Dane do wniosku o uruchomienie studiów podyplomowych:

"**Ochrona informacji w sieciach i systemach teleinformatycznych: projektowanie i audyt zabezpieczeń**"

1). Określa się następujące obszary kształcenia związane ze studiami podyplomowymi *Ochrona informacji w sieciach i systemach teleinformatycznych: projektowanie i audyt zabezpieczeń:*

Obszar nauk technicznych

2). Ustala się następujące efekty kształcenia: *Ochrona informacji w sieciach i systemach teleinformatycznych: projektowanie i audyt zabezpieczeń*

Tabela nr 1. Efekty kształcenia programu Studiów Podyplomowych
"Ochrona informacji w sieciach i systemach teleinformatycznych: projektowanie i audyt zabezpieczeń"

L.p.	Obszar nauki	Symbol	Nr	Efekt kształcenia
1	Obszar nauk technicznych: **wiedza**	T2A_W01	W1	Zna podstawy matematyczne kryptologii i ochrony informacji
		T2A_W03	W2	Ma podstawową wiedzę o sieciach teleinformatycznych niezbędną w technikach ich ochrony
		T2A_W03	W3	Zna podstawowe techniki wykorzystywane w kryptologii i ochronie informacji
		T2A_W04	W4	Zna zagrożenia występujące w sieci i ataki na infrastrukturę i usługi sieciowe
		T2A_W07	W5	Zna oprogramowanie używane w ochronie informacji i ochronie sieci teleinformatycznych
		T2A_W03	W6	Zna podstawowe akty prawne i normy dotyczące bezpieczeństwa informacji
		T2A_W03	W7	Zna podstawy zarządzania bezpieczeństwem informacji
2	Obszar nauk technicznych: **umiejętności**	T2A_U01	U1	Umie odczytać dokumentacje techniczną dotyczącą przedmiotu i akty prawne z nią związane
		T2A_U08	U2	Potrafi zaprojektować rozwiązanie techniczne dotyczące zabezpieczeń sieci komputerowych
		T2A_U04	U3	Umie sporządzić dokumentację techniczna zaprojektowanego rozwiązania
		T2A_U15	U4	Umie ocenić przydatność rozwiązania technicznego służącego bezpieczeństwu sieci
		T2A_U09	U5	Potrafi wykorzystać oprogramowanie do analizy bezpieczeństwa i ochrony informacji i usług sieciowych
		T2A_U16	U6	Umie skonfigurować podstawowe usługi bezpieczeństwa sieci stosowane w praktyce
3	Obszar nauk technicznych:	T2A_K01	K1	Rozumie potrzebę uczenia się przez całe życie; potrafi inspirować i organizować proces uczenia się innych osób

	kompetencje społeczne	T2A_K02	K2	Ma świadomość ważności i rozumie pozatechniczne aspekty i skutki działalności inżynierskiej, w tym jej wpływ na środowisko, i związaną z tym odpowiedzialność za podejmowane decyzje
		T2A_K03	K3	Potrafi współdziałać i pracować w grupie, przyjmując w niej różne role
		T2A_04	K4	Potrafi odpowiednio określić priorytety służące realizacji określonego przez siebie lub innych zadania prawidłowo identyfikuje i rozstrzyga dylematy związane z wykonywaniem zawodu

3). Ustala się opis przedmiotów obejmujący:

Efekty kształcenia i ich odniesienie do efektów kształcenia dla programu

Tabela nr 2. Program Studiów Podyplomowych
"Ochrona informacji w sieciach i systemach teleinformatycznych: projektowanie i audyt zabezpieczeń"

L. p.	Przedmiot	L. godzin zajęć dydaktycznych		Pkt. ECTS	Efekt kształcenia (kod, opis)	Odniesienie do efektów kształcenia
		Teoret.	Prakt.			
1	**KRYPTOGRAFIA, PROTOKOŁY KRYPTOGRAFICZ-NE (KPK)**	30	12	12	Zna podstawy matematyczne kryptografii i umie wykonywać niezbędne obliczenia w algorytmach i protokołach	W1
					Zna podstawowe algorytmy i protokoły kryptograficzne i umie wybrać właściwy ich zestaw do własnych zastosowań	W1
					Umie odczytać dokumentacje techniczną, zaprojektować, skonfigurować i praktycznie wykorzystać podstawowe protokoły kryptograficzne	U1 K1
					Umie wykorzystać protokoły biblioteczne do zabezpieczenia poczty elektronicznej i wymiany danych w sieciach lokalnych i w Internecie	U1 U4
					Zna podstawy wykorzystania kryptograficznych kart elektronicznych w systemach zabezpieczeń, potrafi zaprojektować protokół wykorzystujący karty	W2 W3
					Umie sporządzić podstawową dokumentację dotyczącą kryptograficznych systemów zabezpieczeń	U3
2	**BEZPIECZEŃSTWO SIECI (BS)**	40	20	16	Zna podstawowe rodzaje ataków na sieci oraz metody steganograficzne oraz umie opisać ich wpływ na aspekty społeczne, ekonomiczne oraz prawne funkcjonowania sieci komputerowych	W2 W4
					Umie zaprojektować, adekwatne do zidentyfikowanych zagrożeń, zabezpieczenia w oparciu o systemy firewall, VPN, AAA oraz IDS/IPS	W4 U2 U6 K3
					Zna sposoby konfiguracji urządzeń sieciowych oraz umie wskazać podatności i zidentyfikować sposoby utwardzania tych urządzeń	W4 W2 U6
					Zna podstawowe usługi bezpieczeństwa i umie wskazać narzędzia oraz protokoły do ich realizacji w sieciach telekomunikacyjnych	W1 W5 U4

						U6
					Umie rozwiązać postawiony problem dotyczący bezpieczeństwa sieci oraz zrealizować prosty program służący monitorowaniu zdarzeń w sieci lub kontroli bezpieczeństwa zasobów	W5 U2 U5 K4
					Umie wykorzystać dokumentację techniczną do pozyskania informacji niezbędnych do obsługi systemu Cisco IOS oraz potrafi sporządzić dokumentację do samodzielnie stworzonego programu	U1 U3
					Umie zidentyfikować zagrożenia bezpieczeństwa na podstawie zgromadzonych danych dotyczących ruchu przenoszonego w sieciach opartych o stos TCP/IP	W4 U5
3	**AUDYT SIECI, BEZPIECZNE OPROGRAMOWANIE (ASBO)**	16	16	12	Zna podstawowe zagrożenia bezpieczeństwa i metody ich neutralizowania	W2 W3 W4
					Umie wykorzystywać podatności wykryte podczas przeprowadzania testów bezpieczeństwa	U5
					Umie odczytać dokumentację techniczną, skonfigurować i praktycznie wykorzystać narzędzia służące do przeprowadzania testów bezpieczeństwa	U1 U5
					Zna i umie wykorzystywać środki służące do zabezpieczania infrastruktury sieciowej, serwerowej oraz oprogramowania	W5 U6
					Zna podstawowe zagadnienia bezpieczeństwa, związane z aplikacjami webowymi, umie zidentyfikować oraz poprawić błędy występujące w tych aplikacjach	W4 U2
					Umie sporządzić podstawową dokumentację dotyczącą przeprowadzania testów bezpieczeństwa	U3
					Umie rozwijać narzędzia służące do przeprowadzania testów bezpieczeństwa	U5 K3
4	**ZARZĄDZANIE BEZPIECZEŃ-STWEM (ZB)**	20	10	12	Zna podstawowe modele bezpieczeństwa (Bell-LaPadula, Biba, Clark-Wilson, chińskie mury), modele dostępu (DAC, MAC) i reprezentacje uprawnień (macierze dostępu, capabilities, ACLs, RBAC)	W1 W3
					Zna podstawowe kryteria oceny systemów bezpieczeństwa (Common Criteria, TCSEC, TNI, ITSEC, SEI-CMMI, SSE-SMM)	W6 W7
					Zna podstawy zarządzanie bezpieczeństwem opartego na analizie ryzyka	W6 W7
					Umie wykorzystać w praktyce metody postępowania z ryzykiem: wykrywające, odstraszające, prewencyjne, korekcyjne, odtwarzające, odszkodowawcze	U2 K2
					Umie odczytać i wykorzystać w praktyce dokumenty i normy dotyczące zarządzania bezpieczeństwem, w szczególności normy serii ISO 27000	W7 U1
					Umie sporządzić podstawową dokumentację dotyczącą ISMS przykładowej organizacji	W6 W7 U3
					Potrafi zaprojektować, zweryfikować, eksploatować i użytkować model dostępu przykładowego systemu informacyjnego.	U2 U3 U4 K3
5	**ASPEKTY PRAWNE BEZPIECZEŃSTWA**	16	0	8	Zna podstawowe akty prawne dotyczące ochrony informacji	W6 K2

	(APB)				Zna zasady odpowiedzialności karnej i służbowej w przypadku naruszeń bezpieczeństwa	W6 W7 K2
					Zna wymogi dotyczące sporządzania dokumentacji bezpieczeństwa	W6 W7 U1 U3
					Umie odnaleźć dokument prawny dotyczący zaistniałej sytuacji związanej z incydentem bezpieczeństwa	U1 W6 W7
					Umie sporządzić podstawową dokumentację dotyczącą incydentów bezpieczeństwa	W7 U3
Razem		122	58	60		

Matrycę efektów kształcenia (zamierzone efekty kształcenia dla programu – moduły kształcenia, w których osiągnięty jest efekt)

Tabela nr 3 Matryca efektów kształcenia

	P-T-KPK	P-T-BS	P-T-ASBO	P-T-ZB	P-T-APB
W1	X	X		X	
W2	X	X	X		
W3	X		X	X	
W4		X	X		
W5		X	X		
W6				X	X
W7				X	X
U1	X	X	X	X	X
U2		X	X	X	
U3	X	X	X	X	X
U4	X	X		X	
U5		X	X		
U6		X	X		
K1	X				
K2				X	X
K3		X	X		
K4		X			

4) Program studiów

Program studiów podyplomowych

Ochrona informacji w sieciach i systemach teleinformatycznych: projektowanie i audyt zabezpieczeń

l.p.	Przedmiot	Kod	Wymiar		Semestr I				Semestr II			
			W	L/C	w	c	l	p	w	c	l	p
1	**Kryptografia, protokoły kryptograficzne**	**P-T-KPK**	30	12	30	12		30				
2	**Bezpieczeństwo sieci**	**P-T-BS**	40	20	22		10	45	18		10	25
3	**Audyt sieci, bezpieczne oprogramowanie**	**P-T-ASBO**	16	16	8		8	20	8		8	10
4	**Zarządzanie bezpieczeństwem**	**P-T-ZB**	20	10					20	10		30
5	**Aspekty prawne bezpieczeństwa**	**P-T-APB**	16						16			30
	suma		**122**	**58**	60	12	18	95	62	10	18	95
	suma W+L/C		**180**		**90**			**95**	**90**			**95**

w - wykład
c – ćwiczenia
l – laboratorium
p – projekt

5). Zasady przyjmowania na studia (rekrutacji), zalecana liczebność grup zajęciowych;

Udział w Studiach brać mogą absolwenci studiów wyższych I stopnia (inżynierskie, licencjackie) lub II stopnia (magisterskie), zgodnie z § 4 Regulaminu Studiów Podyplomowych w PW. Przyjęcia w kolejności zgłoszeń, po opłaceniu opłaty za pierwszy semestr, do wyczerpania limitu miejsc.

Limit miejsc: 48 osób

Minimalna liczba zapisanych uczestników konieczna do uruchomienia edycji Studiów w danym semestrze: 20 osób

6). Terminy dokonywania opłat lub sposoby ich ustalania;

Studia podyplomowe są odpłatne. Wysokość opłaty wynosi 9500 zł. Opłaty można wnosić w całości, albo w dwóch ratach:

5000 zł przy zapisach,
4500 zł przed rozpoczęciem drugiego semestru.

7). Forma kontroli bieżących postępów w studiowaniu (rejestracji):

Przebieg studiów i postępy w nauce poszczególnych uczestników są kontrolowane na podstawie:

- prowadzenie list obecności na zajęciach,
- przeprowadzanie kolokwiów w czasie semestru,
- odnotowywanie realizacji zadań domowych,
- sprawdzanie postępu w realizacji zadań projektowych,
- zaliczanie realizacji zadań laboratoryjnych,
- udział studentów w konsultacjach,
- odnotowywanie aktywności studentów na wykładach, ćwiczeniach, seminariach i zajęciach laboratoryjnych.

Oceny pośrednie i końcowe odnotowywane są w dzienniku wyników studenta.

8). warunki otrzymania świadectwa ukończenia studiów podyplomowych;

1. Zaliczenie wszystkich przedmiotów, w tym:
- zaliczenie wszystkich zajęć laboratoryjnych,
- zaliczenie zadań projektowych,
- zaliczenie ćwiczeń, jeśli były na nich przewidziane kolokwia,
- zdanie wszystkich egzaminów.

Odpowiada to uzyskaniu **60 pkt. ECTS.**

2. Zdanie egzaminu końcowego.

Absolwenci studiów otrzymują wydane przez Politechnikę Warszawską świadectwo ukończenia studiów podyplomowych w danym zakresie.