Załącznik do Uchwały nr VI/243 Senatu Państwowej Wyższej Szkoły Zawodowej im. Witelona w Legnicy
z dnia 23 czerwca 2020 r.

PROGRAM STUDIÓW PODYPLOMOWYCH

1. **Jednostka organizacyjna prowadząca studia podyplomowe:**
   Wydział Nauk Społecznych i Humanistycznych

2. **Nazwa studiów podyplomowych:**
   Cyberbezpieczeństwo

3. **Forma studiów podyplomowych:**
   Studia podyplomowe prowadzone w formie studiów niestacjonarnych

4. **Założenia ogólne:**
   Studia podyplomowe kierowane są do osób pragnących poznać oraz doskonalić wiedzę i umiejętności z szerokiego spektrum zagadnień cyberbezpieczeństwa. Realizowane w trakcie studiów zagadnienia będą nauczane od podstaw, nie jest więc wymagana znajomość zagadnień technicznych związanych z cyberbezpieczeństwem czy bezpieczeństwem systemów teleinformatycznych. Uczestnikami studiów mogą być zarówno pracownicy przedsiębiorstw, administracji publicznej, w tym: organów ścigania, wymiaru sprawiedliwości oraz służb mundurowych, jak i osoby, dla których wiedza z tej dziedziny będzie uzupełnieniem kompetencji zawodowych.

   Celem studiów podyplomowych jest rozwijanie kompetencji, wiedzy, świadomości i praktycznych umiejętności z zakresu cyberbezpieczeństwa, z uwzględnieniem zdobycia podstawowych informacji dotyczących bezpieczeństwa i ochrony systemów, urządzeń, informacji i infrastruktury teleinformatycznej.

5. **Czas trwania studiów podyplomowych:** dwa semestry

6. **Ogólna liczba godzin zajęć dydaktycznych**: 160 godzin

7. **Ogólna liczba punktów ECTS wymagana do ukończenia studiów:** 30 punktów ECTS

8. **Wymagania wstępne kandydata:** dyplom ukończenia studiów wyższych

9. **Warunki ukończenia studiów podyplomowych:** uzyskanie zaliczeń i zdanie egzaminów przewidzianych w programie studiów oraz zdanie egzaminu końcowego.

10. **Plan studiów**:

I semestr

Lp.	Nazwa przedmiotu	Wykłady [l. godzin]	Ćwiczenia [l. godzin]	Forma zaliczenia	Punkty ECTS	Całkowity nakład pracy słuchacza [l. godzin]
1.	Cyberbezpieczeństwo w systemie bezpieczeństwa narodowego	4	6	zal oc	2	50
2.	Wstęp do informatyki	4	6	zal oc	2	50
3.	Prawo w IT	6	10	zal oc	3	75
4.	Technologie teleinformatyczne i bezpieczeństwo systemów teleinformatycznych	8	6	zal oc	3	75
5.	Bezpieczeństwo w cyberprzestrzeni	8	14	zal oc	4	100
6.	Cyberbezpieczeństwo a ochrona danych osobowych	2	6	zal oc	1	25
Razem		32	48	X	16	375

II semestr

Lp.	Nazwa przedmiotu	Wykłady [l. godzin]	Ćwiczenia [l. godzin]	Forma zaliczenia	Punkty ECTS	Całkowity nakład pracy słuchacza [l. godzin]
1.	Bezpieczeństwo baz danych, aplikacji www i urządzeń mobilnych	6	16	zal oc	4	100
2.	Bezpieczeństwo i obrona systemów i sieci komputerowych (korporacyjnych)	4	10	zal oc	3	75
3.	Zabezpieczanie danych cyfrowych	4	10	zal oc	2	50
4.	Zabezpieczenia informatyczne przed atakami w cyberprzestrzeni	4	10	zal oc	3	75
5.	Elementy kryptografii	4	12	zal oc	3	75
Razem		22	58	X	15	375

11. Określenie kierunkowych efektów kształcenia i ich odniesienie do charakterystyk wybranych efektów kształcenia właściwych dla obszaru kształcenia w zakresie nauk społecznych zawartych w Polskiej Ramie Kwalifikacji na poziomie 6 i 7.

Symbol efektu uczenia się	Kierunkowe efekty uczenia się dla studiów podyplomowych o nazwie „Cyberbezpieczeństwo"	Odniesienie do charakterystyk drugiego stopnia określonych na podstawie art. 7 ust. 3 i 4 ustawy z dnia 22 grudnia 2015 r. o Zintegrowanym Systemie Kwalifikacji na poziomie PRK
WIEDZA: zna i rozumie		
SPK_W01	w zaawansowanym stopniu wybrane fakty i zjawiska oraz dotyczące ich metody i teorie wyjaśniające złożone zależności między nimi, stanowiące podstawową wiedzę ogólną z zakresu cyberbezpieczeństwa	P6S_WG
SPK_W02	główne tendencje rozwojowe w zakresie zapewnienia cyberbezpieczeństwa	P7S-WG
SPK_W03	fundamentalne uwarunkowania prawne, ekonomiczne i etyczne oraz dylematy współczesnej cywilizacji związane z cyberbezpieczeństwem	P6S_WK
UMIEJĘTNOŚCI: potrafi		
SPK_U01	wykorzystywać posiadaną wiedzę w zakresie formułowania i rozwiązywania złożonych i nietypowych problemów występujących w sferze cyberbezpieczeństwa	P6S_UW
SPK_U02	wykonywać zadania związane z zabezpieczeniem systemów i sieci teleinformatycznych, dokumentów oraz urządzeń w warunkach niepewności i nieprzewidywalności poprzez dokonywanie oceny, krytycznej analizy i syntezy, właściwy dobór zaawansowanych metod i narzędzi	P6S_UW
SPK_U03	wykonywać zadania w sferze cyberprzestrzeni poprzez właściwy dobór źródeł i informacji z nich pochodzących oraz komunikować się z	P6S_UW P6S_UK

	otoczeniem z użyciem specjalistycznej terminologii cyberbezpieczeństwa	
SPK_U04	brać merytoryczny udział w dyskusji – przedstawiać i oceniać różne opinie i stanowiska z zakresu uwarunkowań cyberbezpieczeństwa i dyskutować o nich	P6S_UK
KOMPETENCJE SPOŁECZNE: jest gotów do		
SPK_K01	krytycznej oceny posiadanej wiedzy z zakresu cyberbezpieczeństwa, uznawania jej znaczenia w rozwiązywaniu problemów poznawczych i praktycznych oraz zasięgania opinii ekspertów w przypadku trudności z samodzielnym rozwiązaniem problemów z dziedziny bezpieczeństwa w cyberprzestrzeni	P6S_KK P7S_KK
SPK_K02	myślenia i działania w sposób przedsiębiorczy, przynoszący wymierne korzyści w zakresie zapewnienia cyberbezpieczeństwa i przeciwdziałania cyberzagrożeniom oraz działalności niezgodnej z prawem	P6S_KO P7S_KO
SPK_K03	odpowiedzialnego wykonywania ról zawodowych, w tym przestrzegania zapisów prawa oraz zasad etyki zawodowej i wymagania tego od innych	P6S_KR P7S_KR