Załącznik do Uchwały nr 15/2021 Senatu KPSW

KARKONOSKA PAŃSTWOWA SZKOŁA WYŻSZA
w Jeleniej Górze

WYDZIAŁ NAUK MEDYCZNYCH I TECHNICZNYCH

KATEDRA NAUK INFORMATYCZNO-TECHNICZNYCH

Program studiów podyplomowych:

BEZPIECZEŃSTWO I OCHRONA DANYCH

Koordynator projektu studiów:

dr inż. Tadeusz Lewandowski

Autorzy:

mgr inż. Eugeniusz Gronostaj

dr inż. Jerzy Januszewicz

dr inż. Tadeusz Lewandowski

Jelenia Góra, 2021

Spis treści

1. OGÓLNA CHARAKTERYSTYKA STUDIÓW PODYPLOMOWYCH

Informacje podstawowe:

Wydział prowadzący studia podyplomowe	Wydział Nauk Medycznych i Technicznych
Katedra realizująca studia podyplomowe	Katedra Nauk Informatyczno-Technicznych
Nazwa studiów podyplomowych	Bezpieczeństwo i ochrona danych
Nazwa studiów podyplomowych w j. angielskim	Data security and protection
Obszar kształcenia	nauki społeczne/nauki ścisłe
Dyscypliny naukowe	nauki o bezpieczeństwie/informatyka
Liczba semestrów	2
Łączna liczba godzin zajęć dydaktycznych	360
Łączna liczba punktów ECTS	30
Forma studiów	studia podyplomowe realizowane w weekendy (co drugi tydzień) w formie hybrydowej (część zajęć prowadzona on-line, a część stacjonarnie w laboratoriach)

Cel: Celem studiów jest umożliwienie osobom podejmującym kierunek zdobycia obszernej wiedzy w tematyce zarządzania bezpieczeństwem danych oraz profesjonalne przygotowanie słuchaczy do podjęcia i pełnienia funkcji kierowniczych, menedżerskich w zakresie ochrony danych osobowych oraz zarządzania bezpieczeństwem informacji.

Opis kierunku:

Słuchacze studiów podyplomowych zostaną zaznajomieni z teoretyczną i praktyczną problematyką w zakresie zarządzania bezpieczeństwem informacji i ochrony danych osobowych w jednostkach organizacyjnych oraz poznają najistotniejsze akty prawne związane z bezpieczeństwem informacji.

Duża część zajęć, realizowana praktycznie w formie ćwiczeń i laboratoriów, poświęcona będzie wykorzystaniem metod i narzędzi informatycznych wspomagających ochronę danych.

Dodatkowo absolwent zdobędzie specjalistyczną wiedzę w zakresie samodzielnego wdrażania i ulepszania systemów zarządzania bezpieczeństwem informacji w firmach

i organizacjach. Ponadto słuchacze nabędą umiejętności efektywnego zarządzania ryzykiem w organizacji.

Adresaci:
Studia podyplomowe przeznaczone są dla absolwentów studiów wyższych zamierzających podjąć zatrudnienie w charakterze inspektora ochrony danych osobowych (IOD), w działach HR i IT w administracji publicznej, na stanowiskach kierowniczych w zakresie bezpieczeństwa informacji oraz dla osób, które zajmują się zagadnieniami i problematyką ochrony informacji i danych osobowych, chcących poszerzyć wiedzę i umiejętności, a także właścicieli firm, mini firm zajmujących się zabezpieczeniem informatycznym różnego rodzaju instytucji, szkół oraz małych firm produkcyjnych.

Uzasadnienie

Sprawy dotyczące bezpieczeństwa informacji są obecnie kluczowymi w zarządzaniu instytucją (firmą) i regulowane są stosownymi dokumentami wydanymi przez instytucje unijne i krajowe. Z krajowych należy wymienić Krajowe Ramy Interoperacyjności (D.U z dnia 05 grudnia 2017 r.), w których określono minimalne wymagania dla rejestrów publicznych i wymiany informacji w postaci elektronicznej. Zgodnie z wymaganiami, podmiot realizujący zadania publiczne ma obowiązek opracować i ustanowić, wdrożyć i eksploatować, monitorować i przeglądać oraz utrzymywać i doskonalić system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji.

Wymagania w zakresie zapewnienia ochrony danych osobowych zostały określone w nowym unijnym rozporządzeniu RODO, które weszło w życie w dniu 25 maja 2018 r. Tym samym przepisy dotyczące ochrony danych osobowych dla wszystkich państw członkowskich UE zostały ujednolicone. Ochrona danych osobowych wymaga zaprojektowania w instytucji lub przedsiębiorstwie całego systemu tej ochrony, w tym ustanowienia procedur dla wszystkich procesów zachodzących w urzędzie z uwzględnieniem wykorzystania danych osobowych. W każdym przypadku dla zrealizowania celów wynikających z wydanych regulacji prawnych koniecznością staje się przygotowanie zespołu ludzi, którzy wdrożą i będą eksploatować, monitorować i przeglądać oraz utrzymywać i doskonalić system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji.

Zatem zapewnienie bezpieczeństwa przetwarzania informacji w dobie współczesnej jest jednym z najistotniejszych wyzwań stojących przed samorządami, instytucjami i przedsiębiorstwami. Niewłaściwe zarządzanie bezpieczeństwem informacji może doprowadzić do wycieku, utraty lub sfałszowania danych posiadanych przez urząd. Możliwy jest także całkowity paraliż pracy instytucji oraz przedsiębiorstwa.

Rynek pracy

Ochrona danych to młoda specjalizacja, która popularność i szczególne znaczenie w działalności administracyjnej i biznesowej zyskała wraz z niedawnym wejściem w życie przepisów RODO. Rok temu Krajowy koordynator reformy RODO w Ministerstwie Cyfryzacji ocenił, że w skali kraju zapotrzebowanie na inspektorów wynosi nawet 50 tysięcy, a jak pokazują obserwacje rynku – zainteresowanie firm ekspertami w tej dziedzinie nie maleje. Okazuje się, że większość instytucji i przedsiębiorstw preferuje zatrudnienie

specjalisty, powierzając mu obowiązki Inspektora Ochrony Danych Osobowych. Podobne działania obserwuje się w zakresie bezpieczeństwa informacji.

Organizacje mierzą się z koniecznością znalezienia odpowiedzi na pytania o skuteczne sposoby rekrutacji inspektorów. Kandydaci natomiast – z poszukiwaniem pracy w zawodzie i oceną, które podmioty mogą być zainteresowane ich zatrudnieniem. Wynikiem jest obserwowany wzrost zapotrzebowania na ekspertów w zarządzaniu bezpieczeństwem informacji i ochrony danych osobowych.

Pracodawcy poszukujący kandydatów na stanowisko IOD najczęściej oczekują wykształcenia prawniczego lub zdobytego na kierunku związanym z IT oraz nowoczesnymi technologiami informatycznymi. Ogromną uwagę przykładają do merytorycznej wiedzy kandydatów na temat prawa i praktyk w dziedzinie ochrony danych.

Taka też idea przyświeca organizowanym studiom podyplomowym z zakresu Bezpieczeństwa i ochrony danych, które maja przygotować osoby pozyskane z obszaru jeleniogórskiego i przylegających obszarów do wykonywania funkcji z zakresu zarządzania bezpieczeństwem informacji oraz do podjęcia i pełnienia funkcji kierowniczych, menedżerskich w zakresie ochrony danych osobowych oraz zarządzania bezpieczeństwem informacji zgodnie z rozporządzeniem RODO.

Forma zakończenia studiów

Dla pozytywnego zakończenia studiów słuchacz musi mieć zaliczone na ocenę pozytywną wszystkie przedmioty. Z uzyskanych ocen wyznacza się ocenę podsumowującą będącą średnią z uzyskanych ocen. Warunkiem koniecznym jest również napisanie pracy dyplomowej pod kierunkiem jednego z wykładowców kursu. Praca po pozytywnym zaopiniowaniu przez promotora jest broniona przez słuchacza przed komisją w dwuosobowym składzie: kierownik kursu (lub wyznaczona przez niego osoba) i opiekun pracy. Do obrony pracy słuchacz jest dopuszczony pod warunkiem pozytywnego zaliczenia wszystkich przedmiotów objętych programem studiów. Po pozytywnej obronie słuchacz otrzymuje dyplom ukończenia studiów z ogólną ocena będącą średnią z obrony pracy i oceny podsumowującej. Na dyplomie umieszcza się listę przedmiotów realizowanych w ramach programu studiów.

Studia na kierunkach związanych z bezpieczeństwem nie podlegają standardom i nie dają certyfikatów. Studia kierowane są głównie do przyszłych inspektorów ochrony danych. Wymagany od inspektora poziom wiedzy nie jest jednoznacznie określony przez ustawodawcę.

W informacjach zawartych na stronie Urzędu ochrony danych osobowych stwierdzono: „Mimo, iż RODO bardzo mocno akcentuje wymóg wiedzy i fachowości IOD, nie reguluje zasad czy trybu weryfikacji spełnienia tego wymogu. Niemniej certyfikaty, dyplomy oraz inne dokumenty poświadczające wiedzę i doświadczenie inspektora niewątpliwie w większości przypadków będą ważnym kryterium kwalifikacyjnym i argumentem przemawiającym na korzyść osoby wyznaczanej do pełnienia tej funkcji.”

Wynika z tego, że dyplom ukończenia studiów podyplomowych w zakresie „Bezpieczeństwa i ochrony danych” będzie poświadczał wiedzę potrzebną do objęcia stanowiska inspektora ochrony danych ponieważ zakres tematyczny zawarty w programie studiów daje absolwentowi odpowiednią fachową wiedzę.

2. WYKAZ PRZEDMIOTÓW

Moduł I: Informatyka w ochronie danych

1. Zarządzanie informacją

Tematy zajęć:	1. Podstawowe definicje i klasyfikacje informacji. 2. Podstawy teorii informacji. 3. Systemy informacyjne w instytucji. 4. Kultura komunikacji i organizacji informacji. 5. Przetwarzanie i zarządzanie informacją. 6. Projektowanie i eksploatacja systemów informatycznych. 7. Zarządzanie zasobami informatycznymi. 8. Bezpieczeństwo informacji. 9. Nowe technologie informacyjne.
Metoda prowadzenia zajęć/ilość godzin:	Wykład – 15 godzin, Ćwiczenia – 15 godzin Praca samodzielna studenta – 30 godzin
Metoda zaliczenia:	Zaliczenie na ocenę
Efekty uczenia:	**K_W01 -** posiada wiedzę w zakresie zarządzania, bezpieczeństwa i prawnej ochrony informacji, ich miejscu w systemie nauk i relacjach do innych nauk, **K_U02 -** potrafi przygotowywać prace pisemne z uwzględnieniem terminologii właściwej dla nauk o bezpieczeństwie, posługując się odpowiednim aparatem analityczno – badawczym
ECTS	3
Odpowiedzialny:	Wykładowca WNHIS / dr inż. Tadeusz Lewandowski

2. Identyfikacja zagrożeń, ocena i zarządzanie ryzykiem

Tematy zajęć:	1. Ryzyko w sensie ogólnym i technicznym – podstawowe pojęcia. 2. Metody oceny ryzyka. 3. Identyfikacja zagrożeń. 4. Ryzyko i zarządzanie ryzykiem. 5. Ryzyko zawodowe, procesowe i środowiskowe. 6. Podstawowe zasady oceny ryzyka w bezpieczeństwie informatycznym. 7. Ćwiczenia rachunkowe: ryzyko obliczeniowe, diagramy częstości. 8. Ćwiczenia rachunkowe: metody PHA i HAZOP. 9. Ćwiczenia rachunkowe: drzewa błędów i drzewa zdarzeń.
Metoda prowadzenia zajęć/ilość godzin:	Wykład – 30 godzin, Ćwiczenia – 15 godzin Praca samodzielna studenta – 45 godzin
Metoda zaliczenia:	Zaliczenie na ocenę
Efekty uczenia:	**K_W06 -** ma wiedzę z zakresu identyfikacja zagrożeń, oceny i zarządzaniem ryzykiem bezpieczeństwa informacji, **K_U08** - potrafi zidentyfikować i ocenić zagrożenia bezpieczeństwa informacji, a także obliczyć za pomocą wybranej metody ryzyko wystąpienia zagrożenia; potrafi zarządzać ryzykiem,
ECTS	**3**
Odpowiedzialny:	dr inż. Tadeusz Lewandowski

3. Systemowe zarządzanie bezpieczeństwem informacji

Tematy zajęć:	1. Historia systemowego zarządzania bezpieczeństwem informacji, Składniki bezpieczeństwa informacji. Wymagania prawne dotyczące bezpieczeństwa informacji. 2. Korzyści z ochrony informacji. Korzyści biznesowe. Korzyści wewnętrzne. Korzyści zewnętrzne. Korzyści marketingowe. Korzyści dla klientów i innych stron trzecich. 3. Standardy dotyczące zarządzania bezpieczeństwem informacji. Polska edycja norm z zarządzania bezpieczeństwem informacji. Modelowy system zarządzania bezpieczeństwem informacji. 4. Odpowiedzialność, uprawnienia. Dokumentacja w systemie zarządzania bezpieczeństwem informacji. 5. Audyt systemu zarządzania bezpieczeństwem informacji. Cele audytu i zakresy odpowiedzialności. Etapy działań audytowych. **6.** Interpretacja wymagań normy ISO/IEC 27001:2005. Dokumentacja w systemie zarządzania bezpieczeństwem informacji. Odpowiedzialność kierownictw.
Metoda prowadzenia zajęć/ilość godzin:	Wykład – 15 godzin, Ćwiczenia – 15 godzin Praca samodzielna studenta – 30 godzin
Metoda zaliczenia:	Zaliczenie na ocenę
Efekty uczenia:	**K_W08 -** ma podstawową wiedzę z zakresu funkcjonowania systemów informacyjnych w administracji, przemyśle i instytucjach zarządzania kryzysowego, **K_U11** - potrafi wykorzystać i zastosować w działalności kierunkowej niezbędne metody i środki zapewniające ochronę i bezpieczeństwo informacji w ramach różnych rodzajów informacji,
ECTS	**2**
Odpowiedzialny:	mgr inż. Eugeniusz Gronostaj

Moduł II: Narzędzia informatyczne w ochronie danych

1. Przedmiot: Bezpieczeństwo systemów informatycznych

Tematy zajęć:	1. Podstawy systemów informatycznych. 2. Bezpieczeństwo systemów operacyjnych i aplikacji. 3. Kopie rezerwowe 4. Szyfrowanie danych 5. Usuwanie i odzyskiwanie danych (dysków i folderów) 6. Ochrona antywirusowa 7. Sieciowe systemy zaporowe 8. Bezpieczeństwo chmury obliczeniowej 9. Ochrona przed atakami socjotechnicznymi **10.** Ergonomiczne bezpieczeństwo użytkowników systemów informatycznych.
Metoda prowadzenia zajęć/ilość godzin:	Wykład – 15 godzin, Laboratorium 30 godzin Praca samodzielna studenta – 45 godzin
Metoda zaliczenia:	Zaliczenie na ocenę
Efekty uczenia:	**K_W03 –** posiada podstawową wiedzę z zakresu bezpieczeństwa systemów informatycznych oraz bezpieczeństwa elektronicznej komunikacji, **K_U04** – potrafi posłużyć się właściwie dobranym informatycznym oprogramowaniem narzędziowym i użytkowym do realizacji postawionego zadania,
ECTS	**3**
Odpowiedzialny:	dr inż. Jerzy Januszewicz

2. Przedmiot: Bezpieczeństwo elektronicznej komunikacji

Tematy zajęć:	1. Podstawy bezpieczeństwa i ochrony informacji 2. Podstawy kryptografii (algorytmy symetryczne i asymetryczne, funkcja skrótu, standardy szyfrowania) 3. Uwierzytelnianie dokumentów (podpis elektroniczny, infrastruktura klucza publicznego, certyfikaty) 4. Bezpieczne protokoły teleinformatyczne 5. Bezpieczeństwo sieci komputerowych 6. Bezpieczeństwo sieci bezprzewodowych 7. Bezpieczeństwo technologii mobilnych **8.** Technologia blockchain (kryptowaluty i inne)
Metoda prowadzenia zajęć/ilość godzin:	Wykład – 30 godzin, Laboratorium 30 godzin Praca w samodzielna studenta – 45 godzin
Metoda zaliczenia:	Zaliczenie na ocenę
Efekty uczenia:	**K_W03 -** posiada podstawową wiedzę z zakresu bezpieczeństwa systemów informatycznych oraz bezpieczeństwa elektronicznej komunikacji, **K_U04** - potrafi posłużyć się właściwie dobranym informatycznym oprogramowaniem narzędziowym i użytkowym do realizacji postawionego zadania,
ECTS	3
Odpowiedzialny:	dr inż. Jerzy Januszewicz

Moduł III: Ochrona informacji niejawnych i danych osobowych

1. Przedmiot: Ochrona danych osobowych

Tematy zajęć:	1. Akty prawne, zadania administratora i inspektora ochrony danych 2. Audyt RODO 3. Dokumentacja inspektora ochrony danych 4. Obowiązek informacyjny, klauzule informacyjne 5. Analiza ryzyka ogólnego i ocena skutków przetwarzania danych (DPIA) 6. Monitoring wizyjny 7. Praca zdalna 8. Kontrola przestrzegania przepisów o ochronie danych osobowych **9.** Krajowe Ramy Interoperacyjności (KRI), procedury KRI
Metoda prowadzenia zajęć/ilość godzin:	Wykład – 15 godzin, Praca samodzielna studenta – 15 godzin
Metoda zaliczenia:	Zaliczenie na ocenę
Efekty uczenia:	**K_W05 -** posiada wiedzę z zakresu zadań, aspektów działania oraz etyki Inspektora Ochrony Danych (IOD), **K_U07** - potrafi analizować i praktycznie wykorzystać wiedzę w zakresie ochrony danych osobowych i informacji niejawnych, **K_U10** - potrafi wykonywać podstawowe obowiązki na stanowiskach inspektora ochrony danych, specjalisty ds. ochrony informacji niejawnych lub innych stanowiskach związanych z bezpieczeństwem informacji, **K_K03** - ma świadomość ważności działalności specjalisty ds. bezpieczeństwa informacji, jej wpływu na środowisko oraz związanej z tym odpowiedzialności oraz konieczności permanentnego uwzględniania zagadnień z zakresu bezpieczeństwa w środowisku zawodowym,
ECTS	2
Odpowiedzialny:	mgr inż. Jerzy Szelinger

2. Przedmiot: Praktyczne aspekty działania Inspektora Ochrony Danych (IOD

Tematy zajęć:	1. Akty prawne, zadania administratora i inspektora ochrony danych 2. Audyt RODO 3. Dokumentacja inspektora ochrony danych 4. Obowiązek informacyjny, klauzule informacyjne 5. Analiza ryzyka ogólnego i ocena skutków przetwarzania danych (DPIA) 6. Monitoring wizyjny 7. Praca zdalna 8. Kontrola przestrzegania przepisów o ochronie danych osobowych **9.** Krajowe Ramy Interoperacyjności (KRI), procedury KRI
Metoda prowadzenia zajęć/ilość godzin:	Ćwiczenia - 15 godzin Praca samodzielna studenta – 15 godzin
Metoda zaliczenia:	Zaliczenie na ocenę
Efekty uczenia:	**K_W05 -** posiada wiedzę z zakresu zadań, aspektów działania oraz etyki Inspektora Ochrony Danych (IOD), **K_U07** - potrafi analizować i praktycznie wykorzystać wiedzę w zakresie ochrony danych osobowych i informacji niejawnych, **K_U10** - potrafi wykonywać podstawowe obowiązki na stanowiskach inspektora ochrony danych, specjalisty ds. ochrony informacji niejawnych lub innych stanowiskach związanych z bezpieczeństwem informacji, **K_K03** - ma świadomość ważności działalności specjalisty ds. bezpieczeństwa informacji, jej wpływu na środowisko oraz związanej z tym odpowiedzialności oraz konieczności permanentnego uwzględniania zagadnień z zakresu bezpieczeństwa w środowisku zawodowym,
ECTS	2
Odpowiedzialny:	mgr inż. Jerzy Szelinger

3. Przedmiot: Ochrona informacji niejawnych

Tematy zajęć:	1. System ochrony informacji niejawnych 2. Pion ochrony informacji niejawnych 3. Kancelaria tajna i inne kancelarie 4. Postępowanie sprawdzające 5. Bezpieczeństwo teleinformatyczne 6. Odpowiedzialność karna **7.** Bezpieczeństwo przemysłowe.
Metoda prowadzenia zajęć/ilość godzin:	Wykład – 15 godzin, Praca samodzielna studenta – 15 godzin
Metoda zaliczenia:	Zaliczenie na ocenę
Efekty uczenia:	**K_W04** ma wiedzę w zakresie ochrony informacji niejawnej, pionów ochrony informacji niejawnych w instytucji, w tym działalności kancelarii tajnej, **K_U07** - potrafi analizować i praktycznie wykorzystać wiedzę w zakresie ochrony danych osobowych i informacji niejawnych, **K_U10** - potrafi wykonywać podstawowe obowiązki na stanowiskach inspektora ochrony danych, specjalisty ds. ochrony informacji niejawnych lub innych stanowiskach związanych z bezpieczeństwem informacji, **K_K03** - ma świadomość ważności działalności specjalisty ds. bezpieczeństwa informacji, jej wpływu na środowisko oraz związanej z tym odpowiedzialności oraz konieczności permanentnego uwzględniania zagadnień z zakresu bezpieczeństwa w środowisku zawodowym,
ECTS	2
Odpowiedzialny:	dr inż. Janusz Boratyński

Moduł IV: Prawne i organizacyjne podstawy ochrony i bezpieczeństwa danych

1. Przedmiot: Prawna ochrona informacji

Tematy zajęć:	1) Znaczenie dostępu do informacji publicznej. 2) Prawne podstawy informowania jednostki. 3) Pojęcie sprawy publicznej, pojęcie informacji publicznej, pojęcie dostępu do informacji publicznej. Zasady udostępniania informacji publicznej. 4) Podmioty zobowiązane informacyjnie i podmioty uprawnione do uzyskania informacji. 5) Dopuszczalne formy udostępniania wiedzy publicznej w świetle uregulowań ogólnych – ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej. 6) BIP - jako forma bezwnioskowego upubliczniania informacji publicznej. 7) Ograniczenia udostępniania wiedzy publicznej (wynikające z UIDP oraz z przepisów szczególnych).
Metoda prowadzenia zajęć/ilość godzin:	Wykład – 15 godzin, Praca samodzielna studenta – 15 godzin
Metoda zaliczenia:	Zaliczenie na ocenę
Efekty uczenia:	**K_W01 -** posiada wiedzę w zakresie zarządzania, bezpieczeństwa i prawnej ochrony informacji, ich miejscu w systemie nauk i relacjach do innych nauk, **K_U03** - potrafi właściwie posługiwać się konkretnymi normami i regułami: prawnymi, zawodowymi i moralnymi w celu rozwiązania konkretnego zadania w zakresie bezpieczeństwa informatycznego,
ECTS	1
Odpowiedzialny:	dr Adam Banaszkiewicz

2. Przedmiot: Cyberprzestępczość i jej zwalczanie

Tematy zajęć:	1. Definicje podstawowych pojęć cyberprzestępczości. 2. Podstawowy podział i charakterystyka cyberprzestępczości 3. Problemy w zwalczaniu cyberprzestępczości 4. Tendencje i trendy w zagrożeniach bezpieczeństwa cyberprzestrzeni 5. Wydziały do walki z cyberprzestępczością 6. Zapobieganie przed cyberprzestępczością 7. Monitorowanie i zgłaszanie incydentów 8. Metody zabezpieczania dowodów cyberprzestępstwa 9. Odpowiedzialność karna za cyberprzestępstwa **10.** Analiza przykładowych cyberprzestępstw.
Metoda prowadzenia zajęć/ilość godzin:	Wykład – 15 godzin, Praca samodzielna studenta – 15 godzin
Metoda zaliczenia:	Zaliczenie na ocenę
Efekty uczenia:	**K_W07 -** zna problemy i metody zwalczania cyberprzestępczości, **K_U01** - potrafi prawidłowo interpretować zjawiska i zagrożenia cyberbezpieczeństwa w skali globalnej, państwowej, regionalnej i lokalnej,
ECTS	1
Odpowiedzialny:	Komenda Miejska Policji/dr inż. Jerzy Januszewicz

3. Przedmiot: Psychologiczne i socjotechniczne aspekty bezpieczeństwa informacji

Tematy zajęć:	1. Bezpieczeństwo jako pojęcie psychologiczne. 2. Czynnik ludzki w systemie bezpieczeństwa informacji 3. Operacje psychologiczne (kłamstwa i zniekształcenia, oszczerstwa, nękanie, reklamy, manipulowanie informacją. 4. Socjotechnika a bezpieczeństwo informacji. **5.** Cele ataku socjotechnicznego. Ataki socjotechniczne.
Metoda prowadzenia zajęć/ilość godzin:	Wykład – 15 godzin, Praca samodzielna studenta – 15 godzin
Metoda zaliczenia:	Zaliczenie na ocenę
Efekty uczenia:	**K_W08** - zna psychologiczno-komunikacyjne aspekty bezpieczeństwa informacji, **K_U09** - posiada umiejętność komunikowania się z otoczeniem, zbierania, hierarchizowania, przetwarzania i przekazywania informacji, **K_K04** - prawidłowo identyfikuje i rozstrzyga dylematy związane z wykonywaniem zawodu
ECTS	1
Odpowiedzialny:	Wykładowca WNHIS

4. Przedmiot: Polityka bezpieczeństwa cybernetycznego

Tematy zajęć:	1. Modele bezpieczeństwa 2. Przedmiot ochrony instytucji 3. Zagrożenia bezpieczeństwa instytucji 4. Organizacja realizacji polityki bezpieczeństwa w instytucji 5. Podział odpowiedzialności i uprawnień w zakresie bezpieczeństwa cybernetycznego 6. Aspekty ekonomiczne polityki bezpieczeństwa 7. Edukacja i szkolenia w zakresie polityki bezpieczeństwa 8. Projekt polityki bezpieczeństwa dla instytucji. **9.** Audyt polityki bezpieczeństwa
Metoda prowadzenia zajęć/ilość godzin:	Wykład – 15 godzin, Seminarium 15 godzin Praca samodzielna studenta – 30 godzin
Metoda zaliczenia:	Zaliczenie na ocenę
Efekty uczenia:	**K_W02 -** ma uporządkowaną wiedzę niezbędną do zrozumienia zagrożeń bezpieczeństwa cybernetycznego , ich identyfikacji, analizy i oceny, **K_U06** - posiada umiejętność przygotowania typowych dokumentów planistycznych zarządzania kryzysowego na szczeblu instytucji i lokalnej administracji (gmina, powiatu), w szczególności opracować politykę bezpieczeństwa informacji **K_U12 -** umie zorganizować i przeprowadzić szkolenie z wybranych zagadnień związanych z bezpieczeństwem informacji, potrafi w trakcie szkoleń kierować małym zespołem ludzkim w sytuacjach zagrożeń bezpieczeństwa informacji,
ECTS	3
Odpowiedzialny:	dr inż. Jerzy Januszewicz

Moduł V: Dyplomowy

1. Przedmiot: Seminarium dyplomowe

Tematy zajęć:	1. Pierwszy referat-prezentacja opisująca i wyjaśniająca założenia pracy dyplomowej, przewidywany zakres i sposób jej realizacji. Dyskusja pobudzająca do poszukiwania właściwych sposobów i form podejścia do propozycji realizacji pracy dyplomowej. **2.** Drugi referat- prezentacja aktualnych osiągnięć w realizacji pracy dyplomowej, wyników i wniosków wraz wyrobieniem umiejętności uzasadniania i obrony merytorycznej swoich racji
Metoda prowadzenia zajęć/ilość godzin:	Wykład – 15 godzin, Seminarium 15 godzin Praca samodzielna studenta –30 godzin
Metoda zaliczenia:	Zaliczenie na ocenę
Efekty uczenia:	**K_W10 -** ma podstawową wiedzę z zakresu technologii informatycznych wykorzystywanych w bezpieczeństwie informacji. **K_U05** - potrafi zastosować technologie informatyczne w realizacji zadań na rzecz bezpieczeństwa informatycznego, **K_K01** - systematycznie uzupełnia wiedzę i doskonali umiejętności w zakresie bezpieczeństwa rozumiejąc potrzebę uczenia się przez całe życie, **K_K02** - reprezentuje postawę kreatywną i otwartą na inicjatywy, ma świadomość współdziałania w grupie, zarówno jako szeregowy członek, jak i lider zespołu oraz określania zawodowych priorytetów i prowadzenia oraz uczestnictwa w dyskusjach
ECTS	2
Odpowiedzialny:	mgr inż. Eugeniusz Gronostaj

2. Przedmiot: Praca dyplomowa

Tematy zajęć:	Studenci w porozumieniu z wykładowcami wybierają tematy prac dyplomowych i realizują je samodzielnie pod kierunkiem wykładowcy
Metoda prowadzenia zajęć/ilość godzin:	Praca samodzielna studenta – 60 godzin
Metoda zaliczenia:	Obrona pracy dyplomowej
Efekty uczenia:	**K_U05** - potrafi zastosować technologie informatyczne w realizacji zadań na rzecz bezpieczeństwa informatycznego, **K_K01** - systematycznie uzupełnia wiedzę i doskonali umiejętności w zakresie bezpieczeństwa rozumiejąc potrzebę uczenia się przez całe życie,
ECTS	5
Odpowiedzialny:	Opiekunowie prac dyplomowych

3. EFEKTY KSZTAŁCENIA DLA KIERUNKU STUDIÓW PODYPLOMOWYCH

Nazwa kierunku studiów podyplomowych: Bezpieczeństwo i ochrona danych
Dziedziny naukowe: nauki społeczne/nauki ścisłe
Dyscypliny naukowe: nauki o bezpieczeństwie/informatyka

Symbol	Kierunkowe efekty kształcenia	Odniesienie do charakterystyki II stopnia dla kwalifikacji na poziomie 6. Polskiej Ramy Kwalifikacji (kod składnika opisu)
WIEDZA		
K_W01	posiada wiedzę w zakresie zarządzania, bezpieczeństwa i prawnej ochrony informacji, ich miejscu w systemie nauk i relacjach do innych nauk,	P6S_WK P6S_WG
K_W02	ma uporządkowaną wiedzę niezbędną do zrozumienia zagrożeń bezpieczeństwa cybernetycznego , ich identyfikacji, analizy i oceny,	P6S_WK P6S_WG
K_W03	posiada podstawową wiedzę z zakresu bezpieczeństwa systemów informatycznych oraz bezpieczeństwa elektronicznej komunikacji,	P6S_WK P6S_WG
K_W04	ma wiedzę w zakresie ochrony informacji niejawnej, pionów ochrony informacji niejawnych w instytucji, w tym działalności kancelarii tajnej,	P6S_WK P6S_WG
K_W05	posiada wiedzę z zakresu zadań, aspektów działania oraz etyki Inspektora Ochrony Danych (IOD),	P6S_WK P6S_WG
K_W06	ma wiedzę z zakresu identyfikacja zagrożeń, oceny i zarządzaniem ryzykiem bezpieczeństwa informacji,	P6S_WK P6S_WG
K_W07	zna problemy i metody zwalczania cyberprzestępczości,	P6S_WK P6S_WG
K_W08	ma podstawową wiedzę z zakresu funkcjonowania systemów informacyjnych w administracji, przemyśle i instytucjach zarządzania kryzysowego,	P6S_WK P6S_WG
K_W09	zna psychologiczno-komunikacyjne aspekty bezpieczeństwa informacji,	P6S_WK P6S_WG
K_W10	ma podstawową wiedzę z zakresu technologii informatycznych wykorzystywanych w bezpieczeństwie informacji.	P6S_WK P6S_WG

UMIEJĘTNOŚCI		
K_U01	potrafi prawidłowo interpretować zjawiska i zagrożenia cyberbezpieczeństwa w skali globalnej, państwowej, regionalnej i lokalnej,	P6S_UW P6S_UK P6S_UO P6S_UU
K_U02	potrafi przygotowywać prace pisemne z uwzględnieniem terminologii właściwej dla nauk o bezpieczeństwie, posługując się odpowiednim aparatem analityczno – badawczym,	P6S_UW P6S_UK P6S_UO P6S_UU
K_U03	potrafi właściwie posługiwać się konkretnymi normami i regułami: prawnymi, zawodowymi i moralnymi w celu rozwiązania konkretnego zadania w zakresie bezpieczeństwa informatycznego,	P6S_UW P6S_UK P6S_UO P6S_UU
K_U04	potrafi posłużyć się właściwie dobranym informatycznym oprogramowaniem narzędziowym i użytkowym do realizacji postawionego zadania,	P6S_UW P6S_UK P6S_UO P6S_UU
K_U05	potrafi zastosować technologie informatyczne w realizacji zadań na rzecz bezpieczeństwa informatycznego,	P6S_UW P6S_UK P6S_UO P6S_UU
K_U06	posiada umiejętność przygotowania typowych dokumentów planistycznych zarządzania kryzysowego na szczeblu instytucji i lokalnej administracji (gmina, powiatu), w szczególności opracować politykę bezpieczeństwa informacji,	P6S_UW P6S_UK P6S_UO P6S_UU
K_U07	potrafi analizować i praktycznie wykorzystać wiedzę w zakresie ochrony danych osobowych i informacji niejawnych,	P6S_UW P6S_UK P6S_UO P6S_UU
K_U08	potrafi zidentyfikować i ocenić zagrożenia bezpieczeństwa informacji, a także obliczyć za pomocą wybranej metody ryzyko wystąpienia zagrożenia; potrafi zarządzać ryzykiem,	P6S_UW P6S_UK P6S_UO P6S_UU
K_U09	posiada umiejętność komunikowania się z otoczeniem, zbierania, hierarchizowania, przetwarzania i przekazywania informacji,	P6S_UW P6S_UK P6S_UO P6S_UU
K_U10	potrafi wykonywać podstawowe obowiązki na stanowiskach inspektora ochrony danych, specjalisty ds. ochrony informacji niejawnych lub innych stanowiskach związanych z bezpieczeństwem informacji,	P6S_UW P6S_UK P6S_UO P6S_UU
K_U11	potrafi wykorzystać i zastosować w działalności kierunkowej niezbędne metody i środki zapewniające ochronę i bezpieczeństwo informacji w ramach różnych rodzajów informacji,	P6S_UW P6S_UK P6S_UO P6S_UU
K_U12	umie zorganizować i przeprowadzić szkolenie z wybranych zagadnień związanych z bezpieczeństwem informacji, potrafi w trakcie szkoleń kierować małym zespołem ludzkim w sytuacjach zagrożeń bezpieczeństwa informacji,	P6S_UW P6S_UK P6S_UO P6S_UU

	KOMPETENCJE SPOŁECZNE	
K_K01	systematycznie uzupełnia wiedzę i doskonali umiejętności w zakresie bezpieczeństwa rozumiejąc potrzebę uczenia się przez całe życie,	P6S_KK P6S_KO P6S_KR
K_K02	reprezentuje postawę kreatywną i otwartą na inicjatywy, ma świadomość współdziałania w grupie, zarówno jako szeregowy członek, jak i lider zespołu oraz określania zawodowych priorytetów i prowadzenia oraz uczestnictwa w dyskusjach,	P6S_KK P6S_KO P6S_KR
K_K03	ma świadomość ważności działalności specjalisty ds. bezpieczeństwa informacji, jej wpływu na środowisko oraz związanej z tym odpowiedzialności oraz konieczności permanentnego uwzględniania zagadnień **z** zakresu bezpieczeństwa w środowisku zawodowym,	P6S_KK P6S_KO P6S_KR
K_K04	prawidłowo identyfikuje i rozstrzyga dylematy związane z wykonywaniem zawodu	P6S_KK P6S_KO P6S_KR

4. PLAN STUDIÓW PODYPLOMOWYCH „BEZPIECZEŃSTWO I OCHRONA DANYCH”

Zał. nr 1: Plan studiów podyplomowych: **„Bezpieczeństwo i ochrona danych”**

REKTOR
dr n. med. Wioletta Pałczewska
prof. KPSW