**UCHWAŁA NR 24/V/2023**
**SENATU WYŻSZEJ SZKOŁY POLICJI W SZCZYTNIE**

z dnia 30 stycznia 2023 r.

**w sprawie ustalenia programu studiów na studiach podyplomowych w zakresie zwalczania cyberprzestępczości w Wyższej Szkole Policji w Szczytnie**

Na podstawie art. 28 ust. 1 pkt 11 ustawy z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce (t.j. Dz. U. z 2022 r., poz.574) w związku § 15 ust. 1 pkt 9 Statutu Wyższej Szkoły Policji w Szczytnie, uchwalonego uchwałą nr 53/IV/2019 Senatu Wyższej Szkoły Policji w Szczytnie z dnia 10 września 2019 r. w sprawie uchwalenia statutu zatwierdzonego decyzją nr 54 Ministra Spraw Wewnętrznych i Administracji z dnia 27 września 2019 r. w sprawie zatwierdzenia statutu Wyższej Szkoły Policji w Szczytnie (Dz. Urz. MSWiA z 2019 r., poz. 39), uchwala się, co następuje:

**§ 1.**

Senat Wyższej Szkoły Policji w Szczytnie ustala program studiów na studiach podyplomowych w zakresie zwalczania cyberprzestępczości dla uczestników rozpoczynających studia od roku akademickiego 2022/2023 w Wyższej Szkole Policji w Szczytnie, stanowiący załącznik do uchwały.

**§ 2.**

Uchwała wchodzi w życie z dniem podjęcia.

**Przewodniczący Senatu**
**Wyższej Szkoły Policji w Szczytnie**
**Komendant-Rektor**

**nadinsp. dr hab. Iwona Klonowska, prof. WSPol**

Załącznik do Uchwały Nr 24/V /2023
Senatu Wyższej Szkoły Policji
w Szczytnie z dnia 30 stycznia 2023 r.

# Wyższa Szkoła Policji
## w Szczytnie

## Wydział Bezpieczeństwa i Nauk Prawnych

# PROGRAM STUDIÓW PODYPLOMOWYCH

## *w zakresie zwalczania cyberprzestępczości*

SZCZYTNO 2023

# 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 z otwartych 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 kryptografii w cyberprzestrzeni.

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

   Misją Wyższej Szkoły Policji w Szczytnie jest rozwijanie wiedzy i kształtowanie umiejętności funkcjonariuszy Policji skutkujących efektywną realizacją zadań służbowych. Uczestnicy studiów podyplomowych w zakresie cyberprzestępczości pogłębią swoje 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. Komendant – Rektor określa zasady postępowania kwalifikacyjnego, wymagane dokumenty oraz warunki przyjęcia. 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 Wyższej Szkole Policji*

*w Szczytnie*. Absolwent studiów podyplomowych otrzymuje świadectwo ukończenia studiów podyplomowych w zakresie zwalczania cyberprzestępczości.

## I. 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 2020 r. poz. 226) 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** | Ma wiedzę dotyczącą prawnych i społecznych aspektów informatyki w tym własności intelektualnej prywatności i swobód obywatelskich ryzyka i odpowiedzialności związanej z systemami informatycznymi. | **P6S_WG** |
| **K_W02** | Ma wiedzę dotyczącą najważniejszych funkcji i budowy systemów i sieci teleinformatycznych oraz trendów ich rozwoju. | **P6S_WG** |
| **K_W03** | Identyfikuje metody, narzędzia i techniki wykorzystywane w informatyce śledczej. | **P6S_WG** |
| **K_W04** | Ma wiedzę dotycząca metod i technik programistycznych. Rozumie wybrane paradygmaty programowania. | **P6S_WG** |
| **K_W05** | Zna techniki kryptograficzne wykorzystywane obecnie w systemach informatycznych. Zna praktyczne aspekty wykorzystania kryptografii w informatyce. | **P6S_WG** |
| **Umiejętności** | | |
| **K_U01** | Potrafi wskazać źródła zagrożeń oraz kierunki rozwoju przestępstw popełnianych w cyberprzestrzeni. | **P6S_UW** |
| **K_U02** | Wykorzystuje wiedzę w procesie pozyskiwania i analizowania informacji służących rozpoznawaniu zagrożeń w sferze cyberbezpieczeństwa. | **P6S_UW** |
| **K_U03** | Potrafi poznawać, analizować i modelować wymagania stawiane systemom informatycznym przez użytkowników a także projektować i implementować systemy informatyczne spełniające wymagania użytkowników. | **P6S_UW** |
| **K_U04** | Potrafi projektować i zarządzać systemami informatycznymi i sieciami teleinformatycznymi z uwzględnieniem wymagań bezpieczeństwa. | **P6S_UW** |
| **K_U05** | Potrafi prawidłowo stosować taktyki i techniki zabezpieczenia i | **P6S_UW** |

| | | |
|---|---|---|
| | analizy dowodów cyfrowych. | |
| **K_U06** | Posiada umiejętność programowania w wybranym języku oraz stosowania podstawowych pakietów oprogramowania. | **P6S_UW** |
| **K_U07** | 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 informatyki w kształtowaniu życia społecznego oraz świadomości odpowiedzialności zawodowej funkcjonariusza zwalczającego przestępstwa popełniane w cyberprzestrzeni. | **P6S_KK** |
| **K_K02** | Ma świadomość konieczności ustawicznego podnoszenia wiedzy z zakresu wykorzystania nowych technologii w informatyce. | **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)

## II. 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. | Biały wywiad – pozyskiwanie danych z Internetu | 40 | 12 | 28 | **E** | **5** | **1,5** | **3,5** |
| 3. | Zabezpieczenie dowodów i sprzętu elektronicznego do badań | 40 | 18 | 22 | **E** | **5** | **2,2** | **2,8** |
| 4. | Infrastruktura Internetu i usługi sieciowe | 20 | 10 | 10 | **S** | **2** | **1** | **1** |
| | **ŁĄCZNIE w semestrze** | **125** | **53** | **72** | **-** | **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. | Bezpieczeństwo systemów i sieci | 20 | 14 | 6 | **S** | **2** | **1,4** | **0,6** |
| 8. | Algorytmy i mechanizmy kryptograficzne | 20 | 7 | 13 | **S** | **3** | **1** | **2** |
| 9. | Konsultacje | **6** | | | **-** | **-** | **-** | **-** |
| 10. | Egzamin końcowy | **8** | | | **-** | **-** | **-** | **-** |
| | **ŁĄCZNIE w semestrze** | **120+14** | **41** | **79** | **-** | **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:*<br>**Wiedzy:**<br>- Zna i rozumie zakres bezpieczeństwa systemów informatycznych.<br>- Zna i rozumie prawne możliwości ścigania sprawców przestępstw popełnianych w cyberprzestrzeni.<br>**Umiejętności:**<br>- Potrafi rozpoznać źródła zagrożeń w cyberprzestrzeni i przeciwdziałać im.<br>- Potrafi wskazać kierunki rozwoju cyberprzestępczości.<br>**Kompetencji społecznych:**<br>- Jest gotów do uznawania znaczenia wiedzy w rozwiązywaniu problemów poznawczych i praktycznych w zakresie zwalczania cyberprzestępczości. | | | **Czas realizacji**<br>**godz. 25** | | |
| **Lp.** | **Temat** | **Tezy** | Wykład | Ćwiczenia | **Razem** |
| 1 | **Bezpieczeństwo w cyberprzestrzeni** | 1. Przedmioty ochrony i zagrożenia systemów informatycznych.<br>2. Polityka bezpieczeństwa informatycznego. | 2 | 2 | **4** |
| 2 | **Cyberprzestępstwa** | 1. Phishing.<br>2. Kradzież tożsamości.<br>3. Oszustwo telekomunikacyjne.<br>4. Przestępczość z wykorzystaniem elektronicznych instrumentów płatniczych.<br>5. Złośliwe oprogramowanie (Malware, Crimeware as a Service (CaaS).<br>6. Cyberprzestępczość jako usługa. Usługi anonimizujące, fake mailery, fałszywe bramki sms. | 9 | 8 | **17** |
| 3 | **Charakterystyka cyberprzestępczości w Polsce** | 1. Nowy wymiar Cyberbezpieczeństwa.<br>2. Profilaktyka w zakresie cyberprzestępczości. | 2 | 2 | **4** |
| | | **Razem:** | **13** | **12** | **25** |

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

<table>
<tr><td colspan="4">Biały wywiad – pozyskiwanie danych z Internetu</td><td colspan="3">Przedmiot nr 2</td></tr>
<tr><td colspan="4">Efekty uczenia z zakresu:<br>Wiedzy:<br>- Zna wybrane pojęcia dotyczące białego wywiadu.<br>- Zna wybrane portale oraz techniki wykorzystywane przy gromadzeniu informacji w ramach białego wywiadu.<br>- Zna ogólnodostępne narzędzia wykorzystywane przy gromadzeniu informacji w ramach białego wywiadu.<br>Umiejętności:<br>- Potrafi pozyskiwać informacji z portali Internetowych.<br>- Potrafi używać ogólnodostępnych narzędzi do pozyskiwania informacji z otwartych źródeł w Internecie.<br>- Potrafi ocenić przydatność uzyskanych informacji.<br>- Potrafi wykorzystać biały wywiad do rozpoznania zagrożeń w cyberprzestrzeni.<br>Kompetencji społecznych:<br>- Jest gotów do krytycznej oceny posiadanej wiedzy i informacji w zakresie białego wywiadu oraz narzędzi wykorzystywanych do rozpoznawania zagrożeń w cyberprzestrzeni.</td><td colspan="3">Czas realizacji<br><br>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>Open Source Intelligence</td><td>1. Definicja i istota białego wywiadu.<br>2. Pojęcia związane z białym wywiadem: Open Source Data (OSD), Open Source Information (OSIF), Open Source Intelligence (OSINT), walidacja OSINT (OSINT-V).<br>3. Etapy prowadzenia białego wywiadu.</td><td>2</td><td>0</td><td>2</td></tr>
<tr><td>2</td><td>Biały wywiad w Policji</td><td>1. Regulacje prawne wykorzystywania OSINT przez polskie organy ścigania.<br>2. Potencjał informacyjny i dowodowy białego wywiadu.</td><td>4</td><td>2</td><td>6</td></tr>
<tr><td>3</td><td>Wybrane narzędzia przydatne w prowadzeniu białego wywiadu</td><td>1. Wyszukiwarka Google (google hacking, google grafika). Rejestr domen internetowych – WhoIs. WiGLE.net.<br>2. Bazy przedsiębiorców – Centralna Ewidencja i Informacja o Działalności Gospodarczej, Krajowy Rejestr Sądowy, Elektroniczne Księgi Wieczyste, inne.<br>3. Informacje o pojazdach – sprawdzanie numeru VIN.<br>4. Baza polis i szkód ubezpieczeniowych.<br>5. Mapy i zdjęcia, geolokalizacja.<br>6. Narzędzia do analizy metadanych, zdjęć.<br>7. Wyszukiwanie w social mediach, wyszukiwanie ludzi.</td><td>2</td><td>14</td><td>16</td></tr>
<tr><td>4</td><td>Rozpoznanie zagrożeń cyberprzestrzeni (Cyber Threat Intelligence CTI)</td><td>1. Idea CTI.<br>2. Modelowanie zagrożeń.<br>3. Narzędzia wspomagające CTI (Shodan, Maltego).</td><td>4</td><td>12</td><td>16</td></tr>
<tr><td colspan="3">Razem:</td><td>12</td><td>28</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">Zabezpieczenie dowodów i sprzętu elektronicznego do badań</td><td colspan="3">Przedmiot nr 3</td></tr>
<tr><td colspan="3">Efekty uczenia się z zakresu:<br>Wiedzy:<br>- Zna metodykę zabezpieczania sprzętu elektronicznego do badań.<br>- Zna zasadę działania narzędzi wykorzystywanych podczas zabezpieczania sprzętu elektronicznego.<br>- Zna zasady powoływania biegłego z zakresu informatyki śledczej.<br>Umiejętności:<br>- Potrafi zabezpieczyć nośniki cyfrowe i sprzęt elektroniczny do badań.<br>- Potrafi określić źródła dowodowe dotyczące śladów i dowodów cyfrowych.<br>- Potrafi dokonać wstępnej identyfikacji sprzętu elektronicznego do badań.<br>Kompetencji społecznych:<br>- Jest gotów uznawania znaczenia wiedzy w rozwiązywaniu problemów poznawczych i praktycznych w zakresie zabezpieczania śladów i dowodów cyfrowych.</td><td colspan="3">Czas realizacji<br><br>40 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>Podstawowe zasady zabezpieczania sprzętu elektronicznego do badań</td><td>1. Podstawowe pojęcia związane z zabezpieczaniem sprzętu komputerowego.<br>2. Algorytmy zabezpieczania sprzętu komputerowego do badań.</td><td>4</td><td>0</td><td>4</td></tr>
<tr><td>2</td><td>Identyfikacja sprzętu elektronicznego do badań</td><td>1. Budowa i podział sprzętu elektronicznego.<br>2. Klasyfikacja sprzętu elektronicznego pod kątem możliwości badawczych.<br>3. Odnajdywanie cech indywidualnych zabezpieczanych urządzeń.</td><td>4</td><td>2</td><td>6</td></tr>
<tr><td>3</td><td>Wykorzystanie narzędzi i oprogramowania podczas zabezpieczania sprzętu elektronicznego</td><td>1. Skanery sieci.<br>2. Zagłuszacz WiFi i GSM.<br>3. Klatka Faradaya.</td><td>2</td><td>2</td><td>4</td></tr>
<tr><td>4</td><td>Zabezpieczenie sprzętu elektronicznego do badań</td><td>1. Przygotowanie do zabezpieczenia sprzętu elektronicznego. live forensic.<br>2. Dobór odpowiedniej metody zabezpieczenia do rodzaju sprzętu.<br>3. Zabezpieczenie procesowe i techniczne.<br>4. Zabezpieczenie przed ingerencją w dane oraz uszkodzeniem mechanicznym.<br>5. Transport i przechowywanie.<br>6. Najczęstsze błędy podczas zabezpieczania sprzętu komputerowego.<br>7. Sposoby ochrony po stronie przestępców (time bomb, panic buton).</td><td>4</td><td>10</td><td>14</td></tr>
<tr><td>5</td><td>Współpraca z biegłym</td><td>1. Sporządzenie Postanowienia o dopuszczeniu dowodu z opinii biegłego.<br>2. Zaprezentowanie i omówienie przykładowych opinii.</td><td>1</td><td>1</td><td>2</td></tr>
<tr><td>6</td><td>Współpraca z dostawcami usług chmurowych</td><td>1. Zabezpieczenie danych u dostawców usług hostingowych.<br>2. Zabezpieczenie serwerów wirtualnych</td><td>2</td><td>4</td><td>6</td></tr>
</table>

| | | | | | |
|---|---|---|---|---|---|
| | | 3. Zabezpieczanie logów.<br>4. Zabezpieczenie danych transakcyjnych właściciela systemu (kupno usługi). | | | |
| | | **Razem:** | **18** | **22** | **40** |

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

<table>
<tr><td colspan="3">Infrastruktura Internetu i usługi sieciowe</td><td colspan="3">Przedmiot nr 4</td></tr>
<tr><td colspan="3" rowspan="2">Efekty uczenia się z zakresu:<br>Wiedzy:<br>− Zna architekturę i zasadę działania usług sieciowych.<br>− Zna wymagania jakościowe usług sieciowych.<br>− Zna zasadę działania wybranych urządzeń sieciowych.<br>Umiejętności:<br>− Potrafi w oparciu o dostępną dokumentację wdrożyć i uruchomić usługę sieciową.<br>− Potrafi utworzyć dokumentację techniczną powiązaną z wdrożeniem.<br>− Potrafi dokonać konfiguracji systemu teleinformatycznego.<br>− Potrafi administrować systemami teleinformatycznymi.<br>Kompetencji społecznych:<br>− Jest gotów do krytycznej oceny posiadanej wiedzy i informacji w zakresie infrastruktury Internetu i usług sieciowych oraz narzędzi wykorzystywanych do administrowania systemami teleinformatycznymi.</td><td colspan="3">Czas realizacji</td></tr>
<tr><td colspan="3">godz. 20</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>Technologie sieciowe wykorzystywane przy tworzeniu współczesnych sieci komputerowych</td><td>1. Protokoły IP, urządzenia sieciowe, łączenie sieci.<br>2. Technologie sieciowe wykorzystywane przy tworzeniu współczesnych sieci komputerowych.</td><td>2</td><td>2</td><td>4</td></tr>
<tr><td>2</td><td>Chmury obliczeniowe (Cloud computing)</td><td>1. Koncepcja chmury obliczeniowej.<br>2. Modele chmury obliczeniowej.<br>3. Regulacje prawne w obszarze chmury obliczeniowej.<br>4. Bezpieczeństwo usług chmurowych.</td><td>4</td><td>2</td><td>6</td></tr>
<tr><td>3</td><td>Nadużycia protokołów i usług sieciowych</td><td>1. Podstawowe pojęcia.<br>2. Bezpieczeństwo protokołów i usług sieciowych.</td><td>1</td><td>1</td><td>2</td></tr>
<tr><td>4</td><td>Nadużycia w usługach telekomunikacyjnych</td><td>1. Fałszywe numery telefonów.<br>2. Bramki VoIP.</td><td>1</td><td>1</td><td>2</td></tr>
<tr><td>5</td><td>Poczta elektroniczna, niechciane wiadomości SPAM.</td><td>1. Poczta elektroniczna, niechciane wiadomości SPAM.<br>2. Traceroute wiadomości.<br>3. Analiza nagłówków pocztowych (spoofing).</td><td>2</td><td>4</td><td>6</td></tr>
<tr><td colspan="3">Razem:</td><td>10</td><td>10</td><td>20</td></tr>
</table>

| | |
|---|---|
| **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:<br>Wiedzy:<br>- Zna funkcjonalność wybranego oprogramowania i jego zastosowania do odzyskiwania danych z nośników cyfrowych.<br>- Zna metody, techniki oraz narzędzia stosowane przy analizie elektronicznego materiału dowodowego.<br>Umiejętności:<br>- Potrafi odzyskać dane z wybranych nośników elektronicznych.<br>- Potrafi dobrać optymalną metodę odzyskiwania danych w zależności od rodzaju nośnika.<br>- Potrafi analizować dane, a także umiejętnie interpretować otrzymane wyniki.<br>Kompetencji społecznych:<br>- Jest gotów do krytycznej oceny posiadanej wiedzy z zakresu możliwości odzyskiwania danych z nośników cyfrowych.</td><td colspan="3">Czas realizacji<br><br>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.<br>2. Rodzaje systemów operacyjnych i akwizycja danych w tych systemach.<br>3. Rodzaje kopii binarnych oraz metody ich wykonywania w zależności od typu zabezpieczonego urządzenia.<br>4. Narzędzia stosowane od odzyskiwania danych cyfrowych, rekomendowane rozwiązania komercyjne i open source.<br>5. Wykorzystanie dystrybucji systemu Linuks dedykowanych informatyce śledczej (CAINE, DEFT, PALADIN).<br>6. Obliczanie sum kontrolnych i ich znaczenie w łańcuchu dowodowym.<br>7. Odzyskiwanie danych:<br>a. z urządzeń mobilnych,<br>b. usuniętych z dysku,<br>c. ze sformatowanego nośnika,<br>d. z innych nośników.<br>8. Praca z blokerami sprzętowymi i programowymi.</td><td>4</td><td>12</td><td>16</td></tr>
<tr><td>2</td><td>Analiza danych z urządzeń mobilnych</td><td>1. Analiza danych z urządzeń mobilnych przy wykorzystaniu oprogramowania XRY, UFED, MobilEdit, PasswareKit Mobile, Oxygene Forensic, AXIOM. Wady i zalety poszczególnych rozwiązań.<br>2. Deasemblacja i techniki agresywne.</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 programów TrueCrypt, VeraCrypt.<br>2. Mechanizmy kryptograficzne wbudowane w systemy operacyjne Windows (BitLocker), Linux (LUKS) i MacOS (FileVault).<br>3. Praca z nośnikami zaszyfrowanymi – wykrywanie plików zaszyfrowanych, i kontenerów danych, rozpoznawanie typu</td><td>2</td><td>4</td><td>6</td></tr>
</table>

| | | | | | |
|---|---|---|---|---|---|
| | | szyfrowania, możliwości i narzędzia do deszyfracji.<br>4. Taktyka przeprowadzania ataków na pliki szyfrowane. Dobre praktyki. | | | |
| 4 | **Analiza pamięci RAM, plików hiberfil.sys i pagefile.sys** | 1. Analiza pamięci z wykorzystaniem oprogramowania Volatility, X-Ways Forensic, Magnet AXIOM, RoastLamb, Bulk Extractor.<br>2. Analiza plików hiberfil.sys i pagefile.sys.<br>3. Analiza rejestru Windows, Linux oraz MacOS.<br>4. Zabezpieczenie danych ulotnych Windows, Linux i MacOS – możliwości i ograniczenia.<br>5. Taktyczno-techniczne aspekty zabezpieczenia zawartości pamięci.<br>6. Zagrożenia związane z zabezpieczeniem pamięci ulotnej.<br>7. Analiza zrzutów pamięci RAM, plików stronicowania i plików hibernacji z różnych systemów operacyjnych. Narzędzia płatne oraz darmowe.<br>8. Analiza ręczna zrzutów. | 2 | 6 | **8** |
| 5 | **Podstawy badania urządzeń o dużym ryzyku występowania złośliwego oprogramowania** | 1. Podstawy analizy malware – dobre praktyki i możliwości Europol Malware Analysis Solution (EMAS).<br>2. Dobre praktyki. | 0 | 2 | **2** |
| 6 | **Dokumentowanie czynności z analizy cyfrowych nośników danych** | 1. Wykonywania dokumentacji (protokoły oględzin, protokoły przeszukania urządzenia zawierającego dane informatyczne/ systemu informatycznego/ nośnika). | 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:<br>Wiedzy:<br>- Zna i rozumie zasady tworzenia i analizy oprogramowania w środowisku Python.<br>- Zna typowe problemy i algorytmy programowania w języku Python.<br>Umiejętności:<br>- Potrafi poprawnie zainstalować i skonfigurować Pythona<br>- Potrafi tworzyć proste programy wykorzystujące podstawowe typy danych, operatory oraz podstawowe struktury sterujące.<br>- Potrafi tworzyć programy wykorzystujące proste funkcje zwracające wartość.<br>- Potrafi dokonywać operacji na plikach: otwieranie, czytanie, pisanie i zamykanie plików.<br>- Potrafi rozwiązywać wybrane problemy powstające w trakcie tworzenia oprogramowania w środowisku Pythona.<br>Kompetencji społecznych:<br>- 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.<br>2. Regex.<br>3. Analiza SQLite.<br>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.<br>2. Wizualizacja danych, ekstrakcja danych z dokumentu HTML.<br>3. Ekstrakcja danych ze źródeł internetowych.<br>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">Bezpieczeństwo systemów i sieci</td><td colspan="3">Przedmiot nr 7</td></tr>
<tr><td colspan="3" rowspan="2">Efekty uczenia się z zakresu:<br>Wiedzy:<br>- Zna wybrane zagadnienia bezpieczeństwa systemów i sieci.<br>- Zna narzędzia i techniki wykorzystywane do rozpoznawania zagrożeń.<br>Umiejętności:<br>- Potrafi zaprojektować i wdrożyć procedury zapewniające bezpieczeństwo sieci i systemów.<br>- Potrafi konfigurować systemy bezpieczeństwa sieci.<br>- Potrafi wykorzystać narzędzia i techniki do rozpoznawania zagrożeń.<br>Kompetencji społecznych:<br>- Jest gotów do oceniania 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>Bezpieczeństwo systemów</td><td>1. Podstawowe definicje dotyczące bezpieczeństwa.<br>2. Atrybuty i zagrożenia bezpieczeństwa.<br>3. Klasyfikacja przyczyn złego funkcjonowania systemów informatycznych.<br>4. Audyt bezpieczeństwa systemów.</td><td>5</td><td>2</td><td>7</td></tr>
<tr><td>2</td><td>Bezpieczeństwo sieci</td><td>1. Typowe ataki na bezpieczeństwo sieci.<br>2. Konfiguracja serwerów danych i aplikacji.<br>3. Audyt bezpieczeństwa sieci.</td><td>3</td><td>2</td><td>5</td></tr>
<tr><td>3</td><td>Rozwiązania w zakresie zwiększenia bezpieczeństwa sieci i systemów</td><td>1. Systemy ochrony styku z siecią Internet.<br>2. Zero trust security.<br>3. Wielowarstwowa architektura bezpieczeństwa.<br>4. Systemy bezpieczeństwa wewnętrznego.<br>5. Zarządzanie podatnościami (vulnerability management).</td><td>6</td><td>2</td><td>8</td></tr>
<tr><td colspan="3">Razem:</td><td>14</td><td>6</td><td>20</td></tr>
</table>

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

<table>
<tr><td colspan="3">Algorytmy i mechanizmy kryptograficzne</td><td colspan="3">Przedmiot nr 8</td></tr>
<tr><td colspan="3" rowspan="2">Efekty uczenia się z zakresu:<br>Wiedzy:<br>- Zna problematykę i zastosowania protokołów kryptograficznych.<br>- Zna i rozumie mechanizmy szyfrowania danych.<br>Umiejętności:<br>- Potrafi stosować wybrane oprogramowanie kryptograficzne.<br>- Potrafi ocenić przydatność narzędzi szyfrowania i uwierzytelniania.<br>Kompetencji społecznych:<br>- Jest gotów do krytycznej oceny posiadanej wiedzy i informacji w zakresie kryptografii oraz zasięgania opinii ekspertów w przypadku trudności z samodzielnym rozwiązaniem problemu.</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>Kryptologia</td><td>1. Podstawowe pojęcia.<br>2. Atrybuty bezpieczeństwa i siła zabezpieczeń.<br>3. Kryptografia symetryczna i asymetryczna.<br>4. Szyfrowanie blokowe i strumieniowe.</td><td>3</td><td>4</td><td>7</td></tr>
<tr><td>2</td><td>Funkcje skrótu</td><td>1. Klasyfikacja.<br>2. Kryteria.<br>3. Zastosowanie.</td><td>0</td><td>3</td><td>3</td></tr>
<tr><td>3</td><td>Infrastruktura klucza publicznego PKI</td><td>1. Certyfikat klucza publicznego.<br>2. Centra Certyfikacji.<br>3. Hierarchia certyfikatów.<br>4. Unieważnianie certyfikatów.</td><td>2</td><td>0</td><td>2</td></tr>
<tr><td>4</td><td>Szyfrowanie transmisji danych i poczty elektronicznej</td><td>1. Wykorzystanie szyfrowania w transmisji danych.<br>2. Wykorzystanie szyfrowania w poczcie elektronicznej.</td><td>0</td><td>4</td><td>4</td></tr>
<tr><td>5</td><td>Kryptoanaliza</td><td>1. Metody kryptoanalizy.<br>2. Podstawowe pojęcia dotyczące kryptowalut (blockchain, klaster, white paper, hot wallet, cold wallet, mixery, tumblery itp.).<br>3. Podstawy przeprowadzania analiz przepływu kryptowalut z wykorzystaniem narzędzi opensource.</td><td>2</td><td>2</td><td>4</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. | Biały wywiad – pozyskiwanie danych z Internetu. | Zabezpieczenia sprzętu elektronicznego do badań. | Infrastruktura Internetu i usługi sieciowe | Odzyskiwanie i analiza danych z nośników cyfrowych. | Programowanie w języku Python | Bezpieczeństwo systemów i sieci. | Algorytmy i mechanizmy kryptograficzne. |
| **K_W01** | Ma wiedzę dotyczącą prawnych i społecznych aspektów informatyki w tym własności intelektualnej prywatności i swobód obywatelskich ryzyka i odpowiedzialności związanej z systemami informatycznymi. | + | | | | + | | | |
| **K_W02** | Ma wiedzę dotyczącą najważniejszych funkcji i budowy systemów i sieci teleinformatycznych oraz trendów ich rozwoju. | | + | + | + | | | + | |
| **K_W03** | Identyfikuje metody, narzędzia i techniki wykorzystywane w informatyce śledczej. | | + | + | | + | | | |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **K_W04** | Ma wiedzę dotycząca metod i technik programistycznych. Rozumie wybrane paradygmaty programowania. | | | | | | + | | |
| **K_W05** | Zna techniki kryptograficzne wykorzystywane obecnie w systemach informatycznych. Zna praktyczne aspekty wykorzystania kryptografii w informatyce. | | | + | + | | | + | + |
| **K_U01** | Potrafi wskazać źródła zagrożeń oraz kierunki rozwoju przestępstw popełnianych w cyberprzestrzeni. | + | | | | | | | |
| **K_U02** | Wykorzystuje wiedzę w procesie pozyskiwania i analizowania informacji służących rozpoznawaniu zagrożeń w sferze cyberbezpieczeństwa. | | + | | | | | | |
| **K_U03** | Potrafi poznawać, analizować i modelować wymagania stawiane systemom informatycznym przez użytkowników a także projektować i implementować systemy informatyczne spełniające wymagania użytkowników. | | | | + | | | | |
| **K_U04** | Potrafi projektować i zarządzać systemami informatycznymi i sieciami teleinformatycznymi z uwzględnieniem wymagań bezpieczeństwa. | | | | + | | | + | |
| **K_U05** | Potrafi prawidłowo stosować taktyki i techniki zabezpieczenia i analizy dowodów cyfrowych. | | | + | | + | | | |
| **K_U06** | Posiada umiejętność programowania w wybranym języku oraz stosowania podstawowych pakietów oprogramowania. | | | | | | + | | |
| **K_U07** | 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 informatyki w kształtowaniu życia społecznego oraz świadomości odpowiedzialności zawodowej funkcjonariusza zwalczającego przestępstwa popełniane w cyberprzestrzeni. | | + | | + | + | | | + |
| **K_K02** | Ma świadomość konieczności ustawicznego podnoszenia wiedzy z zakresu wykorzystania nowych technologii w informatyce. | + | | + | | | + | | + |
| **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/ zaliczenie z oceną | Kolokwium/ odpowiedź ustna | Realizacja zadania praktycznego | Analiza przypadku |
| **K_W01** | Ma wiedzę dotyczącą prawnych i społecznych aspektów informatyki w tym własności intelektualnej prywatności i swobód obywatelskich ryzyka i odpowiedzialności związanej z systemami informatycznymi. | + | + | | |
| **K_W02** | Ma wiedzę dotyczącą najważniejszych funkcji i budowy systemów i sieci teleinformatycznych oraz trendów ich rozwoju. | + | + | | |
| **K_W03** | Identyfikuje metody, narzędzia i techniki wykorzystywane w informatyce śledczej. | + | + | | |
| **K_W04** | Ma wiedzę dotycząca metod i technik programistycznych. Rozumie wybrane paradygmaty programowania. | + | + | | |
| **K_W05** | Zna techniki kryptograficzne wykorzystywane obecnie w systemach informatycznych. Zna praktyczne aspekty wykorzystania kryptografii w informatyce. | + | + | | |
| **K_U01** | Potrafi wskazać źródła zagrożeń oraz kierunki rozwoju przestępstw popełnianych w cyberprzestrzeni. | + | + | | |
| **K_U02** | Wykorzystuje wiedzę w procesie pozyskiwania i analizowania informacji służących rozpoznawaniu zagrożeń w sferze cyberbezpieczeństwa. | + | + | + | + |
| **K_U03** | Potrafi poznawać, analizować i modelować wymagania stawiane systemom informatycznym przez użytkowników a także projektować i implementować systemy informatyczne spełniające wymagania użytkowników. | + | + | | |
| **K_U04** | Potrafi projektować i zarządzać systemami informatycznymi i sieciami teleinformatycznymi z uwzględnieniem wymagań bezpieczeństwa. | + | + | + | + |
| **K_U05** | Potrafi prawidłowo stosować taktyki i techniki zabezpieczenia i analizy dowodów cyfrowych. | + | + | + | + |
| **K_U06** | Posiada umiejętność programowania w wybranym języku oraz stosowania podstawowych pakietów oprogramowania. | | + | + | + |
| **K_U07** | 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 informatyki w kształtowaniu życia społecznego oraz świadomości odpowiedzialności zawodowej funkcjonariusza zwalczającego przestępstwa popełniane w cyberprzestrzeni. | | + | | |
| **K_K02** | Ma świadomość konieczności ustawicznego podnoszenia wiedzy z zakresu wykorzystania nowych technologii w informatyce. | | + | | |
| **K_K03** | Jest gotów do oceniania swoich działań i przyjmowania odpowiedzialności za bezpośrednie ich skutki. | | + | | |