UCHWAŁA NR 189 /IV/2021
SENATU WYŻSZEJ SZKOŁY POLICJI W SZCZYTNIE

z dnia 24 września 2021 r.

w sprawie ustalenia programu studiów na studiach podyplomowych w zakresie cyberbezpieczeństwa 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 2021 r., poz. 478 ze zm.) 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 cyberbezpieczeństwa dla słuchaczy rozpoczynających studia od roku akademickiego 2021/2022 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

insp. dr hab. Iwona Klonowska

Załącznik do Uchwały Senatu nr 189/IV/2021
Wyższej Szkoły Policji w Szczytnie
z dnia 24.09 2021 r.

Wyższa Szkoła Policji
w Szczytnie

Wydział Bezpieczeństwa i Nauk Prawnych

PROGRAM STUDIÓW PODYPLOMOWYCH

w zakresie cyberbezpieczeństwa

SZCZYTNO 2021

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 *cyberbezpieczeństwa*

3. **Kierunek studiów, do którego przyporządkowane są studia podyplomowe:** Bezpieczeństwo wewnętrzne

4. **Założenia ogólne (ogólna koncepcja kształcenia):**
   Głównym celem kształcenia w ramach studiów podyplomowych w zakresie *cyberbezpieczeństwa* jest przygotowanie słuchacza do skutecznego rozpoznawania, zapobiegania i zwalczania cyberprzestępczości w zakresie:
   - ujawnienia i zabezpieczenia śladów i dowodów działalności cyberprzestępczej wraz z ich wstępną weryfikacją,
   - poszerzenie wiedzy o aktualnych zagrożeniach cyberprzestępczością,
   - zapoznanie z nowoczesnymi technologiami w obszarach badania dowodów cyfrowych,
   - kształcenie umiejętności wykorzystania źródeł i rezultatów białego wywiadu,
   - ukierunkowanego prowadzenia rozpoznania internetowego oraz dokumentowania ww. czynności.

5. **Związek efektów kształcenia z misją i strategią uczelni:**
   Studia podyplomowe w zakresie *cyberbezpieczeństwa* są efektem zaangażowania uczelni w szkolenie i doskonalenie innych służb i podmiotów związanych w ramach swoich kompetencji w przeciwdziałanie i zwalczanie cyberprzestępczości. Adresatem studiów podyplomowych są w szczególności funkcjonariusze i pracownicy Policji i Straży Granicznej, sędziowie, prokuratorzy, pracownicy organów kontroli skarbowej i celnej, Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu oraz Służb Wywiadu i Kontrwywiadu Wojskowego i innych jednostek Ministerstwa Obrony Narodowej oraz pracownicy Ministerstwa Spraw Wewnętrznych i Administracji.

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

7. Zasady rekrutacji:

Zasady rekrutacji kandydatów określa Komendant-Rektor.

8. Warunki ukończenia studiów podyplomowych:

Warunkiem ukończenia studiów podyplomowych jest osiągnięcie 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 ogólnej, 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 *cyberbezpieczeństwa*.

II. 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 CYBERBEZPIECZEŃSTWA **Typ studiów** (kwalifikacyjne/doskonalące): DOSKONALĄCE		
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 metody, techniki, narzędzia stosowane przy korzystaniu z sieci Internet	**P6S_WK**
K_W02	Zna portale, metody, techniki i narzędzia wykorzystywane przy gromadzeniu informacji w ramach białego wywiadu, zna metodykę przeprowadzania białego wywiadu	**P6S_WK**
K_W03	Zna wybrane narzędzia usprawniające/ wizualizujące dedykowane wyszukiwaniu informacji w ramach białego wywiadu	**P6S_WK**
K_W04	Potrafi określić źródła dowodowe dotyczące śladów i dowodów cyfrowych	**P6S_WK**
K_W05	Opisuje metodykę zabezpieczania sprzętu elektronicznego do badań	**P6S_WK**
K_W06	Ma wiedzę ogólną obejmującą kluczowe zagadnienia bezpieczeństwa systemów i sieci	**P6S_WK**
K_W07	Zna narzędzia i techniki wykorzystywane do rozpoznawania zagrożeń	**P6S_WK**
K_W08	Ma wiedzę ogólną obejmującą kluczowe zagadnienia bezpieczeństwa systemów, urządzeń i procesów	**P6S_WK**
K_W09	Ma wiedzę z zakresu mechanizmów szyfrowania danych	**P6S_WK**
K_W10	Posiada wiedzę z zakresu bezpieczeństwa systemów informatycznych	**P6S_WK**
K_W11	Zna i rozumie prawne możliwości ścigania cyberprzestępstw	**P6S_WK**
K_W12	Zna możliwości i zastosowanie oprogramowania do odzyskiwania danych z nośników cyfrowych	**P6S_WK**
K_W13	Zna metody, techniki oraz narzędzia stosowane przy analizie elektronicznego materiału dowodowego	**P6S_WK**
K_W14	Potrafi opisać architekturę usług sieciowych.	**P6S_WK**
K_W15	Określa specyfikację usług sieciowych	**P6S_WK**
K_W16	Posiada wiedzę nt. urządzeń sieciowych omówionych w materiale	**P6S_WK**
K_W17	Posiada wiedzę z zakresu zarządzania ryzykiem systemów informacyjnych	**P6S_WK**
K_W18	Posiada wiedzę z zakresu zarządzania zapewnieniem ciągłości działania	**P6S_WK**
Umiejętności		
K_U01	Potrafi pozyskiwać dane, a także umiejętnie interpretować otrzymanie wyniki	**P6S_UW**

K_U02	Potrafi użyć ogólnodostępnych narzędzi, m.in. wyszukiwarek internetowych i portali społecznościowych, jako źródła danych operacyjnych	**P6S_UW**
K_U03	Potrafi zabezpieczyć sprzęt elektroniczny do badań	**P6S_UW**
K_U04	Dokonuje wstępnej identyfikacji sprzętu elektronicznego do badań	**P6S_UW**
K_U05	Potrafi zaprojektować i wdrożyć procedury zapewniające bezpieczeństwo sieci i systemów	**P6S_UW**
K_U06	Potrafi wykorzystać narzędzia i techniki do rozpoznawania zagrożeń	**P6S_UW**
K_U07	Potrafi posłużyć się właściwie dobranymi metodami i oprogramowaniem kryptograficznym	**P6S_UW**
K_U08	Potrafi ocenić przydatność narzędzi szyfrowania i uwierzytelniania	**P6S_UW**
K_U09	Potrafi rozpoznać i przeciwdziałać zagrożeniom w cyberprzestrzeni	**P6S_UW**
K_U10	Wskazuje kierunki rozwoju cyberprzestępczości.	**P6S_UW**
K_U11	Potrafi odzyskać dane z nośników elektronicznych	**P6S_UW**
K_U12	Potrafi dobrać optymalną metodę odzysku danych w zależności od rodzaju nośnika	**P6S_UW**
K_U13	Potrafi analizować dane, a także umiejętnie interpretować otrzymane wyniki	**P6S_UW**
K_U14	Potrafi w oparciu o dostępną dokumentację wdrożyć i uruchomić usługę sieciową	**P6S_UW**
K_U15	Potrafi utworzyć dokumentację techniczną powiązaną z wdrożeniem	**P6S_UW**
K_U16	Potrafi dokonać konfiguracji systemu komputerowego	**P6S_UW**
K_U17	Potrafi administrować systemami komputerowymi	**P6S_UW**
K_U18	Potrafi identyfikować strukturę i czynniki ryzyka	**P6S_UW**
K_U19	Potrafi wdrożyć i stosować model zarządzania ryzykiem SI	**P6S_UW**
K_U20	Potrafi identyfikować procesy kluczowe i krytyczne	**P6S_UW**
K_U21	Potrafi wdrożyć i stosować model zarządzania zapewnieniem ciągłości działania	**P6S_UW**
Kompetencje społeczne		
K_K01	Zna ograniczenia własnej wiedzy oraz konieczność dalszego poszukiwania i nauki	**P6S_KK**
K_K02	Wskazuje przedsiębiorczość i kreatywność w myśleniu i działaniu	**P6S_KO**
K_K03	Potrafi współdziałać i pracować w grupie, przyjmując w niej różne role	**P6S_KR**
K_K04	Potrafi odpowiednio określić priorytety służące realizacji określonego przez siebie lub innych zadania	**P6S_KR**
K_K05	Rozumie potrzebę uczenia się przez całe życie	**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)

III. 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:** 219 godzin
6. **Plan studiów podyplomowych:**

PLAN STUDIÓW PODYPLOMOWYCH

WYDZIAŁ: BEZPIECZEŃSTWA I NAUK PRAWNYCH
NAZWA STUDIÓW PODYPLOMOWYCH: studia podyplomowe w zakresie Cyberbezpieczeństwa

I ROK 1 SEMESTR								
numer przedmiotu	**Przedmiot**	**liczba jednostek lekcyjnych (godz.)**			**forma zakończenia**	**liczba punktów ECTS**		
		łącznie	**wykład**	**ćwiczenia**		**łącznie**	**BK***	**PS***
1	Cyberprzestępczość	25	13	12	S	4	2,08	1,92
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	2,25	2,75
4	Infrastruktura Internetu i usługi sieciowe	20	10	10	S	4	2	2
	ŁĄCZNIE w semestrze	125	53	72	—	18	7,83	10,17

I ROK 2 SEMESTR								
numer przedmiotu	**Przedmiot**	**liczba jednostek lekcyjnych (godz.)**			**forma zakończenia**	**liczba punktów ECTS**		
		łącznie	**wykład**	**ćwiczenia**		**łącznie**	**BK***	**PS***
5a	Odzyskiwanie i analiza danych z nośników cyfrowych	40	10	30	E	5	$1,25^a$	$3,75^a$
5b	Cyberryzyko i cyberbezpieczeństwo wewnętrzne organizacji		26	14			$3,25^b$	$1,75^b$
6	Bezpieczeństwo systemów i sieci	20	14	6	Z	4	2,8	1,2
7	Algorytmy i mechanizmy kryptograficzne	20	7	13	S	3	1,05	1,95
8	Konsultacje	6			Z	—		
9	Egzamin końcowy	8			—	—		
	ŁĄCZNIE w semestrze	80+14	31	49	—	12	$5,1^a$	$6,9^a$
			47	33			$7,1^b$	$4,9^b$

ECTS	semestr 1	semestr 2	Razem:
Łączna liczba punktów ECTS	18	12	30
BK**	7,83	$5,1^a$	$12,93^b$
		$6,9^a$	$14,73^b$
PS**	10,17	7,1	17,27
		4,9	15,07

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
- **5a, 5b** – przedmiot do wyboru

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:** - Posiada wiedze z zakresu bezpieczeństwa systemów informatycznych. - Zna i rozumie prawne możliwości ścigania cyberprzestępstw. **Umiejętności:** - Potrafi rozpoznać i przeciwdziałać zagrożeniom w cyberprzestrzeni. - Wskazuje kierunki rozwoju cyberprzestępczości. **Kompetencji społecznych:** - Potrafi odpowiednio określić priorytety służące realizacji określonego przez siebie lub innych zadania. - Potrafi współdziałać i pracować w grupie, przyjmując w niej różne role.			**Czas realizacji** **godz. 25**		
Lp.	**Temat**	**Tezy**	Wykład	Ćwiczenia	**Razem**
1	**Bezpieczeństwo w cyberprzestrzeni.**	1. Przedmioty ochrony i zagrożenia systemów informatycznych. 2. Polityka bezpieczeństwa informatycznego.	2	2	**4**
2	**Cyberprzestępstwa.**	1. Phishing 2. Kradzież tożsamości 3. Oszustwo telekomunikacyjne 4. Przestępczość z wykorzystaniem elektronicznych instrumentów płatniczych. 5. Złośliwe oprogramowanie (Malware, Crimeware as a Service (CaaS)) 6. Cyberprzestępczość jako usługa. Usługi anonimizujące, fake mailery, fałszywe bramki sms.	9	8	**17**
3	**Charakterystyka cyberprzestępczości w Polsce.**	1. Nowy wymiar Cyberbezpieczeństwa, 2. Profilaktyka w zakresie cyberprzestępczości.	2	2	**4**
		Razem:	**13**	**12**	**25**

Sposób zakończenia: Zaliczenie z oceną	Punkty ECTS: 4

Biały wywiad – pozyskiwanie danych z Internetu			Przedmiot nr 2		
Efekty uczenia z zakresu: **Wiedzy:** - Zna metody, techniki, narzędzia stosowane przy korzystaniu z sieci Internet. - Zna portale, metody, techniki i narzędzia wykorzystywane przy gromadzeniu informacji w ramach białego wywiadu, zna metodykę przeprowadzania białego wywiadu. - Zna wybrane narzędzia usprawniające/wizualizujące dedykowane wyszukiwaniu informacji w ramach białego wywiadu. **Umiejętności:** - Potrafi pozyskiwać dane, a także umiejętnie interpretować otrzymanie wyniki. - Potrafi użyć ogólnodostępnych narzędzi, m.in. wyszukiwarek internetowych i portali społecznościowych, jako źródła danych operacyjnych. **Kompetencji społecznych:** - Zna ograniczenia własnej wiedzy oraz konieczność dalszego poszukiwania i nauki. - Wskazuje przedsiębiorczość i kreatywność w myśleniu i działaniu. - Potrafi współdziałać i pracować w grupie, przyjmując w niej różne role.			**Czas realizacji** **godz. 40**		
Lp.	**Temat**	**Tezy**	Wykład	Ćwiczenia	**Razem**
1	**Open Source Intelligence.**	1. Definicja i istota białego wywiadu. 2. Pojęcia związane z białym wywiadem: Open Source Data (OSD), Open Source Information (OSIF), Open Source Intelligence (OSINT), walidacja OSINT (OSINT-V). 3. Etapy prowadzenia białego wywiadu.	2	0	**2**
2	**Biały wywiad w Policji.**	1. Regulacje prawne wykorzystywania OSINT przez polskie organy ścigania. 2. Potencjał informacyjny i dowodowy białego wywiadu.	4	2	**6**
3	**Wybrane narzędzia przydatne w prowadzeniu białego wywiadu.**	1. Wyszukiwarka Google (google hacking, google grafika). Rejestr domen internetowych – WhoIs. WiGLE.net. 2. Bazy przedsiębiorców – Centralna Ewidencja i Informacja o Działalności Gospodarczej, Krajowy Rejestr Sądowy, Elektroniczne Księgi Wieczyste, inne. 3. Informacje o pojazdach – sprawdzanie numeru VIN. 4. Baza polis i szkód ubezpieczeniowych. 5. Mapy i zdjęcia, geolokalizacja. 6. Narzędzia do analizy metadanych, zdjęć. 7. Wyszukiwanie w social mediach, wyszukiwanie ludzi.	2	14	**16**
4	**Rozpoznanie zagrożeń cyberprzestrzeni (Cyber Threat Intelligence CTI).**	1. Idea CTI. 2. Modelowanie zagrożeń. 3. Narzędzia wspomagające CTI (Shodan, Maltego).	4	12	**16**
		Razem:	**12**	**28**	**40**

Sposób zakończenia: Egzamin - 1 godzina	Punkty ECTS: 5

Zabezpieczenia sprzętu elektronicznego do badań			Przedmiot nr 3		
Efekty uczenia się z zakresu: **Wiedzy:** - Potrafi określić źródła dowodowe dotyczące śladów i dowodów cyfrowych. - Opisuje metodykę zabezpieczania sprzętu elektronicznego do badań. **Umiejętności:** - Potrafi zabezpieczyć sprzęt elektroniczny do badań. - Dokonuje wstępnej identyfikacji sprzętu elektronicznego do badań. **Kompetencji społecznych:** - Potrafi współdziałać i pracować w grupie, przyjmując w niej różne role. - Potrafi odpowiednio określić priorytety służące realizacji określonego przez siebie lub innych zadania.			Czas realizacji **40 godz.**		
Lp.	**Temat**	**Tezy**	Wykład	Ćwiczenia	**Razem**
1	**Podstawowe zasady zabezpieczania sprzętu elektronicznego do badań.**	1. Podstawowe 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	**Wykorzystanie narzędzi i oprogramowania podczas zabezpieczania sprzętu elektronicznego.**	1. Skanery sieci. 2. Zagłuszacz WiFi i GSM. 3. Klatka Faradaya.	2	2	**4**
4	**Zabezpieczenie sprzętu elektronicznego do badań.**	1. Przygotowanie do zabezpieczenia sprzętu elektronicznego. 2. Dobór odpowiedniej metody zabezpieczenia do rodzaju sprzętu. 3. Zabezpieczenie procesowe i techniczne. 4. Zabezpieczenie przed ingerencją w dane oraz uszkodzeniem mechanicznym. 5. Transport i przechowywanie. 6. Najczęstsze błędy podczas zabezpieczania sprzętu komputerowego. 7. Sposoby ochrony po stronie przestępców (time bomb, panic buton).	4	10	**14**
5	**Współpraca z biegłym.**	1. Sporządzenie Postanowienia o dopuszczeniu dowodu z opinii biegłego. 2. Zaprezentowanie i omówienie przykładowych opinii.	2	4	**6**
6	**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	4	**6**
		Razem:	**18**	**22**	**40**

Sposób zakończenia: Egzamin – 1 godzina	Punkty ECTS: 5

Infrastruktura Internetu i usługi sieciowe			Przedmiot nr 4		
Efekty uczenia się z zakresu: **Wiedzy:** - Potrafi opisać architekturę usług sieciowych. - Określa wymagania jakościowe usług sieciowych. - Posiada wiedzę nt. urządzeń sieciowych omówionych w materiale. **Umiejętności:** - Potrafi w oparciu o dostępną dokumentację wdrożyć i uruchomić usługę sieciową. - Potrafi utworzyć dokumentację techniczną powiązaną z wdrożeniem. - Potrafi dokonać konfiguracji systemu komputerowego. - Potrafi administrować systemami komputerowymi **Kompetencji społecznych:** - Umiejętność pracy w grupie w celu zrealizowania postawionego zadania.			Czas realizacji godz. 20		
Lp.	**Temat**	**Tezy**	Wykład	Ćwiczenia	**Razem**
1	**Technologie sieciowe wykorzystywane przy tworzeniu współczesnych sieci komputerowych.**	1. Protokoły IP, urządzenia sieciowe, łączenie sieci 2. Technologie sieciowe wykorzystywane przy tworzeniu współczesnych sieci komputerowych	2	2	**4**
2	**Chmury obliczeniowe (Cloud computing).**	1. Koncepcja chmury obliczeniowej 2. Modele chmury obliczeniowej 3. Regulacje prawne w obszarze chmury obliczeniowej 4. Bezpieczeństwo usług chmurowych	4	2	**6**
3	**Nadużycia protokołów i usług sieciowych.**	1. Podstawowe pojęcia. 2. Bezpieczeństwo protokołów i usług sieciowych.	1	1	**2**
4	**Nadużycia w usługach telekomunikacyjnych.**	1. Fałszywe numery telefonów. 2. Bramki VoIP.	1	1	**2**
5	**Poczta elektroniczna, niechciane wiadomości SPAM.**	1. Poczta elektroniczna, niechciane wiadomości SPAM.	2	4	**6**
		Razem:	**10**	**10**	**20**

Sposób zakończenia: Zaliczenie z oceną	Punkty ECTS: 4

Odzyskiwanie i analiza danych z nośników cyfrowych			Przedmiot nr 5a		
Efekty uczenia się z zakresu: **Wiedzy:** - Zna możliwości i zastosowanie oprogramowania do odzyskiwania danych z nośników cyfrowych. - Zna metody, techniki oraz narzędzia stosowane przy analizie elektronicznego materiału dowodowego. **Umiejętności:** - Potrafi odzyskać dane z nośników elektronicznych. - Potrafi dobrać optymalną metodę odzysku danych w zależności od rodzaju nośnika. - Potrafi analizować dane, a także umiejętnie interpretować otrzymane wyniki. **Kompetencji społecznych:** - Potrafi współdziałać i pracować w grupie, przyjmując w niej różne role. - Potrafi odpowiednio określić priorytety służące realizacji określonego przez siebie lub innych zadania.			**Czas realizacji** **godz. 40**		
Lp.	**Temat**	**Tezy**	Wykład	Ćwiczenia	**Razem**
1	**Odzyskiwanie danych z elektronicznych nośników pamięci.**	1. Narzędzia stosowane od odzyskiwania danych cyfrowych. 2. Odzyskiwanie danych: a. z urządzeń mobilnych, b. usuniętych z dysku, c. ze sformatowanego nośnika, d. z innych nośników. 3. Praca z blokerami sprzętowymi i programowymi.	4	14	**18**
2	**Analiza danych z urządzeń mobilnych.**	1. Analiza danych z urządzeń mobilnych przy wykorzystaniu oprogramowania XRY, UFED oraz MobilEdit.	2	6	**8**
3	**Analiza zaszyfrowanych kontenerów danych.**	1. Analiza zaszyfrowanych kontenerów danych programów TrueCrypt, VeraCrypt, BitLocker.	2	4	**6**
4	**Analiza pamięci RAM, plików hiberfil.sys i pagefile.sys.**	1. Analiza pamięci z wykorzystaniem oprogramowania Volatility 2. Analiza plików hiberfil.sys i pagefile.sys.	2	6	8
		Razem:	**10**	**30**	**40**

Sposób zakończenia: Egzamin - 1 godzina	Punkty ECTS: 5

Cyberryzyko i cyberbezpieczeństwo wewnętrzne organizacji			Przedmiot nr 5b		
Efekty uczenia się w zakresie: **Wiedzy:** – posiada wiedzę z zakresu zarządzania ryzykiem systemów informacyjnych. – posiada wiedzę z zakresu zarządzania zapewnieniem ciągłości działania. **Umiejętności:** – potrafi identyfikować strukturę i czynniki ryzyka. – potrafi wdrożyć i stosować model zarządzania ryzykiem SI. – potrafi identyfikować procesy kluczowe i krytyczne. – potrafi wdrożyć i stosować model zarządzania zapewnieniem ciągłości działania. **Kompetencji społecznych:** – potrafi odpowiednio określić priorytety służące realizacji określonego przez siebie lub innych zadania. – potrafi współdziałać i pracować w grupie, przyjmując w niej różne role.			**Czas realizacji** **godz. 40**		
Lp.	Temat	Tezy	Wykład	Ćwiczenia	Razem
1	**Ryzyko systemów informacyjnych.**	1. System informacyjny 2. Charakterystyka ryzyka informatycznego i ryzyka SI 3. Struktura i czynniki ryzyka SI	6	2	8
2	**Procesy zarządzania ryzykiem SI.**	1. Podejście procesowe do zarządzania ryzykiem SI 2. Zarządzania zasobami 3. Szacowanie ryzyka SI 4. Postępowanie z ryzykiem SI 5. Monitoring i przegląd ryzyka SI	4	4	**8**
3	**Operacyjna odporność cyfrowa organizacji. Zarządzanie ciągłością działania.**	1. Cyberryzyko 2. Budowanie „ochrony w głąb” 3. BIA (Business Impact Analysis) 4. Strategia zarządzania ciągłością działania 5. Plany ciągłości działania i plany awaryjne 6. Testowanie, utrzymywanie i audyt procesu zarządzania ciągłością działania 7. Outsourcing jako czynnik ryzyka	10	6	16
4	**Architektura Cyberbezpieczeństwa.**	1. Security by design 2. Systemy bezpieczeństwa 3. Wymagania i architektura bezpieczeństwa 4. Obsługa incydentów 6. Zasoby 7. Security awerness	6	2	8
		Razem:	**26**	14	40

Sposób zakończenia: Egzamin - 1 godzina	Punkty ECTS: 5

<table>
<tr><td colspan="3">Bezpieczeństwo systemów i sieci</td><td colspan="3">Przedmiot nr 6</td></tr>
<tr><td colspan="3">Efekty uczenia się z zakresu:
Wiedzy:
- Ma wiedzę ogólną obejmującą kluczowe zagadnienia bezpieczeństwa systemów i sieci.
- Zna narzędzia i techniki wykorzystywane do rozpoznawania zagrożeń.
Umiejętności:
- Potrafi zaprojektować i wdrożyć procedury zapewniające bezpieczeństwo sieci i systemów.
- Potrafi wykorzystać narzędzia i techniki do rozpoznawania zagrożeń.
Kompetencji społecznych:
- Potrafi współdziałać i pracować w grupie, przyjmując w niej różne role.
- Rozumie potrzebę uczenia się przez całe życie.</td><td colspan="3">Czas realizacji

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.
2. Atrybuty i zagrożenia bezpieczeństwa.
3. Klasyfikacja przyczyn złego funkcjonowania systemów informatycznych.
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.
2. Konfiguracja serwerów danych i aplikacji.
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.
2. Zero trust security.
3. Wielowarstwowa architektura bezpieczeństwa.
4. Systemy bezpieczeństwa wewnętrznego.
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	**Punkty ECTS: 4**

Algorytmy i mechanizmy kryptograficzne			Przedmiot nr 7		
Efekty uczenia się z zakresu: **Wiedzy:** - Ma wiedzę ogólną obejmującą kluczowe zagadnienia bezpieczeństwa systemów, urządzeń i procesów. - Ma wiedzę z zakresu mechanizmów szyfrowania danych. **Umiejętności:** - Potrafi posłużyć się właściwie dobranymi metodami i oprogramowaniem kryptograficznym. - Potrafi ocenić przydatność narzędzi szyfrowania i uwierzytelniania. **Kompetencji społecznych:** - Potrafi współdziałać i pracować w grupie, przyjmując w niej różne role. - Rozumie potrzebę uczenia się przez całe życie.			**Czas realizacji** **20 godz.**		
Lp.	**Temat**	**Tezy**	Wykład	Ćwiczenia	**Razem**
1	**Kryptologia.**	1. Podstawowe pojęcia. 2. Atrybuty bezpieczeństwa i siła zabezpieczeń. 3. Kryptografia symetryczna i asymetryczna. 4. Szyfrowanie blokowe i strumieniowe.	3	4	**7**
2	**Funkcje skrótu.**	1. Klasyfikacja. 2. Kryteria. 3. Zastosowanie.	0	3	**3**
3	**Infrastruktura klucza publicznego PKI.**	1. Certyfikat klucza publicznego. 2. Centra Certyfikacji. 3. Hierarchia certyfikatów. 4. Unieważnianie certyfikatów.	2	0	**2**
4	**Szyfrowanie transmisji danych i poczty elektronicznej.**	1. Wykorzystanie szyfrowania w transmisji danych i poczcie elektronicznej.	0	4	**4**
5	**Kryptoanaliza.**	1. Metody kryptoanalizy.	2	2	4
		Razem:	**7**	**13**	20

Sposób zakończenia: Zaliczenie z oceną	Punkty ECTS: 3

8. **Sylabusy poszczególnych kart przedmiotów uwzględniające metody weryfikacji efektów uczenia się osiąganych przez studentów:**

Sylabusy poszczególnych kart przedmiotów, uwzględniające metody weryfikacji efektów uczenia się osiąganych przez studentów, opracowują prowadzący dany przedmiot, na podstawie zatwierdzonego programu studiów podyplomowych.

9. **Wymiar i zasady odbywania praktyk (jeśli program je przewiduje**): Na studiach podyplomowych nie przewiduje się odbywania praktyki zawodowej.

10. **Macierz efektów uczenia się wiążącą zakładane dla studiów podyplomowych: Efekty uczenia się z przedmiotami, w których efekty te są osiągane:**

Macierz efektów uczenia się
dla programu studiów podyplomowych w zakresie *cyberbezpieczeństwa*

Kod efektu uczenia się dla programu kształcenia studiów podyplomowych	Opis efektu uczenia się dla programu kształcenia studiów podyplomowych	Moduły kształcenia (przedmioty)							
		MK_1	MK_2	MK_3	MK_4	MK_5a	MK_5b	MK_6	MK_7
		Cyberprzestępczość.	Biały wywiad – pozyskiwanie danych z Internetu.	Zabezpieczenia sprzętu elektronicznego do badań.	Infrastruktura Internetu i usługi sieciowe	Odzyskiwanie i analiza danych z nośników cyfrowych.	Cyberryzyko i cyberbezpieczeństwo wewnętrzne organizacji	Bezpieczeństwo systemów i sieci.	Algorytmy i mechanizmy kryptograficzne.
K_W01	Zna metody, techniki, narzędzia stosowane przy korzystaniu z sieci Internet.		+						
K_W02	Zna portale, metody, techniki i narzędzia wykorzystywane przy gromadzeniu informacji w ramach białego wywiadu, zna metodykę przeprowadzania białego wywiadu.		+						
K_W03	Zna wybrane narzędzia usprawniające/wizualizujące dedykowane wyszukiwaniu informacji w ramach białego wywiadu.		+						
K_W04	Potrafi określić źródła dowodowe dotyczące śladów i dowodów cyfrowych.			+					
K_W05	Opisuje metodykę zabezpieczania sprzętu elektronicznego do badań.			+					
K_W06	Ma wiedzę ogólną obejmującą kluczowe zagadnienia bezpieczeństwa systemów i sieci.							+	

K_W07	Zna narzędzia i techniki wykorzystywane do rozpoznawania zagrożeń.							+	
K_W08	Ma wiedzę ogólną obejmującą kluczowe zagadnienia bezpieczeństwa systemów, urządzeń i procesów.								+
K_W09	Ma wiedzę z zakresu mechanizmów szyfrowania danych.								+
K_W10	Posiada wiedzę z zakresu bezpieczeństwa systemów informatycznych.	+							
K_W11	Zna i rozumie prawne możliwości ścigania cyberprzestępstw.	+							
K_W12	Zna możliwości i zastosowanie oprogramowania do odzyskiwania danych z nośników cyfrowych.					+			
K_W13	Zna metody, techniki oraz narzędzia stosowane przy analizie elektronicznego materiału dowodowego.					+			
K_W14	Potrafi opisać architekturę usług sieciowych.				+				
K_W15	Określa wymagania jakościowe usług sieciowych.				+				
K_W16	Posiada wiedzę nt. urządzeń sieciowych omówionych w materiale.				+				
K_W17	Posiada wiedzę z zakresu zarządzania ryzykiem systemów informacyjnych.						+		
K_W18	Posiada wiedzę z zakresu zarządzania zapewnieniem ciągłości działania.						+		
K_U01	Potrafi pozyskiwać dane, a także umiejętnie interpretować otrzymanie wyniki.		+						
K_U02	Potrafi użyć ogólnodostępnych narzędzi, m.in. wyszukiwarek internetowych i portali społecznościowych, jako źródła danych operacyjnych.		+						
K_U03	Potrafi zabezpieczyć sprzęt elektroniczny do badań.			+					
K_U04	Dokonuje wstępnej identyfikacji sprzętu elektronicznego do badań.			+					

K_U05	Potrafi zaprojektować i wdrożyć procedury zapewniające bezpieczeństwo sieci i systemów.							+	
K_U06	Potrafi wykorzystać narzędzia i techniki do rozpoznawania zagrożeń.							+	
K_U07	Potrafi posłużyć się właściwie dobranymi metodami i oprogramowaniem kryptograficznym.								+
K_U08	Potrafi ocenić przydatność narzędzi szyfrowania i uwierzytelniania.								+
K_U09	Potrafi rozpoznać i przeciwdziałać zagrożeniom w cyberprzestrzeni.	+							
K_U10	Wskazuje kierunki rozwoju cyberprzestępczości.	+							
K_U11	Potrafi odzyskać dane z nośników elektronicznych.					+			
K_U12	Potrafi dobrać optymalną metodę odzysku danych w zależności od rodzaju nośnika.					+			
K_U13	Potrafi analizować dane, a także umiejętnie interpretować otrzymane wyniki.					+			
K_U14	Potrafi w oparciu o dostępną dokumentację wdrożyć i uruchomić usługę sieciową.				+				
K_U15	Potrafi utworzyć dokumentację techniczną powiązaną z wdrożeniem.				+				
K_U16	Potrafi dokonać konfiguracji systemu komputerowego.				+				
K_U17	Potrafi administrować systemami komputerowymi.				+				
K_U18	Potrafi identyfikować strukturę i czynniki ryzyka.						+		
K_U19	Potrafi wdrożyć i stosować model zarządzania ryzykiem SI.						+		
K_U20	Potrafi identyfikować procesy kluczowe i krytyczne.						+		

K_U21	Potrafi wdrożyć i stosować model zarządzania zapewnieniem ciągłości działania.						+		
K_K01	Zna ograniczenia własnej wiedzy oraz konieczność dalszego poszukiwania i nauki.		+						
K_K02	Wskazuje przedsiębiorczość i kreatywność w myśleniu i działaniu.		+						
K_K03	Potrafi współdziałać i pracować w grupie, przyjmując w niej różne role.	+	+	+	+	+	+	+	+
K_K04	Potrafi odpowiednio określić priorytety służące realizacji określonego przez siebie lub innych zadania.	+		+		+	+		
K_K05	Rozumie potrzebę uczenia się przez całe życie.							+	+

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

11. Sposoby weryfikacji zakładanych efektów uczenia się osiąganych przez słuchacza studiów podyplomowych:

Symbol kierunkowych efektów kształcenia	Opis kierunkowych efektów kształcenia	Metody weryfikacji efektów kształcenia									
		Sposób realizacji efektu	Egzamin/ zaliczenie ustne	Egzamin/ zaliczenie pisemne	Test wiedzy	Kolokwium	Przygotowanie pracy na zadany temat	Przygotowanie i przedstawienie prezentacji/ symulacji	Realizacja zadania praktycznego	Analiza przypadku	Poziom pracy w zespole
K_W01	Zna metody, techniki, narzędzia stosowane przy korzystaniu z sieci Internet.	PzN		X			X		X		X
		PW		X			X		X		X
K_W02	Zna portale, metody, techniki i narzędzia wykorzystywane przy gromadzeniu informacji w ramach białego wywiadu, zna metodykę przeprowadzania białego wywiadu.	PzN		X			X		X		X
		PW		X			X		X		X
K_W03	Zna wybrane narzędzia usprawniające/wizualizujące dedykowane wyszukiwaniu informacji w ramach białego wywiadu.	PzN		X			X		X	X	X
		PW		X			X		X	X	X
K_W04	Potrafi określić źródła dowodowe dotyczące śladów i dowodów cyfrowych.	PzN		X			X		X	X	X
		PW		X			X		X	X	X
K_W05	Opisuje metodykę zabezpieczania sprzętu elektronicznego do badań.	PzN		X			X		X	X	X
		PW		X			X		X	X	X
K_W06	Ma wiedzę ogólną obejmującą kluczowe zagadnienia bezpieczeństwa systemów i sieci.	PzN		X			X		X		X
		PW		X			X		X		X
K_W07	Zna narzędzia i techniki wykorzystywane do rozpoznawania zagrożeń.	PzN		X			X		X		X
		PW		X			X		X		X
K_W08	Ma wiedzę ogólną obejmującą kluczowe zagadnienia bezpieczeństwa systemów, urządzeń i procesów.	PzN		X			X		X		X
		PW		X			X		X		X
K_W09	Ma szczegółową wiedzę z zakresu	PzN		X			X		X		X

	mechanizmów szyfrowania danych.	PW		X			X		X		X
K_W10	Posiada wiedzę z zakresu bezpieczeństwa systemów informatycznych.	PzN		X			X		X		X
		PW		X			X		X		X
K_W11	Zna i rozumie prawne możliwości ścigania cyberprzestępstw.	PzN		X			X		X		X
		PW		X			X		X		X
K_W12	Zna możliwości i zastosowanie oprogramowania do odzyskiwania danych z nośników cyfrowych.	PzN		X			X		X		X
		PW		X			X		X		X
K_W13	Zna metody, techniki oraz narzędzia stosowane przy analizie elektronicznego materiału dowodowego.	PzN		X			X		X		X
		PW		X			X		X		X
K_W14	Potrafi opisać architekturę usług sieciowych.	PzN		X			X		X		X
		PW		X			X		X		X
K_W15	Określa wymagania jakościowe usług sieciowych.	PzN		X			X	X	X		X
		PW		X			X	X	X		X
K_W16	Posiada wiedzę nt. urządzeń sieciowych omówionych w materiale.	PzN		X			X	X	X		X
		PW		X			X	X	X		X
K_W17	Posiada wiedzę z zakresu zarządzania ryzykiem systemów informacyjnych.	PzN		X			X				
		PW		X			X				
K_W18	Posiada wiedzę z zakresu zarządzania ryzykiem systemów informacyjnych.	PzN		X			X				
		PW		X			X				
K_U01	Potrafi pozyskiwać dane, a także umiejętnie interpretować otrzymanie wyniki.	PzN		X			X		X		X
		PW		X			X		X		X
K_U02	Potrafi użyć ogólnodostępnych narzędzi, m.in. wyszukiwarek internetowych i portali społecznościowych, jako źródła danych operacyjnych.	PzN		X			X		X		X
		PW		X			X		X		X
K_U03	Potrafi zabezpieczyć sprzęt elektroniczny do badań.	PzN		X			X		X	X	X
		PW		X			X		X	X	X
K_U04	Dokonuje wstępnej identyfikacji sprzętu elektronicznego do badań.	PzN		X			X		X	X	X
		PW		X			X		X	X	X

K_U05	Potrafi zaprojektować i wdrożyć procedury zapewniające bezpieczeństwo sieci i systemów.	PzN		X			X	X	X		X
		PW		X			X	X	X		X
K_U06	Potrafi wykorzystać narzędzia i techniki do rozpoznawania zagrożeń.	PzN		X			X	X	X		X
		PW		X			X	X	X		X
K_U07	Potrafi posłużyć się właściwie dobranymi metodami i oprogramowaniem kryptograficznym.	PzN		X			X	X	X		X
		PW		X			X	X	X		X
K_U08	Potrafi ocenić przydatność narzędzi szyfrowania i uwierzytelniania.	PzN		X			X		X		X
		PW		X			X		X		X
K_U09	Potrafi rozpoznać i przeciwdziałać zagrożeniom w cyberprzestrzeni.	PzN		X			X		X		X
		PW		X			X		X		X
K_U10	Wskazuje kierunki rozwoju cyberprzestępczości.	PzN		X			X		X		X
		PW		X			X		X		X
K_U11	Potrafi odzyskać dane z nośników elektronicznych.	PzN		X			X		X		X
		PW		X			X		X		X
K_U12	Potrafi dobrać optymalną metodę odzysku danych w zależności od rodzaju nośnika.	PzN		X			X		X		X
		PW		X			X		X		X
K_U13	Potrafi analizować dane, a także umiejętnie interpretować otrzymane wyniki.	PzN		X			X		X		X
		PW		X			X		X		X
K_U14	Potrafi w oparciu o dostępną dokumentację wdrożyć i uruchomić usługę sieciową.	PzN		X			X		X		X
		PW		X			X		X		X
K_U15	Potrafi utworzyć dokumentację techniczną powiązaną z wdrożeniem.	PzN		X			X		X		X
		PW		X			X		X		X
K_U16	Potrafi dokonać konfiguracji systemu komputerowego.	PzN		X			X		X		X
		PW		X			X		X		X
K_U17	Potrafi administrować systemami komputerowymi.	PzN		X			X		X		X
		PW		X			X		X		X
K_U18	Potrafi identyfikować strukturę	PzN		X			X		X		X

	i czynniki ryzyka.	PW		X			X		X		X
K_U19	Potrafi wdrożyć i stosować model zarządzania ryzykiem SI.	PzN		X			X		X		X
		PW		X			X		X		X
K_U20	Potrafi identyfikować procesy kluczowe i krytyczne.	PzN		X			X		X		X
		PW		X			X		X		X
K_U21	Potrafi wdrożyć i stosować model zarządzania zapewnieniem ciągłości działania.	PzN		X			X		X		X
		PW		X			X		X		X
K_K01	Zna ograniczenia własnej wiedzy oraz konieczność dalszego poszukiwania i nauki.	PzN		X			X		X		X
		PW		X			X		X		X
K_K02	Wskazuje przedsiębiorczość i kreatywność w myśleniu i działaniu.	PzN		X			X		X		X
		PW		X			X		X		X
K_K03	Potrafi współdziałać i pracować w grupie, przyjmując w niej różne role.	PzN		X			X		X		X
		PW		X			X		X		X
K_K04	Potrafi odpowiednio określić priorytety służące realizacji określonego przez siebie lub innych zadania.	PzN		X			X		X		X
		PW		X			X		X		X
K_K05	Rozumie potrzebę uczenia się przez całe życie.	PzN		X			X		X		X
		PW		X			X		X		X