UCHWAŁA NR 209/V/2025
SENATU AKADEMII POLICJI W SZCZYTNIE

z dnia 24 września 2025 r.

w sprawie ustalenia programu studiów podyplomowych w zakresie cyberbezpieczeństwa 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 (t.j. Dz. U. z 2023 r., poz.742 ze zm.) w związku z § 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 cyberbezpieczeństwa dla uczestników rozpoczynających studia podyplomowe 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 209/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 cyberbezpieczeństwa

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 cyberbezpieczeństwa

3. **Obszar kształcenia/ obszar kształcenia, do którego przyporządkowane są studia podyplomowe**: nauki społeczne

4. **Założenia ogólne (ogólna koncepcja kształcenia):**

   Głównym celem kształcenia w ramach studiów podyplomowych w zakresie cyberbezpieczeństwa jest przygotowanie uczestników studiów podyplomowych do kompleksowego rozpoznawania i przeciwdziałania zagrożeniom w cyberprzestrzeni, obejmującego:

   - wykorzystanie białego wywiadu w analizie informacji,
   - znajomość zagrożeń w cyberprzestrzeni,
   - wykorzystanie sieci komputerowych,
   - rozwijanie świadomości oraz edukacji w obszarze cyberbezpieczeństwa,
   - identyfikację i ocenę cyberryzyka,
   - bezpieczeństwo systemów i sieci informatycznych,
   - zastosowanie kryptografii w ochronie informacji i komunikacji.

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

   Studia podyplomowe w zakresie cyberbezpieczeństwa są efektem zaangażowania Uczelni w kształcenie i doskonalenie kadr służb oraz innych podmiotów, które w ramach swoich kompetencji uczestniczą w przeciwdziałaniu i zwalczaniu 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, a także 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. **Wymagania wstępne**: ukończone studia wyższe.

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

8. **Zasady rekrutacji**:

   Rekrutacja na studia podyplomowe może być otwarta lub zamknięta (studia dedykowane dla określonej grupy) i odbywa się na zasadzie kolejności zgłoszeń. W przypadku zgłoszenia się liczby kandydatów przekraczającej limit miejsc, o przyjęciu na studia podyplomowe decyduje termin zgłoszenia, ocena zajmowanego stanowiska służbowego oraz ocena i analiza przedłożonych dokumentów.

   Komendant-Rektor określa zasady postępowania kwalifikacyjnego, wymagane dokumenty oraz warunki przyjęcia. Zasady i warunki postępowania kwalifikacyjnego ogłaszane są na stronie internetowej Uczelni. Postępowanie kwalifikacyjne prowadzone jest przez system Internetowej Rejestracji Kandydata.

   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 cyberbezpieczeństwa. W zależności od wyniku postępowania kwalifikacyjnego Komendant-Rektor może zmienić limity przyjęć.

   Po zakończonym postępowaniu kwalifikacyjnym, osoba niezakwalifikowana na studia odbiera dokumenty w Dziekanacie Wydziału Bezpieczeństwa i Nauk Prawnych osobiście, dokumenty nieodebrane w ciągu miesiąca od rozpoczęcia zajęć zostaną odesłane na adres wskazany w postępowaniu kwalifikacyjnym.

9. **Opłaty**:

   Funkcjonariusze i pracownicy służb podległych ministrowi właściwemu do spraw wewnętrznych, którzy uzyskali zgodę na podjęcie studiów podyplomowych w APwSz wydaną przez przełożonego właściwego w sprawach osobowych (skierowanie), nie ponoszą opłat za kształcenie, związanych z podjęciem studiów podyplomowych. Funkcjonariusze i pracownicy podlegli ministrowi właściwemu do spraw wewnętrznych do podjęcia studiów podyplomowych nie ponoszą opłat z tytułu zakwaterowania i wyżywienia podczas zjazdów dydaktycznych. Pracownicy innych służb ponoszą opłaty

za kształcenie związane z prowadzeniem studiów podyplomowych na zasadach określonych w przepisach obowiązujących w Akademii Policji w Szczytnie.

10. Warunki ukończenia studiów podyplomowych:

Warunkiem ukończenia studiów podyplomowych jest osiągniecie efektów uczenia się przewidzianych programem studiów podyplomowych oraz aktywne i systematyczne uczestniczenie w zajęciach, 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 Akademii 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 2024 r. poz. 1606) 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 i rozumie prawne możliwości ścigania cyberprzestępstw	**P6S_WK**
K_W02	Posiada wiedze z zakresu bezpieczeństwa systemów informatycznych	**P6S_WK**
K_W03	Zna metody, techniki, narzędzia stosowane przy korzystaniu z sieci Internet	**P6S_WK**
K_W04	Zna portale, metody, techniki i narzędzia wykorzystywane przy gromadzeniu informacji w ramach białego wywiadu, zna metodykę przeprowadzania białego wywiadu	**P6S_WK**
K_W05	Zna wybrane narzędzia usprawniające/ wizualizujące dedykowane wyszukiwaniu informacji w ramach białego wywiadu	**P6S_WK**
K_W06	Zna specjalistyczne pojęcia dotyczące cyberzagrożeń	**P6S_WK**
K_W07	Zna rodzaje i specyfikację cyberzagrożeń	**P6S_WK**
K_W08	Zna i rozumie zasady przeciwdziałania zagrożeniom w cyberprzestrzeni	**P6S_WK**
K_W09	Ma wiedzę na temat architektury usług sieciowych	**P6S_WK**
K_W10	Ma wiedzę w zakresie wymagań jakościowych usług sieciowych	**P6S_WK**
K_W11	Zna narzędzia i techniki wykorzystywane do rozpoznawania zagrożeń	**P6S_WK**
K_W12	Rozumie pojęcie świadomości w cyberbezpieczeństwie	**P6S_WK**
K_W13	Identyfikuje główne typy zagrożeń wynikających z nieświadomych działań użytkowników	**P6S_WK**
K_W14	Ma wiedzę z zakresu zarządzania ryzykiem systemów informacyjnych	**P6S_WK**
K_W15	Posiada wiedzę z zakresu zarządzania zapewnieniem ciągłości działania	**P6S_WK**
K_W16	Ma wiedzę ogólną obejmującą kluczowe zagadnienia bezpieczeństwa systemów, urządzeń i procesów	**P6S_WK**
K_W17	Zna narzędzia i techniki wykorzystywane do rozpoznawania zagrożeń	**P6S_WK**
K_W18	Ma wiedzę ogólną obejmującą kluczowe zagadnienia bezpieczeństwa systemów, urządzeń i procesów	**P6S_WK**
K_W19	Ma wiedzę z zakresu mechanizmów szyfrowania danych	**P6S_WK**
Umiejętności		
K_U01	Potrafi rozpoznać i przeciwdziałać zagrożeniom w cyberprzestrzeni	**P6S_UW**
K_U02	Wskazuje kierunki rozwoju cyberprzestępczości.	**P6S_UW**
K_U03	Potrafi pozyskiwać dane, a także umiejętnie interpretować otrzymanie wyniki.	**P6S_UW**
K_U04	Potrafi użyć ogólnodostępnych narzędzi, m.in. wyszukiwarek internetowych i portali społecznościowych, jako źródła danych	**P6S_UW**

	operacyjnych	
K_U05	Potrafi identyfikować złożone procesy i nietypowe zagrożenia w cyberprzestrzeni.	**P6S_UW**
K_U06	Potrafi sporządzić program profilaktyczny w zakresie zwalczania nietypowych zagrożeń w cyberprzestrzeni.	**P6S_UW**
K_U07	Potrafi w oparciu o dostępną dokumentację wdrożyć i uruchomić usługę sieciową	**P6S_UW**
K_U08	Potrafi utworzyć dokumentację techniczną powiązaną z wdrożeniem	**P6S_UW**
K_U09	Potrafi dokonać konfiguracji systemu komputerowego	**P6S_UW**
K_U10	Potrafi administrować systemami komputerowymi	**P6S_UW**
K_U11	Potrafi analizować i oceniać sytuacje, w których brak świadomości użytkownika prowadzi do incydentów bezpieczeństwa	**P6S_UW**
K_U12	Potrafi stosować zasady cyberhigieny w pracy i życiu prywatnym	**P6S_UW**
K_U13	Potrafi opracować i zaprezentować program edukacyjny/kampanię podnoszącą świadomość cyberzagrożeń dla wybranej grupy docelowej	**P6S_UW**
K_U14	Potrafi identyfikować strukturę i czynniki ryzyka	**P6S_UW**
K_U15	Potrafi wdrożyć i stosować model zarządzania ryzykiem SI	**P6S_UW**
K_U16	Potrafi identyfikować procesy kluczowe i krytyczne	**P6S_UW**
K_U17	Potrafi wdrożyć i stosować model zarządzania zapewnieniem ciągłości działania	**P6S_UW**
K_U18	Potrafi zaprojektować i wdrożyć procedury zapewniające bezpieczeństwo sieci i systemów	**P6S_UW**
K_U19	Potrafi wykorzystać narzędzia i techniki do rozpoznawania zagrożeń	**P6S_UW**
K_U20	Potrafi posłużyć się właściwie dobranymi metodami i oprogramowaniem kryptograficznym	**P6S_UW**
K_U21	Potrafi ocenić przydatność narzędzi szyfrowania i uwierzytelniania	**P6S_UW**
Kompetencje społeczne		
K_K01	Potrafi odpowiednio określić priorytety służące realizacji określonego przez siebie lub innych zadania	**P6S_KK**
K_K02	Potrafi współdziałać i pracować w grupie, przyjmując w niej różne role	**P6S_KO**
K_K03	Zna ograniczenia własnej wiedzy oraz konieczność dalszego poszukiwania i nauki	**P6S_KR**
K_K04	Wskazuje przedsiębiorczość i kreatywność w myśleniu i działaniu	**P6S_KR**
K_K05	Jest gotów do uznania znaczenia wiedzy w rozwiązywaniu problemów poznawczych i praktycznych w zakresie zwalczania i przeciwdziałania cyberzagrożeniom	**P6S_KK**
K_K06	Jest gotowy do pogłębionej analizy i krytycznej oceny posiadanej wiedzy z zakresu cyberzagrożeń oraz zasięgania opinii ekspertów w przypadku trudności z samodzielnym rozwiązaniem problemu praktycznego	**P6S_KK**
K_K07	Rozumie swoją rolę, jako aktywnego uczestnika w budowaniu kultury bezpieczeństwa w organizacji i społeczeństwie	**P6S_KO**
K_K08	Jest gotów do odpowiedzialnego reagowania na incydenty i dzielenia się wiedzą z innymi	**P6S_KK**
K_K09	Potrafi krytycznie ocenić własne nawyki cyfrowe i korygować zachowania obniżające poziom bezpieczeństwa	**P6S_KK**
K_K10	Rozumie potrzebę uczenia się przez całe życie.	**P6S_KO**

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:** 226 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	Cyberbezpieczeństwo	**25**	**13**	**12**	S	**4**	**2,08**	**1,92**
2	Biały wywiad	**40**	**12**	**28**	E	**5**	**1,5**	**3,5**
3	Encyklopedia zagrożeń w cyberprzestrzeni	**40**	**10**	**30**	E	**5**	**2,25**	**2,75**
4	Sieci komputerowe	**20**	**10**	**10**	S	**4**	**2**	**2**
	ŁĄCZNIE w semestrze	**125**	**45**	**80**	**—**	**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	Świadomość i edukacja w cyberbezpieczeństwie	**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**	S	**4**	**2,8**	**1,2**
7	Kryptografia w zakresie cyberbezpieczeństwa	**20**	**6**	**14**	S	**3**	**1,05**	**1,95**
8	Egzaminy i zaleczenia		**7**		—		**—**	
9	Konsultacje		6		—		—	
10	Egzamin końcowy		8		—		—	
	ŁĄCZNIE w semestrze	**80+21**	**20**	**50**	**—**	**12**	**5,1[a]**	**6,9[a]**
			46	**34**			**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

<table>
<tr><td colspan="3">Cyberbezpieczeństwo</td><td colspan="3">Przedmiot nr 1</td></tr>
<tr><td colspan="3" rowspan="2">Efekty uczenia się w zakresie:
Wiedzy:
− Posiada wiedzę 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.</td><td colspan="3">Czas realizacji</td></tr>
<tr><td colspan="3">25 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 w cyberprzestrzeni</td><td>1. Przedmioty ochrony i zagrożenia systemów informatycznych.
2. Polityka bezpieczeństwa informatycznego.</td><td>2</td><td>2</td><td>4</td></tr>
<tr><td>2</td><td>Cyberprzestępstwa</td><td>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.</td><td>9</td><td>8</td><td>17</td></tr>
<tr><td>3</td><td>Charakterystyka cyberprzestępczości w Polsce</td><td>1. Nowy wymiar Cyberbezpieczeństwa,
2. Profilaktyka w zakresie cyberprzestępczości.</td><td>2</td><td>2</td><td>4</td></tr>
<tr><td colspan="3">Razem:</td><td>13</td><td>12</td><td>25</td></tr>
</table>

Sposób zakończenia: Zaliczenie z oceną (1 godz.)	**Punkty ECTS: 4**

<table>
<tr><td colspan="4">Biały wywiad</td><td colspan="3">Przedmiot nr 2</td></tr>
<tr><td colspan="4">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.</td><td colspan="3">Czas realizacji

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>Open Source Intelligence</td><td>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.</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.
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. Wyszukiwarki internetowe
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.</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.
2. Modelowanie zagrożeń.
3. Narzędzia wspomagające CTI.</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>
</table>

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

Encyklopedia zagrożeń w cyberprzestrzeni			Przedmiot nr 3		
Efekty uczenia się z zakresu: **Wiedzy:** − Zna specjalistyczne pojęcia dotyczące cyberzagrożeń i ich praktyczne zastosowanie w działalności zawodowej. − Zna rodzaje i specyfikację cyberzagrożeń. − Zna i rozumie zasady przeciwdziałania zagrożeniom w cyberprzestrzeni. **Umiejętności:** − Potrafi identyfikować złożone procesy i nietypowe zagrożenia w cyberprzestrzeni. − Potrafi sporządzić program profilaktyczny w zakresie zwalczania nietypowych zagrożeń w cyberprzestrzeni. **Kompetencji społecznych:** − Jest gotów do uznania znaczenia wiedzy w rozwiązywaniu problemów poznawczych i praktycznych w zakresie zwalczania i przeciwdziałania cyberzagrożeniom. − Jest gotowy do pogłębionej analizy i krytycznej oceny posiadanej wiedzy z zakresu cyberzagrożeń oraz zasięgania opinii ekspertów w przypadku trudności z samodzielnym rozwiązaniem problemu praktycznego.			**Czas realizacji** **40 godz.**		
Lp.	**Temat**	**Tezy**	Wykład	Ćwiczenia	**Razem**
1	**Zagrożenia informatyczne w cyberprzestrzeni**	1. Definicje i klasyfikacja zagrożeń 2. Gry i motywacje cyberprzestępców. 3. Rodzaje ataków: aktywne, pasywne; wewnętrzne i zewnętrzne.	2	4	**6**
2	**Malware i złośliwe oprogramowanie**	1. Rodzaje złośliwego oprogramowania (wirusy, robaki, trojany, ransomware). 2. Mechanizmy infekcji i rozprzestrzeniania. 3. Symulacje ataków i ich wykrywanie. 4. Praktyczne metody zabezpieczania systemów przed malware.	2	6	**8**
3	**Ataki sieciowe i infrastrukturalne**	1. Ataki typu DDoS i DoS – mechanizmy i skutki. 2. Sniffing, spoofing, man-in-the-middle. 3. Botnety i ich rola w cyberatakach. 4. Zabezpieczenia sieciowe (firewalle, IDS/IPS).	2	4	**6**
4	**Socjotechnika i cyberbezpieczeństwo człowieka**	1. Znaczenie czynnika ludzkiego w cyberzagrożeniach. 2. Metody profilaktyki i edukacji użytkowników.	2	10	**12**
5	**Profilaktyka cyberprzestępczości i zarządzanie ryzykiem**	1. Polityki bezpieczeństwa i procedury reagowania na incydenty. 2. Strategie minimalizacji ryzyka i zabezpieczeń organizacji. 3. Rola edukacji i szkoleń w profilaktyce	2	6	**8**
		Razem:	**10**	**30**	**40**

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

<table>
<tr><td colspan="4">Sieci komputerowe</td><td colspan="3">Przedmiot nr 4</td></tr>
<tr><td colspan="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.</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>Technologie sieciowe wykorzystywane przy tworzeniu współczesnych sieci komputerowych</td><td>1. Protokoły IP, urządzenia sieciowe, łączenie sieci.
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.
2. Modele chmury obliczeniowej.
3. Regulacje prawne w obszarze chmury obliczeniowej.
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.
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. Falszywe numery telefonów.
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.</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: 4**

<table>
<tr><td colspan="4">Świadomość i edukacja w cyberbezpieczeństwie</td><td colspan="3">Przedmiot nr 5a</td></tr>
<tr><td colspan="4" rowspan="2">Efekty uczenia się z zakresu:
Wiedzy:
− Zna i rozumie pojęcie świadomości w cyberbezpieczeństwie oraz jej znaczenie dla jednostek, organizacji i całego społeczeństwa.
− Identyfikuje główne typy zagrożeń wynikających z nieświadomych działań użytkowników.
Umiejętności:
− Potrafi analizować i oceniać sytuacje, w których brak świadomości użytkownika prowadzi do incydentów bezpieczeństwa.
− Potrafi stosować zasady cyberhigieny w pracy i życiu prywatnym.
− Potrafi opracować i zaprezentować program edukacyjny/kampanię podnoszącą świadomość cyberzagrożeń dla wybranej grupy docelowej.
Kompetencji społecznych:
− Rozumie swoją rolę, jako aktywnego uczestnika w budowaniu kultury bezpieczeństwa w organizacji i społeczeństwie.
− Jest gotów do odpowiedzialnego reagowania na incydenty i dzielenia się wiedzą z innymi.
− Potrafi krytycznie ocenić własne nawyki cyfrowe i korygować zachowania obniżające poziom bezpieczeństwa.</td><td colspan="3">Czas realizacji</td></tr>
<tr><td colspan="3">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>Świadomość w zakresie cyberbezpieczeństwa</td><td>1. Definicje i znaczenie świadomości w cyberbezpieczeństwie.
2. Człowiek jako ogniwo w systemie bezpieczeństwa.
3. Analiza rzeczywistych incydentów</td><td>2</td><td>6</td><td>8</td></tr>
<tr><td>2</td><td>Fake news i dezinformacja jako zagrożenie dla bezpieczeństwa informacyjnego</td><td>1. Fake news a zaufanie do instytucji i procesów demokratycznych.
2. Dezinformacja, jako narzędzie wojen hybrydowych i destabilizacji społecznej.
3. Media społecznościowe, jako nośnik i pole walki z dezinformacją.</td><td>4</td><td>6</td><td>10</td></tr>
<tr><td>3</td><td>Cyberhigiena – podstawowe zasady bezpieczeństwa cyfrowego</td><td>1. Hasła, uwierzytelnianie wieloskładnikowe, menedżery haseł.
2. Aktualizacje, kopie zapasowe, segmentacja urządzeń (domowych i biurowych).</td><td>2</td><td>4</td><td>6</td></tr>
<tr><td>4</td><td>Edukacja i kultura cyberbezpieczeństwa</td><td>1. Szkolenia i akcje, jako fundament podnoszenia świadomości w obszarze cyberbezpieczeństwa.
2. Strategie podnoszenia świadomości: kampanie phishingowe, gamifikacja, szkolenia cykliczne.</td><td>2</td><td>14</td><td>16</td></tr>
<tr><td colspan="3">Razem:</td><td>10</td><td>30</td><td>40</td></tr>
</table>

Sposób zakończenia: Egzamin (1 godz.)	**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** **40 godz.**		
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 godz.)	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" rowspan="2">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</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.
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 (1 godz.)	**Punkty ECTS: 4**

<table>
<tr><td colspan="3">Kryptografia w zakresie cyberbezpieczeństwa</td><td colspan="3">Przedmiot nr 7</td></tr>
<tr><td colspan="3" rowspan="2">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.</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>Kryptografia</td><td>1. Podstawowe pojęcia.
2. Atrybuty bezpieczeństwa i siła zabezpieczeń.
3. Kryptografia symetryczna i asymetryczna.
4. Szyfrowanie blokowe i strumieniowe.</td><td>4</td><td>5</td><td>9</td></tr>
<tr><td>2</td><td>Funkcje skrótu</td><td>1. Klasyfikacja.
2. Kryteria.
3. Zastosowanie.</td><td>0</td><td>3</td><td>3</td></tr>
<tr><td>4</td><td>Szyfrowanie transmisji danych i poczty elektronicznej</td><td>1. Wykorzystanie szyfrowania w transmisji danych i poczcie elektronicznej.</td><td>2</td><td>6</td><td>8</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: 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 wiążąca zakładane dla studiów podyplomowyche 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 studiów podyplomowych	Opis efektu uczenia się dla programu kształcenia studiów podyplomowych	Przedmioty							
		NP_1	NP _2	NP _3	NP _4	NP _5a	NP _5b	NP _6	NP _7
		Cyberbezpieczeństwo	Biały wywiad	Encyklopedia zagrożeń w cyberprzestrzenie	Sieci komputerowe	Świadomość i edukacja w cyberbezpieczeństwie	Cyberryzyko i cyberbezpieczeństwo wewnętrzne organizacji	Bezpieczeństwo systemów i sieci.	Kryptografia w zakresie cyberbezpieczeństwa
K_W01	Zna i rozumie prawne możliwości ścigania cyberprzestępstw	+							
K_W02	Posiada wiedze z zakresu bezpieczeństwa systemów informatycznych	+							
K_W03	Zna metody, techniki, narzędzia stosowane przy korzystaniu z sieci Internet		+						
K_W04	Zna portale, metody, techniki i narzędzia wykorzystywane przy gromadzeniu informacji w ramach białego wywiadu, zna metodykę przeprowadzania białego wywiadu		+						
K_W05	Zna wybrane narzędzia usprawniające/ wizualizujące dedykowane wyszukiwaniu informacji w ramach białego wywiadu		+						

K_W06	Zna specjalistyczne pojęcia dotyczące cyberzagrożeń			+					
K_W07	Zna rodzaje i specyfikację cyberzagrożeń			+					
K_W08	Zna i rozumie zasady przeciwdziałania zagrożeniom w cyberprzestrzeni			+					
K_W09	Ma wiedzę na temat architektury usług sieciowych				+				
K_W10	Ma wiedzę w zakresie wymagań jakościowych usług sieciowych				+				
K_W11	Zna narzędzia i techniki wykorzystywane do rozpoznawania zagrożeń				+				
K_W12	Rozumie pojęcie świadomości w cyberbezpieczeństwie					+			
K_W13	Identyfikuje główne typy zagrożeń wynikających z nieświadomych działań użytkowników					+			
K_W14	Ma wiedzę z zakresu zarządzania ryzykiem systemów informacyjnych						+		
K_W15	Posiada wiedzę z zakresu zarządzania zapewnieniem ciągłości działania						+		
K_W16	Ma wiedzę ogólną obejmującą kluczowe zagadnienia bezpieczeństwa systemów, urządzeń i procesów							+	
K_W17	Zna narzędzia i techniki wykorzystywane do rozpoznawania zagrożeń							+	
K_W18	Ma wiedzę ogólną obejmującą kluczowe zagadnienia bezpieczeństwa systemów, urządzeń i procesów								+
K_W19	Ma wiedzę z zakresu mechanizmów szyfrowania danych								+
K_U01	Potrafi rozpoznać i przeciwdziałać zagrożeniom w cyberprzestrzeni	+							

K_U02	Wskazuje kierunki rozwoju cyberprzestępczości.	+							
K_U03	Potrafi pozyskiwać dane, a także umiejętnie interpretować otrzymanie wyniki.		+						
K_U04	Potrafi użyć ogólnodostępnych narzędzi, m.in. wyszukiwarek internetowych i portali społecznościowych, jako źródła danych operacyjnych		+						
K_U05	Potrafi identyfikować złożone procesy i nietypowe zagrożenia w cyberprzestrzeni.			+					
K_U06	Potrafi sporządzić program profilaktyczny w zakresie zwalczania nietypowych zagrożeń w cyberprzestrzeni.			+					
K_U07	Potrafi w oparciu o dostępną dokumentację wdrożyć i uruchomić usługę sieciową				+				
K_U08	Potrafi utworzyć dokumentację techniczną powiązaną z wdrożeniem				+				
K_U09	Potrafi dokonać konfiguracji systemu komputerowego				+				
K_U10	Potrafi administrować systemami komputerowymi				+				
K_U11	Potrafi analizować i oceniać sytuacje, w których brak świadomości użytkownika prowadzi do incydentów bezpieczeństwa					+			
K_U12	Potrafi stosować zasady cyberhigieny w pracy i życiu prywatnym					+			
K_U13	Potrafi opracować i zaprezentować program edukacyjny/kampanię podnoszącą świadomość cyberzagrożeń dla wybranej grupy docelowej					+			
K_U14	Potrafi identyfikować strukturę i czynniki ryzyka						+		
K_U15	Potrafi wdrożyć i stosować model zarządzania ryzykiem SI						+		

K_U16	Potrafi identyfikować procesy kluczowe i krytyczne						+		
K_U17	Potrafi wdrożyć i stosować model zarządzania zapewnieniem ciągłości działania						+		
K_U18	Potrafi zaprojektować i wdrożyć procedury zapewniające bezpieczeństwo sieci i systemów							+	
K_U19	Potrafi wykorzystać narzędzia i techniki do rozpoznawania zagrożeń							+	
K_U20	Potrafi posłużyć się właściwie dobranymi metodami i oprogramowaniem kryptograficznym								+
K_U21	Potrafi ocenić przydatność narzędzi szyfrowania i uwierzytelniania								+
K_K01	Potrafi odpowiednio określić priorytety służące realizacji określonego przez siebie lub innych zadania	+					+		
K_K02	Potrafi współdziałać i pracować w grupie, przyjmując w niej różne role	+	+		+		+	+	+
K_K03	Zna ograniczenia własnej wiedzy oraz konieczność dalszego poszukiwania i nauki		+						
K_K04	Wskazuje przedsiębiorczość i kreatywność w myśleniu i działaniu		+						
K_K05	Jest gotów do uznania znaczenia wiedzy w rozwiązywaniu problemów poznawczych i praktycznych w zakresie zwalczania i przeciwdziałania cyberzagrożeniom			+					
K_K06	Jest gotowy do pogłębionej analizy i krytycznej oceny posiadanej wiedzy z zakresu cyberzagrożeń oraz zasięgania opinii ekspertów w przypadku trudności z samodzielnym rozwiązaniem problemu praktycznego			+					
K_K07	Rozumie swoją rolę, jako aktywnego uczestnika w budowaniu kultury bezpieczeństwa w organizacji i społeczeństwie					+			

K_K08	Jest gotów do odpowiedzialnego reagowania na incydenty i dzielenia się wiedzą z innymi					+			
K_K09	Potrafi krytycznie ocenić własne nawyki cyfrowe i korygować zachowania obniżające poziom bezpieczeństwa					+			
K_K10	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 uczestników 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 i rozumie prawne możliwości ścigania cyberprzestępstw	PzN		X			X		X		X
		PW		X			X		X		X
K_W02	Posiada wiedzę z zakresu bezpieczeństwa systemów informatycznych	PzN		X			X		X		X
		PW		X			X		X		X
K_W03	Zna metody, techniki, narzędzia stosowane przy korzystaniu z sieci Internet	PzN		X			X		X	X	X
		PW		X			X		X	X	X
K_W04	Zna portale, metody, techniki i narzędzia wykorzystywane przy gromadzeniu informacji w ramach białego wywiadu, zna metodykę przeprowadzania białego wywiadu	PzN		X			X		X	X	X
		PW		X			X		X	X	X
K_W05	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_W06	Zna specjalistyczne pojęcia dotyczące cyberzagrożeń	PzN		X			X		X		X
		PW		X			X		X		X
K_W07	Zna rodzaje i specyfikację cyberzagrożeń	PzN		X			X		X		X
		PW		X			X		X		X
K_W08	Zna i rozumie zasady przeciwdziałania zagrożeniom w cyberprzestrzeni	PzN		X			X		X		X
		PW		X			X		X		X

K_W09	Ma wiedzę na temat architektury usług sieciowych	PzN		X			X		X		X
		PW		X			X		X		X
K_W10	Ma wiedzę w zakresie wymagań jakościowych usług sieciowych	PzN		X			X		X		X
		PW		X			X		X		X
K_W11	Zna narzędzia i techniki wykorzystywane do rozpoznawania zagrożeń	PzN		X			X		X		X
		PW		X			X		X		X
K_W12	Rozumie pojęcie świadomości w cyberbezpieczeństwie	PzN		X			X		X		X
		PW		X			X		X		X
K_W13	Identyfikuje główne typy zagrożeń wynikających z nieświadomych działań użytkowników	PzN		X			X		X		X
		PW		X			X		X		X
K_W14	Ma wiedzę z zakresu zarządzania ryzykiem systemów informacyjnych	PzN		X			X		X		X
		PW		X			X		X		X
K_W15	Posiada wiedzę z zakresu zarządzania zapewnieniem ciągłości działania	PzN		X			X	X	X		X
		PW		X			X	X	X		X
K_W16	Ma wiedzę ogólną obejmującą kluczowe zagadnienia bezpieczeństwa systemów, urządzeń i procesów	PzN		X			X	X	X		X
		PW		X			X	X	X		X
K_W17	Zna narzędzia i techniki wykorzystywane do rozpoznawania zagrożeń	PzN		X			X				
		PW		X			X				
K_W18	Ma wiedzę ogólną obejmującą kluczowe zagadnienia bezpieczeństwa systemów, urządzeń i procesów	PzN		X			X				
		PW		X			X				
K_W19	Ma wiedzę z zakresu mechanizmów szyfrowania danych	PzN		X			X				
		PW		X			X				
K_U01	Potrafi rozpoznać i przeciwdziałać zagrożeniom w cyberprzestrzeni	PzN		X			X		X		X
		PW		X			X		X		X
K_U02	Wskazuje kierunki rozwoju cyberprzestępczości	PzN		X			X		X		X
		PW		X			X		X		X
K_U03	Potrafi pozyskiwać dane, a także umiejętnie interpretować otrzymanie wyniki	PzN		X			X		X	X	X
		PW		X			X		X	X	X

K_U04	Potrafi użyć ogólnodostępnych narzędzi, m.in. wyszukiwarek internetowych i portali społecznościowych, jako źródła danych operacyjnych	PzN		X			X		X	X	X
		PW		X			X		X	X	X
K_U05	Potrafi identyfikować złożone procesy i nietypowe zagrożenia w cyberprzestrzeni	PzN		X			X	X	X		X
		PW		X			X	X	X		X
K_U06	Potrafi sporządzić program profilaktyczny w zakresie zwalczania nietypowych zagrożeń w cyberprzestrzeni	PzN		X			X	X	X		X
		PW		X			X	X	X		X
K_U07	Potrafi w oparciu o dostępną dokumentację wdrożyć i uruchomić usługę sieciową	PzN		X			X	X	X		X
		PW		X			X	X	X		X
K_U08	Potrafi utworzyć dokumentację techniczną powiązaną z wdrożeniem	PzN		X			X		X		X
		PW		X			X		X		X
K_U09	Potrafi dokonać konfiguracji systemu komputerowego	PzN		X			X		X		X
		PW		X			X		X		X
K_U10	Potrafi administrować systemami komputerowymi	PzN		X			X		X		X
		PW		X			X		X		X
K_U11	Potrafi analizować i oceniać sytuacje, w których brak świadomości użytkownika prowadzi do incydentów bezpieczeństwa	PzN		X			X		X		X
		PW		X			X		X		X
K_U12	Potrafi stosować zasady cyberhigieny w pracy i życiu prywatnym	PzN		X			X		X		X
		PW		X			X		X		X
K_U13	Potrafi opracować i zaprezentować program edukacyjny/kampanię podnoszącą świadomość cyberzagrożeń dla wybranej grupy docelowej	PzN		X			X		X		X
		PW		X			X		X		X
K_U14	Potrafi identyfikować strukturę i czynniki ryzyka	PzN		X			X		X		X
		PW		X			X		X		X
K_U15	Potrafi wdrożyć i stosować model zarządzania ryzykiem SI	PzN		X			X		X		X
		PW		X			X		X		X
K_U16	Potrafi identyfikować procesy kluczowe i krytyczne	PzN		X			X		X		X
		PW		X			X		X		X

K_U17	Potrafi wdrożyć i stosować model zarządzania zapewnieniem ciągłości działania	PzN		X			X		X		X
		PW		X			X		X		X
K_U18	Potrafi zaprojektować i wdrożyć procedury zapewniające bezpieczeństwo sieci i systemów	PzN		X			X		X		X
		PW		X			X		X		X
K_U19	Potrafi wykorzystać narzędzia i techniki do rozpoznawania zagrożeń	PzN		X			X		X		X
		PW		X			X		X		X
K_U20	Potrafi posłużyć się właściwie dobranymi metodami i oprogramowaniem kryptograficznym	PzN		X			X		X		X
		PW		X			X		X		X
K_U21	Potrafi ocenić przydatność narzędzi szyfrowania i uwierzytelniania	PzN		X			X		X		X
		PW		X			X		X		X
K_K01	Potrafi odpowiednio określić priorytety służące realizacji określonego przez siebie lub innych zadania	PzN		X			X		X		X
		PW		X			X		X		X
K_K02	Potrafi współdziałać i pracować w grupie, przyjmując w niej różne role	PzN		X			X		X		X
		PW		X			X		X		X
K_K03	Zna ograniczenia własnej wiedzy oraz konieczność dalszego poszukiwania i nauki	PzN		X			X		X		X
		PW		X			X		X		X
K_K04	Wskazuje przedsiębiorczość i kreatywność w myśleniu i działaniu	PzN		X			X		X		X
		PW		X			X		X		X
K_K05	Jest gotów do uznania znaczenia wiedzy w rozwiązywaniu problemów poznawczych i praktycznych w zakresie zwalczania i przeciwdziałania cyberzagrożeniom	PzN		X			X		X		X
		PW		X			X		X		X
K_K06	Jest gotowy do pogłębionej analizy i krytycznej oceny posiadanej wiedzy z zakresu cyberzagrożeń oraz zasięgania opinii ekspertów w przypadku trudności z samodzielnym rozwiązaniem problemu praktycznego	PzN		X			X		X		X
		PW		X			X		X		X

K_K07	Rozumie swoją rolę, jako aktywnego uczestnika w budowaniu kultury bezpieczeństwa w organizacji i społeczeństwie	PzN		X			X		X		X
		PW		X			X		X		X
K_K08	Jest gotów do odpowiedzialnego reagowania na incydenty i dzielenia się wiedzą z innymi	PzN		X			X		X		X
		PW		X			X		X		X
K_K09	Potrafi krytycznie ocenić własne nawyki cyfrowe i korygować zachowania obniżające poziom bezpieczeństwa	PzN		X			X		X		X
		PW		X			X		X		X
K_K10	Rozumie potrzebę uczenia się przez całe życie	PzN		X			X		X		X
		PW		X			X		X		X