UCHWAŁA NR 208/V/2025
SENATU AKADEMII POLICJI W SZCZYTNIE

z dnia 24 września 2025 r.

w sprawie ustalenia programu studiów podyplomowych w zakresie zwalczania cyberprzestępczości w Akademii Policji w Szczytnie

Na podstawie art. 28 ust. 1 pkt 11 ustawy z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce (Dz. U. z 2024 r., poz. 1571 z późn. zm.) w związku § 15 ust. 1 pkt 9 Statutu Akademii Policji w Szczytnie, uchwalonego uchwałą nr 93/V/2023 Senatu Akademii Policji w Szczytnie z dnia 3 listopada 2023 r. w sprawie uchwalenia statutu zatwierdzonego decyzją nr 41 Ministra Spraw Wewnętrznych i Administracji z dnia 16 listopada 2023 r. w sprawie zatwierdzenia statutu Akademii Policji w Szczytnie (Dz. Urz. MSWiA z 2023 r., poz. 46), uchwala się, co następuje:

§ 1.

Senat Akademii Policji w Szczytnie ustala program studiów podyplomowych w zakresie zwalczania cyberprzestępczości dla uczestników rozpoczynających studia od roku akademickiego 2025/2026 w Akademii Policji w Szczytnie, stanowiący załącznik do uchwały.

§ 2.

Uchwała wchodzi w życie z dniem podjęcia.

Przewodniczący Senatu
Akademii Policji w Szczytnie
Komendant-Rektor

nadinsp. dr Agata Malasińska-Nagórny

Załącznik do Uchwały Nr 208/V/2025
Senatu Akademii Policji w Szczytnie
z dnia 24 września 2025 r.

Akademia Policji
w Szczytnie

Wydział Bezpieczeństwa i Nauk Prawnych

PROGRAM STUDIÓW PODYPLOMOWYCH

w zakresie zwalczania cyberprzestępczości

SZCZYTNO 2025

I. Ogólny opis i charakterystyka studiów podyplomowych.

1. **Nazwa jednostki prowadzącej studia podyplomowe:** Wydział Bezpieczeństwa i Nauk Prawnych
2. **Nazwa studiów podyplomowych:** studia podyplomowe w zakresie zwalczania cyberprzestępczości
3. **Obszar kształcenia/obszary kształcenia, do którego przyporządkowane są studia podyplomowe:** nauki społeczne
4. **Założenia ogólne (ogólna koncepcja kształcenia):**

Głównym celem kształcenia w ramach studiów podyplomowych w zakresie zwalczania cyberprzestępczości jest przygotowanie uczestnika studiów podyplomowych do wykonywania zadań w zakresie:

- Zapewnienia bezpieczeństwa systemów informatycznych i sieci,
- Uzyskiwania danych ze źródeł w cyberprzestrzeni,
- Identyfikacji oraz zabezpieczania sprzętu elektronicznego do odzyskiwania i analizy ich zawartości,
- Funkcjonowania infrastruktury Internetu i wybranych usług sieciowych,
- Programowania w języku Python,
- Zastosowania technik kryptograficznych wykorzystywanych w systemach, teleinformatycznych.

5. **Związek efektów kształcenia z misją i strategią uczelni:**

Misją Akademii Policji w Szczytnie jest rozwijanie wiedzy i kształtowanie umiejętności funkcjonariuszy Policji skutkujących efektywną realizacją zadań służbowych. Uczestnicy studiów podyplomowych w zakresie cyberprzestępczości pogłębią swoją wiedzę i umiejętności w zakresie rozpoznawania i zwalczania cyberprzestępczości oraz identyfikacji zagrożeń bezpieczeństwa pochodzących z sieci.

6. **Różnice w stosunku do innych studiów podyplomowych o podobnie zdefiniowanych celach i efektach uczenia się prowadzonych na uczelni**:

Uczelnia nie realizuje studiów podyplomowych o podobnie zdefiniowanych celach i efektach kształcenia. Niemniej jednak w swojej ofercie posiada studia podyplomowe w zakresie cyberbezpieczeństwa, których treści programowe ukierunkowane są na aspekty bezpieczeństwa teleinformatycznego. Natomiast studia podyplomowe z zakresu zwalczania cyberprzestępczości skierowane są do funkcjonariuszy Policji zajmujących się rozpoznawaniem i zwalczaniem przestępstw popełnianych w cyberprzestrzeni.

7. **Wymagania wstępne:**

Studia podyplomowe w zakresie zwalczania cyberprzestępczości przeznaczone są dla osób legitymujących się dyplomem ukończenia studiów (pierwszego lub drugiego stopnia lub jednolitych studiów magisterskich).

8. **Zasady rekrutacji**:

O przyjęcie na studia podyplomowe w zakresie zwalczania cyberprzestępczości mogą ubiegać się funkcjonariusze oraz pracownicy Policji, którzy uzyskali zgodę przełożonego właściwego w sprawach osobowych na skierowanie na studia podyplomowe. Postępowanie kwalifikacyjne może się odbywać przy użyciu systemu Internetowej Rekrutacji Kandydata (IRK) albo w drodze składania dokumentów. Postępowanie

kwalifikacyjne na studia podyplomowe przeprowadza komisja kwalifikacyjna powołana przez Komendanta-Rektora. Komendant-Rektor określa również jej zadania. Komendant-Rektor określa limity przyjęć na studia podyplomowe w zakresie zwalczania cyberprzestępczości. W zależności od wyników postępowania kwalifikacyjnego, Komendant-Rektor może zmienić limity przyjęć.

9. Warunki ukończenia studiów podyplomowych:

Warunkiem ukończenia studiów podyplomowych jest osiągniecie efektów uczenia się przewidzianych programem studiów podyplomowych oraz aktywne i systematyczne uczestniczenie w zajęciach przewidzianych programem studiów podyplomowych, złożenie wszystkich egzaminów i uzyskanie zaliczeń z przedmiotów przewidzianych programem studiów podyplomowych, uzyskanie 30 punktów ECTS, oraz przystąpienie i uzyskanie pozytywnej oceny z egzaminu końcowego.

Zakres tematyczny egzaminu końcowego powinien dotyczyć tematyki, która obejmuje program studiów podyplomowych możliwie proporcjonalnie do ilości godzin realizowanego przedmiotu. Szczegółowe warunki i zasady przeprowadzania egzaminu końcowego, jego oceniania oraz sposób obliczania ostatecznego wyniku studiów podyplomowych określa *Regulamin studiów podyplomowych w Akademii Policji w Szczytnie*. Absolwent studiów podyplomowych otrzymuje świadectwo ukończenia studiów podyplomowych w zakresie zwalczania cyberprzestępczości.

10. Opis zakładanych efektów uczenia się

Opis zakładanych efektów uczenia się uwzględnia uniwersalne charakterystyki poziomów w PRK określone w ustawie z dnia 22 grudnia 2015 r. o Zintegrowanym Systemie Kwalifikacji (t.j. Dz.U. z 2024 r. poz. 1606 z późn. zm.) oraz charakterystyki drugiego stopnia efektów uczenia się dla kwalifikacji na poziomach 6-8 Polskiej Ramy Kwalifikacji określone w rozporządzeniu Ministra Nauki i Szkolnictwa Wyższego z dnia 14 listopada 2018 r. (Dz. U. z 2018 r., poz. 2218).

Nazwa Wydziału: WYDZIAŁ BEZPIECZEŃSTWA I NAUK PRAWNYCH **Nazwa studiów podyplomowych:** w zakresie zwalczania CYBERPRZESTĘPCZOŚCI **Typ studiów (**kwalifikacyjne/doskonalące): DOSKONALĄCE **Obszar kształcenia/obszary kształcenia, do którego przyporządkowane są studia podyplomowe:** nauki społeczne		
Kod efektu uczenia się	**Zakładane efekty uczenia się dla studiów podyplomowych**	**Odniesienie do ogólnych charakterystyk efektów uczenia się dla kwalifikacji na poziomie 6 Polskiej Ramy Kwalifikacji**
Wiedza		
K_W01	Zna i rozumie specyfikę najczęściej występujących form cyberprzestępczości oraz charakterystyczne metody działania sprawców.	**P6S_WG**
K_W02	Zna i rozumie wybrane pojęcia, procesy i zjawiska związane z bezpieczeństwem w cyberprzestrzeni oraz ich znaczenie dla funkcjonowania współczesnego społeczeństwa.	**P6S_WG**
K_W03	Ma wiedzę dotyczącą najważniejszych funkcji i budowy sieci anonimizujących oraz szyfrowanej poczty elektronicznej.	**P6S_WG**
K_W04	Identyfikuje metody, narzędzia i techniki wykorzystywane	**P6S_WG**

	w informatyce śledczej.	
K_W05	Zna techniki kryptograficzne wykorzystywane obecnie w systemach informatycznych. Zna praktyczne aspekty wykorzystania kryptografii w informatyce.	**P6S_WG**
K_W06	Ma wiedzę dotycząca metod i technik programistycznych. Rozumie wybrane paradygmaty programowania.	**P6S_WG**
Umiejętności		
K_U01	Potrafi wskazać źródła zagrożeń oraz kierunki rozwoju przestępstw popełnianych w cyberprzestrzeni, a także dobierać odpowiednie metody przeciwdziałania tym zagrożeniom.	**P6S_UW**
K_U02	Wykorzystuje wiedzę w procesie pozyskiwania i analizowania informacji służących rozpoznawaniu zagrożeń w sferze cyberbezpieczeństwa.	**P6S_UW**
K_U03	Potrafi świadomie posługiwać się wybranymi narzędziami służącymi do ukrywania tożsamości w cyberprzestrzeni.	**P6S_UW**
K_U04	Potrafi prawidłowo stosować taktyki i techniki zabezpieczenia i analizy dowodów cyfrowych.	**P6S_UW**
K_U05	Posiada umiejętność programowania w wybranym języku oraz stosowania podstawowych pakietów oprogramowania.	**P6S_UW**
K_U06	Potrafi analizować i rozwiązywać proste problemy naukowe i techniczne w oparciu o posiadaną wiedzę, stosując metody analityczne, numeryczne symulacyjne i eksperymentalne.	**P6S_UW**
Kompetencje społeczne		
K_K01	Ma świadomość roli rozwoju technologii informatycznej w kształtowaniu życia społecznego oraz świadomości odpowiedzialności zawodowej funkcjonariusza zwalczającego przestępstwa popełniane w cyberprzestrzeni.	**P6S_KK**
K_K02	Jest gotów do stałego podnoszenia kompetencji oraz aktualizowania wiedzy w dziedzinie prawa, technologii i bezpieczeństwa informatycznego.	**P6S_KK**
K_K03	Jest gotów do oceniania swoich działań i przyjmowania odpowiedzialności za bezpośrednie ich skutki.	**P6S_KK**

Objaśnienia oznaczeń w kodzie:
P – poziom wg. Polskiej Ramy Kwalifikacji
K (przed podkreślnikiem) — kierunkowe Efekty uczenia się
W — kategoria wiedzy
U — kategoria umiejętności
K (po podkreślniku) — kategoria kompetencji społecznych
01, 02, 03 i kolejne — numer efektu kształcenia
- numer efektu w obrębie danej kategorii, zapisany w postaci dwóch cyfr dziesiętnych (numery 1-9 są poprzedzone cyfrą 0)

I. **Opis programu studiów podyplomowych**

1. **Typ studiów podyplomowych:** doskonalące
2. **Język studiów podyplomowych:** polski
3. **Czas trwania studiów podyplomowych (liczba semestrów):** dwa semestry
4. **Ogólna liczba punktów ECTS konieczna do uzyskania kwalifikacji podyplomowych:** 30 punktów ECTS
5. **Ogólna liczba godzin zajęć dydaktycznych:** 259 godzin
6. **Plan studiów podyplomowych:**

PLAN STUDIÓW PODYPLOMOWYCH
WYDZIAŁ: BEZPIECZEŃSTWA I NAUK PRAWNYCH

NAZWA STUDIÓW PODYPLOMOWYCH: studia podyplomowe w zakresie zwalczania cyberprzestępczości

I ROK 1 SEMESTR								
Numer przedmiotu	nazwa przedmiotu	liczba jednostek lekcyjnych (godz.)			forma zakończenia	liczba punktów ECTS		
		łącznie	wykład	ćwiczenia		łącznie	BK*	PS*
1.	Cyberprzestępczość	25	13	12	**S**	**3**	**1,5**	**1,5**
2.	Darknet i anonimizacja w sieci	40	8	32	**E**	**5**	**1,5**	**3,5**
3.	Zabezpieczenie dowodów i sprzętu elektronicznego do badań	40	18	22	**E**	**5**	**2,2**	**2,8**
4.	Przestępstwa z wykorzystaniem kryptowalut	20	10	10	**S**	**2**	**1**	**1**
ŁĄCZNIE w semestrze		**125**	**49**	**76**	-	**15**	**6,2**	**8,8**

I ROK 2 SEMESTR								
Numer przedmiotu	nazwa przedmiotu	liczba jednostek lekcyjnych (godz.)			forma zakończenia	liczba punktów ECTS		
		łącznie	wykład	ćwiczenia		łącznie	BK*	PS*
5.	Odzyskiwanie i analiza danych z nośników cyfrowych	40	10	30	**E**	**5**	**1,3**	**3,7**
6.	Programowanie w języku Python	40	10	30	**E**	**5**	**1,3**	**3,7**
7.	Live Forensics	20	6	14	**S**	**2**	**1,4**	**0,6**
8.	Pozyskiwanie danych z Internetu	20	7	13	**S**	**3**	**1**	**2**
9.	Konsultacje	**6**			**-**	**-**	**-**	**-**
10.	Egzamin końcowy	**8**			**-**	**-**	**-**	**-**
ŁĄCZNIE w semestrze		**120+14**	**33**	**87**	**-**	**15**	**5**	**10**

ECTS	semestr 1	semestr 2	Razem:
Łączna liczba punktów ECTS	**15**	**15**	**30**
BK**	6,2	5	11,2
PS**	8,8	10	18,8

LEGENDA:
- FORMA ZAKOŃCZENIA: E – egzamin; **S –** zaliczenie z oceną**; Z –** zaliczenie
- LICZBA PUNKTÓW ECTA: BK - liczba punktów ECTS za bezpośredni kontakt z nauczycielem; **PS -** liczba punktów ECTS za pracę samodzielną

7. Wykaz przedmiotów wraz z przypisaną im liczbą punktów ECTS i odniesieniem do efektów uczenia się

Cyberprzestępczość			**Przedmiot nr 1**		
Efekty uczenia się w zakresie: **Wiedzy:** - Zna i rozumie akty prawne dotyczące cyberprzestępczości, regulacje międzynarodowe oraz przepisy prawa polskiego. - Zna i rozumie specyfikę najczęściej występujących form cyberprzestępczości oraz metody działania sprawców tych przestępstw. **Umiejętności:** - Potrafi rozpoznać źródła zagrożeń w cyberprzestrzeni i przeciwdziałać im. - Potrafi wskazać kierunki rozwoju cyberprzestępczości. **Kompetencji społecznych:** - Jest świadomy znaczenia odpowiedzialnego i bezpiecznego korzystania z technologii informatycznych w zakresie zwalczania cyberprzestępczości.			**Czas realizacji** **godz. 25**		
Lp.	**Temat**	**Tezy**	Wykład	Ćwiczenia	**Razem**
1	**Przestępstwa komputerowe w świetle polskich i międzynarodowych przepisów**	1. Konwencja o cyberprzestępczości i inne przepisy prawa międzynarodowego. 2. Przepisy prawa polskiego w zakresie cyberprzestępczości.	2	0	**2**
2	**Cyberprzestępstwa**	1. Phishing. 2. Kradzież tożsamości. 3. Oszustwo telekomunikacyjne. 4. Przestępczość z wykorzystaniem elektronicznych instrumentów płatniczych. 5. Złośliwe oprogramowanie. 6. Cyberprzestępczość jako usługa.	9	10	**19**
3	**Charakterystyka cyberprzestępczości w Polsce**	1. Specyfikacja zagrożeń i przestępstw w cyberprzestrzeni. 2. Charakterystyka i metody działania sprawców. 3. Profilaktyka w zakresie cyberbezpieczeństwa.	2	2	**4**
		Razem:	13	12	25

Sposób zakończenia: Zaliczenie z oceną (1 godz.)	**Punkty ECTS: 3**

<table>
<tr><td colspan="4">Darknet i anonimizacja w sieci</td><td colspan="3">Przedmiot nr 2</td></tr>
<tr><td colspan="4" rowspan="2">Efekty uczenia z zakresu:
Wiedzy:
- Zna pojęcie Darknetu i rozumie zasadę jego funkcjonowania.
- Zna i rozumie funkcjonowanie sieci animizujących w Internecie
- Zna zasadę działania szyfrowanej poczty z wykorzystaniem kluczy PGP.
Umiejętności:
- Potrafi instalować i konfigurować narzędzia anonimizujące.
- Potrafi posługiwać się wybranymi narzędziami służącymi do anonimizacji w cyberprzestrzeni.
- Potrafi generować, zarządzać i stosować klucze kryptograficzne (PGP) w procesie bezpiecznej komunikacji
- Potrafi identyfikować zagrożenia wynikające z niewłaściwego korzystania z anonimowych usług w sieciach darknetowych i szyfrowanych kanałach komunikacji.
Kompetencji społecznych:
- Jest gotów do uznawania wiedzy w rozwiązywani problemów z zakresu technik ukrywania tożsamości w Internecie oraz zasięgania opinii ekspertów w przypadku trudności z samodzielnym ich rozwiązaniem.
- Jest świadomy etycznego i prawnego wymiaru korzystania z rozwiązań zwiększających anonimowość i bezpieczeństwo komunikacji.</td><td colspan="3">Czas realizacji</td></tr>
<tr><td colspan="3">godz. 40</td></tr>
<tr><td>Lp.</td><td>Temat</td><td>Tezy</td><td>Wykład</td><td>Ćwiczenia</td><td>Razem</td></tr>
<tr><td>1</td><td>Ciemna strona Internetu</td><td>1. Podstawowe pojęcia.
2. Deepweb/Darkweb.
3. Darknet jako źródło informacji oraz zagrożeń.</td><td>2</td><td>0</td><td>2</td></tr>
<tr><td>2</td><td>Serwery PROXY</td><td>1. Rodzaje serwerów PROXY i zasada ich działania.
2. Przykłady wykorzystania.</td><td>2</td><td>10</td><td>12</td></tr>
<tr><td>3</td><td>Sieci wirtualne</td><td>1. Zasada działania i rodzaje sieci wirtualnych.
2. TOR.
3. Freenet.</td><td>2</td><td>12</td><td>14</td></tr>
<tr><td>4</td><td>Bezpieczna poczta</td><td>1. Protonmail, Tutanota i inne.
2. Klucze PGP, tokeny.
3. Wykorzystanie szyfrowanej poczty.</td><td>2</td><td>10</td><td>12</td></tr>
<tr><td colspan="3">Razem:</td><td>8</td><td>32</td><td>40</td></tr>
<tr><td colspan="4">Sposób zakończenia: Egzamin (1 godz.)</td><td colspan="3">Punkty ECTS: 5</td></tr>
</table>

Zabezpieczenie dowodów i sprzętu elektronicznego do badań			**Przedmiot nr 3**		
Efekty uczenia się z zakresu: **Wiedzy:** - Zna metodykę zabezpieczania sprzętu elektronicznego do badań. - Zna zasadę działania narzędzi wykorzystywanych podczas zabezpieczania sprzętu elektronicznego. - Zna zasady powoływania biegłego z zakresu informatyki śledczej. **Umiejętności:** - Potrafi zabezpieczyć nośniki cyfrowe i sprzęt elektroniczny do badań. - Potrafi określić źródła dowodowe dotyczące śladów i dowodów cyfrowych. - Potrafi dokonać wstępnej identyfikacji sprzętu elektronicznego do badań. **Kompetencji społecznych:** - Jest gotów uznawania znaczenia wiedzy w rozwiązywaniu problemów poznawczych i praktycznych w zakresie zabezpieczania śladów i dowodów cyfrowych.			**Czas realizacji** **40 godz.**		
Lp.	**Temat**	**Tezy**	Wykład	Ćwiczenia	**Razem**
1	**Zasady zabezpieczania sprzętu elektronicznego do badań**	1. Wybrane pojęcia związane z zabezpieczaniem sprzętu komputerowego. 2. Algorytmy zabezpieczania sprzętu komputerowego do badań.	4	0	**4**
2	**Identyfikacja sprzętu elektronicznego do badań**	1. Budowa i podział sprzętu elektronicznego. 2. Klasyfikacja sprzętu elektronicznego pod kątem możliwości badawczych. 3. Odnajdywanie cech indywidualnych zabezpieczanych urządzeń.	4	2	**6**
3	**Zabezpieczenie sprzętu elektronicznego do badań**	1. Przygotowanie do zabezpieczenia sprzętu 2. elektronicznego. 3. Dobór odpowiedniej metody zabezpieczenia do rodzaju sprzętu. 4. Zabezpieczenie procesowe i techniczne. 5. Zabezpieczenie przed ingerencją w dane oraz uszkodzeniem mechanicznym. 6. Transport i przechowywanie. 7. Najczęstsze błędy podczas zabezpieczania sprzętu komputerowego. 8. Sposoby ochrony po stronie przestępców (time bomb, panic buton).	6	12	**18**
4	**Współpraca z biegłym**	1. Sporządzenie Postanowienia o dopuszczeniu dowodu z opinii biegłego. 2. Zaprezentowanie i omówienie przykładowych opinii.	1	1	**2**
5	**Współpraca z dostawcami usług chmurowych**	1. Zabezpieczenie danych u dostawców usług hostingowych. 2. Zabezpieczenie serwerów wirtualnych 3. Zabezpieczanie logów. 4. Zabezpieczenie danych transakcyjnych właściciela systemu (kupno usługi).	2	8	**10**

Razem:	**18**	**22**	**40**

Sposób zakończenia: Egzamin (1 godz.)	**Punkty ECTS: 5**

Przestępstwa z wykorzystaniem kryptowalut	**Przedmiot nr 4**
Efekty uczenia się z zakresu: **Wiedzy:** - Zna genezę powstania i mechanizmy działania wybranych kryptowalut oraz rozumie technologię blockchain w tym mechanizmy konsensusu i walidacji transakcji. - Zna wybrane portfele kryptowalut, rozumie ich architekturę, sposoby przechowywania kluczy i związane z nimi poziomy bezpieczeństwa. - Zna i rozumie najważniejsze techniczne metody oraz procesowe rozwiązania służące zabezpieczaniu kryptowalut. **Umiejętności:** - Potrafi użyć ogólnodostępnych narzędzi do analizy i śledzenia wybranych kryptowalut. - Potrafi korzystać z wybranych portfeli kryptowalut z uwzględnieniem zasad bezpieczeństwa - Potrafi technicznie i procesowo zabezpieczać wybrane kryptowaluty. **Kompetencji społecznych:** - Jest świadomy etycznych i prawnych konsekwencji korzystania z kryptowalut, w tym zagrożeń związanych z ich wykorzystaniem do działań przestępczych.	**Czas realizacji** **godz. 20**

Lp.	**Temat**	**Tezy**	Wykład	Ćwiczenia	**Razem**
1	**Geneza kryptowalut**	1. Geneza i początek bitcoina. 2. Powstanie altcoinów. 3. Rozwój i dalsza przyszłość kryptowalut.	2	0	**2**
2	**Wybrane kryptowaluty i mechanizmy ich funkcjonowania**	1. BTC – Bitcoin. 2. ETH – Ethereum. 3. XMR – Monero. 4. Altcoiny.	2	0	**2**
3	**Portfele**	1. Programowe. 2. Sprzętowe. 3. Online.	2	4	**6**
4	**Analiza kryptowalut**	1. Aspekty ekonomiczne. 2. Zastosowanie. 3. Bezpieczeństwo.	2	3	**5**
5	**Zabezpieczanie kryptowalut**	1. Techniczne. 2. Procesowe.	2	3	**5**
		Razem:	**10**	**10**	**20**

Sposób zakończenia: Zaliczenie z oceną (1 godz.)	**Punkty ECTS: 2**

<table>
<tr><td colspan="4">Odzyskiwanie i analiza danych z nośników cyfrowych</td><td colspan="3">Przedmiot nr 5</td></tr>
<tr><td colspan="4">Efekty uczenia się z zakresu:
Wiedzy:
- Zna funkcjonalność wybranego oprogramowania i jego zastosowania do odzyskiwania danych z nośników cyfrowych.
- Zna metody, techniki oraz narzędzia stosowane przy analizie elektronicznego materiału dowodowego.
Umiejętności:
- Potrafi odzyskać dane z wybranych nośników elektronicznych.
- Potrafi dobrać optymalną metodę odzyskiwania danych w zależności od rodzaju nośnika.
- Potrafi analizować dane, a także umiejętnie interpretować otrzymane wyniki.
Kompetencji społecznych:
- Jest gotów do krytycznej oceny posiadanej wiedzy z zakresu możliwości odzyskiwania danych z nośników cyfrowych.</td><td colspan="3">Czas realizacji

godz. 40</td></tr>
<tr><td>Lp.</td><td>Temat</td><td>Tezy</td><td>Wykład</td><td>Ćwiczenia</td><td>Razem</td></tr>
<tr><td>1</td><td>Odzyskiwanie danych z elektronicznych nośników pamięci</td><td>1. Rodzaje nośników danych oraz sposoby ich zabezpieczania.
2. Rodzaje systemów operacyjnych i akwizycja danych w tych systemach.
3. Zasada działania i zastosowanie programowych i sprzętowych blokerów danych.
4. Rodzaje kopii binarnych oraz metody ich wykonywania w zależności od typu zabezpieczonego urządzenia.
5. Narzędzia stosowane od odzyskiwania danych z cyfrowych nośników.
6. Obliczanie funkcji skrótu i jej znaczenie w łańcuchu dowodowym.</td><td>4</td><td>12</td><td>16</td></tr>
<tr><td>2</td><td>Analiza odzyskanych danych</td><td>1. Analiza odzyskanych danych z wykorzystaniem oprogramowania stosowanego w informatyce śledczej
2. Interpretacja wyników.</td><td>2</td><td>4</td><td>6</td></tr>
<tr><td>3</td><td>Analiza zaszyfrowanych kontenerów danych</td><td>1. Analiza zaszyfrowanych kontenerów danych.
2. Mechanizmy kryptograficzne wbudowane w systemy operacyjne.
3. Praca z zaszyfrowanymi nośnikami danych – wykrywanie zaszyfrowanych plików i kontenerów danych, rozpoznawanie typu szyfrowania, możliwości i narzędzia do deszyfracji.
4. Taktyka przeprowadzania ataków na szyfrowane pliki. Dobre praktyki.</td><td>2</td><td>4</td><td>6</td></tr>
<tr><td>4</td><td>Analiza pamięci RAM, plików hiberfil.sys i pagefile.sys</td><td>1. Analiza zrzutów pamięci.
2. Analiza plików hiberfil.sys i pagefile.sys.
3. Analiza rejestrów systemów operacyjnych.
4. Zabezpieczenie i analiza danych ulotnych w systemach operacyjnych – możliwości i ograniczenia.</td><td>2</td><td>8</td><td>10</td></tr>
</table>

		5. Zagrożenia związane z zabezpieczeniem pamięci ulotnej.			
5	**Dokumentowanie czynności z analizy cyfrowych nośników danych**	1. Sporządzanie dokumentacji.	0	2	**2**
		Razem:	**10**	**30**	**40**

Sposób zakończenia: Egzamin (1 godz.)	**Punkty ECTS: 5**

<table>
<tr><td colspan="3">Programowanie w języku Python</td><td colspan="3">Przedmiot nr 6</td></tr>
<tr><td colspan="3" rowspan="2">Efekty uczenia się w zakresie:
Wiedzy:
- Zna i rozumie zasady tworzenia i analizy oprogramowania w środowisku Python.
- Zna typowe problemy i algorytmy programowania w języku Python.
Umiejętności:
- Potrafi poprawnie zainstalować i skonfigurować Pythona.
- Potrafi tworzyć proste programy wykorzystujące podstawowe typy danych, operatory oraz podstawowe struktury sterujące.
- Potrafi tworzyć programy wykorzystujące proste funkcje zwracające wartość.
- Potrafi dokonywać operacji na plikach: otwieranie, czytanie, pisanie i zamykanie plików.
- Potrafi rozwiązywać wybrane problemy powstające w trakcie tworzenia oprogramowania w środowisku Pythona.
Kompetencji społecznych:
- Jest gotowy do pogłębionej analizy i krytycznej oceny posiadanej wiedzy z zakresu programowania w języku Python oraz zasięgania opinii ekspertów w przypadku trudności z samodzielnym rozwiązaniem problemu programistycznego.</td><td colspan="3">Czas realizacji</td></tr>
<tr><td colspan="3">godz. 40</td></tr>
<tr><td>Lp.</td><td>Temat</td><td>Tezy</td><td>Wykład</td><td>Ćwiczenia</td><td>Razem</td></tr>
<tr><td>1</td><td>Wstęp do programowania w języku Python</td><td>1. Semantyka, syntaktyka, wprowadzenie do algorytmiki.</td><td>2</td><td>4</td><td>6</td></tr>
<tr><td>2</td><td>Przetwarzanie tekstu, ekstrakcja danych i analiza</td><td>1. Analiza logów.
2. Regex.
3. Analiza SQLite.
4. Sumy kontrolne.</td><td>4</td><td>14</td><td>18</td></tr>
<tr><td>3</td><td>Przetwarzanie danych</td><td>1. Podstawy numpy i pandas.
2. Wizualizacja danych, ekstrakcja danych z dokumentu HTML.
3. Ekstrakcja danych ze źródeł internetowych.
4. Scrapowanie stron internetowych.</td><td>4</td><td>12</td><td>16</td></tr>
<tr><td colspan="3">Razem:</td><td>10</td><td>30</td><td>40</td></tr>
<tr><td colspan="3">Sposób zakończenia: Egzamin (1 godz.)</td><td colspan="3">Punkty ECTS: 5</td></tr>
</table>

<table>
<tr><td colspan="3">Live forensics</td><td colspan="3">Przedmiot nr 7</td></tr>
<tr><td colspan="3" rowspan="2">Efekty uczenia się z zakresu:
Wiedzy:
- Zna i rozumie istotę informatyki śledczej w zakresie zabezpieczania danych metodą Live Forensics.
- Zna zaawansowane metody, techniki, narzędzia i materiały stosowane przy zabezpieczaniu elektronicznego materiału dowodowego metodą Live Forensics.
Umiejętności:
- Potrafi właściwie dobrać rodzaj urządzenia oraz metodę Live Forensics.
- Potrafi analizować zabezpieczone dane.
Kompetencji społecznych:
- Jest gotów do oceny swoich działań i przyjmowania odpowiedzialności za bezpośrednie ich skutki.</td><td colspan="3">Czas realizacji</td></tr>
<tr><td colspan="3">20 godz.</td></tr>
<tr><td>Lp.</td><td>Temat</td><td>Tezy</td><td>Wykład</td><td>Ćwiczenia</td><td>Razem</td></tr>
<tr><td>1</td><td>Wprowadzenie do Live Forensics – aspekty prawne</td><td>1. Podstawowe narzędzia i oprogramowanie Live Forensics.
2. Zagadnienia prawne związane z zabezpieczaniem danych metodą Live Forensics.</td><td>2</td><td>0</td><td>2</td></tr>
<tr><td>2</td><td>Zabezpieczenie materiału dowodowego metodą Live Forensics</td><td>1. Metodyka Triage w informatyce śledczej.
2. Konfiguracja narzędzi.
3. Zabezpieczanie danych z różnych typów urządzeń.
4. Zabezpieczanie danych z nośników ulotnych.</td><td>2</td><td>10</td><td>12</td></tr>
<tr><td>3</td><td>Analiza danych</td><td>1. Analiza danych z urządzeń.
2. Analiza danych z nośników ulotnych.</td><td>2</td><td>4</td><td>6</td></tr>
<tr><td colspan="3">Razem:</td><td>6</td><td>14</td><td>20</td></tr>
</table>

Sposób zakończenia: Zaliczenie z oceną (1 godz.)	**Punkty ECTS: 2**

<table>
<tr><td colspan="3">Pozyskiwanie danych z Internetu</td><td colspan="3">Przedmiot nr 8</td></tr>
<tr><td colspan="3" rowspan="2">Efekty uczenia z zakresu:
Wiedzy:
- Zna wybrane pojęcia dotyczące źródeł informacji w internecie.
- Zna wybrane narzędzia oraz techniki wykorzystywane przy gromadzeniu informacji z internetu.
Umiejętności:
- Potrafi używać ogólnodostępnych narzędzi do pozyskiwania informacji z otwartych źródeł w Internecie.
- Potrafi ocenić przydatność uzyskanych informacji.
Kompetencji społecznych:
- Jest świadomy etycznych i prawnych aspektów korzystania z informacji pozyskiwanych z internetowych źródeł oraz potrafi stosować je w sposób odpowiedzialny i zgodny z obowiązującymi regulacjami.</td><td colspan="3">Czas realizacji</td></tr>
<tr><td colspan="3">20 godz.</td></tr>
<tr><td>Lp.</td><td>Temat</td><td>Tezy</td><td>Wykład</td><td>Ćwiczenia</td><td>Razem</td></tr>
<tr><td>1</td><td>Wprowadzenie do ogólnodostępnych źródeł informacji w internecie</td><td>1. Identyfikacja dostępnych źródeł informacji.
2. Podstawy prawne uzyskiwania i gromadzenia informacji ze źródeł internetowych.</td><td>2</td><td>0</td><td>2</td></tr>
<tr><td>2</td><td>Wybrane narzędzia przydatne w uzyskiwaniu informacji z internetu</td><td>1. Zaawansowane wykorzystanie wyszukiwarek internetowych.
2. Rejestry domen internetowych.
3. Wykorzystanie portali rządowych do wyszukiwania informacji gospodarczych.
4. Baza ubezpieczycieli i UFG.
5. Mapy i zdjęcia, geolokalizacja.
6. Narzędzia do analizy metadanych.
7. Wyszukiwanie osób w mediach społecznościowych.</td><td>2</td><td>8</td><td>10</td></tr>
<tr><td>3</td><td>Rozpoznanie zagrożeń cyberprzestrzeni (Cyber Threat Intelligence CTI)</td><td>1. Idea CTI.
2. Modelowanie zagrożeń.
3. Narzędzia wspomagające CTI.</td><td>2</td><td>6</td><td>8</td></tr>
<tr><td colspan="3">Razem:</td><td>7</td><td>13</td><td>20</td></tr>
</table>

Sposób zakończenia: Zaliczenie z oceną (1 godz.)	**Punkty ECTS: 3**

Macierz efektów uczenia się
dla programu studiów podyplomowych w zakresie *zwalczania cyberprzestępczości*

Kod efektu uczenia się dla programu studiów podyplomowych	**Opis efektu uczenia się dla programu studiów podyplomowych**	**Przedmioty**							
		NP_1	NP_2	NP_3	NP_4	NP_5	NP_6	NP_7	NP_8
		Cyberprzestępczość.	Darknet i anonimizacja w sieci.	Zabezpieczanie dowodów i sprzętu elektronicznego do badań.	Przestępstwa z wykorzystaniem kryptowalut.	Odzyskiwanie i analiza danych z nośników cyfrowych.	Programowanie w języku Python.	Live Forensics.	Pozyskiwanie danych z internetu.
K_W01	Zna i rozumie specyfikę najczęściej występujących form cyberprzestępczości oraz charakterystyczne metody działania sprawców.	+	+	+	+	+		+	+
K_W02	Zna i rozumie wybrane pojęcia, procesy i zjawiska związane z bezpieczeństwem w cyberprzestrzeni oraz ich znaczenie dla funkcjonowania współczesnego społeczeństwa.	+	+		+			+	+
K_W03	Ma wiedzę dotyczącą najważniejszych funkcji i budowy sieci anonimizujących oraz szyfrowanej poczty elektronicznej.		+	+	+	+		+	+
K_W04	Identyfikuje metody, narzędzia i techniki wykorzystywane w informatyce śledczej.		+	+	+	+		+	+

K_W05	Zna techniki kryptograficzne wykorzystywane obecnie w systemach informatycznych. Zna praktyczne aspekty wykorzystania kryptografii w informatyce.		+		+	+		+	
K_W06	Ma wiedzę dotycząca metod i technik programistycznych. Rozumie wybrane paradygmaty programowania.						+		
K_U01	Potrafi wskazać źródła zagrożeń oraz kierunki rozwoju przestępstw popełnianych w cyberprzestrzeni, a także dobierać odpowiednie metody przeciwdziałania tym zagrożeniom.	+			+			+	
K_U02	Wykorzystuje wiedzę w procesie pozyskiwania i analizowania informacji służących rozpoznawaniu zagrożeń w sferze cyberbezpieczeństwa.		+	+	+	+		+	
K_U03	Potrafi świadomie posługiwać się wybranymi narzędziami służącymi do ukrywania tożsamości w cyberprzestrzeni.	+	+		+				+
K_U04	Potrafi prawidłowo stosować taktyki i techniki zabezpieczenia i analizy dowodów cyfrowych.		+	+	+	+		+	+
K_U05	Posiada umiejętność programowania w wybranym języku oraz stosowania podstawowych pakietów oprogramowania.						+		
K_U06	Potrafi analizować i rozwiązywać proste problemy naukowe i techniczne w oparciu o posiadaną wiedzę, stosując metody analityczne, numeryczne symulacyjne i eksperymentalne.	+	+	+	+	+	+	+	+
K_K01	Ma świadomość roli rozwoju technologii informatycznej w kształtowaniu życia społecznego oraz świadomości odpowiedzialności zawodowej funkcjonariusza zwalczającego przestępstwa popełniane w cyberprzestrzeni.	+	+		+		+	+	+
K_K02	Jest gotów do stałego podnoszenia kompetencji oraz aktualizowania wiedzy w dziedzinie prawa, technologii i bezpieczeństwa informatycznego.	+	+	+	+	+	+	+	+

K_K03	Jest gotów do oceniania swoich działań i przyjmowania odpowiedzialności za bezpośrednie ich skutki.	+	+	+	+	+	+	+	+

Objaśnienia:
Kod efektu tworzą:
K (przed podkreślnikiem) — Efekty uczenia się dla programu kształcenia studiów podyplomowych
W — kategoria wiedzy
U — kategoria umiejętności
K (po podkreślniku) — kategoria kompetencji społecznych
01, 02, 03 i kolejne — numer efektu kształcenia
– MK_1 ….. MK_m kody modułów kształcenia (przedmiotów) – zgodnie z przypisanymi numerami w programie kształcenia; obok kodów modułów kształcenia (przedmiotów) MK_1 ….. MK_m mogą występować nazwy modułów/przedmiotów

8. Sposoby weryfikacji zakładanych efektów uczenia się osiąganych przez uczestnika studiów podyplomowych:

Symbol efektów uczenia się dla programów kształcenia	Efekt uczenia się	Metody weryfikacji efektów uczenia się					
		egzamin ustny/ zaliczenie ustne	egzamin pisemny/ zaliczenie pisemne	test wiedzy/ umiejętności/ kolokwium	prezentacje/ referaty	praca w zespole	realizacja zadania praktycznego
K_W01	Zna i rozumie specyfikę najczęściej występujących form cyberprzestępczości oraz charakterystyczne metody działania sprawców.		+	+			
K_W02	Zna i rozumie wybrane pojęcia, procesy i zjawiska związane z bezpieczeństwem w cyberprzestrzeni oraz ich znaczenie dla funkcjonowania współczesnego społeczeństwa.		+	+			
K_W03	Ma wiedzę dotyczącą najważniejszych funkcji i budowy sieci anonimizujących oraz szyfrowanej poczty elektronicznej.		+	+			
K_W04	Identyfikuje metody, narzędzia i techniki wykorzystywane w informatyce śledczej.		+	+			
K_W05	Zna techniki kryptograficzne wykorzystywane obecnie w systemach informatycznych. Zna praktyczne aspekty wykorzystania kryptografii w informatyce.		+	+			
K_W06	Ma wiedzę dotycząca metod i technik programistycznych. Rozumie wybrane paradygmaty programowania.		+	+			
K_U01	Potrafi wskazać źródła zagrożeń oraz kierunki rozwoju przestępstw popełnianych w cyberprzestrzeni, a także dobierać odpowiednie metody przeciwdziałania tym zagrożeniom.			+		+	+
K_U02	Wykorzystuje wiedzę w procesie pozyskiwania i analizowania informacji służących rozpoznawaniu zagrożeń w sferze cyberbezpieczeństwa.			+		+	+
K_U03	Potrafi świadomie posługiwać się wybranymi narzędziami służącymi do ukrywania tożsamości w cyberprzestrzeni.			+		+	+
K_U04	Potrafi prawidłowo stosować taktyki i techniki zabezpieczenia i analizy dowodów cyfrowych.			+		+	+

K_U05	Posiada umiejętność programowania w wybranym języku oraz stosowania podstawowych pakietów oprogramowania.			+		+	+
K_U06	Potrafi analizować i rozwiązywać proste problemy naukowe i techniczne w oparciu o posiadaną wiedzę, stosując metody analityczne, numeryczne symulacyjne i eksperymentalne.			+		+	+
K_K01	Ma świadomość roli rozwoju technologii informatycznej w kształtowaniu życia społecznego oraz świadomości odpowiedzialności zawodowej funkcjonariusza zwalczającego przestępstwa popełniane w cyberprzestrzeni.			+		+	+
K_K02	Jest gotów do stałego podnoszenia kompetencji oraz aktualizowania wiedzy w dziedzinie prawa, technologii i bezpieczeństwa informatycznego.			+		+	+
K_K03	Jest gotów do oceniania swoich działań i przyjmowania odpowiedzialności za bezpośrednie ich skutki.			+		+	+