Załącznik do Uchwały Senatu Nr 35/V/2023
Wyższej Szkoły Policji w Szczytnie
z dnia 23 maja 2023 r.

Wyższa Szkoła Policji
w Szczytnie

Wydział Bezpieczeństwa i Nauk Prawnych

PROGRAM STUDIÓW

BEZPIECZEŃSTWO W CYBERPRZESTRZENI

(nazwa kierunku studiów)

STUDIA DRUGIEGO STOPNIA

(poziom kształcenia)

PRAKTYCZNY

(profil kształcenia)

NAUKI SPOŁECZNE

(dziedzina nauki)

SZCZYTNO 2023

1. Ogólna charakterystyka prowadzonych studiów zawierająca:
   1) nazwę kierunku studiów – **Bezpieczeństwo w cyberprzestrzeni**;
   2) poziom kształcenia – **studia drugiego stopnia**;
   3) profil kształcenia – **praktyczny**;
   4) formę lub formy studiów – **studia stacjonarne i niestacjonarne**;
   5) tytuł zawodowy uzyskiwany przez absolwenta – **magister**;
   6) liczbę semestrów – **cztery semestry**;
   7) liczbę ECTS konieczną do ukończenia studiów na danym poziomie: **120 ECTS**
   8) wskazanie dyscypliny naukowej, do której przyporządkowany jest kierunek studiów, a w przypadku przyporządkowania kierunku do więcej niż jednej dyscypliny – wskazanie dyscypliny wiodącej, w ramach której będzie uzyskiwana ponad połowa efektów uczenia się, oraz pozostałych dyscyplin;

Wyszczególnienie	Dyscyplina	Procentowy udział efektów uczenia się przypisanych do wskazanej dyscypliny w łącznej liczbie efektów uczenia się
Dyscyplina naukowa wiodąca	nauki o bezpieczeństwie	79,5 %
Pozostałe dyscypliny naukowe	nauki prawne	20,5 %
	Ogółem	**100%**

2. Opis sylwetki absolwenta, obejmujący ogólny opis kształcenia oraz możliwości zatrudnienia (typowe miejsca pracy) i kontynuacji kształcenia przez absolwentów studiów.

Celem kształcenia na kierunku Bezpieczeństwo w cyberprzestrzeni jest przygotowanie wysoko wykwalifikowanych specjalistów do pracy w organach ścigania (m.in. policji, straży granicznej), zajmujących się zwalczaniem cyberprzestępczości oraz w komórkach administracji publicznej, która realizuje zadania w zakresie cyberbezpieczeństwa, chcących podnieść swoje kwalifikacje w dynamicznie rozwijającym się świecie cyfrowym. Studia wyższe drugiego stopnia realizowane w Wyższej Szkole Policji w Szczytnie na kierunku Bezpieczeństwo w cyberprzestrzeni są adresowane do wszystkich osób posiadających kwalifikacje pierwszego stopnia, których aktualna i spodziewana praca (służba) będzie związana z szeroko rozumianym cyberbezpieczeństwem oraz zwalczaniem cyberprzestępczości.

Absolwent studiów drugiego stopnia będzie posiadał wiedzę z zakresu zwalczania przestępczości w cyberprzestrzeni oraz zabezpieczania dowodów w środowisku cyfrowym. Będzie znał funkcjonalność oprogramowania do analizy śledczej, zarówno jednostek centralnych jak i urządzeń mobilnych. Będzie wiedział jak przeprowadzić analizę poszczególnych elementów struktury systemu operacyjnego, a także znał programowe i sprzętowe systemy przeciwdziałania i wykrywania włamań. Pozna działanie sieci anonimizujących oraz poszczególne elementy ich funkcjonowania. Będzie znał zasady działania rynków finansowych w zakresie kryptowalut oraz funkcjonalność narzędzi do analizy i śledzenia wybranych wirtualnych pieniędzy. Absolwent pozna technologie chmur obliczeniowych, ich prawną regulacje oraz rozwiązania istotne z uwagi na pozyskiwanie dowodów działalności przestępczej z chmur obliczeniowych.

Będzie znał organizację i funkcjonowanie podmiotów odpowiedzialnych w sprawach bezpieczeństwa i porządku publicznego. Studia pozwolą absolwentowi na zdobycie wiedzy z zakresu nauk społecznych. Student pozna również wybrane zagadnienia socjotechniki oraz inżynierii społecznej, a także tożsamości społecznej użytkownika Internetu oraz negatywnych zjawisk społecznych związanych z informatyzacją.

W zakresie umiejętności absolwent będzie znał podstawowe techniki włamań do systemów komputerowych i będzie potrafił zabezpieczyć dane dotyczące działań przestępczych w środowisku cyfrowym, w tym możliwości technicznego i procesowego zabezpieczenia kryptowalut. Będzie w stanie przeprowadzić analizę pamięci RAM oraz poszczególnych plików systemowych i innych nieznanego typu zarówno z systemów komputerowych jak i systemów urządzeń mobilnych. Będzie potrafił zabezpieczyć dane z systemów wirtualnych. Będzie w stanie sprawnie pozyskiwać dane z sieci Internet oraz umiejętnie interpretować informacje z aplikacji OSINT-owych. Przeprowadzi samodzielnie audyt bezpieczeństwa systemu komputerowego oraz będzie w stanie stworzyć bezpieczne środowisko i ochronę danych osobowych w przestrzeni internetowej. Sprawnie określi także reguły zarządzania ryzykiem w instytucjach publicznych i biznesowych oraz określi ich wpływ na bezpieczeństwo w przestrzeni publicznej. Będzie posiadał umiejętności odzyskiwania danych z systemów informatycznych i nośników z wykorzystaniem najnowszych technik i narzędzi. Będzie potrafił gromadzić i analizować dane ze źródeł ustrukturyzowanych i nieustrukturyzowanych oraz lokalizować i usuwać źródła nielegalnej aktywności w cyberprzestrzeni.

Absolwent studiów na kierunku Bezpieczeństwo w cyberprzestrzeni będzie świadomy znaczenia i wykorzystania wiedzy w procesie dowodzenia oraz umiejętności samokształcenia, korzystając ze źródeł krajowych, zagranicznych, pism branżowych oraz zasobów cyfrowych. Będzie potrafił przygotować i przedstawić ustandaryzowany raport z analizy bezpieczeństwa IT oraz zaproponować usprawnienia. Będzie przygotowany do pracy na stanowiskach kierowniczych oraz jako lider zespołów w administracji publicznej, w tym w jednostkach organizacyjnych służb państwowych odpowiedzialnych za bezpieczeństwo wewnętrzne państwa.

2. Efekty uczenia się dla kierunku studiów w postaci tabeli.

Opis efektów uczenia się dla kierunku: Bezpieczeństwo w cyberprzestrzeni			
Poziom kształcenia :	studia drugiego stopnia		
Specjalność:	bez specjalności		
Profil kształcenia:	praktyczny		
Kod opisu składnika kierunkowego efektu uczenia się	**Opis kierunkowego efektu uczenia się**	**Kod składnika opisu efektów uczenia się dla kwalifikacji na poziomie 7***	**Odniesienie do uniwersalnej charakterystyki poziomu drugiego stopnia PRK**
w zakresie wiedzy – ZNA I ROZUMIE:			
K_W01	wybrane procesy, zjawiska, definicje i teorie w naukach społecznych i innych związanych z kierunkiem studiów, występujące między nimi złożone zależności oraz w pogłębiony sposób wykorzystuje je w rozwiązywaniu problemów bezpieczeństwa w cyberprzestrzeni, w tym w działalności zawodowej	P7S_WG	P7U_W
K_W02	procesy, zjawiska, terminy, definicje i główne tendencje rozwojowe w naukach o bezpieczeństwie, w tym w szczególności w zakresie bezpieczeństwa w cyberprzestrzeni oraz w pogłębiony sposób wykorzystuje je w rozwiązywaniu problemów bezpieczeństwa w cyberprzestrzeni, w tym w działalności zawodowej	P7S_WG	P7U_W
K_W03	wybrane zagadnienia z zakresu zaawansowanej wiedzy szczegółowej, w tym w szczególności w zakresie informatyki, elektroniki, telekomunikacji i cybernetyki oraz w pogłębiony sposób wykorzystuje je w rozwiązywaniu problemów bezpieczeństwa w cyberprzestrzeni, w tym w działalności zawodowej	P7S_WG	P7U_W
K_W04	metody, techniki, narzędzia stosowane w naukach społecznych, w tym w szczególności w naukach o bezpieczeństwie, służące do wykrywania i zwalczania przestępczości w cyberprzestrzeni oraz w pogłębiony sposób wykorzystuje je w rozwiązywaniu problemów cyberbezpieczeństwa, w tym w działalności zawodowej	P7S_WG	P7U_W
K_W05	kluczowe metody, techniki i narzędzia stosowane w innych naukach związanych z kierunkiem studiów, w tym w szczególności w informatyce, elektronice, telekomunikacji i cybernetyce, służące do wykrywania i zwalczania przestępczości w cyberprzestrzeni oraz w pogłębiony sposób wykorzystuje je w rozwiązywaniu problemów cyberbezpieczeństwa, w tym w działalności zawodowej	P7S_WG	P7U_W
K_W06	zasady działania i funkcje systemów informatycznych, urządzeń, oprogramowania, nośników danych, aplikacji i innych instrumentów mających wpływ na bezpieczeństwo w cyberprzestrzeni oraz rozumie konieczność ich praktycznego zastosowania w działalności zawodowej	P7S_WG	P7U_W
K_W07	systemy norm i reguł prawnych, w tym w szczególności w zakresie bezpieczeństwa w cyberprzestrzeni oraz w pogłębiony sposób wykorzystuje je w rozwiązywaniu problemów praktycznych, w tym w działalności zawodowej	P7S_WG	P7U_W
K_W08	specyfikę postępowania dowodowego, w tym w szczególności o przestępstwa w cyberprzestrzeni	P7S_WG	P7U_W
K_W09	zasady ochrony, dostępu, gromadzenia i przetwarzania danych, w tym w szczególności danych cyfrowych	P7S_WG	P7U_W
K_W10	zadania i zasady funkcjonowania oraz istotę i zakres współpracy krajowych oraz międzynarodowych organizacji zajmujących się bezpieczeństwem w cyberprzestrzeni i zwalczaniem cyberprzestępczości	P7S_WG	P7U_W
K_W11	zasady zarządzania, procesy decyzyjne oraz inne reguły obowiązujące w organizacji, w tym w szczególności w organizacjach zajmujących się bezpieczeństwem w cyberprzestrzeni i zwalczaniem cyberprzestępczości	P7S_WG	P7U_W
K_W12	kluczowe elementy infrastruktury bezpieczeństwa, w tym w szczególności infrastruktury krytycznej i cyberbezpieczeństwa	P7S_WG	P7U_W
K_W13	zróżnicowane zjawiska dewiacyjne i przestępcze oraz czynniki je determinujące, w tym w szczególności w cyberprzestrzeni oraz formy przeciwdziałania i profilaktyki tego rodzaju przestępczości	P7S_WG	P7U_W
K_W14	trendy związane z rozwojem technologii cyfrowych i innych narzędzi	P7S_WG	P7U_W

	informatycznych oraz rozumie ich wpływ na zachowanie człowieka, grup społecznych i innych podmiotów, zarówno w cyberprzestrzeni, jak i środowisku społecznym		
K_W15	fundamentalne dylematy współczesnej cywilizacji i ich wpływ na bezpieczeństwo w cyberprzestrzeni jednostek, grup społecznych i innych podmiotów	P7S_WK	P7U_W
K_W16	ekonomiczne, etyczne i inne uwarunkowania działalności organizacji zajmujących się bezpieczeństwem w cyberprzestrzeni i zwalczaniem cyberprzestępczości	P7S_WK	P7U_W
K_W17	zasady skutecznej komunikacji, zarówno w języku polskim, jak i w języku obcym oraz w pogłębiony sposób wykorzystuje je w rozwiązywaniu problemów bezpieczeństwa w cyberprzestrzeni, w tym w działalności zawodowej	P7S_WK	P7U_W
K_W18	zasady bezpieczeństwa i higieny pracy, ochrony przeciwpożarowej oraz zasady udzielania pierwszej pomocy i wykorzystuje je w działalności zawodowej	P7S_WK	P7U_W
K_W19	systemy biblioteczne i informatyczne wykorzystywane w procesie pozyskiwania informacji i pogłębiania wiedzy, w tym w szczególności w zakresie bezpieczeństwa w cyberprzestrzeni	P7S_WK	P7U_W
w zakresie umiejętności – POTRAFI:			
K_U01	integrować wiedzę oraz wskazywać na zależności procesów i zjawisk z zakresu nauk społecznych i innych nauk związanych z kierunkiem studiów przy formułowaniu i rozwiązywaniu złożonych problemów bezpieczeństwa w cyberprzestrzeni, w tym w działalności zawodowej	P7S_UW	P7U_U
K_U02	wykorzystać pogłębioną wiedzę z nauk o bezpieczeństwie, w tym w szczególności w zakresie bezpieczeństwa w cyberprzestrzeni, przy formułowaniu i rozwiązywaniu złożonych problemów praktycznych oraz zastosować ją podczas realizacji typowych dla działalności zawodowej zadań	P7S_UW	P7U_U
K_U03	wykorzystać wybrane elementy zaawansowanej wiedzy szczegółowej w zakresie informatyki, elektroniki, telekomunikacji i cybernetyki przy formułowaniu i rozwiązywaniu złożonych problemów bezpieczeństwa w cyberprzestrzeni oraz zastosować je podczas realizacji złożonych i nietypowych dla działalności zawodowej zadań, również w warunkach nieprzewidywalnych	P7S_UW	P7U_U
K_U04	w sposób prawidłowy dobierać oraz stosować metody, techniki i narzędzia wykorzystywane w naukach społecznych i innych naukach związanych z kierunkiem studiów, użyteczne w rozwiązywaniu złożonych problemów bezpieczeństwa w cyberprzestrzeni	P7S_UW	P7U_U
K_U05	w sposób prawidłowy dobierać, przystosować oraz zastosować metody, techniki i narzędzia wykorzystywane w naukach o bezpieczeństwie, użyteczne w rozwiązywaniu typowych problemów bezpieczeństwa w cyberprzestrzeni	P7S_UW	P7U_U
K_U06	w sposób prawidłowy dobierać oraz stosować wybrane metody, techniki i narzędzia zaawansowanej wiedzy szczegółowej w zakresie informatyki, elektroniki, telekomunikacji i cybernetyki oraz zastosować je podczas realizacji złożonych i nietypowych dla działalności zawodowej zadań	P7S_UW	P7U_U
K_U07	analizować i interpretować stany faktyczne z wykorzystaniem właściwych źródeł informacji (baz danych, nośników danych, informacji uzyskanych przy użyciu środków cyfrowych lub elektronicznych) w celu rozwiązywania złożonych problemów bezpieczeństwa w cyberprzestrzeni	P7S_UW	P7U_U
K_U08	w sposób prawidłowy zastosować przepisy prawa, analizować stany faktyczne z wykorzystaniem tych przepisów oraz wnioskować o mechanizmie działania przestępczego i jego sprawcy, w tym w szczególności w sprawach o przestępstwa w cyberprzestrzeni	P7S_UW	P7U_U
K_U09	zaplanować i przeprowadzić czynności w ramach postępowania dowodowego w sprawach o przestępstwa w cyberprzestrzeni	P7S_UW	P7U_U
K_U10	sporządzić dokumentację, w tym procesową i techniczną, stosownie do sformułowanego problemu z zakresu bezpieczeństwa w cyberprzestrzeni	P7S_UW	P7U_U
K_U11	stosować zasady bezpiecznego przetwarzania, dostępu, gromadzenia i przetwarzania danych, w tym w szczególności danych cyfrowych	P7S_UW	P7U_U
K_U12	identyfikować zadania i zakres współpracy krajowych oraz międzynarodowych organizacji zajmujących się bezpieczeństwem w cyberprzestrzeni i zwalczaniem cyberprzestępczości oraz zastosować	P7S_UW	P7U_U

	tę wiedzę podczas realizacji typowych dla działalności zawodowej zadań		
K_U13	w sposób twórczy wnioskować o przyczynach i przebiegu zjawisk społecznych, w tym przestępczych, i ich wpływie na bezpieczeństwo jednostek, grup społecznych i innych podmiotów, w tym w szczególności w cyberprzestrzeni oraz zastosować tę wiedzę w działalności zawodowej	P7S_UW	P7U_U
K_U14	samodzielnie wyszukiwać i selekcjonować źródła i informacje, analizować je i krytycznie oceniać, w tym z wykorzystaniem nowoczesnych technologii, w celu rozwiązania złożonego problemu bezpieczeństwa w cyberprzestrzeni	P7S_UW	P7U_U
K_U15	wykorzystywać posiadaną wiedzę z zakresu postępowania z osobą, która uległa wypadkowi	P7S_UW	P7U_U
K_U16	udzielić pierwszej pomocy w stanach zagrożenia życia w sytuacjach standardowych i nietypowych	P7S_UW	P7U_U
K_U17	samodzielnie korzystać z systemów i zbiorów bibliotecznych i w sposób właściwy pozyskiwać i dobierać źródła wykorzystywane w procesie przygotowania pracy pisemnej lub wystąpień ustnych, w tym w szczególności w zakresie bezpieczeństwa w cyberprzestrzeni	P7S_UW	P7U_U
K_U18	opracować prace pisemne i udzielić odpowiedzi ustnych stosownie do sformułowanego problemu w zakresie bezpieczeństwa w cyberprzestrzeni, w tym z wykorzystaniem specjalistycznej terminologii	P7S_UK	P7U_U
K_U19	stosować reguły komunikacji społecznej, zarówno w języku polskim, jak i w języku obcym oraz przy użyciu zaawansowanych technik komunikacyjnych porozumiewać się ze zróżnicowanymi kręgami odbiorców w sposób precyzyjny i spójny, wykorzystując w tym procesie specjalistyczną terminologię	P7S_UK	P7U_U
K_U20	posługiwać się językiem obcym na poziomie B2+ Europejskiego Systemu Opisu Kształcenia Językowego	P7S_UK	P7U_U
K_U21	prezentować własne, innowacyjne pomysły i argumenty, oceniać krytycznie określone stanowiska w kontekście wybranych poglądów, uznanych teorii i opinii innych autorów, prowadzić debatę z użyciem specjalistycznej terminologii	P7S_UK	P7U_U
K_U22	pracować indywidualnie, a także współdziałać i współpracować w grupie, w szczególności jako lider/kierownik zespołu oraz w strukturach instytucjonalnych działających na rzecz bezpieczeństwa w cyberprzestrzeni i zwalczania cyberprzestępczości, wykazując jednocześnie umiejętność planowania i organizacji tej pracy	P7S_UO	P7U_U
K_U23	samodzielnie planować własny rozwój i uczenie się przez całe życie, ukierunkowywać innych w tym zakresie oraz stale pogłębiać wiedzę z zakresu cyberbezpieczeństwa, w tym z wykorzystaniem różnych źródeł i nowoczesnych technologii	P7S_UU	P7U_U
w zakresie kompetencji społecznych – JEST GOTÓW DO:			
K_K01	uznawania znaczenia wiedzy w rozwiązywaniu złożonych problemów poznawczych i praktycznych w zakresie bezpieczeństwa w cyberprzestrzeni oraz ciągłego jej pogłębiania z wykorzystaniem różnych źródeł wiedzy i nowoczesnych technologii	P7S_KK	P7U_K
K_K02	krytycznej oceny posiadanej wiedzy, w tym zmiany opinii wobec racjonalnych argumentów, a także krytycznej oceny odbieranych treści i stosowanych rozwiązań wykorzystywanych w zakresie bezpieczeństwa w cyberprzestrzeni, w tym również w języku obcym	P7S_KK	P7U_K
K_K03	zasięgania opinii ekspertów w przypadku trudności z samodzielnym rozwiązaniem specjalistycznych, złożonych i nietypowych problemów w zakresie bezpieczeństwa w cyberprzestrzeni	P7S_KK	P7U_K
K_K04	wypełniania zobowiązań społecznych oraz aktywnego współdziałania w obszarze cyberbezpieczeństwa na rzecz jednostek, grup społecznych i innych podmiotów społecznych	P7S_KO	P7U_K
K_K05	inicjowania i współorganizowania zróżnicowanych aktywności na rzecz interesu publicznego, w szczególności w zakresie bezpieczeństwa w cyberprzestrzeni i działania w tym zakresie w sposób kreatywny	P7S_KO	P7U_K
K_K06	przestrzegania zasad bezpieczeństwa i higieny pracy, ochrony przeciwpożarowej oraz do udzielania pierwszej pomocy osobie, która uległa wypadkowi, w tym w miejscu pracy	P7S_KO	P7U_K
K_K07	odpowiedzialnego pełnienia roli zawodowej, w tym w szczególności przestrzegania i rozwijania zasad etyki zawodowej oraz dbałości o dorobek i tradycje zawodu	P7S_KR	P7U_K

3. Parametryczna charakterystyka kierunku studiów obejmująca:

Wyszczególnienie	Wielkość parametru wynikająca z programu studiów	
Parametry podstawowe		
Liczba semestrów	**4**	
Łączna liczba godzin zajęć w planie studiów	**1859 na studiach stacjonarnych 1626 na studiach niestacjonarnych**	
Łączna liczba punktów ECTS, konieczna dla uzyskania kwalifikacji odpowiadających poziomowi kształcenia	**120**	
Łączna liczba zajęć prowadzona na kierunku studiów przez nauczycieli zatrudnionych w uczelni jako podstawowym miejscu pracy	**44**	
Łączna liczba punktów ECTS, przypisana w planie studiów do zajęć z języka obcego	**6**	
Łączna liczba punktów ECTS, przypisana w planie studiów do praktyk studenckich	**39**	
Parametry szczegółowe	**Liczba punktów ECTS**	**Udział % w łącznej liczbie punktów ECTS dla całego programu studiów**
Punkty ECTS przypisane do dyscypliny naukowej:		
- wiodącej: **nauki o bezpieczeństwie**	**105,5**	**87,9 %**
- pozostałych: **nauki prawne**	**14,5**	**12,1 %**
Łączna liczba punktów ECTS, jaką student musi uzyskać w ramach zajęć prowadzonych z bezpośrednim udziałem nauczycieli akademickich lub innych osób prowadzących zajęcia	**74,3 na studiach stacjonarnych 65 na studiach niestacjonarnych**	**61,9 % na studiach stacjonarnych 54,2 % na studiach niestacjonarnych**
Łączna liczba punktów ECTS, przypisana w planie studiów do zajęć podlegających wyborowi w wymiarze nie mniejszym niż 30% ogólnej liczby punktów ECTS	**51 na studiach stacjonarnych i niestacjonarnych**	**42,5 %**
Łączna liczba punktów ECTS przypisana do zajęć kształtujących umiejętności praktyczne, w wymiarze większym niż 50% ogólnej liczy punktów ECTS – dotyczy kierunków studiów o profilu praktycznym	**79 na studiach stacjonarnych i niestacjonarnych**	**65,8 %**
Łączna liczba punktów ECTS przypisana do zajęć związanych z prowadzoną w uczelni działalnością naukową w dyscyplinie lub dyscyplinach, do których przyporządkowany jest kierunek studiów – dotyczy kierunków studiów o profilu ogólnoakademickim	**—**	**—**
Łączna liczba punktów ECTS przypisanych do zajęć przygotowujących studentów do prowadzenia działalności naukowej lub udział w tej działalności, w wymiarze większym niż 50% ogólnej liczby punktów ECTS – dotyczy kierunku studiów o profilu ogólnoakademickim	**—**	**—**

4. Plan studiów z zaznaczeniem przedmiotów podlegających wyborowi przez studenta.

WYDZIAŁ: BEZPIECZEŃSTWA I NAUK PRAWNYCH
POZIOM KSZTAŁCENIA: DRUGI STOPIEŃ
KIERUNEK: BEZPIECZEŃSTWO W CYBERPRZESTRZENI
SPECJALNOŚĆ:
PROFIL KSZTAŁCENIA: PRAKTYCZNY
FORMA STUDIÓW: STACJONARNE

I ROK 1 SEMESTR													
numer modułu	**nazwa modułu zajęć**	**typ***	**status***	**liczba jednostek lekcyjnych (godzin)**						**liczba punktów ECTS**		
				łącznie	wykład	ćwiczenia	zajęcia laboratoryjne	warsztaty praktyczne	forma zakończenia*	łącznie	BK*	PS*
1	Przysposobienie biblioteczno-informacyjne i informatyczne	**Og**	**O**	10	—	10	—	—	Z	1	0,4	0,6
2	BHP i pierwsza pomoc	**Og**	**O**	10	4	6	—	—	Z	1	0,4	0,6
3	Język angielski (I/II)	**Og**	**O**	30	—	30	—	—	Z	3	1,2	1,8
4	Ochrona danych osobowych przetwarzanych w cyberprzestrzeni	**P**	**O**	20	10	10	—	—	S	1	0,8	0,2
5	Zarządzanie projektami na rzecz bezpieczeństwa w cyberprzestrzeni	**P**	**O**	20	5	15	—	—	S	1	0,8	0,2
6	Socjologia Internetu	**P**	**O**	20	8	12	—	—	S	1	0,8	0,2
7	Zabezpieczenie dowodów w środowisku cyfrowym	**K**	**O**	45	15	—	30	—	E	3	1,8	1,2
8	Międzynarodowa współpraca w zwalczaniu cyberzagrożeń	**K**	**O**	40	15	25	—	—	S	2	1,6	0,4
9	Encyklopedia zagrożeń informatycznych	**K**	**O**	15	8	—	—	7	Z	1	0,6	0,4
10a	Język niemiecki (I/II)	**Og**	**F**	30	—	30	—	—	Z	3	1,2	1,8
10b	Język rosyjski (I/II)											
11	Praktyka zawodowa(I/III)	**K**	**F**	240	—	240	—	—	Z	13	9,6	3,4
ŁĄCZNIE W SEMESTRZE:				**480**	**65**	**378**	**30**	**7**	**—**	**30**	**19,2**	**10,8**

I ROK 2 SEMESTR												
numer modułu	nazwa modułu zajęć	typ*	status*	liczba jednostek lekcyjnych (godzin)						liczba punktów ECTS		
				łącznie	wykład	ćwiczenia	zajęcia laboratoryjne	warsztaty praktyczne	forma zakończenia*	łącznie	BK*	PS*
3	Język angielski (II/II)	**Og**	**O**	30	—	30	—	—	E	3	1,2	1,8
12	Seminarium dyplomowe (I/III)	**Og**	**O**	15	—	15	—	—	Z	3	0,6	2,4
13	Etiologia przestępczości internetowej	**P**	**O**	20	5	15	—	—	S	1	0,8	0,2
14	Społeczna odpowiedzialność służby zwalczania cyberprzestępczości	**P**	**O**	15	10	5	—	—	S	1	0,6	0,4
15	Analiza dowodów w środowisku cyfrowym	**K**	**O**	45	10	—	35	—	E	3	1,8	1,2
16	Testy penetracyjne IT	**K**	**O**	33	15	—	18	—	S	2	1,3	0,7
10a	Język niemiecki (II/II)	**Og**	**F**	30	—	30	—	—	E	3	1,2	1,8
10b	Język rosyjski (II/II)											
11	Praktyka zawodowa(II/III)	**K**	**F**	240	—	240	—	—	Z	13	9,6	3,4
17a	Cyberprzestępstwa motywowane uprzedzeniami w ujęciu prawnomiędzynarodowym	**K**	**F**	20	8	12	—	—	S	1	0,8	0,2
17b	Język w przestrzeni Internetu											
ŁĄCZNIE W SEMESTRZE:				**448**	**48**	**347**	**53**	**—**	**—**	**30**	**17,9**	**12,1**

II ROK 3 SEMESTR												
numer modułu	nazwa modułu zajęć	typ*	status*	liczba jednostek lekcyjnych (godzin)						liczba punktów ECTS		
				łącznie	wykład	ćwiczenia	zajęcia laboratoryjne	warsztaty praktyczne	forma zakończenia*	łącznie	BK*	PS*
12	Seminarium dyplomowe (II/III)	**Og**	**O**	15	—	15	—	—	Z	3	0,6	2,4
18	Wybrane czynności procesowo-kryminalistyczne	**P**	**O**	20	6	14	—	—	S	1	0,8	0,2
19	Organizacja i funkcjonowanie podmiotów właściwych w sprawach bezpieczeństwa i porządku publicznego	**P**	**O**	20	8	12	—	—	S	1	0,8	0,2
20	Odzyskiwanie i analiza danych z nośników cyfrowych	**K**	**O**	35	10	—	25	—	E	2	1,4	0,6
21	Kryptowaluty	**K**	**O**	30	14	—	—	16	S	2	1,2	0,8
22	Laboratorium statystyczne	**K**	**O**	30	2	—	28	—	E	2	1,2	0,8
23	Technologie chmur obliczeniowych	**K**	**O**	45	10	10	25	—	E	3	1,8	1,2
11	Praktyka zawodowa (III/III)	**K**	**F**	240	—	240	—	—	Z	13	9,6	3,4
24a	Współpraca międzynarodowa Policji w zakresie zapobiegania i zwalczania przestępczości	**P**	**F**	20	8	12	—	—	S	1	0,8	0,2
24b	Standardy międzynarodowe w zakresie zwalczania przestępczości zorganizowanej, ze szczególnym uwzględnieniem cyberprzestępczości.											
25a	Zarządzanie ryzykiem	**P**	**F**	20	8	12	—	—	S	1	0,8	0,2
25b	Zarządzanie strategiczne w instytucjach odpowiedzialnych za cyberbezpieczeństwo											
26a	Zarządzanie kryzysowe w administracji publicznej	**P**	**F**	20	8	12	—	—	S	1	0,8	0,2
26b	Ochrona infrastruktury krytycznej											
ŁĄCZNIE W SEMESTRZE:				**495**	**74**	**327**	**78**	**16**	**—**	**30**	**19,8**	**10,2**

II ROK 4 SEMESTR													
numer modułu	nazwa modułu zajęć	typ*	status*	liczba jednostek lekcyjnych (godzin)						liczba punktów ECTS		
				łącznie	wykład	ćwiczenia	zajęcia laboratoryjne	warsztaty praktyczne	forma zakończenia*	łącznie	BK*	PS*
12	Seminarium dyplomowe (III/III)	**Og**	**O**	30	—	30	—	—	Z	5	1,2	3,8
27	Postępowanie przedsądowe w sprawach o cyberprzestępstwa	**P**	**O**	30	—	—	—	30	S	2	1,2	0,8
28	Procedury decyzyjne w organizacjach	**P**	**O**	30	10	20	—	—	S	2	1,2	0,8
29	Darknet i anonimizacja w sieci	**K**	**O**	36	10	—	—	26	E	2	1,4	0,6
30	OSINT	**K**	**O**	30	12	—	—	18	S	2	1,2	0,8
31	Inżynieria społeczna	**K**	**O**	35	15	20	—	—	S	2	1,4	0,6
32	Udział biegłego w postępowaniu dowodowym w sprawach o przestępstwa komputerowe	**K**	**O**	45	15	—	—	30	E	3	1,8	1,2
33	Ataki i wykrywanie włamań w cyberprzestrzeni	**K**	**O**	35	15	—	20	—	S	2	1,4	0,6
34	Live Forensics	**K**	**O**	35	10	—	25	—	S	2	1,4	0,6
35	Analiza śledcza w sprawach związanych z cyberprzestępczością	**K**	**O**	40	10	—	30	—	S	2	1,6	0,4
36	Bezpieczeństwo aplikacji mobilnych	**K**	**O**	30	12	—	18	—	S	2	1,2	0,8
37	Polityka bezpieczeństwa informacji	**K**	**O**	30	12	—	18	—	S	2	1,2	0,8
38a	Nowoczesne technologie w służbie Policji – symulatory ruchu drogowego	**P**	**F**	30	5	6	—	19	S	2	1,2	0,8
38b	Nowoczesne technologie w służbie Policji – symulator działań Policji w sytuacjach kryzysowych				7	—		23				
ŁĄCZNIE W SEMESTRZE:				**436**	**126[a]** / **128[b]**	**76[a]** / **70[b]**	**111**	**123[a]** / **127[b]**	**—**	**30**	**17,4**	**12,6**

ECTS	semestr 1	semestr 2	semestr 3	semestr 4	RAZEM
Łączna liczba punktów ECTS	**30**	**30**	**30**	**30**	**120**
BK	**19,2**	**17,9**	**19,8**	**17,4**	**74,3**
PS	**10,8**	**12,1**	**10,2**	**12,6**	**45,7**

LEGENDA:
- TYP: Og - ogólny **P -** podstawowy; **K -** kierunkowy;
STATUS: O – obowiązkowy; **F -** fakultatywny (do wyboru)
- FORMA ZAKOŃCZENIA: E – egzamin; **S –** zaliczenie z oceną; **Z –** zaliczenie
- LICZBA PUNKTÓW ECTS: BK - liczba punktów ECTS za bezpośredni kontakt z nauczycielem; **PS -** liczba punktów ECTS za pracę samodzielną

WYDZIAŁ: BEZPIECZEŃSTWA I NAUK PRAWNYCH
POZIOM KSZTAŁCENIA: DRUGI STOPIEŃ
KIERUNEK: BEZPIECZEŃSTWO W CYBERPRZESTRZENI
SPECJALNOŚĆ:
PROFIL KSZTAŁCENIA: PRAKTYCZNY
FORMA STUDIÓW: NIESTACJONARNE

I ROK 1 SEMESTR												
numer modułu	**nazwa modułu zajęć**	**typ***	**status***	**liczba jednostek lekcyjnych (godzin)**						**liczba punktów ECTS**		
				łącznie	wykład	ćwiczenia	zajęcia laboratoryjne	warsztaty praktyczne	forma zakończenia*	łącznie	BK*	PS*
1	Przysposobienie biblioteczno-informacyjne i informatyczne	**Og**	**O**	8	—	8	—	—	Z	1	0,3	0,7
2	BHP i pierwsza pomoc	**Og**	**O**	10	4	6	—	—	Z	1	0,4	0,6
3	Język angielski (I/II)	**Og**	**O**	25	—	25	—	—	Z	3	1	2
4	Ochrona danych osobowych przetwarzanych w cyberprzestrzeni	**P**	**O**	17	7	10	—	—	S	1	0,7	0,3
5	Zarządzanie projektami na rzecz bezpieczeństwa w cyberprzestrzeni	**P**	**O**	15	5	10	—	—	S	1	0,6	0,4
6	Socjologia Internetu	**P**	**O**	14	8	6	—	—	S	1	0,6	0,4
7	Zabezpieczenie dowodów w środowisku cyfrowym	**K**	**O**	30	14	—	16	—	E	3	1,2	1,8
8	Międzynarodowa współpraca w zwalczaniu cyberzagrożeń	**K**	**O**	30	10	20	—	—	S	2	1,2	0,8
9	Encyklopedia zagrożeń informatycznych	**K**	**O**	10	4	—	—	6	Z	1	0,4	0,6
10a	Język niemiecki (I/II)	**Og**	**F**	25	—	25	—	—	Z	3	1	2
10b	Język rosyjski (I/II)											
11	Praktyka zawodowa (I/III)	**K**	**F**	240	—	240	—	—	Z	13	9,6	3,4
ŁĄCZNIE W SEMESTRZE:				**424**	**52**	**350**	**16**	**6**	**—**	**30**	**17**	**13**

I ROK 2 SEMESTR												
numer modułu	nazwa modułu zajęć	typ*	status*	liczba jednostek lekcyjnych (godzin)						liczba punktów ECTS		
				łącznie	wykład	ćwiczenia	zajęcia laboratoryjne	warsztaty praktyczne	forma zakończenia*	łącznie	BK*	PS*
3	Język angielski (II/II)	**Og**	**O**	25	—	25	—	—	E	3	1	2
12	Seminarium dyplomowe (I/III)	**Og**	**O**	15	—	15	—	—	Z	3	0,6	2,4
13	Etiologia przestępczości internetowej	**P**	**O**	15	5	10	—	—	S	1	0,6	0,4
14	Społeczna odpowiedzialność służby zwalczania cyberprzestępczości	**P**	**O**	15	10	5	—	—	S	1	0,6	0,4
15	Analiza dowodów w środowisku cyfrowym	**K**	**O**	35	9	—	26	—	E	3	1,4	1,6
16	Testy penetracyjne IT	**K**	**O**	27	10	—	17	—	S	2	1,1	0,9
10a	Język niemiecki (II/II)	**Og**	**F**	25	—	25	—	—	E	3	1	2
10b	Język rosyjski (II/II)											
11	Praktyka zawodowa (II/III)	**K**	**F**	240	—	240	—	—	Z	13	9,6	3,4
17a	Cyberprzestępstwa motywowane uprzedzeniami w ujęciu prawnomiędzynarodowym	**P**	**F**	15	5	10	—	—	S	1	0,6	0,4
17b	Język w przestrzeni Internetu											
ŁĄCZNIE W SEMESTRZE:				**412**	**39**	**330**	**43**	**—**	**—**	**30**	**16,5**	**13,5**

II ROK 3 SEMESTR												
numer modułu	nazwa modułu zajęć	typ*	status*	liczba jednostek lekcyjnych (godzin)						liczba punktów ECTS		
				łącznie	wykład	ćwiczenia	zajęcia laboratoryjne	warsztaty praktyczne	forma zakończenia*	łącznie	BK*	PS*
12	Seminarium dyplomowe (II/III)	**Og**	**O**	15	—	15	—	—	Z	3	0,6	2,4
18	Wybrane czynności procesowo-kryminalistyczne	**P**	**O**	20	6	14	—	—	S	1	0,8	0,2
19	Organizacja i funkcjonowanie podmiotów właściwych w sprawach bezpieczeństwa i porządku publicznego	**P**	**O**	15	5	10	—	—	S	1	0,6	0,4
20	Odzyskiwanie i analiza danych z nośników cyfrowych	**K**	**O**	26	8	—	18	—	E	2	1	1
21	Kryptowaluty	**K**	**O**	20	10	—	—	10	S	2	0,8	1,2
22	Laboratorium statystyczne	**K**	**O**	20	2	—	18	—	E	2	0,8	1,2
23	Technologie chmur obliczeniowych	**K**	**O**	35	8	8	19	—	E	3	1,4	1,6
11	Praktyka zawodowa (III/III)	**K**	**F**	240	—	240	—	—	Z	13	9,6	3,4
24a	Współpraca międzynarodowa Policji w zakresie zapobiegania i zwalczania przestępczości	**P**	**F**	20	8	12	—	—	S	1	0,8	0,2
24b	Standardy międzynarodowe w zakresie zwalczania przestępczości zorganizowanej											
25a	Zarządzanie ryzykiem	**P**	**F**	20	8	12	—	—	S	1	0,8	0,2
25b	Zarządzanie strategiczne w instytucjach odpowiedzialnych za cyberbezpieczeństwo											
26a	Zarządzanie kryzysowe w administracji publicznej	**P**	**F**	20	8	12	—	—	S	1	0,8	0,2
26b	Ochrona infrastruktury krytycznej											
ŁĄCZNIE W SEMESTRZE:				**451**	**63**	**323**	**55**	**10**	**—**	**30**	**18**	**12**

II ROK 4 SEMESTR												
numer modułu	nazwa modułu zajęć	typ*	status*	liczba jednostek lekcyjnych (godzin)						liczba punktów ECTS		
				łącznie	wykład	ćwiczenia	zajęcia laboratoryjne	warsztaty praktyczne	forma zakończenia*	łącznie	BK*	PS*
16	Seminarium dyplomowe (III/III)	**Og**	**O**	30	—	30	—	—	Z	5	1,2	3,8
27	Postępowanie przedsądowe w sprawach o cyberprzestępstwa w ujęciu praktycznym	**P**	**O**	20	—	—	—	20	S	2	0,8	1,2
28	Procedury decyzyjne w organizacjach	**P**	**O**	20	5	15	—	—	S	2	0,8	1,2
29	Darknet i anonimizacja w sieci	**K**	**O**	22	6	—	—	16	E	2	0,9	1,1
30	OSINT	**K**	**O**	20	9	—	—	11	S	2	0,8	1,2
31	Inżynieria społeczna	**K**	**O**	26	12	14	—	—	S	2	1	1
32	Udział biegłego w postępowaniu dowodowym w sprawach o przestępstwa komputerowe	**K**	**O**	35	11	—	—	24	E	3	1,4	1,6
33	Ataki i wykrywanie włamań w cyberprzestrzeni	**K**	**O**	26	10	—	16	—	S	2	1	1
34	Live Forensics	**K**	**O**	25	8	—	17	—	S	2	1	1
35	Analiza śledcza w sprawach związanych z cyberprzestępczością	**K**	**O**	35	10	—	25	—	S	2	1,4	0,6
36	Bezpieczeństwo aplikacji mobilnych	**K**	**O**	25	11	—	14	—	S	2	1	1
37	Polityka bezpieczeństwa informacji	**K**	**O**	25	11	—	14	—	S	2	1	1
38a	Nowoczesne technologie w służbie Policji – symulatory ruchu drogowego	**P**	**F**	30	5	6	—	19	S	2	1,2	0,8
38b	Nowoczesne technologie w służbie Policji – symulator działań Policji w sytuacjach kryzysowych				7	—		23				
ŁĄCZNIE W SEMESTRZE:				**339**	**98[a]**	**65[a]**	**86**	**90[a]**	**—**	**30**	**13,5**	**16,5**
					100[b]	**59[b]**		**94[b]**				

ECTS	semestr 1	semestr 2	semestr 3	semestr 4	RAZEM
Łączna liczba punktów ECTS	**30**	**30**	**30**	**30**	**120**
BK	**17**	**16,5**	**18**	**13,5**	**65**
PS	**13**	**13,5**	**12**	**16,5**	**55**

LEGENDA:
- TYP: Og - ogólny **P -** podstawowy; **K -** kierunkowy;
- STATUS: O – obowiązkowy; **F -** fakultatywny (do wyboru)
- FORMA ZAKOŃCZENIA: E – egzamin; **S –** zaliczenie z oceną; **Z –** zaliczenie
- LICZBA PUNKTÓW ECTS: BK - liczba punktów ECTS za bezpośredni kontakt z nauczycielem; **PS -** liczba punktów ECTS za pracę samodzielną

Nazwa przedmiotu: Przysposobienie biblioteczno-informacyjne i informatyczne				
Numer przedmiotu: 1	**Punkty ECTS:** 1	**Profil kształcenia:** praktyczny	**Dziedzina nauki/dyscyplina naukowa:** nauki społeczne/nauki o bezpieczeństwie	**Język wykładowy:** polski

Efekty uczenia się		**Symbol kierunkowego efektu uczenia się**	**Symbol składnika opisu charakterystyki drugiego stopnia efektów uczenia się dla kwalifikacji na poziomach 6-7 PRK**	**Treści programowe**
w zakresie wiedzy				
EU_1	Zna i rozumie strukturę biblioteki oraz zadania poszczególnych oddziałów.	K_W19	P7S_WK	Ćw1
EU_2	Zna i rozumie systemy biblioteczne i informatyczne dostępne dla studenta.	K_W19	P7S_WK	Ćw2
w zakresie umiejętności				
EU_3	Potrafi samodzielnie korzystać z elektronicznych systemów bibliotecznych i informatycznych oraz wyszukiwać w bazach bibliotecznych i informatycznych źródła w zakresie bezpieczeństwa w cyberprzestrzeni.	K_U17	P7S_UW	Ćw2-4
EU_4	Potrafi samodzielnie posługiwać się technologiami bibliotecznymi i informatycznymi.	K_U14 K_U17	P7S_UW	Ćw2-4
EU_5	Potrafi zdefiniować problem w dostępie do informacji.	K_U14	P7S_UW	Ćw2-4
EU_6	Potrafi samodzielnie korzystać z zasobów biblioteki oraz z katalogów online innych bibliotek akademickich.	K_U17	P7S_UW	Ćw2-4
EU_7	Potrafi samodzielnie korzystać ze zbiorów bibliotek w procesie przygotowania pracy pisemnej lub wystąpień ustnych w zakresie bezpieczeństwa w cyberprzestrzeni.	K_U17	P7S_UW	Ćw2-4
w zakresie kompetencji społecznych				
EU_8	Jest gotów do uznawania znaczenia wiedzy w rozwiązywaniu problemów poznawczych i praktycznych w zakresie bezpieczeństwa w cyberprzestrzeni.	K_K01	P7S_KK	Ćw1-4

Lp.	**Temat**	**Tezy**	**Forma studiów:**									
			stacjonarna					**Niestacjonarna**				
			Łączna liczba godzin: 10					**Łączna liczba godzin: 8**				
			Wykłady	**Ćwiczenia**	**Zajęcia laboratoryjne**	**Warsztaty praktyczne**	**Razem**	**Wykłady**	**Ćwiczenia**	**Zajęcia laboratoryjne**	**Warsztaty praktyczne**	**Razem**
1.	Struktura organizacyjna biblioteki oraz charakter, lokalizacja i zasady korzystania ze zbiorów	1. Oddziały Biblioteki. 2. Struktura tematyczna i formalna zbiorów. 3. Regulamin korzystania ze zbiorów Biblioteki.	-	2	-	-	**2**	-	2	-	-	**2**

2.	Korzystanie z katalogu komputerowego ALEPH i wybrane cyfrowe źródla informacji	1. System biblioteczny ALEPH. 2. Federacja Bibliotek Cyfrowych. 3. Repozytoria CeON i RepOD. 4. Bazy Biblioteki Narodowej POLONA i ACADEMICA.	-	3	-	-	**3**	-	2	-	-	**2**
3.	Zapoznanie się ze strukturą informatyczną Uczelni w zakresie potrzeb studenta	1. Strony internetowe. 2. Strona intranetowa. 3. System dziekanatowy Bazus.	-	2	-	-	**2**	-	2	-	-	**2**
4.	Wybrane Systemy wspomagające proces edukacyjny	1. Uwarunkowania prawne wykorzystania metod i technik kształcenia na odległość. 2. Edukacja na odległość, podstawowe zagadnienia. 3. Możliwości wykorzystania systemów informatycznych wspomagających proces nauczania, m.in. Kampus, CISCO WEBEX MEETINGSWebEX, MS Teams.	-	3	-	-	**3**	-	2	-	-	**2**
		Razem:	-	**10**	-	-	**10**	-	**8**	-	-	**8**

Forma zakończenia (Z)	**Zaliczenie**												
Efekty uczenia się	**Metody weryfikacji osiągania efektów uczenia się**												
	Egzamin pisemny	Egzamin ustny	Sprawdzian pisemny	Odpowiedź ustna	Referat	Prezentacja indywidualna	Prezentacja grupowa	Projekt indywidualny	Projekt grupowy	Samodzielna realizacja zadania praktycznego	Zespołowa realizacja zadania praktycznego	Aktywność na zajęciach	Test sprawności fizycznej
EU_1										x		x	
EU_2										x		x	
EU_3										x		x	
EU_4										x		x	
EU_5										x		x	
EU_6										x		x	
EU_7										x		x	
EU_8										x		x	

Nazwa przedmiotu: BHP i pierwsza pomoc				
Numer przedmiotu: 2	**Punkty ECTS:** 1	**Profil kształcenia:** praktyczny	**Dziedzina nauki/dyscyplina naukowa:** nauki społeczne/nauki o bezpieczeństwie	**Język wykładowy:** polski

Efekty uczenia się		**Symbol kierunkowego efektu uczenia się**	**Symbol składnika opisu charakterystyki drugiego stopnia efektów uczenia się dla kwalifikacji na poziomach 6-7 PRK**	**Treści programowe**
w zakresie wiedzy				
EU_1	Zna i rozumie potrzebę i zasady niesienia pomocy osobom, które znalazły się w stanie nagłego zagrożenia zdrowotnego spowodowanym wypadkiem lub innym zdarzeniem w miejscu pracy.	K_W18	P7S_WK	W1
EU_2	Zna i rozumie algorytmy postępowania z osobą znajdująca się w sytuacji zagrożenia życia lub zdrowia w ramach udzielania pierwszej pomocy.	K_W18	P7S_WK	W1-2
EU_3	Zna i rozumie zasady ochrony przeciwpożarowej, postępowanie w przypadku pożaru oraz sposoby zapobiegania pożarom.	K_W18	P7S_WK	W3
w zakresie umiejętności				
EU_4	Potrafi wykorzystywać posiadaną wiedzę z zakresu postępowania z osobą, która uległa wypadkowi.	K_U15	P7S_UW	Ćw4
EU_5	Potrafi udzielić pierwszej pomocy w sytuacjach standardowych i nietypowych.	K_U16	P7S_UW	Ćw4
w zakresie kompetencji społecznych				
EU_6	Jest gotów do niesienia pomocy osobie, która uległa wypadkowi w miejscu pracy.	K_K06	P7S_KO	Ćw4
EU_7	Jest gotów do wypełnienia obowiązków społecznych związanych z udzielaniem pierwszej pomocy.	K_K06	P7S_KO	Ćw4
EU_8	Jest gotów do odpowiedzialnego pełnienia roli lidera w zespole udzielającym pierwszej pomocy.	K_K07	P7S_KR	Ćw4

Lp.	**Temat**	**Tezy**	**Forma studiów:**									
			stacjonarna					**niestacjonarna**				
			Łączna liczba godzin: 10					**Łączna liczba godzin: 10**				
			Wykłady	**Ćwiczenia**	**Zajęcia laboratoryjne**	**Warsztaty praktyczne**	**Razem**	**Wykłady**	**Ćwiczenia**	**Zajęcia laboratoryjne**	**Warsztaty praktyczne**	**Razem**
1.	Wybrane zagadnienia z zakresu prawa pracy oraz podstawowe zasady bezpieczeństwa i higieny pracy w Uczelni	1. Wybrane zagadnienia z prawa pracy. 2. Obowiązki prawne w zakresie udzielania pierwszej pomocy. 3. Podstawowe zasady bezpieczeństwa i higieny pracy obowiązujące w Uczelni.	1	-	-	-	**1**	1	-	-	-	**1**

2.	Postępowanie w razie zaistnienia wypadku studenta w Uczelni	1. Definicja wypadku. 2. Postępowanie w razie zaistnienia wypadku w Uczelni. 3. Okoliczności i przyczyny wypadków, do których może dojść na Uczelni. 4. Tryb dochodzenia roszczeń odszkodowawczych.	2	-	-	-	**2**	2	-	-	-	**2**
3.	Identyfikacja czynników szkodliwych lub uciążliwych dla zdrowia oraz ochrona przeciwpożarowa	1. Czynniki niebezpieczne, szkodliwe i uciążliwe oraz środki ochrony indywidualnej przysługujące studentom w zależności od specyfiki i rodzaju zajęć. 2. Podstawowe zasady ochrony przeciwpożarowej, postępowanie w przypadku pożaru oraz sposoby zapobiegania pożarom. 3. Prawidłowe użycie sprzętu gaśniczego w sytuacji pożaru. 4. Organizacja i warunki ewakuacji.	1	-	-	-	**1**	1	-	-	-	**1**
4.	Zasady udzielania pierwszej pomocy	1. Udzielanie pierwszej pomocy w sytuacjach standardowych i nietypowych. 2. Ocena wstępna poszkodowanego po wypadku. 3. Wzywanie służb ratowniczych. 4. Stosowanie wybranych ratowniczych pozycji ułożeniowych. 5. Wybrane stany zagrożenia życia lub zdrowia. 6. Udzielanie pierwszej pomocy pojedynczo i w zespole.	-	6	-	-	**6**	-	6	-	-	**6**
		Razem:	**4**	**6**	-	-	**10**	**4**	**6**	-	-	**10**

Forma zakończenia (Z)	**Zaliczenie**												
Efekty uczenia się	**Metody weryfikacji osiągania efektów uczenia się**												
	Egzamin pisemny	Egzamin ustny	Sprawdzian pisemny	Odpowiedź ustna	Referat	Prezentacja indywidualna	Prezentacja grupowa	Projekt indywidualny	Projekt grupowy	Samodzielna realizacja zadania praktycznego	Zespołowa realizacja zadania praktycznego	Aktywność na zajęciach	Test sprawności fizycznej
EU_1			x										
EU_2			x										
EU_3			x										
EU_4										x			
EU_5										x			
EU_6										x			
EU_7											x		
EU_8											x		

Nazwa przedmiotu: Język angielski				
Numer przedmiotu: 3	**Punkty ECTS:** 6	**Profil kształcenia:** praktyczny	**Dziedzina nauki/dyscyplina naukowa:** nauki społeczne/ nauki o bezpieczeństwie	**Język wykładowy:** polski/angielski

	Efekty uczenia się	**Symbol kierunkowego efektu uczenia się**	**Symbol składnika opisu charakterystyki drugiego stopnia efektów uczenia się dla kwalifikacji na poziomach 6-7 PRK**	**Treści programowe**
w zakresie wiedzy				
EU_1	Zna i rozumie zasady skutecznej komunikacji w języku polskim i angielskim oraz ich praktyczne zastosowanie w działalności zawodowej.	K_W01 K_W17	P7S_WG P7S_WK	Ćw1
w zakresie umiejętności				
EU_2	Stosuje podczas wypowiedzi ustnych i pisemnych gramatykę języka angielskiego, leksykę specjalistyczną, w tym dotyczącą pracy Policji ze szczególnym uwzględnieniem bezpieczeństwa w cyberprzestrzeni.	K_U01 K_U18 K_U20	P7S_UW P7S_UK	Ćw1
EU_3	Rozumie wypowiedzi i programy informacyjne w języku angielskim dotyczące aktualnych i specjalistycznych tematów, w szczególności związanych z pracą Policji oraz bezpieczeństwem w cyberprzestrzeni.	K_U02 K_U20	P7S_UW P7S_UK	Ćw1
EU_4	Rozumie artykuły i teksty opisujące problematykę współczesną, a także zawierającą leksykę specjalistyczną dotyczącą pracy Policji oraz cyberbezpieczeństwa.	K_U20	P7S_UK	Ćw1
EU_5	Przygotowuje typowe prace pisemne w języku angielskim na specjalistyczne tematy związane z bieżącymi wydarzeniami, pracą Policji, w szczególności w zakresie zwalczania cyberprzestępczości.	K_U18 K_U20	P7S_UK	Ćw1
EU_6	Porozumiewa się swobodnie i spontanicznie w języku angielskim w taki sposób, że interakcje ze zróżnicowanymi kręgami odbiorców, w tym rodzimymi użytkownikami języka angielskiego stają się naturalne, przedstawia swoje poglądy i potrafi je bronić.	K_U19 K_U20	P7S_UK	Ćw1
EU_7	Uczestniczy czynnie w rozmowach, wypowiada się jasno i szczegółowo na tematy specjalistyczne, dotyczące różnych wydarzeń, swoich zainteresowań i pracy Policji, w szczególności w zakresie zwalczania cyberprzestępczości.	K_U19 K_U20 K_U21	P7S_UK	Ćw1
w zakresie kompetencji społecznych				
EU_8	Jest gotów do krytycznej oceny posiadanej wiedzy z języka angielskiego.	K_K02	P7S_KK	Ćw1

Lp.	**Temat**	**Tezy**	**Forma studiów:**									
			Stacjonarna					**niestacjonarna**				
			Łączna liczba godzin: 60					**Łączna liczba godzin: 50**				
			Wykłady	**Ćwiczenia**	**Zajęcia laboratoryjne**	**Warsztaty praktyczne**	**Razem**	**Wykłady**	**Ćwiczenia**	**Zajęcia laboratoryjne**	**Warsztaty praktyczne**	**Razem**
1.	Język ogólny i specjalistyczny	1. Człowiek i środowisko społeczne.	-	10	-	-	**10**	-	9	-	-	**9**
		2. Praca zawodowa.	-	10	-	-	**10**	-	8	-	-	**8**
		3. Problemy współczesnego świata.	-	10	-	-	**10**	-	8	-	-	**8**

		4. Sprawca i ofiara przestępstwa w sieci cybernetycznej.	-	10	-	-	**10**	-	9	-	-	**9**
		5. Zapobieganie i zwalczanie przestępczości w sieci.	-	10	-	-	**10**	-	8	-	-	**8**
		6. Studia przypadków.	-	10	-	-	**10**	-	8	-	-	**8**
		Razem:	-	**60**	-	-	**60**	-	**50**	-	-	**50**

Forma zakończenia (E)	**Egzamin**												
Efekty uczenia się	**Metody weryfikacji osiągania efektów uczenia się**												
	Egzamin pisemny	Egzamin ustny	Sprawdzian pisemny	Odpowiedź ustna	Referat	Prezentacja indywidualna	Prezentacja grupowa	Projekt indywidualny	Projekt grupowy	Samodzielna realizacja zdania praktycznego	Zespołowa realizacja zadania praktycznego	Aktywność na zajęciach	Test sprawności fizycznej
EU_1		x		x		x			x			x	
EU_2		x	x	x		x			x			x	
EU_3			x	x		x			x			x	
EU_4			x			x			x			x	
EU_5			x									x	
EU_6		x		x		x			x			x	
EU_7		x		x		x			x			x	
EU_8		x		x		x			x			x	

Nazwa przedmiotu: Ochrona danych osobowych przetwarzanych w cyberprzestrzeni				
Numer przedmiotu: 4	**Punkty ECTS:** 1	**Profil kształcenia:** praktyczny	**Dziedzina nauki/dyscyplina naukowa:** nauki społeczne/nauki o bezpieczeństwie	**Język wykładowy:** polski

Efekty uczenia się		**Symbol kierunkowego efektu uczenia się**	**Symbol składnika opisu charakterystyki drugiego stopnia efektów uczenia się dla kwalifikacji na poziomach 6-7 PRK**	**Treści programowe**
w zakresie wiedzy				
EU_1	Zna i rozumie wybrane fakty i zjawiska oraz dotyczące ich metody i teorie wyjaśniające złożone zależności między nimi, stanowiące zaawansowaną wiedzę z zakresu danych osobowych i ochrony informacji niejawnych.	K_W02 K_W09	P7S_WG	W1-3 Ćw1-3
EU_2	Zna i rozumie uwarunkowania prawne i etyczne z zakresu danych osobowych przetwarzanych w Internecie i zabezpieczenia informacji niejawnych oraz ich praktyczne zastosowanie w działalności zawodowej.	K_W07 K_W09 K_W16	P7S_WG P7S_WK	W1-3 Ćw1-3
w zakresie umiejętności				
EU_3	Potrafi formułować i rozwiązywać typowe problemy z zakresu przetwarzania danych osobowych w Internecie i zabezpieczenia informacji niejawnych.	K_U02 K_U11	P7S_UW	Ćw1-3
EU_4	Potrafi przedstawiać i oceniać różne opinie i stanowiska na temat przetwarzania danych osobowych w Internecie i zastosowania systemów ochrony informacji niejawnych oraz dyskutować o nich ze zróżnicowanymi kręgami odbiorców.	K_U19 K_U21	P7S_UK	Ćw1-3
w zakresie kompetencji społecznych				
EU_5	Jest gotów do krytycznej oceny posiadanej wiedzy i odbieranych treści w rozwiązywaniu problemów z zakresu danych osobowych przetwarzanych w Internecie i zabezpieczenia informacji niejawnych oraz zasięgania opinii ekspertów w przypadku trudności z samodzielnym rozwiązaniem problemu.	K_K02 K_K03	P7S_KK	W1-3 Ćw1-3

Lp.	**Temat**	**Tezy**	**Forma studiów:**									
			stacjonarna					**niestacjonarna**				
			Łączna liczba godzin: 20					**Łączna liczba godzin: 17**				
			Wykłady	**Ćwiczenia**	**Zajęcia laboratoryjne**	**Warsztaty praktyczne**	**Razem**	**Wykłady**	**Ćwiczenia**	**Zajęcia laboratoryjne**	**Warsztaty praktyczne**	**Razem**
1.	Prawo do ochrony danych osobowych	1. Zakres przedmiotowy i podmiotowy. 2. Zasady przetwarzania danych osobowych.	2	2	-	-	**4**	2	2	-	-	**4**
2.	Przetwarzanie danych osobowych z wykorzystaniem Internetu	1. Prawa osób, której dane dotyczą. 2. Ograniczenia w przetwarzaniu danych osobowych w Internecie. 3. Ochrona danych osobowych w Internecie. 4. Rola IOD, Administratora.	5	5	-	-	**10**	3	5	-	-	**8**

3.	Bezpieczeństwo teleinformatyczne	1. Organizacja ochrony systemów teleinformatycznych informacji niejawnych. 2. Akredytacja bezpieczeństwa systemów teleinformatycznych informacji niejawnych krajowych i międzynarodowych. 3. Certyfikacja środków ochrony elektromagnetycznej urządzeń służących od ochrony informacji niejawnych.	3	3	-	-	**6**	2	3	-	-	**5**
		Razem:	**10**	**10**	-	-	**20**	**7**	**10**	-	-	**17**

Forma zakończenia (S)	**Zaliczenie z oceną**												
Efekty uczenia się	**Metody weryfikacji osiągania efektów uczenia się**												
	Egzamin pisemny	Egzamin ustny	Sprawdzian pisemny	Odpowiedź ustna	Referat	Prezentacja indywidualna	Prezentacja grupowa	Projekt indywidualny	Projekt grupowy	Samodzielna realizacja zdania praktycznego	Zespołowa realizacja zadania praktycznego	Aktywność na zajęciach	Test sprawności fizycznej
EU_1			x	x	x	x	x			x	x	x	
EU_2			x	x	x	x	x			x	x	x	
EU_3			x	x	x	x	x			x	x	x	
EU_4			x	x	x	x	x			x	x	x	
EU_5				x	x	x	x			x	x	x	

Nazwa przedmiotu: Zarządzanie projektami na rzecz bezpieczeństwa w cyberprzestrzeni				
Numer przedmiotu: 5	**Punkty ECTS:** 1	**Profil kształcenia:** praktyczny	**Dziedzina nauki/dyscyplina naukowa:** nauki społeczne/ nauki o bezpieczeństwie	**Język wykładowy:** polski

	Efekty uczenia się	**Symbol kierunkowego efektu uczenia się**	**Symbol składnika opisu charakterystyki drugiego stopnia efektów uczenia się dla kwalifikacji na poziomach 6-7 PRK**	**Treści programowe**
w zakresie wiedzy				
EU_1	Zna i rozumie specjalistyczne pojęcia z zakresu zarządzania projektami, w szczególności na rzecz bezpieczeństwa w cyberprzestrzeni.	K_W01 K_W02	P7S_WG	W1-4 Ćw2-4
EU_2	Zna zróżnicowane metody, techniki i narzędzia stosowane w zarządzaniu projektami, w tym na rzecz bezpieczeństwa w cyberprzestrzeni i zna ich praktyczne zastosowanie w działalności zawodowej.	K_W04	P7S_WG	W2-4 Ćw2-4
w zakresie umiejętności				
EU_3	Potrafi przygotować typowy wniosek aplikacyjny projektu, w szczególności na rzecz bezpieczeństwa w cyberprzestrzeni.	K_U14 K_U18	P7S_UW P7S_UK	Ćw2-4
EU_4	Potrafi zidentyfikować nieprawidłowości we wniosku aplikacyjnym i w zarządzaniu projektem, w szczególności na rzecz bezpieczeństwa w cyberprzestrzeni.	K_U18	P7S_UK	Ćw2
EU_5	Potrafi wykonywać zadania w zespole projektowym, zarówno jako kierownik/menager/lider/wykonawca zespołu, typowe dla działalności zawodowej.	K_U22	P7S_KO	Ćw3
EU_6	Potrafi w sposób prawidłowy dokonać analizy potrzeb w zakresie pozyskiwania funduszy pomocowych na wybrany projekt, w szczególności na rzecz bezpieczeństwa w cyberprzestrzeni.	K_U01 K_U02 K_U18	P7S_UW P7S_UK	Ćw4
w zakresie kompetencji społecznych				
EU_7	Jest gotów do inicjowania działań na rzecz bezpieczeństwa w cyberprzestrzeni oraz myślenia i działania w sposób przedsiębiorczy.	K_K05	P7S_KO	Ćw2-4
EU_8	Jest gotowy do pogłębionej analizy i krytycznej oceny posiadanej wiedzy z zakresu zarządzania projektami na rzecz bezpieczeństwa w cyberprzestrzeni oraz zasięgania opinii ekspertów w przypadku trudności z samodzielnym rozwiązaniem problemu praktycznego.	K_K02 K_K03	P7S_KK	W1-4 Ćw2-4

Lp.	**Temat**	**Tezy**	**Forma studiów:**									
			stacjonarna					**niestacjonarna**				
			Łączna liczba godzin: 20					**Łączna liczba godzin: 15**				
			Wykłady	**Ćwiczenia**	**Zajęcia laboratoryjne**	**Warsztaty praktyczne**	**Razem**	**Wykłady**	**Ćwiczenia**	**Zajęcia laboratoryjne**	**Warsztaty praktyczne**	**Razem**
1.	Istota projektu	1. Pojęcie projektu. 2. Projekt a program. 3. Rodzaje projektów. 4. Źródła i możliwości finansowania/współfinansowania projektów.	1	-	-	-	**1**	1	-	-	-	**1**

2.	Zarządzanie projektami	1. Fisza/karta startowa projektu. Inicjacja i planowanie działań projektowych. 2. Etapy realizacji projektu w tym metody, narzędzia i techniki zarządzania projektami. 3. Zamknięcie projektu. 4. Audyt i kontrola projektu. 5. Ryzyka w projekcie. 6. Nieprawidłowości w zarządzaniu projektami.	2	4	-	-	**6**	2	4	-	-	**6**
3.	Specyfika menagera/kierownika/lidera projektu oraz wykonawców	1. Budowa zespołu zarządzającego projektem i jego zadania. 2. Zadania i odpowiedzialność menagera/kierownika/lidera projektu i wykonawców. 3. Ryzyka w kierowaniu projektami. 4. Archiwizacja dokumentacji projektowej.	1	5	-	-	**6**	1	2	-	-	**3**
4.	Aplikowanie o środki pomocowe na realizacje projektów	1. Analiza potrzeb projektowych. 2. Analiza i omówienie wybranej dokumentacji konkursowej związanej z aplikowaniem o środki pomocowe na realizacje projektów. 3. Opracowanie wniosku aplikacyjnego. 4. Działania wdrożeniowe projektu – rola trwałości projektu po jego zakończeniu.	1	6	-	-	**7**	1	4	-	-	**5**
		Razem:	**5**	**15**	-	-	**20**	**5**	**10**	-	-	**15**

Forma zakończenia (S)	**Zaliczenie z oceną**												
Efekty uczenia się	**Metody weryfikacji osiągania efektów uczenia się**												
	Egzamin pisemny	Egzamin ustny	Sprawdzian pisemny	Odpowiedź ustna	Referat	Prezentacja indywidualna	Prezentacja grupowa	Projekt indywidualny	Projekt grupowy	Samodzielna realizacja zdania praktycznego	Zespołowa realizacja zadania praktycznego	Aktywność na zajęciach	Test sprawności fizycznej
EU_1			x	x								x	
EU_2			x	x							x	x	
EU_3			x								x	x	
EU_4			x								x	x	
EU_5			x								x	x	
EU_6			x								x	x	
EU_7												x	
EU_8												x	

Nazwa przedmiotu: Socjologia Internetu				
Numer przedmiotu: 6	**Punkty ECTS:** 1	**Profil kształcenia:** praktyczny	**Dziedzina nauki/dyscyplina naukowa:** nauki społeczne/ nauki o bezpieczeństwie	**Język wykładowy:** polski

Efekty uczenia się		**Symbol kierunkowego efektu uczenia się**	**Symbol składnika opisu charakterystyki drugiego stopnia efektów uczenia się dla kwalifikacji na poziomach 6-7 PRK**	**Treści programowe**
w zakresie wiedzy				
EU_1	Zna i rozumie wybrane zagadnienia, stanowiące zaawansowaną wiedzę ogólną z zakresu socjologii, ze szczególnym uwzględnieniem istoty społeczeństwa wirtualnego.	K_W01 K_W02	P7S_WG	W1-4 Ćw2-4
EU_2	Zna i rozumie fundamentalne dylematy współczesnej cywilizacji w kontekście możliwości i zagrożeń związanych z korzystaniem z sieci internetowych.	K_W15	P7S_WK	W2-4 Ćw2-4
w zakresie umiejętności				
EU_3	Potrafi wykorzystywać posiadaną wiedzę – formułować i rozwiązywać złożone i nietypowe problemy z zakresu funkcjonowania społeczności internetowych.	K_U01 K_U02	P7S_UW	W2-4 Ćw2-4
EU_4	Potrafi prowadzić debatę i komunikować się na tematy specjalistyczne ze zróżnicowanymi kręgami odbiorców w kontekście aktywności w sieci internetowej.	K_U19 K_U21	P7S_UK	W2-4 Ćw2-4
w zakresie kompetencji społecznych				
EU_5	Jest gotów do krytycznej oceny posiadanej wiedzy i odbieranych treści dotyczących zjawisk społecznych zachodzących w sieci internetowej.	K_K02	P7S_KK	W1-4 Ćw2-4
EU_6	Jest gotów do odpowiedzialnego pelnienia ról zawodowych z uwzględnieniem zmieniających się potrzeb społecznych związanych z rozwojem sieci internetowych.	K_K07	P7S_KR	W2-4 Ćw2-4

Lp.	**Temat**	**Tezy**	**Forma studiów:**									
			stacjonarna					**niestacjonarna**				
			Łączna liczba godzin: 20					**Łączna liczba godzin: 14**				
			Wykłady	**Ćwiczenia**	**Zajęcia laboratoryjne**	**Warsztaty praktyczne**	**Razem**	**Wykłady**	**Ćwiczenia**	**Zajęcia laboratoryjne**	**Warsztaty praktyczne**	**Razem**
1.	Społeczeństwo informacyjne – powstanie społeczeństwa opartego na informacji (w odróżnieniu od społeczeństw agrarnych, przemysłowych)	1. Znaczenie informacji w XXI w. 2. Rola technologii w rewolucji informacyjnej.	2	-	-	-	**2**	2	-	-	-	**2**
2.	Tożsamość społeczna użytkownika Internetu	1. Awatar – postać graficzna reprezentująca realną osobę w wirtualnym świecie. 2. Komunikatory internetowe, media społecznościowe i ich rola w tworzeniu społeczności wirtualnych.	2	4	-	-	**6**	2	2	-	-	**4**

3.	Internet jako narzędzie partycypacji społecznej	1. Internet w służbie społeczeństwu (szybka komunikacja, praca zdalna, nauczanie na odległość, możliwość znalezienia ludzi o podobnych zainteresowaniach, nieograniczony dostęp wiedzy, akcje internetowe). 2. Internet w Polsce, Polacy w sieci.	2	4	-	-	**6**	2	2	-	-	**4**
4.	Negatywne zjawiska społeczne związane z informatyzacją	1. Obiektywne zagrożenia społeczne związane z korzystaniem z sieci internetowych (wykluczenie społeczne spowodowane brakiem dostępu do nowych technologii; zmiany na rynku pracy z powodu redukcji zatrudnienia w tradycyjnych branżach). 2. Zagrożenia subiektywne wynikające z korzystania z Internetu (manipulowanie informacją; rozluźnienie więzi społecznych; uzależnienia; hejt internetowy jako przyczyna zachowań suicydalnych młodzieży).	2	4	-	-	**6**	2	2	-	-	**4**
		Razem:	**8**	**12**	-	-	**20**	**8**	**6**	-	-	**14**

Forma zakończenia (S)	**Zaliczenie z oceną**												
Efekty uczenia się	**Metody weryfikacji osiągania efektów uczenia się**												
	Egzamin pisemny	Egzamin ustny	Sprawdzian pisemny	Odpowiedź ustna	Referat	Prezentacja indywidualna	Prezentacja grupowa	Projekt indywidualny	Projekt grupowy	Samodzielna realizacja zdania praktycznego	Zespołowa realizacja zadania praktycznego	Aktywność na zajęciach	Test sprawności fizycznej
EU_1			x									x	
EU_2			x									x	
EU_3			x		x							x	
EU_4			x				x		x			x	
EU_5												x	
EU_6												x	

Nazwa przedmiotu: Zabezpieczanie dowodów w środowisku cyfrowym				
Numer przedmiotu: 7	**Punkty ECTS:** 3	**Profil kształcenia:** Praktyczny	**Dziedzina nauki/dyscyplina naukowa:** nauki społeczne/ nauki o bezpieczeństwie	**Język wykładowy:** polski

Efekty uczenia się		**Symbol kierunkowego efektu uczenia się**	**Symbol składnika opisu charakterystyki drugiego stopnia efektów uczenia się dla kwalifikacji na poziomach 6-7 PRK**	**Treści programowe**
w zakresie wiedzy				
EU_1	Zna zróżnicowane metody, techniki, narzędzia i materiały stosowane przy zabezpieczaniu elektronicznego materiału dowodowego.	K_W03 K_W05 K_W06	P7S_WG	W1,3-4,6-8 L2, 4-8
EU_2	Zna tendencje rozwojowe w informatyce oraz rozumie ich wpływ na przetwarzanie i magazynowanie danych w systemach komputerowych.	K_W14	P7S_WG	W1,3-4,6-8 L2, 4-8
w zakresie umiejętności				
EU_3	Potrafi przygotować stanowisko do zabezpieczania wybranych typów danych.	K_U06 K_U07	P7S_UW	L2,4-7
EU_4	Potrafi pozyskiwać dane, a także umiejętnie interpretować otrzymane wyniki.	K_U06 K_U07	P7S_UW	L2,4-8
EU_5	Potrafi poprawnie zabezpieczać dane pozyskane z urządzeń mobilnych.	K_U06 K_U07	P7S_UW	L5,8
EU_6	Potrafi zlokalizować i umiejętnie zabezpieczyć dane ukryte.	K_U06 K_U07	P7S_UW	L8
w zakresie kompetencji społecznych				
EU_7	Jest gotów do rozwiązywania problemów praktycznych związanych z zabezpieczaniem dowodów w środowisku cyfrowym.	K_K01	P7S_KK	W1,3-4,6-8 L2, 4-8
EU_8	Jest gotów do pogłębionej analizy i krytycznej oceny posiadanej wiedzy z zakresu zabezpieczania dowodów w środowisku cyfrowym oraz zasięgania opinii ekspertów w przypadku trudności z samodzielnym rozwiązaniem problemu praktycznego.	K_K02 K_K03	P7S_KK	W1,3-4,6-8 L2, 4-8

Lp.	**Temat**	**Tezy**	**Forma studiów:**									
			stacjonarna					**niestacjonarna**				
			Łączna liczba godzin: 45					**Łączna liczba godzin: 30**				
			Wykłady	**Ćwiczenia**	**Zajęcia laboratoryjne**	**Warsztaty praktyczne**	**Razem**	**Wykłady**	**Ćwiczenia**	**Zajęcia laboratoryjne**	**Warsztaty praktyczne**	**Razem**
1.	Dowód cyfrowy	1. Pojęcie dowodu cyfrowego. 2. Rodzaje dowodów cyfrowych.	3	-	-	-	**3**	2	-	-	-	**2**

2.	Tworzenie obrazów nośników z wykorzystaniem blokerów sprzętowych i programowych	1. Pojęcie blokera sprzętowego i programowego. 2. Dobór odpowiedniego sposobu wykonania obrazu bądź klona nośnika z danymi. 3. Weryfikacja utworzonych obrazów i klonów nośników, wyliczanie sum kontrolnych z wykonanych obrazów i klonów.	-	-	4	-	**4**	-	-	2	-	**2**
3.	Klasyfikacja typów danych i miejsca ich występowania	1. Omówienie popularnych typy plików. 2. Programy generujące popularne typy plików i ich lokalizacja w systemie.	2	-	-	-	**2**	2	-	-	-	**2**
4.	Miejsca przechowywania istotnych danych w popularnych systemach operacyjnych	1. Lokalizacja danych z przeglądarek internetowych, programów pocztowych i komunikatorów. 2. Zabezpieczanie danych pochodzących z przeglądarek internetowych, programów pocztowych i komunikatorów.	2	-	4	-	**6**	2	-	4	-	**6**
5.	Zabezpieczanie danych z urządzeń mobilnych	1. Sposoby zabezpieczania danych z urządzeń mobilnych. 2. Urządzenia mobilne z systemem Windows. 3. Urządzenia z systemem iOS. 4. Urządzenia z systemem Symbian, Android, Bada_OS i inne.	-	-	6	-	**6**	-	-	2	-	**2**
6.	Zabezpieczanie plików z danymi	1. Zasady prawidłowego zabezpieczania plików z danymi. 2. Oprogramowanie służące do zabezpieczania danych. 3. Wyliczanie sum kontrolnych z zabezpieczonych plików. 4. Zabezpieczenie techniczne i procesowe.	4	-	6	-	**10**	4	-	2	-	**6**
7.	Zabezpieczenie pamięci RAM, plików hiberfil.sys i pagefile.sys	1. Zasady zabezpieczania pamięci RAM. 2. Rodzaje programowania służącego do zabezpieczania pamięci RAM.	2	-	6	-	**8**	2	-	4	-	**6**
8.	Ukrywanie danych	1. Ukryte nośniki i kontenery danych. 2. Odtwarzanie, uzyskiwanie nielegalnego kontentu danych.	2	-	4	-	**6**	2	-	2	-	**4**
		Razem:	**15**	-	**30**	-	**45**	**14**	-	**16**	-	**30**

Forma zakończenia (E)	**Egzamin**												
Efekty uczenia się	**Metody weryfikacji osiągania efektów uczenia się**												
	Egzamin pisemny	Egzamin ustny	Sprawdzian pisemny	Odpowiedź ustna	Referat	Prezentacja indywidualna	Prezentacja grupowa	Projekt indywidualny	Projekt grupowy	Samodzielna realizacja zdania praktycznego	Zespołowa realizacja zadania praktycznego	Aktywność na zajęciach	Test sprawności fizycznej
EU_1	x			x						x	x	x	
EU_2	x			x						x	x	x	
EU_3	x									x	x	x	
EU_4	x									x	x	x	
EU_5	x									x	x	x	
EU_6	x									x	x	x	
EU_7											x	x	
EU_8											x	x	

Nazwa przedmiotu: Międzynarodowa współpraca w zwalczaniu cyberzagrożeń				
Numer przedmiotu: 8	**Punkty ECTS:** 2	**Profil kształcenia:** praktyczny	**Dziedzina nauki/dyscyplina naukowa:** nauki społeczne/ nauki prawne	**Język wykładowy:** polski

Efekty uczenia się		**Symbol kierunkowego efektu uczenia się**	**Symbol składnika opisu charakterystyki drugiego stopnia efektów uczenia się dla kwalifikacji na poziomach 6-7 PRK**	**Treści programowe**
w zakresie wiedzy				
EU_1	Zna zasady i rozumie złożone mechanizmy funkcjonowania społeczności międzynarodowej oraz odmienności systemu prawa międzynarodowego w odniesieniu do porządku krajowego.	K_W01 K_W07	P7S_WG	W1-4 Ćw1-4
EU_2	Zna zasady współpracy międzynarodowej oraz istotę i zakres zadań podmiotów zaangażowanych w zwalczanie przestępczości, w tym przestępstw w cyberprzestrzeni.	K_W10	P7S_WG	W1-4 Ćw1-4
w zakresie umiejętności				
EU_3	Potrafi formułować i rozwiązywać typowe problemy prawne w oparciu o analizę międzynarodowych aktów prawnych w dziedzinie cyberprzestępczości.	K_U01 K_U08 K_U14	P7S_UW	Ćw1,3-4
EU_4	Potrafi identyfikować typowe formy cyberzagrożeń objętych zakresem międzynarodowego współdziałania.	K_U08 K_U12	P7S_UW	Ćw2-4
w zakresie kompetencji społecznych				
EU_5	Jest gotów do krytycznej oceny posiadanej wiedzy na temat międzynarodowej współpracy w zakresie zwalczania cyberprzestępczości.	K_K02	P7S_KK	W1-4 Ćw1-4

Lp.	**Temat**	**Tezy**	**Forma studiów:**									
			stacjonarna					**niestacjonarna**				
			Łączna liczba godzin: 40					**Łączna liczba godzin: 30**				
			Wykłady	**Ćwiczenia**	**Zajęcia laboratoryjne**	**Warsztaty praktyczne**	**Razem**	**Wykłady**	**Ćwiczenia**	**Zajęcia laboratoryjne**	**Warsztaty praktyczne**	**Razem**
1.	Akty międzynarodowe dotyczące statusu i zasad działania organów bezpieczeństwa	1. Charakter i funkcje regulacji przyjmowanych przez ONZ i Radę Europy. 2. Akty odnoszące się do statusu funkcjonariuszy porządku prawnego.	2	2	-	-	**4**	2	2	-	-	**4**
2.	Współpraca międzynarodowa w zwalczaniu przestępczości	1. Współpraca na podstawie umów dwustronnych i wielostronnych. 2. Współpraca w ramach organizacji międzynarodowych i pozarządowych.	4	4	-	-	**8**	2	3	-	-	**5**
3.	Wybrane zagadnienia międzynarodowego prawa karnego	1. Standaryzacja ustawodawstw karnych. 2. Międzynarodowa pomoc w sprawach karnych, jej zakres i zasady udzielania.	4	6	-	-	**10**	4	5	-	-	**9**

4.	Problematyka cyberprzestępczości w ujęciu międzynarodowym	1. Akty prawa międzynarodowego w obszarze cyberprzestępczości. 2. Międzynarodowy wymiar prac nad cyberprzestępczością. 3. Główne formy cyberprzestępczości objęte zakresem międzynarodowego współdziałania. 4. Europejskie Centrum ds. Walki z Cyberprzestępczością. 5. Współpraca pozaoperacyjna oraz wymiana i współpraca szkoleniowa.	5	13	-	-	**18**	2	10	-	-	**12**
		Razem:	**15**	**25**	-	-	**40**	**10**	**20**	-	-	**30**

Forma zakończenia (S)	**Zaliczenie z oceną**												
Efekty uczenia się	**Metody weryfikacji osiągania efektów uczenia się**												
	Egzamin pisemny	Egzamin ustny	Sprawdzian pisemny	Odpowiedź ustna	Referat	Prezentacja indywidualna	Prezentacja grupowa	Projekt indywidualny	Projekt grupowy	Samodzielna realizacja zdania praktycznego	Zespołowa realizacja zadania praktycznego	Aktywność na zajęciach	Test sprawności fizycznej
EU_1			x	x	x	x						x	
EU_2			x	x	x	x						x	
EU_3			x	x	x	x						x	
EU_4			x	x	x	x						x	
EU_5												x	

Nazwa przedmiotu: Encyklopedia zagrożeń informatycznych				
Numer przedmiotu: 9	**Punkty ECTS:** 1	**Profil kształcenia:** praktyczny	**Dziedzina nauki/dyscyplina naukowa:** nauki o bezpieczeństwie/nauki o bezpieczeństwie	**Język wykładowy:** polski

Efekty uczenia się		**Symbol kierunkowego efektu uczenia się**	**Symbol składnika opisu charakterystyki drugiego stopnia efektów uczenia się dla kwalifikacji na poziomach 6-7 PRK**	**Treści programowe**
w zakresie wiedzy				
EU_1	Zna specjalistyczne pojęcia dotyczące cyberzagrożeń i ich praktyczne zastosowanie w działalności zawodowej.	K_W02	P7S_WG	W1
EU_2	Zna rodzaje i specyfikację cyberzagrożeń.	K_W02 K_W15	P7S_WG P7S_WK	W2 WP2
EU_3	Zna i rozumie zasady przeciwdziałania zagrożeniom w cyberprzestrzeni.	K_W02	P7S_WG	W3 WP3
w zakresie umiejętności				
EU_4	Potrafi identyfikować złożone procesy i nietypowe zagrożenia w cyberprzestrzeni.	K_U01 K_U02 K_U13	P7S_UW	W2 WP2
EU_5	Potrafi sporządzić program profilaktyczny w zakresie zwalczania nietypowych zagrożeń w cyberprzestrzeni.	K_U18 K_U19	P7S_UK	W3 WP3
w zakresie kompetencji społecznych				
EU_6	Jest gotów do uznania znaczenia wiedzy w rozwiązywaniu problemów poznawczych i praktycznych w zakresie zwalczania i przeciwdziałania cyberzagrożeniom.	K_K01	P7S_KK	W2-3 WP2-3
EU_7	Jest gotowy do pogłębionej analizy i krytycznej oceny posiadanej wiedzy z zakresu cyberzagrożeń oraz zasięgania opinii ekspertów w przypadku trudności z samodzielnym rozwiązaniem problemu praktycznego.	K_K02 K_K03	P7S_KK	W2-3 WP2-3

Lp.	**Temat**	**Tezy**	**Forma studiów:**									
			stacjonarna					**niestacjonarna**				
			Łączna liczba godzin: 15					**Łączna liczba godzin: 10**				
			Wykłady	**Ćwiczenia**	**Zajęcia laboratoryjne**	**Warsztaty praktyczne**	**Razem**	**Wykłady**	**Ćwiczenia**	**Zajęcia laboratoryjne**	**Warsztaty praktyczne**	**Razem**
1.	Wstęp do zagrożeń informatycznych – pojęcia	1. Bezpieczeństwo systemów informacyjnych – wprowadzenie do pojęć. 2. Inżynieria bezpieczeństwa. 3. Abc cyberbezpieczeństwa według NASK.	2	-	-	-	**2**	1	-	-	-	**1**

2.	Zagrożenia - rodzaje i specyfikacja	1. Włamanie do systemu komputerowego. 2. Nieuprawnione pozyskanie informacji. 3. Destrukcja danych i programów. 4. Sabotaż (sparaliżowanie pracy) systemu. 5. Piractwo komputerowe, kradzież oprogramowania. 6. Oszustwo komputerowe i falszerstwo komputerowe. 7. Szpiegostwo komputerowe.	4	-	-	5	**9**	2	-	-	4	**6**
3.	Profilaktyka w zakresie cyberzagrożeń	1. Obowiązujące zasady przeciwdziałania. 2. Zasoby ludzkie – najsłabsze ogniwo. 3. Unijna strategia walki z zagrożeniami informatycznymi.	2	-	-	2	**4**	1	-	-	2	**3**
		Razem:	**8**	-	-	**7**	**15**	**4**	-	-	**6**	**10**

Forma zakończenia (Z)	**Zaliczenie**												
Efekty uczenia się	**Metody weryfikacji osiągania efektów uczenia się**												
	Egzamin pisemny	Egzamin ustny	Sprawdzian pisemny	Odpowiedź ustna	Referat	Prezentacja indywidualna	Prezentacja grupowa	Projekt indywidualny	Projekt grupowy	Samodzielna realizacja zdania praktycznego	Zespołowa realizacja zadania praktycznego	Aktywność na zajęciach	Test sprawności fizycznej
EU_1										x	x	x	
EU_2										x	x	x	
EU_3										x	x	x	
EU_4										x	x	x	
EU_5										x	x	x	
EU_6										x		x	
EU_7										x		x	

Nazwa przedmiotu: Język niemiecki				
Numer przedmiotu: 10a	**Punkty ECTS:** 6	**Profil kształcenia:** praktyczny	**Dziedzina nauki/dyscyplina naukowa:** nauki społeczne/ nauki o bezpieczeństwie	**Język wykładowy:** polski/niemiecki

Efekty uczenia się		**Symbol kierunkowego efektu uczenia się**	**Symbol składnika opisu charakterystyki drugiego stopnia efektów uczenia się dla kwalifikacji na poziomach 6-7 PRK**	**Treści programowe**
w zakresie wiedzy				
EU_1	Zna i rozumie zasady skutecznej komunikacji w języku polskim i niemieckim oraz ich praktyczne zastosowanie w działalności zawodowej.	K_W01 K_W17	P7S_WG P7S_WK	Ćw1
w zakresie umiejętności				
EU_2	Stosuje podczas wypowiedzi ustnych i pisemnych gramatykę języka niemieckiego, leksykę specjalistyczną, w tym dotyczącą pracy Policji, ze szczególnym uwzględnieniem bezpieczeństwa w cyberprzestrzeni.	K_U01 K_U18 K_U20	P7S_UW P7S_UK	Ćw1
EU_3	Rozumie wypowiedzi i programy informacyjne w języku niemieckim dotyczące aktualnych i specjalistycznych tematów, w szczególności związanych z pracą Policji oraz bezpieczeństwem w cyberprzestrzeni.	K_U02 K_U20	P7S_UW P7S_UK	Ćw1
EU_4	Rozumie artykuły i teksty opisujące problematykę współczesną, a także zawierającą leksykę specjalistyczną dotyczącą pracy Policji oraz cyberbezpieczeństwa.	K_U20	P7S_UK	Ćw1
EU_5	Przygotowuje typowe prace pisemne w języku niemieckim na specjalistyczne tematy związane z bieżącymi wydarzeniami, swoimi zainteresowaniami, pracą Policji, w szczególności w zakresie zwalczania cyberprzestępczości.	K_U18 K_U20	P7S_UK	Ćw1
EU_6	Porozumiewa się swobodnie i spontanicznie w języku niemieckim, w taki sposób, że interakcje ze zróżnicowanymi kręgami odbiorców, w tym z rodzimymi użytkownikami języka niemieckiego stają się naturalne, przedstawia swoje poglądy i potrafi je bronić.	K_U19 K_U20	P7S_UK	Ćw1
EU_7	Uczestniczy czynnie w rozmowach, wypowiada się jasno i szczegółowo na tematy specjalistyczne, dotyczące różnych wydarzeń, swoich zainteresowań i pracy Policji, w szczególności w zakresie zwalczania cyberprzestępczości.	K_U19 K_U20 K_U21	P7S_UK	Ćw1
w zakresie kompetencji społecznych				
EU_8	Jest gotów do krytycznej oceny posiadanej wiedzy z języka niemieckiego.	K_K02	P7S_KK	Ćw1

Lp.	**Temat**	**Tezy**	**Forma studiów:**									
			stacjonarna					**niestacjonarna**				
			Łączna liczba godzin: 60					**Łączna liczba godzin: 50**				
			Wykłady	**Ćwiczenia**	**Zajęcia laboratoryjne**	**Warsztaty praktyczne**	**Razem**	**Wykłady**	**Ćwiczenia**	**Zajęcia laboratoryjne**	**Warsztaty praktyczne**	**Razem**
1.	Język ogólny i specjalistyczny	1. Człowiek i środowisko społeczne.	-	10	-	-	**10**	-	9	-	-	**9**
		2. Praca zawodowa.	-	10	-	-	**10**	-	8	-	-	**8**

		3. Problemy współczesnego świata.	-	10	-	-	**10**	-	8	-	-	**8**
		4. Sprawca i ofiara przestępstwa w sieci cybernetycznej.	-	10	-	-	**10**	-	9	-	-	**9**
		5. Zapobieganie i zwalczacie przestępczości w sieci.	-	10	-	-	**10**	-	8	-	-	**8**
		6. Studia przypadków.	-	10	-	-	**10**	-	8	-	-	**8**
		Razem:	-	**60**	-	-	**60**	-	**50**	-	-	**50**

Forma zakończenia (E)	**Egzamin**												
Efekty uczenia się	**Metody weryfikacji osiągania efektów uczenia się**												
	Egzamin pisemny	Egzamin ustny	Sprawdzian pisemny	Odpowiedź ustna	Referat	Prezentacja indywidualna	Prezentacja grupowa	Projekt indywidualny	Projekt grupowy	Samodzielna realizacja zdania praktycznego	Zespołowa realizacja zadania praktycznego	Aktywność na zajęciach	Test sprawności fizycznej
EU_1		x		x		x			x			x	
EU_2		x	x	x		x			x			x	
EU_3			x	x		x			x			x	
EU_4			x			x			x			x	
EU_5			x									x	
EU_6		x		x		x			x			x	
EU_7		x		x		x			x			x	
EU_8		x		x		x			x			x	

Nazwa przedmiotu: Język rosyjski				
Numer przedmiotu: 10b	**Punkty ECTS:** 6	**Profil kształcenia:** praktyczny	**Dziedzina nauki/dyscyplina naukowa:** nauki społeczne/ nauki o bezpieczeństwie	**Język wykładowy:** polski/rosyjski

Efekty uczenia się		**Symbol kierunkowego efektu uczenia się**	**Symbol składnika opisu charakterystyki drugiego stopnia efektów uczenia się dla kwalifikacji na poziomach 6-7 PRK**	**Treści programowe**
w zakresie wiedzy				
EU_1	Zna i rozumie zasady skutecznej komunikacji w języku polskim i rosyjskim oraz jej praktyczne zastosowanie w działalności zawodowej.	K_W01 K_W17	P7S_WG P7S_WK	Ćw1
w zakresie umiejętności				
EU_2	Stosuje podczas wypowiedzi ustnych i pisemnych gramatykę języka rosyjskiego, leksykę specjalistyczną dotyczącą pracy Policji, ze szczególnym uwzględnieniem bezpieczeństwa w cyberprzestrzeni.	K_U01 K_U18 K_U20	P7S_UW P7S_UK	Ćw1
EU_3	Rozumie wypowiedzi i programy informacyjne w języku rosyjskim dotyczące aktualnych i specjalistycznych tematów, w szczególności związanych z pracą Policji oraz bezpieczeństwem w cyberprzestrzeni.	K_U02 K_U20	P7S_UW P7S_UK	Ćw1
EU_4	Rozumie artykuły i teksty opisujące problematykę współczesną, a także zawierającą leksykę specjalistyczną dotyczącą pracy Policji oraz cyberbezpieczeństwa.	K_U20	P7S_UK	Ćw1
EU_5	Przygotowuje typowe prace pisemne w języku rosyjskim na tematy związane z bieżącymi wydarzeniami, pracą Policji, w szczególności w zakresie cyberprzestępczości.	K_U18 K_U20	P7S_UK	Ćw1
EU_6	Porozumiewa się swobodnie i spontanicznie w języku rosyjskim, w taki sposób, że interakcje ze zróżnicowanymi kręgami odbiorców, w tym z rodzimymi użytkownikami języka rosyjskiego stają się naturalne, przedstawia swoje poglądy i potrafi je bronić.	K_U19 K_U20	P7S_UK	Ćw1
EU_7	Uczestniczy czynnie w rozmowach, wypowiada się jasno i szczegółowo na tematy specjalistyczne, dotyczące różnych wydarzeń, swoich zainteresowań i pracy Policji, w szczególności w zakresie zwalczania cyberprzestępczości.	K_U19 K_U20 K_U21	P7S_UK	Ćw1
w zakresie kompetencji społecznych				
EU_8	Jest gotów do krytycznej oceny posiadanej wiedzy z języka rosyjskiego.	K_K02	P7S_KK	Ćw1

Lp.	**Temat**	**Tezy**	**Forma studiów:**									
			stacjonarna					**niestacjonarna**				
			Łączna liczba godzin: 60					**Łączna liczba godzin: 50**				
			Wykłady	**Ćwiczenia**	**Zajęcia laboratoryjne**	**Warsztaty praktyczne**	**Razem**	**Wykłady**	**Ćwiczenia**	**Zajęcia laboratoryjne**	**Warsztaty praktyczne**	**Razem**
1.	Język ogólny i specjalistyczny	1. Człowiek i środowisko społeczne.	-	10	-	-	**10**	-	9	-	-	9
		2. Praca zawodowa.	-	10	-	-	**10**	-	8	-	-	8
		3. Problemy współczesnego świata.	-	10	-	-	**10**	-	8	-	-	8

		4. Sprawca i ofiara przestępstwa w sieci cybernetycznej.	-	10	-	-	**10**	-	9	-	-	9
		5. Zapobieganie i zwalczacie przestępczości w sieci.	-	10	-	-	**10**	-	8	-	-	8
		6. Studia przypadków.	-	10	-	-	**10**	-	8	-	-	8
		Razem:	-	**60**	-	-	**60**	-	**50**	-	-	**50**

Forma zakończenia (E)	**Egzamin**												
Efekty uczenia się	**Metody weryfikacji osiągania efektów uczenia się**												
	Egzamin pisemny	Egzamin ustny	Sprawdzian pisemny	Odpowiedź ustna	Referat	Prezentacja indywidualna	Prezentacja grupowa	Projekt indywidualny	Projekt grupowy	Samodzielna realizacja zdania praktycznego	Zespołowa realizacja zadania praktycznego	Aktywność na zajęciach	Test sprawności fizycznej
EU_1		x		x		x			x			x	
EU_2		x	x	x		x			x			x	
EU_3			x	x		x			x			x	
EU_4			x			x			x			x	
EU_5			x									x	
EU_6		x		x		x			x			x	
EU_7		x		x		x			x			x	
EU_8		x		x		x			x			x	

Nazwa przedmiotu: Praktyka zawodowa				
Numer przedmiotu: 11	**Punkty ECTS:** 39	**Profil kształcenia:** praktyczny	**Dziedzina nauki/dyscyplina naukowa:** nauki społeczne/ nauki o bezpieczeństwie	**Język wykładowy:** polski

	Efekty uczenia się	**Symbol kierunkowego efektu uczenia się**	**Symbol składnika opisu charakterystyki drugiego stopnia efektów uczenia się dla kwalifikacji na poziomach 6-7 PRK**	**Treści programowe**
w zakresie wiedzy				
EU_1	Zna i rozumie strukturę organizacyjną, zadania instytucji, oraz zakres działania poszczególnych komórek organizacyjnych i stanowisk instytucji, w której student odbywa praktykę.	K_W10 K_W11	P7S_UW	Ćw1-4
EU_2	Zna i rozumie przepisy regulujące działanie instytucji, w której student odbywa praktykę.	K_W07	P7S_UW	Ćw1-4
EU_3	Zna i rozumie zasady metodyki pracy właściwe dla działalności instytucji, w której student odbywa praktykę.	K_W11	P7S_UW	Ćw1-4
w zakresie umiejętności				
EU_4	Potrafi wykonywać złożone zadania techniczno-organizacyjne, istotne z punktu widzenia specyfiki działalności instytucji, w której student odbywa praktykę.	K_U08 K_U13 K_U14	P7S_UW	Ćw1-11
EU_5	Potrafi wykorzystać wiedzę zdobytą na wykładach, ćwiczeniach i laboratoriach oraz umiejętnie zaplanować pracę indywidualną oraz pracować w zespole.	K_U01 K_U02 K_U22	P7S_UW P7S_UO	Ćw5-11
EU_6	Potrafi dokonać krytycznej analizy sposobu funkcjonowania systemów informatycznych w miejscu praktyki.	K_U07 K_U11	P7S_UW	Ćw5-11
EU_7	Potrafi opracować dokumentację dotyczącą realizacji nietypowych zadań w ramach praktyki, a także referuje ustnie prezentowane w niej zagadnienia.	K_U10 K_U18	P7S_UK	Ćw5-11
w zakresie kompetencji społecznych				
EU_8	Jest gotów do uznawania wiedzy w rozwiązywaniu problemów oraz zasięgania opinii ekspertów w przypadku trudności z samodzielnym rozwiązaniem problemów identyfikowanych w związku z wykonywaniem zadań w podmiotach prowadzących działalność związaną z zapewnieniem bezpieczeństwa w cyberprzestrzeni.	K_K01 K_K03	P7S_KK	Ćw1-11
EU_9	Jest gotów do odpowiedzialnego wypełniania zobowiązań społecznych w ramach wykonywania zadań w podmiotach prowadzących działalność w zakresie bezpieczeństwa w cyberprzestrzeni.	K_K04	P7S_KO	Ćw1-11
EU_10	Jest gotów do odpowiedzialnego pełnienia roli zawodowej, związanej z kierunkiem studiów, w tym przestrzegania zasad etyki zawodowej i wymagania tego od innych.	K_K07	P7S_KR	Ćw1-11

Lp.	Temat	Tezy	Forma studiów:									
			stacjonarna					niestacjonarna				
			Łączna liczba godzin: 720					Łączna liczba godzin: 720				
			Wykłady	Ćwiczenia	Zajęcia laboratoryjne	Warsztaty praktyczne	Razem	Wykłady	Ćwiczenia	Zajęcia laboratoryjne	Warsztaty praktyczne	Razem
1.	Szkolenie BHP, a w szczególności przepisy dotyczące pracy przy komputerze.											
2.	Zapoznanie się z zakresem działalności i charakterystyką zakładu pracy.											
3.	Zapoznanie się z procedurami funkcjonowania zakładu pracy, normami jakościowymi ISO, audytorem itp.											
4.	Zapoznanie się z zakresem obowiązków i specyfiką pracy informatyka w zakładzie pracy.											
5.	Administrowanie, instalacja i konfiguracja sieci komputerowych.			720			**720**		720			**720**
6.	Administrowanie, instalacja i konfiguracja oprogramowania sieciowego.											
7.	Współpraca przy archiwizowaniu danych.											
8.	Udział w procesie serwisowania sprzętu komputerowego.											
9.	Udział w instalowaniu nowych lub uaktualnionych wersji oprogramowania.											
10.	Wykorzystanie oprogramowania narzędziowego do konserwacji systemu.											
11.	Obsługa i konserwacja urządzeń peryferyjnych.											
		Razem:	**-**	**720**	**-**	**-**	**720**	**-**	**720**	**-**	**-**	**720**

Forma zakończenia (Z)	**Zaliczenie**												
Efekty uczenia się	**Metody weryfikacji osiągania efektów uczenia się**												
	Egzamin pisemny	Egzamin ustny	Sprawdzian pisemny	Odpowiedź ustna	Referat	Prezentacja indywidualna	Prezentacja grupowa	Projekt indywidualny	Projekt grupowy	Samodzielna realizacja zdania praktycznego	Zespołowa realizacja zadania praktycznego	Aktywność na zajęciach	Test sprawności fizycznej
EU_1										x	x	x	
EU_2										x	x	x	
EU_3										x	x	x	
EU_4										x	x	x	
EU_5										x	x	x	
EU_6										x	x	x	
EU_7										x	x	x	
EU_8												x	
EU_9												x	
EU_10												x	

Nazwa przedmiotu: Seminarium dyplomowe				
Numer przedmiotu: 12	**Punkty ECTS:** 11	**Profil kształcenia:** praktyczny	**Dziedzina nauki/dyscyplina naukowa:** nauki społeczne/ nauki o bezpieczeństwie	**Język wykładowy:** polski

Efekty uczenia się		**Symbol kierunkowego efektu uczenia się**	**Symbol składnika opisu charakterystyki drugiego stopnia efektów uczenia się dla kwalifikacji na poziomach 6-7 PRK**	**Treści programowe**
w zakresie wiedzy				
EU_1	Zna metody i narzędzia naukowej deskrypcji stosowane przy pisaniu pracy dyplomowej.	K_W04 K_W05	P7S_WG	Ćw1
EU_2	Zna metody i narzędzia służące do pozyskiwania danych i prowadzenia badań w zakresie modelowania struktur społecznych i procesów w nich zachodzących związanych z bezpieczeństwem w cyberprzestrzeni.	K_W04	P7S_WG	Ćw2-6
EU_3	Zna wybrane normy i reguły organizacyjne, zawodowe i kulturowe określające prawidłowości oraz zmiany w sposobach działalności instytucji odpowiedzialnych za bezpieczeństwo w cyberprzestrzeni.	K_W07 K_W16	P7S_WG P7S_WK	Ćw3-4
EU_4	Zna i rozumie złożone przyczyny i skutki zjawisk społecznych determinujących bezpieczeństwo w cyberprzestrzeni.	K_W13 K_W15	P7S_WG P7S_WK	Ćw5-6
EU_5	Rozumie procesy zachodzące w obszarze cyberbezpieczeństwa.	K_W14	P7S_WG	Ćw6-7
w zakresie umiejętności				
EU_6	Potrafi analizować zjawiska społeczne i relacje zachodzące między nimi wpływające na poziom cyberbezpieczeństwa.	K_U01 K_U02	P7S_UW	Ćw1-5
EU_7	Potrafi analizować przyczyny i przebieg procesów i zjawisk społecznych determinujących cyberbezpieczeństwo.	K_U13	P7S_UW	Ćw2-7
EU_8	Potrafi wykorzystać metody badawcze do poznania zjawisk społecznych związanych z bezpieczeństwem w cyberprzestrzeni.	K_U04 K_U05	P7S_UW	Ćw2-7
EU_9	Potrafi formułować opinie na temat zjawisk społecznych i metod ich analiz w kontekście współczesnych zagrożeń bezpieczeństwa w cyberprzestrzeni.	K_U13 K_U19 K_U21	P7S_UW P7S_UK	Ćw3-7
EU_10	Potrafi formułować i testować hipotezy badawcze dotyczące przyczyn i przebiegu procesów i zjawisk społecznych kształtujących poziom cyberbezpieczeństwa.	K_U04 K_U05	P7S_UW	Ćw4
EU_11	Potrafi wykorzystywać interdyscyplinarne metody i narzędzia do modelowania procesów społecznych w zakresie cyberbezpieczeństwa.	K_U01 K_U02	P7S_UW	Ćw5
w zakresie kompetencji społecznych				
EU_12	Jest gotów do uznawania wiedzy w rozwiązywaniu problemów oraz zasięgania opinii ekspertów w przypadku trudności z samodzielnym rozwiązaniem problemów poznawczych i praktycznych w zakresie bezpieczeństwa w cyberprzestrzeni.	K_K01 K_K03	P7S_KK	Ćw1-7
EU_13	Jest gotów do odpowiedzialnego wypełniania zobowiązań społecznych w ramach wykonywania zadań w podmiotach prowadzących działalność w zakresie bezpieczeństwa w cyberprzestrzeni.	K_K04	P7S_KO	Ćw1-7
EU_14	Jest gotów do odpowiedzialnego pełnienia roli zawodowej, związanej z kierunkiem studiów, w tym przestrzegania zasad etyki zawodowej i wymagania tego od innych.	K_K07	P7S_KR	Ćw1-7

Lp.	Temat	Tezy	Forma studiów:									
			stacjonarna					niestacjonarna				
			Łączna liczba godzin: 60					Łączna liczba godzin: 60				
			Wykłady	Ćwiczenia	Zajęcia laboratoryjne	Warsztaty praktyczne	Razem	Wykłady	Ćwiczenia	Zajęcia laboratoryjne	Warsztaty praktyczne	Razem
1.	Wprowadzenie do problematyki pisania pracy dyplomowej	1. Omówienie wymagań merytorycznych pracy: zakres tematyczny, wykład autora, narzędzia badawcze. 2. Omówienie wymagań formalnych: a) konstrukcja pracy, b) aparatury pojęciowej i terminologicznej, c) wymagania językowe, d) konstrukcja odsyłaczy, e) źródła, f) istota praw autorskich oraz plagiatu.	-	5	-	-	**5**	-	5	-	-	**5**
2	Sformułowanie problemów badawczych i przedmiotu badań i określenie tematu pracy	1. Istota problemu naukowego. 2. Problem główny. 3. Problemy szczegółowe.	-	5	-	-	**5**	-	5	-	-	**5**
3	Sformułowanie hipotez, dobór metod, technik i narzędzi badawczych, źródeł oraz ustalenie istotnych ograniczeń badawczych	1. Rodzaje i istota hipotez. 2. Dobór i uzasadnienie doboru metod badawczych. 3. Procedury przewidywanych metod rozwiązania problemów badawczych	-	5	-	-	**5**	-	5	-	-	**5**
4	Ustalenie i omówienie planu badań i opracowanie koncepcji pracy	1. Wymagania koncepcji pracy magisterskiej. 2. Istota i cel planu badań i koncepcji pracy. 3. Układ koncepcji pracy magisterskiej.	-	5	-	-	**5**	-	5	-	-	**5**
5	Prezentacja treści opracowanych rozdziałów pracy	1. Prezentacja wyników badań cząstkowych wraz z uzasadnieniem. 2. Dyskusja i polemiki.	-	15	-	-	**15**	-	15	-	-	**15**
6	Prezentacja wyników prowadzonych sukcesywnie badań	1. Prezentacja wyników badań cząstkowych wraz z uzasadnieniem. 2. Dyskusja i polemiki.	-	15	-	-	**15**	-	15	-	-	**15**
7	Przygotowanie do egzaminu dyplomowego	1. Forma i zakres egzaminu. 2. Sposób prezentacji odpowiedzi na pytania. 3. Prezentacja dorobku pracy.	-	10	-	-	**10**	-	10	-	-	**10**
		Razem:	-	**60**	-	-	**60**	-	**60**	-	-	**60**

Forma zakończenia (Z)	**Zaliczenie**												
Efekty uczenia się	**Metody weryfikacji osiągania efektów uczenia się**												
	Egzamin pisemny	Egzamin ustny	Sprawdzian pisemny	Odpowiedź ustna	Referat	Prezentacja indywidualna	Prezentacja grupowa	Projekt indywidualny	Projekt grupowy	Samodzielna realizacja zdania praktycznego	Zespołowa realizacja zadania praktycznego	Aktywność na zajęciach	Test sprawności fizycznej
EU_1								x		x		x	
EU_2								x		x		x	
EU_3								x		x		x	
EU_4								x		x		x	
EU_5								x		x		x	
EU_6								x		x		x	
EU_7								x		x		x	
EU_8								x		x		x	
EU_9								x		x		x	
EU_10								x		x		x	
EU_11								x		x		x	
EU_12								x		x		x	
EU_13								x		x		x	
EU_14								x		x		x	

Nazwa przedmiotu: Etiologia przestępczości internetowej				
Numer przedmiotu: 13	**Punkty ECTS:** 1	**Profil kształcenia:** praktyczny	**Dziedzina nauki/dyscyplina naukowa:** nauki społeczne/nauki prawne	**Język wykładowy:** polski

Efekty uczenia się		**Symbol kierunkowego efektu uczenia się**	**Symbol składnika opisu charakterystyki drugiego stopnia efektów uczenia się dla kwalifikacji na poziomach 6-7 PRK**	**Treści programowe**
w zakresie wiedzy				
EU_1	Zna i rozumie kryminologiczne aspekty przestępczości internetowej oraz wzajemne relacje, zależności między kryminologią a normami prawa.	K_W01 K_W04	P7S_WG	W1-3 Ćw1-4
EU_2	Zna strukturę, zadania oraz możliwości współpracy, komunikacji instytucji krajowych i międzynarodowych zajmujących się kontrolą przestępczości z użyciem komputerów i ich sieci.	K_W10	P7S_WG	W1-3 Ćw1-4
w zakresie umiejętności				
EU_3	Potrafi identyfikować, interpretować i wyjaśniać złożone procesy i zjawiska społeczne w odniesieniu do etiologii i fenomenologii zjawiska cyberprzestępczości.	K_U01 K_U08 K_U13	P7S_UW	Ćw1-4
EU_4	Potrafi publicznie prezentować swoje argumenty i opinie dotyczące zagadnień związanych z etiologią, fenomenologią oraz zapobieganiem cyberprzestępczości.	K_U13 K_U21	P7S_UW P7S_UK	Ćw1-4
w zakresie kompetencji społecznych				
EU_5	Jest gotów do uznania znaczenia wiedzy w rozwiązywaniu problemów poznawczych i praktycznych w zakresie etiologii zjawiska cyberprzestępczości.	K_K01	P7S_KK	W1-3 Ćw1-4

Lp.	**Temat**	**Tezy**	**Forma studiów:**									
			stacjonarna					**niestacjonarna**				
			Łączna liczba godzin: 20					**Łączna liczba godzin: 15**				
			Wykłady	**Ćwiczenia**	**Zajęcia laboratoryjne**	**Warsztaty praktyczne**	**Razem**	**Wykłady**	**Ćwiczenia**	**Zajęcia laboratoryjne**	**Warsztaty praktyczne**	**Razem**
1.	Fenomen przestępczości z użyciem komputerów i ich sieci	1. Społeczeństwo informacyjne. 2. Przestępczość komputerowa. 3. Przestępczość internetowa. 4. Cyberprzestępczość jako szczególna forma przestępczości.	1	4	-	-	**5**	1	2	-	-	**3**
2.	Etiologia przestępczości	1. Etiologia jako dział kryminologii. 2. Determinanty przestępczości. 3. Charakterystyka przestępczości i sprawców przestępstw. 4. Kryminologiczne aspekty powrotu do przestępstwa.	3	5	-	-	**8**	3	5	-	-	**8**

3.	Teoria podkultur przestępczych	1. Hacker. 2. Cracker. 3. Wandal. 4. Piraci komputerowi. 5. Phreakerzy. 6. Carderzy. 7. Blackhat.	1	4	-	-	**5**	1	2	-	-	**3**
4.	Profilaktyka przestępczości komputerów i ich sieci	1. Działania o charakterze informacyjnym i edukacyjnym. 2. Krajowa Rama Polityki Cyberbezpieczeństwa RP. 2. Threat Intelligence. 3. CERT.	-	2	-	-	**2**	-	1	-	-	**1**
		Razem:	**5**	**15**	**-**	**-**	**20**	**5**	**10**	**-**	**-**	**15**

Forma zakończenia (S)	**Zaliczenie z oceną**												
Efekty uczenia się	**Metody weryfikacji osiągania efektów uczenia się**												
	Egzamin pisemny	Egzamin ustny	Sprawdzian pisemny	Odpowiedź ustna	Referat	Prezentacja indywidualna	Prezentacja grupowa	Projekt indywidualny	Projekt grupowy	Samodzielna realizacja zdania praktycznego	Zespołowa realizacja zadania praktycznego	Aktywność na zajęciach	Test sprawności fizycznej
EU_1			x		x		x	x				x	
EU_2			x		x		x	x				x	
EU_3			x		x		x	x				x	
EU_4			x		x		x	x				x	
EU_5					x		x					x	

Nazwa przedmiotu: Społeczna odpowiedzialność służby zwalczania cyberprzestępczości				
Numer przedmiotu: 14	**Punkty ECTS:** 1	**Profil kształcenia:** praktyczny	**Dziedzina nauki/dyscyplina naukowa**: nauki społeczne/nauki o bezpieczeństwie	**Język wykładowy:** polski

	Efekty uczenia się	**Symbol kierunkowego efektu uczenia się**	**Symbol składnika opisu charakterystyki drugiego stopnia efektów uczenia się dla kwalifikacji na poziomach 6-7 PRK**	**Treści programowe**
	w zakresie wiedzy			
EU_1	Zna i rozumie zróżnicowane teorie z zakresu nauk społecznych oraz zjawiska społeczne wywierające wpływ na stopień przestępczości w kraju oraz konieczność oddziaływania służb państwowych na rzecz rozwoju dobra publicznego i dobrostanu obywateli.	K_W01 K_W13 K_W15	P7S_WG P7S_WK	W1-5 Ćw1-5
EU_2	Zna i rozumie znaczenie reguł społecznej odpowiedzialności funkcjonariuszy i instytucji publicznych w kształtowaniu kapitału społecznego, instytucjonalnego i obywatelskiego oraz bezpieczeństwa wewnętrznego.	K_W11	P7S_WG	W1-5 Ćw1-5
EU_3	Zna i rozumie ekonomiczne, prawne i etyczne uwarunkowania działalności Policji, w tym służby zwalczania cyberprzestępczości w zakresie ochrony życia, zdrowia i mienia obywateli oraz instytucjonalne rozwiązania krajowe i wspólnotowe w sferze społecznej odpowiedzialności instytucji publicznych.	K_W16	P7S_WK	W1-5 Ćw1-5
	w zakresie umiejętności			
EU_4	Potrafi wykorzystać posiadaną wiedzę z zakresu społecznej odpowiedzialności na rzecz analizowania zjawisk, zagrożeń oraz procesów społecznych oraz formułowania i rozwiązywania złożonych problemów związanych z wykonywaniem zadań funkcjonariuszy służby zwalczania cyberprzestępczości w sferze bezpieczeństwa kraju.	K_U01 K_U13	P7S_WG	W1-5 Ćw1-5
EU_5	Potrafi wykorzystywać posiadaną wiedzę zakresu społecznej odpowiedzialności w celu doboru adekwatnych do sytuacji metod i technik w zakresie analizowania przestępczości i ścigania jej sprawców oraz doboru różnych norm i zasad społecznie akceptowanych.	K_U04 K_U13	P7S_WG	W1-5 Ćw1-5
EU_6	Potrafi planować i organizować pracę indywidualną oraz w zespole i współpracować w ramach prac zespołowych wykorzystując reguły społecznej odpowiedzialności instytucji publicznej i partnerskiej *community policing*.	K_U18 K_U22	P7S_UK P7S_UO	W1-5 Ćw1-5
	w zakresie kompetencji społecznych			
EU_7	Jest gotów do krytycznej oceny posiadanej wiedzy i odbieranych treści z zakresu społecznej odpowiedzialności instytucji publicznej i zwalczania cyberprzestępczości oraz jest gotów do korzystania z wiedzy eksperckiej w przypadku trudności w samodzielnym rozwiazywaniu problemów cyberprzestępczości oraz do uzupełniania posiadanej wiedzy;	K_K02 K_K03	P7S_KK	W1-5 Ćw1-5
EU_8	Jest gotów do wypełniania zobowiązań społecznych i współorganizowania działalności na rzecz poprawy dobrostanu obywateli oraz na rzecz interesu publicznego.	K_K04	P7S_KO	W1-5 Ćw1-5
EU_9	Jest gotów do odpowiedzialnego pełnienia ról zawodowych w sferze służby zwalczania cyberprzestępczości oraz przestrzegania reguł dobrej roboty i zasad etyki funkcjonariuszy publicznych, w tym policjantów.	K_K07	P7S_KR	W1-5 Ćw1-5

Lp.	Temat	Tezy	Forma studiów:									
			Stacjonarna					niestacjonarna				
			Łączna liczba godzin:15					Łączna liczba godzin: 15				
			Wykłady	Ćwiczenia	Zajęcia laboratoryjne	Warsztaty praktyczne	Razem	Wykłady	Ćwiczenia	Zajęcia laboratoryjne	Warsztaty praktyczne	Razem
1.	Idea społecznej odpowiedzialności instytucji publicznych w Unii Europejskiej i etapy jej rozwoju	1. Istota społecznej odpowiedzialności organizacji i instytucji publicznych. 2. Powstanie koncepcji społecznej odpowiedzialności organizacji i etapy jej rozwoju. 3. Bariery rozwojowe i patologie społeczno-gospodarcze neoliberalizmu w Polsce. 4. Instytucjonalizacja społecznej odpowiedzialności instytucji publicznych w kraju i UE. 5. Znaczenie norm społecznej odpowiedzialności organizacji i instytucji w funkcjonowaniu społeczeństwa. 6. Udział Policji i jej służby zwalczania cyberprzestępczości w rozwijaniu idei społecznej odpowiedzialności podmiotów społeczno-gospodarczych.	2	1	-	-	**3**	2	1	-	-	**3**
2.	Rola kapitału społecznego i instytucjonalnego w państwie demokratycznym oraz zadania Policji i służby zwalczania cyberprzestępczości w ich rozwoju	1. Definiowanie kapitału społecznego i instytucjonalnego oraz ich społeczne role. 2. Wewnętrzny i zewnętrzny kapitał społeczny Policji. 3. Funkcje zaufania, norm moralnych i wartości w kształtowaniu kapitału społecznego i instytucjonalnego w Polsce. 4. Pomiar kapitału społecznego i jego ocena w kraju. 5. Funkcje Policji w rozwoju kapitału społecznego, instytucjonalnego i obywatelskiego w kraju.	2	1	-	-	**3**	2	1	-	-	**3**

3.	Metody i sfery społecznego zaangażowania Policji, w tym służby zwalczania cyberprzestępczości na rzecz dobra publicznego	1. Prospołeczny zakres działania Policji, w tym służby zwalczania cyberprzestępczości w Polsce. 2. Dobro publiczne i jego znaczenie w życiu społeczeństw. 3. Metody i instrumenty stosowane przez Policję na rzecz kształtowania dobrostanu ludzi i organizacji. 4. Możliwe do stosowania metody i środki zwalczania cyberprzestępczości w kraju.	2	1	-	-	**3**	2	1	-	-	**3**
4.	Partnerska kultura *community policing* płaszczyzną funkcjonowania służby zwalczania cyberprzestępczości	1. Główne założenia idei *community policing, community justice* i partnerskiej *community policing.* 2. Patologie w funkcjonowaniu Policji, w tym służby zwalczania cyberprzestępczości. 3. Kierunki działania KGP na rzecz poprawy sprawności działania formacji i poprawy stanu bezpieczeństwa obywateli. 4. Zasady dobrych praktyk w funkcjonowaniu służby zwalczania cyberprzestępczości. 5. Reguły marketingu wewnętrznego Policji według koncepcji 11P i marketingu zewnętrznego według koncepcji 5W.	2	1	-	-	**3**	2	1	-	-	**3**
5.	Społeczna odpowiedzialność komunikacji marketingowej służby zwalczania cyberprzestępczości	1. Proces komunikacji marketingowej i jego modele. Kryteria wyboru form i środków komunikacji marketingowej służby zwalczania cyberprzestępczości. 2. Zasady informowania w sytuacjach kryzysowych. 3. Etyczne aspekty działań informacyjnych służby zwalczania cyberprzestępczości.	2	1	-	-	**3**	2	1	-	-	**3**
Razem:			**10**	**5**	-	-	**15**	**10**	**5**	-	-	**15**

Forma zakończenia (S)	**Zaliczenie z oceną**												
Efekty uczenia się	**Metody weryfikacji osiągania efektów uczenia się**												
	Egzamin pisemny	Egzamin ustny	Sprawdzian pisemny	Odpowiedź ustna	Referat	Prezentacja indywidualna	Prezentacja grupowa	Projekt indywidualny	Projekt grupowy	Samodzielna realizacja zdania praktycznego	Zespołowa realizacja zadania praktycznego	Aktywność na zajęciach	Test sprawności fizycznej
EU_1				x	x	x	x				x	x	
EU_2				x	x	x	x				x	x	
EU_3				x	x	x	x				x	x	
EU_4				x	x	x	x				x	x	
EU_5				x	x	x	x				x	x	
EU_6				x	x	x	x				x	x	
EU_7												x	
EU_8												x	
EU_9												x	

Nazwa przedmiotu: Analiza dowodów w środowisku cyfrowym				
Numer przedmiotu: 15	**Punkty ECTS:** 3	**Profil kształcenia:** praktyczny	**Dziedzina nauki/dyscyplina naukowa:** nauki społeczne/ nauki o bezpieczeństwie	**Język wykładowy:** polski

Efekty uczenia się		**Symbol kierunkowego efektu uczenia się**	**Symbol składnika opisu charakterystyki drugiego stopnia efektów uczenia się dla kwalifikacji na poziomach 6-7 PRK**	**Treści programowe**
w zakresie wiedzy				
EU_1	Zna tendencje rozwojowe w informatyce i rozumie ich wpływ na przetwarzanie i magazynowanie danych w komputerach.	K_W02 K_W14	P7S_WG	W1 L1
EU_2	Zna zaawansowane metody, techniki, narzędzia i materiały stosowane przy analizie elektronicznego materiału dowodowego.	K_W05 K_W06	P7S_WG	W2-5 L2-6
w zakresie umiejętności				
EU_3	Potrafi w sposób prawidłowy dobierać źródła informacji, dokonywać ich krytycznej analizy i ocenić przydatność danych do realizacji wybranego zagadnienia.	K_U07	P7S_UW	L1-6
EU_4	Potrafi analizować dane, a także umiejętnie interpretować otrzymane wyniki.	K_U13	P7S_UW	L1-6
EU_5	Potrafi posługiwać się oprogramowaniem do analizy śledczej.	K_U06 K_U07	P7S_UW	L1-6
EU_6	Potrafi odzyskiwać dane z obrazów fizycznych nośników elektronicznych.	K_U06	P7S_UW	L6
w zakresie kompetencji społecznych				
EU_7	Jest gotów do uznania znaczenia wiedzy w rozwiązywaniu problemów poznawczych i praktycznych w zakresie analizy dowodów w środowisku cyfrowym.	K_K01	P7S_KK	W1-5 L1-6
EU_8	Jest gotowy do zasięgania opinii ekspertów w przypadku trudności z samodzielnym rozwiązaniem problemu praktycznego.	K_K03	P7S_KK	W1-5 L1-6

Lp.	**Temat**	**Tezy**	**Forma studiów:**									
			stacjonarna					**niestacjonarna**				
			Łączna liczba godzin: 45					**Łączna liczba godzin: 35**				
			Wykłady	**Ćwiczenia**	**Zajęcia laboratoryjne**	**Warsztaty praktyczne**	**Razem**	**Wykłady**	**Ćwiczenia**	**Zajęcia laboratoryjne**	**Warsztaty praktyczne**	**Razem**
1.	Oprogramowanie do analizy śledczej	1. Podstawowe pojęcia związane z analizą śledczą: a) bit i system dwójkowy, b) system szesnastkowy, c) czas i jego zapis, d) wyrażenia regularne, e) funkcje skrótu, f) metadane. 2. Narzędzia i oprogramowanie.	2	-	5	-	**7**	1	-	4	-	**5**

2.	Analiza danych z przeglądarek internetowych, programów pocztowych i komunikatorów	1. Analiza danych z: a) przeglądarek internetowych, b) programów pocztowych, c) komunikatorów. 2. Wykorzystanie narzędzi open source: a) NirSoft, b)MiTeC.	2	-	5	-	**7**	2	-	4	-	**6**
3.	Analiza pamięci RAM, plików hiberfil.sys i pagefile.sys	1. Analiza pamięci z wykorzystaniem narzędzia Volatility. a) zaznajomienie się z narzędziem, b) zrozumienie szeregu poleceń, c) analiza pełnego przechwytu pamięci. 2. Analiza pliku hiberfil.sys. 3. Analiza pliku pagefile.sys.	2	-	6	-	**8**	2	-	4	-	**6**
4.	Analiza plików nieznanego typu	1. Rozpoznanie formatu plików i jego atrybutów. 2. Tworzenie bazy sygnatur i wyszukiwanie danych w oparciu o bazę sygnatur. 3. Analiza pliku binarnego w celu określenia struktury zawartych w nim danych. 4. Analiza pliku nieznanego typu w edytorze szesnastkowym.	2	-	5	-	**7**	2	-	4	-	**6**
5.	Analiza danych z urządzeń mobilnych	1. Analiza danych z urządzeń mobilnych. 2. Wykorzystanie oprogramowania XRY oraz UFED.	2	--	4	-	**6**	2	-	4	-	**6**
6.	Tworzenie i odczyt danych z obrazu nośnika danych	1. Praktyczne laboratoria z zakresu informatyki śledczej: a) podłączanie obrazu nośnika i przeglądanie zgromadzonych na nim danych, b) tworzenie obrazów nośników z wykorzystaniem blokerów sprzętowych i programowych, c) uruchomienie i praca z wykorzystaniem wirtualnych maszyn, d) wykorzystanie środowiska Sandboxie do analizy plików i programów.	-	-	10	-	**10**	-	-	6	-	**6**
		Razem:	**10**	-	**35**	-	**45**	**9**	-	**26**	-	**35**

Forma zakończenia (E)	**Egzamin**												
Efekty uczenia się	**Metody weryfikacji osiągania efektów uczenia się**												
	Egzamin pisemny	Egzamin ustny	Sprawdzian pisemny	Odpowiedź ustna	Referat	Prezentacja indywidualna	Prezentacja grupowa	Projekt indywidualny	Projekt grupowy	Samodzielna realizacja zdania praktycznego	Zespołowa realizacja zadania praktycznego	Aktywność na zajęciach	Test sprawności fizycznej
EU_1	x											x	
EU_2	x											x	
EU_3	x									x		x	
EU_4	x									x	x	x	
EU_5	x									x	x	x	
EU_6	x										x	x	
EU_7											x	x	
EU_8											x	x	

Nazwa przedmiotu: Testy penetracyjne IT				
Numer przedmiotu: 16	**Punkty ECTS:** 2	**Profil kształcenia:** praktyczny	**Dziedzina nauki/dyscyplina naukowa:** nauki społeczne/ nauki o bezpieczeństwie	**Język wykładowy:** polski

Efekty uczenia się		**Symbol kierunkowego efektu uczenia się**	**Symbol składnika opisu charakterystyki drugiego stopnia efektów uczenia się dla kwalifikacji na poziomach 6-7 PRK**	**Treści programowe**
w zakresie wiedzy				
EU_1	Zna i rozumie wybrane elementy modelu OSI/ISO sieci komputerowych.	K_W03	P7S_WG	W1-3 L2-3
EU_2	Zna i rozumie zaawansowane mechanizmy działania oraz stosowania zabezpieczeń w sieciach teleinformatycznych.	K_W06 K_W09	P7S_WG	W1-5 L2-5
EU_3	Zna i rozumie złożone metody monitorowania zabezpieczeń, detekcji intruzów, analizy logów i dzienników zdarzeń.	K_W05 K_W06	P7S_WG	W2-5 L2-5
w zakresie umiejętności				
EU_4	Potrafi skonfigurować narzędzia służące do testów penetracyjnych.	K_U06 K_U07	P7S_UW	L2-4
EU_5	Potrafi znaleźć i wykorzystać wybrane luki w zabezpieczeniach systemów oraz przeprowadzić testy penetracyjne.	K_U06 K_U07	P7S_UW	L2-4
EU_6	Potrafi dokonać oceny dokonanych testów penetracyjnych i sporządzić z nich raport.	K_U06 K_U07	P7S_UW	L5
w zakresie kompetencji społecznych				
EU_7	Jest gotów do uznania znaczenia wiedzy w rozwiązywaniu problemów poznawczych i praktycznych w zakresie testów penetracyjnych IT.	K_K01	P7S_KK	W1-5 L2-5
EU_8	Jest gotowy do zasięgania opinii ekspertów w przypadku trudności z samodzielnym rozwiązaniem problemu praktycznego.	K_K03	P7S_KK	W1-5 L2-5

Lp.	**Temat**	**Tezy**	**Forma studiów:**									
			stacjonarna					**niestacjonarna**				
			Łączna liczba godzin: 33					**Łączna liczba godzin: 27**				
			Wykłady	**Ćwiczenia**	**Zajęcia laboratoryjne**	**Warsztaty praktyczne**	**Razem**	**Wykłady**	**Ćwiczenia**	**Zajęcia laboratoryjne**	**Warsztaty praktyczne**	**Razem**
1.	Wprowadzenie do zagadnienia testu penetracyjnego	1. Przygotowanie do testów penetracyjnych. 2. Etyka i hacking. 3. Przygotowanie laboratorium. 4. Zarządzanie projektem testu penetracyjnego. 5. Generowanie wykresów 2D, 3D i ich eksport. 6. System składu tekstu - projekt.	2	-	-	-	**2**	2	-	-	-	**2**

2.	Zbieranie informacji	1. Pasywne zbieranie informacji. 2. Aktywne zbieranie informacji. 3. Wykrywanie luk w zabezpieczeniach. 4. Wykorzystanie luk w zabezpieczeniach.	3	-	5	-	**8**	2	-	5	-	**7**
3.	Eskalacja uprawnień	1. Ataki na hasła. 2. Podsłuchiwanie pakietów sieciowych. 3. Socjotechnika. 4. Manipulacje danymi dzienników zdarzeń. 5. Ukrywanie plików.	3	-	5	-	**8**	2	-	5	-	**7**
4.	Ataki na systemy pomocnicze	1. Ataki na bazy danych. 2. Ataki na sieci. 3. Ataki na aplikacje sieciowe.	5	-	5	-	**10**	2	-	5	-	**7**
5.	Prezentacja wyników testu	1. Raport wstępny. 2. Raport końcowy.	2	-	3	-	**5**	2	-	2	-	**4**
		Razem:	**15**	-	**18**	-	**33**	**10**	-	**17**	-	**27**

Forma zakończenia (S)	**Zaliczenie z oceną**												
Efekty uczenia się	**Metody weryfikacji osiągania efektów uczenia się**												
	Egzamin pisemny	Egzamin ustny	Sprawdzian pisemny	Odpowiedź ustna	Referat	Prezentacja indywidualna	Prezentacja grupowa	Projekt indywidualny	Projekt grupowy	Samodzielna realizacja zdania praktycznego	Zespołowa realizacja zadania praktycznego	Aktywność na zajęciach	Test sprawności fizycznej
EU_1			x	x							x	x	
EU_2			x	x							x	x	
EU_3			x	x							x	x	
EU_4			x								x	x	
EU_5			x								x	x	
EU_6			x								x	x	
EU_7											x	x	
EU_8											x	x	

Nazwa przedmiotu: Cyberprzestępstwa motywowane uprzedzeniami w ujęciu prawnomiędzynarodowym				
Numer przedmiotu: 17a	**Punkty ECTS:** 1	**Profil kształcenia:** praktyczny	**Dziedzina nauki/dyscyplina naukowa:** nauki społeczne/nauki prawne	**Język wykładowy:** polski

	Efekty uczenia się	**Symbol kierunkowego efektu uczenia się**	**Symbol składnika opisu charakterystyki drugiego stopnia efektów uczenia się dla kwalifikacji na poziomach 6-7 PRK**	**Treści programowe**
w zakresie wiedzy				
EU_1	Zna i rozumie istotę i specyfikę przestępstw z nienawiści, ze szczególnym uwzględnieniem przestępstw popełnianych w cyberprzestrzeni.	K_W01 K_W02	P7S_UW	W1-5 Ćw1-5
EU_2	Zna i rozumie zakres regulacji międzynarodowych aktów prawnych odnoszących się do karania i ścigania przestępstw z nienawiści.	K_W07	P7S_UW	W1-5 Ćw1-5
EU_3	Zna regulacje prawa humanitarnego odnoszące się do penalizacji zbrodni wojennych i ludobójstwa.	K_W07	P7S_UW	W1-5 Ćw1-5
w zakresie umiejętności				
EU_4	Potrafi w sposób prawidłowy dobierać źródła prawa międzynarodowego dotyczące przestępstw z nienawiści, ze szczególnym uwzględnieniem przestępstw popełnianych w cyberprzestrzeni oraz dokonywać ich krytycznej analizy w celu realizacji zadań typowych dla działalności zawodowej.	K_U08 K_U13 K_U14	P7S_UW	W1-5 Ćw1-5
EU_5	Potrafi kategoryzować poszczególne typy i rodzaje przestępstw z nienawiści, ze szczególnym uwzględnieniem przestępstw popełnianych w cyberprzestrzeni.	K_U08	P7S_UW	W1-5 Ćw1-5
w zakresie kompetencji społecznych				
EU_6	Jest gotów do uznawania wiedzy w rozwiązywaniu problemów prawnych oraz zasięgania opinii ekspertów w przypadku trudności z samodzielnym ich rozwiązaniem.	K_K01 K_K03	P7S_KK	W1-5 Ćw1-5

Lp.	**Temat**	**Tezy**	**Forma studiów:**									
			stacjonarna					**niestacjonarna**				
			Łączna liczba godzin: 20					**Łączna liczba godzin: 15**				
			Wykłady	**Ćwiczenia**	**Zajęcia laboratoryjne**	**Warsztaty praktyczne**	**Razem**	**Wykłady**	**Ćwiczenia**	**Zajęcia laboratoryjne**	**Warsztaty praktyczne**	**Razem**
1.	Prawnomiędzynarodowe standardy prawne dotyczące ścigania i karania przestępstw z nienawiści	1. Standardy ONZ. 2. Rada Europy wobec zwalczania przestępstw z nienawiści. 3. Standardy UE.	1	3	-	-	**4**	1	2	-	-	**3**

2.	Cyberprzestępstwa motywowane uprzedzeniem a zwalczanie międzynarodowej przestępczości zorganizowanej	1. Międzynarodowe standardy prawne dotyczące zwalczania przestępczości zorganizowanej w cyberprzestrzeni. 2. Przestępstwa motywowane uprzedzeniami a działalność zorganizowanych grup przestępczych.	2	2	-	-	**4**	1	2	-	-	**3**
3.	Orzecznictwo Europejskiego Trybunału Praw Człowieka a przestępstwa z nienawiści w cyberprzestrzeni	1. Zobowiązania pozytywne dla państw-stron w aspekcie zwalczania przestępstw motywowanych uprzedzeniami. 2. Standardy dotyczące czynności procesowych w zakresie przestępstw motywowanych uprzedzeniami.	1	3	-	-	**4**	1	2	-	-	**3**
4.	Prawo humanitarne wobec przestępstw motywowanych uprzedzeniami	1. Konflikty zbrojne motywowane uprzedzeniem. 2. Pojęcie zbrodni wojennej motywowanej uprzedzeniem i zbrodni ludobójstwa. 3. Przykłady orzeczeń trybunałów międzynarodowych w sprawach dotyczących odpowiedzialności za zbrodnie ludobójstwa.	2	2	-	-	**4**	1	2	-	-	**3**
5.	Zakaz dyskryminacji w prawie międzynarodowym a przestępstwa z nienawiści	1. Zakaz dyskryminacji jako naczelna zasada korzystania z praw człowieka. 2. Dyskryminacja a przestępstwa motywowane uprzedzeniami.	2	2	-	-	**4**	1	2	-	-	**3**
		Razem:	**8**	**12**	-	-	**20**	**5**	**10**	-	-	**15**

Forma zakończenia (S)	**Zaliczenie z oceną**												
Efekty uczenia się	**Metody weryfikacji osiągania efektów uczenia się**												
	Egzamin pisemny	Egzamin ustny	Sprawdzian pisemny	Odpowiedź ustna	Referat	Prezentacja indywidualna	Prezentacja grupowa	Projekt indywidualny	Projekt grupowy	Samodzielna realizacja zdania praktycznego	Zespołowa realizacja zadania praktycznego	Aktywność na zajęciach	Test sprawności fizycznej
EU_1			x	x			x			x	x	x	
EU_2			x	x			x			x	x	x	
EU_3			x	x			x			x	x	x	
EU_4			x	x			x			x	x	x	
EU_5			x	x			x			x	x	x	
EU_6												x	

Nazwa przedmiotu: Język w przestrzeni Internetu				
Numer przedmiotu: 17b	**Punkty ECTS:** 1	**Profil kształcenia:** praktyczny	**Dziedzina nauki/dyscyplina naukowa:** nauki społeczne/ nauki o bezpieczeństwie	**Język wykładowy:** polski

Efekty uczenia się		**Symbol kierunkowego efektu uczenia się**	**Symbol składnika opisu charakterystyki drugiego stopnia efektów uczenia się dla kwalifikacji na poziomach 6-7 PRK**	**Treści programowe**
w zakresie wiedzy				
EU_1	Zna i rozumie specjalistyczne pojęcia z dziedziny językoznawstwa i w zaawansowanym zakresie je wykorzystuje w działalności zawodowej.	K_W01	P7S_UW	W1-3
EU_2	Zna typy i gatunki wypowiedzi językowych oraz osobliwości językowe funkcjonujące w Internecie.	K_W01	P7S_UW	W1-4 Ćw3-5
EU_3	Rozumie poprawność ortograficzną, interpunkcyjną, stylistyczną, leksykalną, fleksyjną i składniową tekstów funkcjonujących Internecie.	K_W01 K_W17	P7S_UW P7S_WK	W3 Ćw3
w zakresie umiejętności				
EU_4	Potrafi posługiwać się językiem jako narzędziem komunikowania się w działalności zawodowej ze zróżnicowanym kręgiem odbiorców.	K_U18 K_U19 K_U21	P7S_UK	W1-4 Ćw2-5
EU_5	Potrafi sprawnie, etycznie i z zachowaniem zasad poprawności językowej komunikować się z otoczeniem z użyciem specjalistycznej terminologii w zakresie cyberprzestępczości.	K_U18 K_U19 K_U21	P7S_UK	W1-4 Ćw3-5
w zakresie kompetencji społecznych				
EU_6	Jest gotów do inicjowania działań komunikacyjnych na rzecz interesu publicznego, w tym na rzecz podnoszenia społecznego poziomu języka w Internecie.	K_K05	P7S_KO	W1-4 Ćw3-5

Lp.	Temat	Tezy	Forma studiów:									
			stacjonarna					niestacjonarna				
			Łączna liczba godzin: 20					Łączna liczba godzin: 15				
			Wykłady	Ćwiczenia	Zajęcia laboratoryjne	Warsztaty praktyczne	Razem	Wykłady	Ćwiczenia	Zajęcia laboratoryjne	Warsztaty praktyczne	Razem
1.	Wyjaśnienie podstawowych pojęć. Właściwości komunikacji językowej w Internecie	1.Wyjaśnienie pojęć: język, norma językowa, błąd językowy, uzus, idiolekt. 2. Wyjaśnienie pojęć: mowa, pismo, tekst. 3. Wyjaśnienie pojęć: Internet, komunikacja internetowa. 4. Dialogowość, spontaniczność, sytuacyjność, trwałość, zasięg, multimedialność, trwałość, zasięg, multimedialność, hipertekstowość, hierarchiczność, automatyzacja, dynamiczność oraz inne właściwości.	2	-	-	-	**2**	2	-	-	-	**2**
2.	Typy i gatunki wypowiedzi językowych funkcjonujących w Internecie	1. Tematyka i cele wypowiedzi internetowych. 2. Wypowiedzi nieoficjalne, konwersacyjne (czaty, pogawędki). 3. Wypowiedzi oficjalne, m.in. korespondencja elektroniczna. 4. Wypowiedzi hipertekstowe (witryny, blogi). 5. Gatunki tekstów internetowych.	2	2	-	-	**4**	1	1	-	-	**2**
3.	Poprawność językowa tekstów funkcjonujących Internecie wybrane zagadnienia	1. Poprawność ortograficzna oraz interpunkcyjna. 2. Poprawność stylistyczna. 3. Poprawność leksykalna i fleksyjna. 4. Poprawność składniowa.	2	4	-	-	**6**	1	4	-	-	**5**
4.	Osobliwości językowe wypowiedzi funkcjonujących w Internecie	1. Modyfikacje pisowni oraz interpunkcji. 2. Adresy elektroniczne, pseudonimy, emotikony oraz akronimy jako leksyka internetowa. 3. Osobliwości stylistyczne i pragmatyczne języka w Internecie. 4. Internet a szanse i zagrożenia dla języka.	2	2	-	-	**4**	1	2	-	-	**3**

5.	Wypowiedź językowa w Internecie jako ślad zostawiony przez przestępcę	1. Zadania lingwistyki kryminalistycznej. 2. Przydatność interpretacji językoznawczej wypowiedzi internetowych w praktyce organów ścigania - wybrane przykłady.	-	4	-	-	**4**	-	3	-	-	**3**
		Razem:	**8**	**12**	**-**	**-**	**20**	**5**	**10**	**-**	**-**	**15**

Forma zakończenia (S)	**Zaliczenie z oceną**												
Efekty uczenia się	**Metody weryfikacji osiągania efektów uczenia się**												
	Egzamin pisemny	Egzamin ustny	Sprawdzian pisemny	Odpowiedź ustna	Referat	Prezentacja indywidualna	Prezentacja grupowa	Projekt indywidualny	Projekt grupowy	Samodzielna realizacja zdania praktycznego	Zespołowa realizacja zadania praktycznego	Aktywność na zajęciach	Test sprawności fizycznej
EU_1			x	x								x	
EU_2			x	x								x	
EU_3			x							x	x	x	
EU_4										x	x	x	
EU_5										x	x	x	
EU_6										x	x	x	

Nazwa przedmiotu: Wybrane czynności procesowo-kryminalistyczne				
Numer przedmiotu: 18	**Punkty ECTS:** 1	**Profil kształcenia:** praktyczny	**Dziedzina nauki/dyscyplina naukowa:** nauki społeczne/nauki prawne	**Język wykładowy:** polski

Efekty uczenia się		**Symbol kierunkowego efektu uczenia się**	**Symbol składnika opisu charakterystyki drugiego stopnia efektów uczenia się dla kwalifikacji na poziomach 6-7 PRK**	**Treści programowe**
w zakresie wiedzy				
EU_1	Zna i rozumie zasady fotografii kryminalistycznej i w zaawansowanym zakresie wykorzystuje je w działalności zawodowej.	K_W02 K_W03	P7S_WG	W1 Ćw1
EU_2	Zna i rozumie zróżnicowane metody i narzędzia ujawniania oraz procesowego i technicznego zabezpieczania dowodów przestępstw.	K_W05 K_W06 K_W08	P7S_WG	W2-3 Ćw2-3
w zakresie umiejętności				
EU_3	Potrafi w sposób prawidłowy zastosować wybrane metody i narzędzia oraz techniki w toku wykonywanych zadań związanych z ujawnianiem i zabezpieczaniem śladów kryminalistycznych.	K_U03 K_U06 K_U09	P7S_UW	W1-3 Ćw1-3
EU_4	Potrafi prawidłowo udokumentować czynności zabezpieczające miejsce zdarzenia oraz wybrane czynności procesowe.	K_U09 K_U10 K_U19	P7S_UW P7S_UK	W1-3 Ćw1-3
w zakresie kompetencji społecznych				
EU_5	Jest gotów do odpowiedzialnego pełnienia roli zawodowej i rozwiązywania problemów związanych z pracą w zespołach zabezpieczających miejsce zdarzenia.	K_K07	P7S_KR	W1-3 Ćw1-3

Lp.	**Temat**	**Tezy**	**Forma studiów:**									
			stacjonarna					**niestacjonarna**				
			Łączna liczba godzin: 20					**Łączna liczba godzin: 20**				
			Wykłady	**Ćwiczenia**	**Zajęcia laboratoryjne**	**Warsztaty praktyczne**	**Razem**	**Wykłady**	**Ćwiczenia**	**Zajęcia laboratoryjne**	**Warsztaty praktyczne**	**Razem**
1.	Fotografia kryminalistyczna	1. Fotografia dokumentacyjna. 2. Techniki fotografowania: a) panorama liniowa, b) panorama obrotowa, c) rejestracja obrazu w trudnych warunkach oświetleniowych.	2	4	-	-	**6**	2	4	-	-	**6**
2.	Wybrane procesowo-kryminalistyczne czynności dowodowe	1. Kryminalistyczne badanie miejsca zdarzenia. 2. Ekspertyza kryminalistyczna.	3	6	-	-	**9**	3	6	-	-	**9**

3.	Zabezpieczenie wybranych urządzeń rejestrujących	1. Procesowe i techniczne zabezpieczenie tachografów. 2. Ujawnianie i zabezpieczanie urządzeń rejestrujących obraz i dźwięk w pojazdach. 3. Zabezpieczanie urządzeń rejestrujących obraz w obrębie miejsc zdarzeń.	1	4	-	-	**5**	1	4	-	-	**5**
		Razem:	**6**	**14**	-	-	**20**	**6**	**14**	-	-	**20**

Forma zakończenia (S)	**Zaliczenie z oceną**												
Efekty uczenia się	**Metody weryfikacji osiągania efektów uczenia się**												
	Egzamin pisemny	Egzamin ustny	Sprawdzian pisemny	Odpowiedź ustna	Referat	Prezentacja indywidualna	Prezentacja grupowa	Projekt indywidualny	Projekt grupowy	Samodzielna realizacja zdania praktycznego	Zespołowa realizacja zadania praktycznego	Aktywność na zajęciach	Test sprawności fizycznej
EU_1			x	x						x	x	x	
EU_2			x	x						x	x	x	
EU_3			x	x						x	x	x	
EU_4			x	x						x	x	x	
EU_5										x	x	x	

Nazwa przedmiotu: Organizacja i funkcjonowanie podmiotów właściwych w sprawach bezpieczeństwa i porządku publicznego				
Numer przedmiotu: 19	**Punkty ECTS:** 1	**Profil kształcenia:** praktyczny	**Dziedzina nauki/dyscyplina naukowa:** nauki społeczne/nauki o bezpieczeństwie	**Język wykładowy:** polski

Efekty uczenia się		**Symbol kierunkowego efektu uczenia się**	**Symbol składnika opisu charakterystyki drugiego stopnia efektów uczenia się dla kwalifikacji na poziomach 6-7 PRK**	**Treści programowe**
w zakresie wiedzy				
EU_1	Zna i rozumie zróżnicowane teorie z zakresu zjawisk społecznych wywierających wpływ na funkcjonowanie jednostek i komórek organizacyjnych odpowiedzialnych za cyberbezpieczeństwo.	K_W01 K_W02	P7S_WG	W1-5 Ćw1-5
EU_2	Zna i rozumie uwarunkowania różnych rodzajów działalności zawodowej związanej z funkcjonowaniem jednostek i komórek organizacyjnych odpowiedzialnych za cyberbezpieczeństwo w tym zasady, metody i narzędzia z zakresu zarządzania zmianą, marketingowego, jakością oraz projektem.	K_W11 K_W16	P7S_WG P7S_WK	W1-5 Ćw1-5
w zakresie umiejętności				
EU_3	Potrafi wykorzystać posiadaną wiedzę z zakresu zarządzania zmianą, marketingowego, jakością oraz projektem na rzecz analizowania zjawisk, zagrożeń oraz procesów społecznych oraz formułowania i rozwiązywania złożonych problemów związanych z funkcjonowaniem jednostek i komórek organizacyjnych odpowiedzialnych za cyberbezpieczeństwo.	K_U01 K_U12	P7S_UW	W1-5 Ćw1-5
EU_4	Potrafi planować i organizować pracę indywidualną oraz w zespole i współpracować w ramach prac zespołowych w jednostkach i komórkach organizacyjnych odpowiedzialnych za cyberbezpieczeństwo.	K_U22	P7S_UO	W1-5 Ćw1-5
w zakresie kompetencji społecznych				
EU_5	Jest gotów do wypełniania zobowiązań społecznych, inspirowania i organizowania działalności na rzecz środowiska społecznego, myślenia i działania w sposób przedsiębiorczy.	K_K04	P7S_KO	Ćw1-5
EU_6	Jest gotów do odpowiedzialnego pełnienia ról zawodowych w jednostkach i komórkach organizacyjnych odpowiedzialnych za cyberbezpieczeństwo, z uwzględnieniem zmieniających się potrzeb społecznych, w tym: rozwijania dorobku zawodu, podtrzymywania etosu zawodu, przestrzegania i rozwijania zasad etyki zawodowej oraz działania na rzecz przestrzegania tych zasad.	K_K07	P7S_KR	Ćw1-5

Lp.	Temat	Tezy	Forma studiów:									
			stacjonarna					niestacjonarna				
			Łączna liczba godzin: 20					Łączna liczba godzin: 15				
			Wykłady	Ćwiczenia	Zajęcia laboratoryjne	Warsztaty praktyczne	Razem	Wykłady	Ćwiczenia	Zajęcia laboratoryjne	Warsztaty praktyczne	Razem
1.	Wybrane zagadnienia wprowadzające do problematyki organizacji i zarządzania	1. Rola teorii w zarządzaniu organizacją. 2. Zarządzanie i praca kierownika. 3. Charakterystyczne cechy współczesnego zarządzania organizacjami.	1	2			**3**	1	2	-	-	**3**
2.	Zarządzanie zmianą i rozwojem organizacji	1. Cykl życia organizacji. 2. Zmiany w otoczeniu i ich wpływ na funkcjonowanie i rozwój organizacji. 3. Rodzaje zmian organizacyjnych i opory wobec ich wprowadzania.	2	3			**5**	1	2	-	-	**3**
3.	Zarządzanie jakością	1. Zarządzanie jakością. 2. Systemy zarządzania jakością. 3. Metody i techniki doskonalenia funkcjonowania organizacji.	2	3	-	-	**5**	1	2	-	-	**3**
4.	Zarządzanie marketingowe	1. Pojęcie marketingu i jego miejsce w funkcjonowaniu organizacji. 2. Kompozycja marketingowa (marketing mix). 3. Komunikacja marketingowa.	2	2	-	-	**4**	1	2	-	-	**3**
5.	Zarządzanie projektem	1. Inicjacja projektu 2. Planowanie i realizacja projektu. 3. Kontrola i zamknięcie projektu.	1	2	-	-	**3**	1	2	-	-	**3**
		Razem:	**8**	**12**	-	-	**20**	**5**	**10**	-	-	**15**

Forma zakończenia (S)	**Zaliczenie z oceną**												
Efekty uczenia się	**Metody weryfikacji osiągania efektów uczenia się**												
	Egzamin pisemny	Egzamin ustny	Sprawdzian pisemny	Odpowiedź ustna	Referat	Prezentacja indywidualna	Prezentacja grupowa	Projekt indywidualny	Projekt grupowy	Samodzielna realizacja zdania praktycznego	Zespołowa realizacja zadania praktycznego	Aktywność na zajęciach	Test sprawności fizycznej
EU_1				x	x		x				x		
EU_2				x	x		x				x		
EU_3				x	x		x				x		
EU_4				x	x		x				x		
EU_5				x			x				x		
EU_6				x			x				x		

Nazwa przedmiotu: Odzyskiwanie i analiza danych z nośników cyfrowych				
Numer przedmiotu: 20	**Punkty ECTS:** 2	**Profil kształcenia:** praktyczny	**Dziedzina nauki/dyscyplina naukowa:** nauki społeczne/ nauki o bezpieczeństwie	**Język wykładowy:** polski

	Efekty uczenia się	**Symbol kierunkowego efektu uczenia się**	**Symbol składnika opisu charakterystyki drugiego stopnia efektów uczenia się dla kwalifikacji na poziomach 6-7 PRK**	**Treści programowe**
w zakresie wiedzy				
EU_1	Zna procedury, zasady oraz specyfikę postępowania z elektronicznymi nośnikami danych.	K_W06 K_W09	P7S_UW	W1-2 L1-2
EU_2	Zna możliwości i zastosowania darmowych oraz komercyjnych aplikacji do odzyskiwania danych cyfrowych.	K_W06 K_W14	P7S_UW	W3-4 L3-4
w zakresie umiejętności				
EU_3	Potrafi dokonać rozróżnienia nośników danych w celu wybrania optymalnej metody odzyskiwania danych.	K_U03	P7S_UW	L1-2
EU_4	Potrafi dobrać optymalną metodę odzysku danych w zależności od rodzaju nośnika i systemu zapisu plików.	K_U06 K_U07	P7S_UW	L3
EU_5	Potrafi odzyskać dane z nośników elektronicznych.	K_U06 K_U07	P7S_UW	L4
w zakresie kompetencji społecznych				
EU_6	Jest gotów do uznawania wiedzy w rozwiązywaniu problemów z zakresu odzyskiwania i analizy danych z nośników cyfrowych oraz zasięgania opinii ekspertów w przypadku trudności z samodzielnym ich rozwiązaniem.	K_K01 K_K03	P7S_KK	W1-4 L1-4

Lp.	**Temat**	**Tezy**	**Forma studiów:**									
			stacjonarna					**niestacjonarna**				
			Łączna liczba godzin: 35					**Łączna liczba godzin: 26**				
			Wykłady	**Ćwiczenia**	**Zajęcia laboratoryjne**	**Warsztaty praktyczne**	**Razem**	**Wykłady**	**Ćwiczenia**	**Zajęcia laboratoryjne**	**Warsztaty praktyczne**	**Razem**
1.	Cyfrowe nośniki informacji	1. Podstawowe pojęcia związane z nośnikami cyfrowymi. 2. Budowa i sposób zapisu danych na nośnikach cyfrowych: a) nośniki magnetyczne, b) nośniki optyczne, c) nośniki elektroniczne (półprzewodnikowe).	2	-	2	-	**4**	2	-	2	-	**4**
2.	Budowa i zasady działania pamięci masowych	1. Dyski HDD. 2. Dyski SSD. 3. Inne systemy pamięci masowej. 4. Struktura logiczna dysku.	2	-	2	-	**4**	2	-	2	-	**4**

3.	Systemy zapisu plików	1. Podstawowe funkcje systemu plików. 2. System FAT 32 (atrybuty, budowa, funkcjonalność). 3. System NTFS (atrybuty, budowa, funkcjonalność). 4. Zalety i wady podstawowych systemów plików.	4	-	8	-	**12**	2	-	4	-	**6**
4.	Odzyskiwanie danych z elektronicznych nośników pamięci	1. Narzędzia stosowane od odzysku danych cyfrowych. 2. Odzyskiwanie danych: a) z urządzeń mobilnych, b) usuniętych z dysku, c) ze sformatowanego nośnika, d) z innych nośników.	2	-	13	-	**15**	2	-	10	-	**12**
		Razem:	**10**	-	**25**	-	**35**	**8**	-	**18**	-	**26**

Forma zakończenia (E)	**Egzamin**												
Efekty uczenia się	**Metody weryfikacji osiągania efektów uczenia się**												
	Egzamin pisemny	Egzamin ustny	Sprawdzian pisemny	Odpowiedź ustna	Referat	Prezentacja indywidualna	Prezentacja grupowa	Projekt indywidualny	Projekt grupowy	Samodzielna realizacja zdania praktycznego	Zespołowa realizacja zadania praktycznego	Aktywność na zajęciach	Test sprawności fizycznej
EU_1	x			x								x	
EU_2	x			x								x	
EU_3	x									x		x	
EU_4	x									x		x	
EU_5										x		x	
EU_6										x		x	

Nazwa przedmiotu: Kryptowaluty				
Numer przedmiotu: 21	**Punkty ECTS:** 2	**Profil kształcenia:** praktyczny	**Dziedzina nauki/dyscyplina naukowa:** nauki społeczne/nauki o bezpieczeństwie	**Język wykładowy:** polski

Efekty uczenia się		**Symbol kierunkowego efektu uczenia się**	**Symbol składnika opisu charakterystyki drugiego stopnia efektów uczenia się dla kwalifikacji na poziomach 6-7 PRK**	**Treści programowe**
w zakresie wiedzy				
EU_1	Zna mechanizmy powstawania i rozumie funkcjonowanie kryptowalut.	K_W02 K_W14	P7S_WG P7S_WK	W1-3
EU_2	Zna i rozumie istotę zastosowania technologii blockchain.	K_W06	P7S_WG	W1-3
EU_3	Zna i rozumie zasady funkcjonowania giełd kryptowalutowych.	K_W02 K_W06 K_W14	P7S_WG P7S_WK	L3-6
w zakresie umiejętności				
EU_4	Potrafi posługiwać się wybranymi kryptowalutami.	K_U02 K_U07 K_U11	P7S_UW	L3-6
EU_5	Potrafi użyć ogólnodostępnych narzędzi do analizy i śledzenia wybranych kryptowalt.	K_U05	P7S_UW	L3-6
EU_6	Potrafi technicznie i procesowo zabezpieczać wybrane kryptowaluty.	K_U08 K_U09	P7S_UW	L3-6
w zakresie kompetencji społecznych				
EU_7	Jest gotów do krytycznej oceny posiadanej wiedzy z zakresu kryptowalut.	K_K02	P7S_KK	W1-3 L3-6
EU_8	Jest gotów do uznawania wiedzy w rozwiązywaniu problemów z zakresu kryptowalut oraz zasięgania opinii ekspertów w przypadku trudności z samodzielnym ich rozwiązaniem.	K_K03	P7S_KK	W1-3 L3-6

Lp.	**Temat**	**Tezy**	**Forma studiów:**									
			stacjonarna					**niestacjonarna**				
			Łączna liczba godzin: 30					**Łączna liczba godzin: 20**				
			Wykłady	**Ćwiczenia**	**Zajęcia laboratoryjne**	**Warsztaty praktyczne**	**Razem**	**Wykłady**	**Ćwiczenia**	**Zajęcia laboratoryjne**	**Warsztaty praktyczne**	**Razem**
1.	Geneza kryptowalut	1. Geneza i początek bitcoina. 2. Powstanie altcoinów. 3. Rozwój i dalsza przyszłość kryptowalut.	4	-	-	-	**4**	2	-	-	-	**2**
2.	Wybrane kryptowaluty i mechanizmy ich funkcjonowania	1. BTC – Bitcoin. 2. ETH – Ethereum. 3. XMR – Monero. 4. Altcoiny.	6	-	-	-	**6**	4	-	-	-	**4**
3.	Portfele	1. Programowe. 2. Sprzętowe. 3. Online.	2	-	-	4	**6**	2	-	-	4	**6**
4.	Giełdy	1. Polskie. 2. Zagraniczne.	-	-	-	4	**4**	-	-	-	2	**2**
5.	Analiza kryptowalut	1. Aspekty ekonomiczne. 2. Zastosowanie. 3. Bezpieczenstwo.	-	-	-	4	**4**	-	-	-	2	**2**

6.	Zabezpieczanie kryptowalut	1. Techniczne. 2. Procesowe.	2	-	-	4	**6**	2	-	-	2	**4**
		Razem:	**14**	-	-	**16**	**30**	**10**	-	-	**10**	**20**

Forma zakończenia (S)	**Zaliczenie z oceną**												
Efekty uczenia się	**Metody weryfikacji osiągania efektów uczenia się**												
	Egzamin pisemny	Egzamin ustny	Sprawdzian pisemny	Odpowiedź ustna	Referat	Prezentacja indywidualna	Prezentacja grupowa	Projekt indywidualny	Projekt grupowy	Samodzielna realizacja zdania praktycznego	Zespołowa realizacja zadania praktycznego	Aktywność na zajęciach	Test sprawności fizycznej
EU_1			x	x								x	
EU_2			x	x								x	
EU_3			x	x								x	
EU_4			x							x		x	
EU_5			x							x		x	
EU_6			x							x		x	
EU_7										x		x	
EU_8										x		x	

Nazwa przedmiotu: Laboratorium statystyczne				
Numer przedmiotu: 22	**Punkty ECTS:** 2	**Profil kształcenia:** praktyczny	**Dziedzina nauki/dyscyplina naukowa:** nauki społeczne/ nauki o bezpieczeństwie	**Język wykładowy:** polski

Efekty uczenia się		**Symbol kierunkowego efektu uczenia się**	**Symbol składnika opisu charakterystyki drugiego stopnia efektów uczenia się dla kwalifikacji na poziomach 6-7 PRK**	**Treści programowe**
w zakresie wiedzy				
EU_1	Zna zróżnicowane metody statystyki oraz rozumowania logicznego i ich praktyczne zastosowanie w działalności zawodowej.	K_W03	P7S_WG	W1
EU_2	Zna i rozumie rolę analizy informacji w procesie wykrywczym.	K_W03 K_W04 K_W05	P7S_WG	W1
w zakresie umiejętności				
EU_3	Potrafi przygotować dane i wykorzystać w tym celu oprogramowanie pomocnicze.	K_U03 K_U07	P7S_UW	L2
EU_4	Potrafi wykorzystywać narzędzia informatyczne w zakresie analizy danych.	K_U06 K_U07	P7S_UW	L2
EU_5	Potrafi prowadzić wnioskowania statystyczne, także z wykorzystaniem narzędzi komputerowych.	K_U06 K_U07 K_U13	P7S_UW	L2
w zakresie kompetencji społecznych				
EU_6	Jest gotów do uznawania wiedzy w rozwiązywaniu problemów z zakresu analizy informacji w procesie wykrywczym oraz zasięgania opinii ekspertów w przypadku trudności z samodzielnym ich rozwiązaniem.	K_K01 K_K03	P7S_KK	W1 L2

Lp.	**Temat**	**Tezy**	**Forma studiów:**									
			stacjonarna					**niestacjonarna**				
			Łączna liczba godzin: 30					**Łączna liczba godzin: 20**				
			Wykłady	**Ćwiczenia**	**Zajęcia laboratoryjne**	**Warsztaty praktyczne**	**Razem**	**Wykłady**	**Ćwiczenia**	**Zajęcia laboratoryjne**	**Warsztaty praktyczne**	**Razem**
1.	Wstęp do analizy statystycznej	1. Podstawowe pojęcia statystyczne. 2. Oprogramowanie do analiz statystycznych.	2	-	-	-	**2**	2	-	-	-	**2**
2.	Analizy statystyczne	1. Przygotowanie danych do analizy. 2. Analizy statystyczne. 3. Wizualizacja i raportowanie wyników analiz statystycznych.	-	-	28	-	**28**	-	-	18	-	**18**
		Razem:	**2**	-	**28**	-	**30**	**2**	-	**18**	-	**20**

Forma zakończenia (E)	**Egzamin**												
Efekty uczenia się	**Metody weryfikacji osiągania efektów uczenia się**												
	Egzamin pisemny	Egzamin ustny	Sprawdzian pisemny	Odpowiedź ustna	Referat	Prezentacja indywidualna	Prezentacja grupowa	Projekt indywidualny	Projekt grupowy	Samodzielna realizacja zdania praktycznego	Zespołowa realizacja zadania praktycznego	Aktywność na zajęciach	Test sprawności fizycznej
EU_1	x			x		x			x			x	
EU_2	x			x		x			x			x	
EU_3	x			x		x			x			x	
EU_4	x			x		x			x			x	
EU_5	x			x		x			x			x	
EU_6												x	

Nazwa przedmiotu: Technologie chmur obliczeniowych				
Numer przedmiotu: 23	**Punkty ECTS:** 3	**Profil kształcenia:** praktyczny	**Dziedzina nauki/dyscyplina naukowa:** nauki społeczne/ nauki prawne	**Język wykładowy:** polski

Efekty uczenia się		**Symbol kierunkowego efektu uczenia się**	**Symbol składnika opisu charakterystyki drugiego stopnia efektów uczenia się dla kwalifikacji na poziomach 6-7 PRK**	**Treści programowe**
w zakresie wiedzy				
EU_1	Zna i rozumie regulacje prawne oraz rozwiązania instytucjonalne istotne w kontekście pozyskiwania dowodów z chmur obliczeniowych.	K_W07 K_W10	P7S_WG	W1, 3 Ćw1, 3
EU_2	Zna wybrane inicjatywy europejskie dotyczące chmur obliczeniowych w walce z cyberprzestępczością.	K_W06 K_W14	P7S_WG	W2 Ćw2
EU_3	Zna funkcjonalność chmur obliczeniowych oraz możliwości zabezpieczania danych z nich.	K_W06 K_W09	P7S_WG	W4 L4
w zakresie umiejętności				
EU_4	Potrafi interpretować przepisy prawne istotne w kontekście gromadzenia i zabezpieczania danych z usług chmur obliczeniowych.	K_U08	P7S_UW	Ćw1-3
EU_5	Potrafi korzystać z narzędzi informatyki kryminalistycznej w warstwie wirtualizacji danych.	K_U03 K_U06	P7S_UW	L4
EU_6	Potrafi zabezpieczać dane z systemów wirtualnych.	K_U07	P7S_UW	L4
w zakresie kompetencji społecznych				
EU_7	Jest gotów dokonać krytycznej oceny posiadanej wiedzy z zakresu technologii informatycznych.	K_K02	P7S_KK	W1-4 Ćw1-3 L4

Lp.	**Temat**	**Tezy**	**Forma studiów:**									
			stacjonarna					**niestacjonarna**				
			Łączna liczba godzin: 45					**Łączna liczba godzin: 35**				
			Wykłady	**Ćwiczenia**	**Zajęcia laboratoryjne**	**Warsztaty praktyczne**	**Razem**	**Wykłady**	**Ćwiczenia**	**Zajęcia laboratoryjne**	**Warsztaty praktyczne**	**Razem**
1.	Międzynarodowe uregulowania prawne i rozwiązania instytucjonalne istotne w kontekście pozyskiwania dowodów z chmur obliczeniowych	1. Problematyka gromadzenie dowodów elektronicznych – ilustracja problematyki. 2. Inicjatywy międzynarodowe na rzecz współpracy w walce z cyberprzestępczością. 3. Instrumenty prawne współpracy międzynarodowej.	2	3	-	-	**5**	2	2	-	-	**4**
2.	Inicjatywy europejskie w walce z cyberprzestępczością	1. Działania Rady Europy w kontekście problematyki transgranicznego dostępu do danych elektronicznych i jurysdykcji. 2. Działania Unii Europejskiej w kontekście problematyki transgranicznego dostępu do danych i jurysdykcji.	2	3	-	-	**5**	2	2	-	-	**4**

3.	Krajowe regulacje prawne istotne w kontekście pozyskiwania i analizy danych z chmur obliczeniowych	1. Ustawa z dnia 6 czerwca 1997 r. - Kodeks karny. 2. Ustawa z dnia 6 czerwca 1997 r. – Kodeks. postępowania karnego 3. Ustawa z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne. 4. Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną. 5. Ustawa z dnia 6 kwietnia 1990 r. o Policji.	2	4	-	-	**6**	2	4	-	-	**6**
4.	Informatyka kryminalistyczna w środowisku chmur obliczeniowych	1. Zdalne zabezpieczanie danych z systemów wirtualnych. 2. Narzędzia informatyki kryminalistycznej w warstwie wirtualizacji danych. 3. Zabezpieczanie danych z urządzeń mobilnych oraz systemów komputerowych w kontekście usług chmur obliczeniowych.	4	-	25	-	**29**	2	-	19	-	**21**
		Razem:	**10**	**10**	**25**	-	**45**	**8**	**8**	**19**	-	**35**

Forma zakończenia (E)	**Egzamin**												
Efekty uczenia się	**Metody weryfikacji osiągania efektów uczenia się**												
	Egzamin pisemny	Egzamin ustny	Sprawdzian pisemny	Odpowiedź ustna	Referat	Prezentacja indywidualna	Prezentacja grupowa	Projekt indywidualny	Projekt grupowy	Samodzielna realizacja zdania praktycznego	Zespołowa realizacja zadania praktycznego	Aktywność na zajęciach	Test sprawności fizycznej
EU_1	x							x		x	x	x	
EU_2	x							x		x	x	x	
EU_3	x							x		x	x	x	
EU_4	x							x		x	x	x	
EU_5	x							x		x	x	x	
EU_6	x							x		x	x	x	
EU_7								x		x	x	x	

Nazwa przedmiotu: Współpraca międzynarodowa Policji w zakresie zapobiegania i zwalczania przestępczości				
Numer przedmiotu: 24a	**Punkty ECTS:** 1	**Profil kształcenia:** praktyczny	**Dziedzina nauki/dyscyplina naukowa:** nauki społeczne/ nauki prawne	**Język wykładowy:** polski

Efekty uczenia się		**Symbol kierunkowego efektu uczenia się**	**Symbol składnika opisu charakterystyki drugiego stopnia efektów uczenia się dla kwalifikacji na poziomach 6-7 PRK**	**Treści programowe**
w zakresie wiedzy				
EU_1	Zna i rozumie rolę oraz zakres działania instytucji międzynarodowych odpowiedzialnych za współpracę w zakresie zapobiegania i zwalczania przestępczości.	K_W02 K_W10 K_W13	P7S_WG	W1-4 Ćw1-4
EU_2	Zna i rozumie relacje między polskimi i międzynarodowymi podmiotami i instytucjami odpowiedzialnymi za międzynarodową współpracę w zakresie zapobiegania i zwalczania przestępczości.	K_W02 K_W10 K_W13	P7S_WG	W1-4 Ćw1-4
w zakresie umiejętności				
EU_3	Potrafi w sposób prawidłowy analizować przepisy z zakresu międzynarodowej współpracy w zakresie zapobiegania i zwalczania przestępczości.	K_U08 K_U19	P7S_UW P7S_UK	W1-4 Ćw1-4
w zakresie kompetencji społecznych				
EU_4	Jest gotów do odpowiedzialnego pełnienia roli zawodowej z uwzględnieniem zmieniających się potrzeb społecznych i inicjowania działań na interesu publicznego.	K_K04 K_K05 K_K07	P7S_KK P7S_KR	Ćw1-4

Lp.	**Temat**	**Tezy**	**Forma studiów:**									
			stacjonarna					**niestacjonarna**				
			Łączna liczba godzin: 20					**Łączna liczba godzin: 20**				
			Wykłady	**Ćwiczenia**	**Zajęcia laboratoryjne**	**Warsztaty praktyczne**	**Razem**	**Wykłady**	**Ćwiczenia**	**Zajęcia laboratoryjne**	**Warsztaty praktyczne**	**Razem**
1.	Przesłanki współpracy międzynarodowej Policji w zakresie zwalczania międzynarodowej przestępczości zorganizowanej	1. Globalizacja i rozwój międzynarodowej przestępczości. 2. Współczesny stan zagrożenia międzynarodową przestępczością zorganizowaną i cyberprzestępczością. 3. Formy i przedmiotowy zakres współpracy Policji. 4. Struktura i zadania KGP we współpracy policyjnej. 5. Oficerowie łącznikowi.	2	3	-	-	**5**	2	3	-	-	**5**

2.	Zwalczanie przestępczości zorganizowanej na szczeblu ONZ	1. Rola ONZ w zwalczaniu przestępczości zorganizowanej. 2. Najważniejsze traktaty dotyczące zwalczania przestępczości zorganizowanej. 3. Narzędzia i formy współpracy międzynarodowej.	2	3	-	-	**5**	2	3	-	-	**5**
3.	Działania Rady Europy wobec zwalczania przestępczości zorganizowanej, w tym cyberprzestępczości	1. Prawa człowieka zobowiązania państw do zwalczania przestępczości zorganizowanej. 2. Najważniejsze narzędzia prawne Rady Europy. 3. Szczególne implikacje Konwencji budapesztańskiej w kontekście walki z cyberprzestępczością.	2	3	-	-	**5**	2	3	-	-	**5**
4.	Współpraca międzynarodowa Policji na szczeblu UE	1. Rola Europolu. 2. System Schengen a współpraca międzynarodowa Policji. 3. Szczególne formy współpracy Policji w ramach instrumentów prawnych UE.	2	3	-	-	**5**	2	3	-	-	**5**
		Razem:	**8**	**12**	-	-	**20**	**8**	**12**	-	-	**20**

Forma zakończenia (S)	**Zaliczenie z oceną**												
Efekty uczenia się	**Metody weryfikacji osiągania efektów uczenia się**												
	Egzamin pisemny	Egzamin ustny	Sprawdzian pisemny	Odpowiedź ustna	Referat	Prezentacja indywidualna	Prezentacja grupowa	Projekt indywidualny	Projekt grupowy	Samodzielna realizacja zdania praktycznego	Zespołowa realizacja zadania praktycznego	Aktywność na zajęciach	Test sprawności fizycznej
EU_1			x			x	x					x	
EU_2			x			x	x					x	
EU_3			x			x	x					x	
EU_4												x	

Nazwa przedmiotu: Standardy międzynarodowe w zakresie zwalczania przestępczości zorganizowanej, ze szczególnym uwzględnieniem cyberprzestępczości				
Numer przedmiotu: 24b	**Punkty ECTS:** 1	**Profil kształcenia:** praktyczny	**Dziedzina nauki/dyscyplina naukowa:** nauki społeczne/nauki o bezpieczeństwie	**Język wykładowy:** polski

Efekty uczenia się		**Symbol kierunkowego efektu uczenia się**	**Symbol składnika opisu charakterystyki drugiego stopnia efektów uczenia się dla kwalifikacji na poziomach 6-7 PRK**	**Treści programowe**
w zakresie wiedzy				
EU_1	Zna i rozumie rolę oraz zakres działania instytucji międzynarodowych odpowiedzialnych za współpracę w zakresie zapobiegania i zwalczania cyberprzestępczości.	K_W02 K_W10 K_W13	P7S_WG	W1-5 Ćw1-5
EU_2	Zna i rozumie specyfikę instrumentów prawnych dotyczących zwalczania cyberprzestępczości.	K_W02 K_W10 K_W13	P7S_WG	W5 Ćw5
w zakresie umiejętności				
EU_3	Potrafi właściwie analizować przepisy dotyczące międzynarodowej współpracy w zakresie zapobiegania i zwalczania cyberprzestępczości.	K_U08 K_U19	P7S_UW P7S_UK	W1-5 Ćw1-5
w zakresie kompetencji społecznych				
EU_4	Jest gotów do odpowiedzialnego pełnienia roli zawodowej z uwzględnieniem zmieniających się potrzeb społecznych i inicjowania działań na interesu publicznego.	K_K04 K_K05 K_K07	P7S_KK P7S_KR	Ćw1-5

Lp.	**Temat**	**Tezy**	**Forma studiów:**									
			stacjonarna					**niestacjonarna**				
			Łączna liczba godzin: 20					**Łączna liczba godzin: 20**				
			Wykłady	**Ćwiczenia**	**Zajęcia laboratoryjne**	**Warsztaty praktyczne**	**Razem**	**Wykłady**	**Ćwiczenia**	**Zajęcia laboratoryjne**	**Warsztaty praktyczne**	**Razem**
1.	Znaczenie i rola prawa międzynarodowego publicznego w zwalczaniu przestępczości zorganizowanej	1. Źródła prawa międzynarodowego dotyczące zwalczania przestępczości zorganizowanej. 2. Rola umów międzynarodowych w zwalczaniu przestępczości zorganizowanej. 3.Globalny wymiar przestępczości zorganizowanej a standaryzacja prawa międzynarodowego.	2	2	-	-	**4**	2	2	-	-	**4**

2.	Implementacja standardów prawa międzynarodowego w aspekcie zwalczania przestępczości zorganizowanej	1. Miejsce standardów międzynarodowych w krajowym systemie prawa. 2. Działalność służb mundurowych a stosowanie prawa międzynarodowego. 3. Rola orzecznictwa międzynarodowych sądów i trybunałów w zwalczaniu zorganizowanej przestępczości międzynarodowej.	2	2	-	-	**4**	2	2	-	-	**4**
3.	Rola międzynarodowych organizacji procesie przeciwdziałania i zwalczania przestępczości zorganizowanej	1. System uniwersalny a zapobieganie i zwalczanie przestępczości zorganizowanej. 2. Rola Rady Europy w procesie kształtowania zobowiązań państw w zakresie zwalczania przestępczości zorganizowanej. 3. Implikacje dla zwalczania przez państwa przestępczości zorganizowanej wynikające z przynależności do UE i systemu Schengen.	2	2	-	-	**4**	2	2	-	-	**4**
4.	Wybrane przykłady jurysprudencji Europejskiego Trybunału Praw Człowieka dot. zwalczania przestępczości zorganizowanej i cybersprzestępczości	1. Rola ETPCz w przeciwdziałaniu przestępczości zorganizowanej. 2. Wybrane sprawy dot. zobowiązań w zakresie działań służb mundurowych w zwalczaniu przestępczości zorganizowanej. 3. Cyberprzestępczość w wyrokach ETPCz.	1	3	-	-	**4**	1	3	-	-	**4**
5.	Cyberprzestępczość jako szczególna forma przestępczości zorganizowanej w prawie międzynarodowym	1. Potrzeba szczególnych form współpracy w zakresie zwalczania cyberprzestępczości. 2. Instrumenty prawne poświęcone zwalczaniu cyberprzestępczości. 3. Przykłady dobrych praktyk i rekomendacji organizacji międzynarodowych w zakresie zwalczania cyberprzestępczości.	1	3	-	-	**4**	1	3	-	-	**4**
		Razem:	**8**	**12**	-	-	**20**	**8**	**12**	-	-	**20**

Forma zakończenia (S)	**Zaliczenie z oceną**												
Efekty uczenia się	**Metody weryfikacji osiągania efektów uczenia się**												
	Egzamin pisemny	Egzamin ustny	Sprawdzian pisemny	Odpowiedź ustna	Referat	Prezentacja indywidualna	Prezentacja grupowa	Projekt indywidualny	Projekt grupowy	Samodzielna realizacja zdania praktycznego	Zespołowa realizacja zadania praktycznego	Aktywność na zajęciach	Test sprawności fizycznej
EU_1			x			x	x					x	
EU_2			x			x	x					x	
EU_3			x			x	x					x	
EU_4			x									x	

Nazwa przedmiotu: Zarządzanie ryzykiem				
Numer przedmiotu: 25a	**Punkty ECTS:** 1	**Profil kształcenia:** praktyczny	**Dziedzina nauki/dyscyplina naukowa:** nauki społeczne/ nauki prawne	**Język wykładowy:** polski

Efekty uczenia się		**Symbol kierunkowego efektu uczenia się**	**Symbol składnika opisu charakterystyki drugiego stopnia efektów uczenia się dla kwalifikacji na poziomach 6-7 PRK**	**Treści programowe**
w zakresie wiedzy				
EU_1	Zna i rozumie znaczenie reguł zarządzania ryzykiem w instytucjach publicznych i innych organizacjach oraz jego wpływ na bezpieczeństwo wewnętrzne w przestrzeni publicznej i życia obywateli.	K_W01 K_W11	P7S_WG	W1-5 Ćw1-5
EU_2	Zna i rozumie ekonomiczne, prawne i etyczne uwarunkowania działalności Policji i służby zwalczania cyberprzestępczości w zakresie ochrony życia, zdrowia i mienia obywateli oraz instytucjonalne rozwiązania krajowe i wspólnotowe w sferze zarządzania ryzykiem.	K_W11 K_W16	P7S_WG P7S_WK	W1-5 Ćw1-5
w zakresie umiejętności				
EU_3	Potrafi wykorzystać posiadaną wiedzę z zakresu zarządzania ryzykiem na rzecz analizowania zjawisk, zagrożeń oraz procesów społecznych oraz formułowania i rozwiązywania złożonych problemów związanych z wykonywaniem zadań funkcjonariuszy służby zwalczania cyberprzestępczości w sferze bezpieczeństwa kraju.	K_U01 K_U02 K_U13	P7S_UW	W1-5 Ćw1-5
EU_4	Potrafi wykorzystywać posiadaną wiedzę zakresu zarządzania ryzykiem w celu doboru adekwatnych do sytuacji metod i technik w zakresie analizowania przestępczości i ścigania jej sprawców.	K_U01 K_U04	P7S_UW	W1-5 Ćw1-5
w zakresie kompetencji społecznych				
EU_5	Jest gotów do wypełniania zobowiązań społecznych i współorganizowania działalności na rzecz poprawy dobrostanu obywateli oraz na rzecz interesu publicznego.	K_K04 K_K05	P7S_KO	Ćw1-5

Lp.	**Temat**	**Tezy**	**Forma studiów:**									
			stacjonarna					**niestacjonarna**				
			Łączna liczba godzin: 20					**Łączna liczba godzin: 20**				
			Wykłady	**Ćwiczenia**	**Zajęcia laboratoryjne**	**Warsztaty praktyczne**	**Razem**	**Wykłady**	**Ćwiczenia**	**Zajęcia laboratoryjne**	**Warsztaty praktyczne**	**Razem**
1.	Transdyscyplinarne podstawy zarządzania ryzykiem	1. Definiowanie ryzyka i zarządzania ryzykiem. 2. Rozwój transdyscyplinarnych badań nad ryzykiem i zarządzaniem ryzykiem. 3. Ogólny proces zarządzania ryzykiem. 4. Teoretyczne podstawy pomiaru ryzyka. 5. Taksonomia i typologia ryzyka. Podstawowe zasady interdyscyplinarnego zarządzania ryzykiem.	2	2	-	-	**4**	2	2	-	-	**4**

2.	Teoria zarządzania ryzykiem we współczesnych organizacjach	1. Miejsce i funkcje systemu zarządzania ryzykiem w systemie zarządzania organizacją. 2. Zasady zarządzania ryzykiem. Strategie reakcji na ryzyko systemowe i nadsystemowe. 3. Główne koncepcje struktury procesów zarządzania ryzykiem i metodyki oceny ryzyka. 4. Struktura programu zarządzania ryzykiem w organizacji. 5. Sfery analizy ryzyka organizacyjnego. 6. Funkcje ryzyka w procesach decyzyjnych. 7. Modele podejmowania decyzji w warunkach niepewności. 8. Diagnozowanie obszarów zagrożeń i ich identyfikacja.	2	2	-	-	**4**	2	2	-	-	**4**
3.	Zarządzanie ryzykiem w organizacjach publicznych	1. Zarządzanie ryzykiem jako składnik kontroli zarządczej. 2. Metody opisu ryzyka. 3. Metody identyfikacji obszarów potencjalnego ryzyka. 4. Zasady tworzenia zbiorowych tabel identyfikacji ryzyka, ich analizy w układzie matrycy. 5. Zasady tworzenia map i rejestrów ryzyka. 6. Decyzje i działania podejmowane w ramach procesów zarządzania ryzykiem i kontroli zarządczej. 7. Dokumentowanie efektów kontroli zarządczej i jej standardy. 8. Komponenty monitoringu ryzyka. 9. Raportowanie i sprawozdawczość z zarządzania ryzykiem. 10. Mechanizmy nadzoru i kontroli systemów informatycznych. 11. Aspekty prawne i administracyjne procesu zarządzania ryzykiem w zarzadzaniu kryzysowym. 12. Procesy i obszary zarządzania ryzykiem w jednostkach organizacyjnych Policji. 13. Zachowania dysfunkcyjne i kontrproduktywne funkcjonariuszy jako zagrożenia.	2	4	-	-	**6**	2	4	-	-	**6**

4.	Ryzyko i przestępczość w cyberprzestrzeni	1. Rodzaje ryzyka i przestępstw komputerowych. 2. Analiza zagrożeń komputerowych. 3. Zarządzanie ryzykiem komputerowym oraz środki zapobiegawcze. 4. Prawo informatyczne i odpowiedzialność karna. 5. Stany nadzwyczajne i zarządzanie kryzysowe w cyberprzestrzeni.	1	2	-	-	**3**	1	2	-	-	**3**
5.	Koncepcje pozytywnego zarządzania i kierowania redukujące ryzyko systemowe	1. Organizacyjne mechanizmy kontrolne ryzyka. 2. Funkcje sprawnościowe uczciwego zarządzania. 3. Rola zarządzania poprzez zaufanie w redukowaniu ryzyka. 4. Miejsce i funkcje działania zorientowanego na porozumienie i na jakość w profilaktyce organizacyjnej. 5. Dobre praktyki w zarządzaniu redukujące ryzyko działania. 6. Modele kultur organizacyjnych w aspekcie redukowania ryzyka systemowego: kultura doskonałych organizacji; kultura „zdrowej" organizacji; kultura integracyjna/ wysokiej tolerancji niepewności; kultura aksjonormatywna; kultura zaangażowania.	1	2	-	-	**3**	1	2	-	-	**3**
		Razem:	**8**	**12**	-	-	**20**	**8**	**12**	-	-	**20**

Forma zakończenia (S)	**Zaliczenie z oceną**												
Efekty uczenia się	**Metody weryfikacji osiągania efektów uczenia się**												
	Egzamin pisemny	Egzamin ustny	Sprawdzian pisemny	Odpowiedź ustna	Referat	Prezentacja indywidualna	Prezentacja grupowa	Projekt indywidualny	Projekt grupowy	Samodzielna realizacja zdania praktycznego	Zespołowa realizacja zadania praktycznego	Aktywność na zajęciach	Test sprawności fizycznej
EU_1				x	x	x	x		x		x	x	
EU_2				x	x	x	x		x		x	x	
EU_3				x	x	x	x		x		x	x	
EU_4				x	x	x	x		x		x	x	
EU_5												x	

Nazwa przedmiotu: Zarządzanie strategiczne w instytucjach odpowiedzialnych za cyberbezpieczeństwo				
Numer przedmiotu: 25b	**Punkty ECTS:** 1	**Profil kształcenia:** praktyczny	**Dziedzina nauki/dyscyplina naukowa:** nauki społeczne/nauki o bezpieczeństwie	**Język wykładowy:** polski

Efekty uczenia się		**Symbol kierunkowego efektu uczenia się**	**Symbol składnika opisu charakterystyki drugiego stopnia efektów uczenia się dla kwalifikacji na poziomach 6-7 PRK**	**Treści programowe**
w zakresie wiedzy				
EU_1	Zna i rozumie złożone zjawiska społeczne wywierające wpływ na funkcjonowanie jednostek i komórek organizacyjnych odpowiedzialnych za cyberbezpieczeństwo.	K_W01 K_W11	P7S_WG	W1-5 Ćw1-5
EU_2	Zna i rozumie uwarunkowania różnych rodzajów działalności zawodowej związanej z funkcjonowaniem jednostek i komórek organizacyjnych odpowiedzialnych za cyberbezpieczeństwo w tym zasady, metody i narzędzia z zakresu zarządzania strategicznego	K_W11 K_W16	P7S_WG P7S_WK	W1-5 Ćw1-5
w zakresie umiejętności				
EU_3	Potrafi wykorzystać posiadaną wiedzę z zakresu zarządzania strategicznego na rzecz analizowania zjawisk, zagrożeń oraz procesów społecznych oraz formułowania i rozwiązywania złożonych problemów związanych z funkcjonowaniem jednostek i komórek organizacyjnych odpowiedzialnych za cyberbezpieczeństwo.	K_U01 K_U02 K_U13	P7S_UW	W1-5 Ćw1-5
EU_4	Potrafi wykorzystywać posiadaną wiedzę zakresu zarządzania strategicznego w celu doboru adekwatnych do sytuacji metod i technik w zakresie funkcjonowania jednostek i komórek organizacyjnych odpowiedzialnych za cyberbezpieczeństwo.	K_U01 K_U04	P7S_UW	W1-5 Ćw1-5
w zakresie kompetencji społecznych				
EU_5	Jest gotów do wypełniania zobowiązań społecznych, inspirowania i organizowania działalności na rzecz środowiska społecznego, myślenia i działania w sposób przedsiębiorczy.	K_K04 K_K05	P7S_KO	Ćw1-5

Lp.	**Temat**	**Tezy**	**Forma studiów:**									
			stacjonarna					**niestacjonarna**				
			Łączna liczba godzin: 20					**Łączna liczba godzin: 20**				
			Wykłady	**Ćwiczenia**	**Zajęcia laboratoryjne**	**Warsztaty praktyczne**	**Razem**	**Wykłady**	**Ćwiczenia**	**Zajęcia laboratoryjne**	**Warsztaty praktyczne**	**Razem**
1.	Koncepcje zarządzania strategicznego	1. Pojęcie zarządzania strategicznego. 2. Geneza zarządzania strategicznego. 3. Szkoły i nurty w zarządzaniu strategicznym.	1	3	-	-	**4**	1	3	-	-	**4**

2.	Typologia strategii zarządzania	1. Pojęcie strategii zarządzania. 2. Cele strategiczne w organizacjach odpowiedzialnych za cyberbezpieczeństwo. 3. Misja i wizja organizacji odpowiedzialnej za cyberbezpieczeństwo 4. Podział strategii zarządzania.	2	3	-	-	**5**	2	3	-	-	**5**
3.	Analiza strategiczna	1. Istota i zakres analizy strategicznej. 2. Przegląd metod analizy makrootoczenia. 3. Przegląd metod analizy sektorowej. 4. Przegląd metod analizy strategicznej.	2	2	-	-	**4**	2	2	-	-	**4**
4.	Planowanie strategiczne	1. Planowanie strategiczne jako narzędzie rozwoju organizacji. 2. Analiza zdolności rozwojowej organizacji. 3. Strategia restrukturyzacji organizacyjnej. 4. Programowanie strategiczne.	1	2	-	-	**3**	1	2	-	-	**3**
5.	Kontrola strategiczna	1. Kontrola strategiczna w praktyce. 2. Instrumenty analizy działalności operacyjnej. 3. Analiza zasobów ludzkich.	2	2	-	-	**4**	2	2	-	-	**4**
		Razem:	**8**	**12**	-	-	**20**	**8**	**12**	-	-	**20**

Forma zakończenia (S)	**Zaliczenie z oceną**												
Efekty uczenia się	**Metody weryfikacji osiągania efektów uczenia się**												
	Egzamin pisemny	Egzamin ustny	Sprawdzian pisemny	Odpowiedź ustna	Referat	Prezentacja indywidualna	Prezentacja grupowa	Projekt indywidualny	Projekt grupowy	Samodzielna realizacja zdania praktycznego	Zespołowa realizacja zadania praktycznego	Aktywność na zajęciach	Test sprawności fizycznej
EU_1				x	x	x	x		x		x	x	
EU_2				x	x	x	x		x		x	x	
EU_3				x	x	x	x		x		x	x	
EU_4				x	x	x	x		x		x	x	
EU_5												x	

Nazwa przedmiotu: Zarządzanie kryzysowe w administracji publicznej				
Numer przedmiotu: 26a	**Punkty ECTS:** 1	**Profil kształcenia:** praktyczny	**Dziedzina nauki/dyscyplina naukowa:** nauki społeczne/nauki o bezpieczeństwie	**Język wykładowy:** polski

Efekty uczenia się

	Efekty uczenia się	**Symbol kierunkowego efektu uczenia się**	**Symbol składnika opisu charakterystyki drugiego stopnia efektów uczenia się dla kwalifikacji na poziomach 6-7 PRK**	**Odniesienie do treści przedmiotu**
w zakresie wiedzy				
EU_1	Zna i rozumie wybrane fakty, obiekty i zjawiska oraz dotyczące ich metody i teorie wyjaśniające złożone zależności między nimi, stanowiące zaawansowaną wiedzę ogólną z zakresu zarządzania kryzysowego.	K_W02 K_W12	P7S_WG	W1-2 Ćw2
EU_2	Zna i rozumie obowiązujące regulacje prawne oraz tendencje rozwojowe zarządzania kryzysowego w Polsce.	K_W07 K_W14	P7S_WG	W2, 4-5 Ćw2,4-5
w zakresie umiejętności				
EU_3	Potrafi właściwie dobierać źródła informacji o sytuacjach kryzysowych, dokonywać ich ocen, krytycznie analizować i twórczo je interpretować.	K_U01 K_U02 K_U13 K_U14	P7S_UW	W1 Ćw1
EU_4	Potrafi wykonywać zadania w zespole zarządzania kryzysowego, zarówno jako kierownik, jak i członek zespołu, kierować pracą zespołu oraz współdziałać z innymi osobami w ramach prac zespołowych i podejmować wiodącą rolę w zespołach zarządzania kryzysowego.	K_U22	P7S_UO	W1-5 Ćw1-5
w zakresie kompetencji społecznych				
EU_5	Jest gotów do odpowiedzialnego pełnienia funkcji w administracji publicznej w zakresie zarządzania kryzysowego.	K_K07	P7S_KR	Ćw1-5

Lp.	**Temat**	**Tezy**	**Forma studiów:**									
			stacjonarna					**niestacjonarna**				
			Łączna liczba godzin: 20					**Łączna liczba godzin: 20**				
			Wykłady	**Ćwiczenia**	**Zajęcia laboratoryjne**	**Warsztaty praktyczne**	**Razem**	**Wykłady**	**Ćwiczenia**	**Zajęcia laboratoryjne**	**Warsztaty praktyczne**	**Razem**
1.	Podstawy zarządzania kryzysowego	1. Współczesne zagrożenia państwa powodujące sytuacje kryzysowe. 2. Ujęcie sytuacji kryzysowej. 3. Istota zarządzania kryzysowego. 4. Fazy zarządzania kryzysowego.	1	2	-	-	**3**	1	2	-	-	**3**
2.	Zarządzanie kryzysowe w RP	1. Podstawy prawne zarządzania kryzysowego w RP. 2. Organy zarządzania kryzysowego w RP i ich kompetencje. 3. Organizacja pracy organów zarządzania kryzysowego.	2	4	-	-	**6**	2	4	-	-	**6**

3.	Podmioty wykonawcze w sytuacjach kryzysowych	1. Instytucje publiczne. 2. Organizacje pozarządowe 3. Systemy ratownicze RP	2	2	-	-	**4**	2	2	-	-	**4**
4.	Stany nadzwyczajne państwa	1. Ujęcie stanów nadzwyczajnych. 2. Rodzaje stanów nadzwyczajnych w RP 3. Regulacje stanów nadzwyczajnych w RP.	1	2	-	-	**3**	1	2	-	-	**3**
5.	Świadczenia w sytuacjach kryzysowych	1. Podstawy prawne świadczeń w RP. 2. Świadczenia osobiste. 3. Świadczenia rzeczowe.	2	2	-	-	**4**	2	2	-	-	**4**
		Razem:	**8**	**12**	-	-	**20**	**8**	**12**	-	-	**20**

Forma zakończenia (S)	**Zaliczenie z oceną**												
Przedmiotowe efekty uczenia się	**Metody weryfikacji osiągania efektów uczenia się**												
	Egzamin pisemny	Egzamin ustny	Sprawdzian pisemny	Odpowiedź ustna	Referat	Prezentacja indywidualna	Prezentacja grupowa	Projekt indywidualny	Projekt grupowy	Samodzielna realizacja zdania praktycznego	Zespołowa realizacja zadania praktycznego	Aktywność na zajęciach	Test sprawności fizycznej
EU_1			x	x			x					x	
EU_2			x	x	x		x					x	
EU_3			x	x	x		x					x	
EU_4			x	x	x		x					x	
EU_5												x	

Nazwa przedmiotu: Ochrona infrastruktury krytycznej				
Numer przedmiotu: 26b	**Punkty ECTS:** 1	**Profil kształcenia:** praktyczny	**Dziedzina nauki/dyscyplina naukowa:** nauki społeczne/nauki o bezpieczeństwie	**Język wykładowy:** polski

Efekty uczenia się		**Symbol kierunkowego efektu uczenia się**	**Symbol składnika opisu charakterystyki drugiego stopnia efektów uczenia się dla kwalifikacji na poziomach 6-7 PRK**	**Treści programowe**
w zakresie wiedzy				
EU_1	Zna i rozumie zasady dotyczące ochrony prawnej infrastruktury krytycznej.	K_W07 K_W12	P7S_WG	W1,5 Ćw1,5
EU_2	Zna i rozumie zagadnienia bezpieczeństwa infrastruktury krytycznej wynikające z powiązań i złożonych zależności oraz charakteru współczesnych zagrożeń.	K_W02 K_W12	P7S_WG	W1-5 Ćw1-2
w zakresie umiejętności				
EU_3	Potrafi identyfikować, interpretować i wyjaśniać złożone procesy będące źródłem zagrożeń infrastruktury krytycznej.	K_U13 K_U14	P7S_UW	W1-2, 5 Ćw1-2,5
EU_4	Potrafi posługiwać się różnorodnymi systemami normatywnymi przy rozwiązywaniu problemów z zakresu ochrony infrastruktury krytycznej.	K_U08	P7S_UW	Ćw1-5
w zakresie kompetencji społecznych				
EU_5	Jest gotów do odpowiedzialnego pełnienia funkcji w administracji publicznej w zakresie ochrony infrastruktury krytycznej.	K_K07	P7S_KR	Ćw1-5

Lp.	**Temat**	**Tezy**	**Forma studiów:**									
			stacjonarna					**niestacjonarna**				
			Łączna liczba godzin: 20					**Łączna liczba godzin: 20**				
			Wykłady	**Ćwiczenia**	**Zajęcia laboratoryjne**	**Warsztaty praktyczne**	**Razem**	**Wykłady**	**Ćwiczenia**	**Zajęcia laboratoryjne**	**Warsztaty praktyczne**	**Razem**
1.	Podstawowe pojęcia i normy prawne dotyczące infrastruktury krytycznej	1. Infrastruktura krytyczna i jej znaczenie dla bezpieczeństwa państwa. 2. Podstawowe pojęcia dotyczące infrastruktury kluczowej i jej ochrony. 2. Akty prawne regulujące działania na rzecz ochrony infrastruktury krytycznej. 3. Modele powiązań i zależności elementów systemów kluczowych państwa ze szczególnym uwzględnieniem cyberpowiązań.	2	3	-	-	**5**	2	3	-	-	**5**

2.	Współczesne zagrożenia infrastruktury krytycznej	1. Źródła i rodzaje zagrożeń. 2. Charakterystyka zagrożeń. 3. Konflikty hybrydowe jako specyficzny rodzaj zagrożeń infrastruktury krytycznej. 4. Wojna informacyjna i jej wpływ na bezpieczeństwo infrastruktury krytycznej.	1	3	-	-	**4**	1	3	-	-	**4**
3.	Narodowy Program Ochrony Infrastruktury Krytycznej (NPOIK)	1. Założenia programu NPOIK. 2. Elementy NPOIK.	2	2	-	-	**4**	2	2	-	-	**4**
4.	Zapewnienie bezpieczeństwa infrastruktury krytycznej	1. Podmioty zaangażowane w ochronę infrastruktury krytycznej w Polsce. 2. Działania prowadzone na rzecz zapewnienia. bezpieczeństwa infrastruktury krytycznej (w tym plany ochrony infrastruktury krytycznej).	1	2	-	-	**3**	1	2	-	-	**3**
5.	Europejska infrastruktura krytyczna	1. Europejskie unormowania prawne dotyczące infrastruktury krytycznej i jej ochrony. 2. Usługi kluczowe. 3. Zadania operatorów usług kluczowych.	2	2	-	-	**4**	2	2	-	-	**3**
		Razem:	**8**	**12**	-	-	**20**	**8**	**12**	-	-	**20**

Forma zakończenia (S)	**Zaliczenie z oceną**												
Efekty uczenia się	**Metody weryfikacji osiągania efektów uczenia się**												
	Egzamin pisemny	Egzamin ustny	Sprawdzian pisemny	Odpowiedź ustna	Referat	Prezentacja indywidualna	Prezentacja grupowa	Projekt indywidualny	Projekt grupowy	Samodzielna realizacja zdania praktycznego	Zespołowa realizacja zadania praktycznego	Aktywność na zajęciach	Test sprawności fizycznej
EU_1			x								x	x	
EU_2			x								x	x	
EU_3							x		x			x	
EU_4			x				x		x			x	
EU_5												x	

Nazwa przedmiotu: Postępowanie przedsądowe w sprawach o cyberprzestępstwa				
Numer przedmiotu: 27	**Punkty ECTS:** 2	**Profil kształcenia:** praktyczny	**Dziedzina nauki/dyscyplina naukowa:** nauki społeczne/nauki prawne	**Język wykładowy:** polski

Efekty uczenia się		**Symbol kierunkowego efektu uczenia się**	**Symbol składnika opisu charakterystyki drugiego stopnia efektów uczenia się dla kwalifikacji na poziomach 6-7 PRK**	**Treści programowe**
w zakresie wiedzy				
EU_1	Zna i rozumie wybrane zagadnienia prawa karnego procesowego w zakresie postępowania przedsądowego.	K_W07 K_W08	P7S_WG	WP1-5
EU_2	Zna i rozumie prawne i etyczne uwarunkowania przeprowadzania dowodów w postępowaniu przedsądowym w sprawach o przestępstwa dokonywane w cyberprzestrzeni.	K_W07 K_W16	P7S_WG P7S_WK	WP3-4
w zakresie umiejętności				
EU_3	Potrafi sporządzać wybrane pisma procesowe oraz pisemne analizy i interpretacje konkretnych problemów w sprawach o przestępstwa dokonywane w cyberprzestrzeni.	K_U08 K_U10 K_U18	P7S_UW P7S_UK	WP1-5
EU_4	Potrafi komunikować się z otoczeniem z użyciem specjalistycznej terminologii z zakresu postępowania karnego niezbędnej w sprawach o przestępstwa dokonywane w cyberprzestrzeni.	K_U18 K_U19	P7S_UK	WP3-4
w zakresie kompetencji społecznych				
EU_5	Jest gotów do krytycznej oceny posiadanej wiedzy i odbieranych treści typowych dla postępowań przedsądowych w sprawach o cyberprzestępstwa.	K_K02	P7S_KK	WP1-5
EU_6	Jest gotów do odpowiedzialnego pełnienia roli zawodowej jako przedstawiciel organu procesowego w postępowaniu przedsądowym w sprawach o przestępstwa dokonywane w cyberprzestrzeni.	K_K07	P7S_KR	WP1-5

Lp.	**Temat**	**Tezy**	**Forma studiów:**									
			stacjonarna					**niestacjonarna**				
			Łączna liczba godzin: 30					**Łączna liczba godzin: 20**				
			Wykłady	**Ćwiczenia**	**Zajęcia laboratoryjne**	**Warsztaty praktyczne**	**Razem**	**Wykłady**	**Ćwiczenia**	**Zajęcia laboratoryjne**	**Warsztaty praktyczne**	**Razem**
1.	Czynności poprzedzające wszczęcie postępowania przygotowawczego	1. Źródła informacji o przestępstwach dokonywanych w cyberprzestrzeni. 2. Przyjęcie pisemnego lub ustnego zawiadomienia o przestępstwie. 3. Uzupełnianie danych zawartych w zawiadomieniu. 4. Wydanie postanowienia o odmowie wszczęcia dochodzenia.	-	-	-	8	**8**	-	-	-	6	**6**

2.	Wszczęcie postępowania przygotowawczego	1. Wydanie postanowienia o wszczęciu dochodzenia. 2. Obowiązki związane ze wszczęciem postępowania karnego.	-	-	-	2	**2**		-	-	2	**2**
3.	Zbieranie dowodów w sprawach o przestępstwa dokonywane w cyberprzestrzeni	1. Wykonywanie czynności z osobowymi źródłami dowodowymi. 2. Pozyskiwanie danych od podmiotów świadczących usługi drogą elektroniczną oraz danych objętych tajemnicą bankową, pocztową i telekomunikacyjną. 3. Zatrzymanie i odebranie rzeczy oraz przeszukanie.	-	-	-	6	**6**	-	-	-	4	**4**
4.	Czynności wykonywane po ustaleniu sprawcy przestępstwa	1. Wydanie postanowienia o przedstawieniu zarzutów. 2. Przedstawienie zarzutów i przesłuchanie podejrzanego. 3. Zbieranie danych osobopoznawczych. 4. Połączenie postępowań do wspólnego prowadzenia z uwagi na łączność podmiotową. 5. Zawieszenie postępowania. 6. Środki przymusu.	-	-	-	10	**10**	-	-	-	6	**6**
5.	Czynności związane z zakończenie postępowania przygotowawczego	1. Rozwiązania konsensualne wynikające z art. 335 k.p.k. 2. Końcowe zaznajomienie podejrzanego z materiałami postępowania. 3. Akt oskarżenia.	-	-	-	4	**4**	-	-	-	2	**2**
		Razem:	**-**	**-**	**-**	**30**	**30**	**-**	**-**	**-**	**20**	**20**

Forma zakończenia (S)	**Zaliczenie z oceną**												
Kierunkowe efekty uczenia się	**Metody weryfikacji osiągania efektów uczenia się**												
	Egzamin pisemny	Egzamin ustny	Sprawdzian pisemny	Odpowiedź ustna	Referat	Prezentacja indywidualna	Prezentacja grupowa	Projekt indywidualny	Projekt grupowy	Samodzielna realizacja zdania praktycznego	Zespołowa realizacja zadania praktycznego	Aktywność na zajęciach	Test sprawności fizycznej
EU_1										x	x	x	
EU_2										x	x	x	
EU_3										x	x	x	
EU_4										x	x	x	
EU_5											x	x	
EU_6											x	x	

Nazwa przedmiotu: Procedury decyzyjne w organizacjach				
Numer przedmiotu: 28	**Punkty ECTS:** 2	**Profil kształcenia:** praktyczny	**Dziedzina nauki/dyscyplina naukowa:** nauki społeczne/ nauki o bezpieczeństwie	**Język wykładowy:** polski

Efekty uczenia się		**Symbol kierunkowego efektu uczenia się**	**Symbol składnika opisu charakterystyki drugiego stopnia efektów uczenia się dla kwalifikacji na poziomach 6-7 PRK**	**Treści programowe**
w zakresie wiedzy				
EU_1	Zna metody i narzędzia, w tym techniki pozyskiwania danych do prowadzenia badań w zakresie modelowania struktur organizacyjnych oraz procesów w nich zachodzących związanych z cyberbezpieczeństwem.	K_W01 K_W02 K_W11	P7S_WG	W1-3 Ćw1-3
EU_2	Zna przyczyny, przebieg i rozumie skutki zjawisk społecznych determinujących zjawiska cyberbezpieczeństwa.	K_W02 K_W13 K_W15	P7S_WG P7S_WK	W1-3 Ćw1-3
w zakresie umiejętności				
EU_3	Potrafi formułować i rozwiązywać złożone problemy decyzyjne w organizacjach, w tym w szczególności odpowiedzialnych za cyberbezpieczeństwo.	K_U02 K_U13 K_U14	P7S_UW	Ćw1-3
EU_4	Potrafi współdziałać z innymi osobami w ramach prac zespołowych w obszarze procedur decyzyjnych w organizacjach i podejmować wiodącą rolę w tych zespołach.	K_U22	P7S_UO	Ćw1-3
w zakresie kompetencji społecznych				
EU_5	Jest gotów do odpowiedzialnego pełnienia ról zawodowych w związku z realizacją procesu decyzyjnego w organizacji.	K_K07	P7S_KR	Ćw1-3

Lp.	**Temat**	**Tezy**	**Forma studiów:**									
			stacjonarna					**niestacjonarna**				
			Łączna liczba godzin: 30					**Łączna liczba godzin: 20**				
			Wykłady	**Ćwiczenia**	**Zajęcia laboratoryjne**	**Warsztaty praktyczne**	**Razem**	**Wykłady**	**Ćwiczenia**	**Zajęcia laboratoryjne**	**Warsztaty praktyczne**	**Razem**
1.	Wprowadzenie do teorii podejmowania decyzji - decyzje w zarządzaniu organizacją	1. Proces decyzyjny, istota podejmowania decyzji. 2. Formy i typy podejmowania decyzji. 3. Działanie zorganizowane.	4	6	-	-	**10**	2	4	-	-	**6**
2.	Decyzje kierownicze w zarządzaniu organizacją odpowiedzialną za cyberbezpieczeństwo	1. Problemy decyzyjne, istota decyzji kierowniczych. 2. Strategiczne decyzje kierownicze. 3. Wpływ informacji na decyzje, techniki decyzyjne.	2	4	-	-	**6**	1	3	-	-	**4**

3.	Skuteczne podejmowanie decyzji w organizacjach odpowiedzialnych za cyberbezpieczeństwo	1. Zarządzanie zmianą. 2. Struktura procesu decyzyjnego. 3. Praca własna i kierownika/managera. 4. Warunki efektywności procesu decyzyjnego.	4	10	-	-	**14**	2	8	-	-	**10**
		Razem:	**10**	**20**	-	-	**30**	**5**	**15**	-	-	**20**

Forma zakończenia (S)	**Zaliczenie z oceną**												
Efekty uczenia się	**Metody weryfikacji osiągania efektów uczenia się**												
	Egzamin pisemny	Egzamin ustny	Sprawdzian pisemny	Odpowiedź ustna	Referat	Prezentacja indywidualna	Prezentacja grupowa	Projekt indywidualny	Projekt grupowy	Samodzielna realizacja zdania praktycznego	Zespołowa realizacja zadania praktycznego	Aktywność na zajęciach	Test sprawności fizycznej
EU_1			x	x	x							x	
EU_2			x	x	x							x	
EU_3			x	x	x							x	
EU_4			x						x	x	x	x	
EU_5										x		x	

Nazwa przedmiotu: Darknet i anonimizacja w sieci				
Numer przedmiotu: 29	**Punkty ECTS:** 2	**Profil kształcenia:** praktyczny	**Dziedzina nauki/dyscyplina naukowa:** nauki społeczne/nauki o bezpieczeństwie	**Język wykładowy:** polski

Efekty uczenia się		**Symbol kierunkowego efektu uczenia się**	**Symbol składnika opisu charakterystyki drugiego stopnia efektów uczenia się dla kwalifikacji na poziomach 6-7 PRK**	**Treści programowe**
w zakresie wiedzy				
EU_1	Zna pojęcie Darknetu i rozumie zasadę jego funkcjonowania.	K_W03 K_W06 K_W14	P7S_UW	W1-4 WP2-4
EU_2	Zna i rozumie funkcjonowanie sieci anonimizujących w Internecie.	K_W03 K_W06	P7S_UW	W1-6 WP2-6
EU_3	Zna zasadę działania szyfrowanej poczty oraz komunikatorów internetowych.	K_W03 K_W06	P7S_UW	W5-6 WP5-6
w zakresie umiejętności				
EU_4	Potrafi instalować i konfigurować narzędzia anonimizujące.	K_U03 K_U06	P7S_UW	WP2-6
EU_5	Potrafi posługiwać się wybranymi narzędziami anonimizującymi w sieci Internet.	K_U03 K_U06	P7S_UW	WP2-6
EU_6	Potrafi zachować bezpieczeństwo w sieci.	K_U11	P7S_UW	WP2-6
w zakresie kompetencji społecznych				
EU_7	Jest gotów do uznawania wiedzy w rozwiązywaniu problemów z zakresu technik ukrywania tożsamości w Internecie oraz zasięgania opinii ekspertów w przypadku trudności z samodzielnym ich rozwiązaniem.	K_K01 K_K03	P7S_KK	W1-6 WP2-6

Lp.	**Temat**	**Tezy**	**Forma studiów:**									
			stacjonarna					**niestacjonarna**				
			Łączna liczba godzin: 36					**Łączna liczba godzin: 22**				
			Wykłady	**Ćwiczenia**	**Zajęcia laboratoryjne**	**Warsztaty praktyczne**	**Razem**	**Wykłady**	**Ćwiczenia**	**Zajęcia laboratoryjne**	**Warsztaty praktyczne**	**Razem**
1.	Ciemna strona Internetu	1. Podstawowe pojęcia. 2. Deepweb/Darkweb. 3. Darknet jako źródło informacji oraz zagrożeń.	2	-	-	-	**2**	1	-	-	-	**1**
2.	Serwery PROXY	1. Rodzaje serwerów PROXY i zasada ich działania. 2. Przykłady wykorzystania.	1	-	-	2	**3**	1	-	-	2	**3**
3.	Sieci wirtualne	1. Zasada działania i rodzaje sieci wirtualnych. 2. Praktyczne zastosowanie.	1	-	-	2	**3**	1	-	-	2	**3**
4.	Sieci anonimizujące	1. TOR. 2. Freenet. 3. I2P. 4. Inne.	2	-	-	10	**12**	1	-	-	6	**7**
5.	Bezpieczna poczta	1. Protonmail, Tutanota i inne. 2. Klucze PGP, tokeny. 3. Wykorzystanie szyfrowanej poczty.	2	-	-	6	**8**	1	-	-	3	**4**

6.	Komunikatory	1. Charakterystyka popularnych komunikatorów (WhatsApp, Telegram, Discord, Signal). 2. Wykorzystanie komunikatorów w celach anonimizacji.	2	-	-	6	**8**	1	-	-	3	**4**
		Razem:	**10**	-	-	**26**	**36**	**6**	-	-	**16**	**22**

Forma zakończenia (E)	**Egzamin**												
Efekty uczenia się	**Metody weryfikacji osiągania efektów uczenia się**												
	Egzamin pisemny	Egzamin ustny	Sprawdzian pisemny	Odpowiedź ustna	Referat	Prezentacja indywidualna	Prezentacja grupowa	Projekt indywidualny	Projekt grupowy	Samodzielna realizacja zdania praktycznego	Zespołowa realizacja zadania praktycznego	Aktywność na zajęciach	Test sprawności fizycznej
EU_1	x			x								x	
EU_2	x			x								x	
EU_3	x			x								x	
EU_4	x									x		x	
EU_5	x									x		x	
EU_6										x		x	
EU_7										x		x	

Nazwa przedmiotu: OSINT				
Numer przedmiotu: 30	**Punkty ECTS:** 2	**Profil kształcenia:** praktyczny	**Dziedzina nauki/dyscyplina naukowa:** nauki społeczne/nauki o bezpieczeństwie	**Język wykładowy:** polski

Efekty uczenia się		**Symbol kierunkowego efektu uczenia się**	**Symbol składnika opisu charakterystyki drugiego stopnia efektów uczenia się dla kwalifikacji na poziomach 6-7 PRK**	**Treści programowe**
w zakresie wiedzy				
EU_1	Zna zaawansowane metody, techniki, narzędzia stosowane przy wyszukiwaniu informacji w sieci Internet.	K_W03 K_W05 K_W06	P7S_WG	W1-3,5 WP2-4,6
EU_2	Zna wybrane domeny internetowe wykorzystywane przy gromadzeniu informacji w ramach białego wywiadu, rozumie metodykę prowadzenia białego wywiadu w sieci.	K_W03 K_W06	P7S_WG	W3,5 WP3
w zakresie umiejętności				
EU_3	Potrafi pozyskiwać dane istotne dla procesu wykrywczego z sieci Internet oraz umiejętnie interpretować otrzymane wyniki.	K_U03 K_U06 K_U07 K_U09	P7S_UW	WP2-4,6
EU_4	Potrafi użyć ogólnodostępnych wybranych narzędzi jako źródła danych operacyjnych.	K_U06 K_U14	P7S_UW	WP2-4,6
EU_5	Potrafi ocenić przydatność i sklasyfikować uzyskane informacje.	K_U03 K_U06 K_U07	P7S_UW	WP2-4,6
w zakresie kompetencji społecznych				
EU_6	Jest gotów dokonać krytycznej oceny posiadanej wiedzy w zakresie wyszukiwania informacji w Internecie.	K_K02	P7S_KK	W1-3,5 WP2-4,6

Lp.	**Temat**	**Tezy**	**Forma studiów:**									
			stacjonarna					**niestacjonarna**				
			Łączna liczba godzin: 30					**Łączna liczba godzin: 20**				
			Wykłady	**Ćwiczenia**	**Zajęcia laboratoryjne**	**Warsztaty praktyczne**	**Razem**	**Wykłady**	**Ćwiczenia**	**Zajęcia laboratoryjne**	**Warsztaty praktyczne**	**Razem**
1.	Wprowadzenie do OSINT	1. Definicja i istota białego wywiadu. 2. Rodzaje białego wywiadu. 3. Kto korzysta z technik białego wywiadu i do czego może zostać wykorzystany.	2	-	-	-	**2**	1	-	-	-	**1**
2.	Przygotowanie warsztatu pracy	1. Bezpieczeństwo pracy. 2. Zachowanie prywatności. 3. Płatności za usługi. 4. Budowanie tożsamości. 5. Wirtualizacja. 6. Wtyczki i narzędzia.	4	-	-	4	**8**	3	-	-	2	**5**

3.	Wyszukiwanie informacji na zadany temat	1. Metody i techniki gromadzenia informacji. 2. Wyszukiwarki internetowe i ich działanie. 3. DeepWeb. 4. Przestrzeń nazw domen. 5. Ustalenia adresów Ip. 6. Metadane. 7. Strony archiwalne. 8. Wyszukiwanie na podstawie zdjęcia. 9. Analiza wiadomości e-mail. 10. Geolokalizacja. 11. Portale społecznościowe.	4	-	-	6	**10**	4	-	-	4	**8**
4.	Metody zabezpieczania materiału dowodowego z Internetu	1. Zabezpieczanie stron internetowych. 2. Zabezpieczanie materiału wideo.	-	-	-	2	**2**	-	-	-	1	**1**
5.	Źródła białego wywiadu	1. Rejestry państwowe. 2. Źródła komercyjne.	2	-	-	-	**2**	1	-	-	-	**1**
6.	Automatyzacja OSINT-u	1. Metawyszukiwarki. 2. Programy wspomagające OSINT. 3. Przydatne strony białego wywiadu.	-	-	-	6	**6**	-	-	-	4	**4**
		Razem:	**12**	-	-	**18**	**30**	**9**	-	-	**11**	**20**

Forma zakończenia (S)	**Zaliczenie z oceną**												
Efekty uczenia się	**Metody weryfikacji osiągania efektów uczenia się**												
	Egzamin pisemny	Egzamin ustny	Sprawdzian pisemny	Odpowiedź ustna	Referat	Prezentacja indywidualna	Prezentacja grupowa	Projekt indywidualny	Projekt grupowy	Samodzielna realizacja zdania praktycznego	Zespołowa realizacja zadania praktycznego	Aktywność na zajęciach	Test sprawności fizycznej
EU_1			x	x								x	
EU_2			x	x								x	
EU_3			x							x		x	
EU_4			x							x		x	
EU_5			x							x		x	
EU_6										x		x	

Nazwa przedmiotu: Inżyniera społeczna				
Numer przedmiotu: 31	**Punkty ECTS:** 2	**Profil kształcenia:** praktyczny	**Dziedzina nauki/dyscyplina naukowa:** nauki społeczne/ nauki o bezpieczeństwie	**Język wykładowy:** polski

Efekty uczenia się		**Symbol kierunkowego efektu uczenia się**	**Symbol składnika opisu charakterystyki drugiego stopnia efektów uczenia się dla kwalifikacji na poziomach 6-7 PRK**	**Treści programowe**
w zakresie wiedzy				
EU_1	Zna i rozumie wybrane zagadnienia socjotechniki.	K_W01	P7S_WG	W1 Ćw2-3
EU_2	Zna zasady wywierania wpływu społecznego oraz rozumie istotę działań perswazyjnych.	K_W01 K_W15	P7S_WG P7S_WK	W2-3 Ćw2-3
w zakresie umiejętności				
EU_3	Potrafi wykorzystać narzędzia do działań perswazyjnych oraz analizuje wpływ innych osób, obrazów i treści na własne działania.	K_U01 K_U04	P7S_UW	Ćw2-3
EU_4	Potrafi rozpoznać rodzaje i skutki działań perswazyjnych różnych podmiotów politycznych, ekonomicznych i społecznych.	K_U13	P7S_UW	Ćw2-3
w zakresie kompetencji społecznych				
EU_5	Jest gotów dokonać krytycznej oceny posiadanej wiedzy w zakresie wywierania wpływu społecznego oraz działań perswazyjnych.	K_K02	P7S_KK	W1-3 Ćw2-3

Lp.	**Temat**	**Tezy**	**Forma studiów:**									
			stacjonarna					**niestacjonarna**				
			Łączna liczba godzin: 35					**Łączna liczba godzin: 26**				
			Wykłady	**Ćwiczenia**	**Zajęcia laboratoryjne**	**Warsztaty praktyczne**	**Razem**	**Wykłady**	**Ćwiczenia**	**Zajęcia laboratoryjne**	**Warsztaty praktyczne**	**Razem**
1.	Podstawowe zagadnienia inżynierii społecznej	1. Psychologiczne aspekty socjotechniki. Reguły socjotechniczne – techniki wywierania wpływu na ludzi. 2. Profilowanie przez komunikację.	5	-	-	-	**5**	4	-	-	-	**4**
2.	Socjotechniki w komunikowaniu politycznym. Opinia publiczna i sondaże opinii publicznej jako element socjotechniki	1. Tworzenie dzieła sztuki - perswazyjność obrazu. 2. Socjotechniki w nowych mediach: hakowanie ludzi. 3. Czynniki ograniczające skuteczność socjotechnik. 4. M.A.P.A.	5	10	-	-	**15**	4	7	-	-	**11**

3.	Socjotechnika na przykładach	1. Perswazyjność obrazu. 2. Reguły socjometryczne w reklamie komercyjnej i społecznej. 3. Media społecznościowe a reguły socjotechniczne. 4. Manipulacje danymi dzienników zdarzeń. 5. Socjotechnika w Internecie.	5	10	-	-	**15**	4	7	-	-	**11**
		Razem:	**15**	**20**	-	-	**35**	**12**	**14**	-	-	**26**

Forma zakończenia (S)	**Zaliczenie z oceną**												
Efekty uczenia się	**Metody weryfikacji osiągania efektów uczenia się**												
	Egzamin pisemny	Egzamin ustny	Sprawdzian pisemny	Odpowiedź ustna	Referat	Prezentacja indywidualna	Prezentacja grupowa	Projekt indywidualny	Projekt grupowy	Samodzielna realizacja zdania praktycznego	Zespołowa realizacja zadania praktycznego	Aktywność na zajęciach	Test sprawności fizycznej
EU_1			x	x		x						x	
EU_2			x	x		x						x	
EU_3			x			x						x	
EU_4			x			x						x	
EU_5						x						x	

Nazwa przedmiotu: Udział biegłego w postępowaniu dowodowym w sprawach o przestępstwa komputerowe				
Numer przedmiotu: 32	**Punkty ECTS:** 3	**Profil kształcenia:** praktyczny	**Dziedzina nauki/dyscyplina naukowa:** nauki społeczne/nauki prawne	**Język wykładowy:** polski

Efekty uczenia się		**Symbol kierunkowego efektu uczenia się**	**Symbol składnika opisu charakterystyki drugiego stopnia efektów uczenia się dla kwalifikacji na poziomach 6-7 PRK**	**Treści programowe**
w zakresie wiedzy				
EU_1	Zna i rozumie regulacje prawne i zasady powoływania biegłych w sprawach o przestępstwa komputerowe.	K_W07 K_W08	P7S_WG	W1 WP1
EU_2	Zna i rozumie zasady współpracy z biegłym w postępowaniu dowodowym w sprawach o przestępstwa komputerowe.	K_W01 K_W08	P7S_WG	W2 WP1-2
w zakresie umiejętności				
EU_3	Potrafi w sposób celowy dokonać doboru biegłego w zależności od rodzaju zabezpieczonego materiału dowodowego w sprawach o przestępstwa komputerowe.	K_U01 K_U09	P7S_UW	W1 WP1
EU_4	Potrafi w sposób efektywny współpracować z biegłym oraz podejmować odpowiednie decyzje.	K_U09 K_U22	P7S_UW P7S_UO	W2 WP1-2
EU_5	Potrafi sporządzić postanowienie o dopuszczeniu dowodu z opinii biegłego w sprawach o przestępstwa komputerowe oraz odpowiednio sformułować pytania.	K_U09 K_U10	P7S_UW	W2 WP1-2
EU_6	Potrafi dokonać krytycznej oceny opinii biegłego wydanej w sprawach o przestępstwa komputerowe.	K_U08	P7S_UW	W2 WP1-2
w zakresie kompetencji społecznych				
EU_7	Jest gotów do współpracy z biegłym w zakresie badań informatycznych.	K_K03	P7S_KK	WP1-2

Lp.	**Temat**	**Tezy**	**Forma studiów:**									
			stacjonarna					**niestacjonarna**				
			Łączna liczba godzin: 45					**Łączna liczba godzin: 35**				
			Wykłady	**Ćwiczenia**	**Zajęcia laboratoryjne**	**Warsztaty praktyczne**	**Razem**	**Wykłady**	**Ćwiczenia**	**Zajęcia laboratoryjne**	**Warsztaty praktyczne**	**Razem**
1.	Dowody w postępowaniu	1. Biegły i jego status prawny. 2. Grupy biegłych. 3. Charakterystyka dowodu z opinii biegłego. 4. Narzędzia stosowane przez biegłych sądowych.	7	-	-	5	**12**	5	-	4	-	**9**

2.	Współpraca z biegłym	1. Zasady współpracy z biegłym podczas zabezpieczania danych elektronicznych. 2. Przybranie biegłego w toku czynności procesowych – oględzin. 3. Nadzór nad biegłym. 4. Sporządzanie „Postanowienie o dopuszczeniu dowodu z opinii biegłego". 5. Zaprezentowanie i omówienie przykładowych opinii.	8	-	-	25	**33**	6	-	20	-	**26**
		Razem:	**15**	-	-	**30**	**45**	**11**	-	**24**	-	**35**

Forma zakończenia (E)	**Egzamin**												
Efekty uczenia się	**Metody weryfikacji osiągania efektów uczenia się**												
	Egzamin pisemny	Egzamin ustny	Sprawdzian pisemny	Odpowiedź ustna	Referat	Prezentacja indywidualna	Prezentacja grupowa	Projekt indywidualny	Projekt grupowy	Samodzielna realizacja zdania praktycznego	Zespołowa realizacja zadania praktycznego	Aktywność na zajęciach	Test sprawności fizycznej
EU_1	x										x	x	
EU_2	x										x	x	
EU_3	x										x	x	
EU_4	x										x	x	
EU_5	x										x	x	
EU_6											x	x	
EU_7											x	x	

Nazwa przedmiotu: Ataki i wykrywanie włamań w cyberprzestrzeni				
Numer przedmiotu: 33	**Punkty ECTS:** 2	**Profil kształcenia:** praktyczny	**Dziedzina nauki/dyscyplina naukowa:** nauki społeczne/ nauki o bezpieczeństwie	**Język wykładowy:** polski

Efekty uczenia się		**Symbol kierunkowego efektu uczenia się**	**Symbol składnika opisu charakterystyki drugiego stopnia efektów uczenia się dla kwalifikacji na poziomach 6-7 PRK**	**Treści programowe**
w zakresie wiedzy				
EU_1	Zna i rozumie zasady przetwarzania informacji, budowy sieci i aplikacji sieciowych oraz rodzaje i sposoby ataków na infrastrukturę teleinformatyczną.	K_W03 K_W06	P7S_WG	W1-2 L1-2
EU_2	Zna wybrane pojęcia i rozumie zasady z zakresu ochrony danych i zasobów sieciowych.	K_W03	P7S_WG	W1-2 L1-2
w zakresie umiejętności				
EU_3	Potrafi ocenić poziom bezpieczeństwa systemów i sieci teleinformatycznych, stosując techniki i programy do analizy sieci.	K_U06 K_U07	P7S_UW	L1
EU_4	Potrafi zidentyfikować luki w systemach teleinformatycznych.	K_U06 K_U07	P7S_UW	L1
EU_5	Potrafi zaprojektować proces testowania bezpieczeństwa sieci i wyciągnąć wnioski.	K_U06 K_U07	P7S_UW	L2
w zakresie kompetencji społecznych				
EU_6	Jest gotów do pogłębionej analizy i krytycznej oceny posiadanej wiedzy z zakresu bezpieczeństwa sieci i systemów teleinformatycznych oraz zasięgania opinii ekspertów w przypadku trudności z samodzielnym rozwiązaniem problemu praktycznego.	K_K02 K_K03	P7S_KK	W1-2 L1-2

Lp.	**Temat**	**Tezy**	**Forma studiów:**									
			stacjonarna					**niestacjonarna**				
			Łączna liczba godzin: 35					**Łączna liczba godzin: 26**				
			Wykłady	**Ćwiczenia**	**Zajęcia laboratoryjne**	**Warsztaty praktyczne**	**Razem**	**Wykłady**	**Ćwiczenia**	**Zajęcia laboratoryjne**	**Warsztaty praktyczne**	**Razem**
1.	Wybrane metody ataków	1. Definicje atrybutów bezpieczeństwa. 2. Złośliwe oprogramowanie - malware 3. Protokoły i usługi sieciowe - identyfikacja niebezpiecznych sygnatur. 4. Snifing, spoofing, HiJacking - incydenty i zabezpieczenia. 5. Ataki DoS i DDoS.	7	-	10	-	**17**	4	-	8	-	**12**

2.	Programowe i sprzętowe systemy przeciwdziałania i wykrywania włamań	1. Systemy IDS. 2. Systemy IPS. 3. Zabezpieczenia w systemie operacyjnym. 4. Konfiguracja systemów antywirusowych i antyspamowych. 5. Wykorzystanie narzędzi monitoringu ruchu sieciowego. 6. Konfigurowanie punktów dostępowych w sieciach Wi-Fi. 7. Konfiguracja i wykorzystanie pakietu Snort.	8	-	10	-	**18**	6	-	8	-	**14**
		Razem:	**15**	-	**20**	-	**35**	**10**	-	**16**	-	**26**

Forma zakończenia (S)	**Zaliczenie z oceną**												
Efekty uczenia się	**Metody weryfikacji osiągania efektów uczenia się**												
	Egzamin pisemny	Egzamin ustny	Sprawdzian pisemny	Odpowiedź ustna	Referat	Prezentacja indywidualna	Prezentacja grupowa	Projekt indywidualny	Projekt grupowy	Samodzielna realizacja zdania praktycznego	Zespołowa realizacja zadania praktycznego	Aktywność na zajęciach	Test sprawności fizycznej
EU_1			x	x								x	
EU_2			x	x								x	
EU_3			x	x						x		x	
EU_4			x	x						x		x	
EU_5										x		x	
EU_6										x		x	

Nazwa przedmiotu: Live Forensics				
Numer przedmiotu: 34	**Punkty ECTS:** 2	**Profil kształcenia:** praktyczny	**Dziedzina nauki/dyscyplina naukowa:** nauki społeczne/ nauki o bezpieczeństwie	**Język wykładowy:** polski

Efekty uczenia się		**Symbol kierunkowego efektu uczenia się**	**Symbol składnika opisu charakterystyki drugiego stopnia efektów uczenia się dla kwalifikacji na poziomach 6-7 PRK**	**Treści programowe**
w zakresie wiedzy				
EU_1	Zna i rozumie istotę informatyki śledczej w zakresie zabezpieczania danych metodą Live Forensics.	K_W02 K_W03	P7S_WG	W1-4 L1-4
EU_2	Zna zaawansowane metody, techniki, narzędzia i materiały stosowane przy zabezpieczaniu elektronicznego materiału dowodowego metodą Live Forensics.	K_W05 K_W06	P7S_WG	W2-4 L2-4
w zakresie umiejętności				
EU_3	Potrafi właściwie dobrać rodzaj urządzenia oraz prawidłowo zastosować metodę Live Forensics.	K_U06 K_U07	P7S_UW	L1-4
EU_4	Potrafi właściwie zastosować zaawansowane narzędzia do pozyskiwania dowodów elektronicznych za pomocą metody Live Forensics.	K_U03 K_U06	P7S_UW	L1-4
EU_5	Potrafi zabezpieczyć typowe dowody elektroniczne w celu ich dalszej analizy.	K_U06 K_U07	P7S_UW	L4
w zakresie kompetencji społecznych				
EU_6	Jest gotów do uznania znaczenia wiedzy w rozwiązywaniu problemów poznawczych i praktycznych w zakresie zabezpieczania danych metodą Live Forensics.	K_K01	P7S_KK	W1-4 L1-4
EU_7	Jest gotowy do pogłębionej analizy i krytycznej oceny posiadanej wiedzy z zakresu zabezpieczania danych metodą Live Forensics oraz zasięgania opinii ekspertów w przypadku trudności z samodzielnym rozwiązaniem problemu praktycznego.	K_K02 K_K03	P7S_KK	W1-4 L1-4

Lp.	**Temat**	**Tezy**	**Forma studiów:**									
			stacjonarna					**niestacjonarna**				
			Łączna liczba godzin: 35					**Łączna liczba godzin: 25**				
			Wykłady	**Ćwiczenia**	**Zajęcia laboratoryjne**	**Warsztaty praktyczne**	**Razem**	**Wykłady**	**Ćwiczenia**	**Zajęcia laboratoryjne**	**Warsztaty praktyczne**	**Razem**
1.	Wprowadzenie do Live Forensics – aspekty prawne	1. Podstawowe narzędzia i oprogramowanie Live Forensics. 2. Zagadnienia prawne związane z zabezpieczaniem danych metodą Live Forensics. 3. Konfiguracja narzędzi Live Forensics.	4	-	4	-	**8**	2	-	3	-	**5**
2.	Metoda Triage- wstępna ocena materiału dowodowego	1. Metodyka Triage w informatyce śledczej. 2. Omówienie technik Triage.	2	-	6	-	**8**	2	-	4	-	**6**

3.	Proces zabezpieczenia materiału dowodowego metodą Live Forensics	1. Zabezpieczanie danych z różnych typów urządzeń. 2. Zabezpieczanie danych z nośników ulotnych.	2	-	8	-	**10**	2	-	6	-	**8**
4.	Analiza danych	1. Analiza danych z urządzeń. 2. Analiza danych z nośników ulotnych.	2	-	7	-	**9**	2	-	4	-	**6**
		Razem:	**10**	-	**25**	-	**35**	**8**	-	**17**	-	**25**

Forma zakończenia (S)	**Zaliczenie z oceną**												
Efekty uczenia się	**Metody weryfikacji osiągania efektów uczenia się**												
	Egzamin pisemny	Egzamin ustny	Sprawdzian pisemny	Odpowiedź ustna	Referat	Prezentacja indywidualna	Prezentacja grupowa	Projekt indywidualny	Projekt grupowy	Samodzielna realizacja zdania praktycznego	Zespołowa realizacja zadania praktycznego	Aktywność na zajęciach	Test sprawności fizycznej
EU_1			x	x								x	
EU_2			x	x								x	
EU_3			x							x		x	
EU_4			x							x		x	
EU_5			x							x		x	
EU_6												x	
EU_7												x	

Nazwa przedmiotu: Analiza śledcza w sprawach związanych z cyberprzestępczością				
Numer przedmiotu: 35	**Punkty ECTS:** 2	**Profil kształcenia:** praktyczny	**Dziedzina nauki/dyscyplina naukowa:** nauki społeczne/nauki o bezpieczeństwie	**Język wykładowy:** polski

Efekty uczenia się		**Symbol kierunkowego efektu uczenia się**	**Symbol składnika opisu charakterystyki drugiego stopnia efektów uczenia się dla kwalifikacji na poziomach 6-7 PRK**	**Treści programowe**
w zakresie wiedzy				
EU_1	Zna i rozumie istotę analizy śledczej i jej praktyczne zastosowanie w sprawach związanych z cyberprzestępczością.	K_W02 K_W03	P7S_UW	W1-5 L1-5
EU_2	Zna lokalizację artefaktów w systemach operacyjnych i rozumie ich znaczenie w analizie śledczej.	K_W05	P7S_UW	W2-5 L2-5
w zakresie umiejętności				
EU_3	Potrafi korzystać z różnych rozwiązań programowych niezbędnych w analizie śledczej w sprawach związanych z cyberprzestępczością i rozwiązywać problemy typowe dla działalności zawodowej.	K_U03 K_U06 K_U07	P7S_UW	L1-5
EU_4	Potrafi dokonać analizy różnych plików.	K_U03 K_U06 K_U07	P7S_UW	L1-5
EU_5	Potrafi korzystać z narzędzi automatyzujących analizę śledczą w sprawach związanych z cyberprzestępczością.	K_U03 K_U06 K_U07	P7S_UW	L1-5
w zakresie kompetencji społecznych				
EU_6	Jest gotów do uznania znaczenia wiedzy w rozwiązywaniu problemów poznawczych i praktycznych w zakresie wykorzystania analizy śledczej w sprawach związanych z cyberprzestępczością.	K_K01	P7S_KK	W1-5 L1-5
EU_7	Jest gotowy do zasięgania opinii ekspertów w przypadku trudności z samodzielnym rozwiązaniem problemu praktycznego.	K_K03	P7S_KK	L1-5

Lp.	**Temat**	**Tezy**	**Forma studiów:**									
			stacjonarna					**niestacjonarna**				
			Łączna liczba godzin: 40					**Łączna liczba godzin: 35**				
			Wykłady	**Ćwiczenia**	**Zajęcia laboratoryjne**	**Warsztaty praktyczne**	**Razem**	**Wykłady**	**Ćwiczenia**	**Zajęcia laboratoryjne**	**Warsztaty praktyczne**	**Razem**
1.	Podstawy analizy śledczej w sprawach związanych z cyberprzestepczością	1. Analiza zawartości nośników danych. 2. Kontenery specjalne. 3. Funkcje skrótu. 4. Odzyskiwanie danych. 5. Tworzenie kopii binarnych.	2	-	6	-	**8**	2	-	5	-	**7**
2.	Systemy plików i artefakty	1. Systemy plików w systemie Windows. 2. Rejestr. 3. Dzienniki zdarzeń. 4. Pliki prefetch, skrótów, wykonalne.	2	-	6	-	**8**	2	-	5	-	**7**

3.	Artefakty internetowe	1. Artefakty przeglądarek internetowych. 2. Artefakty poczty elektronicznej.	2	-	6	-	**8**	2	-	5	-	**7**
4.	Analiza plików	1. Podstawowe zagadnienia analizy plików. 2. Pliki graficzne. 3. Pliki audio. 4. Pliki wideo. 5. Pliki archiwum. 6. Pliki dokumentów.	2	-	6	-	**8**	2	-	5	-	**7**
5.	Automatyzacja procesów informatyki kryminalistycznej	1. Graficzne środowiska wspomagające analizę śledczą. 2. Automatyzacja procesu identyfikacji i wyodrębniania artefaktów. 3. Analiza chronologii zdarzeń.	2	-	6	-	**8**	2	-	5	-	**7**
		Razem:	**10**	-	**30**	-	**40**	**10**	-	**25**	-	**35**

Forma zakończenia (S)	**Zaliczenie z oceną**												
Efekty uczenia się	**Metody weryfikacji osiągania efektów uczenia się**												
	Egzamin pisemny	Egzamin ustny	Sprawdzian pisemny	Odpowiedź ustna	Referat	Prezentacja indywidualna	Prezentacja grupowa	Projekt indywidualny	Projekt grupowy	Samodzielna realizacja zdania praktycznego	Zespołowa realizacja zadania praktycznego	Aktywność na zajęciach	Test sprawności fizycznej
EU_1								x		x	x	x	
EU_2								x		x	x	x	
EU_3								x		x	x	x	
EU_4								x		x	x	x	
EU_5								x		x	x	x	
EU_6										x	x	x	
EU_7										x	x	x	

Nazwa przedmiotu: Bezpieczeństwo aplikacji mobilnych				
Numer przedmiotu: 36	**Punkty ECTS:** 2	**Profil kształcenia:** praktyczny	**Dziedzina nauki/dyscyplina naukowa:** nauki społeczne/ nauki o bezpieczeństwie	**Język wykładowy:** polski

Efekty uczenia się		**Symbol kierunkowego efektu uczenia się**	**Symbol składnika opisu charakterystyki drugiego stopnia efektów uczenia się dla kwalifikacji na poziomach 6-7 PRK**	**Treści programowe**
w zakresie wiedzy				
EU_1	Zna i rozumie zagadnienia związane z bezpieczeństwem mobilnych systemów informatycznych.	K_W06 K_W09	P7S_UW	W1-5 L1-5
EU_2	Zna i rozumie zagrożenia bezpieczeństwa dotyczące aplikacji webowych i urządzeń mobilnych.	K_W06 K_W14	P7S_UW	W2-5 L2-5
EU_3	Zna i rozumie pojęcia i zjawiska w zakresie bezpieczeństwa aplikacji mobilnych oraz metody i przykłady ataków związanych ze specyfikacją systemów urządzeń mobilnych.	K_W06 K_W14	P7S_UW	W3-5 L3-5
w zakresie umiejętności				
EU_4	Potrafi pracować w środowiskach systemów urządzeń mobilnych.	K_U03	P7S_UW	L1
EU_5	Potrafi rozpoznać techniki ataków na aplikacje mobilne.	K_U06	P7S_UW	L2-5
EU_6	Potrafi przeprowadzić analizę podatności aplikacji mobilnej i wdrożyć działania aby je usunąć.	K_U06 K_U07	P7S_UW	L4-5
EU_7	Potrafi zabezpieczyć aplikacje mobilne przed atakami.	K_U06	P7S_UW	L1-5
w zakresie kompetencji społecznych				
EU_8	Jest gotów do uznawania wiedzy w rozwiązywaniu problemów z zakresu bezpieczeństwa aplikacji mobilnych oraz zasięgania opinii ekspertów w przypadku trudności z samodzielnym ich rozwiązaniem.	K_K01 K_K03	P7S_KK	W1-5 L1-5

Lp.	**Temat**	**Tezy**	**Forma studiów:**									
			stacjonarna					**niestacjonarna**				
			Łączna liczba godzin: 30					**Łączna liczba godzin: 25**				
			Wykłady	**Ćwiczenia**	**Zajęcia laboratoryjne**	**Warsztaty praktyczne**	**Razem**	**Wykłady**	**Ćwiczenia**	**Zajęcia laboratoryjne**	**Warsztaty praktyczne**	**Razem**
1	Architektury mobilnych systemów operacyjnych	1. iOS. 2. Android.	2	-	4	-	**6**	2	-	2	-	**4**
2	Bezpieczeństwo urządzeń mobilnych	1. Zabezpieczenie danych w urządzeniach mobilnych. 2. Wpływ domyślnych zabezpieczeń urządzeń na bezpieczeństwo aplikacji. 3. Data wiping. 4. System uprawnień (Android). 5. Data Protection (iOS). 6. Keychain (iOS).	2	-	4	-	**6**	2	-	2	-	**4**

3	Przełamywanie zabezpieczeń systemów urządzeń mobilnych	1. Eskalacja uprawnień w systemach mobilnych (jailbreak). 2. Wpływ eskalacji uprawnień na bezpieczeństwo aplikacji 3. Dostęp do danych użytkowników (m.in. SMS, e-mail, dane GPS). 4. Analiza systemu plików (ich struktur i typów). 5. Przełamywanie szyfrowania danych.	3	-	4	-	**7**	2	-	4	-	**6**
4	Bezpieczeństwo aplikacji	1. Analiza sposobów dystrybucji aplikacji i ryzyka z nią związane. 2. Reverse Engineering aplikacji (Cycript, baksmali, apktool). 3. Utrudnianie analizy kodu i modyfikacji działania aplikacji (m.in. blokowanie debugerów, obfuskacja kodu, ASLR). 4. Wykrywanie środowisk z podwyższonymi uprawnieniami (jailbreak). 5. Narzędzia wspomagające analizę bezpieczeństwa aplikacji.	3	-	4	-	**7**	3	-	4	-	**7**
5	Ataki związane ze specyfikacją systemów urządzeń mobilnych	1. Multitasking (app state/GUI caching). 2. Wprowadzanie danych (input caching). 3. Identyfikacja urządzeń i użytkowników (UDID). 4. Zarządzanie logami.	2	-	2	-	**4**	2	-	2	-	**4**
		Razem:	**12**	-	**18**	-	**30**	**11**	-	**14**	-	**25**

Forma zakończenia (S)	**Zaliczenie z oceną**												
Efekty uczenia się	**Metody weryfikacji osiągania efektów uczenia się**												
	Egzamin pisemny	Egzamin ustny	Sprawdzian pisemny	Odpowiedź ustna	Referat	Prezentacja indywidualna	Prezentacja grupowa	Projekt indywidualny	Projekt grupowy	Samodzielna realizacja zdania praktycznego	Zespołowa realizacja zadania praktycznego	Aktywność na zajęciach	Test sprawności fizycznej
EU_1			x	x		x						x	
EU_2			x	x		x						x	
EU_3			x	x		x						x	
EU_4			x			x						x	
EU_5			x			x						x	
EU_6			x			x						x	
EU_7			x			x						x	
EU_8			x			x						x	

Nazwa przedmiotu: Polityka bezpieczeństwa informacji				
Numer przedmiotu: 37	**Punkty ECTS:** 2	**Profil kształcenia:** praktyczny	**Dziedzina nauki/dyscyplina naukowa:** nauki społeczne/ nauki o bezpieczeństwie	**Język wykładowy:** polski

Efekty uczenia się		**Symbol kierunkowego efektu uczenia się**	**Symbol składnika opisu charakterystyki drugiego stopnia efektów uczenia się dla kwalifikacji na poziomach 6-7 PRK**	**Treści programowe**
w zakresie wiedzy				
EU_1	Zna i rozumie zasady organizacji bezpieczeństwa informacji.	K_W06 K_W09	P7S_UW	W1-3 L1-3
EU_2	Zna aspekty bezpieczeństwa i rozumie wymogi prawne polityki bezpieczeństwa informacji.	K_W06	P7S_UW	W4 L4
EU_3	Zna i rozumie standardy stosowane w polityce bezpieczeństwa informacji.	K_W07	P7S_UW	W5 L5
w zakresie umiejętności				
EU_4	Potrafi omówić i zinterpretować elementy organizacji bezpieczeństwa informacji.	K_U03	P7S_UW	L1-3
EU_5	Potrafi interpretować i zastosować akty prawne dotyczące ciągłości działania w sferze bezpieczeństwa informacji.	K_U08	P7S_UW	L4
EU_6	Potrafi scharakteryzować podstawowe wymagania określne w standardach w zakresie bezpieczeństwa informacji.	K_U05	P7S_UW	L5
w zakresie kompetencji społecznych				
EU_7	Jest gotów do uznawania wiedzy w rozwiązywaniu problemów z zakresu bezpieczeństwa informacji oraz zasięgania opinii ekspertów w przypadku trudności z samodzielnym ich rozwiązaniem.	K_K01 K_K03	P7S_KK	W1-5 L1-5

Lp.	**Temat**	**Tezy**	**Forma studiów:**									
			stacjonarna					**niestacjonarna**				
			Łączna liczba godzin: 30					**Łączna liczba godzin: 25**				
			Wykłady	**Ćwiczenia**	**Zajęcia laboratoryjne**	**Warsztaty praktyczne**	**Razem**	**Wykłady**	**Ćwiczenia**	**Zajęcia laboratoryjne**	**Warsztaty praktyczne**	**Razem**
1	Organizacja bezpieczeństwa informacji	1. Organizacja wewnętrzna. 2. Podmioty zewnętrzne.	2	-	4	-	**6**	2	-	2	-	**4**
2	Bezpieczeństwo fizyczne i środowiskowe	1. Strefy bezpieczeństwa. 2. Bezpieczeństwo sprzętu.	2	-	4	-	**6**	2	-	2	-	**4**
3	Kontrola dostępu	1. Zarządzanie dostępem użytkowników. 2. Kontrola dostępu do sieci i systemów. 3. Kontrola dostępu do aplikacji i informacji. 4. Komputery mobilne i praca zdalna.	3	-	4	-	**7**	2	-	4	-	**6**
4	Zarządzanie ciągłością działania	1. Aspekty bezpieczeństwa informacji. 2. Wymogi prawne.	3	-	4	-	**7**	3	-	4	-	**7**

5	Standardy w zakresie bezpieczeństwa informacji	1. Narodowy standard cyberbezpieczeństwa (NSC). 2. Ramy cyberbezpieczeństwa (NIST). 3. System zarządzania bezpieczeństwem informacji (ISO 270001). 4. Zarządzania ciągłością działania (ISO 22301).	2	-	2	-	**4**	2	-	2	-	**4**
		Razem:	**12**	-	**18**	-	**30**	**11**	-	**14**	-	**25**

Forma zakończenia (S)	**Zaliczenie z oceną**												
Efekty uczenia się	**Metody weryfikacji osiągania efektów uczenia się**												
	Egzamin pisemny	Egzamin ustny	Sprawdzian pisemny	Odpowiedź ustna	Referat	Prezentacja indywidualna	Prezentacja grupowa	Projekt indywidualny	Projekt grupowy	Samodzielna realizacja zdania praktycznego	Zespołowa realizacja zadania praktycznego	Aktywność na zajęciach	Test sprawności fizycznej
EU_1			x	x		x						x	
EU_2			x	x		x						x	
EU_3			x	x		x						x	
EU_4			x			x						x	
EU_5			x			x						x	
EU_6			x			x						x	
EU_7			x			x						x	

Nazwa przedmiotu: Nowoczesne technologie w służbie Policji – symulatory ruchu drogowego				
Numer przedmiotu: 38a	**Punkty ECTS:** 2	**Profil kształcenia:** praktyczny	**Dziedzina nauki/dyscyplina naukowa:** nauki społeczne/nauki o bezpieczeństwie	**Język wykładowy:** polski

Efekty uczenia się		**Symbol kierunkowego efektu uczenia się**	**Symbol składnika opisu charakterystyki drugiego stopnia efektów uczenia się dla kwalifikacji na poziomach 6-7 PRK**	**Treści programowe**
w zakresie wiedzy				
EU_1	Zna i rozumie kluczowe rozwiązania z zakresu prawa o ruchu drogowym oraz zna rolę instytucji odpowiedzialnych za bezpieczeństwo w ruchu drogowym.	K_W02 K_W11	P7S_WG	W1-3
EU_2	Zna i rozumie zastosowanie symulatorów w systemie kształcenia zawodowego funkcjonariuszy Policji.	K_W06	P7S_WG	W1-3
w zakresie umiejętności				
EU_3	Potrafi rozstrzygać dylematy w zakresie bezpieczeństwa ruchu drogowego, w tym odnośnie taktyki i techniki kierowania pojazdem oraz obsługi zdarzeń drogowych.	K_U02 K_U13	P7S_UW	WP1-3 Ćw2-3
EU_4	Potrafi posługiwać się symulatorami w ramach wykonywania czynności na miejscu zdarzenia drogowego oraz kierowania pojazdem w różnych sytuacjach drogowych.	K_U02 K_U05	P7S_UW	WP1-3 Ćw2-3
EU_5	Potrafi samodzielnie planować własny rozwój i uczenie się przez całe życie, ukierunkowywać innych w tym zakresie oraz stale pogłębiać wiedzę z zakresu cyberbezpieczeństwa, w tym z wykorzystaniem różnych źródeł i nowoczesnych technologii.	K_U23	P7S_UU	WP1-3 Ćw2-3
w zakresie kompetencji społecznych				
EU_6	Jest gotów do rozstrzygania dylematów oraz określa priorytety w realizowanych przez siebie lub zespół zadaniach.	K_K02	P7S_KK	W1-3 Wp1-3 Ćw2-3

Lp.	**Temat**	**Tezy**	**Forma studiów:**									
			stacjonarna					**niestacjonarna**				
			Łączna liczba godzin: 30					**Łączna liczba godzin: 30**				
			Wykłady	**Ćwiczenia**	**Zajęcia laboratoryjne**	**Warsztaty praktyczne**	**Razem**	**Wykłady**	**Ćwiczenia**	**Zajęcia laboratoryjne**	**Warsztaty praktyczne**	**Razem**
1.	Podstawy korzystania z nowoczesnych technologii w służbie Policji	1. Zakres bezpieczeństwa publicznego. 2. Udział nowoczesnych technologii w systemie kształcenia. 3. Aspekty wykorzystania symulatorów w procesie kształcenia. 4. Czynności na miejscu zdarzenia w wirtualnej rzeczywistości. 5. Bezpieczne korzystanie z pojazdów w wirtualnej rzeczywistości.	1	-	-	2	**3**	1	-	-	2	**3**

2.	Kształcenie bezpiecznych zachowań z wykorzystaniem symulatora kierowania pojazdem	1. Bezpieczeństwo ruchu drogowego w Polsce. 2. Ruch pojazdów uprzywilejowanych. 3. Prawidłowe operowanie kołem kierownicy – wirtualny plac manewrowy. 4. Kierowanie pojazdem w rzeczywistości wirtualnej. 5. Taktyka i technika kierowania pojazdem w różnych sytuacjach drogowych. 6. Kierowanie symulatorem pojazdu w sytuacjach typowych i ekstremalnych. 7. Kierowanie symulatorem pojazdu podczas wykonywania czynności w ramach prowadzonych eskort, jazda w kolumnie. 8. Kierowanie symulatorem pojazdu w trakcie prowadzenia działań pościgowo-blokadowych.	2	2	-	8	**12**	2	2	-	8	**12**
3.	Wykonywanie prawidłowych czynności na miejscu zdarzenia drogowego z wykorzystaniem symulatora	1. Rodzaje zdarzeń drogowych. 2. Kompetencje służb na miejscu zdarzenia drogowego. 3. Obowiązki uczestnika zdarzenia drogowego. 4. Sposób postępowania policjanta na miejscu zdarzenia drogowego. 5. Dokumentowanie czynności wykonanych na miejscu kolizji i wypadku drogowego. 6. Polecenia i sygnały wydawane przez policjanta kierującego ruchem. 7. Zabezpieczenie miejsca zdarzenia w rzeczywistości wirtualnej. 8. Wyznaczanie punktów odniesienia i wymiarowanie w rzeczywistości wirtualnej. 9. Prawidłowe wykonywanie czynności na miejscu zdarzenia w wirtualnej rzeczywistości. 10. Zakończenie czynności na miejscu zdarzenia, postępowanie wobec sprawcy zdarzenia.	2	4	-	9	**15**	2	4	-	9	**15**
		Razem:	**5**	**6**	**-**	**19**	**30**	**5**	**6**	**-**	**19**	**30**

Forma zakończenia (S)	**Zaliczenie z oceną**												
Efekty uczenia się	**Metody weryfikacji osiągania efektów uczenia się**												
	Egzamin pisemny	Egzamin ustny	Sprawdzian pisemny	Odpowiedź ustna	Referat	Prezentacja indywidualna	Prezentacja grupowa	Projekt indywidualny	Projekt grupowy	Samodzielna realizacja zdania praktycznego	Zespołowa realizacja zadania praktycznego	Aktywność na zajęciach	Test sprawności fizycznej
EU_1			x	x	x	x		x	x	x	x	x	
EU_2			x	x	x	x		x	x	x	x	x	
EU_3			x	x	x	x		x	x	x	x	x	
EU_4										x	x	x	
EU_5			x	x				x		x		x	
EU_6				x				x	x		x	x	

Nazwa przedmiotu: Nowoczesne technologie w służbie Policji – symulator działań Policji w sytuacjach kryzysowych				
Numer przedmiotu: 38b	**Punkty ECTS:** 2	**Profil kształcenia:** praktyczny	**Dziedzina nauki/dyscyplina naukowa:** nauki społeczne/nauki o bezpieczeństwie	**Język wykładowy:** polski

Efekty uczenia się		**Symbol kierunkowego efektu uczenia się**	**Symbol składnika opisu charakterystyki drugiego stopnia efektów uczenia się dla kwalifikacji na poziomach 6-7 PRK**	**Treści programowe**
w zakresie wiedzy				
EU_1	Zna i rozumie specjalistyczne zagadnienia z zakresu zarządzania kryzysowego oraz organizacji akcji i operacji.	K_W02 K_W11	P7S_WG	W1-3 WP2-3
EU_2	Zna i rozumie zastosowanie symulatorów w systemie kształcenia zawodowego funkcjonariuszy Policji.	K_W06	P7S_WG	W1-3 WP2-3
w zakresie umiejętności				
EU_3	Potrafi w sposób praktyczny wykorzystać możliwości symulatorów do planowana i koordynowania akcji i operacji policyjnych związanych z zabezpieczeniem imprez masowych zgromadzeń i uroczystości.	K_U02 K_U05	P7S_UW	W1-3 WP2-3
EU_4	Potrafi wykorzystać posiadaną wiedzę z zakresu zabezpieczenia imprez masowych w celu rozwiązywania złożonych i nietypowych sytuacji kryzysowych w warunkach nieprzewidywalnych.	K_U02 K_U13	P7S_UW	WP2-3
EU_5	Potrafi samodzielnie planować własny rozwój i uczenie się przez całe życie, ukierunkowywać innych w tym zakresie oraz stale pogłębiać wiedzę z zakresu cyberbezpieczeństwa, w tym z wykorzystaniem różnych źródeł i nowoczesnych technologii	K_U23	P7S_UU	WP2-3
W zakresie kompetencji społecznych				
EU_6	Jest gotów do rozstrzygania dylematów oraz określa priorytety w realizowanych przez siebie lub zespół zadaniach.	K_K02	P7S_KK	W1-3 WP2-3

Lp.	**Temat**	**Tezy**	**Forma studiów:**									
			stacjonarna					**niestacjonarna**				
			Łączna liczba godzin: 30					**Łączna liczba godzin: 30**				
			Wykłady	**Ćwiczenia**	**Zajęcia laboratoryjne**	**Warsztaty praktyczne**	**Razem**	**Wykłady**	**Ćwiczenia**	**Zajęcia laboratoryjne**	**Warsztaty praktyczne**	**Razem**
1.	Symulator działań Policji w sytuacjach kryzysowych	1. Zasady bezpieczeństwa pracowni. 2. Budowa pracowni. 3. Wyposażenie poszczególnych stanowisk. 4. Obsługa na wybranych stanowiskach.	2	-	-	-	**2**	2	-	-	-	**2**

2.	Taktyka działań zespołowych Policji	1. Szyki oddziałów i pododdziałów Policji. 2. Ugrupowania oddziałów i pododdziałów Policji. 3. Przemieszczanie oddziałów i pododdziałów Policji. 4. Używanie środków przymusu bezpośredniego. 5. Łączność w trakcie działań. 6. Metody i formy działań Policji.	2	-	-	4	**6**	2	-	-	4	**6**
3.	Praktyczne wykorzystanie symulatora	1.Budowa i wprowadzanie do scenariusza. 2.Wykonywanie poleceń osób ćwiczących. 3.Omówienie i podsumowanie ćwiczenia.	3	-	-	19	**22**	3	-	-	19	**22**
		Razem:	**7**	**-**	**-**	**23**	**30**	**7**	**-**	**-**	**23**	**30**

Forma zakończenia (S)	**Zaliczenie z oceną**												
Efekty uczenia się	**Metody weryfikacji osiągania efektów uczenia się**												
	Egzamin pisemny	Egzamin ustny	Sprawdzian pisemny	Odpowiedź ustna	Referat	Prezentacja indywidualna	Prezentacja grupowa	Projekt indywidualny	Projekt grupowy	Samodzielna realizacja zdania praktycznego	Zespołowa realizacja zadania praktycznego	Aktywność na zajęciach	Test sprawności fizycznej
EU_1				x							x	x	
EU_2				x							x	x	
EU_3				x							x	x	
EU_4				x							x	x	
EU_5				x								x	
EU_6											x	x	

Symbol efektu uczenia się dla kierunku studiów	Metody weryfikacji osiągania efektów uczenia się													
	Opis efektu uczenia się dla kierunku studiów	**Egzamin pisemny**	**Egzamin ustny**	**Sprawdzian pisemny**	**Odpowiedź ustna**	**Referat**	**Prezentacja indywidualna**	**Prezentacja grupowa**	**Projekt indywidualny**	**Projekt grupowy**	**Samodzielna realizacja zadania praktycznego**	**Zespołowa realizacja zadania praktycznego**	**Aktywność na zajęciach**	**Test sprawności fizycznej**
w zakresie wiedzy – ZNA I ROZUMIE:														
K_W01	wybrane procesy, zjawiska, definicje i teorie w naukach społecznych i innych związanych z kierunkiem studiów, występujące między nimi złożone zależności oraz w pogłębiony sposób wykorzystuje je w rozwiązywaniu problemów bezpieczeństwa w cyberprzestrzeni, w tym w działalności zawodowej	+	+	+	+	+	+	+	+	+	+	+	+	
K_W02	procesy, zjawiska, terminy, definicje i główne tendencje rozwojowe w naukach o bezpieczeństwie, w tym w szczególności w zakresie bezpieczeństwa w cyberprzestrzeni oraz w pogłębiony sposób wykorzystuje je w rozwiązywaniu problemów bezpieczeństwa w cyberprzestrzeni, w tym w działalności zawodowej	+		+	+	+	+	+	+	+	+	+	+	
K_W03	wybrane zagadnienia z zakresu zaawansowanej wiedzy szczegółowej, w tym w szczególności w zakresie informatyki,	+		+	+		+		+	+	+	+	+	

	elektroniki, telekomunikacji i cybernetyki oraz w pogłębiony sposób wykorzystuje je w rozwiązywaniu problemów bezpieczeństwa w cyberprzestrzeni, w tym w działalności zawodowej													
K_W04	metody, techniki, narzędzia stosowane w naukach społecznych, w tym w szczególności w naukach o bezpieczeństwie, służące do wykrywania i zwalczania przestępczości w cyberprzestrzeni oraz w pogłębiony sposób wykorzystuje je w rozwiązywaniu problemów cyberbezpieczeństwa, w tym w działalności zawodowej	+		+	+	+	+	+	+	+	+	+	+	
K_W05	kluczowe metody, techniki i narzędzia stosowane w innych naukach związanych z kierunkiem studiów, w tym w szczególności w informatyce, elektronice, telekomunikacji i cybernetyce, służące do wykrywania i zwalczania przestępczości w cyberprzestrzeni oraz w pogłębiony sposób wykorzystuje je w rozwiązywaniu problemów cyberbezpieczeństwa, w tym w działalności zawodowej	+		+	+		+		+	+	+	+	+	
K_W06	zasady działania i funkcje systemów informatycznych, urządzeń, oprogramowania, nośników danych, aplikacji i innych instrumentów mających wpływ na bezpieczeństwo w cyberprzestrzeni oraz rozumie konieczność ich praktycznego zastosowania w działalności zawodowej	+		+	+	+	+		+	+	+	+	+	
K_W07	systemy norm i reguł prawnych, w tym w szczególności w zakresie bezpieczeństwa w cyberprzestrzeni oraz w pogłębiony sposób wykorzystuje je w rozwiązywaniu problemów	+		+	+	+	+	+	+		+	+	+	

	praktycznych, w tym w działalności zawodowej													
K_W08	specyfikę postępowania dowodowego, w tym w szczególności o przestępstwa w cyberprzestrzeni	+		+	+						+	+	+	
K_W09	zasady ochrony, dostępu, gromadzenia i przetwarzania danych, w tym w szczególności danych cyfrowych	+		+	+	+	+	+	+		+	+	+	
K_W10	zadania i zasady funkcjonowania oraz istotę i zakres współpracy krajowych oraz międzynarodowych organizacji zajmujących się bezpieczeństwem w cyberprzestrzeni i zwalczaniem cyberprzestępczości	+		+	+	+	+	+	+		+	+	+	
K_W11	zasady zarządzania, procesy decyzyjne oraz inne reguły obowiązujące w organizacji, w tym w szczególności w organizacjach zajmujących się bezpieczeństwem w cyberprzestrzeni i zwalczaniem cyberprzestępczości			+	+	+	+	+	+	+	+	+	+	
K_W12	kluczowe elementy infrastruktury bezpieczeństwa, w tym w szczególności infrastruktury krytycznej i cyberbezpieczeństwa			+	+			+				+	+	
K_W13	zróżnicowane zjawiska dewiacyjne i przestępcze oraz czynniki je determinujące, w tym w szczególności w cyberprzestrzeni oraz formy przeciwdziałania i profilaktyki tego rodzaju przestępczości			+	+	+	+	+	+		+	+	+	
K_W14	trendy związane z rozwojem technologii cyfrowych i innych narzędzi informatycznych oraz rozumie ich wpływ na zachowanie człowieka, grup społecznych i innych	+		+	+	+		+	+		+	+	+	

	podmiotów, zarówno w cyberprzestrzeni, jak i środowisku społecznym													
K_W15	fundamentalne dylematy współczesnej cywilizacji i ich wpływ na bezpieczeństwo w cyberprzestrzeni jednostek, grup społecznych i innych podmiotów			+	+	+	+	+	+		+	+	+	
K_W16	ekonomiczne, etyczne i inne uwarunkowania działalności organizacji zajmujących się bezpieczeństwem w cyberprzestrzeni i zwalczaniem cyberprzestępczości			+	+	+	+	+	+	+	+	+	+	
K_W17	zasady skutecznej komunikacji, zarówno w języku polskim, jak i w języku obcym oraz w pogłębiony sposób wykorzystuje je w rozwiązywaniu problemów bezpieczeństwa w cyberprzestrzeni, w tym w działalności zawodowej		+	+	+		+			+	+	+	+	
K_W18	zasady bezpieczeństwa i higieny pracy, ochrony przeciwpożarowej oraz zasady udzielania pierwszej pomocy i wykorzystuje je w działalności zawodowej			+										
K_W19	systemy biblioteczne i informatyczne wykorzystywane w procesie pozyskiwania informacji i pogłębiania wiedzy, w tym w szczególności w zakresie bezpieczeństwa w cyberprzestrzeni										+		+	
w zakresie umiejętności - POTRAFI:														
K_U01	integrować wiedzę oraz wskazywać na zależności procesów i zjawisk z zakresu nauk społecznych i innych nauk związanych z kierunkiem studiów przy formułowaniu i rozwiązywaniu złożonych problemów bezpieczeństwa w cyberprzestrzeni, w tym	+	+	+	+	+	+	+	+	+	+	+	+	

	w działalności zawodowej													
K_U02	wykorzystać pogłębioną wiedzę z nauk o bezpieczeństwie, w tym w szczególności w zakresie bezpieczeństwa w cyberprzestrzeni, przy formułowaniu i rozwiązywaniu złożonych problemów praktycznych oraz zastosować ją podczas realizacji typowych dla działalności zawodowej zadań			+	+	+	+	+	+	+	+	+	+	
K_U03	wykorzystać wybrane elementy zaawansowanej wiedzy szczegółowej w zakresie informatyki, elektroniki, telekomunikacji i cybernetyki przy formułowaniu i rozwiązywaniu złożonych problemów bezpieczeństwa w cyberprzestrzeni oraz zastosować je podczas realizacji złożonych i nietypowych dla działalności zawodowej zadań, również w warunkach nieprzewidywalnych	+		+	+		+		+	+	+	+	+	
K_U04	w sposób prawidłowy dobierać oraz stosować metody, techniki i narzędzia wykorzystywane w naukach społecznych i innych naukach związanych z kierunkiem studiów, użyteczne w rozwiązywaniu złożonych problemów bezpieczeństwa w cyberprzestrzeni			+	+	+	+	+	+	+	+	+	+	
K_U05	w sposób prawidłowy dobierać, przystosować oraz zastosować metody, techniki i narzędzia wykorzystywane w naukach o bezpieczeństwie, użyteczne w rozwiązywaniu typowych problemów bezpieczeństwa w cyberprzestrzeni			+	+				+		+	+	+	
K_U06	w sposób prawidłowy dobierać oraz stosować wybrane metody, techniki i narzędzia zaawansowanej wiedzy szczegółowej	+		+	+		+		+	+	+	+	+	

	w zakresie informatyki, elektroniki, telekomunikacji i cybernetyki oraz zastosować je podczas realizacji złożonych i nietypowych dla działalności zawodowej zadań													
K_U07	analizować i interpretować stany faktyczne z wykorzystaniem właściwych źródeł informacji (baz danych, nośników danych, informacji uzyskanych przy użyciu środków cyfrowych lub elektronicznych) w celu rozwiązywania złożonych problemów bezpieczeństwa w cyberprzestrzeni	+		+	+		+		+	+	+	+	+	
K_U08	w sposób prawidłowy zastosować przepisy prawa, analizować stany faktyczne z wykorzystaniem tych przepisów oraz wnioskować o mechanizmie działania przestępczego i jego sprawcy, w tym w szczególności w sprawach o przestępstwa w cyberprzestrzeni	+		+	+	+	+	+	+	+	+	+	+	
K_U09	zaplanować i przeprowadzić czynności w ramach postępowania dowodowego w sprawach o przestępstwa w cyberprzestrzeni	+		+	+						+	+	+	
K_U10	sporządzić dokumentację, w tym procesową i techniczną, stosownie do sformułowanego problemu z zakresu bezpieczeństwa w cyberprzestrzeni	+		+	+						+	+	+	
K_U11	stosować zasady bezpiecznego przetwarzania, dostępu, gromadzenia i przetwarzania danych, w tym w szczególności danych cyfrowych			+	+	+	+	+			+	+	+	
K_U12	identyfikować zadania i zakres współpracy krajowych oraz międzynarodowych organizacji zajmujących się bezpieczeństwem			+	+	+	+	+				+	+	

	w cyberprzestrzeni i zwalczaniem cyberprzestępczości oraz zastosować tą wiedzę podczas realizacji typowych dla działalności zawodowej zadań													
K_U13	w sposób twórczy wnioskować o przyczynach i przebiegu zjawisk społecznych, w tym przestępczych, i ich wpływie na bezpieczeństwo jednostek, grup społecznych i innych podmiotów, w tym w szczególności w cyberprzestrzeni oraz zastosować tą wiedzę w działalności zawodowej	+		+	+	+	+	+	+	+	+	+	+	
K_U14	samodzielnie wyszukiwać i selekcjonować źródła i informacje, analizować je i krytycznie oceniać, w tym z wykorzystaniem nowoczesnych technologii, w celu rozwiązania złożonego problemu bezpieczeństwa w cyberprzestrzeni			+	+	+	+	+		+	+	+	+	
K_U15	wykorzystywać posiadaną wiedzę z zakresu postępowania z osobą, która uległa wypadkowi										+			
K_U16	udzielić pierwszej pomocy w stanach zagrożenia życia w sytuacjach standardowych i nietypowych										+			
K_U17	samodzielnie korzystać z systemów i zbiorów bibliotecznych i w sposób właściwy pozyskiwać i dobierać źródła wykorzystywane w procesie przygotowania pracy pisemnej lub wystąpień ustnych, w tym w szczególności w zakresie bezpieczeństwa w cyberprzestrzeni										+		+	
K_U18	opracować prace pisemne i udzielić odpowiedzi ustnych stosownie do sformułowanego problemu w zakresie		+	+	+	+	+	+		+	+	+	+	

	bezpieczeństwa w cyberprzestrzeni, w tym z wykorzystaniem specjalistycznej terminologii													
K_U19	stosować reguły komunikacji społecznej, zarówno w języku polskim, jak i w języku obcym oraz przy użyciu zaawansowanych technik komunikacyjnych porozumiewać się ze zróżnicowanymi kręgami odbiorców w sposób precyzyjny i spójny, wykorzystując w tym procesie specjalistyczną terminologię		+	+	+	+	+	+	+	+	+	+	+	
K_U20	posługiwać się językiem obcym na poziomie B2+ Europejskiego Systemu Opisu Kształcenia Językowego		+	+	+		+		+	+	+		+	
K_U21	prezentować własne, innowacyjne pomysły i argumenty, oceniać krytycznie określone stanowiska w kontekście wybranych poglądów, uznanych teorii i opinii innych autorów, prowadzić debatę z użyciem specjalistycznej terminologii		+	+	+	+	+	+	+	+	+	+	+	
K_U22	pracować indywidualnie, a także współdziałać i współpracować w grupie, w szczególności jako lider/kierownik zespołu oraz w strukturach instytucjonalnych działających na rzecz bezpieczeństwa w cyberprzestrzeni i zwalczania cyberprzestępczości, wykazując jednocześnie umiejętność planowania i organizacji tej pracy	+		+	+	+	+	+		+	+	+	+		
K_U23	samodzielnie planować własny rozwój i uczenie się przez całe życie, ukierunkowywać innych w tym zakresie oraz stale pogłębiać wiedzę z zakresu cyberbezpieczeństwa, w tym z wykorzystaniem różnych źródeł			+	+				+		+		+	

	i nowoczesnych technologii													
w zakresie kompetencji społecznych – JEST GOTÓW DO:														
K_K01	uznawania znaczenia wiedzy w rozwiązywaniu złożonych problemów poznawczych i praktycznych w zakresie bezpieczeństwa w cyberprzestrzeni oraz ciągłego jej pogłębiania z wykorzystaniem różnych źródeł wiedzy i nowoczesnych technologii					+		+	+		+	+	+	
K_K02	krytycznej oceny posiadanej wiedzy, w tym zmiany opinii wobec racjonalnych argumentów, a także krytycznej oceny odbieranych treści i stosowanych rozwiązań wykorzystywanych w zakresie bezpieczeństwa w cyberprzestrzeni, w tym również w języku obcym		+		+	+	+	+	+	+	+	+	+	
K_K03	zasięgania opinii ekspertów w przypadku trudności z samodzielnym rozwiązaniem specjalistycznych, złożonych i nietypowych problemów w zakresie bezpieczeństwa w cyberprzestrzeni		+		+	+	+	+	+		+	+	+	
K_K04	wypełniania zobowiązań społecznych oraz aktywnego współdziałania w obszarze cyberbezpieczeństwa na rzecz jednostek, grup społecznych i innych podmiotów społecznych				+			+	+		+	+	+	
K_K05	inicjowania i współorganizowania zróżnicowanych aktywności na rzecz interesu publicznego, w szczególności w zakresie bezpieczeństwa w cyberprzestrzeni i działania w tym zakresie w sposób kreatywny										+	+	+	

K_K06	przestrzegania zasad bezpieczeństwa i higieny pracy, ochrony przeciwpożarowej oraz do udzielania pierwszej pomocy osobie, która uległa wypadkowi, w tym w miejscu pracy											+		
K_K07	odpowiedzialnego pełnienia roli zawodowej, w tym w szczególności przestrzegania i rozwijania zasad etyki zawodowej oraz dbałości o dorobek i tradycje zawodu				+			+	+		+	+	+	

Gdzie:
Symbol (+) oznacza zastosowanie danej metody do weryfikacji kierunkowego uczenia się

Opis zasad i form odbywania praktyk studenckich

Program przewiduje praktyki zawodowe, które są organizowane i odbywają się na zasadach określonych w regulaminie praktyk zawodowych studentów Uczelni, wprowadzonym przez Komendanta-Rektora Wyższej Szkoły Policji w Szczytnie w drodze zarządzenia.

Koncepcja, program i termin praktyki są zintegrowane z procesem uczenia się. Celem praktyki jest połączenie wiedzy teoretycznej nabywanej w toku studiów z jej praktycznym zastosowaniem oraz uzyskanie umiejętności pracy w zespole.

Praktyka w I semestrze I roku studiów:
Czas realizacji: 240 godzin

Cel główny praktyki:

Studenci poznają wybrane aspekty struktur organizacyjnych i zakres działania instytucji realizujących zadania z obszaru bezpieczeństwa w cyberprzestrzeni, w tym walki z zagrożeniami bezpieczeństwa i porządku publicznego.

Cele cząstkowe obejmują:

- zapoznanie się ze strukturą organizacyjną i przepisami regulującymi działanie instytucji,
- zapoznanie się z zakresem działania poszczególnych komórek organizacyjnych i stanowisk komórki,
- zapoznanie się z metodyką pracy właściwą dla działalności instytucji, w której student odbywa praktykę,
- przygotowanie do praktycznego stosowania przepisów stanowiących podstawę realizowanych zadań w instytucji.
- poznanie praktycznego zastosowania przepisów stanowiących podstawę podejmowania czynności w instytucji,
- zapoznanie się z praktycznym zastosowaniem zasad oraz typowych metod służących analizowaniu, syntezowaniu i wnioskowaniu, wykorzystywanych w naukach prawnych,
- zapoznanie się z zasadami związanymi z projektowaniem i kierowaniem zespołami zadaniowymi w obrębie poszczególnych komórek oraz całej jednostki organizacyjnej.

Praktyka w II semestrze I roku studiów:
Czas realizacji: 240 godzin

Cel główny praktyki:

Studenci poznają wybrane aspekty struktur organizacyjnych i zakres działania instytucji realizujących zadania z obszaru bezpieczeństwa w cyberprzestrzeni, w tym walki z zagrożeniami bezpieczeństwa i porządku publicznego.

Cele cząstkowe obejmują:

- wykonywanie zadań techniczno-organizacyjnych, uznanych przez osoby bezpośrednio nadzorujące przebieg praktyki za istotne z punktu widzenia specyfiki działalności instytucji,
- zapoznanie się zasadami opracowywania projektów pism i innej dokumentacji, związanej ze specyfiką działalności instytucji.
- przygotowywanie projektów pism i innej dokumentacji, związanej ze specyfiką działalności instytucji,

- zapoznanie się z zasadami obiegu dokumentacji w instytucji,
- zapoznanie się z zasadami archiwizacji dokumentacji w instytucji.

Praktyka w III semestrze II roku studiów:
Czas realizacji: 240 godzin

Cel główny praktyki:

Studenci poznają praktyczne aspekty funkcjonowania instytucji realizujących zadania z obszaru bezpieczeństwa w cyberprzestrzeni, w tym walki z zagrożeniami bezpieczeństwa i porządku publicznego.

Cele cząstkowe obejmują:

- wykonywanie zadań techniczno-organizacyjnych, uznanych przez osoby bezpośrednio nadzorujące przebieg praktyki za istotne z punktu widzenia specyfiki działalności instytucji,
- zapoznanie się zasadami opracowywania projektów pism i innej dokumentacji, związanej ze specyfiką działalności instytucji,
- przygotowywanie projektów pism i innej dokumentacji, związanej ze specyfiką działalności instytucji,
- zapoznanie się z zasadami obiegu dokumentacji w instytucji,
- zapoznanie się z zasadami archiwizacji dokumentacji w instytucji.

Punkty ECTS przyznawane są po zaliczeniu każdej z praktyk. Łączna liczba punktów ECTS, którą student musi uzyskać realizując praktykę zawodową wynosi 39.