenie do spraw Bezpieczeństwa Systemów Informacyjnych [https://www.issa.org.pl/], które jest organizacją non-profit zrzeszającą profesjonalistów zajmujących się ochroną systemów informacyjnych.

Oprócz modelowej ścieżki dydaktycznej w ekosystemie **Cyber:Town**, obejmującej studia pierwszego i drugiego stopnia studiów, możliwe jest również rozwijanie umiejętności w dziedzinie cyberbezpieczeństwa na studiach podyplomowych.

Studia podyplomowe stacjonarne **Inżynieria Cyberbezpieczeństwa** przeznaczone są dla absolwentów studiów technicznych oraz studiów z zakresu nauk ścisłych. Uczestnicy studiów uzyskają fundamentalną wiedzę oraz niezbędne umiejętności techniczne w obszarze cyberbezpieczeństwa, takie jak:

- podstawy cyberbezpieczeństwa i programowanie w języku Python,
- bezpieczeństwo sieci,
- zabezpieczanie komputerów i systemów informatycznych,
- testowanie i audytowanie systemów informatycznych,
- analizowane incydentów i cyberzagrożeń.

Uzupełnieniem do części technicznej jest wprowadzenie do zarządzania cyberbezpieczeństwem, które umożliwia poznanie różnych kontekstów pracy w obszarze cyberbezpieczeństwa. Program studiów jest nastawiony na umiejętności praktyczne. Większość zajęć stanowią zajęcia komputerowe oraz laboratoria, a praktycznym zadaniem do realizacji w drugim semestrze studiów jest grupowy projekt na temat wybranego zagadnienia z obszaru cyberbezpieczeństwa [**https://icyb.tele.pw.edu.pl/**].

MBA (Master of Business Administration) Cybersecurity Management (realizowane we współpracy ze Szkołą Biznesu PW) to dwusemestralne studia podyplomowe adresowane do osób o innowacyjnym podejściu do zarządzania cyberbezpieczeństwem. Celem studiów jest zdobycie wiedzy teoretycznej i umiejętności praktycznych, a także doskonalenie kompetencji w zarządzaniu cyberbezpieczeństwem. Program umożliwia zapoznanie się z nowoczesnymi metodami wykorzystywanymi w zarządzaniu cyberbezpieczeństwem, a także poznanie technicznych podstaw działania całości infrastruktury teleinformatycznej [**https://biznes.edu.pl/oferta/mba-cybersecurity-management/**].

Całość działań w ramach **Cyber:Town** wspierana jest przez **Centrum Cyberbezpieczeństwa PW**. Centrum Cyberbezpieczeństwa to podmiot scalający cyberbezpieczeństwo PW. Jego kluczową częścią jest zespół reagowania na incydenty, odpowiednik CERT, w którym panują idealne warunki, aby kształtować i rozwijać swoje zainteresowania cyberbezpieczeństwem przy okazji prawdziwych zdarzeń związanych z naruszeniem bezpieczeństwa.

Otoczenie naukowo-dydaktycznie **Cyber:Town** umożliwia studentom, nawet na wczesnych etapach nauki, udział w prowadzonych projektach badawczych. Wyniki naukowe uzyskiwane w trakcie ich realizacji stają się podstawą prac naukowych publikowanych w czasopismach oraz materiałach konferencyjnych (współautorzy będący doktorantami wdrożeniowymi lub studentami kierunku **Cyberbezpieczeństwo** zostali wyróżnieni poprzez pogrubienie i podkreślenie ich nazwisk i imion):

Gryka Paweł, Gradoń Kacper, Kozłowski Marek, **Kutyła Miłosz**, Janicki Artur: Detection of AI-Generated Emails - A Case Study, W: ARES 2024: The 19th International Conference on Availability, Reliability and Security, 2024, Association for Computing Machinery, Association for Computing Machinery, New York, NY, United States, s.1-8, Numer artykułu:141, ISBN 979-8-4007-1718-5. https://dl.acm.org/doi/10.1145/3664476.3670465

Gryka Paweł, Gradoń Kacper, Kozłowski Marek, **Kutyła Miłosz**, Janicki Artur: Impact of Spelling and Editing Correctness on Detection of LLM-Generated Emails, W: Proceedings of the 19th Conference on Computer Science and Intelligence Systems - FedCSIS'2024 / Bolanowski Marek [i in.] (red.), Annals of Computer Science and Information Systems, 2024, vol. 39, Institute of Electrical and Electronics Engineers, s.595–600, ISBN 978-83-969601-6-0

Hościłowicz Jakub, **Popiołek Paweł**, **Rudkowski Jan**, Bieniasz Jędrzej, Janicki Artur: Unconditional Token Forcing: Extracting Text Hidden Within LLM, W: Proceedings of the 19th Conference on Computer Science and Intelligence Systems - FedCSIS'2024 / Bolanowski Marek [i in.] (red.), Annals of Computer Science and Information Systems, 2024, vol. 39, Institute of Electrical and Electronics Engineers, s.613–616, ISBN 978-83-969601-6-0. https://annals-csis.org/Volume_39/drp/4511.html

Murat Kacper, Topyła Dominik, **Zdulski Krzysztof**, Marzęcki Michał, Bieniasz Jędrzej, Paczesny Daniel, Szczypiorski Krzysztof: Security Analysis of Low-Budget IoT Smart Home Appliances Embedded

Software and Connectivity, Electronics (Switzerland), 2024, vol. 13, nr 12, s.1-27, Numer artykułu:2371. DOI:10.3390/electronics13122371

Dracewicz Weronika, Sepczuk Mariusz, Detecting Fake Accounts on Social Media Portals—The X Portal Case Study. Electronics (Switzerland), 2024, 13, Numer artykułu: 13. https://doi.org/10.3390/electronics13132542

Gryka Paweł, Janicki Artur: Detecting Fake Reviews in Google Maps—A Case Study, Applied Sciences-Basel, 2023, vol. 13, nr 10, s.1-16, Numer artykułu: 6331. https://www.mdpi.com/2076-3417/13/10/6331

Sosnowski Krzysztof, Sepczuk Mariusz, SURE: A Smart Failover Blockchain-Based Solution for the Recycling Reuse Process. Electronics (Switzerland), 2023, 12, Numer artykułu: 10. https://doi.org/10.3390/electronics12102201

Wolert Rafał, Rawski Mariusz: Email Phishing Detection with BLSTM and Word Embeddings, International Journal of Electronics and Telecommunications, Komitet Elektroniki i Telekomunikacji PAN, vol. 69, nr 3, 2023, s. 485-491, https://doi.org/10.24425/ijet.2023.146496

Murat Kacper, **Zdulski Krzysztof**, Topyła Dominik, Marzęcki Michał, Bieniasz Jędrzej: Analiza bezpieczeństwa protokołów komunikacyjnych urządzeń inteligentnego domu opartych na mikrokontrolerze ESP, Przegląd Telekomunikacyjny - Wiadomości Telekomunikacyjne, 2022, nr 4/2022, s.295-298, Numer artykułu:138968. https://doi.org/10.15199/59.2022.4.43

Topyła Dominik, Murat Kacper, **Zdulski Krzysztof**, Paczesny Daniel, Bieniasz Jędrzej: Analiza bezpieczeństwa komunikacji urządzeń Internetu Rzeczy wykorzystujących protokół ZIGBEE: narzędzia i scenariusze testowania, Przegląd Telekomunikacyjny - Wiadomości Telekomunikacyjne, 2022, nr 4/2022, s.234-237, Numer artykułu:138952. https://doi.org/10.15199/59.2022.4.29

Zdulski Krzysztof, Topyła Dominik, Murat Kacper, Paczesny Daniel, Bieniasz Jędrzej: Modyfikacja oprogramowania urządzeń Internetu Rzeczy: analiza możliwości i wpływu na bezpieczeństwo, Przegląd Telekomunikacyjny - Wiadomości Telekomunikacyjne, 2022, nr 4/2022, s.238-241, Numer artykułu:138953. https://doi.org/10.15199/59.2022.4.30

Studenci kierunku **Cyberbezpieczeństwo** uzyskują również nagrody i wyróżnienia w konkursach.
W 2023 roku w konkursie **#Engineer 4 Science 2023** dwóch studentów zostało wyróżnionych w kategorii **„Telekomunikacja i Cyberbezpieczeństwo”** (w latach wcześniejszych konkurs nie obejmował tematyki cyberbezpieczeństwa):

- najlepsza praca inżynierska: **inż. Paweł Gryka**, temat pracy: „Detection of Fake Reviews on Google Maps” promotor: dr hab. inż. Artur Janicki, prof. uczelni,
- wyróżnienie I stopnia: **inż. Bartosz Gutowski**, temat pracy: „SentiSteg: System steganograficzny oparty na rozpoznawaniu wydźwięku”, promotor: dr hab. inż. Artur Janicki, prof. Uczelni.

W 2024 roku w konkursie **#Cyber 4 Science 2024** nagrodzonych zostało dwóch studentów:

- II miejsce: **inż. Mateusz Borkowski**, temat pracy „Modularne narzędzie do analizy pakietów DNS na potrzeby wykrywania tunelowania i komunikacji złośliwego oprogramowania”, promotor: dr inż. Jędrzej Bieniasz,
- III miejsce: **inż. Daniel Kuciński**, temat pracy „Wykorzystanie rozwiązań typu honeypot do zbierania wiedzy o zagrożeniach dla systemów przemysłowych”, promotor: dr inż. Jędrzej Bieniasz.

W edycji 2023/2024 Ogólnopolskiego Konkursu SIT na najlepszą pracę dyplomową w zakresie telekomunikacji nagrodzony został student:

- wyróżnienie w kategorii prac inżynierskich: **inż. Rafał Wolert**, temat pracy „Email phishing detection with BLSTM and word embeddings", promotor dr hab. inż. Mariusz Rawski, prof. Uczelni.

Wśród innych istotnych wyróżnień należy wymienić również:

- medal „Medallion of Excellence" dla **Jakuba Bliźniuka**, studenta I stopnia na kierunku **Cyberbezpieczeństwo**, w konkursie "WorldSkills" Lyon 2024 w konkurencji **Cyberbezpieczeństwo**,
- 1 miejsce w rankingu polskim i 3 miejsce w rankingu międzynarodowym w konkursie PingCTF 2023 dla **członków Koła Naukowego Cyberbezpieczeństwa**, będących studentami kierunku **Cyberbezpieczeństwo**:
- I stopnia: **Michał Zdulski**, **Artur Grochal**, **Jakub Szweda**, **Mateusz Orzełowski**, **Jakub Bliźniuk**, **Kacper Paluch**,
- II stopnia: **Krzysztof Zdulski**, **Maciej Włodarczyk**,
- 3 miejsce dla **Krzysztofa Zdulskiego**, studenta I stopnia kierunku **Cyberbezpieczeństwo**, w 1. edycji konkursu CTF „Time to Hack" organizowanym przez Agencję Wywiadu.

W ramach prac dyplomowych inżynierskich i magisterskich, realizowanych przez studentów kierunku **Cyberbezpieczeństwo,** znacząca część podejmuje zagadnienia opracowywane wspólnie z otoczeniem społeczno-gospodarczym, realizując prace w tematyce powiązanej z miejscem zatrudnienia lub też, których wyniki są wdrażane w miejscu pracy, wśród przykładów wymienić można:

- **Michał Adrjan**
- „Automatyzacja obsługi zgłoszeń dotyczących powtarzalnych incydentów bezpieczeństwa", praca magisterska (2024) - Rozwiązanie opracowywane w ramach pracy Dyplomanta w CERT Polska, rozwiązanie wdrożone testowo

- **Mateusz Borkowski**
- „Modularne narzędzie do analizy pakietów DNS na potrzeby wykrywania tunelowania i komunikacji złośliwego oprogramowania", praca inżynierska (2023) - Temat powiązany z zatrudnieniem w CERT Polska
- **Mateusz Kozieł**
- „Wdrażanie mechanizmów bezpieczeństwa definiowanych kodem dla środowiska chmurowego Kubernetes", praca inżynierska (2024) - Temat powiązany z rolą zawodową Dyplomanta – specjalista DevOps
- **Szymon Kasperek**
- „Metody i narzędzia kryminalistyki cyfrowej w analizie półzamkniętych systemów operacyjnych na przykładzie Google ChromeOS", praca inżynierska (2024) - Temat powiązany z rolą zawodową Dyplomanta – specjalista kryminalistyki cyfrowej i zarządzania incydentami (DFIR)
- **Zofia Krzyżanowska**
- „Wykrywanie ataków wycelowanych w użytkowników na podstawie analizy zdarzeń systemowych", praca inżynierska (2023) - Temat powiązany z rolą zawodową Dyplomantki – specjalistka/analityczka SOC
- **Bartłomiej Grabowski**
- „Rozwiązanie automatyzujące wdrożenie usługi monitorowania i logowania zdarzeń w sieciach teleinformatycznych", praca inżynierska (2023) - Temat powiązany z rolą zawodową Dyplomanta – specjalista ds. wdrożeń systemów cyberbezpieczeństwa

- **Paweł Popiołek**
  „Praktyczna realizacja ataków omijania systemów wykrywania włamań w sieciach", praca magisterska (2024) - Temat pracy powiązany ze zrealizowanym grantem badawczym Dyplomanta - „Badanie praktycznej realizacji ataków na algorytmy uczenia maszynowego w budowane w systemy wykrywania anomalii stosowane w domenie cyberbezpieczeństwa", dofinansowanego w konkursie CyberSummer@WUT-3 w programie IDUB PW (2023),
  „Klasyfikacja zdarzeń bezpieczeństwa do faz cyberataku APT z wykorzystaniem metod uczenia maszynowego", praca inżynierska (2023) - Temat pracy powiązany z realizowanym projektem badawczo-rozwojowym
- **Krzysztof Zdulski**
- „Metodyczna analiza bezpieczeństwa domowych systemów IoT na przykładzie rozwiązań Philips Hue", praca inżynierska (2023) -Temat pracy powiązany z realizowanym projektem badawczo-rozwojowym dofinansowanym przez Narodowe Centrum Badań i Rozwoju - Temat pracy powiązany z rolą zawodową Dyplomanta – specjalista ds. analizy wstecznej oprogramowania i badań bezpieczeństwa systemów
- **Kacper Grzegorzewski**
- „Model bezpiecznej sieci sterowanej programowo realizującej założenia koncepcji Zero Trust", praca magisterska (2024) - Temat pracy powiązany z rolą zawodową Dyplomanta – specjalista ds. projektowania bezpiecznej architektury sieci
- **Hubert Decyusz**
- „Skalowalna platforma do zarządzania i realizacji testowania rozmytego systemów pod kątem wykrywania błędów bezpieczeństwa", praca magisterska (2024) - Temat pracy powiązany z rolą zawodową Dyplomanta – specjalista ds. testów penetracyjnych i badań bezpieczeństwa systemów
- **Kacper Musiał**
- „Testowanie bepieczeństwa systemów Internetu Rzeczy na przykładzie inteligentnej kamery domowej TP-Link", praca inżynierska (2024) - Temat pracy powiązany z rolą zawodową Dyplomanta – specjalista ds. testów penetracyjnych i badań bezpieczeństwa systemów

- **Kacper Paluch**
- „Implementacja automatycznego skanera do wykrywania podatności wstrzykiwania w bazach danych NoSQL", praca inżynierska (2024) - Temat pracy powiązany z rolą zawodową Dyplomanta – specjalista ds. testów penetracyjnych i badań bezpieczeństwa systemów
- **Agnieszka Gadoś**
- Praca utajnonia – Temat pracy powiązany z rolą zawodową Dyplomantki – specjalista ds. bezpieczeństwa produktu

Absolwenci i studenci kierunku **Cyberbezpieczeństwo** są też rozpoznawani jako **eksperci** w dziedzinie i z coraz większą częstotliwością kształtują opinie w środkach masowego przekazu, gdzie wyjaśniają naturę cyberzagrożeń, wskazują środki zaradcze oraz określają potencjalne kierunki dotyczące profilaktyki według najlepszych praktyk [dla przykładu: **mgr inż. Michał Dondajewski** (specjalista CERT Polska) dla Czwórka Polskie Radio w temacie bezpieczeństwa w Internecie i sposobach dbania o prywatność lub KS Poranek na Kanale Sportowym w kontekście oszustw w mediach społecznościowych i wyłudzeń za pomocą metod bankowości elektronicznej np. szybkich przelewów BLIK].

Prowadzone na PW studia na kierunku **Cyberbezpieczeństwo** stały się tematem następujących publikacji:

- Kraśniewski Andrzej, Szczypiorski Krzysztof: Kształcenie w zakresie Cyberbezpieczeństwa w Politechnice Warszawskiej, Przegląd Telekomunikacyjny - Wiadomości Telekomunikacyjne, SIGMA NOT, nr 4, 2022, s. 152-155, DOI:10.15199/59.2022.4.31
- Case study: Cybersecurity at the Warsaw University of Technology, rozdział nr 5 w monografii: Kraśniewski Andrzej: Cybersecurity Research, Education and Management: University Perspective, Oficyna Wydawnicza PW, 2021, ISBN 978-83-8156-317-8

Programy pierwszego i drugiego stopnia studiów na kierunku **Cyberbezpieczeństwo** zostały wyróżnione następującymi nagrodami:

- **nagroda zespołowa Ministra Edukacji i Nauki za 2020 r.** w zakresie działalności dydaktycznej za opracowanie i uruchomienie na Wydziale Elektroniki i Technik Informacyjnych Politechniki Warszawskiej innowacyjnego programu studiów pierwszego stopnia o profilu ogólnoakademickim na kierunku **Cyberbezpieczeństwo**, przyznana w 2021 roku,

  Nagroda została przyznana na podstawie opinii opracowanych m.in. przez Przewodniczącego Parlamentu Studentów RP, Przewodniczącego Komisji ds. Kształcenia Rady Głównej Nauki i Szkolnictwa Wyższego oraz Dyrektora Departamentu Cyberbezpieczeństwa w ówczesnym Ministerstwie Cyfryzacji – nagrodę Ministra Edukacji i Nauki za osiągnięcia dydaktyczne. Szczególnym aspektem tego wyróżnienia było to, że wśród nagrodzonych było dwoje studentów – przypadek bez precedensu w historii tego typu nagród przeznaczonych z zasady dla kadry akademickiej.
- **Nagroda Rektora PW I stopnia za osiągnięcie dydaktyczne** za opracowanie i uruchomienie innowacyjnego programu studiów drugiego stopnia o profilu ogólnoakademickim na kierunku **Cyberbezpieczeństwo** na Wydziale Elektroniki i Technik Informacyjnych Politechniki Warszawskiej, przyznana prof. dr hab. inż. Andrzejowi Kraśniewskiemu, prof. dr hab. Krzysztofowi Szczypiorskiemu, dr inż. Danielowi Paczesnemu.

Programy te wyróżniono także w inny sposób:

- 20 maja 2019 r. program był prezentowany na zorganizowanej przez Ministerstwo Nauki i Szkolnictwa Wyższego konferencji NKN (Narodowy Kongres Nauki) Forum - Kształcenie, która zgromadziła ok. 350 uczestników. "Zamówiona" przez organizatorów prezentacja programu (jedyna prezentacja ilustrowana multimedialnie podczas obrad plenarnych) koncentrowała się na prostudenckich aspektach programu, a przedstawili ją wspólnie: prof. Andrzej Kraśniewski z Zakładu Cyberbezpieczeństwa oraz Gabriela Maciejewska - studentka II roku, ówczesna przewodnicząca Wydziałowej Rady Samorządu (nagranie prezentacji można znaleźć na stronie: https://cyber.elka.pw.edu.pl/studia.html
- Program został objęty patronatem Ministerstwa Cyfryzacji. Na stronie internetowej Rządu RP:

  https://www.gov.pl/web/cyfryzacja/bezpieczenstwo-przede-wszystkim-zostan-studentem-pionierskiego-kierunku-

  znalazły się (i nadal są dostępne [dostęp 21.02.2025]) m.in. następujące informacje:

  „Ministerstwo Cyfryzacji objęło patronat nad nowym kierunkiem studiów Politechniki Warszawskiej. Naszym zdaniem ich program może być uznawany przez inne uczelnie za modelowy. Mamy nadzieję, że zachęci je to do uruchamiania bliźniaczych kierunków.”

  "To jest pewne: studenci cyberbezpieczeństwa - dzięki temu, czego nauczą się w trakcie studiów - staną się pożądanymi przez pracodawców kandydatami do pracy w m.in. administracji publicznej,

instytucjach sektora finansowego, instytucjach zajmujących się różnymi aspektami bezpieczeństwa państwa, czy w firmach komercyjnych."

- Gabriela Maciejewska - ówczesna przewodnicząca Wydziałowej Rady Samorządu – jedna z osób aktywnie uczestniczących w opracowaniu programu studiów na kierunku Cyberbezpieczeństwo – została zaproszona do udziału w dyskusji panelowej “Cybersecurity – challenges for education and science: Building competencies to ensure the state's cybernetic safety” (z udziałem m.in. Wiceministrów Cyfryzacji i Obrony Narodowej) w ramach zorganizowanej przez Perspektywy 13-14 listopada 2019 r. konferencji Women in Tech Summit (ok. 6000 uczestników). Zaprezentowała m.in. zalety nowego programu studiów prowadzonego na Wydziale Elektroniki i Technik Informacyjnych, a w szczególności jego atrakcyjność dla dziewcząt zainteresowanych studiami na kierunkach związanych z naukami ścisłymi i technicznymi.

W 2021 roku zespół, który opracował ten program, uzyskał – na podstawie opinii opracowanych m.in. przez Przewodniczącego Parlamentu Studentów RP, Przewodniczącego Komisji ds. Kształcenia Rady Głównej Nauki i Szkolnictwa Wyższego oraz Dyrektora Departamentu Cyberbezpieczeństwa w ówczesnym Ministerstwie Cyfryzacji – nagrodę Ministra Edukacji i Nauki za osiągnięcia dydaktyczne. Szczególnym aspektem tego wyróżnienia było to, że wśród nagrodzonych było dwoje studentów – przypadek bez precedensu w historii tego typu nagród przeznaczonych z zasady dla kadry akademickiej.

Studia I stopnia cieszą się niesłabnącym zainteresowaniem, a studiujący bardzo pozytywnie oceniają program studiów i metody jego realizacji, o czym świadczą wyniki wewnętrznych ankiet przeprowadzanych po pierwszym semestrze.

1.6. Kluczowe kierunkowe efekty uczenia się, z ukazaniem ich związku z koncepcją, poziomem oraz profilem studiów, a także z dyscypliną/dyscyplinami, do której/których kierunek jest przyporządkowany

Koncepcja kształcenia na kierunku **Cyberbezpieczeństwo** ma bezpośredni związek z badaniami naukowymi prowadzonymi przez pracowników Wydziału Elektroniki i Technik Informacyjnych. Kluczowe efekty uczenia się odnoszące się do wiedzy z zakresu podstawowego w dziedzinach takich jak matematyka, fizyka, informatyka (języki programowania i paradygmaty programowania) dają bazę do rozwijania kompetencji szczegółowych, zaawansowanych i interdyscyplinarnych.

Za kluczowe w zakresie wiedzy należy uznać efekty uczenia się stanowiące bardzo solidną i szeroką bazę do rozwijania bardziej szczegółowej wiedzy w ramach pracy dyplomowej i w ciągu kariery zawodowej. Istotne są także efekty odpowiadające za wykształcenie szerokiego wachlarza umiejętności praktycznych popartych wiedzą teoretyczną w zakresie najważniejszych obszarów cyberbezpieczeństwa. Istotnym elementem jest wyrobienie nawyku ciągłego uczenia się i aktualizacji wiedzy oraz postawy otwartości na nowe tendencje co do metod, narzędzi i rozwiązań. Za ważne uznano kształtowanie umiejętności współpracy w zespole oraz dokumentowania, prezentowania i uzasadniania wyników pracy. W zakresie kompetencji społecznych kluczowe są efekty związane z kreatywnością i rolą społeczną absolwenta uczelni technicznej.

Kierunkowe efekty uczenia się (dla obu poziomów, załącznik ***2.1.Efekty***) są powiązane z dyscypliną **informatyka techniczna i telekomunikacja**. Za kluczowe w zakresie wiedzy należy uznać efekty uczenia się W_01 – W_07 (studia pierwszego stopnia), stanowiące solidną i szeroką bazę do rozwijania bardziej szczegółowej wiedzy w ramach pracy dyplomowej i w ciągu kariery zawodowej. W przypadku efektów uczenia się zdefiniowanych dla umiejętności, poza stricte związanymi z cyberbezpieczeństwem (U_01 – U_08) nie mniej istotne są także efekty związane z komunikacją, w tym z krytycznym wykorzystaniem różnorodnych źródeł danych oraz samokształcenia się i ciągłego uzupełniania wiedzy (U_09 – U_13). K01-K05). W zakresie kompetencji społecznych kluczowe są efekty związane z przewidywaniem

i przyjmowaniem odpowiedzialności podejmowane decyzje i działania oraz świadomość pozatechnicznych aspektów ściśle związanych z działalnością inżyniera (K01-K03).

1.7. Efekty uczenia się prowadzących do uzyskania kompetencji inżynierskich, z ukazaniem przykładowych rozwinięć na poziomie wybranych zajęć lub grup zajęć służących zdobywaniu tych kompetencji, w przypadku kierunku studiów kończących się uzyskaniem tytułu zawodowego inżyniera/magistra inżyniera

Absolwent-inżynier ma uporządkowaną wiedzę, umiejętności i kompetencje społeczne, zdefiniowane w postaci efektów uczenia się dla programu studiów (załącznik ***2.1.Efekty***):

W04
ma wiedzę w zakresie techniki cyfrowej i sprzętowych komponentów systemów komputerowych i sieci teleinformatycznych, obejmującą m.in.:

- podstawy techniki cyfrowej,
- metody projektowania układów i systemów cyfrowych z wykorzystaniem różnych typów komponentów,
- architekturę i organizację systemów komputerowych,

tworzącą podstawy do projektowania warstwy sprzętowej systemów teleinformatycznych, w szczególności rozwiązań związanych z zapewnieniem cyberbezpieczeństwa tych systemów

Wiedzę w tym zakresie student uzyskuje przede wszystkim w ramach przedmiotów obowiązkowych:

- Podstawy techniki cyfrowej,
- Systemy cyfrowe,
- Systemy komputerowe: architektura i programowanie,

odpowiadających zakresom wiedzy wymienionym w opisie tego efektu.

Wiedza uzyskiwana przez studenta jest sprawdzana bezpośrednio na sprawdzianach realizowanych w warunkach audytoryjnych (kolokwiach oraz – w przypadku przedmiotu Podstawy techniki cyfrowej – także na egzaminie), obejmujących głównie rozwiązywanie zadań. Przede wszystkim jest jednak sprawdzana w sposób pośredni, a zarazem najważniejszy z punktu widzenia wykształcenia inżyniera – przez weryfikację umiejętności jej wykorzystania. W ramach ww. przedmiotów następuje to na zajęciach praktycznych (z każdym z tych przedmiotów są związane zajęcia laboratoryjne i projekt), podczas których studenci, wykorzystując wiedzę wyniesioną z wykładów i samodzielnych studiów, projektują, realizują i testują komponenty sprzętowe stanowiące rozwiązania prostych zadań inżynierskich.

Umiejętnością wykorzystania zdobytej na ww. przedmiotach wiedzy student musi się także wykazać na bardziej zaawansowanych przedmiotach, w szczególności przedmiotach:

- Komputerowe i sieciowe systemy operacyjne,
- Komutacja i routing w Internecie,
- Sieci bezprzewodowe komórkowe, lokalne i sensorowe,
- Sieci lokalne i sieci centrów,
- Bezpieczeństwo systemów i oprogramowania,
- Kryminalistyka cyfrowa,

w ramach, których – na zajęciach praktycznych – projektuje i analizuje w laboratoriach rozwiązania używane w warstwie sprzętowej systemów teleinformatycznych, w szczególności rozwiązania związane z zapewnieniem cyberbezpieczeństwa tych systemów. Jakość tych rozwiązań, wynikająca z posiadanej przez studenta wiedzy i umiejętności jej wykorzystania, jest weryfikowana metodami przyjętymi w tych przedmiotach (patrz załączniki ***2.1.Przedmioty1, 2.1.Przedmioty2***).

W przypadku studentów realizujących w ramach procesu dyplomowania projekt zawierający komponent sprzętowy, odpowiednio pogłębiona – na przedmiotach obowiązkowych i obieralnych oraz w ramach samodzielnych studiów – wiedza z zakresu techniki cyfrowej stanowi podstawę do realizacji projektu dyplomowego i jest weryfikowana w procesie recenzowania pracy dyplomowej i podczas jej obrony.

U05

potrafi – przy identyfikowaniu problemów i formułowaniu specyfikacji zadań inżynierskich oraz problemów badawczych związanych z zapewnieniem cyberbezpieczeństwa oraz rozwiązywaniu tych zadań – dostrzec i uwzględnić ich aspekty systemowe i pozatechniczne (ekonomiczne, społeczne, etyczne, czynnik ludzki i inne) oraz dokonać wstępnej oceny ekonomicznej proponowanych rozwiązań.

Formułowanie i rozwiązywanie zadań inżynierskich z zakresu cyberbezpieczeństwa to podstawowe umiejętności zdobywane w ramach grupy przedmiotów CYBERBEZPIECZEŃSTWO. Obejmuje to także aspekty systemowe i pozatechniczne. Reprezentatywnymi przykładami przedmiotów dających studentom umiejętności w tym zakresie są:

- Bezpieczeństwo komunikacji,
- Bezpieczeństwo organizacyjne, społeczne i zarządzanie cyberbepieczeństwem.

Pierwszy z przedmiotów, Bezpieczeństwo komunikacji, w ramach ćwiczeń laboratoryjnych, uświadamia studentom zagrożenia wynikające ze złośliwych działań użytkowników sieci i prezentuje możliwe opcje stosowania zabezpieczeń, wybierane z uwzględnieniem aspektów ekonomicznych (koszt pozyskania, nakład pracy przy wdrożeniu, itp.). Stopień opanowania tych umiejętności jest sprawdzany w czasie prezentacji raportów z ćwiczeń laboratoryjnych i sprawozdania z projektu.

Przedmiot Bezpieczeństwo organizacyjne, społeczne i zarządzanie cyberbepieczeństwem jest w całości poświęcony systemowym i pozatechnicznym aspektom cyberbezpieczeństwa związanym ze stosowaniem technologii ochrony informacji i zasobów sieciowych. Zajęcia praktyczne w formie case study są w tym przypadku idealną metodą zdobywania i weryfikowania, także w czasie dyskusji i wzajemnej oceny w ramach grupy studenckiej, umiejętności dotyczących zarządzania bezpieczeństwem, ekonomii bezpieczeństwa i aspektów socjotechnicznych cyberbezpieczeństwa. Raport z projektu i egzamin są podsumowującym elementem sprawdzenia zdobytych umiejętności.

Znaczne pogłębienie umiejętności określonych przez U05 następuje w ramach realizacji przez każdego studenta co najmniej 3 przedmiotów z grupy CYBERBEZPIECZEŃSTWO – PRZEDMIOTY OBIERALNE.

Efekt U05 jest uzyskiwany także, choć może w mniejszym stopniu, na przedmiotach z innych klas, zwłaszcza z grupy przedmiotów TELEINFORMATYKA.

W przypadku wielu studentów, rozwiązujących w ramach procesu dyplomowania zadania inżynierskie oraz problemy badawcze związane z zapewnieniem cyberbezpieczeństwa, analiza aspektów systemowych i pozatechnicznych, w tym ekonomicznych, proponowanych rozwiązań stanowi integralną część pracy, a umiejętność przeprowadzenia takiej analizy jest weryfikowana w procesie recenzowania pracy dyplomowej i podczas jej obrony.

U07

potrafi ocenić możliwości funkcjonowania systemu lub sieci w warunkach wystąpienia zagrożeń; potrafi przewidzieć skutki (techniczne, ekonomiczne, społeczne i inne) ataków stwarzających zagrożenie dla bezpieczeństwa systemów informacyjnych i sieci teleinformatycznych oraz zaproponować działania minimalizujące te skutki.

Klasa CYBERBEZPIECZEŃSTWO dotyczy w całości zagrożeń bezpieczeństwa rozumianych wieloaspektowo, od ich identyfikacji, poprzez ocenę skutków technicznych, ekonomicznych i społecznych, do propozycji przeciwdziałań i próby ich realizacji. Umiejętności z tym związane, z naciskiem na aspekt techniczny, student uzyskuje głównie w ramach przedmiotów:

- Wprowadzenie do cyberbezpieczeństwa,
- Bezpieczeństwo danych,
- Bezpieczeństwo systemów i oprogramowania,
- Bezpieczeństwo komunikacji,
- Kryminalistyka cyfrowa.

Weryfikacja zdobytych umiejętności następuje podczas rozwiązywania zadań o charakterze praktycznym na egzaminach (przedmioty: Bezpieczeństwo danych, Bezpieczeństwo systemów i oprogramowania, Bezpieczeństwo komunikacji) oraz w znacznie większym stopniu, w trakcie realizacji zadań projektowych i realizacji ćwiczeń laboratoryjnych.

Zajęcia praktyczne związane z przedmiotem Wprowadzenie do cyberbezpieczeństwa dają studentowi szerokie (na podstawowym poziomie) umiejętności postępowania z zagrożeniami, weryfikowane przez realizację i raportowanie wyników ćwiczeń laboratoryjnych, obejmujących zadania związane z monitorowaniem sieci i systemów, modelowaniem, symulowaniem i wykrywaniem zagrożeń oraz testów penetracyjnych systemów. Zadanie projektowe weryfikuje umiejętności dotyczące postępowania z incydentami bezpieczeństwa w podstawowym zakresie. Ta umiejętność zostaje później, w ramach przedmiotu Kryminalistyka cyfrowa, znacznie rozwinięta i powtórnie zweryfikowana na zaawansowanym poziomie w ramach zajęć laboratoryjnych, podczas których realizowane są zadania śledcze z wykorzystaniem specjalistycznych technik i oprogramowania.

Trzy pozostałe ww. przedmioty z grupy CYBERBEZPIECZEŃSTWO: Bezpieczeństwo danych, Bezpieczeństwo komunikacji i Bezpieczeństwo systemów i oprogramowania rozwijają umiejętności związane z bezpieczeństwem zasobów informacyjnych, sieci teleinformatycznych i serwerów/węzłów sieci. Projekt związany z przedmiotem Bezpieczeństwo danych, uzupełniony o dwa ćwiczenia laboratoryjne, umożliwi weryfikację umiejętności studentów w zakresie doboru rozwiązań bezpieczeństwa, ich implementacji i oceny jakości dla systemów przechowujących i przetwarzanych dane. Laboratoria i projekt związane z przedmiotem Bezpieczeństwo komunikacji umożliwią weryfikację tych umiejętności dla systemów transmisyjnych, a projekt związany z przedmiotem Bezpieczeństwo systemów i oprogramowania zweryfikuje stopień opanowania przez studentów umiejętności ochrony urządzeń stosowanych w sieciach teleinformatycznych wraz z ich oprogramowaniem.

Wymienione wyżej metody weryfikacji umiejętności uwzględniają nie tylko techniczny aspekt cyberbezpieczeństwa. Każda implementacja, przeprowadzone badanie laboratoryjne lub analiza bezpieczeństwa wiąże się z koniecznością wyboru konkretnego rozwiązania, a ten wybór dokonywany jest na podstawie szerszej analizy uwzgledniającej aspekt ekonomiczny. Ponadto, w ramach przedmiotu Kryminalistyka cyfrowa dużo uwagi poświęca się aspektom społecznym (odpowiedzialność dostawcy/użytkownika usługi, konsekwencje działań, itp.), a przyjęte sposoby weryfikacji zdobytych przez studenta na zajęciach praktycznych umiejętności obejmują także sprawdzenie kompetencji w tym zakresie.

Podsumowując, przyjęte w przedmiotach obowiązkowych z grupy CYBERBEZPIECZEŃSTWO sposoby weryfikacji umiejętności studenta zapewniają osiągnięcie w pełni efektu U07. W praktyce, znaczne pogłębienie umiejętności określonych przez U07 następuje w ramach realizacji przez każdego studenta co najmniej 3 przedmiotów z grupy CYBERBEZPIECZEŃSTWO – PRZEDMIOTY OBIERALNE.

Efekt U07 jest uzyskiwany także, choć może w mniejszym stopniu, na przedmiotach z innych klas, zwłaszcza z grupy TELEINFORMATYKA.

W przypadku wielu studentów, rozwiązujących w ramach procesu dyplomowania zadania inżynierskie oraz problemy badawcze związane z oceną skutków ataków stwarzających zagrożenie dla bezpieczeństwa systemów informacyjnych i sieci teleinformatycznych oraz opracowaniem rozwiązań

minimalizujących te skutki, umiejętność przeprowadzenia takiej oceny i zaproponowania mechanizmów przeciwdziałania jest weryfikowana w procesie recenzowania pracy dyplomowej i podczas jej obrony.

U13
ma umiejętność samokształcenia się, m.in. w celu podnoszenia kompetencji zawodowych
oraz

KS01
rozumie potrzebę stałego aktualizowania i wzbogacania posiadanej wiedzy – podnoszenia kompetencji zawodowych, osobistych i społecznych

Te dwa efekty omawiane są łącznie ze względu na bliską relację metod weryfikacji. Weryfikacja KS01, jak każdego z innego efektu z grupy kompetencji społecznych, opisujących postawy (a nie umiejętności), nastręcza trudności. Toteż przyjmuje się, że uzyskanie przez studenta tego typu trudno weryfikowalnych efektów następuje w wyniku stosowania odpowiednich metod kształcenia stymulujących kreowanie pożądanych postaw.

W przypadku „rozumienia potrzeby stałego aktualizowania i wzbogacania posiadanej wiedzy – podnoszenia kompetencji zawodowych, osobistych i społecznych" polega to m.in. na takiej koncepcji prowadzenia przedmiotów, która czyni samodzielne poszukiwanie i analizowanie przez studenta materiałów źródłowych warunkiem wykonania zadań przewidzianych w programie przedmiotu.

W opracowanym programie studiów występuje wiele przedmiotów, w których opisie w sposób jawny uwidoczniono umiejętność samokształcenia – samodzielnego zdobywana przez studenta wiedzy – jako warunku realizacji zadań, zwykle zadań o charakterze projektowym. Przykładami takich przedmiotów, prowadzonych na początkowych semestrach, kiedy zdobycie umiejętności samokształcenia i zrozumienie potrzeby stałego wzbogacania posiadanej wiedzy ma szczególnie istotne znaczenie, są:

- Pozatechniczne aspekty pracy inżyniera,
- Szybkie prototypowanie inżynierskie,
- przedmioty z grupy MATEMATYKA,
- Wprowadzenie do cyberbezpieczeństwa.

Efekty U03 oraz KS01 są oczywiście uzyskiwane także na bardziej zaawansowanych przedmiotach, a zwłaszcza w procesie dyplomowania.

Kryterium 2. Realizacja programu studiów: treści programowe, harmonogram realizacji programu studiów oraz formy i organizacja zajęć, metody kształcenia, praktyki zawodowe, organizacja procesu nauczania i uczenia się

2.1. Dobór kluczowych treści kształcenia, w tym treści związanych z wynikami działalności naukowej uczelni w dyscyplinie, do której jest przyporządkowani kierunek oraz w zakresie znajomości języków obcych, ze wskazaniem przykładowych powiązań treści kształcenia z kierunkowymi efektami uczenia się oraz dyscypliną, do której kierunek jest przyporządkowany

Kluczowe treści kształcenia na kierunku **Cyberbezpieczeństwo** są precyzyjnie powiązane z działalnością naukową Wydziału, przede wszystkim prowadzoną w dyscyplinie **informatyka techniczna i telekomunikacja**, a treści programowe przedmiotów na kierunku odpowiadają dyscyplinie. Punktem wyjścia do doboru treści kształcenia były sylwetki absolwenta, które opracowano uwzględniając potrzeby rynkowe. Wymienione w punkcie K1.6 kluczowe efekty uczenia się – szczególnie w zakresie umiejętności – osiągane są często na kilku przedmiotach przy zastosowaniu różnorodnych form kształcenia (ćwiczenia, laboratoria, projekty, praca własna). Powiązanie treści kształcenia i efektów przedmiotowych z efektami kierunkowymi jest podane w opisie każdego przedmiotu.

Proces dydaktyczny jest skojarzony z badaniami naukowymi prowadzonymi w ramach dyscypliny **informatyka techniczna i telekomunikacja**. Wyraża się to powierzaniem prowadzenia przedmiotów kierunkowych nauczycielom akademickim uczestniczącym w projektach badawczych, których tematyka jest zgodna z tematyką przedmiotu. Prowadzone badania są często inspiracją do zgłaszania tematów prac dyplomowych zgodnych z profilem kształcenia na kierunku. W ten pośredni sposób, studenci są włączani do prowadzonych badań naukowych. Dobrym wskaźnikiem zaangażowania studentów w prace badawcze oraz prace powstałe we współpracy z otoczeniem społeczno-gospodarczym jest lista obronionych prac dyplomowych przedstawiona w załączniku ***2.6.PraceDyp***.

Powiązanie treści kształcenia z wybranymi obszarami badań ilustruje tabela 2.1.

Tabela 2.1. Powiązanie treści kształcenia z wybranymi obszarami działalności naukowej

Obszar badawczy	Wybrane przedmioty
Bezpieczeństwo danych	Bezpieczeństwo danych, Zarządzanie bezpieczeństwem informacji
Bezpieczeństwo sieci	Bezpieczeństwo komunikacji, Bezpieczeństwo sieci 5G i 6G, Bezpieczeństwo internetu rzeczy
Bezpieczeństwo oprogramowania	Bezpieczeństwo rozwiązań usługowo-sieciowych, Bezpieczeństwo oprogramowania i testy penetracyjne, Tworzenie bezpiecznego oprogramowania
Bezpieczeństwo systemów	Bezpieczeństwo systemów i oprogramowania, Bezpieczne systemy cyfrowe
Okołotechniczne aspekty cyberbezpieczeństwa	Bezpieczeństwo społeczne, organizacyjne i zarządzanie cyberbezpieczeństwem, Non-Technical Dimensions of Cybersecurity, Cyberprzestępczość - wyzwania prawne
Analiza danych	Uczenie maszynowe, Techniki i technologie Big Data, Analiza danych w cyberbezpieczeństwie, Archiwa cyfrowe, Metody matematyczne w cyberbezpieczeństwie, Kryminalistyka cyfrowa, Pattern recogniton
Sygnały i systemy teletransmisyjne	Sygnały i systemy, Transmisja sygnałów i media transmisyjne, Systemy cyfrowe
Usługi i aplikacje	Projektowanie usług i aplikacji internetowych i mobilnych, Usługi i aplikacje Internetu, Programowanie systemów internetu rzeczy i aplikacji sieciowych, Projektowanie i testowanie systemów i protokołów
Sieci	Zarządzanie sieciami i usługami, Sieci i chmury teleinformatyczne, Sieci lokalne i centra danych
Interdyscyplinarne aspekty cyberbezpieczeństwa	Wstęp do cyberbiobezpieczeństwa

2.2. Dobór metod kształcenia i ich cech wyróżniających, ze wskazaniem przykładowych powiązań metod z efektami uczenia się w zakresie wiedzy, umiejętności oraz kompetencji społecznych, w tym w szczególności umożliwiających przygotowanie studentów do prowadzenia działalności naukowej w zakresie dyscypliny, do której kierunek jest przyporządkowany lub udział w tej działalności, stosowanie właściwych metod i narzędzi, w tym zaawansowanych technik informacyjno-komunikacyjnych, jak również nabycie kompetencji językowych w zakresie znajomości języka obcego

Przyjęta dla studiów pierwszego i drugiego stopnia koncepcja programowa zakłada odejście – na ile to możliwe i uzasadnione – od kształcenia masowego, opartego na biernym uczestnictwie w zajęciach (narzucającym pozyskiwanie wiedzy teoretycznej i pasywne jej odtwarzanie na sprawdzianach) na rzecz stosowania metod kształcenia opartego na rozwiązywaniu problemów i realizacji projektów oraz innych form prowadzenia zajęć aktywizujących studentów.

W zestawie przedmiotów tworzących program studiów występują przedmioty, w których wykorzystane są m.in. następujące formy prowadzenia zajęć:

- projekty i zajęcia laboratoryjne, realizowane indywidualnie i w zespołach,
- zajęcia projektowe prowadzone zgodnie z koncepcją „design thinking”,
- zajęcia obejmujące szybkie prototypowanie,
- projekty i zajęcia laboratoryjne – także na przedmiotach prowadzonych tradycyjnie w inny sposób, np. na przedmiotach z zakresu matematyki,
- samodzielne uczenie się studentów (zdobywanie wiedzy wykraczającej poza materiał wykładowy) i prezentacja wyników tego samokształcenia na zajęciach grupowych,
- zajęcia wymagające formułowania i rozwiązywania problemów „otwartych”, w tym problemów o charakterze badawczym,
- zajęcia warsztatowo-treningowe,
- samoocena oraz wzajemna ocena studentów przez studentów.

Dobrym wskaźnikiem stopnia wykorzystania w proponowanym programie metod kształcenia uwzględniających samodzielne uczenie się studentów oraz aktywizujących form pracy ze studentami jest znaczne ograniczenie udziału wykładów jako formy prowadzenia zajęć w ogólnym bilansie „godzin kontaktowych”. W przedmiotach obowiązkowych występujących w planie studiów (bez dyplomowania) wykłady stanowią jedynie 39.0% godzin zajęć kontaktowych – wyraźnie mniej niż w przypadku innych programów studiów prowadzonych na Wydziale i na Uczelni. Szczególnie warta uwagi jest w tym kontekście nowa koncepcja nauczania matematyki, w której jedynie 35.3% zajęć ma formę wykładów, a pozostałe formy to ćwiczenia (23.5% zajęć), laboratoria (17.7% zajęć) i projekty (23.5% zajęć).

Program studiów charakteryzuje się ponadto kilkoma oryginalnymi, niezbyt powszechnie występującymi w praktyce polskich uczelni rozwiązaniami.

Zestaw zajęć na 1. semestrze został zaprojektowany z myślą o ułatwieniu „aklimatyzacji” nowo przyjętym studentom, ich wzajemnej integracji, wzmocnieniu zainteresowania studiami technicznymi, motywacji do studiowania na Wydziale, a zarazem z intencją wyposażenia ich w istotne kompetencje uniwersalne, przydatne w dalszym kształceniu. Obejmuje on m.in. następujące przedmioty/moduły zajęć:

- Wprowadzenie do cyberbezpieczeństwa – przedmiot, na którym studenci współdziałając z prowadzącymi, realizują swoje pierwsze, proste projekty związane z zagadnieniami cyberbezpieczeństwa,

- Pozatechniczne aspekty pracy inżyniera – zajęcia, mające charakter warsztatowo-treningowy, w ramach których studenci rozwiązują problemy, analizując studia przypadku, biorąc pod uwagę społeczne, ekonomiczne, prawne, etyczne i inne pozatechniczne uwarunkowania działalności zawodowej inżyniera, pogłębiają wiedzę poprzez samodzielne wyszukanie i analizę treści odpowiednich materiałów źródłowych i przedstawiają wyniki swoich prac w formie opracowań i prezentacji, przygotowanych zgodnie z omówionymi na zajęciach zasadami,
- Szybkie prototypowanie inżynierskie – zajęcia, w trakcie których studenci, początkowo indywidualnie, a następnie w zespołach, konstruują mini-roboty, rywalizując o osiągnięcie jak najlepszych parametrów swoich projektów (tak więc już na 1. semestrze student projektuje i konstruuje fizyczne obiekty, odnosząc w ten sposób pierwsze „realne" sukcesy w karierze inżyniera).
- Algorytmy i programowanie 1 - wykład prowadzony z elementami aktywizującymi studentów w postaci metodyki "klasy odwróconej". Wykorzystanie na wykładach platformy nauczenia zdalnego LeON do odpowiadania na zadane zagadnienia z możliwością konsultowania odpowiedzi w grupie studenckiej sprzyja integracji studenckiej oraz wymianie wiedzy i pierwszych doświadczeń.

Zróżnicowanym formom prowadzenia zajęć odpowiadają zróżnicowane formy weryfikacji i oceny efektów uczenia się. Stosowane są niemal wszystkie wymienione w aktach prawa wewnętrznego PW formy sprawdzania efektów uczenia się, tj. egzamin pisemny, egzamin ustny, kolokwium, laboratorium + sprawozdanie pisemne z realizacji zajęć, projekt + sprawozdanie pisemne z realizacji zadania, prezentacja indywidualna/zespołowa, praca domowa, ocena aktywności podczas zajęć.

Weryfikacja i oceny efektów uczenia się osiągniętych przez studenta w trakcie całego cyklu uczenia się (całego programu studiów) odbywa się przede wszystkim na poziomie poszczególnych przedmiotów (w sposób uwidoczniony w sylabusach). Pełne pokrycie efektów uczenia się zdefiniowanych dla programu studiów przez efekty uczenia się zdefiniowane (i weryfikowane) dla przedmiotów tworzących ten program zapewnia weryfikację efektów kierunkowych (efektów uczenia się osiągniętych przez studenta w trakcie całego cyklu uczenia się).

Liczne projekty badawcze realizowane w zespołach działających na Wydziale stanowią podstawę do formułowania tematów i realizacji przez studentów badań w ramach prac dyplomowych, a także w ramach projektów związanych z występującymi w programie studiów przedmiotami z zakresu teleinformatyki i cyberbezpieczeństwa. Realizacja prac dyplomowych, ale także projektów w ramach poszczególnych przedmiotów obejmuje najczęściej:

- sformułowanie problemu,
- dobór metod i narzędzi badawczych,
- przeprowadzenie badań, opracowanie implementacji,
- opracow*a*nie i prezentację wyników badań.

Przyjęcie tak zdefiniowanego podejścia do doboru metod kształcenia skutkuje skutecznym zaangażowaniem studentów w prace badawcze.

Ogólna koncepcja procesu kształcenia oraz unikatowe – w przypadku wielu przedmiotów – metody kształcenia, w tym weryfikacji jego efektów, nie pozostały niezauważone i przyczyniły się w znacznym stopniu do przyznania programom studiów na kierunku **Cyberbezpieczeństwo** nagród i wyróżnień wymienionych w punkcie 1.5.

2.3. Zakres korzystania z metod i technik kształcenia na odległość

Politechnika Warszawska od wybuchu pandemii COVID-19 rozwinęła w znacznym stopniu centralne narzędzia informatyczne do obsługi studentów oraz narzędzia do prowadzenia procesu dydaktycznego. W obszarze obsługi studentów szeroko rozwijany jest system USOS i USOSWeb, gdzie Centrum Informatyzacji PW projektuje, opracowuje i wdraża kolejne moduły wspierające obsługę studentów, jak również cyfryzuje kolejne procesy związane z szeroko rozumianą organizacją procesu dydaktycznego. Wśród wielu opracowanych rozwiązań można wyróżnić autorski moduł "e-podań" pozwalający załatwianie spraw studenckich w systemie USOSWeb bez potrzeby pojawiania się w Dziekanacie Wydziału. W obszarze prowadzenia procesu dydaktycznego należy wyróżnić przynajmniej dwa główne narzędzia. Pierwszym z nich jest szeroko i chętne dostępna aplikacja MS Teams używana zarówno przez pracowników jak i studentów. Drugim rozwiązaniem jest platforma nauczania zdalnego – LeON [https://leon.pw.edu.pl], która bazuje na systemie Moodle. Platforma LeON jest zintegrowana z systemem USOSWeb, dzięki czemu tworzenie kursów, synchronizacja list studentów czy ocen końcowych do protokołów przedmiotów w USOSWeb jest w zasadzie automatyczna. Dzięki ponad 20-letnieinu doświadczeniu Ośrodka Kształcenia na Odległość PW w obszarze nauczania zdalnego, LeON dysponuje wieloma bezpiecznymi i sprawdzonymi modułami, które pozwalają na budowanie różnych rozwiązań edukacyjnych. Dlatego LeON wspiera zarówno zajęcia prowadzone stacjonarnie, jak również realizuje wszelkie wsparcie w obszarze metod i technik kształcenia na odległość. W ramach realizacji przedmiotów na kierunku **Cyberbezpieczeństwo** wykorzystywana jest zarówno aplikacja MS Teams, jak również platforma LeON. Należy te narzędzia traktować jako rozwiązania wspierające działania edukacyjne realizowane na przedmiotów uruchamianych w trybie stacjonarnym. Najczęściej wspomniane narzędzia wykorzystywane są do komunikacji ze studentami, zamieszczania materiałów dydaktycznych, publikowania regulaminów, odbierania opinii od studentów, prowadzenia sprawdzianów czy testów online czy offline, prowadzenia spotkań zdalnych synchronicznych oraz niekiedy korzystania z rozwiązań asynchronicznych. Rozwiązania te wspierają także prowadzenie prac dyplomowych. Równolegle, w ostatnich lat Uczelnia w ramach różnych działań i programów (np. Kompetentny Wykładowca) realizuje szkolenia wspierające kadrę w przystosowaniu się do kształcenia zdalnego.

2.4. Dostosowanie procesu uczenia się do zróżnicowanych potrzeb grupowych i indywidualnych studentów, w tym potrzeb studentów z niepełnosprawnością, jak również możliwości realizowania indywidualnych ścieżek kształcenia

Proces uczenia się dostosowywany jest na bieżąco do indywidualnych i grupowych potrzeb studentów. Wydział zapewnia studentom kierunku takie możliwości, które wynikają z Regulaminu Studiów w PW [Regulamin studiów w Politechnice Warszawskiej].

Elastyczność procesu kształcenia wynika z bezpośredniej komunikacji z prowadzącym lub promotorem w ramach zajęć i konsultacji. Elementem dostosowania do potrzeb jest obieralność przedmiotów i tematyka pracy dyplomowej. W szczególności oferta przedmiotów obieralnych technicznych, na studiach I stopnia w wymiarze 39 ECTS, a na studiach II stopnia w wymiarze 12 ECTS, pozwala na elastyczny dobór treści w sposób ułatwiający zdobycie zakładanych efektów uczenia się, jednocześnie umożliwia studentom na rozwijanie swoich zainteresowań.

Podmiotem koordynującym w Uczelni zapewnienie wsparcia osobom z niepełnosprawnością jest Sekcja ds. Osób Niepełnosprawnych w Biurze Spraw Studenckich. Do jej zadań należy m.in. wsparcie merytoryczne w rozwiązywaniu indywidualnych problemów studentów z niepełnosprawnością, wsparcie w dostarczeniu lub wypożyczeniu sprzętu wspomagającego naukę osób z niepełnosprawnością. Studenci z niepełnosprawnością mogą także ubiegać się zapomogi m.in. o dofinansowanie: transportu związanego z aktywnością akademicką. Uczelnia zapewnia tłumacza języka migowego. Dodatkowo studenci z niepełnosprawnością mogą skorzystać z porad psychologa

oraz z doradztwa zawodowego. Pracownicy dziekanatu oraz nauczyciele odbywają szkolenia w zakresie współpracy ze studentem z niepełnosprawnością (np. jedna z pracownic dziekanatu ukończyła dwustopniowy kurs języka migowego). Wprowadzenie kompleksowego systemu komunikacji elektronicznej (platformy MS Office 365, MS Teams, LeON, USOS) również jest istotnym ułatwieniem w procesie studiowania osób czasowo lub trwale niepełnosprawnych.

W latach 2020 – 2023 Politechnika Warszawska realizowała projekt pt. "Politechnika Warszawska Ambasadorem Innowacji na Rzecz Dostępności". Projekt zawierał 10 zadań odpowiadających na najistotniejsze bariery jakie napotykają osoby niepełnosprawne chcące studiować: bariery architektoniczne, mentalne i słabego przygotowania merytorycznego w szkołach, niewystarczającego dostosowania narzędzi informatycznych stosowanych na uczelni. Zwrócono szczególną uwagę na podnoszenie dostępności narzędzi informatycznych oraz wybranych materiałów edukacyjnych w obszarze tak zwanej dostępności cyfrowej WCAG 2.1 oraz wdrożono aplikacje nawigujące po budynkach uczelni PW Navi czy Audio Mapa PW. **PW Navi** służy do nawigacji w pięciu wybranych budynkach PW (Gmach Główny, Gmach Elektroniki, Gmach Fizyki, Budynek Rektorska 4, budynek Centrum Analiz Geoprzestrzennych i Satelitarnych), wykorzystuje do pozycjonowania technologie Beacons Bluetooth Low Energy oraz GNSS. Technologia GNSS to inaczej mówiąc powszechnie znany GPS, rozszerzony o inne systemy satelitarne. Z kolei technologia Beacons BLE to nadajniki znanego również powszechnie sygnału Bluetooth. We wspomnianych budynkach zostało rozmieszczonych blisko 3000 takich małych nadajników. **Audio-Mapa PW** pełni rolę elektronicznego odpowiednika map dotykowych dla osób niewidomych, wykorzystuje do pozycjonowania QR kody i tagi NFC. Mapę można uruchomić w przeglądarkach internetowych oraz na tzw. kioskach informacyjnych umieszczonych w często odwiedzanych miejscach. **SION PW** (System Informacji o Nieruchomościach PW) służy do aktualizacji informacji o budynkach przez wyznaczonych administratorów obiektów. Z kolei **Geo-Trener PW** to narzędzie do treningu orientacji przestrzennej w formie wirtualnych spacerów 3D pozwalających osobom z niepełnosprawnościami na zapoznanie się z przestrzenią budynków PW przed ich odwiedzeniem.

2.5. Harmonogram realizacji studiów z uwzględnieniem: zajęć lub grup zajęć wymagających bezpośredniego udziału nauczycieli akademickich i innych osób prowadzących zajęcia oraz studentów, zajęć lub grup zajęć związanych z działalnością naukową prowadzoną w uczelni oraz zajęć lub grup zajęć rozwijających kompetencje językowe w zakresie znajomości języka obcego, jak również zajęć lub grup zajęć do wyboru

Na kierunku **Cyberbezpieczeństwo** na WEiTI PW:

- Studia stacjonarne I stopnia (polskojęzyczne) realizowane są przez 7 semestrów:
  - pierwszy nabór w semestrze zimowym 2019,
  - pierwsi absolwenci w semestrze zimowym 2022 (luty 2023);
- Studia stacjonarne II stopnia (polskojęzyczne) realizowane są przez 3 semestry:
  - pierwszy nabór w semestrze letnim 2023,
  - pierwsi absolwenci w semestrze letnim 2024 (czerwiec 2024).

Przez pierwsze cztery semestry programu studiów I stopnia zajęcia odbywają się wspólnie dla wszystkich studentów. Na tym wczesnym etapie, stosunkowo niewielu studentów korzysta z możliwości indywidualizacji tempa studiowania. Od piątego semestru studenci wybierają promotora, tematykę pracy dyplomowej oraz realizują przedmioty związane z tą tematyka i inne przedmioty obieralne.

Na stacjonarnych II stopnia studenci od pierwszego semestru w znacznym stopniu sami kształtują program studiów poprzez wybór promotora, tematyki pracy dyplomowej, a od drugiego semestru także przedmiotów obieralnych.

Zajęcia z języków obcych na Politechnice Warszawskiej realizowane są przez Studium Języków Obcych PW [www.sjo.pw.edu.pl] w formie zajęć programowych przygotowujących do egzaminu oraz w formie zajęć wybieranych z szerokiej wielotematycznej oferty kursów poegzaminacyjnych. Zajęcia prowadzone w formie lektoratów, na których osiągane są efekty uczenia się językowe, na studiach pierwszego stopnia obejmują w sumie 180 godzin i 12 ECTS. Studenci są zobowiązani do zdania egzaminu z wybranego języka na poziomie minimum B2.

Na studiach drugiego stopnia studenci są zobowiązani do uzyskania kompetencji z języka obcego na poziomie B2+, przy czym zaleca się, aby było to realizowane poprzez zaliczenie co najmniej jednego przedmiotu prowadzonego w języku obcym lub zaliczenie zajęć z odpowiedniego poziomu lektoratu w wymiarze minimum 30 godzin (zgodnie z Uchwałą Senatu PW 58/L/2020 z dn. 25 11. 2020). Na kierunku **Cyberbezpieczeństwo**, na studiach drugiego stopnia studenci realizują dwa obowiązkowe przedmioty w języku angielskim przewidziane w planie modelowym: Methodological and Ethical Issues of Technoscientific Research (sem.2, 2 ECTS) oraz Non-technical Dimensions of Cybersecurity (sem. 3, 4 ECTS).

W programie studiów pierwszego stopnia przewidziano także zajęcia z wychowania fizycznego. Są one realizowane przez pierwsze trzy semestry studiów w wymiarze 30 godzin na semestr (w sumie 90 godzin).

W ocenie powiązania kształcenia z działalnością naukową uwzględniono przedmioty ogólne, dyplomowe oraz przedmioty kierunkowe techniczne i kierunkowe obieralne, realizowane przez pracowników Wydziału Elektroniki i Technik Informacyjnych. Pozostałe przedmioty prowadzą:

- Wydział Matematyki i Nauk Informacyjnych,
- Wydział Fizyki,
- Studium Języków Obcych,
- Wydział Administracji i Nauk Społecznych,
- Wydział Zarządzania (przedmioty HES).

Dane dot. udziału nakładu pracy studenta w przedmiotach związanych z działalnością naukową (zgodnie z Uchwałą Senatu PW dotyczącą przyporządkowania Kierunku załącznik ***PrzyporzadKier***) względem wszystkich przedmiotów na kierunku podano w załączniku ***1.Zestawienie***, w Tabeli 3, a sposób ich wyznaczenia w załączniku ***WskaznikiIlosc***.

2.6. Dobór form zajęć, proporcji liczby godzin przypisanych poszczególnym formom, a także liczebności grup studenckich oraz organizacji procesu kształcenia, harmonogramu zajęć

Liczebności grup ustala kierownik jednostki (Wydziału), dla każdego przedmiotu uwzględniając specyfikę zajęć. Zalecane liczebności podaje Regulamin pracy PW i przewidziano w nim, że wykłady odbywają się dla grup 15-100 osób, ćwiczenia audytoryjne przeciętnie dla 12 do 24 studentów, ćwiczenia projektowe dla 8-12 studentów, zajęcia laboratoryjne dla 8-10 studentów, zajęcia komputerowe dla 10-20 studentów, lektoraty dla 10-14 studentów, seminaria dla 10-16 osób. Dla grup dziekańskich liczniejszych niż zalecana, tworzone są zespoły. Na wniosek opiekuna przedmiotu zespoły mogą być mniejsze niż wskazane w regulaminie.

W harmonogramie zajęcia są planowane z równomiernym rozkładem obciążenia. Czas zajęć kontaktowych w ciągu dnia jest układany, o ile to możliwe, w bloki kilku różnych przedmiotów. W ramach jednego bloku związanego z przedmiotem są typowo 2-3 godziny zajęć, w celu zapewnienia dobrych warunków psychofizycznych studentów. Przykładowy rozkład zajęć dla semestru 2 i 4 został przedstawiony w załączniku ***2.3.Harmonogram***.

2.7 Program i organizacja praktyk, w tym w szczególności ich wymiaru i terminu realizacji oraz doboru instytucji, w których odbywają się praktyki, a także liczby miejsc praktyk – w przypadku, gdy w planie studiów na ocenianym kierunku zostały uwzględnione praktyki zawodowe

Na Politechnice Warszawskiej wytyczne dotyczące praktyk obowiązkowych reguluje Zarządzenie Rektora PW nr 45/2021 (załącznik ***ZarzPraktyki***), w którym znajdują się również obowiązujące w Uczelni wzory dokumentów. Praktyki obowiązkowe odbywają się w oparciu o porozumienie pomiędzy Uczelnią a pracodawcą i trwają 4 tygodnie (minimum 160 godzin roboczych). Wydział w obszarze praktyk studenckich ma podpisanych szereg umów i porozumień, do czego w dużej mierze przyczyniają się organizowane dwukrotnie w roku Targi Pracy i Praktyk dla Elektroników i Informatyków (załącznik ***TargiPracy***). Wydarzenia te cieszą się dużym zainteresowaniem zarówno ze strony firm jak i studentów, którzy już od pierwszego semestru mają tym samym możliwość zetknięcia się z przedstawicielami branży związanej bezpośrednio ze studiowanym kierunkiem. Sytuacja ta sprzyja między innymi podejmowaniu pracy zawodowej już na wczesnych latach studiów, co w połączeniu ze zdobywaniem wiedzy akademickiej pozwala na szybsze i szersze zdobywanie niezbędnych na rynku kwalifikacji.

Sprawami praktyk zajmuje się na Wydziale pełnomocnik Dziekana ds. praktyk oraz opiekunowie praktyk w poszczególnych instytutach. Wspierają oni studentów w wyborze miejsca praktyk oraz weryfikują poprawność programu praktyk i sprawozdania z odbycia praktyk.

W praktyce – zgodnie z podstawowym celem praktyk, które mają dać studentowi zetknięcie się z rzeczywistością rynku pracy – zdecydowana większość studentów realizuje tzw. praktyki dobrowolne. Pierwszym zadaniem studenta jest znalezienie interesującego miejsca praktyk (tu bardzo pomocne są Targi Pracy i Praktyk) i przejście procesu rekrutacji. W przypadku problemów z realizacją któregoś z tych kroków opiekunowie praktyk służą pomocą i poradą.

W przypadku studentów kierunku **Cyberbezpieczeństwo**, ze względu na szeroki zakres firm, w których można wykorzystać zdobytą podczas studiów wiedzę, liczba przedsiębiorstw, w których są realizowane praktyki jest znaczna. Część studentów wybiera firmy związane z telekomunikacją (tak jak studenci kierunku Telekomunikacja), a część odbywa praktyki w firmach szczególnie zainteresowanych studentami kierunku **Cyberbezpieczeństwo,** czyli w bankach i firmach związanych z ubezpieczeniami. Do najpopularniejszych firm, w których odbywają się praktyki obowiązkowe, zaliczają się Orange Polska S.A. (od lat przyjmuje największą liczbę naszych studentów), Netia S.A., Samsung Electronics Polska Sp. z o.o., Polkomtel Sp. z o.o., Nokia Solutions & Networks Sp. z o.o. z firm związanych z telekomunikacją, a także PwC Advisory Sp. z o.o. Sp.k., Bank Ochrony Środowiska, PZU Centrum Operacyjne S.A., Bank Gospodarstwa Krajowego.

Praktyki są zwykle płatne, a zakres obowiązków studentów nie odbiega znacząco od zakresu obowiązków nowo przyjętego pracownika. Sposób udokumentowania praktyk dobrowolnych jest bardzo podobny – student przedstawia zaświadczenie z firmy/instytucji o odbyciu praktyk oraz składa raport z praktyk, sporządzony według szablonu umieszczonego na stronie Wydziału, zawierający m.in.: krótką informację o miejscu praktyk, wymaganiach i oczekiwaniach pracodawcy, opis merytoryczny wykonanych prac, informację, jaką wiedzę i umiejętności zdobyte na studiach student wykorzystał w trakcie praktyki, informację o wiedzy i umiejętnościach zdobytych przez studenta w trakcie praktyki, uwagi własne, wnioski dla młodszych kolegów.

2.8. Dobór treści i metod kształcenia, form, liczebności grup studenckich w odniesieniu do zajęć lub grup zajęć, na których studenci osiągają efekty uczenia się prowadzące o uzyskania kompetencji inżynierskich, w przypadku kierunku studiów kończących się uzyskaniem tytułu zawodowego inżyniera/magistra inżyniera

Przyjęta koncepcja programowa zakłada stosowanie metod kształcenia opartych na rozwiązywaniu problemów i realizacji projektów oraz innych form prowadzenia zajęć aktywizujących studentów.

Elementami realizacji tego podejścia są rozwijanie umiejętności wyszukiwania informacji, kreatywnej konceptualizacji problemów, także w formach zespołowych (np. burza mózgów), wybór adekwatnych metod i narzędzi służących rozwiązaniu problemu, umiejętności krytycznej oceny osiągniętych rezultatów i doskonalenia rozwiązań oraz opracowywania i prezentacji wyników, także w postaci artykułów naukowych.

Z punktu widzenia uzyskania kompetencji inżynierskich zasadnicze znaczenie ma proces dyplomowania, realizowane przez studentów zajęcia laboratoryjne w 2-4 osobowych grupach oraz projekty, często także realizowane w zespołach. Laboratoria i projekty stanowią składnik większości przedmiotów technicznych na studiach inżynierskich oraz na studiach magisterskich. Ćwiczenia (w tym ćwiczenia komputerowe) oraz laboratoria pozwalają na skrócenie czasu uczenia się przy wprowadzaniu nowej tematyki i narzędzi w programie studiów.

Informacje dotyczące doboru treści i metod kształcenia, form, liczebności grup studenckich znajdują się także w Kryteriach 2.1, 2.2 i 2.6.

Kryterium 3. Przyjęcie na studia, weryfikacja osiągnięcia przez studentów efektów uczenia się, zaliczanie poszczególnych semestrów i lat oraz dyplomowanie

3.1. Wymagania stawiane kandydatom, warunków rekrutacji na studia oraz kryteriów kwalifikacji kandydatów na każdy z poziomów studiów

Osiągnięcia kandydata są poddawane konkursowej procedurze kwalifikacyjnej. Szczegółowe zasady rekrutacji wynikają z Uchwał Senatu. (Uchwała nr 393/L/2023 z dnia 28/06/2023 w sprawie warunków i trybu rekrutacji na studia jednolite magisterskie oraz studia pierwszego i drugiego stopnia, profili kształcenia oraz form tych studiów na poszczególnych kierunkach, prowadzonych w roku akademickim 2024/2025).

Rekrutacja na studia pierwszego stopnia jest realizowana zgodnie z jednolitymi zasadami przyjętymi przez Uczelnię, na podstawie wyniku egzaminu maturalnego z odpowiednio przypisanymi wagami dla przedmiotów i poziomów matury. W przypadku kandydatów z innych państw obowiązują inne zasady.

Przyjęcia na studia drugiego stopnia przeprowadzane są na podstawie rankingu. Kandydaci kończący ten sam kierunek przyjmowani są na podstawie wyników ukończonych studiów I stopnia - ocen zawartych w suplemencie do dyplomu. W przypadku absolwentów studiów I stopnia z innego wydziału lub z innej uczelni, przeprowadzana jest ocena kompetencji w odniesieniu do wymagań wynikających z programu studiów I stopnia. Takie podejście pozwala na osiągnięcie jednolitej, wysokiej jakości kształcenia wszystkich studentów.

3.2. Zasady, warunki i tryb uznawania efektów uczenia się i okresów kształcenia oraz kwalifikacji uzyskanych w innej uczelni, w tym w uczelni zagranicznej

Szczegółowe zasady uznawania efektów uczenia określa Regulamin Studiów i uczelniana procedura przewidująca ocenę kompetencji na podstawie dokumentacji z innej uczelni, w której w przypadku studiów pierwszego stopnia odniesiono się do systemów kształcenia wybranych państw. W przypadku studiów drugiego stopnia określono sposób ubiegania się o apostille, legalizację lub nostryfikację. (Uchwała nr 387/XLIX/2019 Senatu Politechniki Warszawskiej z dnia 18 września 2019 r., Zarządzenie nr 51/2019 Rektora Politechniki Warszawskiej z dnia 23 września 2019 r.).

3.3. Zasady, warunki i tryb potwierdzania efektów uczenia się uzyskanych w procesie uczenia się poza systemem studiów

Osoba chcąca skorzystać z możliwości uzyskania potwierdzenia efektów uczenia się powinna skontaktować się z Prodziekanem ds. Nauczania. Istnieje np. możliwość uznania efektów uczenia się dla przedmiotu, osiągniętych w wyniku uczestniczenia studenta w pracach koła naukowego.

3.4. Zasady, warunki i tryb dyplomowania na każdym z poziomów studiów

Na studiach pierwszego stopnia tematyka dyplomowania wiąże się z dorobkiem naukowym nauczycieli akademickich. W 5 semestrze wydawane są tematy prac dyplomowych proponowane przez przyszłych promotorów i zatwierdzane przez zespół składający się z dyrektorów ds. nauczania w Instytutach i kierownika kierunku. Całość procesu realizowana jest z wykorzystaniem systemu APD-USOS (Archiwum Prac Dyplomowych).

Postęp prac studenta nad wykonywaniem pracy dyplomowej jest monitorowany ramach konsultacji przez promotora oraz podczas zajęć w przedmiocie „Seminarium Dyplomowe" przez prowadzącego te zajęcia.

Praca dyplomowa inżynierska powinna stanowić samodzielne opracowane przez Dyplomanta rozwiązanie problemu technicznego o charakterze inżynierskim oraz wykazywać wiedzę inżynierską Dyplomanta w zakresie kierunku kształcenia.

Na studiach II stopnia praca dyplomowa magisterska powinna stanowić samodzielne rozwiązanie przez autora zaawansowanego problemu technicznego o charakterze inżynierskim – koncepcyjnym i projektowym, naukowym lub badawczym oraz wykazywać jego wiedzę inżynierską i teoretyczną w zakresie kierunku kształcenia. Postęp prac studenta nad wykonywaniem pracy dyplomowej jest monitorowany przez promotora w ramach konsultacji i w przedmiocie „Pracowania dyplomowa magisterska" i „Przygotowanie pracy dyplomowej magisterskiej".

Praca dyplomowa magisterska powinna wykazać umiejętność korzystania z metod badawczych i analitycznych oraz umiejętność definiowania i rozwiązywania problemów danej dziedziny. Po zakończeniu realizacji pracy student zgłasza gotowość do obrony potwierdzoną przez promotora/tutora. Student wprowadza pracę do platformy APD-USOS (Archiwum Prac Dyplomowych), która służy archiwizacji i sprawdzaniu antyplagiatowemu wszystkich prac w Jednolitym Systemie Antyplagiatowym (JSA). Wyznaczone przez Dziekana osoby - dyrektorzy ds. nauczania i kierownicy kierunku proponują recenzentów. Co najmniej trzy dni przed obroną student ma możliwość zapoznania się z opinią promotora/tutora i recenzenta. Ocena jest proponowana przez promotora i recenzenta. W czasie egzaminu dyplomowego komisja ustala ocenę za pracę dyplomową, ocenę z egzaminu oraz – uwzględniając przebieg studiów- ocenę końcową (ostateczny wynik studiów).

3.5. Sposoby oraz narzędzia monitorowania i ocena postępów studentów (np. liczby kandydatów, przyjętych na studia, odsiewu studentów, liczby studentów kończących studia w terminie) oraz działań podejmowanych na podstawie tych informacji, jak również sposobów wykorzystania analizy wyników nauczania w doskonaleniu procesu nauczania i uczenia się studentów

Co roku dokonywana jest analiza liczby przyjętych studentów i na tej podstawie podejmowana decyzja o limicie rekrutacyjnym w kolejnym roku akademickim. Wyniki rekrutacji prezentowane są na posiedzeniach Rady Wydziału oraz analizowane przez prodziekana odpowiedzialnego za sprawy rekrutacji. Największy ubytek studentów następuje po pierwszym semestrze studiów, dlatego już po tym semestrze (a nie po roku) dokonywane są skreślenia. Jest to charakterystyczne dla tego typu studiów– nie wszyscy radzą sobie z nauką i podjęta przez nich próba nie kończy się sukcesem.

Monitorowanie postępów studentów przebiega na podstawie analizy wyników rekrutacji (liczby przyjętych, wymaganych punktów z matury i rezygnacji w procesie przyjmowania na studia), skreśleń z listy studentów ze względu na brak postępów, wyników rejestracji i analizy ocen. Syntetyczne parametry są raportowane na posiedzeniach Rady Wydziału, przez prodziekana ds. nauczania i stanowią podstawę do dalszych decyzji w postaci ustalania limitów przyjęć, ustalania przyszłych warunków rejestracyjnych a także planów długoterminowych polityki jakości. Ocena postępów w nauce w ujęciu zdawalności przedmiotów, liczby osób skreślanych z listy studentów, wyników rejestracji, naboru specjalności, rozkładu ocen jest prowadzona przez m.in. prodziekana ds. nauczania. Wyniki analiz odnoszone są do wyników ocen uzyskany z ankiet studenckich. W konsekwencji mogą być podejmowane działania mające na celu ustalenie źródeł potencjalnych nieprawidłowości.

Ocenie poddawany jest także proces dyplomowania i zaliczania praktyk. W wyniku monitorowania wyników osiąganych na poszczególnych przedmiotach oraz opinii studentów dokonywane są zmiany w sposobie prowadzenia przedmiotów lub osób prowadzących. Nie dokonuje się jednak zmian obniżających poziom kształcenia, zakładając, że wartością nadrzędną jest osiągnięcie wszystkich efektów uczenia się, a nie osiągnięcie wysokich wartości wskaźników sukcesu. Losy absolwentów monitorowane są przez ogólnouczelniane jednostki – Biuro Karier i Dział Analiz Strategicznych (DAS). Na wydziale działa również Stowarzyszenie Absolwentów (http://www.elka.pw.edu.pl/Spolecznosc/Absolwenci). W ogólności absolwenci wydziału osiągają wysoką pozycję na rynku pracy, bez względu na ukończony kierunek studiów.

3.6. Ogólne zasady sprawdzania i oceniania stopnia osiągania efektów uczenia się

Ogólne zasady sprawdzania i oceniania stopnia osiągania efektów uczenia się określa Część V Regulaminu Studiów w Politechnice Warszawskiej. Zobowiązuje on kierownika przedmiotu m.in. do określenia metod etapowej i/lub końcowej weryfikacji osiągnięcia efektów uczenia się (egzamin, sprawdziany pisemne i ustne, sprawozdania z wykonanych ćwiczeń laboratoryjnych, projektów i in.), zasad zaliczania przedmiotu i wystawiania oceny końcowej z przedmiotu, terminów i trybu ogłaszania ocen uzyskiwanych przez studentów oraz zasad poprawiania ocen, możliwości i zasad udziału studentów w dodatkowych terminach sprawdzianów i egzaminów. Szczegółowe zasady sprawdzania i oceniania stopnia osiągania efektów uczenia się ustalane są dla każdego przedmiotu osobno. Regulaminy przedmiotów są dostępne w formie elektronicznej w systemach USOSWeb oraz na platformie LeON. Po zalogowaniu się do systemów, każdy pracownik i student, może zapoznać się z dowolnym regulaminem przedmiotu. Dodatkowo Dziekan Wydziału dysponuje narzędziem zintegrowany w USOSWeb pokazującym aktualną liczbę opublikowanych regulaminów przedmiotów. Jest też możliwość wysłania szybkiej wiadomości do koordynatorów, którzy mają opóźnienie w publikacji regulaminów. Wprowadzenie elektronicznych regulaminów przedmiotów, nie tylko stanowi ułatwienie organizacyjne, ale niesie za sobą również walor edukacyjny i projakościowy szczególnie dla kierowników przedmiotów. Testy, rozwiązania zadań, raporty, sprawozdania w przypadku wersji elektronicznej są archiwizowane na platformie edukacyjnej LeON lub Studia. W przypadku przeprowadzenia weryfikacji w formie pisemnej (papierowej) wykładowcy są zobowiązani do archiwizowania dokumentacji zgodnie z Zarządzeniem nr 144 Rektora PW z dnia 20 listopada 2020 r. (oraz Zarządzenie nr 114/2021 Rektora PW z dnia 25/11/2021) w sprawie zasad przechowywania dokumentacji poświadczającej dokonanie weryfikacji osiąganych efektów uczenia się dla przedmiotu. Pozytywna ocena z przedmiotu oznacza osiągnięcie przez studenta wszystkich efektów uczenia się dla przedmiotu.

3.7. Dobór metod sprawdzania i oceniania efektów uczenia się w zakresie wiedzy, umiejętności oraz kompetencji społecznych osiąganych przez studentów w trakcie i na zakończenie procesu kształcenia (dyplomowania), w tym metod sprawdzania efektów uczenia się osiąganych na praktykach zawodowych (o ile praktyki zawodowe są uwzględnione w programie studiów), ukazując przykładowe powiązania metod sprawdzania i oceniania z efektami uczenia się odnoszącymi się do

działalności naukowej w zakresie dyscypliny, do której kierunek jest przyporządkowany, efektami dotyczącymi stosowania właściwych metod i narzędzi, w tym zaawansowanych technik informacyjno-komunikacyjnych, jak również kompetencji językowych w zakresie znajomości języka obcego

Dobór metod sprawdzania efektów ucznia wynika ze specyfiki przedmiotu lub podejmowanej tematyki. Kolokwia są prowadzone w czasie semestru i służą do weryfikacji etapowej osiągania efektów uczenia się. Prowadzący określa warunki weryfikacji w regulaminie przedmiotu w tym np. możliwość korzystania z materiałów. Formy weryfikacji mogą być w postaci opisowych problemów, zdań, rysunków lub testów. Zasady zaliczenia przedmiotów są przedstawiane studentom na pierwszych zajęciach. Oceny podsumowujące prowadzone są w postaci kolokwiów lub egzaminów. Egzaminy najczęściej odbywające się w sesji i mają postać pisemnych zadań problemowych, testów, odpowiedzi ustnych.

Wiedza zdobywana w czasie zajęć z nauczycielami jest ugruntowywana podczas studiów własnych, których integralną częścią jest zapoznanie się z literaturą, w tym naukową, w tym w języku obcym, zwykle angielskim. Krótkie prace pisemne (tzw. wejściówki) przy rozpoczęciu zajęć, w szczególności laboratoryjnych, mają na celu weryfikację przygotowania studentów do zajęć. Przygotowanie to bywa też sprawdzane przez odpowiedzi ustne lub oceną aktywności i samodzielności.

Przyjęta dla studiów pierwszego i drugiego stopnia koncepcja programowa zakładająca odejście – na ile to możliwe i uzasadnione – od kształcenia opartego na biernym uczestnictwie w zajęciach (narzucającym pozyskiwanie wiedzy teoretycznej i pasywne jej odtwarzanie na sprawdzianach) na rzecz stosowania metod kształcenia opartego na rozwiązywaniu problemów i realizacji projektów oraz innych form prowadzenia zajęć aktywizujących studentów ma istotny wpływ na sposób weryfikacji efektów uczenia się. Odzwierciedla to m.in. względnie mała liczba egzaminów (na studiach II stopnia egzamin jako forma weryfikacji efektów uczenia się występuje jedynie w trzech spośród kilkunastu przedmiotów obowiązkowych). Przeważają formy typowe dla kształcenia opartego na rozwiązywaniu problemów i realizacji projektów.

W odniesieniu do kompetencji językowych są one weryfikowane wielotorowo. Poza lektoratami kompetencje językowe są rozwijane w przedmiotach i pracach. W pracy dyplomowej student przedstawia streszczenie w języku angielskim. W strukturze pracy wymagane jest wprowadzenie będące odniesieniem do literatury specjalistycznej w tym naukowej, najczęściej dostępnej w języku obcym. Literatura ta pozostaje w związku z profilem specjalności, dyplomowania i naukową obsady kierunku. Egzamin dyplomowy składa się z części dotyczącej zakresu studiów, w postaci dwóch pytań i z obrony przedstawionej przez dyplomanta pracy w formie jej prezentacji i ustosunkowania się do recenzji pracy oraz pytań komisji. Po zakończeniu praktyk student przekazuje opiekunowi sprawozdanie z przebiegu, zaświadczenie o odbyciu praktyk wraz z oceną opiekuna ze strony firmy o osiągnięciu efektów uczenia się. Na podstawie przedstawionych przez studenta dokumentów opiekun praktyk ocenia nabycie przez studenta zakładanych dla praktyki studenckiej efektów uczenia się. Osiągnięcie wszystkich zakładanych dla praktyk efektów uczenia się jest warunkiem udzielenia zaliczenia praktyki studenckiej. Nadzór nad praktyką polega na kontaktach bezpośrednich np. telefonicznych, ocenie profilu z dostępnych danych, stałej współpracy z firmami także na innych polach.

3.8. Dobór metod sprawdzania i oceniania efektów uczenia się w zakresie wiedzy, umiejętności oraz kompetencji społecznych prowadzących do uzyskania kompetencji inżynierskich, z ukazaniem przykładowych powiązań tych metod z efektami uczenia się, w przypadku kierunku studiów kończących się uzyskaniem tytułu zawodowego inżyniera/magistra inżyniera

Do sprawdzania i oceniania efektów uczenia się prowadzących do uzyskania kompetencji inżynierskich wykorzystywane są wszystkie omawiane w punkcie 3.7 metody. Dobór konkretnych metod jest

dopasowany do charakteru przedmiotu. W przypadku kierunku **Cyberbezpieczeństwo** często stosowaną formą weryfikacji umiejętności inżynierskich jest wykonywanie prac projektowych, w tym programistycznych. Metody weryfikacji wiedzy dla poszczególnych przedmiotów podane są w kartach przedmiotów. Metody weryfikacji efektów uczenia się w zakresie kompetencji społecznych związane są z realizacją prac wymagających samodzielnego rozwiązywania problemów oraz pracy w zespole. Kompetencje społeczne są także weryfikowane w czasie seminariów dyplomowych.

3.9. Rodzaj, tematyka i metodyka prac etapowych i egzaminacyjnych, projektów

Tematyka prac etapowych, egzaminacyjnych i projektów jest ściśle powiązana z treściami kształcenia i efektami uczenia się przedmiotu, w ramach którego są realizowane. Szczegółowy zakres w/w prac jest opisany w regulaminie każdego z przedmiotów, ponadto jest prezentowany studentom na pierwszych zajęciach w każdym semestrze, w którym przedmiot jest uruchamiany. Prace są sprawdzane przez prowadzących zajęcia i oceniane zgodnie z kryteriami podanymi w regulaminie przedmiotu. Oceny cząstkowe z tych prac dają podstawę do oceny końcowej uzyskiwanej przez studenta z przedmiotu.

3.10. Rodzaj, tematyka i metodyka prac dyplomowych, ze szczególnym uwzględnieniem nabywania i weryfikacji osiągnięcia przez studentów kompetencji związanych z prowadzeniem działalności naukowej oraz kompetencji inżynierskich (w przypadku, gdy oceniany kierunek prowadzi do uzyskania tytułu zawodowego inżyniera lub magistra inżyniera)

Tematyka prac dyplomowych jest powiązana z tematyką prac badawczo-rozwojowych prowadzonych przez nauczyciela akademickiego. Propozycje tematów prac tematów dyplomowych są zgłaszane przez nauczycieli akademickich w systemie APD. Po weryfikacji i zatwierdzeniu przez kierowników specjalności tematy prac są udostępniane studentom. Z listy dostępnych tematów student może wybrać interesujący go temat, szczegółowy zakres pracy jest uzgadniany podczas konsultacji z nauczycielem akademickim. Praca dyplomowa inżynierska jest realizowana nominalnie w czasie dwóch semestrów, praca magisterska – trzech. Na zakończenie każdego semestru student przygotowuje sprawozdanie z opisem wyników uzyskanych w danym semestrze. Sprawozdanie jest oceniane przez promotora oraz osobę (profesora lub dra hab.) desygnowaną przez kierownika zakładu, w którym realizowana jest praca dyplomowa, do przeprowadzenia zaliczenia poszczególnych etapów realizacji procesu dyplomowania (w każdym z semestrów, w których realizowany jest ten proces). W ostatnim semestrze realizacji pracy przygotowywana jest praca dyplomowa, która musi być złożona terminie określonym w Zarządzenie Rektora PW. Po złożeniu pracy dyplomowej podlega ona ocenie przez promotora pracy i recenzenta zgodnie z obowiązującymi kryteriami. Ostateczna ocena pracy dyplomowej jest wystawiania podczas egzaminu dyplomowego.

3.11. Sposoby dokumentowania efektów uczenia się osiągniętych przez studentów (np. testy, prace egzaminacyjne, pisemne prace etapowe, raporty, zadania wykonane przez studentów, projekty zrealizowane przez studentów, wypełnione dzienniki praktyk, prace artystyczne, prace dyplomowe, protokoły egzaminów dyplomowych.)

Uzyskanie efektów uczenia osiągniętych przez studentów jest weryfikowane na podstawie wyników sprawdzianów pisemnych, egzaminów, realizacji ćwiczeń laboratoryjnych i/lub projektów zgodnie z wymaganiami opisanymi w regulaminie przedmiotu. Wszystkie prace studenckie są przechowywane albo w postaci elektronicznej (platforma LeON lub Serwer studia) lub papierowej zgodnie z Zarządzeniami Rektora nr 144/2020 oraz 114/2021.

System Archiwum Prac Dyplomowych - APD umożliwia cyfrowe archiwizowanie najważniejszych kroków związanych z procesem dyplomowanie. W systemie tym zatwierdzany jest temat pracy dyplomowej zgłoszony przez promotora. Zatwierdzenia tematu dokonuje kierownik kierunku,

natomiast przypisanie tematu do studenta prowadzi powołana komisja. Sama realizacja pracy dyplomowej jest dokumentowana przez promotora pracy dyplomowej i w tym zakresie nie zostały sformułowane szczegółowe wytyczne. System APD jest wykorzystywany w ostatnim etapie dyplomowania, gdzie jest umieszczana praca dyplomowa, następnie zatwierdzana przez promotora, w dalszej kolejności podlega sprawdzeniu przez JSA, oraz wystawiana jest opinia i recenzja. W ostatniej części procesu jest odnotowywany wynik egzaminu dyplomowego.

3.12. Wyniki monitoringu losów absolwentów ukazujące stopień przydatności na rynku pracy efektów uczenia się osiągniętych na ocenianym kierunku oraz luki kompetencyjne, jak również informacje dotyczące kontynuowania kształcenia przez absolwentów ocenianego kierunku.

Losy absolwentów śledzone są przez Wydział przez utrzymanie więzi i kontaktów z absolwentami. Usystematyzowane badania prowadzone są w ramach Uczelni przez Dział Badan i Analiz oraz Biuro Karier. Biuro Karier prowadzi „Monitoring Karier Zawodowych Absolwentów PW", w formie cyklicznego badania ilościowego. Wyniki badania MKZA były analizowane na posiedzeniach: Komisji Wydziałowych, Spotkań Opiekunów kierunku ze strony Wydziałów, Kolegium dziekańskim. Jednym z wniosków analiz badania jest: konieczność zwiększenia udziału absolwentów, w tym celu rozwijane są strony Wydziałowe. Politechnika Warszawska realizuje dwa badania absolwentów PW:

- a. badania ilościowe pt. „Monitoring Karier Zawodowych Absolwentów PW" (które w 2021 r. zostało przeprowadzone po raz 10), dostęp: https://das.pw.edu.pl/Raporty-i-publikacje/Badania-absolwentow/MKZA-Monitoring-Karier-Zawodowych-Absolwentow/Poprzednie-edycje-badania-MKZA
- b. badania jakościowe pt. „Success Stories. Absolwenci Politechniki Warszawskiej – diagnoza czynników wspierających osiąganie sukcesu zawodowego", dostęp: https://das.pw.edu.pl/Raporty-i-publikacje/Badania-absolwentow/Success-stories.-Absolwenci-PW

Wyniki badań w postaci raportów i sprawozdań były przedstawiane na spotkaniach z Wydziałowym Pełnomocnikiem ds. Jakości Kształcenia, na posiedzeniach Uczelnianej Rady ds. Jakości Kształcenia, Radzie Wydziału oraz seminariach organizowanych przez DAS (wcześniejsza nazwa jednostki Dział Badań i Analiz CZIiTT).

Na zlecenie Prorektora ds. Studenckich Dział Analiz Strategicznych w 2024 r. zrealizował także badanie Motywacje wyboru studiów I stopnia w PW (2024.01)

W 2024 r. przeprowadzono także diagnozę zjawiska drop-outu w celu poznania przyczyn przedwczesnego kończenia nauki i przerywania kształcenia: Wyniki analizy i diagnoza przyczyn zjawiska przedwczesnego kończenia nauki i przerywania kształcenia w PW (drop out).

Kryterium 4. Kompetencje, doświadczenie, kwalifikacje i liczebność kadry prowadzącej kształcenie oraz rozwój i doskonalenie kadry

4.1. Liczba, struktura kwalifikacji oraz dorobek naukowy nauczycieli akademickich oraz innych osób prowadzących zajęcia ze studentami na ocenianym kierunku, jak również ich kompetencji dydaktycznych (z uwzględnieniem przygotowania do prowadzenia zajęć z wykorzystaniem metod i technik kształcenia na odległość oraz w językach obcych). W tym kontekście warto wymienić najważniejsze osiągnięcia dydaktyczne jednostki z ostatnich 5 lat w zakresie ocenianego kierunku studiów (własne zasoby dydaktyczne, podręczniki autorstwa kadry, miejsca w prestiżowych rankingach dydaktycznych, popularyzacja)

Szczegółowe sylwetki osób zatrudnionych na stanowiskach naukowo-dydaktycznych i dydaktycznych osób, które prowadzą zajęcia na kierunku Cyberbezpieczeństwo zamieszczono w Załączniku ***2.4.Charakterystyki.***

Wśród osiągnięć wskazywanych przez nauczycieli akademickich (załącznik ***2.4.Charakterystyki***) są:

- wspólne publikacje naukowe ze studentami w tym w wysoko punktowanych czasopismach także z listy JCR i konferencyjne,
- opracowanie nowych przedmiotów,
- zdobycie doświadczenia związanego z różnym podejściem do kształcenia, a także w czasie staży naukowych w ośrodkach Uniwersyteckich.

Dydaktycy biorą udział w szkoleniach, kursach i warsztatach dydaktycznych. W programie Kompetentny wykładowca, organizowanym przez Dział Szkoleń CZIiTT pracownicy z obsady kierunku uczestniczyli w kilkudziesięciu szkoleniach. Kursy obejmują takie obszary kompetencji dydaktycznych jak: innowacyjne umiejętności dydaktyczne, umiejętności informatyczne, umiejętności prezentacyjne, a także w zakresie prowadzenia dydaktyki w języku obcym i zarządzania informacją, autoprezentacji, emisji głosu, technik tworzenia prezentacji w tym multimedialnych i narzędzi zdalnych.

Nauczyciele akademiccy posiadają kompetencje językowe potwierdzone licznymi publikacjami w renomowanych czasopismach. Ponadto Uczelnia umożliwia pracownikom rozwój kompetencji językowych oferując specjalistyczne kursy języka angielskiego.

W odniesieniu do osiągnięć Uczelni należy przywołać wysoką pozycję Politechniki Warszawskiej w rankingu Perspektyw a w kategorii Absolwent na rynku i Prestiż, w których to kategoriach Uczelnia jest w ścisłej czołówce.

4.2. Obsada zajęć, ze szczególnym uwzględnieniem zajęć, które prowadzą do osiągania przez studentów kompetencji zawiązanych z prowadzeniem działalności naukowej oraz inżynierskich (w przypadku, gdy oceniany kierunek prowadzi do uzyskania tytułu zawodowego inżyniera lub magistra inżyniera)

Przedmioty techniczne (prowadzące do osiągania kompetencji inżynierskich) prowadzone są przez nauczycieli akademickich wyznaczanych przez Dziekana i posiadających odpowiednie kompetencje w zakresie prowadzonej tematyki, co zapewnia osiągnięcie wymaganych efektów uczenia się. Dorobek wybranych wykładowców jest bardziej szczegółowo wykazany w załączniku ***2.4.Charakterystyki***, ***2.2.Obsada.***

Przedmioty podstawowe prowadzą pracownicy rekrutujący się z różnych jednostek Uczelni (np. wydziału Matematyki i Nauk Informacyjnych, Wydziału Fizyki). Przedmioty specjalistyczne, bezpośrednio dotyczące informatyki, elektroniki i telekomunikacji, prowadzone są przede przez pracowników wszystkich instytutów WEiTI.

4.3. Łączenie przez nauczycieli akademickich i inne osoby prowadzące zajęcia działalności dydaktycznej z działalnością naukową oraz włączanie studentów w prowadzenie działalności naukowej

Na podstawie formalnego przeglądu tematyki prac dyplomowych, stwierdzono bezpośrednie odniesienia do prowadzonej działalności naukowej tj. do tematów badawczych (grantów, projektów) w przeważającej części prac dyplomowych. Prace te realizowane są najczęściej z użyciem infrastruktury badawczej Wydziału. Wymiernym wskaźnikiem udziału studentów są wspólne publikacje, także w renomowanych czasopismach. W przypadku realizacji prac o charakterze pomocniczym, bez istotnego udziału w rozwiązaniu problemu naukowego, częstą praktyką są podziękowania. Szczegółowy opis łączenia przez nauczycieli akademickich i inne osoby prowadzące zajęcia działalności

dydaktycznej z działalnością naukową oraz włączanie studentów w prowadzenie działalności naukowej zostały omówione w Kryterium 1.5.

4.4. Założenia, cele i skuteczność prowadzonej polityki kadrowej, z uwzględnieniem metod i kryteriów doboru oraz rekrutacji kadry, sposobów, zasad i kryteriów oceny jakości kadry oraz udziału w tej ocenie różnych grup interesariuszy, w tym studentów, a także wykorzystania wyników oceny w rozwoju i doskonaleniu kadry

Na kierunku **Cyberbezpieczeństwo** zatrudniani są pracownicy prowadzący badania naukowe oraz publikujący w liczących się czasopismach o zasięgu międzynarodowym oraz aplikujący o granty badawcze. Jest to także kryterium awansów na stanowiska np. profesora uczelni w grupie osób ze stopniem doktora habilitowanego. Doskonalenie kompetencji kadry wspierają procesy oceny w tym: oceny okresowej nauczyciela akademickiego i oceny procesu kształcenia ze strony studentów w formie anonimowej ankietyzacji zajęć. Ankietyzacja jest prowadzona dla wszystkich przedmiotów. Z wynikami obu ocen zapoznaje się indywidualnie każdy nauczyciel i jego bezpośredni przełożony.

Z inicjatywy studentów jest też organizowany plebiscyt Złotej Kredy na najlepszego nauczyciela w różnych kategoriach.

W polityce kadrowej Wydziału zwraca się szczególną uwagę na wymianę pokoleniową kadry oraz awanse pracowników. Zgodnie ze Sprawozdaniem Dziekana WEiTI w roku 2020 miało miejsce 9 awansów (w tym 4 profesorów i profesorów uczelni), zatrudniono 26 osób na stanowiskach asystentów lub adiunktów, przy odejściu 15 osób. W 2021 roku nastąpiło 20 awansów (w tym 12 profesorów i profesorów uczelni). 16 osób zostało zatrudnionych (w tym dwóch profesorów), odeszło 7 osób. W 2022 roku 21 awansów (5 profesorów i profesorów uczelni) Zatrudniono 22 osoby przy 9 odejściach. Rok 2023 w obszarze kadrowym przyniósł 10 awansów na stanowisko adiunkta. Odeszło 15 osób, a zatrudniono 26 osób. W roku 2024 pięciu pracowników WEiTI otrzymało tytuł naukowy, jedna osoba uzyskała stopień doktora habilitowanego. 8 aktualnych pracowników WEiTI w 2024 uzyskało stopień doktora.

Podstawowym elementem polityki kadrowej są otwarte konkursy. Komisje konkursowe powoływane w tym celu określają zasady rozpisywanych konkursów zgodnie z zaleceniami Europejskiej Karty Naukowca (EKN) oraz określonymi zarządzeniami Rektora. Ważnymi kryteriami w ocenie kandydatów na stanowiska naukowo-dydaktyczne jest dorobek publikacyjny, udział w projektach badawczych, doświadczenia zdobyte w ośrodkach zagranicznych. Strategia rozwoju młodej kadry zakłada systematyczne zatrudnianie najlepszych absolwentów studium doktoranckiego (obecnie szkół doktorskich) oraz osób posiadających doświadczenie w firmach komercyjnych.

W doskonaleniu kadry wykorzystywany jest system oceny okresowej pracowników oraz ankietyzacja prowadzonych zajęć dydaktycznych, realizowana dla wszystkich przedmiotów w formie anonimowej przez studentów oraz hospitacje zajęć dydaktycznych. Wspomagana jest działalność badawcza i publikacyjna.

4.5. System wspierania i motywowania kadry do rozwoju naukowego lub artystycznego oraz podnoszenia kompetencji dydaktycznych. W tym kontekście warto przedstawić awanse naukowe kadry związanej z ocenianym kierunkiem studiów

W ramach wsparcia i motywowania kadry są oferowane przez jednostki centralne PW szkolenia takie jak np.: nowe programy oferujące wizyty studyjno–szkoleniowe w czołowych światowych uczelniach zagranicznych, studia podyplomowe w obszarze podnoszenia kompetencji zarządczych, coaching indywidualny i zespołowy, specjalistyczne szkolenia certyfikowane.

Istotnym elementem systemu jest podejście indywidualne. Na poziomie wydziałów i zakładów polega to na wspieraniu rozwoju poszczególnych pracowników (w obszarach naukowym, dydaktycznym i organizacyjnym) z uwzględnieniem ich potencjału osobistego.

System wspierania i motywowania kadry do rozwoju naukowego obejmuje:

- przyznawanie grantów badawczych wspierających prowadzenie działalności naukowej w ramach środków finansowych pochodzących z subwencji na Wydziale;
- przyznawanie grantów w ramach "Inicjatywa Doskonałości–Uczelnia Badawcza" IDUB;
- przyznawanie nagród za osiągniecia naukowe w ramach Projektu "Inicjatywa Doskonałości–Uczelnia Badawcza" (IDUB);
- nagrody Rektora za osiągnięcia naukowe;
- możliwość obniżania pensum dydaktycznego w przypadku kierowania grantami zewnętrznymi pozyskanymi w drodze konkursów;
- organizowanie seminariów naukowych w ramach jednostek i konferencji;
- możliwość korzystania ze staży zagranicznych (płatne urlopy naukowe);
- bezpłatne szkolenia w zakresie wykorzystania narzędzi i technologii informatycznych w procesie dydaktycznym.

System wspierania i motywowania kadry do podnoszenia kompetencji dydaktycznych obejmuje:

- szkolenia, na których mogą rozwinąć kompetencje w zakresie innowacyjnych umiejętności dydaktycznych, informatycznych, prezentacyjnych, a także w zakresie prowadzenia dydaktyki w języku obcym i zarządzania informacją. Szkolenia realizowane były w ramach projektów NERW i NERW2 realizowanych w latach 2018-2023 w PW;
- szkolenia w ramach projektu „Politechnika Warszawska Ambasadorem Innowacji na Rzecz Dostępności" (finansowanie z Programu Operacyjny Wiedza Edukacja Rozwój), którego celem było zwiększenie poziomu dostosowania Politechniki Warszawskiej do potrzeb osób z niepełnosprawnościami m.in. w zakresie procedur kształcenia i wyposażenia pracowników w umiejętności przydatne w kontakcie z osobami z różnymi niepełnosprawnościami;
- staże dydaktyczne w ramach projektu ENHANCE, ERASMUS+,
- przyznawanie przez Samorząd Studencki nagród w konkursie „Złota Kreda" dla najlepszych nauczycieli akademickich (w kategoriach: prowadzący wykłady, prowadzący ćwiczenia/ laboratoria/projekty, najbardziej przyjazny studentom);
- w początkowym okresie pandemii na Uczelni i Wydziale przeprowadzono szkolenia wspomagające umiejętność zdalnego nauczania. Wszyscy zainteresowani pracownicy mieli możliwość w nich uczestnictwa. W miarę możliwości finansowych realizowane są zakupy nowego sprzętu komputerowego (laptopy, tablety graficzne, kamery, głośniki);
- działalność Studium Języków Obcych skierowana do pracowników: pomoc w tłumaczeniach, konsultacje językowe, wsparcie metodyczno-językowe.

W przypadku Wydziału wsparcie polega na głównie na rozwój naukowym pracowników poprzez:

- możliwość uzyskania na wydziale stopnia naukowego (posiadanie uprawnień do nadawania stopni naukowych),
- rozwój studiów doktoranckich, udział pracowników Wydziału w Radzie Szkoły Doktorskiej,
- rozwijanie współpracy krajowej i międzynarodowej umożliwiającej odbywanie przez pracowników staży w wiodących krajowych i zagranicznych placówkach naukowych,

- prowadzenie projektów badawczych,
- prowadzenie systemu motywującego pracowników naukowych do pozyskiwania środków na prowadzenie badań (w tym w ramach międzynarodowych programów badawczych) oraz do aktywnej działalności publikacyjnej (nagrody Dziekana, Rektora, Ministra),
- rozwój infrastruktury potrzebnej do prowadzenia badań.

System wspierania i motywowania kadry do rozwoju i awansów w obszarach naukowym, dydaktycznym i organizacyjnym przebiega dwutorowo.

Pierwszym elementem systemu jest podejście indywidualne zmierzające do utrzymywania i rozwijania jednostek organizacyjnych zgodnie z obowiązującymi przepisami. Na poziomie instytutów i zakładów polega to na wspieraniu rozwoju poszczególnych pracowników (w obszarach naukowym, dydaktycznym i organizacyjnym) z uwzględnieniem ich potencjału osobistego. Wsparcie finansowe rozwoju naukowego obejmuje m.in. granty dla młodych naukowców (dziekańskie, rektorskie), granty dydaktyczne (Rektora), nagrody za publikacje naukowe (na Wydziałach i przyznawane przez Rektora), nagrody dydaktyczne (Rektora). Przyznawanie dodatku za aktywność na aktualny rok za wkład w rozwój Wydziału w poprzednim roku.

Innym elementem wystąpienia sytuacji konfliktowych, przejawów mobbingu lub dyskryminacji pracownicy mogą korzystać ze wsparcia rzeczników zaufania. Politykę Uczelni oraz regulacje prawne w tym zakresie ustalają dokumenty m.in. Zarządzenie Rektora PW 176/2020 w sprawie przeciwdziałania mobbingowi i dyskryminacji w Politechnice Warszawskiej oraz Pismo Okólne nr 3/2021 Rektora PW określające Politykę przeciwdziałania mobbingowi i dyskryminacji w Politechnice Warszawskiej. Corocznie prowadzona jest także przez Dział Analiz Strategicznych (DAS) ankieta samooceny wydziałów zawierająca także pytania dotyczące sytuacji konfliktowych.

Przybliżenie specjalizacji kadry Politechniki Warszawskiej było możliwe dzięki katalogom B+R, prezentującym zespoły badawcze PW. Taki katalog powstał również dla Wydziału EiTI:

- Zespoły Badawcze Politechniki Warszawskiej. Oferta B+R, Warszawa 2022, dostęp: https://www.cziitt.pw.edu.pl/wp-content/uploads/2022/12/KATALOGWEITI.pdf

W zakresie badania kompetencji kadry na zlecenie Działu ds. Szkoleń przeprowadzane były badania potrzeb szkoleniowych, dzięki którym możliwe jest dostosowanie oferty dodatkowych kursów dla osób pracujących na PW. Wyniki przedstawia seria raportów:

- Profesjonalizacja szkoleń w PW. Potrzeby jednostek organizujących szkolenia w zakresie informowania (2023.01)
- Profesjonalizacja szkoleń w PW. Dobre praktyki wiodących uczelni w zakresie szkoleń kadry uczelni (2023.02)
- Profesjonalizacja szkoleń w PW. Potrzeby osób uczestniczących w szkoleniach w zakresie informowania o szkoleniach – perspektywa odbiorcy (2023.03)

Dodatkowe informacje, które uczelnia uznaje za ważne dla oceny kryterium 4

Trzon kadry akademickiej prowadzącej zajęcia na kierunku **Cyberbezpieczeństwo** stanowią pracownicy Zakładu Cyberbezpieczeństwa. W gronie kilkunastu nauczycieli akademickich tego Zakładu znajduje się pięcioro laureatów Złotej Kredy – wyróżnienia przyznawanego corocznie przez Wydziałową Radę Samorządu dwóm najwyżej ocenianym przez studentów nauczycielom Wydziału.

Kryterium 5. Infrastruktura i zasoby edukacyjne wykorzystywane w realizacji programu studiów oraz ich doskonalenie

5.1. Stan, nowoczesność, rozmiar i kompleksowości bazy dydaktycznej i naukowej służącej realizacji zajęć oraz działalności naukowej na ocenianym kierunku w dyscyplinie, do której kierunek jest przyporządkowany

Studenci kierunku **Cyberbezpieczeństwo** korzystają z infrastruktury dydaktycznej w Gmachu Wydziału Elektroniki i Technik Informacyjnych im. prof. Janusza Groszkowskiego (Gmachu Elektroniki) położonym przy ul. Nowowiejskiej 15/19.

Przykładowo w Gmachu Elektroniki znajdują się sale wykładowe o powierzchni ponad 2500 m2 wyposażone w rzutniki multimedialne. Na WEiTI znajduje się ponad 100 laboratoriów o łącznej powierzchni ok. 6000 m2. Część laboratoriów to laboratoria komputerowe, inne to laboratoria specjalistyczne, w których są prowadzone zajęcia wykorzystujące specjalistyczny sprzęt i/lub oprogramowanie.

Infrastruktura architektoniczna Gmachu Elektroniki i Gmachu Głównego jest przystosowana do potrzeb osób z niepełnosprawnością. W budynkach znajdują się podjazdy, windy oraz WC dla osób z niepełnosprawnością. Szczegółowy opis bazy dydaktycznej zamieszczono w załączniku ***2.5.Baza***.

5.2. Infrastruktura i wyposażenie instytucji, w których prowadzone są zajęcia poza uczelnią oraz praktyki zawodowe (w przypadku, gdy w planie studiów na ocenianym kierunku zostały uwzględnione praktyki zawodowe)

Wszystkie zajęcia na kierunku **Cyberbezpieczeństwo** są prowadzone w pomieszczeniach znajdujących się na uczelni. Nie dotyczy to w sposób oczywisty praktyk zawodowych, prowadzonych u różnych pracodawców.

Inne zajęcia, obejmują ok. 5% wszystkich zajęć i należą do nich np. wychowanie fizyczne są prowadzone w obiektach sportowych PW (np. stadion, sale sportowe Riwiery, basen).

5.3. Dostęp do technologii informacyjno-komunikacyjnej (w tym Internetu a także platformy e-learningowej, w przypadku, gdy na ocenianym kierunku prowadzone jest kształcenie z wykorzystaniem metod i technik kształcenia na odległość) oraz stopnia jej wykorzystania w procesie nauczania i uczenia się studentów oraz w działalności i komunikacji naukowej

Niemal wszystkie pomieszczenia w Gmachu Elektroniki i Gmachu Głównym znajdują się w zasięgu sieci bezprzewodowej, która jest dostępna dla wszystkich pracowników i studentów. Wszystkie laboratoria komputerowe mają dostęp do Internetu (złącze światłowodowe)

W ramach e-usług na kierunku funkcjonuje platforma edukacyjna LeON oraz uczelniany system informatyczny USOS. Studenci kierunku rejestrują się (zapisują) na przedmioty w systemie USOS. USOS wykorzystywany jest również jako narzędzie administracyjne, obsługa podań, wraz z APD – procesu dyplomowania, służy do obsługi rejestracji postępów studentów. Posiada też (ograniczone) możliwości komunikowania się asynchronicznego ze studentami. W procesie dydaktycznym wykorzystywana jest platforma edukacyjna LeON, służąca do umieszczania materiałów dydaktycznych, przeprowadzania testów i zadań oraz komunikacji ze studentami. Dla każdego przedmiotu założona jest witryna przedmiotu (kurs), a uczestniczący w kursie studenci są automatycznie przenoszeni z systemu zapisów w USOS. Poza tym platforma zawiera informacje i ogłoszenia istotne dla wszystkich jej użytkowników. Platforma jest dodatkowa zintegrowana z narzędziem do komunikacji synchronicznej (wideo spotkań) Big Blue Button - BBB. Wszyscy studenci PW mają dostęp do narzędzi MS Office 365, a przez to również do kolejnego narzędzia do komunikacji synchronicznej – MS Teams. Wszystkie wymienione powyżej

narzędzia są intensywnie wykorzystywane przez studentów i wykładowców kierunku **Cyberbezpieczeństwo**, a ich obsługą i pomocą użytkownikom zajmuje się dział IT.

5.4. Udogodnienia w zakresie infrastruktury i wyposażenia dostosowanych do potrzeb studentów z niepełnosprawnością

W wyniku realizacji w kilku ostatnich latach projektów inwestycyjnych, wszystkie budynki WEiTI i Gmach Główny są przystosowane do potrzeb studentów z niepełnosprawnością. W obu budynkach znajdują się wejścia i windy przystosowane dla osób z niepełnosprawnością oraz toalety przystosowane dla osób niepełnosprawnych. Szczegółowe informacje przedstawiono w odpowiednich sekcjach raportu, m.in. w Kryterium 2.4 oraz załączniku ***Bib.Niepelnos***.

5.5. Dostępność infrastruktury, w tym aparatury naukowej, oprogramowania specjalistycznego i materiałów dydaktycznych, w celu wykonywania przez studentów zadań wynikających z programu studiów w ramach pracy własnej

Zajęcia praktyczne odbywają się w salach laboratoryjnych przeznaczonych zarówno do prowadzenia badań jak i procesu dydaktycznego. W załączniku ***2.5.Baza***, do kryterium 5 zebrano laboratoria o przeznaczeniu naukowo-dydaktycznym wykorzystywane w zajęciach dla kierunku **Cyberbezpieczeństwo**. Są to głównie laboratoria komputerowe lub pracownie dla przedmiotów podstawowych realizowanych na studiach pierwszego i drugiego stopnia.

Dystrybucją oprogramowania podstawowego (np. systemów operacyjnych), jak również specjalistycznego, inżynierskiego, na uczelni zajmuje się Centrum Informatyzacji PW. Szczegółowe informacje obejmujące wykaz oprogramowania oraz warunki uzyskania licencji (dostępu) są przedstawione na stronie https://www.ci.pw.edu.pl/Uslugi/Dystrybucja-oprogramowania. Centrum organizuje także podstawowe szkolenia z obsługi wybranych pakietów, np. z MATLAB-a.

Na liście programów są: ABAQUS, ANSYS, AUTODESK, LabVIEW, MATHEMATICA, MATLAB, NX, Oprogramowanie firmy MSC Software ORIGIN, Platforma ArcGIS, QuickerSim CFD Toolbox dla oprogramowania Matlab, SAS, SolidEdge, SOLIDWORKS, STATGRAPHICS Centurion, STATISTICA. W Bibliotece Wydziałowej każdego Wydziału i Głównej oraz Filii znajduje się czytelnia internetowa a oprogramowanie biblioteczne dostępne zdalnie, które zapewnia szeroki dostęp do publikacji cyfrowych (szczegóły w załączniku ***Biblioteka***).

Przedmioty na specjalnościach mają część praktyczną i z reguły poprowadzone są w laboratoriach badawczych, często z użyciem sprzętu badawczego.

Do dyspozycji studentów i pracowników Uczelnia udostępnia oprogramowanie m.in. pakiet Office 365, w którym oprócz podstawowych narzędzi biurowych udostępniono także inne narzędzia w tym platformę komunikacji zdalnej MS Teams. Narzędzie to zostało zalecone od marca 2020 do prowadzenia kontaktowo zajęć zdalnych i realizowania innych potrzeb komunikacyjnych. Przeprowadzono liczne szkolenia przygotowujące do korzystania z platformy zarówno dla studentów jak pracowników. Dostępne jest forum informacji i wsparcie techniczne obsługiwane przez Centrum Informatyzacji, które jest ogólnouczelnianą jednostką wspierającą kształcenie zdalne i informatyzację kształcenia i nauki. Prace nad kanałami komunikacji odbywają się obecnie z dużym natężeniem i skutkują udostępnianiem kolejnych kanałów komunikacyjnych.

5.6. System biblioteczno-informacyjnego uczelni, w tym dostępu do aktualnych zasobów informacji naukowej w formie tradycyjnej i elektronicznej, o zasięgu międzynarodowym oraz zakresie dostosowanym do potrzeb wynikających z procesu nauczania i uczenia się na ocenianym kierunku, a także działalności naukowej w zakresie dyscypliny/dyscyplin, do której/których przyporządkowany jest kierunek, w tym w szczególności dostępu do piśmiennictwa zalecanego w sylabusach

Studenci kierunku **Cyberbezpieczeństwo** mają możliwość korzystania z kilku jednostek bibliotecznych na terenie uczelni, w szczególności ze zbiorów Biblioteki, bibliotek instytutowych na WEiTI oraz Biblioteki Głównej PW.

Biblioteka Główna PW, oprócz tradycyjnego dostępu do Wypożyczalni, oferuje dostęp do zasobów elektronicznych.

Obejmuje on następujące bazy danych:

- katalog tradycyjnych zasobów zrealizowany w systemie Aleph, obejmujący księgozbiory wszystkich bibliotek Politechniki;
- bibliotekę cyfrową, zrealizowaną przy użyciu oprogramowania D-libra (zasoby historyczne i archiwalne);
- moduł E-źródła dający dostęp do 127 baz danych bibliograficzno-abstraktowych i pełnotekstowych (160 tys. tytułów książek i 6 tys. tytułów czasopism w dostępie pełnotekstowym). Do najważniejszych komercyjnych baz danych należą Web of Science, Scopus, CSA, PROQUEST, INSPEC, oraz bazy największych wydawców (m.in.: Elsevier, Emerald, Springer, IEEE, ACM DL, Taylor and Francis, Wiley) – co oznacza pełen dostęp do liczących się bazy danych w zakresie cyberbezpieczeństwa;
- Bazę Wiedzy Politechniki Warszawskiej, która obejmuje zasoby piśmiennicze autorstwa pracowników PW (w tym także pełne teksty), prace dyplomowe i rozprawy doktorskie.

Studenci i pracownicy Wydziału mogą korzystać z usług ponad dwudziestu jednostek systemu biblioteczno-informacyjnego Politechniki Warszawskiej, w szczególności: z Bibliotek Wydziałowych, z Biblioteki Głównej, a także Fili Biblioteki Głównej Campusu Południowego. Zbiory Biblioteki PW obejmują zarówno tomy drukowanych książek i czasopism, czasopisma elektroniczne, źródła informacji, książki elektroniczne jak i bazy danych.

Na Uczelni funkcjonuje zintegrowany informatyczny system biblioteczny, który pozwala na jednoczesne przeszukiwanie wszystkich katalogów bibliotek uczelnianych, a także możliwość rezerwowania, zamawiania, wypożyczania i samodzielnego przedłużania terminu wypożyczenia książek, ze zbiorów wybranych bibliotek oraz zdalnego dostępu do zasobów cyfrowych książek i czasopism.

Biblioteka WEiTI w swoich zbiorach posiada 17 198 woluminów (załącznik ***Biblioteka***). Gromadzone są tu dokumenty z zakresu cyberbezpieczeństwa, elektroniki, informatyki, telekomunikacji, inżynierii biomedycznej, automatyki, robotyki i dziedzin ściśle powiązanych z kierunkami Wydziału. Studenci kierunku **Cyberbezpieczeństwo** mają dostęp do tradycyjnych podręczników (w formie drukowanej i elektronicznej). Gromadzenie księgozbioru opiera się na sylabusach i informacji bezpośrednio przekazywanej do Biblioteki przez nauczycieli akademickich, a także przez samych studentów, którzy chcieliby mieć jakiś konkretny tytuł w zbiorach biblioteki, związany z kierunkiem studiów. Zbiory uzupełniamy także o nowości wydawnicze, które nie zawsze znajdują się w sylabusach, ale są literaturą wartościową poszerzającą wiedzę i rozwijającą zainteresowania związane z kierunkiem studiów lub kierunkami pokrewnymi u naszych studentów. Staramy się być Biblioteką, która nie tylko spełnia podstawowe zapotrzebowanie, ale dostarcza materiały, które wychodzą poza programowe minimum i zachęca do korzystania z nich.

Studenci, którzy wybrali kierunek Cyberbezpieczeństwo mają dostęp w Bibliotece Wydziałowej między innymi do takiej literatury z tej dziedziny:

1. Kurz, Constanze : Pożeracze danych. Warszawskie Wydawnictwo Literackie Muza SA, 2013, 3 egz.
2. Drake, Joshua J.: Android™. Helion, cop. 2015, 3 egz.
3. Parker, Carey: Firewall nie powstrzyma prawdziwego smoka, czyli Jak zadbać o cyberbezpieczeństwo, Helion SA, 2019, 2 egz.

4. Krawiec, Jerzy: Cyberbezpieczeństwo. Oficyna Wydawnicza Politechniki Warszawskiej, 2019, 5 egz.
5. Wheeler, David: The IoT architect's guide to attainable security & privacy, CRC Press is an imprint of the Taylor & Francis Group, an informa business, © 2020, 2 egz.
6. Newman, Sam: Building microservices. O'Reilly, cop. © 2021, 2 egz.
7. Kraśniewski, Andrzej: Cybersecurity research, education and management: university perspective, Warsaw University of Technology Press, 2021, 2 egz.
8. Newman, Sam: Budowanie mikrousług. Helion, © 2022, 3 egz.
9. Mitnick, Kevin D.: Duch w sieci. Helion, cop. 2022, 2 egz.
10. Long, David: Podręcznik inżynierii systemów opartej na modelach. Vitech Corporation, Helion, cop. © 2022, 10 egz.
11. Harper, Allen: Gray hat hacking. McGraw Hill, cop. © 2022, 3 egz.
12. Dela, Piotr: Założenia działań w cyberprzestrzeni. PWN, cop. © 2022, 2 egz.
13. Andress, Jason: Podstawy bezpieczeństwa informacji. Helion, cop. © 2022, 2 egz.
14. Tevault, Donald A.: Mastering Linux security and hardening. Packt, cop. © 2023, 2 egz.
15. Ortega Candel, José Manuel: Python for security and networking. Packt, cop. © 2023, 2 egz.
16. Nowocień, Artur: Digitalizacja w systemach automatyki SIMATIC. Helion, cop. 2023, 1 egz.
17. Lat, Joshua Arvin: Building and automating penetration testing labs in the cloud. Packt, 2023, 2 egz.
18. Kofler, Michael: Hacking and security. Rheinwerk Publishing, Inc., © 2023, 2 egz.
19. Kelley, Diana: Practical cybersecurity architecture. Packt, cop. © 2023, 2 egz.
20. Baker, Rae: Deep dive. Wiley, cop. © 2023, 2 egz.
21. Tevault, Donald A.: Bezpieczeństwo systemu Linux. Helion, cop. © 2024, 2 egz.
22. Sehgal, Kunal: Cyberbezpieczeństwo i strategie blue teamów. Helion, © 2024, 2 egz.
23. Rains, Tim: Zagrożenia cyberbezpieczeństwa i rozwój złośliwego oprogramowania. Helion,
24. cop. © 2024, 2 egz.
25. Markstedter, Maria: Niebieski lis. Helion, cop. 2024, 2 egz.
26. Johansen, Gerard: Informatyka śledcza. Helion, © 2024, 2 egz.
27. Enoka, Seth: Cyberbezpieczeństwo w małych sieciach. Helion, © 2024, 2 egz.
28. Bodungen, Clint E.: ChatGPT for cybersecurity cookbook. Packt, cop. © 2024, 2 egz.
29. Baker, Rae: Prawdziwa głębia OSINT. Helion, © 2024, 2 egz.
30. Anderson, Ross: Inżynieria zabezpieczeń : T. 1. PWN, 2024, 1 egz.
31. Anderson, Ross: Inżynieria zabezpieczeń : T. 2. PWN, 2024, 1 egz.
32. Kohnfelder, Loren: Po pierwsze: bezpieczeństwo, Heliion, copyright ©2023, 2 egz.
33. Chantzis, Fotios: Hakowanie internetu rzeczy w praktyce: |b przewodnik po skutecznych metodach atakowania IoT, Helion, 2022, 4 egz.
34. Flow, Sparc: Hakuj jak duch: łamanie zabezpieczeń środowisk chmurowych, Helion, 2022, 35.2 egz.
36. Hickey, Matthew, Warsztat hakera: testy penetracyjne i inne techniki wykrywania podatności, Helion, 2022, 4 egz.
37. Sikorski, Michael, |Praktyczna analiza malware: przewodnik po usuwaniu złośliwego oprogramowania, Helion, 2021, 2 egz.
38. Shetty, Sachin S.: Blockchain i bezpieczeństwo systemów rozproszonych, PWN, 2020, 2 egz.
40. Tanenbaum, Andrew S.: Sieci komputerowe, Helion, 2012, 12 egz.

41. Kurose, James F.: Sieci komputerowe: ujęcie całościowe, Helion, 2019, 33 egz.
42. Kluczewski, Jerzy: Bezpieczeństwo sieci komputerowych: praktyczne przykłady i ćwiczenia w symulatorze Cisco Packet Tracer, iTSt@rt Wydawnictwo informatyczne, 2019, 4 egz.

W Czytelni Cyfrowej studenci mają do swojej dyspozycji 9 stanowisk komputerowych z dostępem do Internetu i pakietem LibreOffice. Wydziałowe Wi-Fi umożliwia im korzystanie z elektronicznych baz naukowych (w sumie 93 bazy), które gromadzą czasopisma recenzowane, zawierające abstrakty lub pełnotekstowe publikacje, m. in. ACM Digital Library, IEEE/IEE Electronic Library, Science Direct on Line, SPIE Digital Library, SpringrLink, JoVe, a także Ebookpoint i Ibuk Libra– gdzie w formie cyfrowej wypożyczalni studenci PW mogą wypożyczyć książki m. in. Wydawnictwa Naukowego PWN, Oficyny Wydawniczej PW, czy Wydawnictwa Helion

W Bibliotece WEiTI zarówno dokumenty tradycyjne, jak i elektroniczne, użytkownicy mogą wyszukać i przeglądać poprzez wyszukiwarkę PRIMO. Biblioteka WEiTI dysponują dwiema czytelniami:

- Czytelnią naukową, w której użytkownicy mają dostęp do naukowych czasopism polsko i angielskojęzycznych, podręczników akademickich oraz nowości wydawniczych tematycznie powiązanych z kierunkami studiów. Czytelnicy mają też dostęp do gniazd elektrycznych, do których mogą podłączyć zasilacze własnych laptopów. Można podłączyć komputer do sieci Wi-Fi, a tym samym można korzystać z elektronicznych źródeł naukowych. Ze zbiorów czytelni mogą na miejscu korzystać wszyscy zainteresowani. Każda z czytelni jednorazowo może pomieścić około 30 osób.
- Czytelnia cyfrowa jest miejscem do pracy w grupach. Można w niej głośno rozmawiać. Jest pomieszczeniem sprzyjającym „burzy mózgów". Znajdują się tam komputery (9) na Wydziale EiTI.
- Biblioteki wyposażone są w komputery z dostępem do Internetu. Użytkownicy mają do swojej dyspozycji 40 miejsc WEiTI. Czytelnia Cyfrowa Biblioteki Wydziału EiTI umożliwia dostęp do wydawnictw naukowych bez konieczności logowania.

W bibliotece Głównej można korzystać ze wsparcia technicznego dla osób z niepełnosprawnością. Osoby poruszające się na wózkach mają łatwy dostęp do Biblioteki, ponieważ mieści się ona na parterze. Przy wejściu głównym do budynku Wydziału jest podjazd.

W samej Bibliotece Czytelnia ogólna znajduje się na niższym poziomie. Ale tutaj również znajduje się podjazd ułatwiający osobom z niepełnosprawnością poruszanie się i korzystanie z Czytelni.

Dla osób poruszających się na wózkach do Czytelni Cyfrowej jest oddzielne wejście z podnośnikiem w skrzydle C budynku Wydziału.

Dla osób niewidomych i słabo widzących, tak jak w całym budynku, w Bibliotece zastosowano tabliczki informacyjne w alfabecie Braille'a (załącznik ***Bib.Niepelnos***)

W ramach współpracy z Sekcją ds. Osób z Niepełnosprawnościami w Politechnice Warszawskiej w 2022 roku otrzymaliśmy elektroniczną lupę dla osób słabo widzących.

W czytelni dysponujemy biurkiem z elektroniczną regulacją wysokości. Jest to udogodnienie nie tylko dla osób poruszających się na wózkach. Dzięki regulacji wysokości biurko można dostosować do wzrostu użytkownika, przez co miejsce nauki staje się bardziej ergonomiczne i wygodne.

W styczniu 2023 roku powstał plakat informacyjny dotyczący sprzętu, który znajduje się w poszczególnych bibliotekach PW i ma za zadanie ułatwić osobom z niepełnosprawnościami dostęp do różnych publikacji, czy pomóc w przygotowaniu materiałów na zajęcia. Plakat był owocem współpracy Biblioteki WEiTI z Biblioteką Główną i pozostałymi bibliotekami PW.

Na stronie Biblioteki Głównej w zakładce „Biblioteka bez barier" są zamieszczane i aktualizowane informacje o infrastrukturze ułatwiającej dostęp do zasobów bibliotecznych w bibliotekach PW. https://bg.pw.edu.pl/index.php/o-nas/biblioteka-bez-barier

5.7. Sposoby, częstotliwość i zakres monitorowania, oceny i doskonalenia bazy dydaktycznej i naukowej oraz systemu biblioteczno-informacyjnego, a także udziału w ocenie różnych grup interesariuszy, w tym studentów

Baza dydaktyczna monitorowana jest co roku, a jej stan raportowany w sprawozdaniu Wydziału dla Rektora. Przeglądy BHP prowadzone są dla wszystkich pomieszczeń przed rozpoczęciem zajęć. W ramach przygotowania merytorycznego opiekunowie przedmiotów przygotowują i oceniają na własne potrzeby stan używanego sprzętu.

Potrzeby modernizacji, doskonalenia oraz tworzenia nowych stanowisk oraz laboratoriów specjalistycznych mogą być zgłaszane przez studentów co semestr w ramach cyklicznych akcji ankietyzacji zajęć dydaktycznych. W jednostkach przeprowadzana jest okresowa ocena stanu technicznego pomieszczeń laboratoryjnych i pracowniczych. Każde z laboratoriów ma kierownika, który na bieżąco monitoruje stan aparatury i wyposażenia.

Zespół biblioteczny wychodzi naprzeciw oczekiwaniom użytkowników poprzez rozwijanie i przystosowywanie dla nich pomieszczeń bibliotecznych, a także rozwijanie własnych kompetencji.

- Od 2015 roku studenci mają Czytelnię cyfrową, miejsce do pracy grupowej, tworzenia różnych projektów, wspólnego uczenia się. Tutaj można korzystać z wydziałowego Wi-Fi i bez konieczności logowania czerpać informacje z e-źródeł. Jest to także miejsce relaksu, czemu służą miękkie pufy i sofy.
- Wprowadzenie komputerowego systemu Aleph (2009 r.) pozwoliło na całkowite zautomatyzowanie Biblioteki. Aleph zintegrował konta biblioteczne czytelników w Bibliotece Głównej i Bibliotece Wydziałowej, jak również w innych bibliotekach systemu uczelnianego, które przystąpiły do Sieci Bibliotek PW. Czytelnicy od tej pory mają jedną kartę biblioteczną, którą stała się legitymacja (w przypadku studentów). Jest to olbrzymie ułatwienie dla studenta, który wszystkie swoje wypożyczenia z bibliotek PW widzi na jednym koncie. Może sam monitorować swoje zamówienia, wypożyczenia, zwroty i prolongaty. System także przypomina o zbliżających się terminach zwrotów wysyłając czytelnikom monity. Aleph to wreszcie system, który pozwala użytkownikom zamawiać literaturę online. Czytelnicy również mogą samodzielnie trzykrotnie przedłużyć swoje wypożyczenia.
- Od października 2020 roku istnieje możliwość wypełnienia deklaracji i zapisania się do Biblioteki online. Czytelnicy nie muszą osobiście pojawiać się w tym celu w Bibliotece. Bardzo to usprawniło naszą pracę i przyczyniło się do poprawy jakości usług. Skróciły się kolejki w wypożyczalni, a studenci mogą szybciej odebrać swoje zamówienia, ponieważ nie są blokowani przez osoby, które dopiero chcą założyć konto biblioteczne. Oczywiście jeżeli ktoś poprosi o założenie konta i w tym celu przyjdzie do biblioteki – taką usługę od nas otrzyma, ale dzięki aktywacji online, zdarza się to teraz sporadycznie, a czytelników wcale nie ubywa.
- Od 2022 roku system Aleph synchronizuje się z systemem USOS i dzięki temu precyzyjnie ustawia ważność kont bibliotecznych naszych studentów. Zasady są transparentne. Przestały być problemem sytuacje, braku identyfikacji, czy student kontynuuje naukę na II stopniu, czy już zakończył.
- Biblioteka prowadzi działalność dydaktyczną: dla studentów I semestru naszego Wydziału prowadzimy przysposobienie biblioteczne.

- Zespół biblioteczny służy każdemu informacją o tym, jak sporządzić przypisy i bibliografię załącznikową w pracy dyplomowej, informuje o specjalnych do tego celu programach tj. Zotero czy Mendeley. Studenci mogą także skorzystać z prezentacji na ten temat, zamieszczonej na stronie Biblioteki.
- Na stronie internetowej Wydziału w zakładce „Biblioteka" umieszczony jest krótki film prezentujący kandydatom i studentom wydziałową Bibliotekę https://www.youtube.com/watch?v=fs3XtT21ADQ&t=16s
- Gromadzenie zbiorów zostało oparte na wywiadzie i ankietach studentów. Każdy członek społeczności wydziałowej jest zaproszony do zgłaszania literatury związanej z kierunkami studiów na Wydziale i wzbogacającej istniejący już księgozbiór.
- W Czytelni znajduje się komputer, umożliwiający studentom przeglądanie prac doktorskich powstałych w PW. Komputer przeznaczony jest jedynie do tego celu (zablokowane połączenia wychodzące TCP do innych adresów aniżeli repo.pw.edu.pl, cas.usos.pw.edu.pl i fonts.googleapis,com; a także zablokowana możliwość podłączenia urządzeń pamięci masowej USB; czy też funkcja printscreen).

Kryterium 6. Współpraca z otoczeniem społeczno-gospodarczym w konstruowaniu, realizacji i doskonaleniu programu studiów oraz jej wpływ na rozwój kierunku

6.1. Zakres i formy współpracy uczelni z instytucjami otoczenia społeczno-gospodarczego, w tym z pracodawcami oraz jej wpływu na koncepcję kształcenia, efekty uczenia się, program studiów i jego realizację, w tym realizację praktyk zawodowych (w przypadku, gdy w planie studiów na ocenianym kierunku zostały uwzględnione praktyki zawodowe)

Zakres i formy współpracy Wydziału z instytucjami otoczenia społeczno-gospodarczego, monitorowane i analizowane są cyklicznie zarówno na poziomie centralnym Uczelni, jak i na poziomie Wydziału.

Współpraca na poziomie Wydziału obejmuje takie działania jak: praktyki i staże, wspólne prace dyplomowe, projekty badawcze realizowane ze studentami, udział w wydarzeniach takich jak targi w tym targi pracy, konferencje, wykłady i zajęcia zapraszane, wizyty i wycieczki, wolontariat, szkolenia, użyczenie sprzętu. W czasie tych kontaktów uzyskiwana jest wiedza o potrzebach rynku pracy i otoczenia społeczno-gospodarczego, a także jest zbierana opinia o spełnieniu tych oczekiwań przez kompetencje absolwentów i studentów. Informacje te są przedmiotem dyskusji w ramach Rady Wydziału, Seminariów Wydziałowych i spotkań Komisji Wydziałowych oraz opiekunów specjalności i kierunków. Wyniki są dostępne w sprawozdaniach Wydziału.

W odniesieniu do praktyk (częściowo omówione w opisie Kryterium 2), współpraca polega na przyjmowaniu studentów przez firmy (na 4 tygodnie) na podstawie porozumienia. Ocena osiągania efektów uczenia się jak i przygotowania studenta po 3 roku studiów do podjęcia działalności zawodowej prowadzona jest zarówno przez opiekuna praktyk ze strony firmy, opiekuna praktyk dla specjalności ze strony Wydziału jak i samego studenta w formie ankiety. Ocena osiągnięcia efektów uczenia przez opiekuna ze strony przemysłu niesie informację o przygotowaniu praktykanta, a zatem pośrednio o ocenie programach studiów i skuteczności jego realizacji. Samoocena studenta w ankiecie po praktykach dotycząca przydatności wiedzy i umiejętności uzyskanych w toku studiów jest podstawą do wniosków i dalszych konsultacji z otoczeniem gospodarczym.

Wydział współpracuje ze szkołami średnimi w procesie dydaktycznym. Uczniom szkół średnich udostępnianie są pracownie i laboratoria Wydziału, ponadto wybrane zajęcia z uczniami prowadzone są przez nauczycieli akademickich. Uczniom szkół średnich udostępniane są również zasobowy biblioteczne Wydziału, w tym źródła elektroniczne.

W 2019 roku zmienił się profil podejmowanych w ramach Wszechnicy działań mających na celu popularyzację wiedzy i promowanie Wydziału w środowisku młodzieży szkół średnich. W 2019 roku w ramach współpracy Wydziału z Ośrodkiem Edukacji Informatycznej i Zastosowań Komputerów w Warszawie oraz XXVII Liceum Ogólnokształcącym im. Tadeusza Czackiego w Warszawie Centrum został powołany Projekt Edukacyjny Stem PW. W jego ramach został zorganizowany pierwszy ogólnopolski konkurs STEM PW. W pierwszej edycji wzięło udział blisko 1000 uczniów z całej Polski. Warto podkreślić, że w trakcie drugiego etapu konkursu organizowane są warsztaty i szkolenia dla nauczycieli. Natomiast trzeci praktyczny etap jest poprzedzony warsztatami dla uczestników, którzy zakwalifikowali się do finału. Pomysł okazał się dużym sukcesem. W jego efekcie powstał też Rabyte - liczący ponad 20 osób zespół uczniów szkół średnich. Zespół ten w lutym 2020 roku wziął udział w międzynarodowym konkursie FIRST Robotics Competitions w Stambule. Patronat nad zespołem objął Wydział Elektroniki i Technik informacyjnych.

W drugiej edycji konkursu w 2020 roku wzięło udział blisko 1200 uczniów. Ze względu na wystąpienie stanu epidemii nie odbył się trzeci etap konkursu. Laureaci i finaliści zostali wyłonieni na podstawie rezultatów drugiego etapu.

Po rocznej przerwie związanej z pandemią COVID-19 organizatorzy projektu STEM PW w porozumieniu ze środowiskiem nauczycieli szkół średnich postanowili zorganizować trzecią edycję tego konkursu. W grudniu 2021 został przeprowadzony pierwszy szkolny etap, do którego przystąpiło 501 uczniów z 47 szkół z całej Polski. Do drugiego etapu zostało zakwalifikowanych 88 uczniów w tym 57 osób ze szkół warszawskich i 31 osób spoza stolicy. Warto zaznaczyć, że do konkursu zgłosiły się szkoły znajdujące się w ścisłej czołówce rankingu Perspektyw a patronat nad konkursem objęły: Ministerstwo Edukacji i Nauki oraz Narodowe Centrum Badań i Rozwoju.

W chwili obecnej rozpoczynają się przygotowania do kolejnej – piątej edycji konkursu. https://stem.pw.edu.pl/

Znaczenie współpracy z podmiotami zewnętrznymi jest jednym z priorytetów w polityce Wydziału.

Wydział Elektroniki i Technik Informacyjnych przywiązuje dużą wagę do współpracy z otoczeniem społeczno-gospodarczym. Na stronie internetowej:

http://www.elka.pw.edu.pl/Wydzial/Wspolpraca/Wspolpraca-z-przemyslem-administracja-i biznesem/

można znaleźć listę instytucji, z którymi podpisane zostały umowy o współpracy lub listy intencyjne. Współpraca Wydziału WEiTI obejmuje ponad 60 przedsiębiorstw przemysłowych, jednostek administracyjnych i firm biznesowych.

Współpraca ma na celu przygotowanie i realizację projektów badawczych i rozwojowych, pozostających we wspólnym zainteresowaniu stron; wymianę specjalistów, naukowców, studentów (w tym realizację praktyk zawodowych); wspólnych publikacji, organizacji i udziału w konferencjach. Współpraca z instytucjami zewnętrznymi ma istotny wpływ na kształtowanie programu studiów przez przekazywanie potrzeb pracodawców w zakresie wymaganych kompetencji absolwentów. Potrzeby gospodarcze omawiane są z członkami Stowarzyszenia Absolwentów i Przyjaciół WEiTI. Promowane jest prowadzenie prac dyplomowych we współpracy z przedsiębiorstwami.

6.2. Sposoby, częstotliwość i zakres monitorowania, ocena i doskonalenie form współpracy i wpływu jej rezultatów na program studiów i doskonalenie jego realizacji

Zadania na poziomie Uczelni koordynuje Dział Analiz Strategicznych (DAS), będące jednostkami Centrum Zarządzania Innowacjami i Transferem Technologii.

Od dnia 1 maja 2023 r. Centrum Zarządzania Innowacjami i Transferem Technologii rozwinęło się w 3 odrębne jednostki:

=> Centrum Projektów Rozwojowych (CPR) – www.cpr.pw.edu.pl,

=> Centrum Innowacji (CINN),

=> Dział Analiz Strategicznych (DAS).

Monitorowanie potrzeb otoczenia społeczno-gospodarczego – badanie „Diagnoza potrzeb pracodawców i instytucji współpracujących z PW" – przebiega dwutorowo poprzez:

- panele pracodawców (spotkania z pracodawcami organizowane w ramach dyscyplin naukowych), które mają charakter moderowanych badań jakościowych,
- badania ankietowe.

Wyniki badań, w postaci raportów i sprawozdań były przedstawiane na spotkaniach z Wydziałowym Pełnomocnikiem ds. Jakości Kształcenia oraz Radzie Wydziału.

- Diagnoza potrzeb pracodawców – dyscyplina: automatyka, elektronika i elektrotechnika (2019.51)
- Diagnoza potrzeb pracodawców – dyscyplina: informatyka techniczna i telekomunikacja (2019.53)

Ponadto, w ostatnim czasie przeprowadzono dodatkowe badania i analizy:

- Identyfikacja potrzeb innowacyjnych podmiotów gospodarczych (2021.60)
- Potrzeby innowacyjnych podmiotów gospodarczych względem uczelni, w tym PW (raport podsumowujący Ogólnopolskie badanie ankietowe potrzeb innowacyjnych podmiotów gospodarczych) (2022.60)

Wyniki badań, w postaci raportów i sprawozdań są przedstawiane na spotkaniach z Wydziałowym Pełnomocnikiem ds. Jakości Kształcenia oraz Radzie Wydziału.

Współpraca z otoczeniem inicjuje podejmowanie działań w zakresie dydaktyki – wprowadzaniu zmian i udoskonaleń w realizowanych programach studiów, kreowaniu oferty dydaktycznej wydziału, uwzględniającej potrzeby społeczno-gospodarcze. Ponadto współpraca ta przekłada się na nowe obszary prowadzonych badań naukowych, aplikacyjność prowadzonych prac, pogłębianie wiedzy i umiejętności mających znaczenie w gospodarce.

Celem uzupełnienia informacji o najnowsze dane, w 2025 przeprowadzono analizę pn. „Identyfikacja potrzeb otoczenia społeczno-gospodarczego w zakresie kształcenia kadr cyberbezpieczeństwa". Celem przeglądu danych zastanych (artykuły naukowe, ogólnodostępne raporty analityczne i konsultingowe) było określenie kompetencji oczekiwanych od specjalistów bezpieczeństwa IT. Opracowanie pozwoliło zgromadzić wiedzę w obszarach: 1) wiodące wyzwania w zakresie cyberbezpieczeństwa (skala globalna, europejska i krajowa); 2) braki kadrowe w sektorze cyberbezpieczeństwa; 3) kluczowe kompetencje wskazywane w ofertach pracy dla specjalistów bezpieczeństwa IT.

Kryterium 7. Warunki i sposoby podnoszenia stopnia umiędzynarodowienia procesu kształcenia na kierunku

7.1. Rola umiędzynarodowienia procesu kształcenia w koncepcji kształcenia i planach rozwoju kierunku (przy uwzględnieniu każdego z ocenianych poziomów studiów)

Wydział Elektroniki i Technik Informacyjnych prowadzi szeroką współpracę z zagranicą w ramach programów międzynarodowych, a także umów bilateralnych z ośrodkami akademickimi, w związku z realizacją badań oraz wymianą akademicką zarówno nauczycieli, jak też studentów.

Studenci kierunku **Cyberbezpieczeństwo**, zarówno studiów pierwszego stopnia, jak też studiów drugiego stopnia, mają możliwość uczestnictwa we wszystkich formach wymiany międzynarodowej dostępnej na Wydziale Elektroniki i Technik Informacyjnych i uczelni.

Niezależnie od programów międzynarodowej wymiany studentów stale rośnie liczba obcokrajowców, którzy przyjeżdżają na całe studia, co ilustruje tabela 7.1.

Tabela 7.1. Liczba obcokrajowców studiujących na kierunku Cyberbezpieczeństwo w latach akademickich 2019-2025

Lp.	Kraj	liczba obcokrajowców na studiach pierwszego stopnia	liczba obcokrajowców na studiach drugiego stopnia	liczba obcokrajowców ogółem
1	Ukraina	4	-	4
2	Białoruś	8	-	8
	Razem	12	-	12

7.2. Aspekty programu studiów i jego realizacji, które służą umiędzynarodowieniu, ze szczególnym uwzględnieniem kształcenia w językach obcych

Na studiach pierwszego stopnia prowadzonych jest 180 godzin (12 ECTS) lektoratów. Na studiach drugiego stopnia jest wymóg zrealizowania lektoratu (30 godzin). W ramach studiów literaturowych w przedmiotach jak i w pracach dyplomowych, przez związek z działalnością naukową, zwykle polecane są pozycje naukowe w języku angielskim. Studentom oferowane są zajęcia obieralne w językach obcych. Znacząca liczba studentów decyduje się pisać prace dyplomowe w języku angielskim. W ostatnich latach na kierunku **Cyberbezpieczeństwo** powstało 5 takich prac, z czego 4 na studiach pierwszego stopnia, a 1 na studiach drugiego stopnia, co ilustruje tabela 7.2.

*Tabela 7.2. Liczba prac dyplomowych napisanych w języku angielskim na kierunku **Cyberbezpieczeństwo** w latach akademickich 2022-2025*

Lp.	Rok akademicki	liczba prac dyplomowych w języku angielskim na studiach pierwszego stopnia	liczba prac dyplomowych w języku angielskim na studiach drugiego stopnia	liczba prac dyplomowych w języku angielskim ogółem
1	2024/2025	2	–	2
2	2023/2024	1	1	2
3	2022/2023	1	–	1
	Razem	**4**	**1**	**5**

Zdobywanie kompetencji w języku angielskim jest istotnym elementem kształcenia będącym odpowiedzią na potrzeby otoczenia społeczno-gospodarczego, oraz gotowość do ich pogłębiania wraz z narastającą złożonością świata.

Na poziomie uczelni dostępne są programy szkoleniowe dotyczące kompetencji językowych jak i programy wymiany akademickiej.

7.3. Stopnień przygotowania studentów do uczenia się w językach obcych i sposobów weryfikacji osiągania przez studentów wymaganych kompetencji językowych oraz ich oceny

Kandydaci na studia na kierunku **Cyberbezpieczeństwo** dysponują znajomością języka obcego, głównie angielskiego, na poziomie pozwalającym na ukierunkowanie ich rozwoju na specyfikę języka technicznego. Weryfikacja kompetencji językowych na zajęciach typu lektoraty przebiega w formie zaliczeń pisemnych, ustnych i oceny prac domowych.

Kompetencje z języka technicznego są sprawdzane m. in. przez weryfikacje zdobytej wiedzy przekazanej w materiałach i zajęciach w języku obcym, zwykle angielskim oraz ma to miejsce w ramach własnych studiów literaturowych i realizacji prac dyplomowych.

7.4. Skala i zasięg mobilności i wymiany międzynarodowej studentów i kadry

Na Wydziale Elektroniki i Technik Informacyjnych jest powołany Pełnomocnik Dziekana ds. międzynarodowej wymiany studentów, do którego może zgłosić się każdy student. Studenci korzystają z międzyuczelnianej wymiany studentów ramach programów Erasmus+, ATHENS oraz na zasadzie umów dwustronnych z uniwersytetami zagranicznymi. Wydział ma podpisanych ponad 100 umów o wymianie studenckiej z uczelniami zagranicznymi, w tym ma 3 umowy o podwójnym dyplomowaniu.

Wymiana międzynarodowa obejmuje zarówno studentów przyjeżdzających, jak też wyjeżdżających na wymianę w ramach programu Erasmus+ oraz innych programów i umów bilateralnych, a także doktorantów i nauczycieli akademickich. W tabeli 7.3 zestawiono dane dotyczące wymiany studentów za ostatni rok kalendarzowy, tj. 2023.

Tabela 7.3. Liczba studentów uczestniczących w wymianie międzynarodowej w roku kalendarzowym 2023 (w semestrze letnim 2022/2023 lub semestrze zimowym 2023/2024)

Nazwa programu/umowa	liczba osób przyjeżdżających	liczba osób wyjeżdżających
Erasmus+	(66 + 90) = 156	(25 + 44) = 69
Program Erasmus+ – krótkie programy mieszane (ang. Blended Intensive Programme)	0	(6 + 0) = 6
Praktyki/Szkolenia Erasmus+	0	(3 + 1) = 4
Szkoły letnie	0	(1 + 0) = 1
Umowa o podwójnym dyplomowaniu między PW i Kyungpook National University, Daegu, Korea	(1 + 0) = 1	(5 + 4) = 9
Swiss Mobility European Programme	0	(1 + 1) = 2
Umowa dwustronna między PW i National University of Singapore, Singapur	(1 + 0) = 1	0
Umowa dwustronna między PW i Aoyama Gakuin University, Tokio, Japonia	(1 + 0) = 1	(1 + 0) = 1
Umowa dwustronna między PW i Kyongpook National University, Daegu, Korea Południowa	(0 + 3) = 3	0
Umowa o podwójnym dyplomowaniu między PW i Beibu Gulf University, Qinzhou, Chiny	(0 + 15) = 15	0
Program ATHENS	(25 + 27) = 52	(29 + 35) = 64
Razem	229	156

Uwagi dotyczące tabeli 7.3

1. W tabeli 7.3 uwzględniono także studentów, którzy przyjechali w ramach umów o podwójnym dyplomowaniu.
2. Uwzględniono także tych studentów, którzy przyjechali (lub wyjechali) na wymianę wcześniej (np. w semestrze zimowym 2022/2023), ale ich pobyt zawierał się też w roku kalendarzowym 2023 (np. w semestrze letnim 2022/2023)

Podane informacje dotyczą całego wydziału Elektroniki i Technik Informacyjnych, natomiast jeśli chodzi o kierunek **Cyberbezpieczeństwo** to w latach akademickich 2021-2025 za granicę wyjechało 29 studentów tego kierunku (na co najmniej jeden semestr), w tym 19 na studiach pierwszego stopnia i 10 na studiach drugiego stopnia. W tabeli 7.4 przedstawiono dane za ostatnich 4 lat akademickich.

*Tabela 7.4. Liczba studentów kierunku **Cyberbezpieczeństwo** uczestniczących w wymianie międzynarodowej, którzy spędzili za granicą co najmniej semestr w latach akademickich 2021-2025*

Lp.	Rok akademicki	liczba osób wyjeżdżających na studiach pierwszego stopnia	liczba osób wyjeżdżających na studiach drugiego stopnia	liczba osób wyjeżdżających ogółem
1	2024/2025	5	3	8
2	2023/2024	8	3	11
3	2022/2023	4	4	8
4	2021/2022	2	–	2
	Razem	**19**	**10**	**29**

7.5. Udział wykładowców z zagranicy w prowadzeniu zajęć na ocenianym kierunku

Na Wydziale Elektroniki i Technik Informacyjnych jest kilku obcokrajowców od lat zatrudnionych na etatach badawczo-dydaktycznych. Jeden z nich jest Kierownikiem Zakładu Techniki Subterahercowej w Instytucie Radioelektroniki i Technik Multimedialnych.

7.6. Sposoby, częstotliwość i zakres monitorowania i oceny umiędzynarodowienia procesu kształcenia oraz doskonalenia warunków sprzyjających podnoszeniu jego stopnia, jak również wpływu rezultatów umiędzynarodowienia na program studiów i jego realizację

Monitorowanie wymiany studentów na Wydziale Elektroniki i Technik Informacyjnych należy do obowiązku Pełnomocnika Dziekana ds. międzynarodowej wymiany studentów. Corocznie sporządzane są zestawienia prezentowane na Radzie Wydziału i zamieszczane w Sprawozdaniu Dziekana.

Kryterium 8. Wsparcie studentów w uczeniu się, rozwoju społecznym, naukowym lub zawodowym i wejściu na rynek pracy oraz rozwój i doskonalenie form wsparcia

8.1. Dostosowanie systemu wsparcia do potrzeb różnych grup studentów, w tym potrzeb studentów z niepełnosprawnością

System wsparcia obejmuje różne grupy studentów. Wsparcie studentów w procesie uczenia się w PW jest wielotorowe i uwzględnia zróżnicowane potrzeby studentów. Wyróżnić można 4 podstawowe systemy wsparcia: pomoc we wchodzeniu na rynek pracy, pomoc w rozwoju naukowym, pomoc w procesie nauczania oraz pomoc materialną. Dzięki tym formom pomoc trafia zarówno do studentów szczególnie uzdolnionych i zaangażowanych, jak i osób w trudnej sytuacji życiowej, również osób niepełnosprawnych.

Studenci będący młodymi rodzicami mogą korzystać ze wsparcia w postaci urlopów, elastyczności terminów zaliczeń, zakwaterowania w domach studenckich, zasiłków losowych.

8.2. Zakres i forma wspierania studentów w procesie uczenia się

W procesie uczenia wspierane jest rozwijanie wiedzy, umiejętności i kompetencji studentów w ramach wykonywanych przez nich prac pod opieką nauczyciela akademickiego, konsultacji, możliwość studiowania według indywidualnego planu studiów a także zdobywania doświadczeń w uczestniczeniu w zlecanych wydziałowi przez przemysł.

Wsparcie w procesie uczenia jest zapewnione przez zapewnienie infrastruktury w tym informatycznej z zapewnieniem odpowiedniego przeszkolenia.

System opieki materialnej obejmuje: stypendia socjalne, zapomogi, stypendium specjalne dla osób niepełnosprawnych; wykazujących osiągnięcia sportowe, osiągnięcia naukowe. Uczelnia zapewnienie możliwości ubiegania się o miejsce w Domach Studenckich PW, dostęp do infrastruktury sportowej (sale, basen). Na terenie uczelni działają kluby ogólnouczelniane a na Wydziale są kluby studenckie np. Amplitron, Maluch.

Osobom bardziej zaangażowanym oferowany jest udział w kołach naukowych: http://www.elka.pw.edu.pl/Spolecznosc/Studenci-i-doktoranci/Organizacje-studenckie-kolanaukowe-i-kluby.

8.3. Formy wsparcia

a. krajowej i międzynarodowej mobilności studentów,

Studenci mogą korzystać z faktu, że wydział uczestniczy w programach wymiany międzynarodowej i ma zawarte umowy o współpracy w zakresie prowadzenia działalności naukowej oraz publikowania lub prezentacji jej wyników.

Dzięki praktycznemu stosowaniu od lat Europejskiego Systemu Transferu Punktów (ECTS) Wydział wypracował skuteczne procedury uznawania kompetencji zdobywanych na innych uczelniach zarówno zagranicznych, jak i krajowych.

b. prowadzenia działalności naukowej oraz publikowania lub prezentacji jej wyników, jak również w uczestniczeniu w różnych formach komunikacji naukowej lub twórczości artystycznej,

Uczelnia zapewnia studentom dostęp do źródeł literatury fachowej w postaci elektronicznej, w tym licznych baz danych, dostępnych za pomocą konta bibliotecznego jak i z zasobów własnych biblioteki (szczegółowo w Kryterium 5). Na pierwszym roku wszyscy studenci przygotowywani są do korzystania z zasobów w obowiązkowym szkoleniu.

Studenci wyższych lat i studiów II stopnia mogą rozwijać warsztat naukowy przez udział w prowadzonych na Wydziałach projektach, co uwidacznia się w współautorskich publikacjach. Wydział oferuje wsparcie dla studenckich kół naukowych. Koła mogą uzyskać finansowanie w postaci grantów. Studenci ostatnich lat studiów, na obu stopniach studiów (dyplomanci) jak i zrzeszeni w kołach naukowych mają dostęp do laboratoriów specjalistycznych. Studenci mogą korzystać z różnorodnej oferty kursów np. z Centrum Studiów Zaawansowanych, Centrum Zarządzania Innowacjami i Transferem Technologii i innych.

c. we wchodzeniu na rynek pracy lub kontynuowaniu edukacji,

Na poziomie uczelni wsparcie w wejściu na rynek pracy zapewnia Biuro Karier organizując badania, doradztwo i działania wspierające kontakt z pracodawcami jak np. „targi pracy", konsultacje i warsztaty dotyczące planowania ścieżki kariery, oraz wiele innych. Inne działania związane są także z badaniem potrzeb pracodawców w celu kształtowania adekwatnych do ich potrzeb programów.

Obowiązkowe praktyki po trzecim roku studiów I stopnia pozwalają studentom zarówno zdobywać doświadczenie, jak i nawiązywać kontakty z potencjalnymi pracodawcami. O miejscu odbywania decyduje student, jednak często z firmą lub instytucją nawiązywany jest dzięki współpracy kadry naukowej Wydziału z tymi jednostkami.

Część prac dyplomowych realizowana jest we współpracy z podmiotami zewnętrznymi dzięki kontaktom pracowników. Często realizacja praktyki lub pracy dyplomowej owocuje zatrudnieniem (byłego) studenta w podmiocie.

Elementem wspierającym zdobywanie doświadczenia praktycznego jest układ planu dostosowany do potrzeb studentów, jak również koncentracja zajęć regularnych w początku VII semestru, co pozwala na aplikacje na II stopień studiów.

d. aktywności studentów: sportowej, artystycznej, organizacyjnej, w zakresie przedsiębiorczości,

Uczelnia organizuje wydarzenia sportowe np. biegi. Uczelnia funduje stypendium rektora za wysokie osiągnięcia w sporcie. Oprócz licznych sekcji sportowych przy AZS PW, na uczelni działa Chór Politechniki Warszawskiej i Zespół Tańca pozwalający na realizację potrzeb ekspresji artystycznej, organizowane są wydarzenia artystyczne jak wystawy, pokazy, instalacje i inne.

Samorząd Studentów czynnie uczestniczy w życiu Wydziału nie tylko w zakresie wydarzeń kulturalnych, ale również w działalności organizacyjnej i legislacyjnej.

W odniesieniu do przedsiębiorczości organizowane są liczne akcje (opis kryterium 6) np. „Światowy tydzień przedsiębiorczości". Oferowane są zajęcia z grupy przedmiotów humanistyczno-ekonomicznospołecznych i innych przedmiotów, do których przypisane są efekty uczenia odnoszące się do przedsiębiorczości. Działania organizacyjne koordynuje też Wydziałowa Rada Samorządu Studenckiego. Innymi elementami są działania na rzecz społeczności akademickiej jak budżet partycypacyjny, akcje charytatywne, krwiodawstwa, szlachetna paczka itp.

8.4. System motywowania studentów do osiągania lepszych wyników w nauce oraz działalności naukowej oraz sposobów wsparcia studentów wybitnych

Głównym narzędziem motywującym studentów do osiągania lepszych wyników w nauce jest system stypendiów i nagród. Studenci mogą uzyskać stypendium za wysokie wyniki w nauce z Własnego Funduszu Stypendialnego PW oraz nagrody i wyróżnienia. Do systemu motywacyjnego należy zaliczyć również działalność studenckich kół naukowych oraz szeroką ofertę wyjazdów zagranicznych. Ponadto uzyskane wyniki definiują priorytety przy zapisie na przedmioty obieralne.

8.5. Sposoby informowania studentów o systemie wsparcia, w tym pomocy materialnej

Opis systemu stypendialnego, wraz ze wszystkimi aktami prawnymi i wymaganymi formularzami dostępny jest ze strony wydziałowej i znajduje się pod adresem
https://www.bss.ca.pw.edu.pl/Stypendia.
Natomiast pod adresem https://www.ca.pw.edu.pl/Biuro-ds.-Spolecznej-Odpowiedzialnosci-Uczelni. znajdują się informacje przydatne dla osób niepełnosprawnych. Szczegółowe informacje studenci mogą uzyskać w dziekanacie, w sekretariacie Prodziekana ds. studenckich. W kontekście wsparcia studentów PW, warto również wspomnieć o cyklicznych sondażach studenckich PW #powiedzPW .

8.6. Sposoby rozstrzygania skarg i rozpatrywania wniosków zgłaszanych przez studentów oraz jego skuteczności

Student może przekazać swoje uwagi, wnioski oraz skargi Dziekanowi oraz złożyć odwołanie lub skargę do JM Rektora. Wszystkie działania są realizowane zgodnie z Regulaminem Studiów PW. Uzasadnione wnioski i skargi są realizowane bezzwłocznie. Studenci mogą również zgłaszać uwagi przez Wydziałową Radę Samorządu, której przedstawiciele uczestniczą w zebraniach Komisji ds. Kształcenia oraz posiedzeniach Rady Wydziału i mogą zabierać głos w dyskusji dotyczącej sposobu realizacji procesu dydaktycznego. W uczelni działają również Komisje Dyscyplinarne (ds. Studentów i Doktorantów oraz ds. Nauczycieli), do których studenci mogą się zwrócić w przypadkach skrajnych.

W zależności od charakteru zgłaszanego problemu studenci mogą korzystać ze wsparcia rzecznika zaufania (informacja na stronie wydziałowej), rzecznika zaufania studentów (informacja na stronie PW BSS). Student zgłaszający problem lub przedstawiciel studentów z WRSS kontaktuje się z wybraną osobą i ustala tok postępowania zgodnie z obowiązującymi przepisami.

8.7. Zakres, poziom i skuteczność systemu obsługi administracyjnej studentów, w tym kwalifikacji kadry wspierającej proces kształcenia

Obsługa administracyjna studentów realizowana jest przez dziekanat, pracowników wsparcia informatycznego Wydziałów i Centrum Informatyzacji, pracowników bibliotek, pracowników administracji Centralnej np. Biura Spraw Studenckich, sekretariaty instytutów. Narzędzia informatyczne do obsługi toku studiów są integrowane z system USOS. Jest on rozwijany i stał się, w październiku 2020, elementem platformy ePW (Elektroniczna Politechnika Warszawska).

Obsługa administracyjna studentów jest realizowana w dziekanacie WEiTI oraz Sekretariatach dydaktycznych Instytutów. Studentów obcokrajowców obsługują pracownicy ze znajomością języków obcych. Pracownicy doskonalą swój warsztat, m.in. uczestniczą regularnie w kursach doskonalenia lub nauki języka angielskiego finansowanych przez Dziekana. Sprawy studenckie są rozpatrywane bezpośrednio w dziekanacie, przez kontakt drogą internetową lub telefonicznie. Zakres obsługi studentów w dziekanacie obejmuje m.in. prowadzenie teczki personalnej studenta, przygotowanie i wydawanie zaświadczeń o statusie studenta, przyjmowanie wniosków o Elektroniczne Legitymacje Studenckie oraz ich duplikaty, wniosków o pomoc materialną, stypendia i zapomogi, wydawaniem suplementów do dyplomów oraz dyplomów ukończenia studiów, wydawaniem odpisów oraz wyciągów ocen.

Działanie systemu obsługi administracyjnej studentów jest oceniane przez Dziekana Wydziału oraz przez bezpośrednich przełożonych w systemie oceny okresowej pracowników administracyjnych Politechniki funkcjonującym na Uczelni. W Systemie Oceny Pracowników (SOP) dla poszczególnych grup zawodowych określane są wymagane kompetencje i kryteria oceny. W pierwszej fazie pracownik dokonuje samooceny, jak również ocenia go przełożony. Następnym etapem jest rozmowa dwóch stron, w której wskazane zostają silne i słabe strony pracownika. Natomiast skuteczność systemu obsługi jest analizowana na podstawie informacji przekazywanych przez studentów bezpośrednio do Dziekana lub Prodziekanów.

8.8. Działania informacyjne i edukacyjne dotyczące bezpieczeństwa studentów, przeciwdziałania dyskryminacji i przemocy, zasad reagowania w przypadku zagrożenia lub naruszenia bezpieczeństwa, dyskryminacji i przemocy wobec studentów, jak również pomocy jej ofiarom

Studenci przechodzą obowiązkowe szkolenia BHP organizowane przez Dział ds. Szkoleń https://www.szkolenia.pw.edu.pl/Szkolenia-BHP, a na zajęciach wymagających szczególnego bezpieczeństwa udzielany jest instruktaż stanowiskowy. Studenci mają dostęp do opieki medycznej w placówkach medycznych współdziałających z PW. Informacje o opiece medycznej są dostępne na

stronie https://www.centermed.pl/pw/student. Studenci mogą zgłaszać wszelkie przypadki dyskryminacji, przemocy czy innych zagrożeń do Prodziekana ds. Studenckich, Dziekana oraz Prorektora ds. Studenckich. Na uczelni funkcjonuje Komisja Dyscyplinarna ds. Studentów i Doktorantów oraz Komisja Odwoławcza. W Biurze Spraw Studenckich PW działa również Sekcja ds. Osób Niepełnosprawnych oraz dostępna jest pomoc psychologiczna https://www.ca.pw.edu.pl/Biuro-ds.-Spolecznej-Odpowiedzialnosci-Uczelni. Na szczeblu uczelni i wydziału funkcjonuje studencki rzecznik zaufania, który może podejmować działania w sprawach zgłaszanych przez studentów. Uczelnianą politykę przeciwdziałania mobbingowi i dyskryminacji, a w szczególności rolę wydziałowych rzeczników zaufania oraz studenckiego rzecznika zaufania, określa Zarządzenie Rektora nr 59/2014 wraz ze zmianami wprowadzonymi przez Zarządzenie Rektora nr 22/2018.

8.9. Współpraca z samorządem studentów i organizacjami studenckimi

Samorząd studencki działa opiniując działania podejmowane na Radzie Wydziału i uczestnicząc w pracach Komisji Wydziałowych. Opiniuje programy w zakresie kształcenia, wsparcia, rozwoju, kadr i wielu innych. Organizuje i współuczestniczy w różnych aktywnościach Wydziałów takich jak imprezy, (Juwenalia, święto Politechniki), spotkania (z pracodawcami, studentów, naukowe), czy działania promocyjne (dni otwarte, szkolenia).

Wydziałowa Rada Samorządu Studenckiego organizuje liczne działania społecznie, akcje np. krwiodawstwa, wsparcia szkoleniowego, wsparcia studentów w organizacji zajęć uzupełniających (tzw. pościgów), wyjazdy integracyjne, imprezy jak np. juwenalia, wspiera akcje np.: „Drzwi Otwartych PW", "Dziewczyny na Politechniki" dla kandydatów na studia, charytatywne i wiele innych. WRSS ma co roku przyznawane finansowanie w ramach własnego budżetu na potrzeby działań na Wydziale.

Na WEiTI działa Samorząd Studencki oraz kilka klubów i organizacji studenckich http://www.elka.pw.edu.pl/pol/Spolecznosc/Studenci-i-doktoranci/Organizacje-studenckie-kolanaukowe-i-kluby. Studenci z WRS i Wydziałowego Klubu Studenckiego Amplitron aktywnie angażują się w pomoc przy organizacji wszystkich ogólnowydziałowych imprez i wydarzeń, np. obchodów Dnia Wydziału, Drzwi Otwartych PW, Elkonaliów, Juwenaliów. Z ramienia WRS została wyznaczona osoba, której zadaniem jest wspieranie przepływu informacji między kołami naukowymi, WRS i Wydziałem. Przedstawiciele WRS uczestniczą aktywnie w spotkaniach Komisji ds. Kształcenia i mają znaczący wpływ na sprawy programowe. Przedstawiciele WRS i kół naukowych uczestniczą w każdym miesiącu w Radach Wydziału.

8.10. Sposoby, częstości i zakresu monitorowania, oceny i doskonalenia systemu wsparcia oraz motywowania studentów, jak również oceny kadry wspierającej proces kształcenia, a także udziału w ocenie różnych grup interesariuszy, w tym studentów

System jest monitorowany wielotorowo. Jednym z elementów oceny jest doroczny raport Wydziału dotyczący wszystkich aspektów działalności, omawiany na Radzie Wydziału i dostępny w Raporcie Rektora dla Uczelni. Na poziomie jakości kształcenia raportowanie odbywa się w Ankiecie Samooceny dla Uczelnianej Rady ds. Jakości Kształcenia sprawozdawanej na Radzie Wydziału i przedstawianej w odniesieniu do Wszystkich Wydziałów na Uczelnianej Radzie ds. Jakości Kształcenia.

Dodatkowe informacje, które uczelnia uznaje za ważne dla oceny kryterium 8

W kontekście wsparcia studentów PW, warto również wspomnieć o cyklicznych sondażach studenckich PW #powiedzPW. Ich celem jest zwiększenie bezpośredniego uczestnictwa studentów w procesie podejmowania decyzji dotyczących środowiska akademickiego. Gromadzenie opinii studentów w kwestiach edukacyjnych, organizacyjnych i kulturalnych pozwoli na dostosowanie działań Uczelni do ich oczekiwań oraz zwiększenie ich satysfakcji ze studiowania na Politechnice Warszawskiej. Sondaż jest

prostym, szybkim i skutecznym narzędziem do komunikacji władz Uczelni, jednostek PW oraz organizacji studenckich ze społecznością studencką PW. Zleceniodawcami badania są władze Politechniki Warszawskiej. Władze Politechniki Warszawskiej w określeniu tematyki poszczególnych edycji sondażu mogą, dzięki opracowanej technice zbierania zapotrzebowania w tym zakresie, uwzględniać potrzeby władz poszczególnych Wydziałów PW oraz innych jednostek PW. Zgłoszenie tematyki konsultacji będzie możliwe poprzez wypełnienie formularza przez przedstawicieli jednostki PW na stronie internetowej. Inicjatywa organizowana jest od 2017 r. i do tej pory miała już 14 edycji, tj.:

- Sondaż studencki #powiedzPW Temat: Sklep PW (badanie pilotażowe),
- Sondaż studencki #powiedzPW Temat: Wydarzenia w PW,
- Sondaż studencki #powiedzPW Temat: Przedsiębiorczość. Czym jest dla studentów?
- Sondaż studencki #powiedzPW Temat: Organizacje studenckie,
- Sondaż studencki #powiedzPW Temat: Domy studenckie 2019,
- Sondaż studencki #powiedzPW Temat: Strona internetowa PW,
- Sondaż studencki #powiedzPW Temat: Społeczna Odpowiedzialność Uczelni,
- Sondaż studencki #powiedzPW Temat: Inkubator Innowacyjności,
- Sondaż studencki #powiedzPW Temat: Działalność Samorządu Studentów PW,
- Sondaż studencki #powiedzPW Temat: Nowe role społeczne kampusów w czasach pandemii,
- Sondaż studencki #powiedzPW Temat: Domy studenckie 2022,
- Sondaż studencki #powiedzPW Temat: Pomoc psychologiczna dla osób studiujących i doktoryzujących się na PW,
- Sondaż studencki #powiedzPW Temat: Zajęcia sportowe na PW,
- Sondaż studencki #powiedzPW Temat: Pomoc materialna dla osób studiujących na PW.

Wyniki sondaży udostępniono w Intranecie PW:
https://intranet.pw.edu.pl/strateg/SitePages/Sonda%C5%BC--powiedzPW.aspx?web=1 /
oraz ogólnodostępne pod adresem: https://das.pw.edu.pl/Raporty/powiedzPW/Raporty-i-infografiki-powiedzPW

Kryterium 9. Publiczny dostęp do informacji o programie studiów, warunkach jego realizacji i osiąganych rezultatach

9.1. Zakres, sposób zapewnienia aktualności i zgodności z potrzebami różnych grup odbiorców, w tym przyszłych i obecnych studentów, udostępnianej publicznie informacji o warunkach przyjęć na studia, programie studiów, jego realizacji i osiąganych wynikach

Publiczny dostęp do informacji dla Studentów, Kandydatów, Pracodawców i innych interesariuszy realizowany jest przez:

- strony Uczelni,
- strony Wydziałów,
- strony jednostek specjalizowanych jak Centrum Zarządzania Innowacjami i Transferem Technologii,
- USOS,
- pocztę elektroniczną,
- platformę Elektronicznej Politechniki Warszawskiej EPW integrującej:
    a. Uczelniany System Obsługi Studiów USOS, o pocztę Politechniki Warszawskiej, o platformy pracy zdalnej LeON;

b. katalog karty przedmiotów ePW Asystent (proces migracji w toku,
c. system biblioteczny,
d. bazy wiedzy i osiągnieciach naukowych – Repozytorium PW,

- inne media - w tym społecznościowe wspierające identyfikację z Politechniką Warszawską.

Wszelkie informacje udostępnione są dla kandydatów, studentów, pracowników oraz innych zainteresowanych odbiorców przez stronę internetową WEiTI http://www.elka.pw.edu.pl/ oraz stronę PW https://pw.edu.pl/. Strony zawierają obszerne informacje o oferowanych kierunkach studiów, opis programów studiów, szczegółowe plany studiów, rekrutacji i spraw studenckich. Poza serwisem publicznym dla studentów dostępne są dodatkowe informacje na platformie edukacyjnej oraz w USOSweb PW usosweb.usos.pw.edu.pl. W serwisie wewnętrznym studenci mogą sprawdzić swoje plany, osiągnięcia, zapisać się na przedmioty, złożyć wnioski (podania) elektroniczne. Informacje dotyczące szczegółowych treści kształcenia na wszystkich kierunkach są także dostępne w katalogach umieszczonych na stronach internetowych Uczelni https://ects.coi.pw.edu.pl/menu2/programy. W obecnej chwili trwa migracja do nowego systemu – ePW Asystent (https://asystent.usos.pw.edu.pl).

Na stronie https://www.bip.pw.edu.pl/ można znaleźć wszystkie informacje o charakterze publicznym, w tym uchwały Senatu, zarządzenia i decyzje Rektora i inne akty prawne. Z kolei w bazie wiedzy PW http://repo.bg.pw.edu.pl/index.php/pl/ można znaleźć informacje dotyczące aktywności badawczej, w tym informacje o publikacjach wszystkich pracowników PW.

Strony jednostek wspierających jak np. CPR, CINN, DAS zawierają m.in. informacje o prowadzonych działaniach wspierających i ich wynikach np. badań potrzeb rynku, szkoleń, zdobywania środków na rozwój kształcenia itp.

9.2. Sposoby, częstotliwość i zakres oceny publicznego dostępu do informacji, udziału w ocenie różnych grup interesariuszy, w tym studentów, a także skuteczności działań doskonalących w tym zakresie

Za politykę informacyjną na poziomie uczelni odpowiedzialne jest Biuro Promocji i Informacji, które monitoruje skuteczność polityki informacyjnej, w tym np. prowadzi statystyki odsłon stron internetowych we wszystkich zakładkach, kierowanych do różnych grup odbiorców, w tym do studentów i pracowników. Jest również odpowiedzialne za aktualizację informacji i śledzenie mediów społecznościowych. Biuro przygotowuje także raporty samooceny oraz informacje na temat pozycji PW i jej jednostek w różnych rankingach, obejmujących także kształcenie. Raport przygotowywany jest comiesięcznie i rozsyłany do Dziekanów Wydziałów.

Element oceny kanałów komunikacji jest prowadzony przez prodziekanów, opiekunów kierunku i pełnomocników ds. jakości kształcenia a bieżący nadzór prowadzi dziekanat. Strony są aktualnie w trakcie reorganizacji i dostosowania do zmian centralnych PW. W ciągu roku powinna nastąpić migracja treści. Regularnie opiniują je WRSS.

Kryterium 10. Polityka jakości, projektowanie, zatwierdzanie, monitorowanie, przegląd i doskonalenie programu studiów

10.1. Sposoby sprawowania nadzoru merytorycznego, organizacyjnego i administracyjnego nad kierunkiem studiów, kompetencji i zakresu odpowiedzialności osób odpowiedzialnych za kierunek, w tym kompetencje i zakres odpowiedzialności w zakresie ewaluacji i doskonalenia jakości kształcenia na kierunku

W Księdze Jakości Kształcenia Wydziału opisana jest misja i strategia w zakresie kształcenia. Przedstawione tam zapisy są spójne w swoich podstawowych założeniach. Odpowiedzialność za

realizacje procesów określają kompetencje dziekana, prodziekanów, dyrekcji Instytutów, Kierowników Zakładów, Pełnomocników Dziekana, Komisji Rady Wydziału i Opiekunów specjalności, kierunku, praktyk.

Za monitorowanie programów i procesów kształcenia w Uczelni oraz wprowadzanie nowych form i technik kształcenia oraz sposobów organizacji studiów itp. odpowiedzialny jest Prorektor ds. Studiów; za monitorowanie skuteczności i ciągłe doskonalenie USZJK PW Pełnomocnik ds. Jakości Kształcenia i Akredytacji. Na szczeblu Wydziałów Elektroniki i Technik Informacyjnych nadzór należy odpowiednio do Prodziekana ds. Nauczania i Prodziekana ds. studiów oraz pełnomocników: Dziekana Wydziału Elektroniki i Technik Informacyjnych ds. Wydziałowego Systemów Zapewniania Jakości Kształcenia.

(Księga Jakości Kształcenia na Wydziale podlega w chwilo obecnej procesowi korekty ze względu na sugestie wskazane przez Komisję PKA wizytującą kierunek Elektronika (pozytywna opinia o kierunku została wydana w styczniu tego roku)).

10.2. Zasady projektowania, dokonywania zmian i zatwierdzania programu studiów

PW prowadzi studia na określonym kierunku przyporządkowanym do dyscyplin naukowych, poziomie i profilu na podstawie programów studiów, które określają efekty uczenia się (z uwzględnieniem charakterystyk pierwszego stopnia i drugiego stopnia PRK), opis procesu prowadzącego do uzyskania efektów uczenia się i liczbę punktów ECTS przypisanych do zajęć. Ustalanie programów studiów w formie uchwały, w tym wprowadzanie zmian do istniejących programów studiów jest kompetencją Senatu. Przygotowując dokumentację programu studiów i charakterystyki studiów należy kierować się ustaleniami: uchwały Senatu PW nr 58/L/2020 w sprawie ustalania programów studiów w Politechnice Warszawskiej oraz zarządzeniem Rektora PW nr 158/2020 w sprawie procedury tworzenia studiów, zaprzestania prowadzenia studiów oraz procedury wprowadzania zmian w programie studiów.

Nowe programy studiów i zmiany w programie są opiniowane przez Radę Wydziału, a wniosek o zmiany składa Dziekan Wydziału za pośrednictwem Działu ds. Studiów. Programy są opiniowane przez WRS. Kierowany na Senat wniosek jest opiniowany przez Senacką Komisją ds. Kształcenia pod kątem formalnym, a także m.in. pod względem wpływu uruchamianego kierunku studiów na inne kierunki prowadzone w Uczelni (unikalność uruchamianego kierunku), zgodności proponowanego kierunku studiów z wyznaczonymi kierunkami działalności Uczelni w zakresie kształcenia, rentowości uruchamianego przedsięwzięcia.

10.3. Sposoby i zakres bieżącego monitorowania oraz okresowego przeglądu programu studiów na ocenianym kierunku oraz źródeł informacji wykorzystywanych w tych procesach

Ocena programów studiów prowadzona jest systematycznie na wielu poziomach:

a. przedmiotów przez opiekunów przedmiotów,
b. spójności treści zawartych w różnych przedmiotach przez opiekunów specjalności i kierunku
c. zakładów prowadzących specjalności,
d. kierunków na poziomie Rady Wydziału.

Wnioski oceny podejmowane są na podstawie wyników analizy procesu kształcenia np. analizy ocen w tym prac etapowych i końcowych, informacji płynących z otoczenia społeczno-gospodarczego w tym systematycznych badań rynku pracy, karier absolwentów (Kryterium 6), potrzeb kandydatów, opinii studentów (Kryterium 8), opinii nauczycieli akademickich. Dane do analiz pochodzą z procesu kształcenia, realizowanych przez jednostki wspierające dedykowanych badań, analiz danych z GUS, ZUS, z portalu ela.nauka.gov.pl. Analizy inicjują zmiany w programach i efektach.

Program kształcenia monitorowany jest na bieżąco przez Komisję ds. Kształcenia oraz kierowników kierunku. Komisja ds. Kształcenia kontroluje także, czy ewentualne zmiany na innych prowadzonych kierunkach nie

stwarzają konieczności lub możliwości zmian w programie danych studiów, np. propozycja nowego przedmiotu w jednym z prowadzonych kierunków może być interesująca także dla innego.

10.4. Sposób oceny osiągnięcia efektów uczenia się przez studentów ocenianego kierunku, z uwzględnieniem poszczególnych etapów kształcenia, jego zakończenia oraz przydatności efektów uczenia się na rynku pracy lub w dalszej edukacji, jak też wykorzystania wyników tej oceny w doskonaleniu programu studiów

Osiąganie efektów oceniane jest podczas realizacji przedmiotów i prac etapowych przez oceny formujące i końcowe. Na najniższym etapie prowadzi ją kierownik przedmiotu. Jest to kontrola wybranych prac, jak i rozkładu ocen. Ocena taka wykonywana jest także dla wybranych przedmiotów (najczęściej z inicjatywy studentów) przez Prodziekana ds. Nauczania. W przypadku rażących odchyleń podejmowane są dalsze działania, w tym bardziej szczegółowy przegląd treści przedmiotu, sposobów potwierdzania efektów uczenia się itp. Ocena osiągnięcia efektów uczenia się po etapach rejestracji prowadzona jest przez Prodziekana ds. Nauczania.

Przydatność efektów na rynku pracy jest opiniowana a także weryfikowana przez ankiety, badania i monitoring karier. Jej miarą jest pozycja na rynku pracy absolwentów w tym mierzona przez m.in. osiągane zarobki, czas do zatrudnienia, udział zatrudnionych w pierwszym roku (szczegółowy opis w Kryterium 2).

W wyniku analizy przeprowadzonego procesu ankietyzacji ciągłej weryfikacji poddawany jest m.in. program studiów. W efekcie konsultacji ze studentami wprowadzono modyfikacje w przedmiotach matematycznych (Matematyka 1-4), co pozytywnie wpłynęło na możliwość prawidłowego przyswojenia materiału dydaktycznego przez studentów [Uchwała na 28/L/2020 Senatu Politechniki Warszawskiej z dnia 23 września 2020 r. (załącznik ***BIP.Uch.Zmiany1***) oraz Zmiana programu studiów pierwszego stopnia o profilu ogólnoakademickim na kierunku **Cyberbezpieczeństwo** prowadzonych na Wydziale Elektroniki i Technik Informacyjnych załącznik ***BIP.Zmiany1***]. Proces doskonalenia programu studiów jest kontynuowany, w szczególności w związku z możliwością uzyskania informacji zwrotnej od przez pierwszych absolwentów pełnego cyklu studiów - na pierwszym i drugim stopniu.

10.5. Zakres, forma udziału i wpływu interesariuszy wewnętrznych, w tym studentów, i interesariuszy zewnętrznych na doskonalenie i realizację programu studiów

Wpływ interesariuszy obejmuje wewnętrzne oceny realizowane przez nauczycieli i pozostałych pracowników. Wydział traktuje udział studentów w kształtowaniu życia społeczności jako podstawowe ich prawo prowadząc konsultuje: programów (Udział w Komisjach RW), przebieg kształcenia (dyskusja na Radzie Wydziału, ankietyzacja zajęć), system zapewnienia jakości (opiniowanie dokumentów), systemu obsługi studiów (ankieta oceny pracy dziekanatu (załączniki: ***Dziekanat.AnkPyt, Dziekanat.Ank.9.11***, ***Dziekanat.AnkWyniki***), opiniowanie planów zajęć), form współpracy z otoczeniem. Konsultacje prowadzone są z interesariuszami zewnętrznymi m.in. z rynku pracy, preferencji kandydatów (szkoły średnie współpracujące, Strona Wydziału), wniosków od absolwentów (konsultacje, strona Wydziału).

Interesariuszami wewnętrznymi są studenci kierunku i pracownicy uczelni. Wpływ studentów na doskonalenie i realizację programu studiów realizowany jest przede wszystkim za pośrednictwem WRS. Samorząd każdego Wydziału posiada własne pomieszczenie i jest w ciągłym kontakcie z Prodziekanem ds. Nauczania/ds. StudenckichPraktyki. Przedstawiciele studentów są także stałymi członkami komisji dziekańskich i Rady Wydziału. WRS opiniuje decyzje w sprawach dotyczących programów studiów. Druga grupa 7 interesariuszy wewnętrznych to pracownicy Uczelni. Każdy z pracowników ma możliwość zaproponowania (poprzez Komisję ds. Kształcenia) dowolnych zmian w programie studiów jak też poprowadzenia nowego przedmiotu obieralnego.

Interesariusze zewnętrzni to przede wszystkim pracodawcy, zatrudniający absolwentów i praktykantów lub współpracujący z Wydziałem na zasadzie umów lub listów intencyjnych. Ich wpływ na doskonalenie i realizację programu studiów odbywa się przede wszystkim przez przekazywanie uwag dotyczących wymaganych kompetencji absolwentów.

10.6. Sposoby wykorzystania wyników zewnętrznych ocen jakości kształcenia i sformułowanych zaleceń w doskonaleniu programu kształcenia na ocenianym kierunku

Wyniki ocen poddawane są dyskusjom i w uzasadnionych przypadkach skutkują zmianami w programach, treściach, procedurach, organizacji studiów. Programy zostały zmodyfikowane w 2020 dla I stopnia i 2024 dla II stopnia studiów.

Część II. Perspektywy rozwoju kierunku studiów

Analiza SWOT programu studiów na ocenianym kierunku i jego realizacji, z uwzględnieniem szczegółowych kryteriów oceny programowej

	POZYTYWNE	NEGATYWNE
Czynniki wewnętrzne	**Mocne strony** 1. Uczelnia badawcza, konsorcjum ENHANCE, otoczenie gospodarczo społeczne – wysoki poziom kształcenia, wymiana doświadczeń i dobrych praktyk. 2. Środowisko Wydziału - obszary wspólne z telekomunikacją, informatyką, automatyką i robotyką oraz elektroniką. 3. Przenikanie kompetencji z różnych dziedzin pozwala na rozwój nowych specjalności, a nawet "zarodkowanie" nowych kierunków (np. Internet rzeczy) 4. Przechodzenie do kształcenia problemowego opartego na PBL (Problem Based Learning), projektów zespołowych zwiększających umiejętność pracy zespołowej, kompetencji społecznych. 5. Centrum Cyberbezpieczeństwa PW, kierowane przez opiekuna studenckiego Koła Naukowego Cyberbezpieczeństwa wykorzystywane jako naturalny „poligon doświadczalny" dla działalności dydaktycznej	**Słabe strony** 1. Dynamiczny rozwój i popularność kierunku, wymaga dużych zasobów, które są skończone. 2. Ograniczone możliwości zwiększenia bazy lokalowej. 3. Duża liczba studentów utrudnia indywidualne podejście do studenta. 4. Duża dysproporcja w zarobkach kadry dydaktycznej i specjalistów na rynku utrudnia rozbudowę oraz odnowę kadry dydaktycznej. 5. Dziura pokoleniowa w strukturach zatrudnienia kadry dydaktycznej. Niedobory kadry dydaktycznej, a co za tym idzie duże obciążenia godzinowe.
Czynniki zewnętrzne	**Szanse** 1. Udział Uczelni w konsorcjum ENHANCE - prestiż Uczelni, mobilność pracowników i studentów, większe doświadczenie i kompetencje. 2. Coraz większy priorytet aspektów bezpieczeństwa w administracji państwowej, ale także małych i średnich przedsiębiorstwach. 3. Bardzo duży i wciąż rosnący popyt na specjalistów z obszaru cyberbezpieczeństwa. 4. Wysoko ceniony program kierunku, dający praktyczne kompetencje absolwentom, łączący kompetencje techniczne oraz społeczne. 5. Wysoka ocena kompetencji absolwentów Wydziału przez pracodawców; oferty współpracy, także w procesie kształcenia	**Zagrożenia** 1. Dysproporcja zarobków i atrakcyjność pracy na zewnątrz, drenuje kadrę dydaktyczną i znacząco utrudnia (uniemożliwia) szansę na wymianę pokoleniową. 2. Efektywna rekrutacja naszych studentów do pracy i wysokie zarobki powodują spadek motywacji do nauki dla studentów ostatnich semestrów, przejawia się to w wydłużaniu studiów, jak również w spadku zainteresowania kontynuacją kształcenia na studiach II stopnia i w szkole doktorskiej. 3. Zainteresowanie samorozwojem i zwiększaniem kompetencji skutkuje rozpoczynaniem w trakcie studiów innych kierunków (np. ekonomii, zarządzania, psychologii, politologii). 4. Narzędzia oparte na sztucznej inteligencji wymuszają analizę procesów kształcenia, w tym podejścia do nauczania oraz weryfikacji efektów uczenia się.

(Pieczęć uczelni)

…… ……

(podpis Dziekana/Kierownika jednostki) (podpis Rektora)

Warszawa, dnia **27 lutego 2025**

(miejscowość)