Załącznik do Uchwały Nr 62/2024 Senatu UKSW
z dnia 27 czerwca 2024 r.

Program studiów podyplomowych ***Cyberbezpieczeństwo i nowoczesne technologie***

Liczba punktów ECTS konieczna dla ukończenia studiów podyplomowych	36
Forma zakończenia studiów podyplomowych	Egzamin ustny
Liczba semestrów	2
Liczba godzin zajęć	225
Poziom Polskiej Ramy Kwalifikacji	PRK 6
Cel studiów	Celem kształcenia jest przygotowanie słuchacza do rozpoznawania, wykrywania oraz przeciwdziałania zachowaniom niezgodnym z prawem w cyberprzestrzeni. Słuchacz uzyska wszechstronną wiedzę z zakresu zagadnień prawnych w cyberprzestrzeni oraz umiejętności praktyczne z zakresu wykrywania przestępczości komputerowej, prowadzenia czynności dochodzeniowo-śledczych oraz operacyjno-rozpoznawczych. Nabędzie umiejętności w zakresie projektowania i wdrażania systemów zabezpieczeń, monitorowania i analizowania zagrożeń, reagowania na incydenty bezpieczeństwa, oceny systemów bezpieczeństwa, ochrony danych osobowych poufnych, tworzenia polityk i procedur bezpieczeństwa, testowania zabezpieczeń oraz zarządzania ryzykiem. Ponadto rozwinie umiejętności praktyczne niezbędne w codziennej pracy.
Zasady rekrutacji	Złożenie dokumentów
Wymiar, zasady i forma odbywania praktyk (jeśli dotyczy)	Nie dotyczy

Efekty uczenia się w zestawach				
Symbol efektu uczenia się	**Efekt uczenia się**	**Symbol kryterium weryfikacji**	**Kryterium weryfikacji**	**Odniesienie do efektów uczenia się na poziomie 6/7/8* PRK**
PODSTAWY CYBERBEZPIECZEŃSTWA				
CBR_W01	posiada wiedzę ogólną z zakresu podstawowych pojęć cyberbezpieczeństwa	W.1.1	definiuje podstawowe pojęcia z obszaru cyberbezpieczeństwa	P6S_WG
		W.1.2	charakteryzuje cyberprzestępczość, haking, haktywizm, haktywizm patriotyczny, cyberterroryzm, cyberszpiegostwo, militarne wykorzystanie cyberprzestrzeni	
		W.1.3	wylicza konsekwencje analizy wielkich zbiorów danych, możliwe naruszenia prawa do prywatności, prawo do bycia zapomnianym	
		W.1.4	rozpoznaje przyszłe zagrożenia i trendy w cyberbezpieczeństwie	
		W.1.5	omawia strategie obronne	
CBR_W02	posiada wiedzę na poziomie rozszerzonym z zakresu infrastruktury IT	W2.1	charakteryzuje kluczowe komponenty architektury sieciowej (modele OSI i TCP/IP)	P6S_WG
		W2.2	omawia rolę protokołów sieciowych w działaniu Internetu	
		W2.3	omawia systemy adresacji IP, w tym IPv4 i IPv6, oraz zasady routingu i algorytmów wykorzystywanych do przesyłania danych przez sieć	
		W2.4	opisuje narzędzia i metody zarządzania siecią, monitorowania ruchu sieciowego i wykrywania anomalii	
CBR_W03	posiada wiedzę ogólną z zakresu ochrony danych osobowych i informacji niejawnych	W3.1	definiuje podstawowe pojęcia z obszaru ochrony danych osobowych i informacji niejawnych	P6S_WG

		W3.2	omawia zapisy ustawy o ochronie danych osobowych	
		W3.3	identyfikuje główne metody, techniki i narzędzia pozyskiwania i ochrony informacji, w tym informacji niejawnych i danych, w tym danych osobowych	
CBR_W04	posiada wiedzę o polskim oraz unijnym porządku prawnym w obszarze cyberbezpieczeństwa	W4.1	wyjaśnia prawne aspekty zagrożeń w cyberprzestrzeni	P6S_WG
		W4.2	omawia koncepcje zadań operacyjnych w dziedzinie cyberbezpieczeństwa w odniesieniu do obowiązujących aktów prawnych	
		W4.3	omawia zapisy kodeksu karnego w obszarze cyberprzestępczości, ustawy o krajowym systemie cyberbezpieczeństwa, ustawy o działaniach antyterrorystycznych w obszarze cyberbezpieczeństwa, ustawy o usługach zaufania oraz identyfikacji elektronicznej oraz przepisy o własności intelektualnej	
		W4.4	podaje przykłady przestępstw internetowych na gruncie prawa karnego (hakowanie i ataki na systemy informatyczne, oszustwa finansowe i przestępstwa gospodarcze online, naruszenia prywatności i stalking online, usunięcie i zniszczenie danych, przygotowywanie i posiadanie narzędzi hackerskich)	
		W4.5	objaśnia zapisy unijnych aktów prawnych w obszarze cyberbezpieczeństwa	
		W4.6	przywołuje Strategię Cyberbezpieczeństwa RP	
		W4.7	omawia prawne aspekty pozyskiwania danych w Internecie	

		W4.8	opowiada o zwalczaniu przestępstw internetowych o charakterze transgranicznym, międzynarodowych projektach zw. ze zwalczaniem cyberprzestępczości i o roli Interpolu	
CBR_W05	posiada wiedzę z zakresu narzędzi i platform wykorzystywanych do skoordynowanego rozpowszechniania manipulowanych treści	W5.1	wyjaśnia rolę mediów w opinii publicznej	P6S_WG
		W5.2	omawia oprogramowania i algorytmów używanych do monitorowania i analizy zachowań w sieci.	
		W5.3	objaśnia regulacje prawne dotyczące cyberbezpieczeństwa i ochrony danych osobowych, odpowiedzialność za rozpowszechnianie nieprawdziwych informacji	
CBR_U01	wykorzystuje wiedzę o zagrożeniach związanych z cyberprzestrzenią	U1.1	podejmuje pierwsze działania obronne oparte na rozumieniu zasad funkcjonowania sieci	P6S_UW
		U1.2	identyfikuje zadania i zakres współpracy krajowych oraz międzynarodowych organizacji zajmujących się bezpieczeństwem w cyberprzestrzeni	
CBR_U02	wykorzystuje wiedzę o sposobach ochrony danych osobowych	U2.1	przygotowuje dokumentację związaną j z procesem przetwarzania danych osobowych	P6S_UW
CBR_U03	przeprowadza analizę procesu komunikacji	U3.1	analizuje kluczowe protokoły sieciowe, tj. IP, TCP, UDP, HTTP, HTTPS, DNS, i SMTP	P6S_UW
		U3.2	przedstawia proces komunikacji na warstwowym modelu protokołów TCP/IP oraz na modelu odniesienia ISO/OSI	
		U3.3	wykorzystuje protokół SSL do zapewnienia bezpiecznej komunikacji	
CBR_K01	określa kierunki niezbędne dla zapewnienia bezpieczeństwa wewnętrznego w realiach społeczeństwa informacyjnego	K1.1	tworzy i realizuje projekty na rzecz zapewnienia cyberbezpieczeństwa	P6S_KO

CBR_K02	buduje świadomość w zakresie cyberbezpieczeństwa	K2.1	uznaje znaczenie wiedzy w rozwiązywaniu złożonych problemów poznawczych i praktycznych w zakresie bezpieczeństwa w cyberprzestrzeni	P6S_KR
		K2.2	przedstawia problemy bezpieczeństwa w Polsce i na świecie, ma poczucie misji i odpowiedzialności za bezpieczeństwo ludzi w demokratycznym państwie prawnym	
		K2.3	oszacowuje poziom swojej wiedzy, możliwości poznania i własnych ograniczeń, potrzeby stałego poszerzania wiedzy i umiejętności w kontekście podjęcia pracy w instytucjach publicznych i niepublicznych odpowiedzialnych za zapewnienie cyberbezpieczeństwa	
ZARZĄDZANIE RYZYKIEM				
CBR_W14	posiada wiedzę o metodach oceny ryzyka bezpieczeństwa cybernetycznego	W14.1	definiuje sposób identyfikacji luk w zabezpieczeniach (audyty bezpieczeństwa, testy penetracyjne i ocena podatności)	P6Z_WT
		W14.2	charakteryzuje standardy opisujące procesy oceny ryzyka bezpieczeństwa informatycznego, w tym: NIST SP 800-30	
		W14.3	omawia standardy z obszaru bezpieczeństwa informacji opracowane przez organizacje standaryzacyjne, takie jak NIST, ITU-T, ISO, IEEE, ISACA	
		W14.4	omawia regulacje prawne i standardy branżowe dotyczące cyberbezpieczeństwa (GDPR, ISO 27001)	
CBR_U04	zarządza ryzykiem i dokonuje oceny bezpieczeństwa	U4.1	opracowuje dokumentację niezbędną do prowadzenia audytu bezpieczeństwa wewnątrz organizacji	P6Z_UI
		U4.2	przygotowuje organizację do wdrożenia normy ISO 27001	

CBR_U05	formułuje własne opinie w odniesieniu do zjawisk związanych z cyberbezpieczeństwem	U5.1	przygotowuje rekomendacje dotyczące wzmocnienia ochrony systemów, infrastruktury i danych firmy	P6Z_UO
CBR_K03	efektywnie komunikuje się z otoczeniem podczas działań zmierzających do obniżenia ryzyka	K3.1	formułuje czytelne komunikaty, przekazując otoczeniu w sposób kompetentny i fachowy, informacje o istniejących zagrożeniach	P6Z_KW
		K3.2	proponuje najskuteczniejsze rozwiązania w zakresie stosowania skutecznych zabezpieczeń	
		K3.3	wykorzystuje nowoczesne technologie w procesie komunikowania otoczeniem	
BEZPIECZEŃSTWO INFRASTRUKTURY IT				
CBR_W06	posiada wiedzę ogólną z zakresu ochrony infrastruktury teleinformatycznej	W6.1	identyfikuje zagrożenia środowiskowe	P6S_WG
		W6.2	definiuje zagrożenia techniczne	
		W6.3	omawia metody zapobiegania zagrożeniom środowiskowym i technicznym	
		W6.4	charakteryzuje techniki szyfrowania danych oraz zarządzanie tożsamością i dostępem	
CBR_W07	posiada wiedzę na poziomie rozszerzonym w zakresie ochrony elektronicznych systemów płatności	W7.1	opisuje różne formy elektronicznych systemów płatności, w tym płatności kartami, bankowości internetowej, mobilnych systemów płatności oraz kryptowalut	P6Z_WT

		W7.2	omawia podstawowe mechanizmy działania zabezpieczeń stosowanych w systemach płatności	
		W7.3	rozpoznaje metody ochrony elektronicznych systemów płatności, w tym technik szyfrowania, uwierzytelniania wieloskładnikowego i bezpiecznego kodowania	
CBR_W08	posiada wiedzę o strukturze i funkcjonalnościach smart kontraktów	W8.1	analizuje struktury kodu smart kontraktów, ich życiowego cyklu oraz interakcji z blockchainem	P6Z_WZ
		W8.2	omawia potencjalne zagrożenia i luki w bezpieczeństwie, które mogą wystąpić podczas tworzenia i eksploatacji smart kontraktów	
		W8.3	wskazuje metody zapobiegania zagrożeniom, które mogą wystąpić podczas tworzenia i eksploatacji smart kontraktów	
CBR_U06	rozpoznaje ataki na elektroniczne systemy płatności	U6.1	analizuje najczęstsze zagrożenia i ataki na elektroniczne systemy płatności (phishing, malware, ataki typu man-in-the-middle, exploitowanie słabości w oprogramowaniu oraz inne techniki wykorzystywane przez cyberprzestępców)	P6Z_UI
CBR__U07	implementuje strategie obronne w rzeczywistym środowisku pracy	U7.1	identyfikuje zagrożenia w firmowej infrastrukturze IT	P6Z_UO
		U7.2	stosuje techniki szyfrowania, uwierzytelniania wieloskładnikowego i bezpiecznego kodowania	
CBR_K04	określa nowe zdolności obronne państwa	K4.1	uznaje wzrastające znaczenie elementów teleinformatycznych w funkcjonowaniu państwa	P6S_KO
		K4.2	uznaje koncepcję rozwoju zdolności w obszarze cyberbezpieczeństwa infrastruktury krytycznej państwa	
		K4.3	podkreśla znaczenie rozwoju technologii na rzecz zapewnienia cyberbezpieczeństwa, ma poczucie misji i odpowiedzialności za bezpieczeństwo innych osób	

CBR_K05	określa możliwości zastosowania technologii blockchain w realnych scenariuszach biznesowych	K5.1	oceniania w sposób krytyczny możliwości i ograniczenia smart kontraktów, projektowania bezpiecznych i efektywnych rozwiązań opartych na technologii blockchain oraz zastosowania tych umiejętności w realnych scenariuszach biznesowych i prawnych	P6S_KK
FORENSIC				
CBR_W09	posiada wiedzę na poziomie rozszerzonym z zakresu ukrytych segmentów Internetu	W9.1	wyjaśnia funkcjonowanie deep webu, darknetu oraz sieci anonimowych takich jak I2P (Invisible Internet Project) i TOR (The Onion Router),	P6Z_WZ
		W9.2	uzasadnia znaczenie deep webu, darknetu oraz sieci anonimowych i TOR (The Onion Router) dla cyberbezpieczeństwa i śledztw cyfrowych	
		W9.3	opisuje architekturę sieci TOR i I2P	
CBR_W10	posiada wiedzę na poziomie rozszerzonym w zakresie metodyki i narzędzi forensic	W10.1	wymienia metody i narzędzia wykorzystywane w cyberśledztwach i analizie forensic zasobów deep webum i darknetu	P6Z_WT
		W10.2	omawia wyzwania i najlepsze praktyki w gromadzeniu dowodów cyfrowych	
		W10.3	dopasowuje narzędzia niezbędnych do eksploracji deep webu i darknetu	
		W10.4	sporządza diagnozę ataków w cyberprzestrzeni	
		W10.5	wybiera odpowiednie narzędzia (programowe oraz sprzętowe)	

CBR_W11	posiada wiedzę z zakresu podstawowych pojęć OSINT	W11.1	charakteryzuje pojęcie wywiadu z otwartych źródeł	P6S_WK
		W11.2	wyjaśnia znaczenie działań polegających na zdobywaniu i gromadzeniu informacji z otwartych źródeł	
		W11.3	omawia etyczne aspekty pozyskiwania danych z Internetu	
CBR_W12	posiada wiedzę na poziomie rozszerzonym z zakresu narzędzi i techniki OSINT	W12.1	omawia szczegółowo narzędzia, aplikacje do pozyskiwania danych z różnych źródeł internetowych (w tym mediów społecznościowych, for internetowych, baz danych, archiwów online oraz innych dostępnych publicznie zasobów)	P6Z_WO
		W12.2	opisuje techniki monitorowania mediów społecznościowych w celu identyfikacji trendów, zagrożeń i potencjalnych źródeł informacji o charakterze bezpieczeństwa.	
		W12.3	omawia szczegółowo techniki pozyskiwania danych z różnych źródeł internetowych (w tym mediów społecznościowych, for internetowych, baz danych, archiwów online oraz innych dostępnych publicznie zasobów)	
		W12.4	analizuje rzeczywiste przypadki użycia OSINT w kontekście cyberbezpieczeństwa (identyfikacja zagrożeń, zarządzanie kryzysowe i ocena ryzyka)	
CBR_W13	posiada wiedzę ogólną z zakresu podstaw analizy kryminalnej w cyberprzestrzeni	W13.1	omawia najczęstsze formy przestępczości cyfrowej oraz metody ich wykrywania.	P6S_WK
		W13.2	charakteryzuje narzędzia i technikach stosowane do gromadzenia danych z Internetu, sieci społecznościowych, systemów informatycznych oraz innych źródeł cyfrowych, które mogą zawierać informacje o działalności przestępczej	

CBR_U09	raportuje wyniki analiz	U9.1	analizuje rzeczywiste przypadki z wykorzystaniem narzędzi do zbierania danych	P6S_UW
		U9.2	wykorzystuje poznane techniki raportowania	
CBR_U10	monitoruje media społecznościowe w celu identyfikacji zagrożeń	U10.1	wykorzystuje zaawansowane narzędzia do monitorowania mediów	P6Z_UI
		U10.2	tworzy analizę mediów społecznościowych w celu identyfikacji trendów, zagrożeń i potencjalnych źródeł informacji o charakterze bezpieczeństwa.	
CBR_U11	przygotowuje środowisko pracy odpowiednio do danego zadania	U11.1	komponuje narzędzia programowe oraz sprzętowe	P6Z_UO
CBR_U12	reaguje na zagrożenia płynące z ukrytych części Internetu	U12.1	ocenia i analizuje zagrożenia płynące z ukrytych części Internetu (cyberprzestępczość, handel narkotykami, bronią oraz inne nielegalne działania)	P6Z_UO
CBR_U13	planuje i organizuje pracę własną oraz zespołu	U13.1	szacuje czas, opracowuje harmonogram oraz określa priorytety służące realizacji zadań, zarówno pracując indywidualnie, jak i współdziałając z innymi w ramach prac zespołowych	P6S_UO

Opis planu studiów podyplomowych						
L.P.	**Nazwa przedmiotu/modułu zajęć**	**Liczba godzin**	**Forma zajęć**	**Liczba ECTS**	**Odniesienie do efektów uczenia się na studiach podyplomowych**	**Sposób weryfikacji efektów uczenia się**
1	Cyberbezpieczeństwo i jego zagrożenia	12	Wykład - 6 Ćwiczenia - 6	2	W.1.1 W.1.2 K1.1 K2.1 K2.3	egzamin
2	Cyberprzestępczość w ujęciu prawa międzynarodowego i prawa Unii Europejskiej	10	Wykład	2	W4.1 W4.2 W4.5 W4.7 W4.8 W5.3 U1.2 K4.1	zaliczenie z oceną
3	Odpowiedzialność karna i cywilna za naruszanie cyberbezpieczeństwa	8	Wykład - 4 Ćwiczenia - 4	1	W.1.2 W.1.3 W4.1 W4.4 W5.3 K2.2 K2.3	zaliczenie
4	Krajowy system cyberbezpieczeństwa	8	Wykład - 4 Ćwiczenia - 4	1	W.1.4 W.1.5 W4.1 W4.2 W4.3 W4.6 K2.2 K4.1 K4.2 K4.3	zaliczenie
5	Ochrona danych osobowych	16	Wykład - 12 Ćwiczenia - 4	3	W.1.3 W3.1 W3.2 W3.3 W5.3 U2.1 K2.3	zaliczenie z oceną
6	Cyberbezpieczeństwo wewnątrz organizacji	8	Wykład- 4 Ćwiczenia - 4	1	U1.1 U1.2 W14.1 W14.2 K3.1 K3.2 K3.3 W6.1 W6.2 U7.1	zaliczenie
7	Infrastruktura Internetu i usługi sieciowe	8	Wykład- 4 Ćwiczenia - 4	1	W2.1 W2.2 W2.3 W2.4 U3.1 U3.2 U3.3 U5.1	zaliczenie
8	Biały wywiad – pozyskiwanie informacji z Internetu	12	Wykład - 4 Ćwiczenia - 8	2	K3.1 K3.2 K3.3 W11.1 W11.2 W11.3 W12.1 W12.2 W12.3 W12.4 U10.1 U10.2	egzamin
9	Zagrożenia dla elektronicznych systemów płatności	8	Wykład - 4 Ćwiczenia - 4	1	W7.1 W7.2 W7.3 U6.1 U7.2 U11.1	zaliczenie
10	Algorytmy i protokoły kryptograficzne	25	Wykład - 20 Ćwiczenia - 5	4	W5.2 W10.5 U9.2 U11.1 U13.1	egzamin
11	Zintegrowanie kompetencji	10	Konwersatorium	2	W.1.1 K2.1 K2.3 U13.1	zaliczenie

Specjalizacja administracyjno-prawna						
1	Smart kontrakty	12	Wykład - 6 Ćwiczenia - 6	2	W8.1 W8.2 W8.3 K5.1 U9.1 U9.2	zaliczenie z oceną
2	Ochrona własności intelektualnej i informacji niejawnych	12	Wykład	2	W3.1 W4.3 K2.1 K2.3	zaliczenie z oceną
3	Zarządzanie ryzykiem i ocena bezpieczeństwa systemów IT	20	Wykład - 12 Ćwiczenia - 8	4	W14.1 W14.2 W14.3 W14.4 U4.1 U4.2 U5.1 K3.1 K3.2 K3.3	egzamin
4	Narzędzia i techniki manipulowania opinią publiczną	8	Wykład - 4 Ćwiczenia - 4	1	W5.1 K2.3	zaliczenie z oceną
5	Norma ISO 27001	16	Wykład - 8 Ćwiczenia - 8	3	W14.3 U4.2 U5.1	zaliczenie z oceną
6	Zajęcia praktyczne	32	Warsztaty	4	U2.1 K1.1 W14.1 W14.4 U4.1 U4.2 U5.1 W10.4 W11.3 U13.1	zaliczenie
Specjalizacja Informatyka śledcza						
1	Ukryte zasoby Internetu: Deepweb/Darknet/I2P/TOR	12	Wykład - 6 Ćwiczenia - 6	2	W9.1 W9.2 W9.3 W10.1 W10.3 W10.4 U12.1 U13.1	zaliczenie z oceną
2	Bezpieczeństwo systemów i sieci	12	Wykład	2	U1.1 W6.2 W6.4 W8.2	zaliczenie z oceną
3	Analiza kryminalna w procesie zwalczania cyberprzestępczości	20	Wykład - 12 Ćwiczenia - 8	4	W10.5 W13.1 W13.2 U9.1 U9.2 U10.1 U11.1 U12.1 U13.1	egzamin
4	Nośniki danych cyfrowych	8	Wykład - 4 Ćwiczenia - 4	1	W10.2 W10.5 U9.2 U11.1	zaliczenie z oceną
5	Wprowadzenie do informatyki śledczej	16	Wykład - 8 Ćwiczenia - 8	3	K2.3 U6.1 W10.1 W10.4	zaliczenie z oceną
6	Laboratorium informatyki śledczej	32	Warsztaty	4	U1.1 K1.1 U7.2 W10.3 W10.4 W10.5 U11.1 U13.1	zaliczenie
		225		**36**		