Uchwała nr 13/2025
Senatu Akademii Nauk Stosowanych w Wałczu
z dnia 25.06.2025 r.

w sprawie wprowadzenia zmian w programie studiów podyplomowych Cyberbezpieczeństwo

Na podstawie § 30 pkt 10 Statutu Akademii Nauk Stosowanych w Wałczu stanowiącego załącznik do Uchwały nr 9/2023 Senatu ANS w Wałczu z dnia 31.05.2023 r., uchwala się, co następuje:

§ 1

Wprowadza się zmiany do program kształcenia na studiach podyplomowych na kierunku ***Cyberbezpieczeństwo*** w brzmieniu, jak w załączniku do niniejszej uchwały.

§ 2

Wykonanie uchwały powierza się Rektorowi ANS w Wałczu.

§ 3

Uchwała wchodzi w życie z dniem podjęcia.

Przewodniczący
Senatu ANS w Wałczu

/-/ dr Dariusz Skalski, prof. uczelni

Załącznik
do Uchwały nr 13/2025
Senatu ANS w Wałczu
z dnia 25.06.2025 r.

Akademia Nauk Stosowanych w Wałczu

Program Studiów Podyplomowych

CYBERBEZPIECZEŃSTWO
(forma hybrydowa)

Wałcz 2025 r.

SPIS TREŚCI

1. Koncepcja kształcenia

Wirtualna przestrzeń i bezpieczeństwo w cyberprzestrzeni to obecnie jeden z priorytetów w zakresie społecznego komunikowania. Rozwój Internetu pociąga za sobą zagrożenia, które wynikają z jego niewłaściwego zabezpieczenia i niepoprawnego korzystania z zasobów sieci.

Celem studiów jest przekazanie wiedzy i umiejętności w zakresie zarządzania cyberbezpieczeństwem w działalności gospodarczej oraz bezpiecznym funkcjonowaniu instytucji sektora publicznego. Absolwenci będą przygotowani do identyfikowania i przeciwdziałania zachowaniom zagrażającym bezpieczeństwu w sieci, w szczególności przestępczości internetowej oraz zdobędą umiejętności zwalczania różnych form cyberprzestępczości i reagowania na incydenty sieciowe.

Szczególny nacisk kładzie się na zarządzanie bezpieczeństwem operacyjnym oraz dostosowanie działań w obszarze zarządzania ryzykiem do zmieniających się zagrożeń w cyberprzestrzeni – zwłaszcza w kontekście nowej ustawy KSC2 (NIS2)
W ramach studiów omawiane są także standardy, aspekty prawne oraz aspekty techniczne
Zakres i tematyka kształcenia obejmuje wybrane zagadnienia z podstaw sieci informatycznych, podstaw bezpieczeństwa cybernetycznego, cyberprzestępczości, prawa, testów penetracyjnych oraz sztucznej inteligencji.
Studia mają charakter hybrydowy, przekrojowy, obejmujący szerokie spektrum zagadnień cyberbezpieczeństwa. Wszystkie zagadnienia nauczane są od podstaw. Studia rekomendowane są dla osób początkujących lub średnio zaawansowanych. Nie jest wymagana znajomość zagadnień technicznych związanych z bezpieczeństwem systemów informatycznych.

2. Obszary kształcenia, w zakresie których prowadzone będą studia podyplomowe:

Niniejsze studia podyplomowe, z uwagi na ich obszar zainteresowań, należy przyporządkować do dyscypliny wiodącej **informatyka techniczna i telekomunikacja** (dziedzina **nauk inżynieryjno-technicznych**) oraz uzupełniająco do dyscypliny nauki o bezpieczeństwie i do dyscypliny nauki prawne (dziedzina nauk społecznych).

Dziedzina	Dyscyplina	Udział procentowy
Dziedzina nauk inżynieryjno-technicznych	informatyka techniczna i telekomunikacja	***89%***
Dziedzina nauk społecznych	nauki o bezpieczeństwie	**11%**
Dziedzina nauk społecznych	nauki prawne	

3. Nazwa i opis kwalifikacji uzyskiwanych po ukończeniu studiów podyplomowych

Absolwenci uzyskują kwalifikacje cząstkowe na poziomie 6 PRK w zakresie przygotowania do realizacji zadań w strukturach: administracji samorządowej oraz państwowej, policji, straży granicznej, straży miejskiej, Wojska Polskiego, ABW, Państwowej Straży Pożarnej, służby więziennej, zespołów reagowania na incydenty komputerowe (CERT), jako specjaliści od cyberbezpieczeństwa. Warunkiem ukończenia studiów jest certyfikacja COMPTIA SECURITY +

4. Kwalifikacje cząstkowe do których odnoszą się kwalifikacje podyplomowe

Kwalifikacje podyplomowe opisywanych studiów uwzględniają ogólne charakterystyki efektów uczenia się dla kwalifikacji na poziomie 6 Polskiej Ramy Kwalifikacji w części właściwej dla charakterystyk drugiego stopnia Polskiej Ramy Kwalifikacji typowych dla kwalifikacji cząstkowych uzyskiwanych w ramach szkolnictwa wyższego po uzyskaniu kwalifikacji pełnej na poziomie 4 oraz ich rozwinięcie dla obszaru kształcenia w zakresie nauk społecznych i technicznych w ramach szkolnictwa wyższego.

5. Liczba semestrów i liczba punktów ECTS konieczna dla uzyskania kwalifikacji podyplomowych

Studia podyplomowe trwają trzy semestry. Do osiągnięcia efektów uczenia się niezbędne będzie uzyskanie 60 punktów ECTS.

6. Wskazanie dokumentu potwierdzającego kwalifikacje wydawanego absolwentom

Studia zakończą się uzyskaniem kwalifikacji z zakresu cyberbezpieczeństwa potwierdzone świadectwem ukończenia studiów podyplomowych.

7. Wskazanie związku studiów podyplomowych z misją i strategią Uczelni

Studia Podyplomowe *Cyberbezpieczeństwo* wpisują się w misję Uczelni ponieważ realizacja studiów wiąże się ze zwiększeniem atrakcyjności i skuteczności kształcenia oraz rozwój promocji i współpracy z otoczeniem. Studia nawiązują również do strategii Uczelni, którą jest tworzenie odpowiednich warunków do studiowania, pozwalających na sprawne zaspokajanie wszechstronnych aspiracji edukacyjnych regionu, przygotowanie absolwentów do zaistnienia na rynku pracy oraz uświadomienie potrzeby ciągłego dokształcania i doskonalenia zawodowego. Realizacja studiów wiąże się z dwoma spośród trzech celów strategicznych Uczelni: doskonalenie oferty edukacyjnej i jakości kształcenia oraz rozwijanie współpracy

z regionalnym otoczeniem społeczno-gospodarczym. Z jednej strony bowiem realizacja studiów zmierza do wzbogacenia i uelastycznienia oferty edukacyjnej Uczelni zgodnie z oczekiwaniami i aspiracjami społeczności regionu, z drugiej natomiast jest wyrazem poszerzania współpracy z regionalnym otoczeniem społeczno-gospodarczym. Ponadto, realizacja studiów, będących formą kształcenia ustawicznego, przyczynia się do budowania kapitału ludzkiego w regionie.

Studia podyplomowe, prowadzone w systemie niestacjonarnym, pozwolą na stworzenie dogodnych warunków dla studiowania zwłaszcza osób pracujących zawodowo poprzez elastyczną organizację studiów, realizując tym samym jedną z podstawowych założeń misji Akademii Nauk Stosowanych w Wałczu. Ponadto zakres tematyczny studiów podyplomowych *Cyberbezpieczeństwo* wpłynie na rozwój regionu wałeckiego, i województwa zachodniopomorskiego przez przygotowanie wysoko wykwalifikowanej kadry, specjalistów z zakresu cyberbezpieczeństwa.

8. Charakterystyka absolwenta, ze szczególnym uwzględnieniem wskazania nowych umiejętności niezbędnych na rynku pracy w systemie uczenia się przez całe życie

Absolwent Studiów Podyplomowych *Cyberbezpieczeństwo* zostanie wyposażony w interdyscyplinarną wiedzę i umiejętności związane z identyfikowaniem i zarządzaniem ryzykiem związanym z prowadzeniem działalności gospodarczej w odniesieniu do zagrożeń związanych z wykorzystaniem technologii IT oraz zarządzaniem ich bezpieczeństwem, analizy bezpieczeństwa firmy oraz instytucji.

Absolwent uzyska wiedzę i praktyczne umiejętności umożliwiające podjęcie pracy związanej z administracją i bezpieczeństwem systemów komputerowych, opracowywaniem polityk bezpieczeństwa, ich wdrażania, utrzymania oraz rozwoju. Pozna podstawy informatyki śledczej oraz najnowsze metody ataków i zagrożenia dla systemów informatycznych. Będzie potrafił przeciwdziałać ich rozprzestrzenianiu i skutkom. Będzie umiał poszukiwać, gromadzić i zabezpieczać materiał dowodowy. Absolwent pozna podstawy analizy kryminalnej, będzie potrafił analizować dane związane z wystąpieniem incydentu teleinformatycznego, wykrywać i identyfikować związki między nimi, określać przesłanki, wyciągać wnioski i oceniać ich wiarygodność. Będzie umiał sporządzić raport z przebiegu incydentu, jego faktycznych i prawdopodobnych skutków, podjętych działań oraz proponowanych działań zapobiegawczych na przyszłość. Pozna sposób postępowania w przypadku zgłaszania popełnienia przestępstwa organom ścigania oraz prawa pokrzywdzonego. Będzie potrafił współdziałać z organami przestrzegania prawa w zakresie rozpoznania i zwalczania cyberprzestępczości, jak również będzie przygotowany do prowadzenia szkoleń w zakresie bezpieczeństwa teleinformatycznego dla pracowników swojej firmy lub instytucji.

Uzyskane przez absolwenta wiedza i umiejętności pozwolą identyfikować i zarządzać ryzykiem związanym z prowadzeniem działalności gospodarczej w cyberprzestrzeni. Dotyczy to m.in. wiedzy dotyczącej metodyki budowania programu cyberbezpieczeństwa, aspektów prawych i konsekwencji biznesowych. Studenci o wykształceniu nie informatycznym

uzyskają również podstawową wiedzę o stosowanych technologiach i rozwiązaniach informatycznych.

9. Efekty uczenia się.

9.1. Formalne i merytoryczne przesłanki uwzględnione przy opracowaniu efektów uczenia się

Efekty uczenia się opracowano na bazie wybranych efektów na poziomie 6 PRK spośród uniwersalnej charakterystyki pierwszego stopnia PRK oraz charakterystyk drugiego stopnia PRK typowych dla kwalifikacji: uzyskiwanych w ramach szkolnictwa wyższego oraz o charakterze zawodowym.

9.2. Opis efektów uczenia się dla studiów podyplomowych

9.2.1. Odniesienie ogólnych efektów uczenia się dla cząstkowych kwalifikacji studiów podyplomowych do uniwersalnej charakterystyki pierwszego stopnia PRK

Absolwent studiów podyplomowych:

kategoria	Ogólne efekty studiów podyplomowych	Uniwersalne charakterystyki 6 poziomu PRK
zna i rozumie	PO6W *1.* Elementarne fakty i pojęcia oraz zależności między wybranymi zjawiskami w zakresie praktycznych zastosowań informatyki w ujęciu zarówno systemowym jak i indywidualny dla rozwiązywania typowych problemów, dla zagadnień cyberprzestępczości. *2.* Różnorodne, złożone uwarunkowania prowadzonej działalności w kontekście zagrożeń związanych z cyberprzestępczością oraz szeroko rozumianym bezpieczeństwem IT	P6U_W • elementarne fakty i pojęcia oraz zależności między wybranymi zjawiskami przyrodniczymi, społecznymi i w sferze wytworów ludzkiej myśli; • różnorodne, złożone uwarunkowania prowadzonej działalności
potrafi:	PO6U 1. Wykorzystywać nowe technologie IT oraz ich innowacyjność w rozwiązywaniu zadań o dużym stopniu złożoności i w nie w pełni przewidywalnych	P6U_U 1. innowacyjnie wykonywać zadania oraz rozwiązywać złożone i nietypowe problemy w zmiennych i nie w pełni przewidywalnych warunkach; 2. samodzielnie planować własne

kategoria	Ogólne efekty studiów podyplomowych	Uniwersalne charakterystyki 6 poziomu PRK
	warunkach. 2. Samodzielnie planować własne uczenie się przez całe życie i ukierunkowywać innych w tym zakresie. Wykorzystywać zdobytą wiedzę w trafnym doborze metod samokształcenia. 3. Komunikować się ze zróżnicowanymi kręgami odbiorców, odpowiednio uzasadniać stanowiska.	uczenie się przez całe życie; 3. komunikować się z otoczeniem, uzasadniać swoje stanowisko
jest gotów do:	PO6K 1. Przyjmowania odpowiedzialności związanej z uczestnictwem w różnych wspólnotach oraz respektowania zobowiązań wynikających z tego faktu. 2. Funkcjonowania w złożonych sytuacjach pod bezpośrednim nadzorem w zorganizowanych warunkach. 3. Oceniania swoich działań i przyjmowania odpowiedzialności za ich skutki.	P6U_K *1.* respektowania zobowiązań wynikających z przynależności do różnych wspólnot; *2.* działania i współdziałania pod bezpośrednim nadzorem w zorganizowanych warunkach; *3.* oceniania swoich działań i przyjmowania odpowiedzialności za bezpośrednie ich skutki

W macierzy ogólnych efektów uczenia się stosowano następujące oznaczenia - kody:
PO – ogólny efekt studiów podyplomowych,
P6U_ – uniwersalne charakterystyki PRK dla poziomu 6,
W – wiedza,
U – umiejętności,
K – kompetencje społeczne;

9.2.2. Macierz efektów uczenia się dla cząstkowych kwalifikacji studiów podyplomowych z odniesieniem do charakterystyk drugiego stopnia PRK typowych dla kwalifikacji: uzyskiwanych w ramach szkolnictwa wyższego (oraz o charakterze zawodowym – jeśli dotyczy)

KODY EFEKTÓW STUDIÓW PODYPLOMOWYCH	TREŚĆ EFEKTÓW STUDIÓW PODYPLOMOWYCH	KODY CHARAKTERYSTYKI DRUGIEGO STOPNIA PRK TYPOWYCH DLA KWALIFIKACJI O CHARAKTERZE ZAWODOWYM – POZIOM 6	KODY CHARAKTERYSTYKI DRUGIEGO STOPNIA TYPOWEJ DLA KWALIFIKACJI UZYSKIWANYCH W RAMACH SZKOLNICTWA WYŻSZEGO Z ROZWINIĘCIEM DLA POSZCZEGÓLNYCH OBSZARÓW KSZTAŁCENIA– POZIOM 6, PROFILU PRAKTYCZNEGO
SP_W01	W zaawansowanym stopniu zna i rozumie zagadnienia dotyczące bezpieczeństwa sieci i systemów teleinformatycznych,	*P6Z_WT*	*P6S_WG* *P6S_WG_T01*
SP_W02	Ma pogłębioną wiedzę na temat podstawowych występujących zagrożeń bezpieczeństwa teleinformatycznego, wymagania w tym zakresie oraz wybrane techniki ochrony sieci i systemów;		*P6S_WG* *P6S_WG_T01*
SP_W03	W zaawansowanym stopniu Zna i rozumie trendy rozwojowe i najistotniejsze nowe osiągnięciach w wybranych zagadnieniach informatyki i telekomunikacji z uwzględnieniem ich bezpieczeństwa;	*P6Z_WO*	*P6S_WG* *P6S_WG_T01*
SP_W04	W zaawansowanym stopniu Rozumie rolę sieci Internet we współczesnym świecie, zagadnienia związków technologii informacyjnych ze światowym rynkiem ekonomicznym oraz wybrane kwestie prywatności i dostępności informacji, również w aspekcie mediów społecznościowych oraz rozwoju Internetu rzeczy (Internet of Things).	*P6Z_WT*	*P6S_WK* *P6S_WG_S02*
SP_W05	W zaawansowanym stopniu zna i rozumie wybrane aspekty prawne cyberbezpieczeństwa oraz ma wiedzę niezbędną do rozumienia społecznych, ekonomicznych, prawnych i innych pozatechnicznych uwarunkowań bezpieczeństwa teleinformatycznego oraz ich uwzględniania w praktyce zawodowej.	*P6Z_WT*	*P6S_WK* *P6S_WG_S01*
	UMIEJĘTNOŚCI		
SP_U01	Potrafi przygotować projekt wybranej sieci teleinformatycznej biorąc pod uwagę konieczność łączenia różnych technik, aspekty	*P6Z_UO*	*P6S_UW* *P6S_UW_T03* *P6S_UW_T04*

KODY EFEKTÓW STUDIÓW PODYPLOMOWYCH	TREŚĆ EFEKTÓW STUDIÓW PODYPLOMOWYCH	KODY CHARAKTERYSTYKI DRUGIEGO STOPNIA PRK TYPOWYCH DLA KWALIFIKACJI O CHARAKTERZE ZAWODOWYM – POZIOM 6	KODY CHARAKTERYSTYKI DRUGIEGO STOPNIA TYPOWEJ DLA KWALIFIKACJI UZYSKIWANYCH W RAMACH SZKOLNICTWA WYŻSZEGO Z ROZWINIĘCIEM DLA POSZCZEGÓLNYCH OBSZARÓW KSZTAŁCENIA– POZIOM 6, PROFILU PRAKTYCZNEGO
	bezpieczeństwa i jakości świadczonych w niej usług.		
SP_U02	Potrafi opracować szczegółową dokumentację wyników realizacji eksperymentu, zadania projektowego lub badawczego; potrafi przygotować opracowanie zawierające omówienie tych wyników.	*P6Z_UO*	*P6S_UW_T04*
SP_U03	Potrafi zaprojektować, uruchomić i przetestować usługę bezpieczeństwa w sieci teleinformatycznej.	*P6Z_UO*	*P6S_UW* *P6S_UW_T01* *P6S_UW_T04*
SP_U04	Potrafi dobrać odpowiedni poziom bezpieczeństwa w celu zapewnienia ochrony przed zagrożeniami oraz zweryfikować ich skuteczność.	*P6Z_UN*	*P6S_UW* *P6S_UW_T01* *P6S_UW_T03* *P6S_UW_T05* *P6S_UW_S03*
SP_U05	Potrafi ocenić przydatność, innowacyjność i możliwość wykorzystania nowych narzędzi i osiągnięć w zakresie sieci teleinformatycznych – ich architektur, protokołów komunikacyjnych, świadczonych usług oraz poziomu bezpieczeństwa.	*P6Z_UI*	*P6S_UW* *P6S_UW_T02* *P6S_UW_T05*
SP_U06	Potrafi pozyskiwać informacje z literatury, baz danych i innych źródeł; potrafi integrować uzyskane informacje, dokonywać ich interpretacji i krytycznej oceny, a także wyciągać wnioski oraz formułować i wyczerpująco uzasadniać opinie.	*P6Z_UI*	*P6S_UW, P6S_UU* *P6S_UW_T03* *P6S_UW_T06*
SP_U07	Jest zorientowany we współczesnych rozwiązaniach bezpieczeństwa i może ocenić ich przydatność oraz wybrać rozwiązanie adekwatne do konkretnej sieci lub systemu	*P6Z_UI, P6Z_UN*	*P6S_UW* *P6S_UW_T06*
SP_U08	Potrafi pracować indywidualnie i w zespole, a także komunikować się i wymieniać informacje przy użyciu technik teleinformatycznych;	*P6Z_UO*	*P6S_UO, P6S_UK*
	KOMPETENCJE		

KODY EFEKTÓW STUDIÓW PODYPLOMOWYCH	TREŚĆ EFEKTÓW STUDIÓW PODYPLOMOWYCH	KODY CHARAKTERYSTYKI DRUGIEGO STOPNIA PRK TYPOWYCH DLA KWALIFIKACJI O CHARAKTERZE ZAWODOWYM – POZIOM 6	KODY CHARAKTERYSTYKI DRUGIEGO STOPNIA TYPOWEJ DLA KWALIFIKACJI UZYSKIWANYCH W RAMACH SZKOLNICTWA WYŻSZEGO Z ROZWINIĘCIEM DLA POSZCZEGÓLNYCH OBSZARÓW KSZTAŁCENIA– POZIOM 6, PROFILU PRAKTYCZNEGO
SP_K01	Potrafi pracować w grupie realizującej wspólny projekt; zna zasady komunikacji, pracy grupowej i role w grupie, również rolę lidera; potrafi wykonywać zadania w oczekiwanym zakresie, czasie i uzgodnionej jakości;	*P6Z_KW*	*P6S_KR*
SP_K02	Jest gotów do przestrzegania zasad obowiązujących w dziedzinie cyberbezpieczeństwa, dotyczących utrzymywania jakości prowadzonej działalności oraz kultury współpracy i kultury konkurencji oraz inicjowania działania na rzecz interesu publicznego myślenia i działania w sposób przedsiębiorczy	*P6Z_KP*	*P6S_KO*
SP_K03	Jest gotów do odpowiedzialnego pełnienia ról zawodowych, w tym: przestrzegania zasad etyki zawodowej i wymagania tego od innych oraz promowania zasad etycznych w dziedzinie cyberbezpieczeństwa	*P6Z_KO*	*P6S_KR*
SP_K04	Jest gotów do podejmowania decyzji w sytuacjach trudnych oraz krytycznej oceny posiadanej wiedzy uznawania znaczenia wiedzy w rozwiązywaniu problemów poznawczych i praktycznych	*P6Z_KO*	*P6S_KK*

W macierzy efektów uczenia się stosowano następujące oznaczenia - kody:

1) dla efektu studiów podyplomowych

P (pierwsza litera kodu) - efekty uczenia się studiów podyplomowych
W - kategoria wiedzy
U - kategoria umiejętności
K (druga litera kodu) - kategoria kompetencji społecznych
01, 02, 03 i kolejne - numer efektu uczenia się

2) dla oznaczeń charakterystyki poziomów PRK uzyskiwanych w ramach kształcenia i szkolenia zawodowego (drugiego stopnia)

P - poziom PRK (1-8)

Z - charakterystyka typowa dla kwalifikacji uzyskiwanych w ramach kształcenia i szkolenia zawodowego
W -wiedza:
T- teorie i zasady
Z – zjawiska i procesy
O – organizacja pracy
N – narzędzia i materiały
U – umiejętność
I - informacje
O - organizacja pracy
N – narzędzia i materiały
U - uczenie się i rozwój zawodowy
K – Kompetencje społeczne
P – przestrzeganie reguł
W – współpraca
O – odpowiedzialność

3) dla oznaczeń charakterystyki poziomów PRK uzyskiwanych w ramach szkolnictwa wyższego (drugiego stopnia) – część główna:
P - poziom PRK (6-8)
S - charakterystyka typowa dla kwalifikacji uzyskiwanych w ramach szkolnictwa wyższego
W -wiedza:
G- głębia i zakres
K- kontekst
U – umiejętność
W – wykorzystanie wiedzy
K – komunikowanie się
O - organizacja pracy
U – uczenie się
K – Kompetencje społeczne
K – krytyczna ocena
O – odpowiedzialność
R – rola zawodowa

4) dla oznaczeń charakterystyki poziomów PRK uzyskiwanych w ramach szkolnictwa wyższego (drugiego stopnia) z rozwinięciem dla poszczególnych obszarów kształcenia– poziom 6, profilu praktycznego:
P - poziom PRK (6-8)
S - charakterystyka typowa dla kwalifikacji uzyskiwanych w ramach szkolnictwa wyższego
W -wiedza:
G- głębia i zakres
K- kontekst
U – umiejętność
W – wykorzystanie wiedzy
K – komunikowanie się
O – organizacja pracy
U – uczenie się
K – Kompetencje społeczne
K – krytyczna ocena

O – odpowiedzialność
R – rola zawodowa

Obszary:
S – nauk społecznych
H – nauk humanistycznych
T – nauk technicznych
M – nauk medycznych i nauk o zdrowiu oraz nauk o kulturze fizycznej

Profile:
P – profilu praktycznego
A – profilu ogólnoakademickiego

01, 02, 03 i kolejne - numer efektu w kolejności umieszczenia w tabelach w rozporządzeniu MNiSW z dnia 26 września 2016 r. w sprawie charakterystyk drugiego stopnia PRK typowych dla kwalifikacji uzyskiwanych w ramach szkolnictwa wyższego po uzyskaniu kwalifikacji pełnej na poziomie 4 – poziomy 6-8;

10. Opis formalnych warunków wstępnych

Warunkiem przyjęcia na studia podyplomowe jest ukończenie studiów wyższych:
1) pierwszego stopnia, poświadczonych dyplomem uczelni wyższej oraz tytułem zawodowym licencjata lub
2) drugiego stopnia, poświadczonych dyplomem uczelni wyższej oraz tytułem zawodowym magistra lub
3) jednolitych studiów magisterskich, poświadczonych dyplomem uczelni wyższej oraz tytułem zawodowym magistra.

11. Opis ogólny przedmiotów/przedmiotów

Poniżej zaprezentowana jest lista przedmiotów, wchodzących w skład planu studiów podyplomowych *Cyberbezpieczeństwo* ze szczegółowym wskazaniem liczby godzin, formy zajęć oraz przewidywanych punktów ECTS za każdy przedmiot.

L.p.	Semestr	Przedmiot / Przedmiot	Forma zajęć		Razem godz.	Forma zaliczenia	Liczba punktów ECTS
			Wykład	Ćwiczenia		b/z/e	
1.	1/3	BEZPIECZEŃSTWO APLIKACJI WEB	10	10	20	Z	4
2.	1/3	AI W CYBERBEZPIECZEŃSTWIE	10	10	20	Z	4
3.	2/3	OSINT	10	10	20	Z	4
4.	3/3	BEZPIECZEŃSTWO ŚRODOWISKA WINDOWS	10	10	20	Z	4

5.	3/3	POWERSHELL W CYBERBEZPIECZEŃSTWIE	10	5	15	Z	4
6.	2/3	METODOLOGIA PENTESTÓW OWASP I OSSTMM	10	10	20	Z	4
7.	3/3	ANALIZA PAKIETÓW	10	5	15	Z	4
8.	1/3	WSTĘP DO PROGRAMOWANIA W PYTHON	10	20	30	Z	4
9.	3/3	PROGRAMOWANIE NARZĘDZIA CYBER W PYTHON	10	10	20	Z	4
10.	3/3	ANALIZA POWŁAMANIOWA - INFORMATYKA ŚLEDCZA	10	10	20	Z	4
11.	1/3	WPROWADZENIE DO CYBERBEZPIECZEŃSTWA	5	10	15	Z	3
12.	1/3	SOCJOTECHNIKI I FIZYCZNE NARZĘDZIA PENTESTERSKIE	5	10	15	Z	3
13.	2/3	BEZPIECZEŃSTWO SIECI KOMPUTEROWYCH	10	20	30	Z	4
14.	2/3	PRAWO A DZIAŁANIA W CYBER	5	10	15	Z	3
15.	2/3	CYBERPRZESTĘCZOŚĆ	5	10	15	Z	3
16.	3/3	CERTYFIKACJA – COMPTIA SECURITY +	-	3	3	E	4
		Razem	**130**	**163**	**293**		**60**

Tab. 1. Realizowane przedmioty w podziale na liczbę godzin, rodzaj realizowanych zajęć i liczbę punktów ECTS

12. Sposoby weryfikacji zakładanych efektów uczenia się, osiąganych przez słuchacza studiów podyplomowych

Podstawową formą weryfikacji i ewaluacji w ramach przedmiotów jest PRZEDMIOTOWE ZALICZENIE NA OCENĘ (Z) - jedno dla wszystkich komponentów przedmiotu razem – w formie projektu – samodzielnego/grupowego opracowania pisemnego wybranych zagadnień w zakresie niezbędnym do weryfikacji przedmiotowych efektów uczenia się wiedzy, umiejętności oraz kompetencji.

Potwierdzeniem finalnej ewaluacji jest certyfikacja – COMPTIA SECURITY +

Zalecana forma opracowania zamieszczona jest poniżej.

Studia podyplomowe
CYBERBEZPIECZEŃSTWO

KARTA EWALUACJI PROJEKTU

Rok akademicki/semestr: _____
Przedmiot: _____
Prowadzący przedmiot:
Wykonawcy (nazwisko, imię):

Tytuł projektu:

Kod efektów: / Nazwisko imię wykonawcy	SPW01						Ocena za projekt

Podpis prowadzącego

Studia podyplomowe
CYBERBEZPIECZEŃSTWO

OPRACOWANIE PROJEKTU

Cel opracowania:

_____

_____

_____

Spis treści:
Wstęp:
1
1.1.
1.2.
……
Zakończenie.

(od nowej strony)
WSTĘP (wielkie litery, pogrubione, 14 pkt.)
Tekst wstępu *(zwykły tekst 12 pkt., akapity blokowo, bez wcięcia, po akapicie odstęp 6 pkt.)*

1. **TYTUŁ USTĘPU***(wielkimi literami, 14 pkt. pogrubiony, odstęp od poprzedniego 18 pkt. odstęp poniżej 12 pkt.)*
2. **TYTUŁ PUNKTU ……** *(wielkimi literami 12 pkt, odstęp od poprzedniego 18 pkt., odstęp poniżej 12 pkt.)*
   Tekst punktu *(zwykły tekst 12 pkt., akapity blokowo, bez wcięcia, po akapicie odstęp 6 pkt.)*

Dla przedmiotów, w ramach których osiągane są wyłącznie efekty wiedzy, dopuszcza się sprawdzian sumujący (pisemny lub ustny), do których dołącza się zbiorcze potwierdzenie weryfikacji. Zalecana forma potwierdzenia weryfikacji znajduje się poniżej.

Akademia Nauk Stosowanych w Wałczu

POTWIERDZENIE WERYFIKACJI KOŃCOWEJ OSIĄGANIA EFEKTÓW KSZTAŁCENIA

STUDIA PODYPLOMOWE		**CYBERBEZPIECZEŃSTWO**	
Nazwa przedmiotu		**Rok akademicki/semestr**	
Komponent	**WYKŁAD**	**Forma weryfikacji i ewaluacji przedmiotowych efektów kształcenia**	**SPRAWDZIAN SUMUJACY**

Lp	**Imię nazwisko słuchacza**	**EFEKT PRZEDMIOTOWY ZGODNIE Z PODANYMI W SYLABUSIE**
		EP_W01
1.		
2.		
3.		
4.		
5.		

(podpis oceniającego)

Dokumentacja dotycząca ewaluacji weryfikacji efektów uczenia się nabywanych przez słuchaczy w toku studiów podyplomowych, na którą składają się protokoły zaliczeń, wykazy weryfikacji końcowych osiągania efektów oraz ocenione prace zaliczeniowe (projekty lub sprawdziany), jest gromadzona, a po zakończeniu procesu kształcenia danego przedmiotu, przekazywana Uczelni, celem archiwizacji.

13. Opis założeń i wytycznych do weryfikacji końcowej, jeżeli są przewidziane programem, lub sposobu weryfikacji końcowej

Warunkiem ukończenia studiów podyplomowych *Cyberbezpieczeństwo* jest zaliczenie wszystkich przedmiotów z programu studiów oraz uzyskanie oceny pozytywnej z egzaminu końcowego. Do egzaminu końcowego dopuszczone są osoby posiadające zaliczenia ze wszystkich przedmiotów objętych programem studiów podyplomowych.

Egzamin końcowy jest egzaminem ustnym i komisyjnym, obejmującym wskazane w programie studiów podyplomowych.

W czasie egzaminu słuchacz odpowiada na dwa wylosowane pytania z zakresu przygotowanych zadań. Z wyników egzaminu sporządza się protokół. W protokole umieszcza się oceny składające się na wynik końcowy oraz ocenę wyniku końcowego studiów.
Na ocenę wyniku końcowego studiów podyplomowych składają się :

1) z wagą 0,6: średnia ważona ocen uzyskanych z egzaminów i zaliczeń oraz przypisanych danym przedmiotom punktów ECTS;
2) ocena egzaminu certyfikującego z wagą 0,4, przy czym zaliczony egzamin oznacza ocenę 5

Na świadectwie ukończenia studiów podyplomowych wpisuje się ostateczny wynik studiów podyplomowych, wyrównany do pełnej oceny według zasady:

od 3,00 do 3,24 – dostateczny,
od 3,25 do 3,74 – dostateczny plus,
od 3,75 do 4,23 – dobry,
od 4,24 do 4,49 – dobry plus,
od 4,50 do 5,00 – bardzo dobry.

14. Opis zapewniania jakości kształcenia

System Zapewnienia Jakości Kształcenia obejmuje: przegląd i doskonalenie programu kształcenia; analizę trybu rekrutacji na studia; analizę realizacji procesu kształcenia; procedury weryfikacji osiągniętych efektów uczenia się ; dbanie o wysoki poziom kadry dydaktycznej. Zamierzenia dotyczące efektów uczenia się kontrolowane są przede wszystkim poprzez **ankietowanie** słuchaczy, celem uzyskania opinii na temat realizacji programu studiów.

15. ZAŁĄCZNIKI:

15.1. Załącznik 1. Matryca osiągania efektów uczenia się studiów podyplomowych w podziale na przedmioty (przedmioty) zajęć

2018	Numery modułów i przedmiotów zgodnie z planem studiów	Cyb.01.1	Cyb.01.2	Cyb.02.1	Cyb.02.2	Cyb.03.1	Cyb.03.2	Cyb.04.1	Cyb.04.2	Cyb.05.1	Cyb.05.2	Cyb.06.1	Cyb.06.2
Symbol modułowych efektów kształcenia	Efekty kierunkowe	Podstawy sieci	Podstawy sieci	Cyberprzestępczość	Cyberprzestępczość	Podstawy bezpieczeństwa cybernetycznego	Podstawy bezpieczeństwa cybernetycznego	Prawo a działania cybernetyczne	Prawo a działania cybernetyczne	Narzędzia sieciowe	Narzędzia sieciowe	Wstęp do metodyk OSSTMM	Wstęp do metodyk OSSTMM
	ECTS:	5	5	5	5	5	5	5	5	5	5	5	5
	formy zajęć:	wykład	ćwiczenia	wykład	ćwiczenia	wykład	ćwiczenia	wykład	ćwiczenia	wykład	ćwiczenia	wykład	ćwiczenia
	WIEDZA												
SP_W01	Zna i rozumie zagadnienia dotyczące bezpieczeństwa sieci i systemów teleinformatycznych,	x	x	x	x	x	x			x	x	x	x
SP_W02	Ma wiedzę na temat podstawowych występujących zagrożeń bezpieczeństwa teleinformatycznego, wymagania w tym zakresie oraz wybrane techniki ochrony sieci i systemów;			x	x	x	x					x	x
SP_W03	Zna i rozumie trendy rozwojowe i najistotniejsze nowe osiągnięciach w zakresie informatyki i telekomunikacji z uwzględnieniem ich bezpieczeństwa;	x	x							x	x	x	x
SP_W04	Rozumie rolę sieci Internet we współczesnym swiecie, zagadnienia związków technologii informacyjnych ze światowym rynkiem ekonomicznym oraz kwestie prywatności i dostępności informacji, również w aspekcie mediów społecznościowych oraz rozwoju Internetu rzeczy (Internet of Things).	x	x	x	x	x	x			x	x		
SP_W05	Zna i rozumie aspekty prawne cyberbezpieczeństwa oraz ma wiedzę niezbędną do rozumienia społecznych, ekonomicznych, prawnych i innych pozatechnicznych uwarunkowań bezpieczeństwa teleinformatycznego oraz ich uwzględniania w praktyce zawodowej.							x	x				
	UMIEJĘTNOŚCI												
SP_U01	Potrafi przygotować projekt wybranej sieci teleinformatycznej biorąc pod uwagę konieczność łączenia różnych technik, aspekty bezpieczeństwa i jakości świadczonych w niej usług.	x	x										
SP_U02	Potrafi opracować szczegółową dokumentację wyników realizacji eksperymentu, zadania projektowego lub badawczego; potrafi przygotować opracowanie zawierające omówienie tych wyników.	x	x					x	x				
SP_U03	Potrafi zaprojektować, uruchomić i przetestować usługę bezpieczeństwa w sieci teleinformatycznej.									x	x	x	x
SP_U04	Potrafi dobrać odpowiedni poziom bezpieczeństwa w celu zapewnienia ochrony przed zagrożeniami oraz zweryfikować ich skuteczność.			x	x	x	x			x	x		
SP_U05	Potrafi ocenić przydatność, innowacyjność i możliwość wykorzystania nowych narzędzi i osiągnięć w zakresie sieci teleinformatycznych – ich architektur, protokołów komunikacyjnych, świadczonych usług oraz poziomu bezpieczeństwa.	x	x									x	x
SP_U06	Potrafi pozyskiwać informacje z literatury, baz danych i innych źródeł; potrafi integrować uzyskane informacje, dokonywać ich interpretacji i krytycznej oceny, a także wyciągać wnioski oraz formułować i wyczerpująco uzasadniać opinie.							x	x				
	KOMPETENCJE												
SP_K01	Potrafi pracować w grupie realizującej wspólny projekt; zna zasady komunikacji, pracy grupowej i role w grupie, również rolę lidera; potrafi wykonywać zadania w oczekiwanym zakresie, czasie i uzgodnionej jakości;	x	x					x	x	x	x	x	x
SP_K02	Jest zorientowany we współczesnych rozwiązaniach bezpieczeństwa i może ocenić ich przydatność oraz wybrać rozwiązanie adekwatne do konkretnej sieci lub systemu			x	x	x	x	x	x				
SP_K03	Potrafi pracować indywidualnie i w zespole, a także komunikować się i wymieniać informacje przy użyciu technik teleinformatycznych;									x	x		

15.2. Załącznik 2: plan studiów podyplomowych Cyberbezpieczeństwo

L.p.	Semestr	Przedmiot / Przedmiot	Forma zajęć		Razem godz.	Forma zaliczenia	Liczba punktów ECTS
			Wykład	Ćwiczenia		b/z/e	
1.	1/3	BEZPIECZEŃSTWO APLIKACJI WEB	10	10	20	Z	4
2.	1/3	AI W CYBERBEZPIECZEŃSTWIE	10	10	20	Z	4
3.	2/3	OSINT	10	10	20	Z	4
4.	3/3	BEZPIECZEŃSTWO ŚRODOWISKA WINDOWS	10	10	20	Z	4
5.	3/3	POWERSHELL W CYBERBEZPIECZEŃSTWIE	10	5	15	Z	4
6.	2/3	METODOLOGIA PENTESTÓW OWASP I OSSTMM	10	10	20	Z	4
7.	3/3	ANALIZA PAKIETÓW	10	5	15	Z	4
8.	1/3	WSTĘP DO PROGRAMOWANIA W PYTHON	10	20	30	Z	4
9.	3/3	PROGRAMOWANIE NARZĘDZIA CYBER W PYTHON	10	10	20	Z	4
10.	3/3	ANALIZA POWŁAMANIOWA - INFORMATYKA ŚLEDCZA	10	10	20	Z	4
11.	1/3	WPROWADZENIE DO CYBERBEZPIECZEŃSTWA	5	10	15	Z	3
12.	1/3	SOCJOTECHNIKI I FIZYCZNE NARZĘDZIA PENTESTERSKIE	5	10	15	Z	3
13.	2/3	BEZPIECZEŃSTWO SIECI KOMPUTEROWYCH	10	20	30	Z	4
14.	2/3	PRAWO A DZIAŁANIA W CYBER	5	10	15	Z	3
15.	2/3	CYBERPRZESTĘCZOŚĆ	5	10	15	Z	3
16.	3/3	CERTYFIKACJA – COMPTIA SECURITY +	-	3	3	E	4
		Razem	**130**	**163**	**293**		**60**

15.3. Załącznik 3: założenia dla sylabusów przedmiotów

1. BEZPIECZEŃSTWO APLIKACJI WEB

Nazwa przedmiotu: Bezpieczeństwo aplikacji web
Nazwa jednostki prowadzącej przedmiot: Akademia Nauk Stosowanych w Wałczu
Nazwa studiów podyplomowych: Cyberbezpieczeństwo
Specjalność: praktyczna
Forma studiów: podyplomowe
Rok studiów: I
Semestr: I
Język wykładowy przedmiotu: polski
Koordynator przedmiotu: [do uzupełnienia]
Prowadzący zajęcia: [do uzupełnienia]

Forma zajęć: Wykład 10h, Laboratoria 10h

Cel przedmiotu
Zapoznać słuchaczy z:

- Identyfikacją i analizą zagrożeń bezpieczeństwa aplikacji webowych
- Metodami testowania i oceny bezpieczeństwa aplikacji
- Implementacją mechanizmów ochrony aplikacji webowych
- Wykorzystaniem narzędzi do automatycznego testowania bezpieczeństwa
- Najlepszymi praktykami secure coding

EFEKTY UCZENIA SIĘ
Wiedza

- SP_W01 Zna i rozumie zagadnienia dotyczące bezpieczeństwa aplikacji webowych
- SP_W02 Ma wiedzę na temat podstawowych zagrożeń bezpieczeństwa aplikacji web oraz techniki ochrony
- SP_W03 Zna najlepsze praktyki secure coding i standardy OWASP

Umiejętności

- SP_U01 Potrafi zidentyfikować i przeanalizować zagrożenia bezpieczeństwa aplikacji webowych
- SP_U02 Potrafi przeprowadzić testy bezpieczeństwa aplikacji przy użyciu specjalistycznych narzędzi
- SP_U03 Potrafi implementować mechanizmy ochrony w aplikacjach webowych

Kompetencje

- SP_K01 Potrafi pracować w grupie realizującej wspólny projekt bezpieczeństwa aplikacji
- SP_K02 Ma świadomość odpowiedzialności za bezpieczeństwo tworzonego oprogramowania

TREŚCI PROGRAMOWE i LICZBA GODZIN

1. Wprowadzenie do bezpieczeństwa aplikacji webowych - 3 godziny
2. OWASP Top 10 - analiza najczęstszych podatności - 4 godziny
3. Testowanie bezpieczeństwa aplikacji - narzędzia i metody - 4 godziny
4. Implementacja zabezpieczeń w aplikacjach webowych - 3 godziny
5. Bezpieczne kodowanie - best practices - 3 godziny
6. Monitoring i reagowanie na incydenty - 3 godziny

Metody kształcenia
Wykład kursowy z prezentacją, ćwiczenia polegające na wykonywaniu laboratoriów zgodnie ze wskazówkami wykładowcy. Forma hybrydowa (wykłady online, laboratoria stacjonarne)
Metody weryfikacji efektów uczenia się
Formą weryfikacji i ewaluacji w ramach przedmiotu jest przedmiotowe zaliczenie na ocenę w formie projektu – samodzielnego/grupowego opracowania pisemnego oraz praktycznej demonstracji umiejętności testowania bezpieczeństwa aplikacji webowej.
Literatura podstawowa

1. Stuttard D., Pinto M., "The Web Application Hacker's Handbook", Wiley

2. OWASP Testing Guide - oficjalna dokumentacja

NAKŁAD PRACY SŁUCHACZA:

	Liczba godzin
Zajęcia dydaktyczne	20
Udział w konsultacjach	5
Przygotowanie się do zajęć	10
Studiowanie literatury	15
Przygotowanie projektu	25
ŁĄCZNY nakład pracy słuchacza w godz.	75
Liczba punktów ECTS	4

2. AI W CYBERBEZPIECZEŃSTWIE

Nazwa przedmiotu: AI w cyberbezpieczeństwie
Nazwa jednostki prowadzącej przedmiot: Akademia Nauk Stosowanych w Wałczu
Nazwa studiów podyplomowych: Cyberbezpieczeństwo
Specjalność: praktyczna
Forma studiów: podyplomowe
Rok studiów: I
Semestr: I
Język wykładowy przedmiotu: polski
Koordynator przedmiotu: [do uzupełnienia]
Prowadzący zajęcia: [do uzupełnienia]

Forma zajęć: Wykład 10h, Laboratoria 10h

Cel przedmiotu
Zapoznać słuchaczy z:

- Zastosowaniami sztucznej inteligencji w cyberbezpieczeństwie
- Metodami machine learning w wykrywaniu zagrożeń
- Narzędziami AI do analizy incydentów bezpieczeństwa
- Ograniczeniami i wyzwaniami AI w cyberbezpieczeństwie
- Praktycznym wykorzystaniem algorytmów AI w ochronie systemów

EFEKTY UCZENIA SIĘ
Wiedza

- SP_W01 Zna i rozumie zastosowania AI w cyberbezpieczeństwie
- SP_W02 Ma wiedzę na temat algorytmów machine learning w kontekście bezpieczeństwa
- SP_W03 Zna ograniczenia i wyzwania związane z AI w cybersecurity

Umiejętności

- SP_U01 Potrafi zastosować narzędzia AI do wykrywania zagrożeń
- SP_U02 Potrafi przeprowadzić analizę incydentów przy użyciu systemów AI
- SP_U03 Potrafi zaprojektować rozwiązanie AI dla konkretnego problemu bezpieczeństwa

Kompetencje

- SP_K01 Potrafi krytycznie ocenić przydatność rozwiązań AI w cyberbezpieczeństwie
- SP_K02 Ma świadomość etycznych aspektów wykorzystania AI w bezpieczeństwie

TREŚCI PROGRAMOWE i LICZBA GODZIN

1. Wprowadzenie do AI w cyberbezpieczeństwie - 3 godziny
2. Machine learning w wykrywaniu anomalii - 4 godziny
3. Systemy AI do analizy malware - 3 godziny
4. Automatyzacja odpowiedzi na incydenty z wykorzystaniem AI - 4 godziny
5. Adversarial AI i obrona przed atakami na systemy AI - 3 godziny
6. Praktyczne implementacje rozwiązań AI - 3 godziny

Metody kształcenia
Wykład kursowy z prezentacją, ćwiczenia polegające na wykonywaniu laboratoriów z wykorzystaniem narzędzi AI. Forma hybrydowa (wykłady online, laboratoria stacjonarne)
Metody weryfikacji efektów uczenia się
Formą weryfikacji jest zaliczenie na ocenę w formie projektu praktycznego wykorzystującego narzędzia AI do rozwiązania konkretnego problemu cyberbezpieczeństwa.
Literatura podstawowa

1. Sarker I.H., "Machine Learning for Cybersecurity", Springer
2. Chio C., Freeman D., "Machine Learning and Security", O'Reilly

NAKŁAD PRACY SŁUCHACZA:

	Liczba godzin
Zajęcia dydaktyczne	20
Udział w konsultacjach	5
Przygotowanie się do zajęć	10
Studiowanie literatury	15
Przygotowanie projektu	25
ŁĄCZNY nakład pracy słuchacza w godz.	75
Liczba punktów ECTS	4

3. OSINT

Nazwa przedmiotu: OSINT
Nazwa jednostki prowadzącej przedmiot: Akademia Nauk Stosowanych w Wałczu
Nazwa studiów podyplomowych: Cyberbezpieczeństwo
Specjalność: praktyczna
Forma studiów: podyplomowe
Rok studiów: I
Semestr: II
Język wykładowy przedmiotu: polski
Koordynator przedmiotu: [do uzupełnienia]
Prowadzący zajęcia: [do uzupełnienia]

Forma zajęć: Wykład 10h, Laboratoria 10h

Cel przedmiotu
Zapoznać słuchaczy z:

- Metodami pozyskiwania informacji z otwartych źródeł
- Narzędziami i technikami OSINT
- Analizą i weryfikacją informacji z różnych źródeł
- Aspektami prawnymi i etycznymi OSINT
- Praktycznym zastosowaniem OSINT w cyberbezpieczeństwie

EFEKTY UCZENIA SIĘ
Wiedza

- SP_W01 Zna i rozumie metodologie OSINT
- SP_W02 Ma wiedzę na temat narzędzi i technik pozyskiwania informacji
- SP_W03 Zna aspekty prawne i etyczne OSINT

Umiejętności

- SP_U01 Potrafi przeprowadzić kompleksową analizę OSINT
- SP_U02 Potrafi weryfikować i korelować informacje z różnych źródeł
- SP_U03 Potrafi wykorzystać narzędzia OSINT w praktyce

Kompetencje

- SP_K01 Potrafi odpowiedzialnie wykorzystywać techniki OSINT
- SP_K02 Ma świadomość ograniczeń prawnych i etycznych

TREŚCI PROGRAMOWE i LICZBA GODZIN

1. Wprowadzenie do OSINT - definicje i zastosowania - 3 godziny
2. Narzędzia i techniki wyszukiwania informacji - 4 godziny
3. Analiza mediów społecznościowych i dark web - 4 godziny
4. Geolokacja i analiza metadanych - 3 godziny
5. Weryfikacja i korelacja informacji - 3 godziny
6. Aspekty prawne i etyczne OSINT - 3 godziny

Metody kształcenia
Wykład kursowy z prezentacją, ćwiczenia praktyczne z wykorzystaniem narzędzi OSINT. Forma hybrydowa (wykłady online, laboratoria stacjonarne)
Metody weryfikacji efektów uczenia się
Zaliczenie na ocenę w formie praktycznego projektu OSINT z pełną dokumentacją procesu i wniosków.
Literatura podstawowa

1. Stewart M., "Open Source Intelligence Techniques", Independently published
2. Materiały OSINT Framework

NAKŁAD PRACY SŁUCHACZA:

	Liczba godzin
Zajęcia dydaktyczne	20
Udział w konsultacjach	5
Przygotowanie się do zajęć	10
Studiowanie literatury	15
Przygotowanie projektu	25
ŁĄCZNY nakład pracy słuchacza w godz.	75
Liczba punktów ECTS	4

4. BEZPIECZEŃSTWO ŚRODOWISKA WINDOWS

Nazwa przedmiotu: Bezpieczeństwo środowiska Windows
Nazwa jednostki prowadzącej przedmiot: Akademia Nauk Stosowanych w Wałczu
Nazwa studiów podyplomowych: Cyberbezpieczeństwo
Specjalność: praktyczna
Forma studiów: podyplomowe
Rok studiów: II
Semestr: I
Język wykładowy przedmiotu: polski
Koordynator przedmiotu: [do uzupełnienia]
Prowadzący zajęcia: [do uzupełnienia]

Forma zajęć: Wykład 10h, Laboratoria 10h

Cel przedmiotu
Zapoznać słuchaczy z:

- Architekturą bezpieczeństwa systemów Windows i mechanizmami ochrony
- Konfiguracją polityk bezpieczeństwa i zarządzaniem uprawnieniami użytkowników
- Zabezpieczaniem Active Directory i infrastruktury domenowej
- Monitorowaniem i audytem środowiska Windows
- Reagowaniem na incydenty bezpieczeństwa w środowisku Windows
- Implementacją zabezpieczeń zgodnie z najlepszymi praktykami Microsoft

EFEKTY UCZENIA SIĘ
Wiedza

- SP_W01 Zna architekturę bezpieczeństwa Windows
- SP_W02 Ma wiedzę na temat mechanizmów ochrony i UAC
- SP_W03 Zna zasady zabezpieczania Active Directory

Umiejętności

- SP_U01 Potrafi skonfigurować polityki bezpieczeństwa Windows
- SP_U02 Potrafi zabezpieczyć infrastrukturę Active Directory
- SP_U03 Potrafi przeprowadzić audyt bezpieczeństwa środowiska Windows

Kompetencje

- SP_K01 Potrafi zaprojektować bezpieczną architekturę Windows
- SP_K02 Ma świadomość odpowiedzialności administratora systemów Windows

TREŚCI PROGRAMOWE i LICZBA GODZIN

1. Architektura bezpieczeństwa Windows - mechanizmy ochrony, UAC, Windows Defender - 3 godziny
2. Konfiguracja Group Policy i zabezpieczeń lokalnych - polityki haseł, audyt, zabezpieczenia - 4 godziny
3. Zabezpieczanie Active Directory - RBAC, Kerberos, zabezpieczenia kontrolerów domeny - 4 godziny
4. Monitoring i audyt Windows - Event Viewer, Performance Monitor, Security Compliance - 3 godziny
5. Windows Defender Advanced Threat Protection i narzędzia antymalware - 3 godziny
6. Analiza incydentów w środowisku Windows - forensyka, reagowanie na zagrożenia - 3 godziny

Metody kształcenia
Wykład kursowy z prezentacją multimedialną, ćwiczenia laboratoryjne na rzeczywistych systemach Windows Server i Windows 10/11. Forma hybrydowa (wykłady online, laboratoria stacjonarne w wyposażonych pracowniach komputerowych)
Metody weryfikacji efektów uczenia się
Formą weryfikacji i ewaluacji w ramach przedmiotu jest przedmiotowe zaliczenie na ocenę w formie kompleksowego projektu praktycznego - konfiguracja zabezpieczeń środowiska Windows Server z Active Directory, implementacja polityk bezpieczeństwa oraz przygotowanie dokumentacji bezpieczeństwa zgodnej ze standardami branżowymi.

Literatura podstawowa

1. Russinovich M., Solomon D., Ionescu A., "Windows Internals, Part 1 & 2", Microsoft Press
2. Microsoft Docs – Windows Security Best Practices, Security Baseline
3. Krause J., Horton B., "Mastering Windows Security and Hardening", Packt Publishing

Literatura uzupełniająca

1. Chapple M., Stewart J.M., Gibson D., "CISSP Official Study Guide", Sybex
2. NIST Cybersecurity Framework - wytyczne dla Windows
3. Center for Internet Security (CIS) Controls for Windows

NAKŁAD PRACY SŁUCHACZA:

	Liczba godzin
Zajęcia dydaktyczne	20
Udział w konsultacjach	5
Przygotowanie się do zajęć	15
Studiowanie literatury	20
Przygotowanie projektu	30
ŁĄCZNY nakład pracy słuchacza w godz.	90
Liczba punktów ECTS	4

5. POWERSHELL W CYBERBEZPIECZEŃSTWIE

Nazwa przedmiotu: PowerShell w cyberbezpieczeństwie
Nazwa jednostki prowadzącej przedmiot: Akademia Nauk Stosowanych w Wałczu
Nazwa studiów podyplomowych: Cyberbezpieczeństwo
Specjalność: praktyczna
Forma studiów: podyplomowe
Rok studiów: II
Semestr: I
Język wykładowy przedmiotu: polski
Koordynator przedmiotu: [do uzupełnienia]
Prowadzący zajęcia: [do uzupełnienia]

Forma zajęć: Wykład 10h, Laboratoria 5h

Cel przedmiotu
Zapoznać słuchaczy z:

- Wykorzystaniem PowerShell w zadaniach cyberbezpieczeństwa
- Automatyzacją procesów bezpieczeństwa za pomocą PowerShell
- Wykrywaniem i analizą zagrożeń przy użyciu PowerShell
- Zabezpieczaniem skryptów PowerShell
- Monitorowaniem aktywności PowerShell

EFEKTY UCZENIA SIĘ
Wiedza

- SP_W01 Zna podstawy PowerShell w kontekście cyberbezpieczeństwa
- SP_W02 Ma wiedzę na temat wykorzystania PowerShell do automatyzacji
- SP_W03 Zna metody zabezpieczania środowiska PowerShell

Umiejętności

- SP_U01 Potrafi tworzyć skrypty PowerShell do zadań bezpieczeństwa
- SP_U02 Potrafi analizować logi i incydenty przy użyciu PowerShell
- SP_U03 Potrafi wykrywać złośliwe użycie PowerShell

Kompetencje

- SP_K01 Potrafi odpowiedzialnie wykorzystywać PowerShell w cyberbezpieczeństwie
- SP_K02 Ma świadomość zagrożeń związanych z PowerShell

TREŚCI PROGRAMOWE i LICZBA GODZIN

1. Podstawy PowerShell dla cyberbezpieczeństwa - 3 godziny
2. Automatyzacja zadań bezpieczeństwa - 3 godziny
3. PowerShell w analizie logów i incydentów - 3 godziny
4. Wykrywanie złośliwego PowerShell - 3 godziny
5. Zabezpieczanie środowiska PowerShell - 3 godziny

Metody kształcenia
Wykład kursowy z prezentacją, ćwiczenia praktyczne pisania skryptów PowerShell. Forma hybrydowa (wykłady online, laboratoria stacjonarne)
Metody weryfikacji efektów uczenia się
Zaliczenie na ocenę w formie projektu praktycznego - zestaw skryptów PowerShell do konkretnych zadań cyberbezpieczeństwa.
Literatura podstawowa

1. Siddaway L., "PowerShell and WMI", Manning
2. Microsoft Docs – PowerShell Security

NAKŁAD PRACY SŁUCHACZA:

	Liczba godzin
Zajęcia dydaktyczne	15
Udział w konsultacjach	3

	Liczba godzin
Przygotowanie się do zajęć	8
Studiowanie literatury	12
Przygotowanie projektu	22
ŁĄCZNY nakład pracy słuchacza w godz.	60
Liczba punktów ECTS	4

6. METODOLOGIA PENTESTÓW OWASP I OSSTMM

Nazwa przedmiotu: Metodologia pentestów OWASP i OSSTMM
Nazwa jednostki prowadzącej przedmiot: Akademia Nauk Stosowanych w Wałczu
Nazwa studiów podyplomowych: Cyberbezpieczeństwo
Specjalność: praktyczna
Forma studiów: podyplomowe
Rok studiów: I
Semestr: II
Język wykładowy przedmiotu: polski
Koordynator przedmiotu: [do uzupełnienia]
Prowadzący zajęcia: [do uzupełnienia]

Forma zajęć: Wykład 10h, Laboratoria 10h

Cel przedmiotu
Zapoznać słuchaczy z:

- Metodologią OWASP Testing Guide i OSSTMM
- Planowaniem i przeprowadzaniem testów penetracyjnych
- Wykorzystaniem narzędzi pentestingowych
- Dokumentowaniem i raportowaniem wyników pentestów
- Aspektami prawnymi i etycznymi testów penetracyjnych

EFEKTY UCZENIA SIĘ
Wiedza

- SP_W01 Zna metodologie OWASP i OSSTMM
- SP_W02 Ma wiedzę na temat planowania testów penetracyjnych
- SP_W03 Zna aspekty prawne i etyczne pentestingu

Umiejętności

- SP_U01 Potrafi zaplanować i przeprowadzić test penetracyjny
- SP_U02 Potrafi wykorzystać narzędzia pentestingowe
- SP_U03 Potrafi przygotować profesjonalny raport z pentestu

Kompetencje

- SP_K01 Potrafi odpowiedzialnie przeprowadzać testy penetracyjne
- SP_K02 Ma świadomość odpowiedzialności etycznej pentatera

TREŚCI PROGRAMOWE i LICZBA GODZIN

1. Wprowadzenie do metodologii OWASP i OSSTMM - 3 godziny
2. Planowanie i przygotowanie testu penetracyjnego - 3 godziny
3. Fazy testu penetracyjnego według OSSTMM - 4 godziny
4. Narzędzia pentestingowe i ich wykorzystanie - 4 godziny
5. Dokumentowanie i raportowanie wyników - 3 godziny
6. Aspekty prawne i etyczne pentestingu - 3 godziny

Metody kształcenia
Wykład kursowy z prezentacją, ćwiczenia praktyczne przeprowadzania testów penetracyjnych.
Forma hybrydowa (wykłady online, laboratoria stacjonarne)
Metody weryfikacji efektów uczenia się
Zaliczenie na ocenę w formie kompleksowego projektu - przeprowadzenie testu penetracyjnego z pełną dokumentacją zgodnie z metodologią OSSTMM.
Literatura podstawowa

1. Herzog P., "OSSTMM Guide", ISECOM
2. OWASP Testing Guide v4.2

NAKŁAD PRACY SŁUCHACZA:

	Liczba godzin
Zajęcia dydaktyczne	20

	Liczba godzin
Udział w konsultacjach	5
Przygotowanie się do zajęć	10
Studiowanie literatury	15
Przygotowanie projektu	25
ŁĄCZNY nakład pracy słuchacza w godz.	75
Liczba punktów ECTS	4

7. ANALIZA PAKIETÓW

Nazwa przedmiotu: Analiza pakietów
Nazwa jednostki prowadzącej przedmiot: Akademia Nauk Stosowanych w Wałczu
Nazwa studiów podyplomowych: Cyberbezpieczeństwo
Specjalność: praktyczna
Forma studiów: podyplomowe
Rok studiów: II
Semestr: I
Język wykładowy przedmiotu: polski
Koordynator przedmiotu: [do uzupełnienia]
Prowadzący zajęcia: [do uzupełnienia]

Forma zajęć: Wykład 10h, Laboratoria 5h

Cel przedmiotu
Zapoznać słuchaczy z:

- Narzędziami do analizy ruchu sieciowego
- Identyfikacją anomalii i zagrożeń w ruchu sieciowym
- Stosowaniem analizy pakietów w praktyce bezpieczeństwa
- Interpretacją protokołów sieciowych
- Technikami forensyki sieciowej

EFEKTY UCZENIA SIĘ
Wiedza

- SP_W01 Zna narzędzia i techniki analizy pakietów
- SP_W02 Ma wiedzę na temat protokołów sieciowych
- SP_W03 Zna metody forensyki sieciowej

Umiejętności

- SP_U01 Potrafi analizować ruch sieciowy przy użyciu Wireshark
- SP_U02 Potrafi identyfikować anomalije w ruchu sieciowym
- SP_U03 Potrafi przeprowadzić analizę forensyczną sieci

Kompetencje

- SP_K01 Potrafi interpretatować wyniki analizy pakietów
- SP_K02 Ma świadomość ograniczeń analizy sieciowej

TREŚCI PROGRAMOWE i LICZBA GODZIN

1. Wprowadzenie do analizy pakietów - narzędzia i techniki - 3 godziny
2. Analiza protokołów TCP/IP - 3 godziny
3. Wykrywanie anomalii w ruchu sieciowym - 3 godziny
4. Analiza aplikacji i protokołów wyższych warstw - 3 godziny
5. Forensyka sieciowa w praktyce - 3 godziny

Metody kształcenia
Wykład kursowy z prezentacją, ćwiczenia praktyczne z wykorzystaniem Wireshark i innych narzędzi. Forma hybrydowa (wykłady online, laboratoria stacjonarne)
Metody weryfikacji efektów uczenia się
Zaliczenie na ocenę w formie praktycznego projektu analizy rzeczywistego ruchu sieciowego z identyfikacją zagrożeń.
Literatura podstawowa

1. Sanders C., "Practical Packet Analysis", No Starch Press
2. Wireshark User Guide

NAKŁAD PRACY SŁUCHACZA:

	Liczba godzin
Zajęcia dydaktyczne	15
Udział w konsultacjach	3

	Liczba godzin
Przygotowanie się do zajęć	8
Studiowanie literatury	12
Przygotowanie projektu	22
ŁĄCZNY nakład pracy słuchacza w godz.	60
Liczba punktów ECTS	4

8. WSTĘP DO PROGRAMOWANIA W PYTHON

Nazwa przedmiotu: Wstęp do programowania w Python
Nazwa jednostki prowadzącej przedmiot: Akademia Nauk Stosowanych w Wałczu
Nazwa studiów podyplomowych: Cyberbezpieczeństwo
Specjalność: praktyczna
Forma studiów: podyplomowe
Rok studiów: I
Semestr: I
Język wykładowy przedmiotu: polski
Koordynator przedmiotu: [do uzupełnienia]
Prowadzący zajęcia: [do uzupełnienia]

Forma zajęć: Wykład 10h, Laboratoria 20h

Cel przedmiotu
Zapoznać słuchaczy z:

- Podstawami składni i semantyki języka Python
- Strukturami danych i algorytmami w Python
- Programowaniem obiektowym w Python
- Bibliotekami Python przydatnymi w cyberbezpieczeństwie
- Automatyzacją zadań za pomocą skryptów Python

EFEKTY UCZENIA SIĘ
Wiedza

- SP_W01 Zna składnię i semantykę języka Python
- SP_W02 Ma wiedzę na temat struktur danych w Python
- SP_W03 Zna biblioteki Python przydatne w cyberbezpieczeństwie

Umiejętności

- SP_U01 Potrafi programować w języku Python
- SP_U02 Potrafi wykorzystać programowanie obiektowe
- SP_U03 Potrafi tworzyć skrypty automatyzujące zadania

Kompetencje

- SP_K01 Potrafi samodzielnie rozwijać umiejętności programistyczne
- SP_K02 Ma świadomość możliwości języka Python

TREŚCI PROGRAMOWE i LICZBA GODZIN

1. Wprowadzenie do Python - składnia i podstawy - 6 godzin
2. Struktury danych w Python - 6 godzin
3. Funkcje i moduły - 6 godzin
4. Programowanie obiektowe - 6 godzin
5. Obsługa plików i wyjątków - 3 godziny
6. Biblioteki dla cyberbezpieczeństwa - 3 godziny

Metody kształcenia
Wykład kursowy z prezentacją, intensywne ćwiczenia praktyczne programowania. Forma hybrydowa (wykłady online, laboratoria stacjonarne)
Metody weryfikacji efektów uczenia się
Zaliczenie na ocenę w formie projektu programistycznego - zestaw skryptów rozwiązujących konkretne problemy.
Literatura podstawowa

1. Lutz M., "Learning Python", O'Reilly
2. Zelle J., "Python Programming", Franklin, Beedle & Associates

NAKŁAD PRACY SŁUCHACZA:

	Liczba godzin
Zajęcia dydaktyczne	30

	Liczba godzin
Udział w konsultacjach	5
Przygotowanie się do zajęć	15
Studiowanie literatury	20
Przygotowanie projektu	30
ŁĄCZNY nakład pracy słuchacza w godz.	100
Liczba punktów ECTS	4

9. PROGRAMOWANIE NARZĘDZIA CYBER W PYTHON

Nazwa przedmiotu: Programowanie narzędzia cyber w Python
Nazwa jednostki prowadzącej przedmiot: Akademia Nauk Stosowanych w Wałczu
Nazwa studiów podyplomowych: Cyberbezpieczeństwo
Specjalność: praktyczna
Forma studiów: podyplomowe
Rok studiów: II
Semestr: I
Język wykładowy przedmiotu: polski
Koordynator przedmiotu: [do uzupełnienia]
Prowadzący zajęcia: [do uzupełnienia]

Forma zajęć: Wykład 10h, Laboratoria 10h

Cel przedmiotu
Zapoznać słuchaczy z:

- Projektowaniem i implementacją narzędzi cyberbezpieczeństwa w Python
- Wykorzystaniem API i bibliotek sieciowych
- Tworzeniem skryptów do analizy bezpieczeństwa
- Automatyzacją procesów w cyberbezpieczeństwie
- Integracją narzędzi z systemami bezpieczeństwa

EFEKTY UCZENIA SIĘ
Wiedza

- SP_W01 Zna zaawansowane techniki Python dla cybersecurity
- SP_W02 Ma wiedzę na temat API systemów bezpieczeństwa
- SP_W03 Zna metody integracji narzędzi bezpieczeństwa

Umiejętności

- SP_U01 Potrafi projektować narzędzia cyberbezpieczeństwa
- SP_U02 Potrafi implementować automatyzację analizy malware
- SP_U03 Potrafi tworzyć dashboardy i raporty

Kompetencje

- SP_K01 Potrafi samodzielnie tworzyć profesjonalne narzędzia
- SP_K02 Ma świadomość wymagań bezpieczeństwa narzędzi

TREŚCI PROGRAMOWE i LICZBA GODZIN

1. Zaawansowane techniki Python dla cybersecurity - 4 godziny
2. Programowanie narzędzi sieciowych - 4 godziny
3. Automatyzacja analizy malware - 4 godziny
4. Integracja z API systemów bezpieczeństwa - 4 godziny
5. Tworzenie dashboardów i raportów - 4 godziny

Metody kształcenia
Wykład kursowy z prezentacją, ćwiczenia praktyczne tworzenia narzędzi. Forma hybrydowa (wykłady online, laboratoria stacjonarne)
Metody weryfikacji efektów uczenia się
Zaliczenie na ocenę w formie kompleksowego projektu - funkcjonalne narzędzie cyberbezpieczeństwa z dokumentacją.
Literatura podstawowa

1. Seitz J., "Black Hat Python", No Starch Press
2. Hussain M., "Python for Cybersecurity", Packt Publishing

NAKŁAD PRACY SŁUCHACZA:

	Liczba godzin
Zajęcia dydaktyczne	20
Udział w konsultacjach	5

	Liczba godzin
Przygotowanie się do zajęć	10
Studiowanie literatury	15
Przygotowanie projektu	25
ŁĄCZNY nakład pracy słuchacza w godz.	75
Liczba punktów ECTS	4

10. ANALIZA POWŁAMANIOWA - INFORMATYKA ŚLEDCZA

Nazwa przedmiotu: Analiza powłamaniowa - informatyka śledcza
Nazwa jednostki prowadzącej przedmiot: Akademia Nauk Stosowanych w Wałczu
Nazwa studiów podyplomowych: Cyberbezpieczeństwo
Specjalność: praktyczna
Forma studiów: podyplomowe
Rok studiów: II
Semestr: I
Język wykładowy przedmiotu: polski
Koordynator przedmiotu: [do uzupełnienia]
Prowadzący zajęcia: [do uzupełnienia]

Forma zajęć: Wykład 10h, Laboratoria 10h

Cel przedmiotu
Zapoznać słuchaczy z:

- Metodami zabezpieczania i analizy dowodów cyfrowych
- Przeprowadzaniem analizy powłamaniowej
- Narzędziami informatyki śledczej
- Przygotowywaniem raportów z dochodzeń informatycznych
- Aspektami prawnymi cyberdochodzeń

EFEKTY UCZENIA SIĘ
Wiedza

- SP_W01 Zna metodologie informatyki śledczej
- SP_W02 Ma wiedzę na temat zabezpieczania dowodów cyfrowych
- SP_W03 Zna aspekty prawne cyberdochodzeń

Umiejętności

- SP_U01 Potrafi przeprowadzić analizę powłamaniową
- SP_U02 Potrafi odzyskiwać usunięte dane
- SP_U03 Potrafi przygotować raport z dochodzenia

Kompetencje

- SP_K01 Potrafi profesjonalnie przeprowadzać dochodzenia
- SP_K02 Ma świadomość odpowiedzialności prawnej

TREŚCI PROGRAMOWE i LICZBA GODZIN

1. Wprowadzenie do informatyki śledczej - 3 godziny
2. Zabezpieczanie dowodów cyfrowych - 4 godziny
3. Analiza systemów plików i registrów - 4 godziny
4. Odzyskiwanie usuniętych danych - 3 godziny
5. Analiza logów i śladów aktywności - 3 godziny
6. Raportowanie i aspekty prawne - 3 godziny

Metody kształcenia
Wykład kursowy z prezentacją, ćwiczenia praktyczne z wykorzystaniem narzędzi forensycznych.
Forma hybrydowa (wykłady online, laboratoria stacjonarne)
Metody weryfikacji efektów uczenia się
Zaliczenie na ocenę w formie kompleksowego projektu analizy powłamaniowej z pełną dokumentacją procedur i wniosków.
Literatura podstawowa

1. Nelson B., Phillips A., Steuart C., "Guide to Computer Forensics and Investigations", Cengage
2. Sammons J., "The Basics of Digital Forensics", Syngress

NAKŁAD PRACY SŁUCHACZA:

	Liczba godzin
Zajęcia dydaktyczne	20

	Liczba godzin
Udział w konsultacjach	5
Przygotowanie się do zajęć	10
Studiowanie literatury	15
Przygotowanie projektu	25
ŁĄCZNY nakład pracy słuchacza w godz.	75
Liczba punktów ECTS	4

11. WPROWADZENIE DO CYBERBEZPIECZEŃSTWA

Nazwa przedmiotu: Wprowadzenie do cyberbezpieczeństwa
Nazwa jednostki prowadzącej przedmiot: Akademia Nauk Stosowanych w Wałczu
Nazwa studiów podyplomowych: Cyberbezpieczeństwo
Specjalność: praktyczna
Forma studiów: podyplomowe
Rok studiów: I
Semestr: I
Język wykładowy przedmiotu: polski
Koordynator przedmiotu: [do uzupełnienia]
Prowadzący zajęcia: [do uzupełnienia]

Forma zajęć: Wykład 5h, Laboratoria 10h

Cel przedmiotu
Zapoznać słuchaczy z:

- Podstawowymi pojęciami i zagadnieniami cyberbezpieczeństwa
- Głównymi zagrożeniami i metodami ochrony
- Rolą cyberbezpieczeństwa w organizacji
- Standardami i certyfikacjami w cyberbezpieczeństwie
- Karierą w cyberbezpieczeństwie

EFEKTY UCZENIA SIĘ
Wiedza

- SP_W01 Zna podstawowe pojęcia cyberbezpieczeństwa
- SP_W02 Ma wiedzę na temat głównych zagrożeń cybernetycznych
- SP_W03 Zna standardy i certyfikacje w cyberbezpieczeństwie

Umiejętności

- SP_U01 Potrafi zidentyfikować podstawowe zagrożenia
- SP_U02 Potrafi zastosować podstawowe metody ochrony
- SP_U03 Potrafi ocenić poziom cyberbezpieczeństwa organizacji

Kompetencje

- SP_K01 Potrafi świadomie planować karierę w cyberbezpieczeństwie
- SP_K02 Ma świadomość znaczenia cyberbezpieczeństwa

TREŚCI PROGRAMOWE i LICZBA GODZIN

1. Wprowadzenie do cyberbezpieczeństwa - podstawowe pojęcia - 3 godziny
2. Kategorie zagrożeń cybernetycznych - 3 godziny
3. Metody ochrony i zabezpieczeń - 3 godziny
4. Standardy i certyfikacje w cyberbezpieczeństwie - 3 godziny
5. Kariera w cybersecurity - 3 godziny

Metody kształcenia
Wykład kursowy z prezentacją, ćwiczenia praktyczne z analizą przypadków. Forma stacjonarna
Metody weryfikacji efektów uczenia się
Zaliczenie na ocenę w formie testu pisemnego oraz prezentacji grupowej na temat wybranego aspektu cyberbezpieczeństwa.
Literatura podstawowa

1. Andress J., "The Basics of Information Security", Syngress
2. Cole E., "Network Security Bible", Wiley

NAKŁAD PRACY SŁUCHACZA:

	Liczba godzin
Zajęcia dydaktyczne	15
Udział w konsultacjach	3

	Liczba godzin
Przygotowanie się do zajęć	8
Studiowanie literatury	12
Przygotowanie prezentacji	17
ŁĄCZNY nakład pracy słuchacza w godz.	55
Liczba punktów ECTS	3

12. SOCJOTECHNIKI I FIZYCZNE NARZĘDZIA PENTESTERSKIE

Nazwa przedmiotu: Socjotechniki i fizyczne narzędzia pentesterskie
Nazwa jednostki prowadzącej przedmiot: Akademia Nauk Stosowanych w Wałczu
Nazwa studiów podyplomowych: Cyberbezpieczeństwo
Specjalność: praktyczna
Forma studiów: podyplomowe
Rok studiów: I
Semestr: I
Język wykładowy przedmiotu: polski
Koordynator przedmiotu: [do uzupełnienia]
Prowadzący zajęcia: [do uzupełnienia]

Forma zajęć: Wykład 5h, Laboratoria 10h

Cel przedmiotu
Zapoznać słuchaczy z:

- Technikami socjotechnicznymi stosowanymi w atakach
- Fizycznymi narzędziami wykorzystywanymi w pentestingu
- Metodami ochrony przed atakami socjotechnicznymi
- Etyką i prawem w kontekście testów fizycznych
- Przygotowywaniem scenariuszy ataków socjotechnicznych

EFEKTY UCZENIA SIĘ
Wiedza

- SP_W01 Zna techniki socjotechniczne i psychologię ataków
- SP_W02 Ma wiedzę na temat fizycznych narzędzi pentesterskich
- SP_W03 Zna metody obrony przed atakami socjotechnicznymi

Umiejętności

- SP_U01 Potrafi zaprojektować scenariusz ataku socjotechnicznego
- SP_U02 Potrafi wykorzystać fizyczne narzędzia pentesterskie
- SP_U03 Potrafi zaimplementować obronę przed socjotechnikami

Kompetencje

- SP_K01 Potrafi etycznie wykorzystywać wiedzę o socjotechnikach
- SP_K02 Ma świadomość odpowiedzialności prawnej

TREŚCI PROGRAMOWE i LICZBA GODZIN

1. Wprowadzenie do socjotechnik - psychologia ataków - 3 godziny
2. Techniki manipulacji i perswazji - 3 godziny
3. Fizyczne narzędzia pentesterskie - lock picking, RFID - 4 godziny
4. Scenariusze ataków socjotechnicznych - 3 godziny
5. Obrona przed atakami socjotechnicznymi - 2 godziny

Metody kształcenia
Wykład kursowy z prezentacją, intensywne ćwiczenia praktyczne z wykorzystaniem fizycznych narzędzi. Forma stacjonarna
Metody weryfikacji efektów uczenia się
Zaliczenie na ocenę w formie praktycznego projektu - przygotowanie i prezentacja kompleksowego scenariusza ataku socjotechnicznego.
Literatura podstawowa

1. Mitnick K., Simon W.L., "The Art of Deception", Wiley
2. Gragg D., "Social Engineering Fundamentals", SecurityFocus

NAKŁAD PRACY SŁUCHACZA:

	Liczba godzin
Zajęcia dydaktyczne	15
Udział w konsultacjach	3

	Liczba godzin
Przygotowanie się do zajęć	8
Studiowanie literatury	12
Przygotowanie projektu	22
ŁĄCZNY nakład pracy słuchacza w godz.	60
Liczba punktów ECTS	3

13. BEZPIECZEŃSTWO SIECI KOMPUTEROWYCH

Nazwa przedmiotu: Bezpieczeństwo sieci komputerowych
Nazwa jednostki prowadzącej przedmiot: Akademia Nauk Stosowanych w Wałczu
Nazwa studiów podyplomowych: Cyberbezpieczeństwo
Specjalność: praktyczna
Forma studiów: podyplomowe
Rok studiów: I
Semestr: II
Język wykładowy przedmiotu: polski
Koordynator przedmiotu: [do uzupełnienia]
Prowadzący zajęcia: [do uzupełnienia]

Forma zajęć: Wykład 10h, Laboratoria 20h

Cel przedmiotu
Zapoznać słuchaczy z:

- Architekturą i protokołami sieci komputerowych
- Implementacją zabezpieczeń sieciowych
- Monitorowaniem i analizą ruchu sieciowego
- Reagowaniem na incydenty sieciowe
- Projektowaniem bezpiecznej architektury sieciowej

EFEKTY UCZENIA SIĘ
Wiedza

- SP_W01 Zna architektury i protokoły sieci komputerowych
- SP_W02 Ma wiedzę na temat zabezpieczeń sieciowych
- SP_W03 Zna metody monitorowania ruchu sieciowego

Umiejętności

- SP_U01 Potrafi zaprojektować bezpieczną architekturę sieciową
- SP_U02 Potrafi skonfigurować systemy IDS/IPS
- SP_U03 Potrafi reagować na incydenty sieciowe

Kompetencje

- SP_K01 Potrafi kompleksowo podejść do bezpieczeństwa sieci
- SP_K02 Ma świadomość ciągłej ewolucji zagrożeń sieciowych

TREŚCI PROGRAMOWE i LICZBA GODZIN

1. Podstawy sieci komputerowych i protokołów - 5 godzin
2. Zagrożenia sieciowe i metody ataków - 5 godzin
3. Firewalle i systemy IDS/IPS - 6 godzin
4. VPN i szyfrowanie komunikacji - 4 godziny
5. Bezpieczeństwo sieci bezprzewodowych - 4 godziny
6. Monitoring i analiza ruchu sieciowego - 6 godzin

Metody kształcenia
Wykład kursowy z prezentacją, intensywne ćwiczenia laboratoryjne z konfiguracją urządzeń sieciowych. Forma stacjonarna
Metody weryfikacji efektów uczenia się
Zaliczenie na ocenę w formie kompleksowego projektu - projekt i implementacja bezpiecznej architektury sieciowej.
Literatura podstawowa

1. Stallings W., "Network Security Essentials", Pearson
2. Bejtlich R., "The Practice of Network Security Monitoring", No Starch Press

NAKŁAD PRACY SŁUCHACZA:

	Liczba godzin
Zajęcia dydaktyczne	30

	Liczba godzin
Udział w konsultacjach	5
Przygotowanie się do zajęć	15
Studiowanie literatury	20
Przygotowanie projektu	30
ŁĄCZNY nakład pracy słuchacza w godz.	100
Liczba punktów ECTS	4

14. PRAWO A DZIAŁANIA W CYBER

Nazwa przedmiotu: Prawo a działania w cyber
Nazwa jednostki prowadzącej przedmiot: Akademia Nauk Stosowanych w Wałczu
Nazwa studiów podyplomowych: Cyberbezpieczeństwo
Specjalność: praktyczna
Forma studiów: podyplomowe
Rok studiów: I
Semestr: II
Język wykładowy przedmiotu: polski
Koordynator przedmiotu: [do uzupełnienia]
Prowadzący zajęcia: [do uzupełnienia]

Forma zajęć: Wykład 5h, Laboratoria 10h

Cel przedmiotu
Zapoznać słuchaczy z:

- Podstawowymi regulacjami prawnymi dotyczącymi cyberprzestrzeni
- Aspektami prawnymi działań w cyberbezpieczeństwie
- Przepisami dotyczącymi ochrony danych osobowych
- Prawem dotyczącym cyberprzestępczości
- Odpowiedzialnością prawną w cyberprzestrzeni

EFEKTY UCZENIA SIĘ
Wiedza

- SP_W01 Zna podstawowe regulacje prawne w cyberprzestrzeni
- SP_W02 Ma wiedzę na temat RODO i ochrony danych
- SP_W03 Zna prawo dotyczące cyberprzestępczości

Umiejętności

- SP_U01 Potrafi zastosować przepisy prawne w praktyce
- SP_U02 Potrafi przeanalizować przypadek prawny
- SP_U03 Potrafi ocenić aspekty prawne działań w cybersecurity

Kompetencje

- SP_K01 Potrafi odpowiedzialnie działać w ramach prawa
- SP_K02 Ma świadomość konsekwencji prawnych

TREŚCI PROGRAMOWE i LICZBA GODZIN

1. Wprowadzenie do prawa w cyberprzestrzeni - 3 godziny
2. Ustawa o krajowym systemie cyberbezpieczeństwa (NIS2) - 3 godziny
3. RODO i ochrona danych osobowych - 4 godziny
4. Prawo dotyczące cyberprzestępczości - 3 godziny
5. Odpowiedzialność prawna w cyberbezpieczeństwie - 2 godziny

Metody kształcenia
Wykład kursowy z prezentacją, ćwiczenia z analizą przypadków prawnych. Forma stacjonarna
Metody weryfikacji efektów uczenia się
Zaliczenie na ocenę w formie testu pisemnego oraz analizy przypadku prawnego związanego z cyberbezpieczeństwem.
Literatura podstawowa

1. Chomiczewski W., "Prawo w cyberprzestrzeni", Wolters Kluwer
2. Ustawa o krajowym systemie cyberbezpieczeństwa

NAKŁAD PRACY SŁUCHACZA:

	Liczba godzin
Zajęcia dydaktyczne	15
Udział w konsultacjach	3

	Liczba godzin
Przygotowanie się do zajęć	8
Studiowanie literatury	12
Przygotowanie do testu	17
ŁĄCZNY nakład pracy słuchacza w godz.	55
Liczba punktów ECTS	3

15. CYBERPRZESTĘPCZOŚĆ

Nazwa przedmiotu: Cyberprzestępczość
Nazwa jednostki prowadzącej przedmiot: Akademia Nauk Stosowanych w Wałczu
Nazwa studiów podyplomowych: Cyberbezpieczeństwo
Specjalność: praktyczna
Forma studiów: podyplomowe
Rok studiów: I
Semestr: II
Język wykładowy przedmiotu: polski
Koordynator przedmiotu: [do uzupełnienia]
Prowadzący zajęcia: [do uzupełnienia]

Forma zajęć: Wykład 5h, Laboratoria 10h

Cel przedmiotu
Zapoznać słuchaczy z:

- Mechanizmami i rodzajami cyberprzestępczości
- Analizą przypadków przestępstw komputerowych
- Metodami przeciwdziałania cyberprzestępczości
- Współpracą z organami ścigania
- Profilowaniem cyberprzestępców

EFEKTY UCZENIA SIĘ
Wiedza

- SP_W01 Zna typologie i trendy cyberprzestępczości
- SP_W02 Ma wiedzę na temat metod działania cyberprzestępców
- SP_W03 Zna metody przeciwdziałania cyberprzestępczości

Umiejętności

- SP_U01 Potrafi przeanalizować przypadek cyberprzestępstwa
- SP_U02 Potrafi zastosować metody profilaktyki
- SP_U03 Potrafi współpracować z organami ścigania

Kompetencje

- SP_K01 Potrafi profesjonalnie reagować na cyberprzestępstwa
- SP_K02 Ma świadomość społecznej odpowiedzialności

TREŚCI PROGRAMOWE i LICZBA GODZIN

1. Wprowadzenie do cyberprzestępczości - typologie i trendy - 3 godziny
2. Analiza przypadków cyberprzestępstw - 4 godziny
3. Metody działania cyberprzestępców - 3 godziny
4. Przeciwdziałanie i profilaktyka - 3 godziny
5. Współpraca z organami ścigania - 2 godziny

Metody kształcenia
Wykład kursowy z prezentacją, ćwiczenia z analizą rzeczywistych przypadków cyberprzestępstw. Forma stacjonarna
Metody weryfikacji efektów uczenia się
Zaliczenie na ocenę w formie prezentacji grupowej - analiza wybranego przypadku cyberprzestępczości z propozycją metod przeciwdziałania.
Literatura podstawowa

1. Holt T.J., Bossler A.M., "Cybercrime and Digital Forensics", Routledge
2. Wall D.S., "Cybercrime: The Transformation of Crime in the Information Age", Polity

NAKŁAD PRACY SŁUCHACZA:

	Liczba godzin
Zajęcia dydaktyczne	15
Udział w konsultacjach	3

	Liczba godzin
Przygotowanie się do zajęć	8
Studiowanie literatury	12
Przygotowanie prezentacji	17
ŁĄCZNY nakład pracy słuchacza w godz.	55
Liczba punktów ECTS	3