Pozycja w planie studiów (lub kod przedmiotu)	C.2.1

Wydział	Techniczny
Kierunek	Informatyka
Poziom studiów	Pierwszego stopnia
Forma studiów	stacjonarne/niestacjonarne
Profil kształcenia	Praktyczny

PROGRAM PRZEDMIOTU/MODUŁU

A - Informacje ogólne

1. Nazwa przedmiotu	**Projektowanie i analiza sieci**
2. Punkty ECTS	**4**
3. Rodzaj przedmiotu	**Obowiązkowy**
4. Język przedmiotu	**Język polski**
5. Rok studiów	**II**
6. Imię i nazwisko koordynatora przedmiotu oraz prowadzących zajęcia	**Łukasz Lemieszewski**

B – Formy dydaktyczne prowadzenia zajęć i liczba godzin w semestrze

Nr semestru	Studia stacjonarne	Studia niestacjonarne
Semestr 3	**Wykłady**: (15); **Laboratoria**: (30); **Projekt:** (15)	**Wykłady**: (10); **Laboratoria**: (18); **Projekt:** (10)
Liczba godzin ogółem	**60**	**38**

C - Wymagania wstępne

Student nabył podstawową wiedzę z zakresu systemów operacyjnych oraz sieci komputerowych i bezpieczeństwa informacji

D - Cele kształcenia

Wiedza	
CW1	przekazanie wiedzy w zakresie wiedzy technicznej obejmującej terminologię, pojęcia, teorie, zasady, metody, techniki i narzędzia stosowane przy rozwiązywaniu zadań inżynierskich związanych z szeroko pojętą informatyką, procesami planowania i realizacji systemów informatycznych, eksperymentów, tak w procesie przygotowania z udziałem metod symulacji komputerowych, jak i w rzeczywistym środowisku
Umiejętności	
CU1	wyrobienie umiejętności w zakresie doskonalenia wiedzy, pozyskiwania i integrowanie informacji z literatury, baz danych i innych źródeł, opracowywania dokumentacji, prezentowania ich i podnoszenia kompetencji zawodowych
CU2	wyrobienie umiejętności posługiwania się specjalistycznym oprogramowaniem, projektowania systemów, sieci i aplikacji, programowania aplikacji, modelowania systemów, posługiwania się zaawansowanymi środowiskami projektowo-uruchomieniowymi, stosowania nowoczesnych urządzeń i podzespołów peryferyjnych
Kompetencje społeczne	
CK1	przygotowanie do uczenia się przez całe życie, podnoszenie kompetencji zawodowych, osobistych i społecznych w zmieniającej się rzeczywistości, podjęcia pracy związanej z obsługą sprzętu informatycznego, programowaniem i praktycznym posługiwaniem się szerokim spektrum narzędzi informatycznych

E - Efekty kształcenia przedmiotowe i kierunkowe

Przedmiotowy efekt kształcenia (EP) w zakresie wiedzy (W), umiejętności (U) i kompetencji społecznych (K)		Kierunkowy efekt kształcenia
Wiedza (EPW…)		
EPW1	ma wiedzę ogólną obejmującą kluczowe zagadnienia bezpieczeństwa systemów, urządzeń i procesów	K_W05
EPW2	zna podstawowe narzędzia, metody i techniki identyfikacji i analizy zagrożeń	K_W07
Umiejętności (EPU…)		
EPU1	potrafi pozyskiwać informacje z literatury, baz danych i innych źródeł; potrafi integrować uzyskane informacje, dokonywać ich interpretacji, a także wyciągać wnioski oraz formułować i uzasadniać opinie	K_U01
EPU2	potrafi opracować dokumentację dotyczącą realizacji zadania inżynierskiego i przygotować tekst zawierający omówienie wyników realizacji tego zadania	K_U03
EPU3	potrafi ocenić ryzyko i bezpieczeństwo baz danych, aplikacji internetowych, systemów i sieci komputerowych, stosując techniki oraz narzędzia sprzętowe i programowe	K_U12
Kompetencje społeczne (EPK…)		
EPK1	rozumie potrzebę uczenia się przez całe życie	K_K01
EPK2	ma świadomość ważności i rozumie pozatechniczne aspekty i skutki działalności inżynierskiej, w tym jej wpływu na środowisko, i związanej z tym odpowiedzialności za podejmowane decyzje	K_K02
EPK3	prawidłowo identyfikuje i rozstrzyga dylematy związane z wykonywaniem zawodu	K_K06

F - Treści programowe oraz liczba godzin na poszczególnych formach zajęć

Lp.	Treści wykładów	Liczba godzin na studiach	
		stacjonarnych	niestacjonarnych
W1	Program nauczania, zasady zaliczenia oraz podstawowe informacje o przedmiocie. Zakładanie kont netacad.com	1	1
W2	Wprowadzenie do sieci przełączanych. Podstawowe idee i konfiguracja przełączania.	2	1
W3	VLAN. Koncepcje routingu. Routing między VLAN-ami.	2	1
W4	Routing statyczny. Routing dynamiczny.	2	2
W5	Protokół OSPF jednoobszarowy.	2	1
W6	Listy kontroli dostępu (ACL).	2	1
W7	DHCP.	2	1
W8	Translacja adresów dla IPv4	1	1
W9	Zaleczenie.	1	1
	Razem liczba godzin wykładów	15	10

Lp.	Treści laboratoriów	Liczba godzin na studiach	
		stacjonarnych	niestacjonarnych
L1	Packet Tracer - Konfiguracja podstawowych ustawień przełącznika (2.1.1.6)	2	2
L2	Packet Tracer - Konfiguracja aspektów bezpieczeństwa przełącznika (2.2.4.11)	2	2
L3	Packet Tracer – Konfigurowanie sieci VLAN (3.2.1.7)	2	1

	Konfiguracja połączeń trunk (3.2.2.4)		
L4	Konfiguracja VLAN i łącza trunk (3.2.2.5)	2	1
L5	Packet Tracer – Konfigurowanie i weryfikacja małej sieci (4.1.4.5) Badanie tras bezpośrednich (4.3.2.5)	2	1
L6	Podstawowa konfiguracja routera z użyciem IOS (4.1.4.6)	2	1
L7	Packet Tracer - Konfiguracja routera "na patyku" - inter-VLAN routing (5.1.3.6)	2	1
L8	Konfigurowanie tras statycznych i tras domyślnych IPv4 i IPv6 (6.2.4.4)	2	1
L9	Packet Tracer – Porównanie wyboru trasy przez protokoły RIP i EIGRP (7.2.2.4), Konfigurowanie RIPv2 (7.3.1.8)	2	1
L10	Packet Tracer – Konfigurowanie RIPng (7.3.2.3) Podstawowa konfiguracja protokołów RIPv2 oraz RIPng (7.3.2.4)	2	1
L11	Packet Tracer – Konfigurowanie jednoobszarowego OSPFv2 (8.2.2.7)	2	1
L12	Podstawowa konfiguracja OSPFv2 dla pojedynczego obszaru(8.2.4.5)	2	1
L13	Packet Tracer - Konfiguracja i weryfikacja standardowych list kontroli dostępu ACL (9.2.2.7)	2	1
L14	Podstawowa konfiguracja DHCPv4 na routerze (10.1.2.4)	2	1
L15	Packet Tracer - Implementacja statycznego i dynamicznego NAT (11.2.3.6)	2	2
		30	18

Lp.	**Treści projektów**	**Liczba godzin na studiach**	
		stacjonarnych	**niestacjonarnych**
P1	Dla wybranego scenariusza organizacji (budynku) realizacja projektu fizycznej infrastruktury sieciowej. Harmonogram projektu.	2	2
p2	Dla wybranego scenariusza organizacji realizacja logicznej infrastruktury sieciowej pod względem bezpieczeństwa komunikacji.	2	1
P3	Schemat realizacji projektu sieci komputerowej typu LAN i WAN z wyborem medium transmisyjnego (przewodowego, bezprzewodowego).	2	1
P4	Wybór sieciowych protokołów komunikacyjnych i doboru urządzeń sieciowych.	2	1
P5	Infrastruktura logiczna i implementacja protokołów komunikacji.	2	1
P6	Opracowanie kosztorys w programie NORMA PRO.	2	2
P7	Ocena projektów sieci.	3	2
	Razem liczba godzin projektów	15	10

G – Metody oraz środki dydaktyczne wykorzystywane w ramach poszczególnych form zajęć

Forma zajęć	**Metody dydaktyczne (wybór z listy)**	**Środki dydaktyczne**
Wykład	M1 - wykład informacyjny, M3 – pokaz multimedialny	projektor, prezentacja multimedialna
Laboratoria	M5 - ćwiczenia doskonalące obsługę programów do projektowania sieci i analizowania sieciowych protokołów komunikacyjnych.	jednostka komputerowa wyposażona w oprogramowanie oraz z dostępem do sieci Internetu
Projekt	M5 - ćwiczenia doskonalące obsługę programów do projektowania sieci i analizowania sieciowych protokołów komunikacyjnych.	Jednostka komputerowa wyposażona w oprogramowanie oraz z dostępem do sieci Internetu

H - Metody oceniania osiągnięcia efektów kształcenia na poszczególnych formach zajęć

Forma zajęć	**Ocena formująca (F) –** wskazuje studentowi na potrzebę uzupełniania wiedzy lub stosowania określonych metod i narzędzi, stymulujące do doskonalenia efektów pracy **(wybór z listy)**	**Ocena podsumowująca (P) –** podsumowuje osiągnięte efekty kształcenia **(wybór z listy)**
Wykład	F2 - obserwacja poziomu przygotowania do zajęć	P1 – egzamin pisemny
Laboratoria	F2 – obserwacja/aktywność (przygotowanie do zajęć, ocena ćwiczeń wykonywanych podczas zajęć), F3 – praca pisemna (sprawozdanie), F5 - ćwiczenia praktyczne (ćwiczenia sprawdzające umiejętności).	P2 – kolokwium praktyczne
Projekt	F3 – dokumentacja projektu F4 – wystąpienie – analiza projektu	P4 – praca pisemna - projekt

H-1 Metody weryfikacji osiągnięcia przedmiotowych efektów kształcenia (wstawić „x")

Efekty przedmiotowe	Wykład		Laboratoria				Projekt		
	F2	P1	F2	F3	F5	P2	F3	F4	P4
EPW1	x	x							
EPW2	x	x							
EPU1			x	x	x	x	x	x	x
EPU2			x	x	x	x	x	x	x
EPU3			x	x	x	x	x	x	x
EPK1	x	x							
EPK2	x	x							
EPK3	x	x							

I – Kryteria oceniania

Wymagania określające kryteria uzyskania oceny w danym efekcie			
Ocena			
Przedmiotowy efekt kształcenia (EP..)	**Dostateczny dostateczny plus 3/3,5**	**dobry dobry plus 4/4,5**	**bardzo dobry 5**
EPW1	potrafi wskazać i poddać analizie wybrane protokoły komunikacyjne w sieci	potrafi wskazać i poddać analizie większość protokołów komunikacyjnych w sieci	potrafi wskazać i poddać analizie wszystkie protokołów komunikacyjne w sieci
EPW2	potrafi zdefiniować wybrane pojęcia z zakresu projektowania sieci komputerowych	potrafi zdefiniować większość pojęć z zakresu projektowania sieci komputerowych	potrafi zdefiniować wszystkie pojęcia z zakresu projektowania sieci komputerowych
EPU1	potrafi korzystać z wiedzy na temat analizy i projektowania prostych pod względem skomplikowania sieci komputerowych, zawartej w literaturze, internetowych bazach danych i innych źródeł	potrafi korzystać z wiedzy na temat analizy i projektowania średniozaawansowanych pod względem skomplikowania sieci komputerowych, zawartej w literaturze, internetowych bazach danych i innych źródeł	potrafi korzystać z wiedzy na temat analizy i projektowania zaawansowanych pod względem skomplikowania sieci komputerowych, zawartej w literaturze, internetowych bazach danych i innych źródeł
EPU2	potrafi opracować dokumentację prostej pod względem skomplikowania zaprojektowanej sieci komputerowej	potrafi opracować dokumentację średniozaawansowanej pod względem skomplikowania zaprojektowanej sieci komputerowej	potrafi opracować pełną dokumentację zaprojektowanej sieci komputerowej

EPU3	potrafi ocenić ryzyko i bezpieczeństwo zaprojektowanej sieci na podstawie analizy wybranego sieciowego protokołów komunikacyjnych	potrafi w ocenić ryzyko i bezpieczeństwo zaprojektowanej sieci na podstawie analizy podstawowych sieciowych protokołów komunikacyjnych	potrafi w ocenić ryzyko i bezpieczeństwo zaprojektowanej sieci na podstawie analizy wszystkich sieciowych protokołów komunikacyjnych
EPK1	rozumie w podstawowym stopniu potrzebę ciągłego kształcenia z zakresu analizy i projektowania sieci	rozumie potrzebę ciągłego kształcenia z zakresu analizy i projektowania sieci	rozumie potrzebę ciągłego kształcenia z zakresu analizy i projektowania sieci oraz rozumie skutki takiego postępowania
EPK2	potrafi określać niektóre priorytety niezbędne przy analizie sieciowych protokołów komunikacyjnych i projektowaniu komunikacji w sieci	potrafi określać większość priorytetów niezbędnych przy analizie sieciowych protokołów komunikacyjnych i projektowaniu komunikacji w sieci	potrafi określać wszystkie priorytety niezbędnych przy analizie sieciowych protokołów komunikacyjnych i projektowaniu komunikacji w sieci
EPK3	potrafi w słabym stopniu kreatywnie projektować i analizować proste sieci	potrafi w słabym stopniu kreatywnie projektować i analizować proste sieci	potrafi w słabym stopniu kreatywnie projektować i analizować proste sieci

J – Forma zaliczenia przedmiotu

Wykład - egzamin (test)

Laboratorium – zaliczenie z oceną. Na ocenę składa się oddanie min. 7 sprawozdawań, z laboratorium które są podstawą przystąpienia do kolokwium zaliczeniowego.

Projekt– zaliczenie z oceną. Ocenie podlegać będzie projekt sieci komputerowej.

Kryteria ocen dla wykładu, projektu i laboratorium:

0-50 % – niedostateczna
51-60 % – dostateczna
61-70 % – dostateczna plus
71-80 % - dobry
81-90 % dobry plus
91-100 % bardzo dobry

K – Literatura przedmiotu

Literatura obowiązkowa:

1. Chris Sanders, Praktyczna analiza pakietów. Wykorzystanie narzędzia Wireshark do rozwiązywania problemów z siecią. Helion, Gliwice 2013.
2. Stanisław Wszelak, Administrowanie sieciowymi protokołami komunikacyjnymi, Helion, Gliwice 2015
3. Paweł Zaręba, Praktyczne projekty sieciowe. Helion, Gliwice 2019.

Literatura zalecana / fakultatywna:

1. Barrie Sosinsky, Sieci komputerowe. Biblia, Helion, 2011.
2. Mueller S., Rozbudowa i naprawa sieci. Wydanie II, Helion, 2004.

L – Obciążenie pracą studenta:

Forma aktywności studenta	Liczba godzin na realizację	
	na studiach stacjonarnych	na studiach niestacjonarnych
Godziny zajęć z nauczycielem/ami	60	38
Konsultacje	5	5
Czytanie literatury	5	12

Przygotowanie sprawozdań	10	15
Przygotowanie projektów	10	15
Przygotowanie do egzaminu	10	15
Suma godzin:	**100**	**100**
Liczba punktów ECTS dla przedmiotu (suma godzin : 25 godz.):	**4**	**4**

Ł – Informacje dodatkowe

Imię i nazwisko sporządzającego	Łukasz Lemieszewski
Data sporządzenia / aktualizacji	8 grudnia 2019 r.
Dane kontaktowe (e-mail, telefon)	llemieszewski@ajp.edu.pl
Podpis	

Pozycja w planie studiów (lub kod przedmiotu)	C.2.2

Wydział	Techniczny
Kierunek	Informatyka
Poziom studiów	Pierwszego stopnia
Forma studiów	stacjonarne/niestacjonarne
Profil kształcenia	Praktyczny

PROGRAM PRZEDMIOTU/MODUŁU

A - Informacje ogólne

1. Nazwa przedmiotu	**Polityka bezpieczeństwa w firmie**
2. Punkty ECTS	**5**
3. Rodzaj przedmiotu	**obowiązkowy**
4. Język przedmiotu	**język polski**
5. Rok studiów	**II**
6. Imię i nazwisko koordynatora przedmiotu oraz prowadzących zajęcia	**Łukasz Lemieszewski**

B – Formy dydaktyczne prowadzenia zajęć i liczba godzin w semestrze

Nr semestru	Studia stacjonarne	Studia niestacjonarne
Semestr 3	**Wykłady**: (30); **Laboratoria**: (15); **Projekt:** (30)	**Wykłady**: (15); **Laboratoria**: (10); **Projekt:** (18)
Liczba godzin ogółem	**75**	**43**

C - Wymagania wstępne

Student nabył podstawową wiedzę z zakresu systemów operacyjnych, sieci komputerowych oraz programowania

D - Cele kształcenia

	Wiedza
CW1	przekazanie wiedzy w zakresie wiedzy technicznej obejmującej terminologię, pojęcia, teorie, zasady, metody, techniki, narzędzia i materiały stosowane przy rozwiązywaniu zadań inżynierskich związanych z szeroko pojętym bezpieczeństwem i rozpoznawaniem zagrożeń, procesami planowania i realizacji eksperymentów, tak w procesie przygotowania z udziałem metod symulacji komputerowych, jak i w rzeczywistym środowisku
	Umiejętności
CU1	wyrobienie umiejętności w zakresie doskonalenia wiedzy, pozyskiwania i integrowanie informacji z literatury, baz danych i innych źródeł, opracowywania dokumentacji, prezentowania ich i podnoszenia kompetencji zawodowych
	Kompetencje społeczne
CK1	przygotowanie do uczenia się przez całe życie, podnoszenie kompetencji zawodowych, osobistych i społecznych w zmieniającej się rzeczywistości, podjęcia pracy związanej z funkcjonowaniem systemu bezpieczeństwa, którego głównym celem jest ratowanie i ochro-na życia, zdrowia i mienia przed zagrożeniami

E - Efekty kształcenia przedmiotowe i kierunkowe

Przedmiotowy efekt kształcenia (EP) w zakresie wiedzy (W), umiejętności (U) i kompetencji społecznych (K)		Kierunkowy efekt kształcenia
Wiedza (EPW…)		
EPW1	ma wiedzę ogólną obejmującą kluczowe zagadnienia bezpieczeństwa systemów, urządzeń i procesów	K_W05
EPW2	ma podstawową wiedzę niezbędną do rozumienia społecznych, ekonomicznych, prawnych i innych pozatechnicznych uwarunkowań działalności inżynierskiej	K_W17
Umiejętności (EPU…)		
EPU1	potrafi pozyskiwać informacje z literatury, baz danych i innych źródeł; potrafi integrować uzyskane informacje, dokonywać ich interpretacji, a także wyciągać wnioski oraz formułować i uzasadniać opinie	K_U01
EPU2	potrafi dostrzegać aspekty pozatechniczne, w tym środowiskowe, ekonomiczne i prawne przy projektowaniu, stosowaniu systemów zapewniających bezpieczeństwo systemów, sieci i urządzeń	K_U10
Kompetencje społeczne (EPK…)		
EPK1	potrafi myśleć i działać w sposób przedsiębiorczy m. in. tworząc rozwiązania z uwzględnieniem korzyści biznesowe oraz społeczne	K_K04
EPK2	prawidłowo identyfikuje i rozstrzyga dylematy związane z wykonywaniem zawodu	K_K06

F - Treści programowe oraz liczba godzin na poszczególnych formach zajęć

Lp.	Treści wykładów	Liczba godzin na studiach	
		stacjonarnych	niestacjonarnych
W1	Podstawowe definicje na temat polityki bezpieczeństwie informacji.	2	1
W2	Nowoczesne zagrożenia dla systemów i sieci komputerowych.	2	1
W3	Dostosowanie środków technicznych i IT do Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679.	2	1
W4	Dostępność, poufność i integralność systemów wg. normy ISO 27001.	2	1
W5	Uwierzytelnianie, autoryzacja i raportowanie. Zabezpieczanie systemów i urządzeń sieciowych.	2	1
W6	Społeczeństwo Informacyjne - normy i standardy w obszarze systemów zarządzania bezpieczeństwem informacji.	2	1
W7	Wstęp do kryptograficznej ochrona danych i systemów.	2	1
W8	Metody, narzędzia w uwierzytelnianiu i kontroli dostępu.	2	1
W9	Podatności przetwarzania danych i systemów e-Commerce	2	1
W10	Dostosowanie środków organizacyjnych i technicznych. Zarządzanie i planowanie polityki bezpieczeństwa informatycznego	2	1
W11	Dokumentacja ochrony danych osobowych i zarządzania bezpieczeństwem.	2	1
W12	Podejście oparte na ryzyku. Proces szacowania ryzyka.	2	1
W13	Jak stosować podejście oparte na ryzyku. Opis i klasyfikacja przetwarzanych danych.	2	1
W14	Polityka bezpieczeństwa i techniki zarządzania bezpieczeństwem systemów informatycznych.	2	1
W15	Zarządzanie bezpieczeństwem systemów informatycznych zgodnie z normą PN-I-13335-1	2	1
	Razem liczba godzin wykładów	30	15

Lp.	Treści laboratoriów	Liczba godzin na studiach	
		stacjonarnych	niestacjonarnych
L1	Infrastruktura systemów bezpieczeństwie informacji i testów penetracyjnych	2	1
L2	Konfigurowanie i obsługa środowiska Kali Linux	2	1
L3	Model OSI/ISO, analiza transmisji podstawowych protokołów komunikacyjnych m.in. TCP, UDP, FTP, DNS, HTTP	3	2
L4	Testy podatności systemu Android za pomocą narzędzia Metasploit	2	1
L5	Ocena luk w zabezpieczeniach, zarządzanie i badania za pomocą m in. buffer overflows, registers, shellcods, x32,x64 exploitation, gaining shell	2	1
L6	Symulacja ataku na klienta i serwer	2	2
L7	Rootkit w trybie użytkownika (usermode) lub systemu operacyjnego (kernel-mode	2	2
	Razem liczba godzin laboratoriów	15	10

Lp.	Treści projektów	Liczba godzin na studiach	
		stacjonarnych	niestacjonarnych
P1	Infrastruktura systemów bezpieczeństwie informacji i testów penetracyjnych – wprowadzenie do projektowania.	2	1
P2	Wytyczne do zarządzania bezpieczeństwem systemów informatycznych – Model ogólny.	2	1
P3	Tworzenie audytu systemu zarządzania bezpieczeństwem.	2	1
P4	Opracowanie środków organizacyjnych i technicznych zarządzania bezpieczeństwem informacji	2	1
P5	Wytyczne do zarządzania bezpieczeństwem systemów informatycznych – Zarządzanie i planowanie bezpieczeństwa informatycznego.	2	1
P6	Wytyczne do zarządzania bezpieczeństwem systemów informatycznych – Techniki zarządzania bezpieczeństwem systemów informatycznych.	2	2
P7	Analiza ryzyka i dokumentacja zarządzania bezpieczeństwem informacji. Część 1. Poufność.	2	1
P8	Analiza ryzyka i dokumentacja zarządzania bezpieczeństwem informacji. Część 2. Integralność.	2	1
P9	Analiza ryzyka i dokumentacja zarządzania bezpieczeństwem informacji. Część 3. Dostępność.	2	1
P10	Analiza ryzyka i dokumentacja zarządzania bezpieczeństwem informacji. Część 4. Macierz analizy ryzyka.	2	1
P11	Testy podatności systemu i zarządzanie bezpieczeństwem informacji. Część 1	2	1
P12	Testy podatności systemu i zarządzanie bezpieczeństwem informacji. Część 2	2	1
P13	Zachowanie poufności, integralności i dostępności zgodnie z normą ISO 27001 w projekcie zarządzania bezpieczeństwem informacji. Część 1	2	2
P14	Zachowanie poufności, integralności i dostępności zgodnie z normą ISO 27001 w projekcie zarządzania bezpieczeństwem informacji. Część 2	2	1
P15	Ocena dokumentacji projektu bezpieczeństwie wybranego systemu.	2	2
	Razem liczba godzin laboratoriów	30	18

G – Metody oraz środki dydaktyczne wykorzystywane w ramach poszczególnych form zajęć

Forma zajęć	**Metody dydaktyczne (wybór z listy)**	**Środki dydaktyczne**
Wykład	wykład informacyjny jako prelekcja z objaśnieniami połączone z dyskusją oraz możliwością prezentacji prac własnych zrealizowanych jako prezentacje z przeglądu literatury	projektor oraz komputer z dostępem do Internetu
Laboratoria	ćwiczenia doskonalące umiejętność pozyskiwania informacji ze źródeł internetowych i doskonalących obsługę narzędzi informatycznych oraz analiza sprawozdań przedstawionych przez studentów	Wyposażone dla celów zajęć z zakresu bezpieczeństwa komputerowego stanowisko komputerowe z dostępem do Internetu

H - Metody oceniania osiągnięcia efektów kształcenia na poszczególnych formach zajęć

Forma zajęć	**Ocena formująca (F) –** wskazuje studentowi na potrzebę uzupełniania wiedzy lub stosowania określonych metod i narzędzi, stymulujące do doskonalenia efektów pracy **(wybór z listy)**	**Ocena podsumowująca (P) –** podsumowuje osiągnięte efekty kształcenia **(wybór z listy)**
Wykład	F1 - sprawdzian pisemny (kolokwium cząstkowe testy z pytaniami wielokrotnego wyboru i pytaniami otwartymi) F4 – wystąpienie (prezentacja multimedialna, ustne formułowanie i rozwiązywanie problemu, wypowiedź problemowa)	P1 – egzamin (test sprawdzający wiedzę z całego przedmiotu)
Laboratoria	F2 – obserwacja/aktywność (przygotowanie do zajęć, ocena ćwiczeń wykonywanych podczas zajęć), F3 – praca pisemna (sprawozdanie, dokumentacja projektu, pisemna analiza problemu), F5 - ćwiczenia praktyczne (ćwiczenia z wykorzystaniem sprzętu i oprogramowania fachowego)	P3 – ocena podsumowująca powstała na podstawie ocen formujących, uzyskanych w semestrze oraz oceny sprawozdań jako pracy pisemnej
Projekt	F3 – dokumentacja projektu F4 – wystąpienie – analiza projektu	P4 – praca pisemna - projekt

H-1 Metody weryfikacji osiągnięcia przedmiotowych efektów kształcenia (wstawić „x")

Efekty przedmiotowe	Wykład			Laboratoria				Projekt		
	F1	F4	P1	F2	F3	F5	P3	F3	F4	P4
EPW1	x	x	x							
EPW2	x	x	x							
EPU1				x	x	x	x	x	x	x
EPU2				x	x	x	x	x	x	x
EPK1	x	x	x					x	x	x
EPK2	x	x	x							

I – Kryteria oceniania

Wymagania określające kryteria uzyskania oceny w danym efekcie			
Ocena			
Przedmiotowy efekt kształcenia (EP..)	**Dostateczny dostateczny plus 3/3,5**	**dobry dobry plus 4/4,5**	**bardzo dobry 5**
EPW1	Zna wybrane terminy oraz wybrane metody obejmujące kluczowe zagadnienia bezpieczeństwa systemów, urządzeń i procesów	Zna większość terminów oraz metod obejmujących kluczowe zagadnienia bezpieczeństwa systemów, urządzeń i procesów	Zna wszystkie wymagane terminy oraz metody obejmujące kluczowe zagadnienia bezpieczeństwa systemów, urządzeń i procesów
EPW2	ma niepełną wiedzę niezbędną do rozumienia społecznych, ekonomicznych, prawnych i innych pozatechnicznych uwarunkowań działalności inżynierskiej	ma podstawową wiedzę niezbędną do rozumienia społecznych, ekonomicznych, prawnych i innych pozatechnicznych uwarunkowań działalności inżynierskiej	ma niezbędna wiedzę niezbędną do rozumienia społecznych, ekonomicznych, prawnych i innych pozatechnicznych uwarunkowań działalności inżynierskiej
EPU1	Zna wybraną literaturę i niektóre portale internetowe związane z polityką bezpieczeństwa w firmie	Zna wybrane portale internetowe i czasopisma związane z polityką bezpieczeństwa w firmie	Zna wybrane portale internetowe, czasopisma oraz akty prawne obejmujące rozwiązania i normy związane z polityką bezpieczeństwa w firmie
EPU2	przeprowadzić symulację jak również zaprezentować wyniki analityczne dla niektórych z eksperymentów obejmujących zakres bezpieczeństwa systemu komputerowego	przeprowadzić symulację jak również zaprezentować wyniki analityczne dla większości eksperymentów obejmujących zakres bezpieczeństwa systemu komputerowego.	przeprowadzić symulację jak również zaprezentować wyniki analityczne dla większości eksperymentów obejmujących zakres bezpieczeństwa systemu komputerowego.
EPK1	potrafi myśleć i działać w sposób przedsiębiorczy m. in. tworząc wybrane rozwiązania z uwzględnieniem korzyści biznesowe oraz społeczne	potrafi myśleć i działać w sposób przedsiębiorczy m. in. tworząc wybrane rozwiązania z uwzględnieniem korzyści biznesowe oraz społeczne	potrafi myśleć i działać w sposób przedsiębiorczy m. in. tworząc niezbędne rozwiązania z uwzględnieniem korzyści biznesowe oraz społeczne
EPK2	prawidłowo identyfikuje i rozstrzyga niektóre dylematy związane z wykonywaniem zawodu	prawidłowo identyfikuje i rozstrzyga większość dylematów związanych z wykonywaniem zawodu	prawidłowo identyfikuje i rozstrzyga wszystkie znane i omawiane jak również inne nowo opublikowane dylematy związane z wykonywaniem zawodu

J – Forma zaliczenia przedmiotu

Wykład - egzamin (test)

Laboratorium – zaliczenie z oceną. Na ocenę składa się oddanie min. 7 sprawozdawań, z laboratorium które są podstawą przystąpienia do kolokwium zaliczeniowego.

Projekt– zaliczenie z oceną. Ocenie podlegać będzie projekt polityka bezpieczeństwa w wybranej firmie.

Kryteria ocen dla wykładu, projektu i laboratorium:

0-50 % – niedostateczna
51-60 % – dostateczna
61-70 % – dostateczna plus
71-80 % - dobry
81-90 % dobry plus
91-100 % bardzo dobry

K – Literatura przedmiotu

Literatura obowiązkowa:

1. J. Luttgens, M. Pepe, K. Mandia, Incydenty bezpieczeństwa. Metody reagowania w informatyce śledczej, Helion 2016
2. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)

Literatura zalecana / fakultatywna:

1. W. Stallings, Kryptografia i bezpieczeństwo sieci komputerowych. Matematyka szyfrów i techniki kryptologii, Helion 2012
2. Ross, Inżynieria Zabezpieczeń, WNT, Warszawa 2005

L – Obciążenie pracą studenta:

Forma aktywności studenta	Liczba godzin na realizację	
	na studiach stacjonarnych	na studiach niestacjonarnych
Godziny zajęć z nauczycielem/ami	75	43
Konsultacje	5	5
Czytanie literatury	10	35
Przygotowanie sprawozdań	5	12
Przygotowanie do egzaminu	10	10
Przygotowanie do laboratorium	20	20
Suma godzin:	**125**	**125**
Liczba punktów ECTS dla przedmiotu (suma godzin: 25 godz.):	**5**	**5**

Ł – Informacje dodatkowe

Imię i nazwisko sporządzającego	Łukasz Lemieszewski
Data sporządzenia / aktualizacji	27 czerwca 2019 r.
Dane kontaktowe (e-mail, telefon)	llemieszewski@ajp.edu.pl
Podpis	

Pozycja w planie studiów (lub kod przedmiotu)	C.2.3.

	Wydział	Techniczny
	Kierunek	Inżynieria bezpieczeństwa
	Poziom studiów	Studia pierwszego stopnia
	Forma studiów	Stacjonarne / Niestacjonarne
	Profil kształcenia	Profil praktyczny

PROGRAM PRZEDMIOTU/MODUŁU

A - Informacje ogólne

1. Nazwa przedmiotu	**Kryptografia i kryptoanaliza**
2. Punkty ECTS	**5**
3. Rodzaj przedmiotu	**Obowiązkowy**
4. Język przedmiotu	**język polski**
5. Rok studiów	**II**
6. Imię i nazwisko koordynatora przedmiotu oraz prowadzących zajęcia	**Pracownicy WT AJP**

B – Formy dydaktyczne prowadzenia zajęć i liczba godzin w semestrze

Nr semestru	Studia stacjonarne	Studia niestacjonarne
Semestr 4	**W**: 30; **Cw.** 15, **Proj.**: 30;	**W**: 15; **Cw.** 10, **Proj.**: 18;
Liczba godzin ogółem	**75**	**43**

C - Wymagania wstępne

Wiadomości z kursów na temat projektowania i analizy sieci oraz polityki bezpieczeństwa w firmie

D - Cele kształcenia

	Wiedza
CW1	Przekazanie wiedzy w zakresie wiedzy technicznej obejmującej terminologię, pojęcia, teorie, zasady, metody, techniki, narzędzia i materiały stosowane przy rozwiązywaniu zadań inżynierskich związanych z szeroko pojętym bezpieczeństwem i rozpoznawaniem zagrożeń, procesami planowania i realizacji eksperymentów, tak w procesie przygotowania z udziałem metod symulacji komputerowych, jak i w rzeczywistym środowisku.
CW2	Przekazanie wiedzy ogólnej dotyczącej standardów i norm technicznych dotyczących zagadnień inżynierii bezpieczeństwa systemów, urządzeń, procesów, i związanych z tym technik i metod programowania, szyfrowania danych, zarządzania jakością i analizy ryzyka
	Umiejętności
CU1	Wyrobienie umiejętności w zakresie doskonalenia wiedzy, pozyskiwania i integrowanie informacji z literatury, baz danych i innych źródeł, opracowywania dokumentacji, prezentowania ich i podnoszenia kompetencji zawodowych
CU2	Wyrobienie umiejętności projektowania i monitorowania stanu i warunków bezpieczeństwa: wykonywania analiz bezpieczeństwa i ryzyka, kontrolowania przestrzegania przepisów i zasad bezpieczeństwa, kontrolowania warunków pracy i standardów bezpieczeństwa, prowadzenia badań

	okoliczności awarii i wypadków, prowadzenia szkoleń, pełnienia funkcji organizatorskich w zakresie zarządzania bezpieczeństwem oraz prowadzenia dokumentacji związanej z szeroko rozumianym bezpieczeństwem

Kompetencje społeczne	
CK1	Przygotowanie do uczenia się przez całe życie, podnoszenie kompetencji zawodowych, osobistych i społecznych w zmieniającej się rzeczywistości, podjęcia pracy związanej z funkcjonowaniem systemu bezpieczeństwa, którego głównym celem jest ratowanie i ochrona życia, zdrowia i mienia przed zagrożeniami
CK2	Uświadomienie ważności i rozumienia społecznych skutków działalności inżynierskiej, w tym jej wpływu na środowisko i związanej z tym odpowiedzialności za podejmowane decyzje, współdziałanie w grupie i przyjmowanie odpowiedzialności za wspólne realizacje, kreatywność i przedsiębiorczość oraz potrzebę przekazywania informacji odnośnie osiągnięć technicznych i działania inżyniera.

E - Efekty kształcenia przedmiotowe i kierunkowe

Efekty kształcenia (E) w zakresie wiedzy (W), umiejętności (U) i kompetencji społecznych (K)		Kierunkowy efekt kształcenia
Wiedza (EW…)		
EPW1	Student, który zaliczył przedmiot ma elementarną wiedzę z zakresu podstaw informatyki obejmującą przetwarzanie informacji, architekturę i organizację systemów komputerowych, bezpieczeństwo systemów komputerowych, budowę sieci i aplikacji sieciowych	K_W04
EPW2	Student, który zaliczył przedmiot ma wiedzę ogólną obejmującą kluczowe zagadnienia bezpieczeństwa systemów, urządzeń i procesów	K_W05
Umiejętności (EU…)		
EPU1	Student, który zaliczył przedmiot potrafi pozyskiwać informacje z literatury, baz danych i innych źródeł; potrafi integrować uzyskane informacje, dokonywać ich interpretacji, a także wyciągać wnioski oraz formułować i uzasadniać opinie	K_U01
EPU2	Student, który zaliczył przedmiot potrafi posłużyć się właściwie dobranymi metodami i urządzeniami umożliwiającymi zapewnienie bezpieczeństwa systemów i urządzeń	K_U19
Kompetencje społeczne (EK…)		
EPK1	Student, który zaliczył przedmiot ma świadomość ważności i rozumie skutki działalności inżynierskiej oraz związanej z tym odpowiedzialności za podejmowane decyzje	K_K02

F - Treści programowe oraz liczba godzin na poszczególnych formach zajęć

Lp.	Treści wykładów	Liczba godzin na studiach	
		stacjonarnych	niestacjonarnych
W1	Wprowadzenie	2	1
W2	Kryptologia – podstawowe definicje i pojęcia	2	1
W3	Kryptografia– podstawowe definicje i pojęcia	2	1
W4	Klasyfikacje systemów kryptologicznych	2	1
W5	Klasyfikacje systemów kryptograficznych	2	1
W6	Generatory ciągów pseudolosowych – zasada działania	2	2
W7	Generatory ciągów pseudolosowych – wykorzystanie w technikach zapewnienia bezpieczeństwa informacji	2	1
W8	Wybrane zagadnienia z teorii informacji.	2	1
W9	Wybrane zagadnienia z teorii liczb.	2	2
W10	Podatność na kryptoanalizę i zasady bezpieczeństwa	2	2
W11	Metody kryptoanalizy	2	1
W12	Metody łamania zabezpieczeń	2	1
W13	Kryptografia z kluczami jednorazowymi – charakterystyka ogólna	2	1
W14	Kryptografia z kluczami jednorazowymi - przykłady	2	1

W15	Podsumowanie przedmiotu i przygotowanie do zaliczenia	2	1
	Razem liczba godzin wykładów:	**30**	**18**

Lp.	**Treści ćwiczeń**	**Liczba godzin na studiach**	
		stacjonarnych	**niestacjonarnych**
C1	Synchroniczne szyfrowanie strumieniowe	2	1
C2	Samosynchronizujące (asynchroniczne) szyfrowanie strumieniowe	2	1
C3	Generatory ciągów pseudolosowych	2	1
C4	Rejestr przesuwający z liniowym sprzężeniem zwrotnym (LFSR)	2	1
C5	Generatory sterowane zegarem	2	1
C6	Podpis z wykorzystaniem jednokierunkowej funkcji haszującej .	2	2
C7	Niezaprzeczalne podpisy cyfrowe	2	2
C8	Kolokwium	1	1
	Razem liczba godzin ćwiczeń:	**15**	**10**

Lp.	**Treści projektów**	**Liczba godzin na studiach**	
		stacjonarnych	**niestacjonarnych**
P1	Wprowadzenie do realizacji samodzielnych zadań projektowych	2	1
P2	Prezentacja tematyki projektów	2	1
P3	Omówienie zasad przygotowywania prezentacji, przykłady.	2	1
P4	Omówienie zasad prowadzenia prezentacji, przykłady	2	1
P5	Opracowanie listy tematów projektowych i dyskusja	2	1
P6	Przydział tematów projektowych	2	1
P7	Realizacja szkicu projektu w grupach	2	1
P8	Prezentacja szkiców projektów, dyskusja	2	1
P9	Realizacja skorygowanych wersji szkiców projektów	2	2
P10	Prezentacja skorygowanych szkiców projektów, dyskusja	2	1
P11	Realizacja projektów cz. 1	2	1
P12	Realizacja projektów cz. 2	2	1
P13	Prezentacja projektów cz. 1	2	2
P14	Prezentacja projektów cz. 2	2	2
P15	Podsumowanie i zaliczenie przedmiotu	2	1
	Razem liczba godzin projektów	30	18

G – Metody oraz środki dydaktyczne wykorzystywane w ramach poszczególnych form zajęć

Forma zajęć	**Metody dydaktyczne (wybór z listy)**	**Środki dydaktyczne**
Wykład	Wykład informacyjny Wykład problemowy połączony z dyskusją	Komputer i projektor multimedialny, tablica suchościeralna
Projekt	Realizacja zadania inżynierskiego w grupie, Doskonalenie metod i technik analizy zadania inżynierskiego, Selekcjonowanie, grupowanie i dobór informacji do realizacji zadania inżynierskiego,	Komputer i projektor multimedialny, tablica suchościeralna Sala komputerowa z dostępem do internetu

H - Metody oceniania osiągnięcia efektów kształcenia na poszczególnych formach zajęć

Forma zajęć	**Ocena formująca (F) –** wskazuje studentowi na potrzebę uzupełniania wiedzy lub stosowania określonych metod i narzędzi, stymulujące do doskonalenia efektów pracy **(wybór z listy)**	**Ocena podsumowująca (P) –** podsumowuje osiągnięte efekty kształcenia **(wybór z listy)**
Wykład	F2 – obserwacja/aktywność	P1 – egzamin
Ćwiczenia	F2 – obserwacja/aktywność (przygotowanie do zajęć,	P3 – ocena podsumowująca

	ocena ćwiczeń wykonywanych podczas zajęć), F3 – praca pisemna (sprawozdanie, dokumentacja projektu, pisemna analiza problemu), F5 - ćwiczenia praktyczne (ćwiczenia z wykorzystaniem sprzętu i oprogramowania fachowego)	powstała na podstawie ocen formujących, uzyskanych w semestrze oraz oceny sprawozdań jako pracy pisemnej
Projekt	F4 – wystąpienie	P3 – ocena podsumowująca powstała na podstawie ocen formujących, uzyskanych w semestrze

H-1 Metody weryfikacji osiągnięcia przedmiotowych efektów kształcenia (wstawić „x")

Efekty przedmiotowe	Wykład		Projekt		Ćwiczenia		
	F2	P1	F4	P3	F2	F3	F5
EPW1	x	x			x	x	x
EPW2	x	x			x	x	x
EPU1			x	x			
EPU2			x	x			
EPK1	x	x			x	x	x

I – Kryteria oceniania

Wymagania określające kryteria uzyskania oceny w danym efekcie			
Ocena			
Przedmiotowy efekt kształcenia (EP..)	**Dostateczny , dostateczny plus 3/3,5**	**Dobry, dobry plus 4/4,5**	**bardzo dobry 5**
EPW1	Student opanował w stopniu podstawowym elementarną wiedzę z zakresu podstaw informatyki obejmującą przetwarzanie informacji, architekturę i organizację systemów komputerowych, bezpieczeństwo systemów komputerowych, budowę sieci i aplikacji sieciowych	Student opanował w stopniu dobrym elementarną wiedzę z zakresu podstaw informatyki obejmującą przetwarzanie informacji, architekturę i organizację systemów komputerowych, bezpieczeństwo systemów komputerowych, budowę sieci i aplikacji sieciowych	Student w pełni opanował elementarną wiedzę z zakresu podstaw informatyki obejmującą przetwarzanie informacji, architekturę i organizację systemów komputerowych, bezpieczeństwo systemów komputerowych, budowę sieci i aplikacji sieciowych
EPW2	Student ma podstawową wiedzę ogólną obejmującą kluczowe zagadnienia bezpieczeństwa systemów, urządzeń i procesów	Student ma ugruntowaną wiedzę ogólną obejmującą kluczowe zagadnienia bezpieczeństwa systemów, urządzeń i procesów	Student ma bardzo dobrą wiedzę ogólną obejmującą kluczowe zagadnienia bezpieczeństwa systemów, urządzeń i procesów
EPU1	Student potrafi w stopniu elementarnym pozyskiwać informacje z literatury, baz danych i innych źródeł; potrafi integrować uzyskane informacje, dokonywać ich interpretacji, a także wyciągać wnioski oraz formułować i uzasadniać opinie	Student potrafi w stopniu dobrym pozyskiwać informacje z literatury, baz danych i innych źródeł; potrafi integrować uzyskane informacje, dokonywać ich interpretacji, a także wyciągać wnioski oraz formułować i uzasadniać opinie	Student potrafi efektywnie pozyskiwać informacje z literatury, baz danych i innych źródeł; potrafi integrować uzyskane informacje, dokonywać ich interpretacji, a także wyciągać wnioski oraz formułować i uzasadniać opinie
EPU2	Student potrafi w zakresie elementarnym posłużyć się właściwie dobranymi metodami i urządzeniami umożliwiającymi zapewnienie bezpieczeństwa systemów i urządzeń	Student potrafi w stopniu dobrym posłużyć się właściwie dobranymi metodami i urządzeniami umożliwiającymi zapewnienie bezpieczeństwa systemów i urządzeń	Student potrafi efektywnie posłużyć się właściwie dobranymi metodami i urządzeniami umożliwiającymi zapewnienie bezpieczeństwa systemów i urządzeń

EPK1	Student ma podstawową świadomość ważności i zrozumienie skutków działalności inżynierskiej oraz związanej z tym odpowiedzialności za podejmowane decyzje	Student ma zadowalającą świadomość ważności i zrozumienie skutków działalności inżynierskiej oraz związanej z tym odpowiedzialności za podejmowane decyzje	Student ma ugruntowaną świadomość ważności i zrozumienie skutków działalności inżynierskiej oraz związanej z tym odpowiedzialności za podejmowane decyzje

J – Forma zaliczenia przedmiotu

Wykład - egzamin (test)

Laboratorium – zaliczenie z oceną. Na ocenę składa się oddanie min. 7 sprawozdawań, z laboratorium które są podstawą przystąpienia do kolokwium zaliczeniowego.

Ćwiczenia– zaliczenie z oceną. Kolokwium.

Kryteria ocen dla wykładu, projektu i ćwiczeń:

0-50 % – niedostateczna
51-60 % – dostateczna
61-70 % – dostateczna plus
71-80 % - dobry
81-90 % dobry plus
91-100 % bardzo dobry

K – Literatura przedmiotu

Literatura obowiązkowa:

1. C. Adams, S. Lloyd, Podpis elektroniczny. Klucz publiczny, Robomatic, Wrocław 2002.
2. A. J. Menezes, P.C. van Oorschot, S.A Vanstone, Handbook of Applied Cryptography (dostęp: 16.12.2019) https://doc.lagout.org/network/3_Cryptography/CRC%20Press%20-%20Handbook%20of%20applied%20Cryptography.pdf
3. A. Ross, Inżynieria Zabezpieczeń, WNT, Warszawa 2005

Literatura zalecana / fakultatywna:

1. A. Szeląg, Windows Server 2008. Infrastruktura klucza publicznego (PKI), Helion, Gliwice 2008.
2. Rozporządzenie z dnia 7 sierpnia 2002 r. w sprawie określenia warunków technicznych i organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego (Dz.U. 2002 nr 128 poz.1094).
3. Podpis elektroniczny https://www.infor.pl/prawo/encyklopedia-prawa/p/272057,Podpis-elektroniczny.html [dostęp: 08.12.2019]

L – Obciążenie pracą studenta:

Forma aktywności studenta	Liczba godzin na realizację	
	na studiach stacjonarnych	na studiach niestacjonarnych
Godziny zajęć z nauczycielem/ami	75	43
Konsultacje	5	5
Czytanie literatury	10	27
Przygotowanie do zajęć projektowych	5	10
Przygotowanie projektu	10	15
Przygotowanie do kolokwium	10	15
Przygotowanie do egzaminu	10	10
Suma godzin:	**125**	**125**
Liczba punktów ECTS dla przedmiotu (suma godzin : 25 godz.):	**5**	**5**

Ł – Informacje dodatkowe

Imię i nazwisko sporządzającego	Pracownicy Wydziału Technicznego AJP
Data sporządzenia / aktualizacji	27 czerwca 2019 r.
Dane kontaktowe (e-mail, telefon)	wt@ajp.edu.pl
Podpis	

Pozycja w planie studiów (lub kod przedmiotu)	C.2.4

Wydział	Techniczny
Kierunek	Informatyka
Poziom studiów	Pierwszego stopnia
Forma studiów	stacjonarne/niestacjonarne
Profil kształcenia	Praktyczny

PROGRAM PRZEDMIOTU/MODUŁU

A - Informacje ogólne

1. Nazwa przedmiotu	**Ataki i wykrywanie włamań w sieciach**
2. Punkty ECTS	**5**
3. Rodzaj przedmiotu	**Obowiązkowy**
4. Język przedmiotu	**Język polski**
5. Rok studiów	**II**
6. Imię i nazwisko koordynatora przedmiotu oraz prowadzących zajęcia	**Łukasz Lemieszewski**

B – Formy dydaktyczne prowadzenia zajęć i liczba godzin w semestrze

Nr semestru	Studia stacjonarne	Studia niestacjonarne
Semestr 4	**Wykłady**: (30); **Laboratoria**: (15); **Projekt:** (30)	**Wykłady**: (15); **Laboratoria**: (10); **Projekt:** (18)
Liczba godzin ogółem	**75**	**43**

C - Wymagania wstępne

Student nabył podstawową wiedzę z zakresu systemów operacyjnych oraz sieci komputerowych i bezpieczeństwa informacji

D - Cele kształcenia

	Wiedza
CW1	przekazanie wiedzy w zakresie wiedzy technicznej obejmującej terminologię, pojęcia, teorie, zasady, metody, techniki i narzędzia stosowane przy rozwiązywaniu zadań inżynierskich związanych z szeroko pojętą informatyką, procesami planowania i realizacji systemów informatycznych, eksperymentów, tak w procesie przygotowania z udziałem metod symulacji komputerowych, jak i w rzeczywistym środowisku
Umiejętności	
CU1	wyrobienie umiejętności w zakresie doskonalenia wiedzy, pozyskiwania i integrowanie informacji z literatury, baz danych i innych źródeł, opracowywania dokumentacji, prezentowania ich i podnoszenia kompetencji zawodowych
CU2	wyrobienie umiejętności posługiwania się specjalistycznym oprogramowaniem, projektowania systemów, sieci i aplikacji, programowania aplikacji, modelowania systemów, posługiwania się zaawansowanymi środowiskami projektowo-uruchomieniowymi, stosowania nowoczesnych urządzeń i podzespołów peryferyjnych
Kompetencje społeczne	
CK1	przygotowanie do uczenia się przez całe życie, podnoszenie kompetencji zawodowych, osobistych i społecznych w zmieniającej się rzeczywistości, podjęcia pracy związanej z obsługą sprzętu

	informatycznego, programowaniem i praktycznym posługiwaniem się szerokim spektrum narzędzi informatycznych

E - Efekty kształcenia przedmiotowe i kierunkowe

Przedmiotowy efekt kształcenia (EP) w zakresie wiedzy (W), umiejętności (U) i kompetencji społecznych (K)		Kierunkowy efekt kształcenia
Wiedza (EPW…)		
EPW1	ma wiedzę ogólną obejmującą kluczowe zagadnienia bezpieczeństwa systemów, urządzeń i procesów	K_W05
EPW2	zna podstawowe narzędzia, metody i techniki identyfikacji i analizy zagrożeń	K_W07
Umiejętności (EPU…)		
EPU1	potrafi pozyskiwać informacje z literatury, baz danych i innych źródeł; potrafi integrować uzyskane informacje, dokonywać ich interpretacji, a także wyciągać wnioski oraz formułować i uzasadniać opinie	K_U01
EPU2	potrafi opracować dokumentację dotyczącą realizacji zadania inżynierskiego i przygotować tekst zawierający omówienie wyników realizacji tego zadania	K_U03
EPU3	potrafi ocenić ryzyko i bezpieczeństwo baz danych, aplikacji internetowych, systemów i sieci komputerowych, stosując techniki oraz narzędzia sprzętowe i programowe	K_U12
Kompetencje społeczne (EPK…)		
EPK1	rozumie potrzebę uczenia się przez całe życie	K_K01
EPK2	ma świadomość ważności i rozumie pozatechniczne aspekty i skutki działalności inżynierskiej, w tym jej wpływu na środowisko, i związanej z tym odpowiedzialności za podejmowane decyzje	K_K02
EPK3	prawidłowo identyfikuje i rozstrzyga dylematy związane z wykonywaniem zawodu	K_K06

F - Treści programowe oraz liczba godzin na poszczególnych formach zajęć

Lp.	Treści wykładów	Liczba godzin na studiach	
		stacjonarnych	niestacjonarnych
W1	Program nauczania, zasady zaliczenia oraz podstawowe informacje o przedmiocie. Metodologia projektowania lokalnej sieci komputerowej.	2	1
W2	Nowoczesne zagrożenia dla sieci komputerowych	2	1
W3	Zabezpieczanie urządzeń sieciowych	2	1
W4	Techniki i algorytmy szyfrowania danych. Metody ataku na szyfry.	2	1
W5	Rodzaje ataków sieciowych. Anatomia ataku na sieć lub system informatyczny.	2	1
W6	Rejestracja i uwierzytelnianie użytkowników w systemach informatycznych.	2	1
W7	Techniki szyfrowania haseł i ataków na hasła. Tęczowe tablice.	2	1
W8	Uwierzytelnianie, Autoryzacja i Raportowanie	2	1
W9	Zastosowanie kryptografii asymetrycznej w szyfrowaniu danych przesyłanych w sieciach.	2	1
W10	Podnoszenie bezpieczeństwa sieci –firewall, WPA2, VLAN, etc.	2	1
W11	Zabezpieczenie sieci lokalnej	2	1
W12	Systemy kryptograficzne	2	1
W13	Implementacja Wirtualnej Sieci Prywatnej	2	1
W14	Zarządzanie zabezpieczeniami sieciowymi	2	1

W15	Zaliczenie	2	1
	Razem liczba godzin wykładów	30	15

Lp.	**Treści laboratoriów**	**Liczba godzin na studiach**	
		stacjonarnych	**niestacjonarnych**
L1	Obliczanie zadań z zakresu szyfrów podstawieniowych i przestawieniowych.	2	1
L2	Ataki na dane zabezpieczone szyframi podstawieniowymi i przestawieniowymi.	2	1
L3	Atak na system uwierzytelniający z wykorzystaniem tęczowych tablic.	2	1
L4	Atak na sieć lokalną z wykorzystaniem oprogramowania Wireshark. „Podsłuchiwanie" i analiza pakietów sieciowych	2	2
L5	Analiza bezpieczeństwa sieci/systemu z wykorzystaniem oprogramowania LAN Guard.	2	1
L6	Zwiększanie bezpieczeństwa sieci z wykorzystaniem switch'a zarządzalnego poprzez wydzielanie wirtualnych sieci lokalnych (VLAN)	2	2
L7	Ataki na sieci WLAN. Zaliczenie.	3	2
	Razem liczba godzin laboratoriów	15	10

Lp.	**Treści projektów**	**Liczba godzin na studiach**	
		stacjonarnych	**niestacjonarnych**
P1	Założenia do projektów i opracowanie harmonogramu.	1	1
P2	Przygotowanie schematu połączenia odległych lokacji z zastosowaniem technik szyfrowania danych	4	2
P3	Przygotowanie schematu połączenia węzłów sieci w budynku zgodnie z obowiązującymi standardami dotyczącymi bezpieczeństwa.	5	3
P4	Opracowanie schematu graficznego sieci z wykorzystaniem narzędzi wspomagających projektowanie.	5	3
P5	Realizacja projektu sieci komputerowej typu LAN i WAN z wyborem medium transmisyjnego (przewodowego, bezprzewodowego), sieciowych protokołów komunikacyjnych i doboru urządzeń z zachowaniem mechanizmów bezpieczeństwa zewnętrznego i wewnętrznego.	15	9
	Razem liczba godzin projektów	30	18

G – Metody oraz środki dydaktyczne wykorzystywane w ramach poszczególnych form zajęć

Forma zajęć	**Metody dydaktyczne (wybór z listy)**	**Środki dydaktyczne**
Wykład	M1 - wykład informacyjny, M3 – pokaz multimedialny	projektor, prezentacja multimedialna
Laboratoria	M5 - ćwiczenia doskonalące obsługę programów do projektowania sieci i analizowania sieciowych protokołów komunikacyjnych.	jednostka komputerowa wyposażona w oprogramowanie oraz z dostępem do sieci Internetu
Projekt	M5 - ćwiczenia doskonalące obsługę programów do projektowania sieci i analizowania sieciowych protokołów komunikacyjnych.	Jednostka komputerowa wyposażona w oprogramowanie oraz z dostępem do sieci Internetu

H - Metody oceniania osiągnięcia efektów kształcenia na poszczególnych formach zajęć

Forma zajęć	**Ocena formująca (F) –** wskazuje studentowi na potrzebę uzupełniania wiedzy lub stosowania określonych metod i narzędzi, stymulujące do doskonalenia efektów pracy **(wybór z listy)**	**Ocena podsumowująca (P) –** podsumowuje osiągnięte efekty kształcenia **(wybór z listy)**

Wykład	F2 - obserwacja poziomu przygotowania do zajęć	P2 – kolokwium podsumowujące semestr
Laboratoria	F2 – obserwacja/aktywność (przygotowanie do zajęć, ocena ćwiczeń wykonywanych podczas zajęć), F3 – praca pisemna (sprawozdanie), F5 - ćwiczenia praktyczne (ćwiczenia sprawdzające umiejętności).	P2 – kolokwium praktyczne
Projekt	F3 – dokumentacja projektu F4 – wystąpienie – analiza projektu	P4 – praca pisemna - projekt

H-1 Metody weryfikacji osiągnięcia przedmiotowych efektów kształcenia (wstawić „x")

Efekty przedmiotowe	Wykład		Laboratoria				Projekt		
	F2	P1	F2	F3	F5	P2	F3	F4	P4
EPW1	x	x	x						
EPW2	x	x	x						
EPU1				x	x	x	x	x	x
EPU2				x	x	x	x	x	x
EPU3				x	x	x	x	x	x
EPK1	x	x	x						
EPK2	x	x	x						
EPK3	x	x	x						

Wymagania określające kryteria uzyskania oceny w danym efekcie			
Ocena			
Przedmiotowy efekt kształcenia (EP..)	**Dostateczny dostateczny plus 3/3,5**	**dobry dobry plus 4/4,5**	**bardzo dobry 5**
EPW1	potrafi wskazać i poddać analizie wybrane protokoły komunikacyjne w sieci	potrafi wskazać i poddać analizie większość protokołów komunikacyjnych w sieci	potrafi wskazać i poddać analizie wszystkie protokołów komunikacyjne w sieci
EPW2	potrafi zdefiniować wybrane pojęcia z zakresu projektowania sieci komputerowych	potrafi zdefiniować większość pojęć z zakresu projektowania sieci komputerowych	potrafi zdefiniować wszystkie pojęcia z zakresu projektowania sieci komputerowych
EPU1	potrafi korzystać z wiedzy na temat analizy i projektowania prostych pod względem skomplikowania sieci komputerowych, zawartej w literaturze, internetowych bazach danych i innych źródeł	potrafi korzystać z wiedzy na temat analizy i projektowania średniozaawansowanych pod względem skomplikowania sieci komputerowych, zawartej w literaturze, internetowych bazach danych i innych źródeł	potrafi korzystać z wiedzy na temat analizy i projektowania zaawansowanych pod względem skomplikowania sieci komputerowych, zawartej w literaturze, internetowych bazach danych i innych źródeł
EPU2	potrafi opracować dokumentację prostej pod względem skomplikowania zaprojektowanej sieci komputerowej	potrafi opracować dokumentację średniozaawansowanej pod względem skomplikowania zaprojektowanej sieci komputerowej	potrafi opracować pełną dokumentację zaprojektowanej sieci komputerowej

EPU3	potrafi ocenić ryzyko i bezpieczeństwo zaprojektowanej sieci na podstawie analizy wybranego sieciowego protokołów komunikacyjnych	potrafi w ocenić ryzyko i bezpieczeństwo zaprojektowanej sieci na podstawie analizy podstawowych sieciowych protokołów komunikacyjnych	potrafi w ocenić ryzyko i bezpieczeństwo zaprojektowanej sieci na podstawie analizy wszystkich sieciowych protokołów komunikacyjnych
EPK1	rozumie w podstawowym stopniu potrzebę ciągłego kształcenia z zakresu analizy i projektowania sieci	rozumie potrzebę ciągłego kształcenia z zakresu analizy i projektowania sieci	rozumie potrzebę ciągłego kształcenia z zakresu analizy i projektowania sieci oraz rozumie skutki takiego postępowania
EPK2	potrafi określać niektóre priorytety niezbędne przy analizie sieciowych protokołów komunikacyjnych i projektowaniu komunikacji w sieci	potrafi określać większość priorytetów niezbędnych przy analizie sieciowych protokołów komunikacyjnych i projektowaniu komunikacji w sieci	potrafi określać wszystkie priorytety niezbędnych przy analizie sieciowych protokołów komunikacyjnych i projektowaniu komunikacji w sieci
EPK3	potrafi w słabym stopniu kreatywnie projektować i analizować proste sieci	potrafi w słabym stopniu kreatywnie projektować i analizować proste sieci	potrafi w słabym stopniu kreatywnie projektować i analizować proste sieci

J – Forma zaliczenia przedmiotu

Wykład - zaliczenie z oceną (test)

Laboratorium – zaliczenie z oceną. Na ocenę składa się oddanie min. 7 sprawozdawań, z laboratorium które są podstawą przystąpienia do kolokwium zaliczeniowego.

Projekt– zaliczenie z oceną. Ocenie podlegać będzie projekt testów penetracyjnych.

Kryteria ocen dla wykładu, projektu i laboratorium:

0-50 % – niedostateczna
51-60 % – dostateczna
61-70 % – dostateczna plus
71-80 % - dobry
81-90 % dobry plus
91-100 % bardzo dobry

K – Literatura przedmiotu

Literatura obowiązkowa:

4. Chris Sanders, Praktyczna analiza pakietów. Wykorzystanie narzędzia Wireshark do rozwiązywania problemów z siecią. Helion, Gliwice 2013
5. Stanisław Wszelak, Administrowanie sieciowymi protokołami komunikacyjnymi, Helion, Gliwice 2015

Literatura zalecana / fakultatywna:

3. Engebretson P., Hacking i testy penetracyjne. Podstawy, Helion, 2013
4. Barrie Sosinsky, Sieci komputerowe. Biblia, Helion, 2011

L – Obciążenie pracą studenta:

Forma aktywności studenta	Liczba godzin na realizację	
	na studiach stacjonarnych	na studiach niestacjonarnych
Godziny zajęć z nauczycielem/ami	75	43
Konsultacje	5	5
Czytanie literatury	10	27
Przygotowanie sprawozdań	10	20
Przygotowanie projektów	15	15

Przygotowanie do zaliczenia wykładu	10	15
Suma godzin:	**125**	**125**
Liczba punktów ECTS dla przedmiotu (suma godzin : 25 godz.):	**5**	**5**

Ł – Informacje dodatkowe

Imię i nazwisko sporządzającego	Łukasz Lemieszewski
Data sporządzenia / aktualizacji	8 grudzień 2019 r.
Dane kontaktowe (e-mail, telefon)	llemieszewski@ajp.edu.pl
Podpis	

Pozycja w planie studiów (lub kod przedmiotu)	C.2.5.

Wydział	Techniczny
Kierunek	Inżynieria bezpieczeństwa
Poziom studiów	Studia pierwszego stopnia
Forma studiów	Stacjonarne / Niestacjonarne
Profil kształcenia	Profil praktyczny

PROGRAM PRZEDMIOTU/MODUŁU

A - Informacje ogólne

1. Nazwa przedmiotu	**Problemy bezpieczeństwa w inżynierii oprogramowania**
2. Punkty ECTS	**5**
3. Rodzaj przedmiotu	**Obowiązkowy**
4. Język przedmiotu	**język polski**
5. Rok studiów	**II**
6. Imię i nazwisko koordynatora przedmiotu oraz prowadzących zajęcia	**Pracownicy WT AJP**

B – Formy dydaktyczne prowadzenia zajęć i liczba godzin w semestrze

Nr semestru	Studia stacjonarne	Studia niestacjonarne
Semestr 4	**W**: 30; **Lab.**: 30; **Proj.**: 15	**W**: 15; **Lab.**: 18; **Proj.**: 10
Liczba godzin ogółem	**75**	**43**

C - Wymagania wstępne

Podstawy algorytmiki i programowania

D - Cele kształcenia

	Wiedza
CW1	Przekazanie wiedzy w zakresie wiedzy technicznej obejmującej terminologię, pojęcia, teorie, zasady, metody, techniki, narzędzia i materiały stosowane przy rozwiązywaniu zadań inżynierskich związanych z szeroko pojętym bezpieczeństwem i rozpoznawaniem zagrożeń, procesami planowania i realizacji eksperymentów, tak w procesie przygotowania z udziałem metod symulacji komputerowych, jak i w rzeczywistym środowisku.
CW2	Przekazanie wiedzy ogólnej dotyczącej standardów i norm technicznych dotyczących zagadnień inżynierii bezpieczeństwa systemów, urządzeń, procesów, i związanych z tym technik i metod programowania, szyfrowania danych, zarządzania jakością i analizy ryzyka
	Umiejętności
CU1	Wyrobienie umiejętności w zakresie doskonalenia wiedzy, pozyskiwania i integrowanie informacji z literatury, baz danych i innych źródeł, opracowywania dokumentacji, prezentowania ich i podnoszenia kompetencji zawodowych
CU2	Wyrobienie umiejętności projektowania i monitorowania stanu i warunków bezpieczeństwa: wykonywania analiz bezpieczeństwa i ryzyka, kontrolowania przestrzegania przepisów i zasad bezpieczeństwa, kontrolowania warunków pracy i standardów bezpieczeństwa, prowadzenia badań okoliczności awarii i wypadków, prowadzenia szkoleń, pełnienia funkcji organizatorskich w zakresie zarządzania bezpieczeństwem oraz prowadzenia dokumentacji związanej z szeroko rozumianym bezpieczeństwem

Kompetencje społeczne	
CK1	Przygotowanie do uczenia się przez całe życie, podnoszenie kompetencji zawodowych, osobistych i społecznych w zmieniającej się rzeczywistości, podjęcia pracy związanej z funkcjonowaniem systemu bezpieczeństwa, którego głównym celem jest ratowanie i ochrona życia, zdrowia i mienia przed zagrożeniami
CK2	Uświadomienie ważności i rozumienia społecznych skutków działalności inżynierskiej, w tym jej wpływu na środowisko i związanej z tym odpowiedzialności za podejmowane decyzje, współdziałanie w grupie i przyjmowanie odpowiedzialności za wspólne realizacje, kreatywność i przedsiębiorczość oraz potrzebę przekazywania informacji odnośnie osiągnięć technicznych i działania inżyniera.

E - Efekty kształcenia przedmiotowe i kierunkowe

Efekty kształcenia (E) w zakresie wiedzy (W), umiejętności (U) i kompetencji społecznych (K)		Kierunkowy efekt kształcenia
Wiedza (EW…)		
EPW1	Student, który zaliczył przedmiot ma elementarną wiedzę z zakresu podstaw informatyki obejmującą przetwarzanie informacji, architekturę i organizację systemów komputerowych, bezpieczeństwo systemów komputerowych, budowę sieci i aplikacji sieciowych	K_W04
EPW2	Student, który zaliczył przedmiot ma wiedzę ogólną obejmującą kluczowe zagadnienia bezpieczeństwa systemów, urządzeń i procesów	K_W05
Umiejętności (EU…)		
EPU1	Student, który zaliczył przedmiot potrafi pozyskiwać informacje z literatury, baz danych i innych źródeł; potrafi integrować uzyskane informacje, dokonywać ich interpretacji, a także wyciągać wnioski oraz formułować i uzasadniać opinie	K_U01
EPU2	Student, który zaliczył przedmiot potrafi posłużyć się właściwie dobranymi metodami i urządzeniami umożliwiającymi zapewnienie bezpieczeństwa systemów i urządzeń	K_U19
Kompetencje społeczne (EK…)		
EPK1	Student, który zaliczył przedmiot ma świadomość ważności i rozumie skutki działalności inżynierskiej oraz związanej z tym odpowiedzialności za podejmowane decyzje	K_K02

F - Treści programowe oraz liczba godzin na poszczególnych formach zajęć

Lp.	Treści wykładów	Liczba godzin na studiach	
		stacjonarnych	niestacjonarnych
W1	Podstawowe definicje dotyczące bezpieczeństwa	2	1
W2	Klasyfikacja przyczyn złego funkcjonowania systemów informatycznych.	2	1
W3	Serwery aplikacji i danych oraz systemy operacyjne - konfiguracja zwiększająca bezpieczeństwo	2	1
W4	Zalecenia dla wytwarzania bezpiecznego kodu programu.	2	2
W5	Zasady organizacji systemów bezpieczeństwa.	2	2
W6	Metody rozwiązywania problemów związanych z inżynierią bezpieczeństwa	2	1
W7	Bezpieczeństwo fron-end i back-end oprogramowania.	2	1
W8	Kryptografia i systemy kryptograficzne w bezpieczeństwie danych i systemów	2	1
W9	"Przepełnienie bufora" - niebezpieczne funkcje i metody ochrony.	2	2
W10	Architektury wielowarstwowe procesy autoryzacji i walidacji danych.	2	2
W11	Cross-site-scripting - na czym polega i jak się chronić przed wstrzykiwaniem kodu.	2	1
W12	SQL injection - zasady bezpieczeństwa aplikacji bazodanowych	2	1
W13	Metody szpiegostwa informatycznego. Slurping i wykradanie danych.	2	1
W14	Zasady analizy stanu bezpieczeństwa obiektów oraz bezpieczeństwa i higieny pracy, w tym analizy wypadków i oceny ryzyka	2	1

W15	Zaliczenie	2	2
	Razem liczba godzin wykładów:	**30**	**15**

Lp.	**Treści laboratoriów**	**Liczba godzin na studiach**	
		stacjonarnych	**niestacjonarnych**
L1	Podstawowe definicje dotyczące bezpieczeństwa	2	1
L2	Klasyfikacja przyczyn złego funkcjonowania systemów informatycznych.	2	1
L3	Serwery aplikacji i danych oraz systemy operacyjne - konfiguracja zwiększająca bezpieczeństwo	2	1
L4	Zalecenia dla wytwarzania bezpiecznego kodu programu.	2	1
L5	Kryptografia w bezpieczeństwie danych i systemów	2	1
L6	Systemy kryptograficzne w bezpieczeństwie danych i systemów	2	1
L7	"Przepełnienie bufora" - niebezpieczne funkcje	2	1
L8	"Przepełnienie bufora" - metody ochrony	2	1
L9	Cross-site-scripting - na czym polega i jak się chronić przed wstrzykiwaniem kodu	2	1
L10	SQL injection.	2	1
L11	Zasady bezpieczeństwa aplikacji bazodanowych	2	1
L12	Architektury wielowarstwowe	2	1
L13	Procesy autoryzacji danych	2	1
L14	Procesy walidacji danych	2	1
L15	Zaliczenie	2	1
	Razem liczba godzin laboratoriów:	**30**	**15**

Lp.	**Treści projektów**	**Liczba godzin na studiach**	
		stacjonarnych	**niestacjonarnych**
P1	Wprowadzenie do realizacji samodzielnych zadań projektowych	1	1
P2	Prezentacja tematyki projektów	2	1
P3	Omówienie zasad przygotowywania prezentacji, przykłady. Omówienie zasad prowadzenia prezentacji	2	1
P4	Przydział tematów projektowych, dyskusja	2	1
P5	Realizacja szkicu projektu w grupach, prezentacja szkiców projektów, dyskusja	2	1
P6	Realizacja skorygowanych projektów	2	2
P7	Prezentacja projektów	2	2
P8	Podsumowanie i zaliczenie przedmiotu	2	1
	Razem liczba godzin projektów	15	10

G – Metody oraz środki dydaktyczne wykorzystywane w ramach poszczególnych form zajęć

Forma zajęć	**Metody dydaktyczne (wybór z listy)**	**Środki dydaktyczne**
Wykład	Wykład informacyjny Wykład problemowy połączony z dyskusją	Komputer i projektor multimedialny, tablica suchościeralna
Laboratoria	Ćwiczenia doskonalące umiejętność pozyskiwania informacji ze źródeł internetowych Ćwiczenia doskonalące umiejętność selekcjonowania, grupowania i przedstawiania zgromadzonych informacji	Komputer i projektor multimedialny, tablica suchościeralna Sala komputerowa z dostępem do internetu
Projekt	Doskonalenie metod i technik analizy zadania inżynierskiego Selekcjonowanie, grupowanie i dobór informacji do	Komputer i projektor multimedialny, tablica suchościeralna

	realizacji zadania inżynierskiego,	Sala komputerowa z dostępem do internetu

H - Metody oceniania osiągnięcia efektów kształcenia na poszczególnych formach zajęć

Forma zajęć	**Ocena formująca (F) –** wskazuje studentowi na potrzebę uzupełniania wiedzy lub stosowania określonych metod i narzędzi, stymulujące do doskonalenia efektów pracy **(wybór z listy)**	**Ocena podsumowująca (P) –** podsumowuje osiągnięte efekty kształcenia **(wybór z listy)**
Wykład	F2 – obserwacja/aktywność	P2 – kolokwium podsumowujące semestr
Laboratorium	F3 – praca pisemna	P3 – ocena podsumowująca powstała na podstawie ocen formujących, uzyskanych w semestrze
Projekt	F4 – wystąpienie	P3 – ocena podsumowująca powstała na podstawie ocen formujących, uzyskanych w semestrze

H-1 Metody weryfikacji osiągnięcia przedmiotowych efektów kształcenia (wstawić „x")

Efekty przedmiotowe	Wykład		Laboratorium		Projekt	
	F2	P2	F3	P3	F4	P3
EPW1	x	x				
EPW2	x	x				
EPU1			x	x	x	x
EPU2			x	x	x	x
EPK1	x	x				

I – Kryteria oceniania

Wymagania określające kryteria uzyskania oceny w danym efekcie			
Ocena			
Przedmiotowy efekt kształcenia (EP..)	**Dostateczny , dostateczny plus 3/3,5**	**Dobry, dobry plus 4/4,5**	**bardzo dobry 5**
EPW1	Student opanował w stopniu podstawowym elementarną wiedzę z zakresu podstaw informatyki obejmującą przetwarzanie informacji, architekturę i organizację systemów komputerowych, bezpieczeństwo systemów komputerowych, budowę sieci i aplikacji sieciowych	Student opanował w stopniu dobrym elementarną wiedzę z zakresu podstaw informatyki obejmującą przetwarzanie informacji, architekturę i organizację systemów komputerowych, bezpieczeństwo systemów komputerowych, budowę sieci i aplikacji sieciowych	Student w pełni opanował elementarną wiedzę z zakresu podstaw informatyki obejmującą przetwarzanie informacji, architekturę i organizację systemów komputerowych, bezpieczeństwo systemów komputerowych, budowę sieci i aplikacji sieciowych
EPW2	Student ma podstawową wiedzę ogólną obejmującą kluczowe zagadnienia bezpieczeństwa systemów, urządzeń i procesów	Student ma ugruntowaną wiedzę ogólną obejmującą kluczowe zagadnienia bezpieczeństwa systemów, urządzeń i procesów	Student ma bardzo dobrą wiedzę ogólną obejmującą kluczowe zagadnienia bezpieczeństwa systemów, urządzeń i procesów

EPU1	Student potrafi w stopniu elementarnym pozyskiwać informacje z literatury, baz danych i innych źródeł; potrafi integrować uzyskane informacje, dokonywać ich interpretacji, a także wyciągać wnioski oraz formułować i uzasadniać opinie	Student potrafi w stopniu dobrym pozyskiwać informacje z literatury, baz danych i innych źródeł; potrafi integrować uzyskane informacje, dokonywać ich interpretacji, a także wyciągać wnioski oraz formułować i uzasadniać opinie	Student potrafi efektywnie pozyskiwać informacje z literatury, baz danych i innych źródeł; potrafi integrować uzyskane informacje, dokonywać ich interpretacji, a także wyciągać wnioski oraz formułować i uzasadniać opinie
EPU2	Student potrafi w zakresie elementarnym posłużyć się właściwie dobranymi metodami i urządzeniami umożliwiającymi zapewnienie bezpieczeństwa systemów i urządzeń	Student potrafi w stopniu dobrym posłużyć się właściwie dobranymi metodami i urządzeniami umożliwiającymi zapewnienie bezpieczeństwa systemów i urządzeń	Student potrafi efektywnie posłużyć się właściwie dobranymi metodami i urządzeniami umożliwiającymi zapewnienie bezpieczeństwa systemów i urządzeń
EPK1	Student ma podstawową świadomość ważności i zrozumienie skutków działalności inżynierskiej oraz związanej z tym odpowiedzialności za podejmowane decyzje	Student ma zadowalającą świadomość ważności i zrozumienie skutków działalności inżynierskiej oraz związanej z tym odpowiedzialności za podejmowane decyzje	Student ma ugruntowaną świadomość ważności i zrozumienie skutków działalności inżynierskiej oraz związanej z tym odpowiedzialności za podejmowane decyzje

J – Forma zaliczenia przedmiotu

Wykład - zaliczenie z oceną (test)

Laboratorium – zaliczenie z oceną. Na ocenę składa się oddanie min. 7 sprawozdawań, z laboratorium które są podstawą przystąpienia do kolokwium zaliczeniowego.

Projekt– zaliczenie z oceną. Ocenie podlegać będzie propozycja prowadzenia projektu.

Kryteria ocen dla wykładu, projektu i laboratorium:

0-50 % – niedostateczna
51-60 % – dostateczna
61-70 % – dostateczna plus
71-80 % - dobry
81-90 % dobry plus
91-100 % bardzo dobry

K – Literatura przedmiotu

Literatura obowiązkowa:

1. A. Ross, Inżynieria Zabezpieczeń, WNT, Warszawa 2005
2. R. Wobst, Kryptologia. Budowa i łamanie zabezpieczeń, RM, Warszawa, 2002
3. http://www.adavirtus.pl/pl/ada/pewne-i-bezpieczne-oprogramowanie

Literatura zalecana / fakultatywna:

1. M. Kutyłowski i W. B. Strothmann, Kryptografia: Teoria i praktyka zabezpieczania systemów komputerowych, Wyd. READ ME, Warszawa, 1999,
2. A. Lockhart, 100 sposobów na bezpieczeństwo Sieci, Helion, Gliwice 2004
3. M. Serafin, Sieci VPN - zdalna praca i bezpieczeństwo danych, Helion, Gliwice 2008
4. J. McNamara, Arkana szpiegostwa komputerowego, PWN, Warszawa 2003

L – Obciążenie pracą studenta:

Forma aktywności studenta	Liczba godzin na realizację	
	na studiach stacjonarnych	na studiach niestacjonarnych
Godziny zajęć z nauczycielem/ami	75	43
Konsultacje	5	12
Czytanie literatury	15	20
Przygotowanie do zajęć laboratoryjnych	10	10

Przygotowanie projektu	10	15
Przygotowanie do zaliczenia wykładu	10	25
Suma godzin:	**125**	**125**
Liczba punktów ECTS dla przedmiotu (suma godzin : 25 godz.):	**5**	**5**

Ł – Informacje dodatkowe

Imię i nazwisko sporządzającego	Pracownicy Wydziału Technicznego AJP
Data sporządzenia / aktualizacji	8 grudnia 2019 r.
Dane kontaktowe (e-mail, telefon)	wt@ajp.edu.pl
Podpis	

Pozycja w planie studiów (lub kod przedmiotu)	C.2.6

Wydział	Techniczny
Kierunek	Inżynieria Bezpieczeństwa
Poziom studiów	Pierwszego stopnia
Forma studiów	stacjonarne/niestacjonarne
Profil kształcenia	Praktyczny

PROGRAM PRZEDMIOTU/MODUŁU

A - Informacje ogólne

1. Nazwa przedmiotu	**Kontrola i audyt zasobów informatycznych**
2. Punkty ECTS	**4**
3. Rodzaj przedmiotu	**obowiązkowy**
4. Język przedmiotu	**język polski**
5. Rok studiów	**III**
6. Imię i nazwisko koordynatora przedmiotu oraz prowadzących zajęcia	**Łukasz Lemieszewski**

B – Formy dydaktyczne prowadzenia zajęć i liczba godzin w semestrze

Nr semestru	Studia stacjonarne	Studia niestacjonarne
Semestr 5	**Wykłady**: (15); **Lab.(**15), **Projekt:** (30);	**Wykłady**: (10); **Laboratoria**: (10); **Projekt:** (18);
Liczba godzin ogółem	**60**	**38**

C - Wymagania wstępne

Student nabył podstawową wiedzę z zakresu systemów operacyjnych, sieci komputerowych oraz programowania

D - Cele kształcenia

	Wiedza
CW1	przekazanie wiedzy w zakresie wiedzy technicznej obejmującej terminologię, pojęcia, teorie, zasady, metody, techniki, narzędzia i materiały stosowane przy rozwiązywaniu zadań inżynierskich związanych z szeroko pojętym bezpieczeństwem i rozpoznawaniem zagrożeń, procesami planowania i realizacji eksperymentów, tak w procesie przygotowania z udziałem metod symulacji komputerowych, jak i w rzeczywistym środowisku
	Umiejętności
CU1	wyrobienie umiejętności w zakresie doskonalenia wiedzy, pozyskiwania i integrowanie informacji z literatury, baz danych i innych źródeł, opracowywania dokumentacji, prezentowania ich i podnoszenia kompetencji zawodowych
	Kompetencje społeczne
CK1	przygotowanie do uczenia się przez całe życie, podnoszenie kompetencji zawodowych, osobistych i społecznych w zmieniającej się rzeczywistości, podjęcia pracy związanej z funkcjonowaniem systemu bezpieczeństwa, którego głównym celem jest ratowanie i ochro-na życia, zdrowia i mienia przed zagrożeniami

E - Efekty kształcenia przedmiotowe i kierunkowe

Przedmiotowy efekt kształcenia (EP) w zakresie wiedzy (W), umiejętności (U) i kompetencji społecznych (K)		Kierunkowy efekt kształcenia
Wiedza (EPW…)		
EPW1	ma elementarną wiedzę z zakresu podstaw informatyki obejmującą przetwarzanie informacji, architekturę i organizację systemów komputerowych, bezpieczeństwo systemów komputerowych, budowę sieci i aplikacji sieciowych	K_W04
EPW2	zna podstawowe metody, techniki, narzędzia i materiały stosowane przy rozwiązywaniu prostych zadań inżynierskich związanych z bezpieczeństwem	K_W12
Umiejętności (EPU…)		
EPU1	potrafi pozyskiwać informacje z literatury, baz danych i innych źródeł; potrafi integrować uzyskane informacje, dokonywać ich interpretacji, a także wyciągać wnioski oraz formułować i uzasadniać opinie	K_U01
EPU2	potrafi zaprojektować proces testowania bezpieczeństwa oraz — w przypadku wykrycia błędów — przeprowadzić ich diagnozę i wyciągnąć wnioski	K_U14
Kompetencje społeczne (EPK…)		
EPK1	ma świadomość ważności i rozumie pozatechniczne aspekty i skutki działalności inżynierskiej, w tym jej wpływu na środowisko, i związanej z tym odpowiedzialności za podejmowane decyzje	K_K03
EPK2	prawidłowo identyfikuje i rozstrzyga dylematy związane z wykonywaniem zawodu	K_K06

F - Treści programowe oraz liczba godzin na poszczególnych formach zajęć

Lp.	Treści wykładów	Liczba godzin na studiach	
		stacjonarnych	niestacjonarnych
W1	Proces gromadzenia informacji na temat funkcjonowania i zasobów komputerowych.	2	1
W2	Kroki postępowania w procesie kontrolnym. Wprowadzenie do audytu. Techniki przeprowadzania audytów.	2	2
W3	Inwentaryzacja oprogramowania i sprzętu.	2	1
W4	Narzędzia audytora. Licencje i ich ograniczenia.	2	2
W5	Kontrola w ujęciu procesowym.	2	1
W6	Zarządzanie jakością w systemach bezpieczeństwa teleinformatycznego.	2	1
W7	Istota zagadnienia jakości systemu teleinformatycznego i wielkości je charakteryzujące. Zaliczenie.	3	2
	Razem liczba godzin wykładów	15	10

Lp.	Treści laboratoriów	Liczba godzin na studiach	
		stacjonarnych	niestacjonarnych
L1	Kontrola systemów informatycznych. Wzór matrycy kontroli	2	1
L2	Ogólna lista kontrolna oceny charakteru krytycznego	2	2
L3	Matryca kontroli ładu informatycznego.	2	1
L4	Matryca kontroli rozwijania i nabywania	2	2
L5	Matryca kontroli eksploatacji systemów informatycznych.	2	1
L6	Matryca kontroli bezpieczeństwa informacji.	2	1
L7	Matryca kontroli mechanizmów kontroli aplikacji. Wystawienie ocen.	3	2
	Razem liczba godzin laboratoriów	15	10

Lp.	Treści projektów	Liczba godzin na studiach	
		stacjonarnych	niestacjonarnych
P1	Przegląd narzędzi audytora.	2	2
P2	Instalacja wybranego narzędzia audytu oprogramowania i sieci.	2	
P3	Dla wybranego scenariusza organizacji przygotowanie audytu oprogramowania i sprzętu.	4	2
P4	Dla wybranego scenariusza organizacji przeprowadzenie audytu oprogramowania i sprzętu.	2	2
P5	Dla wybranego scenariusza organizacji sprawdzanie zasobów oprogramowania i sprzętu.	4	2
P6	Dla wybranego scenariusza organizacji katalogowanie zasobów oprogramowania i sprzętu.	2	2
P7	Określanie legalności oprogramowania.	4	2
P8	Analiza wyników audytu.	4	2
P9	Inwentaryzacji Zbiorów Danych.	2	2
P10	Oddanie projektów.	4	2
	Razem liczba godzin laboratoriów	30	18

G – Metody oraz środki dydaktyczne wykorzystywane w ramach poszczególnych form zajęć

Forma zajęć	Metody dydaktyczne (wybór z listy)	Środki dydaktyczne
Wykład	M1 - wykład informacyjny, M3 – pokaz multimedialny	projektor, prezentacja multimedialna
Projekt	M5 - ćwiczenia doskonalące obsługę programów do kontroli i audytu zasobów informatycznych	Jednostka komputerowa wyposażona w odpowiednie oprogramowanie oraz z dostępem do sieci Internetu

H - Metody oceniania osiągnięcia efektów kształcenia na poszczególnych formach zajęć

Forma zajęć	Ocena formująca (F) – wskazuje studentowi na potrzebę uzupełniania wiedzy lub stosowania określonych metod i narzędzi, stymulujące do doskonalenia efektów pracy **(wybór z listy)**	Ocena podsumowująca (P) – podsumowuje osiągnięte efekty kształcenia **(wybór z listy)**
Wykład	F2 – obserwacja/aktywność podczas zajęć	P2 – kolokwium podsumowujące semestr
Laboratorium	F2 – obserwacja/aktywność (przygotowanie do zajęć, ocena ćwiczeń wykonywanych podczas zajęć), F3 – praca pisemna (sprawozdanie, dokumentacja projektu, pisemna analiza problemu), F5 - ćwiczenia praktyczne (ćwiczenia z wykorzystaniem sprzętu i oprogramowania fachowego)	P3 – ocena podsumowująca powstała na podstawie ocen formujących, uzyskanych w semestrze oraz oceny sprawozdań jako pracy pisemnej
Projekt	F3 – dokumentacja projektu F4 – wystąpienie – analiza projektu	P4 – praca pisemna - projekt

H-1 Metody weryfikacji osiągnięcia przedmiotowych efektów kształcenia (wstawić „x")

Efekty przedmiotowe	Wykład		Projekt			Laboratorium		
	F2	P2	F2	F5	P2	F2	F3	F5

EPW1	x	x						
EPW2	x	x				x	x	x
EPU1			x	x	x	x	x	x
EPU2			x	x	x		x	
EPK1			x	x	x		x	
EPK2	x	x				x	x	x

I – Kryteria oceniania

Wymagania określające kryteria uzyskania oceny w danym efekcie			
Ocena			
Przedmiotowy efekt kształcenia (EP..)	**Dostateczny dostateczny plus 3/3,5**	**dobry dobry plus 4/4,5**	**bardzo dobry 5**
EPW1	ma wiedzę ogólną obejmującą podstawowe zagadnienia bezpieczeństwa systemów, urządzeń i procesów	ma wiedzę ogólną obejmującą większość kluczowych zagadnienia bezpieczeństwa systemów, urządzeń i procesów	ma wiedzę ogólną obejmującą kluczowe zagadnienia bezpieczeństwa systemów, urządzeń i procesów
EPW2	ma podstawową wiedzę w zakresie standardów i norm technicznych związanych z inżynierią bezpieczeństwa	ma podstawową wiedzę w zakresie standardów i norm technicznych związanych z inżynierią bezpieczeństwa oraz systemów	ma podstawową wiedzę w zakresie standardów i norm technicznych związanych z inżynierią bezpieczeństwa systemów, urządzeń i procesów
EPU1	potrafi pozyskiwać informacje z literatury, baz danych i innych źródeł;	potrafi pozyskiwać informacje z literatury, baz danych i innych źródeł; potrafi integrować uzyskane informacje	potrafi pozyskiwać informacje z literatury, baz danych i innych źródeł; potrafi integrować uzyskane informacje, dokonywać ich interpretacji, a także wyciągać wnioski oraz formułować i uzasadniać opinie
EPU2	potrafi opracować dokumentację dotyczącą realizacji zadania inżynierskiego	potrafi opracować dokumentację dotyczącą realizacji zadania inżynierskiego i przygotować tekst zawierający omówienie wybranych wyników realizacji tego zadania	potrafi opracować dokumentację dotyczącą realizacji zadania inżynierskiego i przygotować tekst zawierający omówienie wyników realizacji tego zadania
EPK1	ma świadomość ważności i rozumie niektóre pozatechniczne aspekty i skutki działalności inżynierskiej, w tym jej wpływu na środowisko, i związanej z tym odpowiedzialności za podejmowane decyzje	ma świadomość ważności i rozumie większość pozatechnicznych aspektów i skutki działalności inżynierskiej, w tym jej wpływu na środowisko, i związanej z tym odpowiedzialności za podejmowane decyzje	ma świadomość ważności i rozumie wszystkie poznane na zajęciach pozatechniczne aspekty i skutki działalności inżynierskiej, w tym jej wpływu na środowisko, i związanej z tym odpowiedzialności za podejmowane decyzje
EPK2	Zna skutki działalności inżynierskiej	ma świadomość ważności i rozumie pozatechniczne aspekty i skutki działalności inżynierskiej	ma świadomość ważności i rozumie pozatechniczne aspekty i skutki działalności inżynierskiej, w tym jej wpływu na środowisko, i związanej z tym odpowiedzialności za podejmowane decyzje

J – Forma zaliczenia przedmiotu

Wykład - zaliczenie z oceną (test)

Laboratorium – zaliczenie z oceną. Na ocenę składa się oddanie min. 7 sprawozdawań, z laboratorium które są podstawą przystąpienia do kolokwium zaliczeniowego.

Projekt– zaliczenie z oceną. Ocenie podlegać będzie wykonanie projektu.

Kryteria ocen dla wykładu, projektu i laboratorium:

0-50 % – niedostateczna
51-60 % – dostateczna
61-70 % – dostateczna plus
71-80 % - dobry
81-90 % dobry plus
91-100 % bardzo dobry

K – Literatura przedmiotu

Literatura obowiązkowa:

1. A. Białas, Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie, WNT, Warszawa 2007.
2. W. Pihowicz, Inżynieria bezpieczeństwa technicznego. Problematyka podstawowa, WNT, Warszawa 2008
3. T. Polaczek, Audyt informacji bezpieczeństwa informacji w praktyce, Helion, Gliwice 2006

Literatura zalecana / fakultatywna:

1. K. Liderman, Analiza ryzyka i ochrona informacji w systemach komputerowych, PWN, Warszawa 2008
2. B. Fischer, W. Świerczyńska, Dostęp do informacji ustawowo chronionych, zarządzanie informacją, Wyd. Uniwersytetu Jagiellońskiego, Kraków 2005.
3. P. Fajgielski, Kontrola i audyt przetwarzania danych osobowych, Wyd. PRESSCOM Sp. z o.o., 2010

L – Obciążenie pracą studenta:

Forma aktywności studenta	Liczba godzin na realizację	
	na studiach stacjonarnych	na studiach niestacjonarnych
Godziny zajęć z nauczycielem/ami	60	38
Konsultacje	5	5
Czytanie literatury	5	27
Przygotowanie sprawozdań	15	15
Przygotowanie projektów	15	15
Suma godzin:	**100**	**100**
Liczba punktów ECTS dla przedmiotu (suma godzin: 25 godz.):	**4**	**4**

Ł – Informacje dodatkowe

Imię i nazwisko sporządzającego	Łukasz Lemieszewski
Data sporządzenia / aktualizacji	8 grudnia 2019 r.
Dane kontaktowe (e-mail, telefon)	llemieszewski@ajp.edu.pl
Podpis	

Pozycja w planie studiów (lub kod przedmiotu)	C.2.7.

	Wydział	Techniczny
	Kierunek	Inżynieria bezpieczeństwa
	Poziom studiów	Studia pierwszego stopnia
	Forma studiów	Stacjonarne / Niestacjonarne
	Profil kształcenia	Profil praktyczny

PROGRAM PRZEDMIOTU/MODUŁU

A - Informacje ogólne

1. Nazwa przedmiotu	**Inteligentne systemy przeciw atakom sieciowym**
2. Punkty ECTS	**5**
3. Rodzaj przedmiotu	**Obowiązkowy**
4. Język przedmiotu	**język polski**
5. Rok studiów	**III**
6. Imię i nazwisko koordynatora przedmiotu oraz prowadzących zajęcia	**Pracownicy WT AJP**

B – Formy dydaktyczne prowadzenia zajęć i liczba godzin w semestrze

Nr semestru	Studia stacjonarne	Studia niestacjonarne
Semestr 5	**W**: 30; **Lab.**: 30; **Proj.** 15	**W**: 15; **Lab.**: 18; **Proj.** 10
Liczba godzin ogółem	**75**	**43**

C - Wymagania wstępne

Znajomość zagadnień z zakresu ataków i wykrywanie włamań w sieciach oraz kryptografii

D - Cele kształcenia

	Wiedza
CW1	Przekazanie wiedzy w zakresie wiedzy technicznej obejmującej terminologię, pojęcia, teorie, zasady, metody, techniki, narzędzia i materiały stosowane przy rozwiązywaniu zadań inżynierskich związanych z szeroko pojętym bezpieczeństwem i rozpoznawaniem zagrożeń, procesami planowania i realizacji eksperymentów, tak w procesie przygotowania z udziałem metod symulacji komputerowych, jak i w rzeczywistym środowisku.
CW2	Przekazanie wiedzy ogólnej dotyczącej standardów i norm technicznych dotyczących zagadnień inżynierii bezpieczeństwa systemów, urządzeń, procesów, i związanych z tym technik i metod programowania, szyfrowania danych, zarządzania jakością i analizy ryzyka
	Umiejętności
CU1	Wyrobienie umiejętności w zakresie doskonalenia wiedzy, pozyskiwania i integrowanie informacji z literatury, baz danych i innych źródeł, opracowywania dokumentacji, prezentowania ich i podnoszenia kompetencji zawodowych
CU2	Wyrobienie umiejętności projektowania i monitorowania stanu i warunków bezpieczeństwa: wykonywania analiz bezpieczeństwa i ryzyka, kontrolowania przestrzegania przepisów i zasad bezpieczeństwa, kontrolowania warunków pracy i standardów bezpieczeństwa, prowadzenia badań okoliczności awarii i wypadków, prowadzenia szkoleń, pełnienia funkcji organizatorskich w zakresie zarządzania bezpieczeństwem oraz prowadzenia dokumentacji związanej z szeroko rozumianym bezpieczeństwem

Kompetencje społeczne	
CK1	Przygotowanie do uczenia się przez całe życie, podnoszenie kompetencji zawodowych, osobistych i społecznych w zmieniającej się rzeczywistości, podjęcia pracy związanej z funkcjonowaniem systemu bezpieczeństwa, którego głównym celem jest ratowanie i ochrona życia, zdrowia i mienia przed zagrożeniami
CK2	Uświadomienie ważności i rozumienia społecznych skutków działalności inżynierskiej, w tym jej wpływu na środowisko i związanej z tym odpowiedzialności za podejmowane decyzje, współdziałanie w grupie i przyjmowanie odpowiedzialności za wspólne realizacje, kreatywność i przedsiębiorczość oraz potrzebę przekazywania informacji odnośnie osiągnięć technicznych i działania inżyniera.

E - Efekty kształcenia przedmiotowe i kierunkowe

Efekty kształcenia (E) w zakresie wiedzy (W), umiejętności (U) i kompetencji społecznych (K)		Kierunkowy efekt kształcenia
Wiedza (EW…)		
EPW1	Student, który zaliczył przedmiot ma elementarną wiedzę z zakresu podstaw informatyki obejmującą przetwarzanie informacji, architekturę i organizację systemów komputerowych, bezpieczeństwo systemów komputerowych, budowę sieci i aplikacji sieciowych	K_W04
EPW2	Student, który zaliczył przedmiot ma wiedzę ogólną obejmującą kluczowe zagadnienia bezpieczeństwa systemów, urządzeń i procesów	K_W05
Umiejętności (EU…)		
EPU1	Student, który zaliczył przedmiot potrafi pozyskiwać informacje z literatury, baz danych i innych źródeł; potrafi integrować uzyskane informacje, dokonywać ich interpretacji, a także wyciągać wnioski oraz formułować i uzasadniać opinie	K_U01
EPU2	Student, który zaliczył przedmiot potrafi posłużyć się właściwie dobranymi metodami i urządzeniami umożliwiającymi zapewnienie bezpieczeństwa systemów i urządzeń	K_U19
Kompetencje społeczne (EK…)		
EPK1	Student, który zaliczył przedmiot ma świadomość ważności i rozumie skutki działalności inżynierskiej oraz związanej z tym odpowiedzialności za podejmowane decyzje	K_K02

F - Treści programowe oraz liczba godzin na poszczególnych formach zajęć

Lp.	Treści wykładów	Liczba godzin na studiach	
		stacjonarnych	niestacjonarnych
W1	Wprowadzenie do przedmiotu, definicje i pojęcia, stan techniki w dziedzinie	2	1
W2	Charakterystyka inteligentnych systemów przeciw atakom sieciowym	2	1
W3	Metody kryptograficzne w identyfikacji, uwierzytelniania i autoryzacji.	2	1
W4	Prawodawstwo w zakresie uwierzytelniania dokumentów	2	1
W5	Uwierzytelnianie oparte na tokenach i znacznikach czasu	2	1
W6	Uwierzytelnianie użytkowników oparte na cechach biomentrycznych	2	2
W7	Uwierzytelnianie oparte na hasłach statycznych i kluczach jednorazowych.	2	1
W8	Systemy uwierzytelniania w serwisach internetowych (RFC 2617)	2	1
W9	Kryptograficzne dowody tożsamości i serwery uwierzytelniania	2	2
W10	RFID - zasada funkcjonowania, zakres zastosowań, wady i zalety	2	2
W11	Procesy autoryzacji w bankowości elektronicznej - wady i zalety rozwiązań	2	1
W12	Autoryzacja za pomocą podpisu elektronicznego ustawodawstwo i rozwój e-government	2	1
W13	Przykłady konfiguracji uwierzytelniania dla sieciowych urządzeń dostępowych	2	1
W14	Uwierzytelnianie przy pomocy KERBEROS	2	1

W15	Podsumowanie przedmiotu	2	1
	Razem liczba godzin wykładów:	**30**	**15**

Lp.	**Treści laboratoriów**	**Liczba godzin na studiach**	
		stacjonarnych	**niestacjonarnych**
L1	Metody kryptograficzne w identyfikacji, uwierzytelniania i autoryzacji	2	1
L2	Wprowadzenie do analizatora sieciowego Wireshark, instalacja i konfiguracja, zasada działania, opcje przechwytu pakietów.	2	1
L3	Analiza protokołu HTTP za pomocą analizatora sieciowego Wireshark.	2	1
L4	Analiza protokołu DNS za pomocą analizatora sieciowego Wireshark.	2	1
L5	Analiza protokołu IP za pomocą analizatora sieciowego Wireshark.	2	1
L6	Analiza protokołu TCP i SSL za pomocą analizatora sieciowego Wireshark.	2	1
L7	Analiza protokołu UDP za pomocą analizatora sieciowego Wireshark.	2	1
L8	Analiza protokołu DHCP za pomocą analizatora sieciowego Wireshark.	2	1
L9	Uwierzytelnianie oparte na tokenach i znacznikach czasu	2	2
L10	Uwierzytelnianie użytkowników oparte na cechach biomentrycznych	2	1
L11	Uwierzytelnianie oparte na hasłach statycznych i kluczach jednorazowych.	2	2
L12	Kryptograficzne dowody tożsamości i serwery uwierzytelniania	2	1
L13	Przykłady konfiguracji uwierzytelniania dla sieciowych urządzeń dostępowych	2	1
L14	Uwierzytelnianie przy pomocy KERBEROS	2	2
L15	Zaliczenie	2	1
	Razem liczba godzin laboratoriów	30	18

Lp.	**Treści projektów**	**Liczba godzin na studiach**	
		stacjonarnych	**niestacjonarnych**
P1	Wprowadzenie do sieciowy systemu wykrywania włamań SNORT.	1	1
P2	Opracowanie projektu wdrożenia systemu wykrywania i zapobiegania włamaniom	2	1
P3	Instalacja i konfiguracja SNORT	2	2
P4	SNORT jako sniffer	2	2
P5	SNORT jako rejestrator pakietów	2	1
P6	Snort jako system IDS (systemy wykrywania i zapobiegania włamaniom)	2	1
P7	Dla wybranego przedsiębiorstwa przeprowadzenie przeprowadzać analizy strumieni pakietów	2	1
P8	Wyniki analizy. Oddanie projektów.	2	1
	Razem liczba godzin projektów	15	10

G – Metody oraz środki dydaktyczne wykorzystywane w ramach poszczególnych form zajęć

Forma zajęć	**Metody dydaktyczne (wybór z listy)**	**Środki dydaktyczne**
Wykład	Wykład informacyjny Wykład problemowy połączony z dyskusją	Komputer i projektor multimedialny, tablica suchościeralna
Laboratoria	Ćwiczenia doskonalące umiejętność pozyskiwania informacji ze źródeł internetowych Ćwiczenia doskonalące umiejętność selekcjonowania, grupowania i przedstawiania zgromadzonych informacji	Komputer i projektor multimedialny, tablica suchościeralna Sala komputerowa z dostępem do internetu
Projekt	Selekcjonowanie, grupowanie i dobór informacji do	omputer i projektor multimedialny,

	realizacji zadania inżynierskiego	tablica suchościeralna Sala komputerowa z dostępem do internetu

H - Metody oceniania osiągnięcia efektów kształcenia na poszczególnych formach zajęć

Forma zajęć	**Ocena formująca (F) –** wskazuje studentowi na potrzebę uzupełniania wiedzy lub stosowania określonych metod i narzędzi, stymulujące do doskonalenia efektów pracy **(wybór z listy)**	**Ocena podsumowująca (P) –** podsumowuje osiągnięte efekty kształcenia **(wybór z listy)**
Wykład	F2 – obserwacja/aktywność podczas zajęć	P1 – egzamin pisemny
Laboratorium	F2 – obserwacja/aktywność (przygotowanie do zajęć, ocena ćwiczeń wykonywanych podczas zajęć), F3 – praca pisemna (sprawozdanie, dokumentacja projektu, pisemna analiza problemu), F5 - ćwiczenia praktyczne (ćwiczenia z wykorzystaniem sprzętu i oprogramowania fachowego)	P3 – ocena podsumowująca powstała na podstawie ocen formujących, uzyskanych w semestrze oraz oceny sprawozdań jako pracy pisemnej
Projekt	F3 – dokumentacja projektu F4 – wystąpienie – analiza projektu	P4 – praca pisemna - projekt

H-1 Metody weryfikacji osiągnięcia przedmiotowych efektów kształcenia (wstawić „x")

Efekty przedmiotowe	Wykład		Projekt			Laboratorium		
	F2	P2	F2	F5	P2	F2	F3	F5
EPW1	x	x						
EPW2	x	x				x	x	x
EPU1			x	x	x	x	x	x
EPU2			x	x	x		x	
EPK1	x	x				x	x	x

I – Kryteria oceniania

Wymagania określające kryteria uzyskania oceny w danym efekcie			
Ocena			
Przedmiotowy efekt kształcenia (EP..)	**Dostateczny , dostateczny plus 3/3,5**	**Dobry, dobry plus 4/4,5**	**bardzo dobry 5**
EPW1	Student opanował w stopniu podstawowym elementarną wiedzę z zakresu podstaw informatyki obejmującą przetwarzanie informacji, architekturę i organizację systemów komputerowych, bezpieczeństwo systemów komputerowych, budowę sieci i aplikacji sieciowych	Student opanował w stopniu dobrym elementarną wiedzę z zakresu podstaw informatyki obejmującą przetwarzanie informacji, architekturę i organizację systemów komputerowych, bezpieczeństwo systemów komputerowych, budowę sieci i aplikacji sieciowych	Student w pełni opanował elementarną wiedzę z zakresu podstaw informatyki obejmującą przetwarzanie informacji, architekturę i organizację systemów komputerowych, bezpieczeństwo systemów komputerowych, budowę sieci i aplikacji sieciowych

EPW2	Student ma podstawową wiedzę ogólną obejmującą kluczowe zagadnienia bezpieczeństwa systemów, urządzeń i procesów	Student ma ugruntowaną wiedzę ogólną obejmującą kluczowe zagadnienia bezpieczeństwa systemów, urządzeń i procesów	Student ma bardzo dobrą wiedzę ogólną obejmującą kluczowe zagadnienia bezpieczeństwa systemów, urządzeń i procesów
EPU1	Student potrafi w stopniu elementarnym pozyskiwać informacje z literatury, baz danych i innych źródeł; potrafi integrować uzyskane informacje, dokonywać ich interpretacji, a także wyciągać wnioski oraz formułować i uzasadniać opinie	Student potrafi w stopniu dobrym pozyskiwać informacje z literatury, baz danych i innych źródeł; potrafi integrować uzyskane informacje, dokonywać ich interpretacji, a także wyciągać wnioski oraz formułować i uzasadniać opinie	Student potrafi efektywnie pozyskiwać informacje z literatury, baz danych i innych źródeł; potrafi integrować uzyskane informacje, dokonywać ich interpretacji, a także wyciągać wnioski oraz formułować i uzasadniać opinie
EPU2	Student potrafi w zakresie elementarnym posłużyć się właściwie dobranymi metodami i urządzeniami umożliwiającymi zapewnienie bezpieczeństwa systemów i urządzeń	Student potrafi w stopniu dobrym posłużyć się właściwie dobranymi metodami i urządzeniami umożliwiającymi zapewnienie bezpieczeństwa systemów i urządzeń	Student potrafi efektywnie posłużyć się właściwie dobranymi metodami i urządzeniami umożliwiającymi zapewnienie bezpieczeństwa systemów i urządzeń
EPK1	Student ma podstawową świadomość ważności i zrozumienie skutków działalności inżynierskiej oraz związanej z tym odpowiedzialności za podejmowane decyzje	Student ma zadowalającą świadomość ważności i zrozumienie skutków działalności inżynierskiej oraz związanej z tym odpowiedzialności za podejmowane decyzje	Student ma ugruntowaną świadomość ważności i zrozumienie skutków działalności inżynierskiej oraz związanej z tym odpowiedzialności za podejmowane decyzje

J – Forma zaliczenia przedmiotu

Wykład - egzamin (test)

Laboratorium – zaliczenie z oceną. Na ocenę składa się oddanie min. 7 sprawozdawań, z laboratorium które są podstawą przystąpienia do kolokwium zaliczeniowego.

Projekt– zaliczenie z oceną. Ocenie podlegać będzie wykonanie projektu.

Kryteria ocen dla wykładu, projektu i laboratorium:

0-50 % – niedostateczna
51-60 % – dostateczna
61-70 % – dostateczna plus
71-80 % - dobry
81-90 % dobry plus
91-100 % bardzo dobry

K – Literatura przedmiotu

Literatura obowiązkowa:

1. J. Pieprzyk, T. Hardjono, J. Seberry, Teoria bezpieczeństwa systemów komputerowych, Helion, Gliwice 2006
2. A. Ross, Inżynieria Zabezpieczeń, WNT, Warszawa 2005

Literatura zalecana / fakultatywna:

1. T. Kifner, Polityka bezpieczeństwa i ochrony informacji, Helion, Gliwice 1999

L – Obciążenie pracą studenta:

Forma aktywności studenta	Liczba godzin na realizację	
	na studiach stacjonarnych	na studiach niestacjonarnych
Godziny zajęć z nauczycielem/ami	75	43

Konsultacje	1	6
Czytanie literatury	10	26
Przygotowanie sprawozdań	10	15
Przygotowanie projektów	14	15
Przygotowanie do egzaminu	15	20
Suma godzin:	**125**	**125**
Liczba punktów ECTS dla przedmiotu (suma godzin : 25 godz.):	**5**	**5**

Ł – Informacje dodatkowe

Imię i nazwisko sporządzającego	Łukasz Lemieszewski
Data sporządzenia / aktualizacji	16 grudnia 2019 r.
Dane kontaktowe (e-mail, telefon)	llemieszewski@ajp.edu.pl
Podpis	

Pozycja w planie studiów (lub kod przedmiotu)	C.2.8.

Wydział	Techniczny
Kierunek	Inżynieria bezpieczeństwa
Poziom studiów	Studia pierwszego stopnia
Forma studiów	Stacjonarne / Niestacjonarne
Profil kształcenia	Profil praktyczny

PROGRAM PRZEDMIOTU/MODUŁU

A - Informacje ogólne

1. Nazwa przedmiotu	**Cyfrowe systemy i narzędzia uwierzytelniania**
2. Punkty ECTS	**4**
3. Rodzaj przedmiotu	Obowiązkowy
4. Język przedmiotu	**język polski**
5. Rok studiów	**III**
6. Imię i nazwisko koordynatora przedmiotu oraz prowadzących zajęcia	**Pracownicy WT AJP**

B – Formy dydaktyczne prowadzenia zajęć i liczba godzin w semestrze

Nr semestru	Studia stacjonarne	Studia niestacjonarne
Semestr 5	**W**: 30; **Lab.**: 15; **Proj.** 15	**W**: 15; **Lab.**: 10; **Proj.** 10
Liczba godzin ogółem	**60**	**35**

C - Wymagania wstępne

Znajomość zagadnień z zakresu ataków i wykrywanie włamań w sieciach oraz kryptografii

D - Cele kształcenia

	Wiedza
CW1	Przekazanie wiedzy w zakresie wiedzy technicznej obejmującej terminologię, pojęcia, teorie, zasady, metody, techniki, narzędzia i materiały stosowane przy rozwiązywaniu zadań inżynierskich związanych z szeroko pojętym bezpieczeństwem i rozpoznawaniem zagrożeń, procesami planowania i realizacji eksperymentów, tak w procesie przygotowania z udziałem metod symulacji komputerowych, jak i w rzeczywistym środowisku.
CW2	Przekazanie wiedzy ogólnej dotyczącej standardów i norm technicznych dotyczących zagadnień inżynierii bezpieczeństwa systemów, urządzeń, procesów, i związanych z tym technik i metod programowania, szyfrowania danych, zarządzania jakością i analizy ryzyka
	Umiejętności
CU1	Wyrobienie umiejętności w zakresie doskonalenia wiedzy, pozyskiwania i integrowanie informacji z literatury, baz danych i innych źródeł, opracowywania dokumentacji, prezentowania ich i podnoszenia kompetencji zawodowych
CU2	Wyrobienie umiejętności projektowania i monitorowania stanu i warunków bezpieczeństwa: wykonywania analiz bezpieczeństwa i ryzyka, kontrolowania przestrzegania przepisów i zasad

	bezpieczeństwa, kontrolowania warunków pracy i standardów bezpieczeństwa, prowadzenia badań okoliczności awarii i wypadków, prowadzenia szkoleń, pełnienia funkcji organizatorskich w zakresie zarządzania bezpieczeństwem oraz prowadzenia dokumentacji związanej z szeroko rozumianym bezpieczeństwem
Kompetencje społeczne	
CK1	Przygotowanie do uczenia się przez całe życie, podnoszenie kompetencji zawodowych, osobistych i społecznych w zmieniającej się rzeczywistości, podjęcia pracy związanej z funkcjonowaniem systemu bezpieczeństwa, którego głównym celem jest ratowanie i ochrona życia, zdrowia i mienia przed zagrożeniami
CK2	Uświadomienie ważności i rozumienia społecznych skutków działalności inżynierskiej, w tym jej wpływu na środowisko i związanej z tym odpowiedzialności za podejmowane decyzje, współdziałanie w grupie i przyjmowanie odpowiedzialności za wspólne realizacje, kreatywność i przedsiębiorczość oraz potrzebę przekazywania informacji odnośnie osiągnięć technicznych i działania inżyniera.

E - Efekty kształcenia przedmiotowe i kierunkowe

Efekty kształcenia (E) w zakresie wiedzy (W), umiejętności (U) i kompetencji społecznych (K)		**Kierunkowy efekt kształcenia**
Wiedza (EW…)		
EPW1	Student, który zaliczył przedmiot ma elementarną wiedzę z zakresu podstaw informatyki obejmującą przetwarzanie informacji, architekturę i organizację systemów komputerowych, bezpieczeństwo systemów komputerowych, budowę sieci i aplikacji sieciowych	K_W04
EPW2	Student, który zaliczył przedmiot ma wiedzę ogólną obejmującą kluczowe zagadnienia bezpieczeństwa systemów, urządzeń i procesów	K_W05
Umiejętności (EU…)		
EPU1	Student, który zaliczył przedmiot potrafi pozyskiwać informacje z literatury, baz danych i innych źródeł; potrafi integrować uzyskane informacje, dokonywać ich interpretacji, a także wyciągać wnioski oraz formułować i uzasadniać opinie	K_U01
EPU2	Student, który zaliczył przedmiot potrafi posłużyć się właściwie dobranymi metodami i urządzeniami umożliwiającymi zapewnienie bezpieczeństwa systemów i urządzeń	K_U19
Kompetencje społeczne (EK…)		
EPK1	Student, który zaliczył przedmiot ma świadomość ważności i rozumie skutki działalności inżynierskiej oraz związanej z tym odpowiedzialności za podejmowane decyzje	K_K02

F - Treści programowe oraz liczba godzin na poszczególnych formach zajęć

Lp.	**Treści wykładów**	**Liczba godzin na studiach**	
		stacjonarnych	**niestacjonarnych**
W1	Wprowadzenie do przedmiotu, pojęcia.	2	1
W2	Systemy kryptograficzne i funkcje skrótu.	2	1
W3	Algorytm Diffiego-Hellmana i protokoły dystrybucji kluczy.	2	1
W4	Ustawa o podpisie cyfrowym. Certyfikaty i ich zastosowania.	2	1
W5	Certyfikaty X.509 klucza publicznego oraz LDAP.	2	1
W6	Zasady uwierzytelniania zdalnych użytkowników	2	1
W7	Wprowadzenie do systemu KERBEROS.	2	1
W8	Komponenty i usługi PKI - metody ochrony przed atakami na PKI	2	1
W9	Elementy bezpieczeństwa sieci. Secure Socket Layer (SSL) i HTTPS	2	1
W10	Poufność i integralność transmisji danych za pomocą Transport Layer Security (TSL)	2	1
W11	Bezpieczeństwo sieci bezprzewodowych IEEE 802.lli	2	1
W12	Bezpieczeństwo poczty elektronicznej. PGE S/MIME i DKIM.	2	1
W13	Polityka bezpieczeństwa według IPsec . Protokół ESP	2	1
W14	Komasacja· skojarzeń bezpieczeństwa i internetowa wymiana kluczy (IKE)	2	1

W15	Zaliczenie przedmiotu	2	1
	Razem liczba godzin wykładów:	**30**	**15**

Lp.	**Treści laboratoriów**	**Liczba godzin na studiach**	
		stacjonarnych	**niestacjonarnych**
L1	Wprowadzenie pojęć i organizacja zajęć	2	1
L2	Generowanie i wykorzystanie certyfikatów bezpieczeństwa	1	1
L3	Konfiguracja bezpieczeństwa przeglądarki i poczty Internetowej	2	2
L4	Certyfikacja usług w systemach rozproszonych - przykłady wykorzystania.	2	2
L5	Narzędzia implementacji elementów infrastruktury usług certyfikacyjnych	2	1
L6	Komponenty JAVA dla generowania i wykorzystania certyfikatów bezpieczeństwa	2	1
L7	Wprowadzenie do zarządzania kluczami w KERBEROS.	2	1
L8	Zaliczenie przedmiotu	2	1
	Razem liczba godzin laboratoriów	15	10

Lp.	**Treści projektów**	**Liczba godzin na studiach**	
		stacjonarnych	**niestacjonarnych**
P1	Wprowadzenie do realizacji samodzielnych zadań projektowych	1	1
P2	Prezentacja tematyki projektów	2	1
P3	Omówienie zasad przygotowywania prezentacji, przykłady. Omówienie zasad prowadzenia prezentacji	2	1
P4	Przydział tematów projektowych, dyskusja	2	1
P5	Realizacja szkicu projektu w grupach, prezentacja szkiców projektów, dyskusja	2	1
P6	Realizacja skorygowanych projektów	2	2
P7	Prezentacja projektów	2	2
P8	Podsumowanie i zaliczenie przedmiotu	2	1
	Razem liczba godzin projektów	15	10

G – Metody oraz środki dydaktyczne wykorzystywane w ramach poszczególnych form zajęć

Forma zajęć	**Metody dydaktyczne (wybór z listy)**	**Środki dydaktyczne**
Wykład	Wykład informacyjny Wykład problemowy połączony z dyskusją	Komputer i projektor multimedialny, tablica suchościeralna
Laboratoria	Ćwiczenia doskonalące umiejętność selekcjonowania, grupowania i przedstawiania zgromadzonych informacji	Komputer i projektor multimedialny, tablica suchościeralna Sala komputerowa z dostępem do internetu
Projekt	Selekcjonowanie, grupowanie i dobór informacji do realizacji zadania inżynierskiego	Komputer i projektor multimedialny, tablica suchościeralna Sala komputerowa z dostępem do internetu

H - Metody oceniania osiągnięcia efektów kształcenia na poszczególnych formach zajęć

Forma zajęć	**Ocena formująca (F) –** wskazuje studentowi na potrzebę uzupełniania wiedzy lub stosowania określonych metod i narzędzi, stymulujące do doskonalenia efektów pracy **(wybór z listy)**	**Ocena podsumowująca (P) –** podsumowuje osiągnięte efekty kształcenia **(wybór z listy)**
Wykład	F2 – obserwacja/aktywność podczas zajęć	P1 – egzamin pisemny
Laboratorium	F2 – obserwacja/aktywność (przygotowanie do zajęć, ocena ćwiczeń wykonywanych podczas zajęć), F3 – praca pisemna (sprawozdanie, dokumentacja projektu, pisemna analiza problemu), F5 - ćwiczenia praktyczne (ćwiczenia z wykorzystaniem sprzętu i oprogramowania fachowego)	P3 – ocena podsumowująca powstała na podstawie ocen formujących, uzyskanych w semestrze oraz oceny sprawozdań jako pracy pisemnej
Projekt	F3 – dokumentacja projektu F4 – wystąpienie – analiza projektu	P4 – praca pisemna - projekt

H-1 Metody weryfikacji osiągnięcia przedmiotowych efektów kształcenia (wstawić „x")

Efekty przedmiotowe	Wykład		Laboratorium		Projekt	
	F2	P1	F3	P3	F4	P3
EPW1	x	x				
EPW2	x	x				
EPU1			x	x	x	x
EPU2			x	x	x	x
EPK1	x	x				

I – Kryteria oceniania

Wymagania określające kryteria uzyskania oceny w danym efekcie			
Ocena			
Przedmiotowy efekt kształcenia (EP..)	**Dostateczny , dostateczny plus 3/3,5**	**Dobry, dobry plus 4/4,5**	**bardzo dobry 5**
EPW1	Student opanował w stopniu podstawowym elementarną wiedzę z zakresu podstaw informatyki obejmującą przetwarzanie informacji, architekturę i organizację systemów komputerowych, bezpieczeństwo systemów komputerowych, budowę sieci i aplikacji sieciowych	Student opanował w stopniu dobrym elementarną wiedzę z zakresu podstaw informatyki obejmującą przetwarzanie informacji, architekturę i organizację systemów komputerowych, bezpieczeństwo systemów komputerowych, budowę sieci i aplikacji sieciowych	Student w pełni opanował elementarną wiedzę z zakresu podstaw informatyki obejmującą przetwarzanie informacji, architekturę i organizację systemów komputerowych, bezpieczeństwo systemów komputerowych, budowę sieci i aplikacji sieciowych
EPW2	Student ma podstawową wiedzę ogólną obejmującą kluczowe zagadnienia bezpieczeństwa systemów, urządzeń i procesów	Student ma ugruntowaną wiedzę ogólną obejmującą kluczowe zagadnienia bezpieczeństwa systemów, urządzeń i procesów	Student ma bardzo dobrą wiedzę ogólną obejmującą kluczowe zagadnienia bezpieczeństwa systemów, urządzeń i procesów
EPU1	Student potrafi w stopniu elementarnym pozyskiwać informacje z literatury, baz danych i innych źródeł; potrafi integrować uzyskane informacje, dokonywać ich interpretacji, a także wyciągać wnioski oraz formułować i uzasadniać opinie	Student potrafi w stopniu dobrym pozyskiwać informacje z literatury, baz danych i innych źródeł; potrafi integrować uzyskane informacje, dokonywać ich interpretacji, a także wyciągać wnioski oraz formułować i uzasadniać opinie	Student potrafi efektywnie pozyskiwać informacje z literatury, baz danych i innych źródeł; potrafi integrować uzyskane informacje, dokonywać ich interpretacji, a także wyciągać wnioski oraz formułować i uzasadniać opinie

EPU2	Student potrafi w zakresie elementarnym posłużyć się właściwie dobranymi metodami i urządzeniami umożliwiającymi zapewnienie bezpieczeństwa systemów i urządzeń	Student potrafi w stopniu dobrym posłużyć się właściwie dobranymi metodami i urządzeniami umożliwiającymi zapewnienie bezpieczeństwa systemów i urządzeń	Student potrafi efektywnie posłużyć się właściwie dobranymi metodami i urządzeniami umożliwiającymi zapewnienie bezpieczeństwa systemów i urządzeń
EPK1	Student ma podstawową świadomość ważności i zrozumienie skutków działalności inżynierskiej oraz związanej z tym odpowiedzialności za podejmowane decyzje	Student ma zadowalającą świadomość ważności i zrozumienie skutków działalności inżynierskiej oraz związanej z tym odpowiedzialności za podejmowane decyzje	Student ma ugruntowaną świadomość ważności i zrozumienie skutków działalności inżynierskiej oraz związanej z tym odpowiedzialności za podejmowane decyzje

J – Forma zaliczenia przedmiotu

Wykład - egzamin (test)

Laboratorium – zaliczenie z oceną. Na ocenę składa się oddanie min. 7 sprawozdawań, z laboratorium które są podstawą przystąpienia do kolokwium zaliczeniowego.

Projekt– zaliczenie z oceną. Ocenie podlegać będzie wykonanie projektu.

Kryteria ocen dla wykładu, projektu i laboratorium:

0-50 % – niedostateczna
51-60 % – dostateczna
61-70 % – dostateczna plus
71-80 % - dobry
81-90 % dobry plus
91-100 % bardzo dobry

K – Literatura przedmiotu

Literatura obowiązkowa:

1. W. Stallings, Kryptografia i bezpieczeństwo sieci komputerowych, Helion 2012.

2. C. Adams, S. Lloyd, Podpis elektroniczny. Klucz publiczny, Robomatic, Wrocław 2002.

3. A. J. Menezes, P.C. van Oorschot, S.A Vanstone, Handbook of Applied Cryptography (dostęp: 16.12.2019) https://doc.lagout.org/network/3_Cryptography/CRC%20Press%20-%20Handbook%20of%20applied%20Cryptography.pdf

Literatura zalecana / fakultatywna:

1. A. Szeląg, Windows Server 2008. Infrastruktura klucza publicznego (PKI), Helion, Gliwice 2008.

2. Rozporządzenie z dnia 7 sierpnia 2002 r. w sprawie określenia warunków technicznych i organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego (Dz.U. 2002 nr 128 poz.1094).

3. A. Ross, Inżynieria Zabezpieczeń, WNT, Warszawa 2005

L – Obciążenie pracą studenta:

Forma aktywności studenta	Liczba godzin na realizację	
	na studiach stacjonarnych	na studiach niestacjonarnych
Godziny zajęć z nauczycielem/ami	60	35
Konsultacje	5	5
Czytanie literatury	5	10
Przygotowanie do zajęć laboratoryjnych	5	10
Opracowanie sprawozdania z ćwiczeń laboratoryjnych	10	15
Przygotowanie projektu	10	15
Przygotowanie do egzaminu	5	10
Suma godzin:	**100**	**100**
Liczba punktów ECTS dla przedmiotu (suma godzin : 25 godz.):	**4**	**4**

Ł – Informacje dodatkowe

Imię i nazwisko sporządzającego	Łukasz Lemieszewski
Data sporządzenia / aktualizacji	16 grudnia 2019 r.
Dane kontaktowe (e-mail, telefon)	llemieszewski@ajp.edu.pl
Podpis	

Pozycja w planie studiów (lub kod przedmiotu)	C.2.9.

Wydział	Techniczny
Kierunek	Inżynieria bezpieczeństwa
Poziom studiów	Studia pierwszego stopnia
Forma studiów	Stacjonarne / Niestacjonarne
Profil kształcenia	Profil praktyczny

PROGRAM PRZEDMIOTU/MODUŁU

A - Informacje ogólne

1. Nazwa przedmiotu	**Bezpieczeństwo systemów komputerowych**
2. Punkty ECTS	**4**
3. Rodzaj przedmiotu	**Obowiązkowy**
4. Język przedmiotu	**język polski**
5. Rok studiów	**III**
6. Imię i nazwisko koordynatora przedmiotu oraz prowadzących zajęcia	**Pracownicy WT AJP**

B – Formy dydaktyczne prowadzenia zajęć i liczba godzin w semestrze

Nr semestru	Studia stacjonarne	Studia niestacjonarne
Semestr 5	**W**: 30; **Lab.**: 15; **Proj.**: 15;	**W**: 15; **Lab.**: 10; **Proj.**: 10;
Liczba godzin ogółem	**60**	**35**

C - Wymagania wstępne

D - Cele kształcenia

Wiedza	
CW1	Przekazanie wiedzy w zakresie wiedzy technicznej obejmującej terminologię, pojęcia, teorie, zasady, metody, techniki, narzędzia i materiały stosowane przy rozwiązywaniu zadań inżynierskich związanych z szeroko pojętym bezpieczeństwem i rozpoznawaniem zagrożeń, procesami planowania i realizacji eksperymentów, tak w procesie przygotowania z udziałem metod symulacji komputerowych, jak i w rzeczywistym środowisku.
CW2	Przekazanie wiedzy ogólnej dotyczącej standardów i norm technicznych dotyczących zagadnień inżynierii bezpieczeństwa systemów, urządzeń, procesów, i związanych z tym technik i metod programowania, szyfrowania danych, zarządzania jakością i analizy ryzyka
Umiejętności	
CU1	Wyrobienie umiejętności w zakresie doskonalenia wiedzy, pozyskiwania i integrowanie informacji z literatury, baz danych i innych źródeł, opracowywania dokumentacji, prezentowania ich i podnoszenia kompetencji zawodowych
CU2	Wyrobienie umiejętności projektowania i monitorowania stanu i warunków bezpieczeństwa: wykonywania analiz bezpieczeństwa i ryzyka, kontrolowania przestrzegania przepisów i zasad bezpieczeństwa, kontrolowania warunków pracy i standardów bezpieczeństwa, prowadzenia badań okoliczności awarii i wypadków, prowadzenia szkoleń, pełnienia funkcji organizatorskich w zakresie zarządzania bezpieczeństwem oraz prowadzenia dokumentacji związanej z szeroko rozumianym bezpieczeństwem
Kompetencje społeczne	

CK1	Przygotowanie do uczenia się przez całe życie, podnoszenie kompetencji zawodowych, osobistych i społecznych w zmieniającej się rzeczywistości, podjęcia pracy związanej z funkcjonowaniem systemu bezpieczeństwa, którego głównym celem jest ratowanie i ochrona życia, zdrowia i mienia przed zagrożeniami
CK2	Uświadomienie ważności i rozumienia społecznych skutków działalności inżynierskiej, w tym jej wpływu na środowisko i związanej z tym odpowiedzialności za podejmowane decyzje, współdziałanie w grupie i przyjmowanie odpowiedzialności za wspólne realizacje, kreatywność i przedsiębiorczość oraz potrzebę przekazywania informacji odnośnie osiągnięć technicznych i działania inżyniera.

E - Efekty kształcenia przedmiotowe i kierunkowe

Efekty kształcenia (E) w zakresie wiedzy (W), umiejętności (U) i kompetencji społecznych (K)		**Kierunkowy efekt kształcenia**
Wiedza (EW…)		
EPW1	Student, który zaliczył przedmiot ma elementarną wiedzę z zakresu podstaw informatyki obejmującą przetwarzanie informacji, architekturę i organizację systemów komputerowych, bezpieczeństwo systemów komputerowych, budowę sieci i aplikacji sieciowych	K_W04
EPW2	Student, który zaliczył przedmiot ma wiedzę ogólną obejmującą kluczowe zagadnienia bezpieczeństwa systemów, urządzeń i procesów	K_W05
Umiejętności (EU…)		
EPU1	Student, który zaliczył przedmiot potrafi pozyskiwać informacje z literatury, baz danych i innych źródeł; potrafi integrować uzyskane informacje, dokonywać ich interpretacji, a także wyciągać wnioski oraz formułować i uzasadniać opinie	K_U01
EPU2	Student, który zaliczył przedmiot potrafi posłużyć się właściwie dobranymi metodami i urządzeniami umożliwiającymi zapewnienie bezpieczeństwa systemów i urządzeń	K_U19
Kompetencje społeczne (EK…)		
EPK1	Student, który zaliczył przedmiot ma świadomość ważności i rozumie skutki działalności inżynierskiej oraz związanej z tym odpowiedzialności za podejmowane decyzje	K_K02

F - Treści programowe oraz liczba godzin na poszczególnych formach zajęć

Lp.	**Treści wykładów**	**Liczba godzin na studiach**	
		stacjonarnych	**niestacjonarnych**
W1	Podstawowe definicje i uwarunkowania prawne– bezpieczeństwa systemów i sieci komputerowych	2	1
W2	Sieć komputerowa – model OSI, protokoły i usługi	2	1
W3	Kryptografia symetryczna – przykłady zastosowań i analiza bezpieczeństwa	2	1
W4	Kryptografia asymetryczna – przykłady i analiza bezpieczeństwa	2	1
W5	Szyfrowanie w usługach: poczty e-mail, praca zdalna, certyfikacja dostępu	2	1
W6	Projekt hackingu	2	1
W7	Wirusy i robaki	2	1
W8	Antywirusy i zapory sieciowe – konfiguracja i możliwości	2	1
W9	Rozproszone ataki DoS	2	1
W10	Praktyczna ocena bezpieczeństwa	2	1
W11	Ochrona prywatności	2	1
W12	Programowe systemy wykrywania i przeciwdziałania incydentom	2	1
W13	Krajowe ramy interoperacyjności	2	1
W14	Własność intelektualna	2	1
W15	Podsumowanie i zaliczenie	2	
	Razem liczba godzin wykładów:	**30**	**15**

Lp.	Treści laboratoriów	Liczba godzin na studiach	
		stacjonarnych	niestacjonarnych
L1	Definicje podatności oraz analiza podatnych zasobów systemu i sieci komputerowych	1	1
L2	Zastosowania kryptografii w zabezpieczaniu danych i systemów sieciowych	2	1
L3	Usługi i ruch sieciowy – wykorzystanie narzędzi Nmap i BurpSuite wanalizie	2	2
L4	Konfiguracji sieci i usług sieciowych z uwzględnieniem metod bezpieczeństwa	2	2
L5	Przepełnienie bufora, XSS oraz SQL injection – metody przeciwdziałania	2	1
L6	Wykorzystanie programu SNORT jako systemu wykrywania incydentów	2	1
L7	Analiza podatności w sieciach bezprzewodowych Wi-fi	2	1
L8	Podsumowanie i zaliczenie	2	1
	Razem liczba godzin laboratoriów	**15**	**10**

Lp.	Treści projektów	Liczba godzin na studiach	
		stacjonarnych	niestacjonarnych
P1	Wprowadzenie do realizacji samodzielnych zadań projektowych	1	1
P2	Prezentacja tematyki projektów	2	1
P3	Omówienie zasad przygotowywania prezentacji, przykłady. Omówienie zasad prowadzenia prezentacji	2	1
P4	Przydział tematów projektowych, dyskusja	2	1
P5	Realizacja szkicu projektu w grupach, prezentacja szkiców projektów, dyskusja	2	1
P6	Realizacja skorygowanych projektów	2	2
P7	Prezentacja projektów	2	2
P8	Podsumowanie i zaliczenie przedmiotu	2	1
	Razem liczba godzin projektów	15	10

G – Metody oraz środki dydaktyczne wykorzystywane w ramach poszczególnych form zajęć

Forma zajęć	Metody dydaktyczne (wybór z listy)	Środki dydaktyczne
Wykład	Wykład informacyjny Wykład problemowy połączony z dyskusją	Komputer i projektor multimedialny, tablica suchościeralna
Laboratoria	Ćwiczenia doskonalące umiejętność selekcjonowania, grupowania i przedstawiania zgromadzonych informacji	Komputer i projektor multimedialny, tablica suchościeralna Sala komputerowa z dostępem do internetu
Projekt	Selekcjonowanie, grupowanie i dobór informacji do realizacji zadania inżynierskiego	Komputer i projektor multimedialny, tablica suchościeralna Sala komputerowa z dostępem do internetu

H - Metody oceniania osiągnięcia efektów kształcenia na poszczególnych formach zajęć

Forma zajęć	**Ocena formująca (F) –** wskazuje studentowi na potrzebę uzupełniania wiedzy lub stosowania określonych metod i narzędzi, stymulujące do doskonalenia efektów pracy **(wybór z listy)**	**Ocena podsumowująca (P) –** podsumowuje osiągnięte efekty kształcenia **(wybór z listy)**
Wykład	F2 – obserwacja/aktywność	P2 – kolokwium podsumowujące semestr
Laboratorium	F3 – praca pisemna	P3 – ocena podsumowująca powstała na podstawie ocen formujących, uzyskanych w semestrze
Projekt	F4 – wystąpienie	P3 – ocena podsumowująca powstała na podstawie ocen formujących, uzyskanych w semestrze

H-1 Metody weryfikacji osiągnięcia przedmiotowych efektów kształcenia (wstawić „x")

Efekty przedmiotowe	Wykład		Laboratorium		Projekt	
	F2	P1	F3	P3	F4	P3
EPW1	x	x				
EPW2	x	x				
EPU1			x	x	x	x
EPU2			x	x	x	x
EPK1	x	x				

I – Kryteria oceniania

Wymagania określające kryteria uzyskania oceny w danym efekcie			
Ocena			
Przedmiotowy efekt kształcenia (EP..)	**Dostateczny , dostateczny plus 3/3,5**	**Dobry, dobry plus 4/4,5**	**bardzo dobry 5**
EPW1	Student opanował w stopniu podstawowym elementarną wiedzę z zakresu podstaw informatyki obejmującą przetwarzanie informacji, architekturę i organizację systemów komputerowych, bezpieczeństwo systemów komputerowych, budowę sieci i aplikacji sieciowych	Student opanował w stopniu dobrym elementarną wiedzę z zakresu podstaw informatyki obejmującą przetwarzanie informacji, architekturę i organizację systemów komputerowych, bezpieczeństwo systemów komputerowych, budowę sieci i aplikacji sieciowych	Student w pełni opanował elementarną wiedzę z zakresu podstaw informatyki obejmującą przetwarzanie informacji, architekturę i organizację systemów komputerowych, bezpieczeństwo systemów komputerowych, budowę sieci i aplikacji sieciowych
EPW2	Student ma podstawową wiedzę ogólną obejmującą kluczowe zagadnienia bezpieczeństwa systemów, urządzeń i procesów	Student ma ugruntowaną wiedzę ogólną obejmującą kluczowe zagadnienia bezpieczeństwa systemów, urządzeń i procesów	Student ma bardzo dobrą wiedzę ogólną obejmującą kluczowe zagadnienia bezpieczeństwa systemów, urządzeń i procesów
EPU1	Student potrafi w stopniu elementarnym pozyskiwać informacje z literatury, baz danych i innych źródeł; potrafi integrować uzyskane informacje, dokonywać ich interpretacji, a także wyciągać wnioski oraz formułować i uzasadniać opinie	Student potrafi w stopniu dobrym pozyskiwać informacje z literatury, baz danych i innych źródeł; potrafi integrować uzyskane informacje, dokonywać ich interpretacji, a także wyciągać wnioski oraz formułować i uzasadniać opinie	Student potrafi efektywnie pozyskiwać informacje z literatury, baz danych i innych źródeł; potrafi integrować uzyskane informacje, dokonywać ich interpretacji, a także wyciągać wnioski oraz formułować i uzasadniać opinie

EPU2	Student potrafi w zakresie elementarnym posłużyć się właściwie dobranymi metodami i urządzeniami umożliwiającymi zapewnienie bezpieczeństwa systemów i urządzeń	Student potrafi w stopniu dobrym posłużyć się właściwie dobranymi metodami i urządzeniami umożliwiającymi zapewnienie bezpieczeństwa systemów i urządzeń	Student potrafi efektywnie posłużyć się właściwie dobranymi metodami i urządzeniami umożliwiającymi zapewnienie bezpieczeństwa systemów i urządzeń
EPK1	Student ma podstawową świadomość ważności i zrozumienie skutków działalności inżynierskiej oraz związanej z tym odpowiedzialności za podejmowane decyzje	Student ma zadowalającą świadomość ważności i zrozumienie skutków działalności inżynierskiej oraz związanej z tym odpowiedzialności za podejmowane decyzje	Student ma ugruntowaną świadomość ważności i zrozumienie skutków działalności inżynierskiej oraz związanej z tym odpowiedzialności za podejmowane decyzje

J – Forma zaliczenia przedmiotu

Wykład - zaliczenie z oceną (test)

Laboratorium – zaliczenie z oceną. Na ocenę składa się oddanie min. 7 sprawozdawań, z laboratorium które są podstawą przystąpienia do kolokwium zaliczeniowego.

Projekt– zaliczenie z oceną. Ocenie podlegać będzie wykonanie projektu.

Kryteria ocen dla wykładu, projektu i laboratorium:

0-50 % – niedostateczna
51-60 % – dostateczna
61-70 % – dostateczna plus
71-80 % - dobry
81-90 % dobry plus
91-100 % bardzo dobry

K – Literatura przedmiotu

Literatura obowiązkowa:

1. A. Ross, Inżynieria zabezpieczeń, WNT, Warszawa 2005.
2. G. Weidman, Bezpieczny System w Praktyce, Wyższa szkoła Hawkingu i testy penetracyjne, Helion Gliwice 2014
3. J. Muniz, A. Lakhani, Kali Linux, Testy penetracyjne, Helion, Gliwice 2013 .

Literatura zalecana / fakultatywna:

1. M. Agarwal, A. Singh, Metasploit Receptury pen testera, Helion, Gliwice 2013
2. V. Remachandran, BackTrack 5, Testy penetracyjne sici wi-fi, Helion, Gliwice 2013
3. M. Zalewski, Splątana sieć, Przewodnik po bezpieczeństwie aplikacji WWW, Helion, Gliwice 2012

L – Obciążenie pracą studenta:

Forma aktywności studenta	Liczba godzin na realizację	
	na studiach stacjonarnych	na studiach niestacjonarnych
Godziny zajęć z nauczycielem/ami	60	35
Konsultacje	5	5
Czytanie literatury	5	10
Przygotowanie do zajęć laboratoryjnych	5	5
Opracowanie sprawozdania z ćwiczeń laboratoryjnych	10	15
Przygotowanie do projektów	10	15
Przygotowanie do egzaminu	5	15
Suma godzin:	**100**	**100**
Liczba punktów ECTS dla przedmiotu (suma godzin : 25 godz.):	**4**	**4**

Ł – Informacje dodatkowe

Imię i nazwisko sporządzającego	Łukasz Lemieszewski
Data sporządzenia / aktualizacji	16 grudnia 2019 r.
Dane kontaktowe (e-mail, telefon)	llemieszewski@ajp.edu.pl
Podpis	

Pozycja w planie studiów (lub kod przedmiotu)	C.2.10

Wydział	Techniczny
Kierunek	Inżynieria bezpieczeństwa
Poziom studiów	Pierwszego stopnia
Forma studiów	Stacjonarne/niestacjonarne
Profil kształcenia	Praktyczny

PROGRAM PRZEDMIOTU/MODUŁU

A - Informacje ogólne

1. Nazwa przedmiotu	**Telekomunikacyjne systemy satelitarne**
2. Punkty ECTS	**5**
3. Rodzaj przedmiotu	**obowiązkowy**
4. Język przedmiotu	**polski**
5. Rok studiów	**III**
6. Imię i nazwisko koordynatora przedmiotu oraz prowadzących zajęcia	**dr inż. Łukasz Lemieszewski pracownicy Wydziału Technicznego AJP**

B – Formy dydaktyczne prowadzenia zajęć i liczba godzin w semestrze

Nr semestru	Studia stacjonarne	Studia niestacjonarne
Semestr 6	**W**: 30; **Lab**.:15; **Pr**oj.: 30	**W**: 15; **Lab**.: 10; **Pr**oj.: 18
Liczba godzin ogółem	**75**	**43**

C - Wymagania wstępne

Znajomość zagadnień z zakresu ataków i wykrywanie włamań w sieciach oraz kryptografii

D - Cele kształcenia

	Wiedza
CW1	Przekazanie wiedzy w zakresie wiedzy technicznej obejmującej terminologię, pojęcia, teorie, zasady, metody, techniki, narzędzia i materiały stosowane przy rozwiązywaniu zadań inżynierskich związanych z szeroko pojętym bezpieczeństwem i rozpoznawaniem zagrożeń, procesami planowania i realizacji eksperymentów, tak w procesie przygotowania z udziałem metod symulacji komputerowych, jak i w rzeczywistym środowisku.
CW2	Przekazanie wiedzy ogólnej dotyczącej standardów i norm technicznych dotyczących zagadnień inżynierii bezpieczeństwa systemów, urządzeń, procesów, i związanych z tym technik i metod programowania, szyfrowania danych, zarządzania jakością i analizy ryzyka
	Umiejętności
CU1	Wyrobienie umiejętności w zakresie doskonalenia wiedzy, pozyskiwania i integrowanie informacji z literatury, baz danych i innych źródeł, opracowywania dokumentacji, prezentowania ich i podnoszenia kompetencji zawodowych
CU2	Wyrobienie umiejętności projektowania i monitorowania stanu i warunków bezpieczeństwa: wykonywania analiz bezpieczeństwa i ryzyka, kontrolowania przestrzegania przepisów i zasad bezpieczeństwa, kontrolowania warunków pracy i standardów bezpieczeństwa, prowadzenia badań okoliczności awarii i wypadków, prowadzenia szkoleń, pełnienia funkcji organizatorskich w zakresie zarządzania bezpieczeństwem oraz prowadzenia dokumentacji związanej z szeroko rozumianym bezpieczeństwem
	Kompetencje społeczne
CK1	Przygotowanie do uczenia się przez całe życie, podnoszenie kompetencji zawodowych, osobistych i społecznych w zmieniającej się rzeczywistości, podjęcia pracy związanej z funkcjonowaniem systemu bezpieczeństwa, którego głównym celem jest ratowanie i ochrona życia, zdrowia i mienia przed

	zagrożeniami
CK2	Uświadomienie ważności i rozumienia społecznych skutków działalności inżynierskiej, w tym jej wpływu na środowisko i związanej z tym odpowiedzialności za podejmowane decyzje, współdziałanie w grupie i przyjmowanie odpowiedzialności za wspólne realizacje, kreatywność i przedsiębiorczość oraz potrzebę przekazywania informacji odnośnie osiągnięć technicznych i działania inżyniera.

E - Efekty kształcenia przedmiotowe i kierunkowe

Efekty kształcenia (E) w zakresie wiedzy (W), umiejętności (U) i kompetencji społecznych (K)		**Kierunkowy efekt kształcenia**
Wiedza (EW…)		
EPW1	Student, który zaliczył przedmiot ma elementarną wiedzę z zakresu podstaw informatyki obejmującą przetwarzanie informacji, architekturę i organizację systemów komputerowych, bezpieczeństwo systemów komputerowych, budowę sieci i aplikacji sieciowych	K_W04
EPW2	Student, który zaliczył przedmiot ma wiedzę ogólną obejmującą kluczowe zagadnienia bezpieczeństwa systemów, urządzeń i procesów	K_W05
Umiejętności (EU…)		
EPU1	Student, który zaliczył przedmiot potrafi pozyskiwać informacje z literatury, baz danych i innych źródeł; potrafi integrować uzyskane informacje, dokonywać ich interpretacji, a także wyciągać wnioski oraz formułować i uzasadniać opinie	K_U01
EPU2	Student, który zaliczył przedmiot potrafi posłużyć się właściwie dobranymi metodami i urządzeniami umożliwiającymi zapewnienie bezpieczeństwa systemów i urządzeń	K_U19
Kompetencje społeczne (EK…)		
EPK1	Student, który zaliczył przedmiot ma świadomość ważności i rozumie skutki działalności inżynierskiej oraz związanej z tym odpowiedzialności za podejmowane decyzje	K_K02

F - Treści programowe oraz liczba godzin na poszczególnych formach zajęć

Lp.	**Treści wykładów**	**Liczba godzin na studiach**	
		stacjonarnych	**niestacjonarnych**
W1	Wprowadzenie do przedmiotu, terminologia, stan techniki w dziedzinie	2	1
W2	Orbity okołoziemskie - parametry, charakterystyka	2	1
W3	Satelita telekomunikacyjny: historia ewolucji, budowa, charakterystyka	2	1
W4	Systemy łączności satelitarnej: historia, stan obecny, perspektywy rozwoju	2	1
W5	Przegląd satelitarnych systemów telekomunikacyjnych.	2	1
W6	Struktura sieci VSAT	2	1
W7	Struktura sieci SCPC	2	1
W8	Budowa satelitarnych systemów telekomunikacyjnych na bazie satelitów geostacjonarnych	2	2
W9	Parametry satelitarnych kanałów danych	2	2
W10	Przegląd sprzętu radiowego satelitarnych stacji naziemnych	2	2
W11	Charakterystyki techniczne i różnice w sprzęcie radiowym	2	1
W12	Obliczanie kanałów satelitarnych VSAT	2	1
W13	Obliczanie kanałów satelitarnych SCPC	2	1
W14	Optymalizacja parametrów kanałów satelitarnych	2	1
W15	Podsumowanie przedmiotu i zaliczenie	2	1
	Razem liczba godzin wykładów	30	18

Lp.	**Treści laboratoriów**	**Liczba godzin na studiach**	
		stacjonarnych	**niestacjonarnych**
L1	Wprowadzenie do systemu HN. Instalacja i konserwacja zdalnych terminali.	2	1
L2	Przygotowywanie i konserwacja NOC Hughes HN	2	1
L3	Obliczenia sieciowe w systemie HN	2	1

L4	Instalacja i konserwacja urządzeń VoIP	2	1
L5	Wprowadzenie do systemu HX. Instalacja i konserwacja zdalnych terminali	2	1
L6	Przygotowywanie i konserwacja NOC Hughes HX	2	2
L7	Konfigurowanie i planowanie systemu HX	2	2
L8	Obliczenia sieciowe w systemie HX. Zaliczenie.	1	1
	Razem liczba godzin projektów	15	10

Lp.	**Treści projektów**	**Liczba godzin na studiach**	
		stacjonarnych	**niestacjonarnych**
P1	Wprowadzenie do realizacji samodzielnych zadań projektowych	2	1
P2	Prezentacja tematyki projektów	2	1
P3	Omówienie zasad przygotowywania prezentacji, przykłady.	2	1
P4	Omówienie zasad prowadzenia prezentacji, przykłady	2	1
P5	Opracowanie listy tematów projektowych i dyskusja	2	1
P6	Przydział tematów projektowych	2	1
P7	Realizacja szkicu projektu w grupach	2	1
P8	Prezentacja szkiców projektów, dyskusja	2	1
P9	Realizacja skorygowanych wersji szkiców projektów	2	1
P10	Prezentacja skorygowanych szkiców projektów, dyskusja	2	1
P11	Realizacja projektów cz. 1	2	1
P12	Realizacja projektów cz. 2	2	1
P13	Prezentacja projektów cz. 1	2	2
P14	Prezentacja projektów cz. 2	2	2
P15	Podsumowanie i zaliczenie przedmiotu	2	2
	Razem liczba godzin projektów	30	18

G – Metody oraz środki dydaktyczne wykorzystywane w ramach poszczególnych form zajęć

Forma zajęć	**Metody dydaktyczne (wybór z listy)**	**Środki dydaktyczne**
Wykład	Wykład informacyjny Wykład problemowy połączony z dyskusją	Komputer i projektor multimedialny, tablica suchościeralna
Laboratoria	Ćwiczenia doskonalące umiejętność selekcjonowania, grupowania i przedstawiania zgromadzonych informacji	Komputer i projektor multimedialny, tablica suchościeralna Sala komputerowa z dostępem do internetu i sprzętem komunikacji satelitarnej HUGHES HN i HX
Projekt	Selekcjonowanie, grupowanie i dobór informacji do realizacji zadania inżynierskiego	Komputer i projektor multimedialny, tablica suchościeralna Sala komputerowa z dostępem do internetu i sprzętem komunikacji satelitarnej HUGHES HN i HX

H - Metody oceniania osiągnięcia efektów kształcenia na poszczególnych formach zajęć

Forma zajęć	**Ocena formująca (F) –** wskazuje studentowi na potrzebę uzupełniania wiedzy lub stosowania określonych metod i narzędzi, stymulujące do doskonalenia efektów pracy **(wybór z listy)**	**Ocena podsumowująca (P) –** podsumowuje osiągnięte efekty kształcenia **(wybór z listy)**
Wykład	F3 – praca pisemna	P2 – kolokwium
Laboratorium	F3 – praca pisemna	P3 – ocena podsumowująca powstała na podstawie ocen formujących, uzyskanych

		w semestrze
Projekt	F4 – wystąpienie	P3 – ocena podsumowująca powstała na podstawie ocen formujących, uzyskanych w semestrze

H-1 Metody weryfikacji osiągnięcia przedmiotowych efektów kształcenia (wstawić „x")

Efekty przedmiotowe	Wykład		Laboratorium		Projekt	
	F3	P2	F4	P3	F4	P3
EPW1	x	x				
EPW2	x	x	x	x		
EPU1			x	x	x	x
EPU2			x	x	x	x
EPK1	x	x			x	x

I – Kryteria oceniania

Wymagania określające kryteria uzyskania oceny w danym efekcie			
Ocena			
Przedmiotowy efekt kształcenia (EP..)	**Dostateczny , dostateczny plus 3/3,5**	**Dobry, dobry plus 4/4,5**	**bardzo dobry 5**
EPW1	Student opanował w stopniu podstawowym elementarną wiedzę z zakresu podstaw informatyki obejmującą przetwarzanie informacji, architekturę i organizację systemów komputerowych, bezpieczeństwo systemów komputerowych, budowę sieci satelitarnych i satelitarnych aplikacji sieciowych	Student opanował w stopniu dobrym elementarną wiedzę z zakresu podstaw informatyki obejmującą przetwarzanie informacji, architekturę i organizację systemów komputerowych, bezpieczeństwo systemów komputerowych, budowę sieci satelitarnych i satelitarnych aplikacji sieciowych	Student w pełni opanował elementarną wiedzę z zakresu podstaw informatyki obejmującą przetwarzanie informacji, architekturę i organizację systemów komputerowych, bezpieczeństwo systemów komputerowych, budowę sieci satelitarnych i satelitarnych aplikacji sieciowych
EPW2	Student ma podstawową wiedzę ogólną obejmującą kluczowe zagadnienia bezpieczeństwa systemów satelitarnych, urządzeń i procesów	Student ma ugruntowaną wiedzę ogólną obejmującą kluczowe zagadnienia bezpieczeństwa systemów satelitarnych, urządzeń i procesów	Student ma bardzo dobrą wiedzę ogólną obejmującą kluczowe zagadnienia bezpieczeństwa systemów satelitarnych, urządzeń i procesów
EPU1	Student potrafi w stopniu elementarnym pozyskiwać informacje z literatury, baz danych i innych źródeł; potrafi integrować uzyskane informacje, dokonywać ich interpretacji, a także wyciągać wnioski oraz formułować i uzasadniać opinie	Student potrafi w stopniu dobrym pozyskiwać informacje z literatury, baz danych i innych źródeł; potrafi integrować uzyskane informacje, dokonywać ich interpretacji, a także wyciągać wnioski oraz formułować i uzasadniać opinie	Student potrafi efektywnie pozyskiwać informacje z literatury, baz danych i innych źródeł; potrafi integrować uzyskane informacje, dokonywać ich interpretacji, a także wyciągać wnioski oraz formułować i uzasadniać opinie
EPU2	Student potrafi w zakresie elementarnym posłużyć się właściwie dobranymi metodami i urządzeniami umożliwiającymi zapewnienie bezpieczeństwa systemów satelitarnych i urządzeń	Student potrafi w stopniu dobrym posłużyć się właściwie dobranymi metodami i urządzeniami umożliwiającymi zapewnienie bezpieczeństwa systemów satelitarnych i urządzeń	Student potrafi efektywnie posłużyć się właściwie dobranymi metodami i urządzeniami umożliwiającymi zapewnienie bezpieczeństwa systemów satelitarnych i urządzeń
EPK1	Student ma podstawową świadomość ważności	Student ma zadowalającą świadomość ważności	Student ma ugruntowaną świadomość ważności

	i zrozumienie skutków działalności inżynierskiej oraz związanej z tym odpowiedzialności za podejmowane decyzje	i zrozumienie skutków działalności inżynierskiej oraz związanej z tym odpowiedzialności za podejmowane decyzje	i zrozumienie skutków działalności inżynierskiej oraz związanej z tym odpowiedzialności za podejmowane decyzje

J – Forma zaliczenia przedmiotu

Wykład - zaliczenie z oceną (test)

Laboratorium – zaliczenie z oceną. Na ocenę składa się oddanie min. 7 sprawozdawań, z laboratorium które są podstawą przystąpienia do kolokwium zaliczeniowego.

Projekt– zaliczenie z oceną. Ocenie podlegać będzie wykonanie projektu.

Kryteria ocen dla wykładu, projektu i laboratorium:

0-50 % – niedostateczna
51-60 % – dostateczna
61-70 % – dostateczna plus
71-80 % - dobry
81-90 % dobry plus
91-100 % bardzo dobry

K – Literatura przedmiotu

Literatura obowiązkowa:
1. Strona producenta systemu komunikacji HUGHES HN, HX - https://www.hughes.com/technologies/broadband-satellite-systems
2. Zieliński Ryszard J., Satelitarne sieci teleinformatyczne, Wydawnictwo Naukowe PWN, Warszawa 2009

Literatura zalecana / fakultatywna:
1. Januszewski J., Systemy satelitarne GPS Galileo i inne. Wydawnictwo naukowe PWN, Warszawa 2010
2. Specht C., System GPS. Wydawnictwo Bernardinum, Pelplin 2007

L – Obciążenie pracą studenta:

Forma aktywności studenta	Liczba godzin na realizację	
	na studiach stacjonarnych	na studiach niestacjonarnych
Godziny zajęć z nauczycielem/ami	75	43
Konsultacje	5	7
Czytanie literatury	10	15
Przygotowanie sprawozdań z laboratorium	10	15
Przygotowanie projektu	10	25
Przygotowanie do zaliczenia wykładu	15	20
Suma godzin:	**125**	**125**
Liczba punktów ECTS dla przedmiotu (suma godzin : 25 godz.):	**5**	**5**

Ł – Informacje dodatkowe

Imię i nazwisko sporządzającego	Łukasz Lemieszewski
Data sporządzenia / aktualizacji	16 grudnia 2019 r.
Dane kontaktowe (e-mail, telefon)	llemieszewski@ajp.edu.pl
Podpis	

Pozycja w planie studiów (lub kod przedmiotu)	C.2.11

Wydział	Techniczny
Kierunek	Inżynieria Bezpieczeństwa
Poziom studiów	Pierwszego stopnia
Forma studiów	stacjonarne/niestacjonarne
Profil kształcenia	Praktyczny

PROGRAM PRZEDMIOTU/MODUŁU

A - Informacje ogólne

1. Nazwa przedmiotu	**System zarządzania bezpieczeństwem informacji**
2. Punkty ECTS	**5**
3. Rodzaj przedmiotu	**obowiązkowy**
4. Język przedmiotu	**język polski**
5. Rok studiów	**III**
6. Imię i nazwisko koordynatora przedmiotu oraz prowadzących zajęcia	**Łukasz Lemieszewski**

B – Formy dydaktyczne prowadzenia zajęć i liczba godzin w semestrze

Nr semestru	Studia stacjonarne	Studia niestacjonarne
Semestr 6	**Wykłady**: (30); **Laboratoria**: (15) **Projekt:** (30)	**Wykłady**: (15); **Laboratoria**: (10) **Projekt:** (18)
Liczba godzin ogółem	**75**	**43**

C - Wymagania wstępne

Student nabył podstawową wiedzę z zakresu systemów operacyjnych oraz sieci komputerowych

D - Cele kształcenia

	Wiedza
CW1	przekazanie wiedzy w zakresie wiedzy technicznej obejmującej terminologię, pojęcia, teorie, zasady, metody, techniki, narzędzia i materiały stosowane przy rozwiązywaniu zadań inżynierskich związanych z szeroko pojętym bezpieczeństwem i rozpoznawaniem zagrożeń, procesami planowania i realizacji eksperymentów, tak w procesie przygotowania z udziałem metod symulacji komputerowych, jak i w rzeczywistym środowisku
	Umiejętności
CU1	wyrobienie umiejętności w zakresie doskonalenia wiedzy, pozyskiwania i integrowanie informacji z literatury, baz danych i innych źródeł, opracowywania dokumentacji, prezentowania ich i podnoszenia kompetencji zawodowych
	Kompetencje społeczne
CK1	przygotowanie do uczenia się przez całe życie, podnoszenie kompetencji zawodowych, osobistych i społecznych w zmieniającej się rzeczywistości, podjęcia pracy związanej z funkcjonowaniem systemu bezpieczeństwa, którego głównym celem jest ratowanie i ochro-na życia, zdrowia i mienia przed zagrożeniami

E - Efekty kształcenia przedmiotowe i kierunkowe

Przedmiotowy efekt kształcenia (EP) w zakresie wiedzy (W), umiejętności (U) i kompetencji społecznych (K)		Kierunkowy efekt kształcenia
Wiedza (EPW…)		
EPW1	ma elementarną wiedzę z zakresu podstaw informatyki obejmującą przetwarzanie informacji, architekturę i organizację systemów komputerowych, bezpieczeństwo systemów komputerowych, budowę sieci i aplikacji sieciowych	K_W04
EPW2	orientuje się w obecnym stanie oraz trendach rozwoju bezpieczeństwa systemów informatycznych, urządzeń i procesów	K_W15
Umiejętności (EPU…)		
EPU1	potrafi ocenić ryzyko i bezpieczeństwo systemów i sieci, stosując techniki oraz narzędzia sprzętowe i programowe	K_U12
EPU2	potrafi zaplanować i przeprowadzić symulację oraz pomiary poziomu bezpieczeństwa systemów, sieci i urządzeń; potrafi przedstawić otrzymane wyniki w formie liczbowej i graficznej, dokonać ich interpretacji i wyciągnąć właściwe wnioski	K_U07
Kompetencje społeczne (EPK…)		
EPK1	prawidłowo identyfikuje i rozstrzyga dylematy związane z wykonywaniem zawodu	K_K06

F - Treści programowe oraz liczba godzin na poszczególnych formach zajęć

Lp.	Treści wykładów	Liczba godzin na studiach	
		stacjonarnych	niestacjonarnych
W1	Podstawowe definicje, normatywa i problemy w bezpieczeństwie informacji	2	1
W2	Dostosowanie środków technicznych i IT do Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679	2	1
W3	System zarządzania bezpieczeństwem informacji opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001	2	1
W4	Ustanawiania zabezpieczeń opracowane na podstawie Polskiej Normy PN-ISO/IEC 27002	2	1
W5	Zarządzanie ryzykiem oraz audytowanie na podstawie Polskiej Normy PN-ISO/IEC 27005	2	1
W6	Odtwarzania techniki informatycznej po katastrofie w ramach zarządzania ciągłością działania na podstawie Polskiej Normy PN-ISO/IEC 24762	2	1
W7	Wymagania służące prezentacji informacji wg. Web Content Accessibility Guidelines (WCAG 2.0), z uwzględnieniem poziomu A i AA	2	1
W8	Wymagania dla systemów teleinformatycznych wg. Polskich Norm: PN-ISO/IEC 20000-1	2	1
W9	Wymagania dla systemów teleinformatycznych wg. Polskich Norm: PN-ISO/IEC 20000-2	2	1
W10	Społeczeństwo Informacyjne -Normy i standardy w obszarze systemów zarządzania bezpieczeństwem informacji	2	1
W11	Wstęp do kryptograficznej ochrona danych i systemów	2	1
W12	Metody, narzędzia w uwierzytelnianiu i kontroli dostępu	2	1
W13	Podatności przetwarzania danych i systemów e-Commerce	2	1
W14	Dostosowanie środków organizacyjnych i technicznych. Dokumentacja ochrony danych osobowych i zarządzania bezpieczeństwem.	2	1
W15	Analiza ryzyka i polityka bezpieczeństwa	2	1
	Razem liczba godzin wykładów	30	15

Lp.	Treści laboratoriów	Liczba godzin na studiach	
		stacjonarnych	niestacjonarnych
L1	Infrastruktura systemów bezpieczeństwie informacji i testów penetracyjnych	2	1
L2	Konfigurowanie i obsługa środowiska Kali Linux	2	1
L3	Model OSI/ISO, analiza transmisji podstawowych protokołów komunikacyjnych m.in. TCP, UDP, FTP, DNS, HTTP	3	2
L4	Testy podatności systemu Android za pomocą narzędzia Metasploit	2	1
L5	Ocena luk w zabezpieczeniach, zarządzanie i badania za pomocą m in. buffer overflows, registers, shellcods, x32,x64 exploitation, gaining shell	2	1
L6	Symulacja ataku na klienta i serwer	2	2
L7	Rootkit w trybie użytkownika (usermode) lub systemu operacyjnego (kernel-mode	2	2
	Razem liczba godzin laboratoriów	15	10

Lp.	Treści projektów	Liczba godzin na studiach	
		stacjonarnych	niestacjonarnych
P1	Infrastruktura systemów bezpieczeństwie informacji – wprowadzenie do projektowania.	2	1
P2	Infrastruktura testów penetracyjnych. Wprowadzenie do Kali Linux.	2	1
P3	Tworzenie audytu systemu zarządzania bezpieczeństwem. Część 1.	2	1
P4	Tworzenie audytu systemu zarządzania bezpieczeństwem. Część 2.	2	1
P5	Opracowanie środków organizacyjnych i technicznych zarządzania bezpieczeństwem informacji.	4	2
P6	Analiza ryzyka i dokumentacja zarządzania bezpieczeństwem informacji.	2	2
P7	Testy podatności systemu i zarządzanie bezpieczeństwem informacji. Część 1. Dostępność	2	2
P8	Testy podatności systemu i zarządzanie bezpieczeństwem informacji. Część 2. Integralność	2	2
P9	Testy podatności systemu i zarządzanie bezpieczeństwem informacji. Część 3. Poufność	4	2
P10	Zachowanie poufności, integralności i dostępności zgodnie z normą ISO 27001 w projekcie zarządzania bezpieczeństwem informacji	4	2
P11	Oddanie i prezentacja projektów. Zaliczenie.	4	2
	Razem liczba godzin laboratoriów	30	18

G – Metody oraz środki dydaktyczne wykorzystywane w ramach poszczególnych form zajęć

Forma zajęć	Metody dydaktyczne (wybór z listy)	Środki dydaktyczne
Wykład	wykład informacyjny, pokaz prezentacji multimedialnej	projektor
Ćwiczenia	przygotowanie sprawozdania	komputer z podłączeniem do sieci Internet
Projekt	ćwiczenia doskonalące obsługę oprogramowania komputerowego wspomagającego zarządzanie zasobami informatycznymi, ćwiczenia doskonalące umiejętność selekcjonowania, grupowania i przedstawiania zgromadzonych informacji na temat zarządzania ich bezpieczeństwem,.	stanowisko komputerowe z dostępem do oprogramowania wspomagającego audyt i zarządzanie zasobami informatycznymi

H - Metody oceniania osiągnięcia efektów kształcenia na poszczególnych formach zajęć

Forma zajęć	**Ocena formująca (F) –** wskazuje studentowi na potrzebę uzupełniania wiedzy lub stosowania określonych metod i narzędzi, stymulujące do doskonalenia efektów pracy **(wybór z listy)**	**Ocena podsumowująca (P) –** podsumowuje osiągnięte efekty kształcenia **(wybór z listy)**
Wykład	F2 - obserwacja poziomu przygotowania do zajęć F4 – wystąpienie (prezentacja multimedialna formułowanie dłuższej wypowiedzi ustnej na wybrany temat, ustne formułowanie i rozwiązywanie problemu, wypowiedź problemowa, analiza projektu itd.),	P1 – ocena podsumowująca na podstawie testu wiedzy
Laboratoria	F2 - ocena ćwiczeń wykonywanych jako praca własna F3 – sprawozdanie	P3 – ocena podsumowująca powstała na podstawie ocen formujących, uzyskanych w semestrze
Projekt	F2 – obserwacja/aktywność (przygotowanie do zajęć, ocena ćwiczeń wykonywanych podczas zajęć i jako pracy własnej), F4 – wystąpienie (prezentacja multimedialna formułowanie dłuższej wypowiedzi ustnej na wybrany temat, ustne formułowanie i rozwiązywanie problemu, wypowiedź problemowa, analiza projektu itd.),	P4 – praca pisemna (projekt, referat, raport),

H-1 Metody weryfikacji osiągnięcia przedmiotowych efektów kształcenia (wstawić „x")

Efekty przedmiotowe	Wykład			Laboratoria			Projekt		
	F2	F4	P1	F2	F3	P3	F2	F4	P4
EPW1	x	x	x	x	x	x			
EPW2	x	x	x	x	x	x			
EPU1				x	x	x	x	x	x
EPU2				x	x	x	x	x	x
EPK1	x	x	x						

I – Kryteria oceniania

Wymagania określające kryteria uzyskania oceny w danym efekcie			
Ocena			
Przedmiotowy efekt kształcenia (EP..)	**Dostateczny dostateczny plus 3/3,5**	**dobry dobry plus 4/4,5**	**bardzo dobry 5**
EPW1	ma wiedzę ogólną obejmującą podstawowe zagadnienia bezpieczeństwa systemów, urządzeń i procesów	ma wiedzę ogólną obejmującą większość kluczowych zagadnienia bezpieczeństwa systemów, urządzeń i procesów	ma wiedzę ogólną obejmującą kluczowe zagadnienia bezpieczeństwa systemów, urządzeń i procesów
EPW2	ma podstawową wiedzę w zakresie standardów i norm technicznych związanych z inżynierią bezpieczeństwa	ma podstawową wiedzę w zakresie standardów i norm technicznych związanych z inżynierią bezpieczeństwa oraz systemów	ma podstawową wiedzę w zakresie standardów i norm technicznych związanych z inżynierią bezpieczeństwa systemów, urządzeń i procesów

EPU1	potrafi pozyskiwać informacje z literatury, baz danych i innych źródeł;	potrafi pozyskiwać informacje z literatury, baz danych i innych źródeł; potrafi integrować uzyskane informacje	potrafi pozyskiwać informacje z literatury, baz danych i innych źródeł; potrafi integrować uzyskane informacje, dokonywać ich interpretacji, a także wyciągać wnioski oraz formułować i uzasadniać opinie
EPU2	potrafi opracować dokumentację dotyczącą realizacji zadania inżynierskiego	potrafi opracować dokumentację dotyczącą realizacji zadania inżynierskiego i przygotować tekst zawierający omówienie wybranych wyników realizacji tego zadania	potrafi opracować dokumentację dotyczącą realizacji zadania inżynierskiego i przygotować tekst zawierający omówienie wyników realizacji tego zadania
EPK1	rozumie potrzebę uczenia się przez całe życie – dalsze kształcenie na studiach II stopnia, studia podyplomowe, kursy specjalistyczne, szczególnie ważne w obszarze nauk technicznych, ze zmieniającymi się szybko technologiami, podnosząc w ten sposób kompetencje zawodowe, osobiste i społeczne	rozumie potrzebę uczenia się przez całe życie – dalsze kształcenie na studiach II stopnia, studia podyplomowe, kursy specjalistyczne, szczególnie ważne w obszarze nauk technicznych, ze zmieniającymi się szybko technologiami, podnosząc w ten sposób kompetencje zawodowe, osobiste i społeczne	rozumie potrzebę uczenia się przez całe życie – dalsze kształcenie na studiach II stopnia, studia podyplomowe, kursy specjalistyczne, szczególnie ważne w obszarze nauk technicznych, ze zmieniającymi się szybko technologiami, podnosząc w ten sposób kompetencje zawodowe, osobiste i społeczne

J – Forma zaliczenia przedmiotu

Wykład - egzamin (test)

Laboratorium – zaliczenie z oceną. Na ocenę składa się oddanie min. 7 sprawozdawań, z laboratorium które są podstawą przystąpienia do kolokwium zaliczeniowego.

Projekt– zaliczenie z oceną. Ocenie podlegać będzie wykonanie projektu.

Kryteria ocen dla wykładu, projektu i laboratorium:

0-50 % – niedostateczna
51-60 % – dostateczna
61-70 % – dostateczna plus
71-80 % - dobry
81-90 % dobry plus
91-100 % bardzo dobry

K – Literatura przedmiotu

Literatura obowiązkowa:

1. Kryptografia i bezpieczeństwo sieci komputerowych. William Stalinks, Helion, Gliwice 2011
2. Kali Linux. Testy penetracyjne. Juned Ahmed Ansari, Helion, Gliwice 2015
3. Ross Anderson „Inżynieria zabezpieczeń", WNT 2005
4. Andrzej Białas „Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie", WNT 2006.
5. K. D. Mitnick, W. L. Simson, Sztuka Podstępu, Łamałem ludzi nie hasła, Helion, Gliwice 2010

Literatura zalecana / fakultatywna:

1. ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) NR 910/2014
2. ROZPORZĄDZENIE WYKONAWCZE KOMISJI (UE) 2015/1502
3. ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/679
4. PN ISO/IEC 27001 Systemy zarządzania bezpieczeństwem informacji. Wymagania.
5. PN ISO/IEC 17799:2005 Praktyczne zasady zarządzania bezpieczeństwem informacji.
6. PN-I-13335-1:1998 Wytyczne do zarządzania bezpieczeństwem systemów informacyjnych - Pojęcia i modele bezpieczeństwa systemów informatycznych.

L – Obciążenie pracą studenta:

Forma aktywności studenta	Liczba godzin na realizację	
	na studiach stacjonarnych	na studiach niestacjonarnych
Godziny zajęć z nauczycielem/ami	75	43
Konsultacje	5	7
Czytanie literatury	5	20
Przygotowanie sprawozdań	15	15
Przygotowanie projektu	15	20
Przygotowanie do egzaminu	10	20
Suma godzin:	**125**	**125**
Liczba punktów ECTS dla przedmiotu (suma godzin: 25 godz.):	**5**	**5**

Ł – Informacje dodatkowe

Imię i nazwisko sporządzającego	Łukasz Lemieszewski
Data sporządzenia / aktualizacji	16 grudnia 2019 r.
Dane kontaktowe (e-mail, telefon)	llemieszewski@ajp.edu.pl
Podpis	

Pozycja w planie studiów (lub kod przedmiotu)	C.2.12.

Wydział	Techniczny
Kierunek	Inżynieria bezpieczeństwa
Poziom studiów	Studia pierwszego stopnia
Forma studiów	Stacjonarne / Niestacjonarne
Profil kształcenia	Profil praktyczny

PROGRAM PRZEDMIOTU/MODUŁU

A - Informacje ogólne

1. Nazwa przedmiotu	**Sprzętowe systemy zabezpieczeń w sieciach**
2. Punkty ECTS	**5**
3. Rodzaj przedmiotu	**Obowiązkowy**
4. Język przedmiotu	**język polski**
5. Rok studiów	**III**
6. Imię i nazwisko koordynatora przedmiotu oraz prowadzących zajęcia	**Pracownicy WT AJP**

B – Formy dydaktyczne prowadzenia zajęć i liczba godzin w semestrze

Nr semestru	Studia stacjonarne	Studia niestacjonarne
Semestr VI	**W**: 30; **Lab.**: 15; **Proj.**: 30;	**W**: 15; **Lab.**: 10; **Proj.**: 18;
Liczba godzin ogółem	**75**	**43**

C - Wymagania wstępne

Student nabył podstawową wiedzę z zakresu systemów operacyjnych oraz sieci komputerowych

D - Cele kształcenia

	Wiedza
CW1	Przekazanie wiedzy w zakresie wiedzy technicznej obejmującej terminologię, pojęcia, teorie, zasady, metody, techniki, narzędzia i materiały stosowane przy rozwiązywaniu zadań inżynierskich związanych z szeroko pojętym bezpieczeństwem i rozpoznawaniem zagrożeń, procesami planowania i realizacji eksperymentów, tak w procesie przygotowania z udziałem metod symulacji komputerowych, jak i w rzeczywistym środowisku.
CW2	przekazanie wiedzy ogólnej dotyczącej standardów i norm technicznych dotyczących zagadnień inżynierii bezpieczeństwa systemów, urządzeń, procesów, i związanych z tym technik i metod programowania, szyfrowania danych, zarządzania jakością i analizy ryzyka, C_W3 przekazanie wiedzy dotyczącej bezpieczeństwa i higieny pracy, ochrony własności przemysłowej, prawa autorskiego niezbędnej dla rozumienia i tworzenia społecznych, ekonomicznych, prawnych i pozatechnicznych uwarunkowań działalności inżynierskiej dla rozwoju form indywidualnej przedsiębiorczości i działalności gospodarczej.
	Umiejętności
CU1	wyrobienie umiejętności w zakresie doskonalenia wiedzy, pozyskiwania i integrowanie informacji z literatury, baz danych i innych źródeł, opracowywania dokumentacji, prezentowania ich i podnoszenia kompetencji zawodowych

CU2	wyrobienie umiejętności projektowania i monitorowania stanu i warunków bezpieczeństwa: wykonywania analiz bezpieczeństwa i ryzyka, kontrolowania przestrzegania przepisów i zasad bezpieczeństwa, kontrolowania warunków pracy i standardów bezpieczeństwa, prowadzenia badań okoliczności awarii i wypadków, prowadzenia szkoleń, pełnienia funkcji organizatorskich w zakresie zarządzania bezpieczeństwem oraz prowadzenia dokumentacji związanej z szeroko rozumianym bezpieczeństwem
Kompetencje społeczne	
CK1	przygotowanie do uczenia się przez całe życie, podnoszenie kompetencji zawodowych, osobistych i społecznych w zmieniającej się rzeczywistości, podjęcia pracy związanej z funkcjonowaniem systemu bezpieczeństwa, którego głównym celem jest ratowanie i ochro-na życia, zdrowia i mienia przed zagrożeniami
CK2	uświadomienie ważności i rozumienia społecznych skutków działalności inżynierskiej, w tym jej wpływu na środowisko i związanej z tym odpowiedzialności za podejmowane decyzje, współdziałanie w grupie i przyjmowanie odpowiedzialności za wspólne realizacje, kreatywność i przedsiębiorczość oraz potrzebę przekazywania informacji odnośnie osiągnięć technicznych i działania inżyniera.

E - Efekty kształcenia przedmiotowe i kierunkowe

Efekty kształcenia (E) w zakresie wiedzy (W), umiejętności (U) i kompetencji społecznych (K)		**Kierunkowy efekt kształcenia**
Wiedza (EW…)		
EPW1	Student, który zaliczył przedmiot ma elementarną wiedzę z zakresu podstaw informatyki obejmującą przetwarzanie informacji, architekturę i organizację systemów komputerowych, bezpieczeństwo systemów komputerowych, budowę sieci i aplikacji sieciowych	K_W04
EPW2	Student, który zaliczył przedmiot ma wiedzę ogólną obejmującą kluczowe zagadnienia bezpieczeństwa systemów, urządzeń i procesów	K_W05
Umiejętności (EU…)		
EPU1	Student, który zaliczył przedmiot potrafi pozyskiwać informacje z literatury, baz danych i innych źródeł; potrafi integrować uzyskane informacje, dokonywać ich interpretacji, a także wyciągać wnioski oraz formułować i uzasadniać opinie	K_U01
EPU2	Student, który zaliczył przedmiot potrafi posłużyć się właściwie dobranymi metodami i urządzeniami umożliwiającymi zapewnienie bezpieczeństwa systemów i urządzeń	K_U19
Kompetencje społeczne (EK…)		
EPK1	Student, który zaliczył przedmiot ma świadomość ważności i rozumie skutki działalności inżynierskiej oraz związanej z tym odpowiedzialności za podejmowane decyzje	K_K02

F - Treści programowe oraz liczba godzin na poszczególnych formach zajęć

Lp.	**Treści wykładów**	**Liczba godzin na studiach**	
		stacjonarnych	**niestacjonarnych**
W1	Wprowadzenie do przedmiotu, pojęcia.	2	1
W2	Systemy kryptograficzne i funkcje skrótu.	2	1
W3	Algorytm Diffiego-Hellmana i protokoły dystrybucji kluczy. Przypomnienie.	2	1
W4	Ustawa o podpisie cyfrowym. Certyfikaty i ich zastosowania. Aktulaizacja.	2	1
W5	Certyfikaty X.509 klucza publicznego oraz LDAP.	2	1
W6	Rozszerzone metody ochrony przed atakami na PKI	2	1
W7	Zaawansowane mechanizmy systemu KERBEROS.	2	1
W8	Bezpieczeństwo systemu Windows -- poprawki, zabezpieczanie portów i dzienników zdarzeń	2	1
W9	Bezpieczeństwo systemu Unix -- zabezpieczanie usług i plików	2	1
W10	Zabezpieczanie Sieci -- korzystanie z zapór ogniowych, certyfikatów i szyfrowania	2	1

W11	Rejestrowanie zdarzeń i monitorowanie Sieci	2	1
W12	Systemy detekcji typu IDS/IPS. Metody wykrywania włamań i reagowanie na ataki.	2	1
W13	Centralny serwer rejestracji zdarzeń. Rejestracja działań użytkowników za pomocą systemu rozliczeń i monitorowania dzienników.	2	1
W14	Podział zadań administracyjnych. Dobre praktyki.	2	1
W15	Zaliczenie przedmiotu	2	1
	Razem liczba godzin wykładów:	**30**	**15**

Lp.	**Treści laboratoriów**	**Liczba godzin na studiach**	
		stacjonarnych	**niestacjonarnych**
L1	Wprowadzenie pojęć i organizacja zajęć	1	1
L2	Generowanie i wykorzystanie certyfikatów bezpieczeństwa	2	1
L3	Konfiguracja bezpieczeństwa przeglądarki i poczty Internetowej	2	2
L4	Certyfikacja usług w systemach rozproszonych - przykłady wykorzystania.	2	2
L5	Narzędzia implementacji elementów infrastruktury usług certyfikacyjnych	2	1
L6	Komponenty JAVA dla generowania i wykorzystania certyfikatów bezpieczeństwa	2	1
L7	Wprowadzenie do zarządzania kluczami w KERBEROS.	2	1
L8	Zaliczenie przedmiotu	2	1
	Razem liczba godzin laboratoriów	15	10

Lp.	**Treści projektów**	**Liczba godzin na studiach**	
		stacjonarnych	**niestacjonarnych**
P1	Wprowadzenie do realizacji samodzielnych zadań projektowych	2	1
P2	Prezentacja tematyki projektów	2	1
P3	Omówienie zasad przygotowywania prezentacji, przykłady.	2	1
P4	Omówienie zasad prowadzenia prezentacji, przykłady	2	1
P5	Opracowanie listy tematów projektowych i dyskusja	2	1
P6	Przydział tematów projektowych	2	1
P7	Realizacja szkicu projektu w grupach	2	1
P8	Prezentacja szkiców projektów, dyskusja	2	1
P9	Realizacja skorygowanych wersji szkiców projektów	2	2
P10	Prezentacja skorygowanych szkiców projektów, dyskusja	2	1
P11	Realizacja projektów cz. 1	2	1
P12	Realizacja projektów cz. 2	2	1
P13	Prezentacja projektów cz. 1	2	2
P14	Prezentacja projektów cz. 2	2	2
P15	Podsumowanie i zaliczenie przedmiotu	2	1
	Razem liczba godzin projektów	30	18

G – Metody oraz środki dydaktyczne wykorzystywane w ramach poszczególnych form zajęć

Forma zajęć	Metody dydaktyczne (wybór z listy)	Środki dydaktyczne
Wykład	Wykład informacyjny Wykład problemowy połączony z dyskusją	Komputer i projektor multimedialny, tablica suchościeralna
Laboratoria	Ćwiczenia doskonalące umiejętność selekcjonowania, grupowania i przedstawiania zgromadzonych informacji	Komputer i projektor multimedialny, tablica suchościeralna Sala komputerowa z dostępem do internetu
Projekt	Selekcjonowanie, grupowanie i dobór informacji do realizacji zadania inżynierskiego	Komputer i projektor multimedialny, tablica suchościeralna Sala komputerowa z dostępem do internetu

H - Metody oceniania osiągnięcia efektów kształcenia na poszczególnych formach zajęć

Forma zajęć	**Ocena formująca (F) –** wskazuje studentowi na potrzebę uzupełniania wiedzy lub stosowania określonych metod i narzędzi, stymulujące do doskonalenia efektów pracy **(wybór z listy)**	**Ocena podsumowująca (P) –** podsumowuje osiągnięte efekty kształcenia **(wybór z listy)**
Wykład	F2 – obserwacja/aktywność	P2 – zaliczenie z oceną
Laboratorium	F3 – praca pisemna	P3 – ocena podsumowująca powstała na podstawie ocen formujących, uzyskanych w semestrze
Projekt	F4 – wystąpienie	P3 – ocena podsumowująca powstała na podstawie ocen formujących, uzyskanych w semestrze

H-1 Metody weryfikacji osiągnięcia przedmiotowych efektów kształcenia (wstawić „x")

Efekty przedmiotowe	Wykład		Laboratorium		Projekt	
	F2	P1	F3	P3	F4	P3
EPW1	x	x				
EPW2	x	x				
EPU1			x	x	x	x
EPU2			x	x	x	x
EPK1	x	x				

I – Kryteria oceniania

Wymagania określające kryteria uzyskania oceny w danym efekcie			
Ocena			
Przedmiotowy efekt kształcenia (EP..)	**Dostateczny , dostateczny plus 3/3,5**	**Dobry, dobry plus 4/4,5**	**bardzo dobry 5**

EPW1	Student opanował w stopniu podstawowym elementarną wiedzę z zakresu podstaw informatyki obejmującą przetwarzanie informacji, architekturę i organizację systemów komputerowych, bezpieczeństwo systemów komputerowych, budowę sieci i aplikacji sieciowych	Student opanował w stopniu dobrym elementarną wiedzę z zakresu podstaw informatyki obejmującą przetwarzanie informacji, architekturę i organizację systemów komputerowych, bezpieczeństwo systemów komputerowych, budowę sieci i aplikacji sieciowych	Student w pełni opanował elementarną wiedzę z zakresu podstaw informatyki obejmującą przetwarzanie informacji, architekturę i organizację systemów komputerowych, bezpieczeństwo systemów komputerowych, budowę sieci i aplikacji sieciowych
EPW2	Student ma podstawową wiedzę ogólną obejmującą kluczowe zagadnienia bezpieczeństwa systemów, urządzeń i procesów	Student ma ugruntowaną wiedzę ogólną obejmującą kluczowe zagadnienia bezpieczeństwa systemów, urządzeń i procesów	Student ma bardzo dobrą wiedzę ogólną obejmującą kluczowe zagadnienia bezpieczeństwa systemów, urządzeń i procesów
EPU1	Student potrafi w stopniu elementarnym pozyskiwać informacje z literatury, baz danych i innych źródeł; potrafi integrować uzyskane informacje, dokonywać ich interpretacji, a także wyciągać wnioski oraz formułować i uzasadniać opinie	Student potrafi w stopniu dobrym pozyskiwać informacje z literatury, baz danych i innych źródeł; potrafi integrować uzyskane informacje, dokonywać ich interpretacji, a także wyciągać wnioski oraz formułować i uzasadniać opinie	Student potrafi efektywnie pozyskiwać informacje z literatury, baz danych i innych źródeł; potrafi integrować uzyskane informacje, dokonywać ich interpretacji, a także wyciągać wnioski oraz formułować i uzasadniać opinie
EPU2	Student potrafi w zakresie elementarnym posłużyć się właściwie dobranymi metodami i urządzeniami umożliwiającymi zapewnienie bezpieczeństwa systemów i urządzeń	Student potrafi w stopniu dobrym posłużyć się właściwie dobranymi metodami i urządzeniami umożliwiającymi zapewnienie bezpieczeństwa systemów i urządzeń	Student potrafi efektywnie posłużyć się właściwie dobranymi metodami i urządzeniami umożliwiającymi zapewnienie bezpieczeństwa systemów i urządzeń
EPK1	Student ma podstawową świadomość ważności i zrozumienie skutków działalności inżynierskiej oraz związanej z tym odpowiedzialności za podejmowane decyzje	Student ma zadowalającą świadomość ważności i zrozumienie skutków działalności inżynierskiej oraz związanej z tym odpowiedzialności za podejmowane decyzje	Student ma ugruntowaną świadomość ważności i zrozumienie skutków działalności inżynierskiej oraz związanej z tym odpowiedzialności za podejmowane decyzje

J – Forma zaliczenia przedmiotu

Wykład – zaliczenie z oceną (test)

Laboratorium – zaliczenie z oceną. Na ocenę składa się oddanie min. 7 sprawozdawań, z laboratorium które są podstawą przystąpienia do kolokwium zaliczeniowego.

Projekt– zaliczenie z oceną. Ocenie podlegać będzie wykonanie projektu.

Kryteria ocen dla wykładu, projektu i laboratorium:

0-50 % – niedostateczna
51-60 % – dostateczna
61-70 % – dostateczna plus
71-80 % - dobry
81-90 % dobry plus
91-100 % bardzo dobry

K – Literatura przedmiotu

Literatura obowiązkowa:

1. W. Stallings, Kryptografia i bezpieczeństwo sieci komputerowych, Helion 2012.

2. C. Adams, S. Lloyd, Podpis elektroniczny. Klucz publiczny, Robomatic, Wrocław 2002.

3. A. J. Menezes, P.C. van Oorschot, S.A Vanstone, Handbook of Applied Cryptography (dostęp: 16.12.2019) https://doc.lagout.org/network/3_Cryptography/CRC%20Press%20-%20Handbook%20of%20applied%20Cryptography.pdf

Literatura zalecana / fakultatywna:

1. A. Szeląg, Windows Server 2008. Infrastruktura klucza publicznego (PKI), Helion, Gliwice 2008.
2. Rozporządzenie z dnia 7 sierpnia 2002 r. w sprawie określenia warunków technicznych i organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego (Dz.U. 2002 nr 128 poz.1094).

L – Obciążenie pracą studenta:

Forma aktywności studenta	Liczba godzin na realizację	
	na studiach stacjonarnych	na studiach niestacjonarnych
Godziny zajęć z nauczycielem/ami	75	43
Konsultacje	5	7
Czytanie literatury	5	15
Przygotowanie do zajęć laboratoryjnych	5	5
Opracowanie sprawozdania z ćwiczeń laboratoryjnych	15	20
Przygotowanie projektów	10	20
Przygotowanie do egzaminu	10	15
Suma godzin:	**125**	**125**
Liczba punktów ECTS dla przedmiotu (suma godzin : 25 godz.):	**5**	**5**

Ł – Informacje dodatkowe

Imię i nazwisko sporządzającego	Łukasz Lemieszewski
Data sporządzenia / aktualizacji	16 grudnia 2019 r.
Dane kontaktowe (e-mail, telefon)	llemieszewski@ajp.edu.pl
Podpis	

Pozycja w planie studiów (lub kod przedmiotu)	C.2.13

	Wydział	Techniczny
	Kierunek	Inżynieria Bezpieczeństwa
	Poziom studiów	Pierwszego stopnia
	Forma studiów	stacjonarne/niestacjonarne
	Profil kształcenia	Praktyczny

PROGRAM PRZEDMIOTU/MODUŁU

A - Informacje ogólne

1. Nazwa przedmiotu	**Zarządzanie przechowywaniem danych**
2. Punkty ECTS	**4**
3. Rodzaj przedmiotu	**obowiązkowy**
4. Język przedmiotu	**język polski**
5. Rok studiów	**IV**
6. Imię i nazwisko koordynatora przedmiotu oraz prowadzących zajęcia	**Łukasz Lemieszewski**

B – Formy dydaktyczne prowadzenia zajęć i liczba godzin w semestrze

Nr semestru	Studia stacjonarne	Studia niestacjonarne
Semestr 7	**Wykłady**: (15); **Laboratoria**: (30); **Projekt:** (15)	**Wykłady**: (10); **Laboratoria**: (18); **Projekt:** (10)
Liczba godzin ogółem	**60**	**38**

C - Wymagania wstępne

Student nabył podstawową wiedzę z zakresu systemów operacyjnych oraz sieci komputerowych

D - Cele kształcenia

	Wiedza
CW1	przekazanie wiedzy w zakresie wiedzy technicznej obejmującej terminologię, pojęcia, teorie, zasady, metody, techniki, narzędzia i materiały stosowane przy rozwiązywaniu zadań inżynierskich związanych z szeroko pojętym bezpieczeństwem i rozpoznawaniem zagrożeń, procesami planowania i realizacji eksperymentów, tak w procesie przygotowania z udziałem metod symulacji komputerowych, jak i w rzeczywistym środowisku
	Umiejętności
CU1	wyrobienie umiejętności w zakresie doskonalenia wiedzy, pozyskiwania i integrowanie informacji z literatury, baz danych i innych źródeł, opracowywania dokumentacji, prezentowania ich i podnoszenia kompetencji zawodowych
	Kompetencje społeczne
CK1	przygotowanie do uczenia się przez całe życie, podnoszenie kompetencji zawodowych, osobistych i społecznych w zmieniającej się rzeczywistości, podjęcia pracy związanej z funkcjonowaniem systemu bezpieczeństwa, którego głównym celem jest ratowanie i ochro-na życia, zdrowia i mienia przed zagrożeniami

E - Efekty kształcenia przedmiotowe i kierunkowe

Przedmiotowy efekt kształcenia (EP) w zakresie wiedzy (W), umiejętności (U) i kompetencji społecznych (K)		Kierunkowy efekt kształcenia
Wiedza (EPW…)		
EPW1	ma szczegółową wiedzę z zakresu mechanizmów szyfrowania danych	K_W10
EPW2	orientuje się w obecnym stanie oraz trendach rozwoju bezpieczeństwa systemów informatycznych, urządzeń i procesów	K_W15
Umiejętności (EPU…)		
EPU1	potrafi pozyskiwać informacje z literatury, baz danych i innych źródeł; potrafi integrować uzyskane informacje, dokonywać ich interpretacji, a także wyciągać wnioski oraz formułować i uzasadniać opinie	K_U01
EPU2	potrafi dostrzegać aspekty pozatechniczne, w tym środowiskowe, ekonomiczne i prawne przy projektowaniu, stosowaniu systemów zapewniających bezpieczeństwo systemów, sieci i urządzeń	K_U10
Kompetencje społeczne (EPK…)		
EPK1	ma świadomość ważności i rozumie i skutki działalności inżynierskiej związanej z tym odpowiedzialności za podejmowane decyzje	K_K02

F - Treści programowe oraz liczba godzin na poszczególnych formach zajęć

Lp.	Treści wykładów	Liczba godzin na studiach	
		stacjonarnych	niestacjonarnych
W1	Zajęcia organizacyjne – omówienie karty przedmiotu (cele i efekty kształcenia, treści programowe, formy i warunki zaliczenia).	1	1
W2	Wprowadzenie do przedmiotu. Znaczenie i ogólna postać systemu przechowywania danych	2	1
W3	Zarządzanie przechowywaniem danych (bezpieczeństwo przechowywania danych, zasoby pamięciowe, cykl życia informacji, kompresja danych).	2	1
W4	Funkcja archiwizacji danych (tworzenie kopii zapasowych, odtwarzanie danych, przechowywanie, testowanie i monitorowanie kopii zapasowych).	2	1
W5	Fizyczne i wirtualne nośniki danych oraz technologie deduplikacji i kompresja danych.	2	1
W6	Systemy do tworzenia kopii zapasowych (np. CommVault Simpana, Symantec NetBackup, Amanda, Backup PC i narzędzia open source).	2	1
W7	Ochrona danych. Strategie tworzenia kopii zapasowych.	2	2
W8	Metodyka oceny efektywności zarządzania przechowywaniem danych (przykład użycia metodyki)	2	2
	Razem liczba godzin wykładów	15	10

Lp.	Treści laboratoriów	Liczba godzin na studiach	
		stacjonarnych	niestacjonarnych
L1	Omówienie zakresu ćwiczeń laboratoryjnych. Podstawy systemu archiwizacji danych na przykładzie darmowych programów.	2	1
L2	IP SAN i prawo Metcalfa	2	1
L3	Konfiguracja i wykonywanie kopii zapasowych. Część 1	2	1
L4	Konfiguracja i wykonywanie kopii zapasowych. Część 2	2	1
L5	Odtwarzanie i weryfikacja odtworzonych danych. Część 1.	2	1

L6	Odtwarzanie i weryfikacja odtworzonych danych. Część 2.	2	1
L7	Konfiguracja nośników danych i urządzeń. Zarządzanie urządzeniami magazynującymi i wolumenami.	2	1
L8	Zaawansowane operacje kopiowania danych.	2	1
L9	Zarządzanie i replikacja.	2	1
L10	Raportowanie i monitorowanie.	2	1
L11	Troubleshooting–alerty systemu, rozwiązywanie podstawowych problemów, codzienna obsługa systemu kopiowania danych.	2	1
L12	Dobór optymalnej infrastruktury pamięci masowej.	2	1
L13	Zabezpieczanie danych przed utratą i uszkodzeniem	2	2
L14	Zastosowanie metodyki oceny efektywności zarządzania przechowywaniem danych.	2	2
L15	Zaliczenie.	2	2
	Razem liczba godzin laboratoriów	30	18

Lp.	**Treści projektów**	**Liczba godzin na studiach**	
		stacjonarnych	**niestacjonarnych**
L1	Dla wybranego scenariusza organizacji (budynku) realizacja projektu przechowywania danych. Harmonogram projektu.	2	1
L2	Dla wybranego scenariusza organizacji realizacja logicznej infrastruktury sieciowej pod względem bezpieczeństwa przechowywania danych.	2	1
L3	Opracowanie projektu systemu zachowania ciągłości pracy.	2	1
L4	Wybór oprogramowania do zachowania ciągłości pracy systemów. Kosztorys.	2	1
L5	Realizacja projektu systemu zarządzania przechowywaniem danych z wyborem medium transmisyjnego (przewodowego, bezprzewodowego), sieciowych protokołów komunikacyjnych oraz doboru urządzeń i metod zarządzania przechowywaniem danych. Cześć 1	2	2
L6	Realizacja projektu systemu zarządzania przechowywaniem danych z wyborem medium transmisyjnego (przewodowego, bezprzewodowego), sieciowych protokołów komunikacyjnych oraz doboru urządzeń i metod zarządzania przechowywaniem danych. Część 2	2	2
L7	Oddanie i prezentacja projektów. Wystawienie ocen.	3	2
	Razem liczba godzin projektów	15	10

G – Metody oraz środki dydaktyczne wykorzystywane w ramach poszczególnych form zajęć

Forma zajęć	**Metody dydaktyczne (wybór z listy)**	**Środki dydaktyczne**
Wykład	M4. Metoda programowana (wykład problemowy z wykorzystaniem materiałów multimedialnych i źródeł internetowych)	projektor multimedialny, komputer (notebook) z dostępem do sieci internetowej;
Laboratoria	M5. Metoda praktyczna (analiza przykładów, ćwiczenia doskonalące)	komputery z zainstalowanym środowiskiem narzędziowym
Projekt	ćwiczenia doskonalące obsługę oprogramowania komputerowego wspomagającego audyt i zarządzanie	stanowisko komputerowe z dostępem do oprogramowania wspomagającego

	zasobami informatycznymi, ćwiczenia doskonalące umiejętność selekcjonowania, grupowania i przedstawiania zgromadzonych informacji na temat zarządzania przechowywaniem danych,	audyt i zarządzanie zasobami informatycznymi

H - Metody oceniania osiągnięcia efektów kształcenia na poszczególnych formach zajęć

Forma zajęć	**Ocena formująca (F) –** wskazuje studentowi na potrzebę uzupełniania wiedzy lub stosowania określonych metod i narzędzi, stymulujące do doskonalenia efektów pracy **(wybór z listy)**	**Ocena podsumowująca (P) –** podsumowuje osiągnięte efekty kształcenia **(wybór z listy)**
Wykład	F2 – obserwacja/aktywność (wypowiedzi ustne na wybrany temat lub zadane pytanie, formułowanie problemów i pytań dotyczących tematyki wykładu	P2 – zaliczenie z oceną (test sprawdzający wiedzę z całego przedmiotu oraz egzamin ustny; uwzględniana jest ocena z laboratoriów i projektu)
Laboratoria	F5 - ćwiczenia praktyczne (ćwiczenia sprawdzające umiejętności, rozwiązywanie zadań	P3 –ocena podsumowująca powstała na podstawie ocen formujących, uzyskanych w semestrze.
Projekt	F2 – obserwacja/aktywność (przygotowanie do zajęć, ocena ćwiczeń wykonywanych podczas zajęć i jako pracy własnej), F4 – wystąpienie (prezentacja multimedialna formułowanie dłuższej wypowiedzi ustnej na wybrany temat, ustne formułowanie i rozwiązywanie problemu, wypowiedź problemowa, analiza projektu itd.),	P4 – praca pisemna (projekt, referat, raport),

H-1 Metody weryfikacji osiągnięcia przedmiotowych efektów kształcenia (wstawić „x")

Efekty przedmiotowe	Wykład		Laboratoria		Projekt		
	F2	P1	F5	P3	F2	F4	P4
EPW1	x	x					
EPW2	x	x					
EPU1				x	x	x	x
EPU2				x	x	x	x
EPK1	x	x	x				

I – Kryteria oceniania

Wymagania określające kryteria uzyskania oceny w danym efekcie			
Ocena			
Przedmiotowy efekt kształcenia (EP..)	**Dostateczny dostateczny plus 3/3,5**	**dobry dobry plus 4/4,5**	**bardzo dobry 5**
EPW1	Student potrafi wymienić i krótko opisać ważniejsze zasady, standardy i narzędzia informatyczne stosowane do zarządzania	Student potrafi wymienić i obszernie opisać ważniejsze powszechnie obowiązujące zasady, standardy i narzędzia	Student potrafi wymienić I obszernie opisać wszystkie (omówione w ramach przedmiotu) powszechnie obowiązujące zasady,

	przechowywaniem danych.	Informatyczne stosowane do zarządzania przechowywaniem danych.	standardy i narzędzia informatyczne stosowane do zarządzania przechowywaniem danych
EPW2	Student potrafi, przy niewielkiej pomocy nauczyciela, potrafi dobrać i zastosować podstawowe metody, narzędzia oraz dobre praktyki w celu zapewnienia wysokiego poziomu bezpieczeństwa procesu przechowywania danych.	Student potrafi samodzielnie dobrać i zastosować podstawowe metody, narzędzia oraz dobre praktyki w celu zapewnienia wysokiego poziomu bezpieczeństwa procesu przechowywania danych.	Student potrafi samodzielnie dobrać i zastosować podstawowe i zaawansowane metody, narzędzia oraz dobre praktyki w celu zapewnienia wysokiego poziomu bezpieczeństwa procesu przechowywania danych.
EPU1	Student potrafi, przy niewielkiej pomocy nauczyciela, zmierzyć i ocenić poziom efektywności zarządzania głównymi funkcjami przechowywania danych	Student potrafi samodzielnie zmierzyć i ocenić poziom efektywności zarządzania głównymi funkcjami przechowywania danych.	Student potrafi samodzielnie I kompleksowo zmierzyć oraz ocenić poziom efektywności zarządzania przechowywaniem danych
EPU2	Student ma świadomość konieczności permanentnego podnoszenia własnych kwalifikacji zawodowych w dziedzinie bezpieczeństwa i zarządzania przechowywaniem danych, jednak nie uwzględnia tego aspektu w realizowanym zadaniu. Nie potrafi w pełni samodzielnie uzupełniać oraz doskonalić nabytej wiedzy i umiejętności.	Student ma pełną świadomość konieczności permanentnego podnoszenia własnych kwalifikacji zawodowych w dziedzinie bezpieczeństwa i zarządzania przechowywaniem danych. Potrafi przy nieznacznej pomocy nauczyciela uzupełniać oraz doskonalić nabytą wiedzę i umiejętności w ramach realizowanego zadania.	Student ma pełną świadomość konieczności permanentnego podnoszenia własnych kwalifikacji zawodowych w dziedzinie bezpieczeństwa i zarządzania przechowywaniem danych. Potrafi w pełni samodzielnie uzupełniać oraz doskonalić nabytą wiedzę i umiejętności w ramach realizowanego zadania
EPK1	Potrafi wykreować rozwiązanie zadania po uzyskaniu dokładnych wskazówek	Potrafi wykreować rozwiązanie zadania po uzyskaniu ogólnych wytycznych.	Potrafi w pełni samodzielnie ustalić sposób rozwiązania zadania.

J – Forma zaliczenia przedmiotu

Wykład – zaliczenie z oceną (test)

Laboratorium – zaliczenie z oceną. Na ocenę składa się oddanie min. 7 sprawozdawań, z laboratorium które są podstawą przystąpienia do kolokwium zaliczeniowego.

Projekt– zaliczenie z oceną. Ocenie podlegać będzie wykonanie projektu.

Kryteria ocen dla wykładu, projektu i laboratorium:

0-50 % – niedostateczna
51-60 % – dostateczna
61-70 % – dostateczna plus
71-80 % - dobry
81-90 % dobry plus
91-100 % bardzo dobry

Literatura obowiązkowa: 1. Preston W. C., Archiwizacja i odzyskiwanie danych, Wydawnictwo „Helion", Gliwice 2012. 2. Nelson S., Profesjonalne tworzenie kopii zapasowych i odzyskiwanie danych, Wydawnictwo „Helion", Gliwice 2012. 3. Swacha J., Zarządzanie przechowywaniem danych. Metodyka oceny efektywności, Agencja Wydawnicza Placet, Warszawa 2009.
Literatura zalecana / fakultatywna: 1. Beach A., Kompresja dźwięku i obrazu wideo Real World, Wydawnictwo „Helion", Gliwice 2009. 2. Przelaskowski A., Kompresja danych. Podstawy, metody bezstratne, kodery obrazów, Wydawnictwo BTC, Legionowo 2005. 3. Toigo J. W., Zarządzanie przechowywaniem danych w sieci, Wydawnictwo „Helion", Gliwice 2004.

L – Obciążenie pracą studenta:

Forma aktywności studenta	Liczba godzin na realizację	
	na studiach stacjonarnych	na studiach niestacjonarnych
Godziny zajęć z nauczycielem/ami	60	38
Konsultacje	5	5
Czytanie literatury	5	25
Przygotowanie sprawozdań	10	12
Przygotowanie projektu	10	10
Przygotowanie do zaliczenia	10	10
Suma godzin:	**100**	**100**
Liczba punktów ECTS dla przedmiotu (suma godzin: 25 godz.):	**4**	**4**

Ł – Informacje dodatkowe

Imię i nazwisko sporządzającego	Łukasz Lemieszewski
Data sporządzenia / aktualizacji	16 grudnia 2019 r.
Dane kontaktowe (e-mail, telefon)	llemieszewski@ajp.edu.pl
Podpis	

Pozycja w planie studiów (lub kod przedmiotu)	C.2.14

Wydział	Techniczny
Kierunek	Inżynieria bezpieczeństwa
Poziom studiów	Studia pierwszego stopnia
Forma studiów	Stacjonarne / Niestacjonarne
Profil kształcenia	Profil praktyczny

PROGRAM PRZEDMIOTU/MODUŁU

A - Informacje ogólne

1. Nazwa przedmiotu	**Projekt zespołowy**
2. Punkty ECTS	**3**
3. Rodzaj przedmiotu	**Obowiązkowy**
4. Język przedmiotu	**język polski**
5. Rok studiów	**IV**
6. Imię i nazwisko koordynatora przedmiotu oraz prowadzących zajęcia	**dr inż. Aleksandra Radomska-Zalas pracownicy Wydziału Technicznego**

B – Formy dydaktyczne prowadzenia zajęć i liczba godzin w semestrze

Nr semestru	Studia stacjonarne	Studia niestacjonarne
Semestr 7	**W**: 15; **Proj.**: 30;	**W**: 10; **Proj.**: 18;
Liczba godzin ogółem	**45**	**28**

C - Wymagania wstępne

D - Cele kształcenia

Wiedza	
CW1	Przekazanie wiedzy w zakresie wiedzy technicznej obejmującej terminologię, pojęcia, teorie, zasady, metody, techniki, narzędzia i materiały stosowane przy rozwiązywaniu zadań inżynierskich związanych z szeroko pojętym bezpieczeństwem i rozpoznawaniem zagrożeń, procesami planowania i realizacji eksperymentów, tak w procesie przygotowania z udziałem metod symulacji komputerowych, jak i w rzeczywistym środowisku.
CW2	Przekazanie wiedzy ogólnej dotyczącej standardów i norm technicznych dotyczących zagadnień inżynierii bezpieczeństwa systemów, urządzeń, procesów, i związanych z tym technik i metod programowania, szyfrowania danych, zarządzania jakością i analizy ryzyka
Umiejętności	
CU1	Wyrobienie umiejętności w zakresie doskonalenia wiedzy, pozyskiwania i integrowanie informacji z literatury, baz danych i innych źródeł, opracowywania dokumentacji, prezentowania ich i podnoszenia kompetencji zawodowych
CU2	Wyrobienie umiejętności projektowania i monitorowania stanu i warunków bezpieczeństwa: wykonywania analiz bezpieczeństwa i ryzyka, kontrolowania przestrzegania przepisów i zasad bezpieczeństwa, kontrolowania warunków pracy i standardów bezpieczeństwa, prowadzenia badań okoliczności awarii i wypadków, prowadzenia szkoleń, pełnienia funkcji organizatorskich w zakresie zarządzania bezpieczeństwem oraz prowadzenia dokumentacji związanej z szeroko rozumianym bezpieczeństwem
Kompetencje społeczne	

CK1	Przygotowanie do uczenia się przez całe życie, podnoszenie kompetencji zawodowych, osobistych i społecznych w zmieniającej się rzeczywistości, podjęcia pracy związanej z funkcjonowaniem systemu bezpieczeństwa, którego głównym celem jest ratowanie i ochrona życia, zdrowia i mienia przed zagrożeniami
CK2	Uświadomienie ważności i rozumienia społecznych skutków działalności inżynierskiej, w tym jej wpływu na środowisko i związanej z tym odpowiedzialności za podejmowane decyzje, współdziałanie w grupie i przyjmowanie odpowiedzialności za wspólne realizacje, kreatywność i przedsiębiorczość oraz potrzebę przekazywania informacji odnośnie osiągnięć technicznych i działania inżyniera.

E - Efekty kształcenia przedmiotowe i kierunkowe

Efekty kształcenia (E) w zakresie wiedzy (W), umiejętności (U) i kompetencji społecznych (K)		**Kierunkowy efekt kształcenia**
Wiedza (EW…)		
EPW1	Student, który zaliczył przedmiot ma elementarną wiedzę z zakresu podstaw informatyki obejmującą przetwarzanie informacji, architekturę i organizację systemów komputerowych, bezpieczeństwo systemów komputerowych, budowę sieci i aplikacji sieciowych	K_W04
EPW2	Student, który zaliczył przedmiot ma wiedzę ogólną obejmującą kluczowe zagadnienia bezpieczeństwa systemów, urządzeń i procesów	K_W05
Umiejętności (EU…)		
EPU1	Student, który zaliczył przedmiot potrafi pozyskiwać informacje z literatury, baz danych i innych źródeł; potrafi integrować uzyskane informacje, dokonywać ich interpretacji, a także wyciągać wnioski oraz formułować i uzasadniać opinie	K_U01
EPU2	Student, który zaliczył przedmiot potrafi posłużyć się właściwie dobranymi metodami i urządzeniami umożliwiającymi zapewnienie bezpieczeństwa systemów i urządzeń	K_U19
Kompetencje społeczne (EK…)		
EPK1	Student, który zaliczył przedmiot ma świadomość ważności i rozumie skutki działalności inżynierskiej oraz związanej z tym odpowiedzialności za podejmowane decyzje	K_K02

F - Treści programowe oraz liczba godzin na poszczególnych formach zajęć

Lp.	**Treści wykładów**	**Liczba godzin na studiach**	
		stacjonarnych	**niestacjonarnych**
W1	Wprowadzenie do tematyki przedsięwzięć informatycznych.	2	1
W2	Podstawowe pojęcia związane z analizą i projektowaniem systemów, cyklem życia oprogramowania.	2	1
W3	Etapy wytwarzania oprogramowania	2	1
W4	Metody prowadzenia projektów programistycznych	2	1
W5	Porównanie środowisk programistycznych	2	2
W6	Metody oceny efektywności oprogramowania	2	2
W7	Ocena stosowanych rozwiązań w zarządzaniu przedsięwzięciami informatycznymi	2	1
W8	Podsumowanie przedmiotu i zaliczenie	1	1
	Razem liczba godzin wykładów:	15	10

Lp.	**Treści projektów**	**Liczba godzin na studiach**	
		stacjonarnych	**niestacjonarnych**
P1	Wprowadzenie do realizacji samodzielnych zadań projektowych	2	1

P2	Prezentacja tematyki projektów	2	1
P3	Wybór środowiska programistycznego.	2	1
P4	Specyfikacja projektu - UML (projektowanie klas, diagramów przypadków użycia)	2	1
P5	Projektowanie interfejsu użytkownika	2	1
P6	Implementacja w wybranym języku programowania, testowanie	2	1
P7	Opracowanie listy tematów projektowych i dyskusja	2	1
P8	Przydział tematów projektowych	2	1
P9	Realizacja szkiców projektów	2	2
P10	Prezentacja szkiców projektów, dyskusja	2	1
P11	Realizacja projektów cz. 1	2	1
P12	Realizacja projektów cz. 2	2	1
P13	Prezentacja projektów cz. 1	2	2
P14	Prezentacja projektów cz. 2	2	2
P15	Podsumowanie i zaliczenie przedmiotu	2	1
	Razem liczba godzin projektów	30	18

G – Metody oraz środki dydaktyczne wykorzystywane w ramach poszczególnych form zajęć

Forma zajęć	**Metody dydaktyczne (wybór z listy)**	**Środki dydaktyczne**
Wykład	Wykład informacyjny	Projektor, tablica, komputer z dostępem do internetu
Projekt	Realizacja zadania inżynierskiego w grupie, Doskonalenie metod i technik analizy zadania inżynierskiego.	Komputer i projektor multimedialny, tablica suchościeralna Sala komputerowa z dostępem do internetu

H - Metody oceniania osiągnięcia efektów kształcenia na poszczególnych formach zajęć

Forma zajęć	**Ocena formująca (F) –** wskazuje studentowi na potrzebę uzupełniania wiedzy lub stosowania określonych metod i narzędzi, stymulujące do doskonalenia efektów pracy **(wybór z listy)**	**Ocena podsumowująca (P) –** podsumowuje osiągnięte efekty kształcenia **(wybór z listy)**
Wykład	F2 – obserwacja/aktywność	P2 – kolokwium
Projekt	F4 – wystąpienie	P3 – ocena podsumowująca powstała na podstawie ocen formujących, uzyskanych w semestrze

H-1 Metody weryfikacji osiągnięcia przedmiotowych efektów kształcenia (wstawić „x")

Efekty przedmiotowe	Wykład		Projekt	
	F2	P2	F4	P3
EPW1	x	x		
EPW2	x	x		
EPU1			x	x
EPU2			x	x
EPK1	x	x		

I – Kryteria oceniania

Wymagania określające kryteria uzyskania oceny w danym efekcie
Ocena

Przedmiotowy efekt kształcenia (EP..)	Dostateczny , dostateczny plus 3/3,5	Dobry, dobry plus 4/4,5	bardzo dobry 5
EPW1	Student opanował w stopniu podstawowym elementarną wiedzę z zakresu podstaw informatyki obejmującą przetwarzanie informacji, architekturę i organizację systemów komputerowych, bezpieczeństwo systemów komputerowych, budowę sieci i aplikacji sieciowych	Student opanował w stopniu dobrym elementarną wiedzę z zakresu podstaw informatyki obejmującą przetwarzanie informacji, architekturę i organizację systemów komputerowych, bezpieczeństwo systemów komputerowych, budowę sieci i aplikacji sieciowych	Student w pełni opanował elementarną wiedzę z zakresu podstaw informatyki obejmującą przetwarzanie informacji, architekturę i organizację systemów komputerowych, bezpieczeństwo systemów komputerowych, budowę sieci i aplikacji sieciowych
EPW2	Student ma podstawową wiedzę ogólną obejmującą kluczowe zagadnienia bezpieczeństwa systemów, urządzeń i procesów	Student ma ugruntowaną wiedzę ogólną obejmującą kluczowe zagadnienia bezpieczeństwa systemów, urządzeń i procesów	Student ma bardzo dobrą wiedzę ogólną obejmującą kluczowe zagadnienia bezpieczeństwa systemów, urządzeń i procesów
EPU1	Student potrafi w stopniu elementarnym pozyskiwać informacje z literatury, baz danych i innych źródeł; potrafi integrować uzyskane informacje, dokonywać ich interpretacji, a także wyciągać wnioski oraz formułować i uzasadniać opinie	Student potrafi w stopniu dobrym pozyskiwać informacje z literatury, baz danych i innych źródeł; potrafi integrować uzyskane informacje, dokonywać ich interpretacji, a także wyciągać wnioski oraz formułować i uzasadniać opinie	Student potrafi efektywnie pozyskiwać informacje z literatury, baz danych i innych źródeł; potrafi integrować uzyskane informacje, dokonywać ich interpretacji, a także wyciągać wnioski oraz formułować i uzasadniać opinie
EPU2	Student potrafi w zakresie elementarnym posłużyć się właściwie dobranymi metodami i urządzeniami umożliwiającymi zapewnienie bezpieczeństwa systemów i urządzeń	Student potrafi w stopniu dobrym posłużyć się właściwie dobranymi metodami i urządzeniami umożliwiającymi zapewnienie bezpieczeństwa systemów i urządzeń	Student potrafi efektywnie posłużyć się właściwie dobranymi metodami i urządzeniami umożliwiającymi zapewnienie bezpieczeństwa systemów i urządzeń
EPK1	Student ma podstawową świadomość ważności i zrozumienie skutków działalności inżynierskiej oraz związanej z tym odpowiedzialności za podejmowane decyzje	Student ma zadowalającą świadomość ważności i zrozumienie skutków działalności inżynierskiej oraz związanej z tym odpowiedzialności za podejmowane decyzje	Student ma ugruntowaną świadomość ważności i zrozumienie skutków działalności inżynierskiej oraz związanej z tym odpowiedzialności za podejmowane decyzje

J – Forma zaliczenia przedmiotu

Wykład – zaliczenie z oceną (test)

Projekt– zaliczenie z oceną. Ocenie podlegać będzie wykonanie projektu.

Kryteria ocen dla wykładu, projektu i laboratorium:

0-50 % – niedostateczna
51-60 % – dostateczna
61-70 % – dostateczna plus
71-80 % - dobry
81-90 % dobry plus
91-100 % bardzo dobry

K – Literatura przedmiotu

Literatura obowiązkowa:

1. Cadle J., Yeates D., Zarządzanie procesem tworzenia systemów informacyjnych, WNT, 2004. 2. Frączkowski K., Zarządzanie projektem informatycznym, Wydawnictwo Oficyna PWR 2002. 3. Fowler M., Scott K, UML w kropelce, LTP, Warszawa 2002. 4. Pressman R.S , Praktyczne podejście do inżynierii oprogramowania, WNT, Warszawa 2004.
Literatura zalecana / fakultatywna: 1. J. Górski, Inżynieria oprogramowania w projekcie informatycznym, Warszawa 2000. 2. W. Gajda, GIMP. Praktyczne projekty, Helion, Gliwice 2006.

L – Obciążenie pracą studenta:

Forma aktywności studenta	Liczba godzin na realizację	
	na studiach stacjonarnych	na studiach niestacjonarnych
Godziny zajęć z nauczycielem/ami	45	28
Konsultacje	1	6
Czytanie literatury	9	11
Przygotowanie projektu	10	15
Przygotowanie do zaliczenia	10	15
Suma godzin:	**75**	**75**
Liczba punktów ECTS dla przedmiotu (suma godzin : 25 godz.):	**3**	**3**

Ł – Informacje dodatkowe

Imię i nazwisko sporządzającego	dr inż. Aleksandra Radomska-Zalas
Data sporządzenia / aktualizacji	16 grudnia 2019 r.
Dane kontaktowe (e-mail, telefon)	ARadomska-zalas@ajp.edu.pl
Podpis	