Możliwość dofinansowania

Studia podyplomowe "Cyberbezpieczeństwo systemów informatycznych"

Numer usługi 2024/11/18/14073/2418300

6 800,00 PLN brutto
6 800,00 PLN netto
37,36 PLN brutto/h
37,36 PLN netto/h

WYŻSZA SZKOŁA INFORMATYKI I ZARZĄDZANIA Z SIEDZIBĄ W RZESZOWIE

★★★★½

zdalna w czasie rzeczywistym
Studia podyplomowe
182 h
11.10.2025 do 30.06.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Identyfikator projektu	Małopolski Pociąg do kariery
Sposób dofinansowania	wsparcie dla osób indywidualnych wsparcie dla pracodawców i ich pracowników
Grupa docelowa usługi	Oferta studiów skierowana jest do osób posiadających wyższe wykształcenie, które są odpowiedzialne za nadzór i bezpieczeństwo systemów informatycznych w firmach i organizacjach. Na studia zapraszamy osoby mające przygotowanie i doświadczenie informatyczne, a w szczególności tytuł zawodowy w obszarze informatyki lub dziedzinie pokrewnej. Usługa również adresowana dla Uczestników Projektu "Małopolski pociąg do kariery - sezon 1" i/lub dla Uczestników Projektu "Nowy start w Małopolsce z EURESem"
Minimalna liczba uczestników	18
Maksymalna liczba uczestników	35
Data zakończenia rekrutacji	10-10-2025
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	182

Podstawa uzyskania wpisu do BUR	art. 163 ust. 1 ustawy z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce (t.j. Dz. U. z 2023 r. poz. 742, z późn. zm.)
Zakres uprawnień	Studia podyplomowe

Cel

Cel edukacyjny

Studia podyplomowe "Cyberbezpieczeństwo systemów informatycznych" wraz z egzaminem potwierdzają przygotowanie do nadzorowania aplikacji i systemów informacyjnych z punktu widzenia ich bezpieczeństwa. Słuchacz tworzy systemy, które zapewniają poufność, dostępność i spójność posiadanych zasobów informatycznych oraz zabezpieczają przed atakami hakerskimi.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Organizuje i zabezpiecza systemy informatyczne poprzez wdrożenie polityk bezpieczeństwa.	Omawia zasady bezpiecznego przesyłania, przechowywania informacji i danych	Wywiad swobodny
Charakteryzuje poziomy cyberbezpieczeństwa w kontekście funkcjonowania organizacji.	Wyjaśnia pojęcia dotyczące cyberbezpieczeństwa, zasad postępowania w przypadku zagrożeń oraz omawia uwarunkowania formalno-prawne.	Wywiad ustrukturyzowany
Analizuje zjawiska i zagrożenia cyberbezpieczeństwa oraz identyfikuje narzędzia wspomagające podejmowanie decyzji.	Projektuje politykę bezpieczeństwa w organizacji i reagowania na incydenty.	Prezentacja
	Przygotowuje, przeprowadza i dokumentuje audyt cyberbezpieczeństwa.	Prezentacja
Buduje świadomość odpowiedzialności za działania na rzecz dobra wspólnego.	Zachęca swoim przykładem do dzielenia się wiedzą, doskonaleniem swoich umiejętności.	Wywiad swobodny
Definiuje podstawowe mechanizmy funkcjonowania systemu cyberbezpieczeństwa i jego wpływu na bezpieczeństwo	Przygotowuje plan audytu bezpieczeństwa w organizacji ze wskazaniem ról i odpowiedzialności	Wywiad swobodny
Charakteryzuje podstawowe pojęcia formalnoprawne charakterystyczne dla obszaru cyberbezpieczeństwa	Wymienia konsekwencje braku stosowania polityki bezpieczeństwa w organizacji, niewłaściwego reagowania na incydenty i zagrożenia	Prezentacja

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Analizuje zjawiska i zagrożenia cyberbezpieczeństwa oraz dokonuje twórczej prezentacji i interpretacji	Wymienia czynniki mające wpływające na stan zagrożenia bezpieczeństwa organizacji	Wywiad swobodny
Ocena stan swojej wiedzy i sposób systematyczny uzupełnia i doskonali umiejętności w zakresie cyberbezpieczeństwa	Planuje aktualizację i rozwój swoich i zespołu umiejętności w obszarze cyberbezpieczeństwa	Wywiad swobodny

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji zawiera opis efektów uczenia się?

Tak. Absolwent studiów podyplomowych uzyskuje świadectwo zgodnie z obowiązującym rozporządzeniem ministerialnym oraz zaświadczenie o osiągniętych efektach uczenia się.

Pytanie 2. Czy dokument potwierdza, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji?

Tak. Każdy przedmiot kończy się zaliczeniem, zaliczeniem na ocenę lub egzaminem zgodnie z wytycznymi zawartymi w kartach przedmiotów.

Pytanie 3. Czy dokument potwierdza zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

Tak. Po uzyskaniu zaliczeń i zdaniu egzaminów przedmiotowych oraz zakończeniu zajęć dydaktycznych słuchacz zdaje egzamin końcowy w formie ustnej wypowiedzi przed powołaną komisją.

Program

Usługa przygotowuje do nadzorowania aplikacji i systemów informatycznych zabezpieczających dane przedsiębiorstwa, organizacji i innych podmiotów

Program studiów podyplomowych:

Cisco CyberOPS Associate

Obsługa systemów operacyjnych pod kątem zabezpieczania przed możliwymi atakami. Planowanie i integrowanie wiedzy z różnych dyscyplin prowadzących do realizacji ataków na sieć lub system operacyjny.

Eksperymenty związane z bezpieczeństwem infrastruktury.

Analiza, monitorowanie i zarządzanie zachowaniem systemów Windows oraz Linux.

Metody i narzędzia wykorzystywane w kontekście zagadnień związanych z bezpieczeństwem sieci, systemów oraz infrastruktury.

Badanie profilu cyberataków, bezpieczeństwo systemu Windows i Linux.

Badanie aplikacji i usług sieciowych pod kątem podatności na ataki, szyfrowanie i deszyfrowanie danych, narzędzia monitoringu sieci.

Podstawowe zagrożenia dla systemów operacyjnych oraz kierunki rozwoju bezpieczeństwa komputerowego.

Metody poprawy bezpieczeństwa serwerów WEB oraz DNS.

Technologie bezpiecznej administracji Linux oraz Windows.

Analiza logów systemowych i bezpieczeństwa aktywnej zawartości.

Wdrażanie metod bezpieczeństwa urządzeń końcowych poprzez wykorzystanie narzędzi administrowania grupowego.

Wprowadzenie do system Kali Linux

Podstawy etycznego hackingu, wskazówki prawne, identyfikacja złośliwych aktorów,

podstawowa terminologia związana z cyberbezpieczeństwem, tworzenie planu bitwy testu

penetracyjnego, platforma Cyber Kill Chain.

Krótki historyczny przegląd, filozofia systemu.

Specyfika dystrybucji , przeznaczenie, różnice względem innych dystrybucji Linuxa.

Przygotowania oraz konfiguracja bezpiecznego laboratorium testowego do przeprowadzania

rzeczywistych ataków i testów penetracyjnych.

Tworzenie maszyn wirtualnych , przy użyciu hipernadzorcy typu drugiego VirtualBox.

Instalacja Kali Linux ,wybór wersji, metody instalacji, konfiguracja podstawowa.

Omówienie podstawowych narzędzi wbudowanych w systemie Kali Linux.

Praca w wierszu poleceń i z plikami, terminal Tmux oraz Tilix.

Zarządzanie systemem Kali Linux.

Wykrywanie hostów w sieci za pomocą arping, fping, hping3, nmap, icmp, netdiscover,

metasploit.

Technologia bind shell, reverse shell, tworzenie zdalnej powłoki.

Pakiet SET (Social-Engineer Toolkit), tworzenie ładunków , ataki , tworzenie stron

phishingowych, kodów QR oraz urządzeń infekujących.

Wprowadzenie do Metasploit-Framework, tworzenie i kodowanie ładunków z

wykorzystaniem msfvenom, ataki MYSQL, ataki na system android oraz windows 10.

Cisco Ethical Hacker

Poznanie znaczenia oraz metodologii i ram etycznego hakowania wraz z testami penetracyjnymi.

Tworzenie wstępnych dokumentów testów penetracyjnych.

Tworzenie zakresu i planu testów penetracyjnych, który uwzględnia

wymagania organizacyjne dotyczące usług.

Wykonywanie działań związanych z gromadzeniem informacji i skanowaniem

podatności.

Socjotechnika.

Wykorzystywanie luk w zabezpieczeniach sieci, aplikacji internetowych, urzadzeń IoT oraz urządzeń mobilnych.

Poznanie działań wykonywanych po przeprowadzeniu eksploatacji celu.

Tworzenie raportów z testów.

Klasyfikacja narzędzi pentestingowych według przypadków użycia.

Systemy zarządzania w bezpieczeństwie informacji

Stworzenie analizy ryzyka wraz ze zdefiniowaniem aktywów w oparciu o wybrane przedsiębiorstwo

Bezpieczeństwo informacji jako proces (wg. modelu żółwia)

Klasyfikacja zasobów informacyjnych

Incydenty i postepowanie z incydentami

Tworzenie prostych planów rozmieszczenia aktywów przedsiębiorstwa pod kątem oceny bezpieczeństwa

Cisco Network Security

Wyjaśnienie bezpieczeństwa sieci, różnych rodzajów zagrożeń i ataków wraz z narzędziami i procedurami łagodzącymi skutki najpopularniejszych ataków sieciowych.

Konfiguracja bezpiecznego dostepu administracyjnego oraz autoryzacji poleceń przy użyciu poziomów uprawnień i CLI opartego na rolach.

Wdrożenie bezpiecznego zarządzania i monitorowania urzadzeń sieciowych.

Konfiguracja AAA oraz list kontroli dostępu.

Zapoznanie się ze sprzętowymi oraz aplikacyjnymi zaporami sieciowymi.

Zapoznanie się z sieciowymi systemami zapobiegania włamaniom.

Bezpieczeństwo urządzeń końcowych oraz warstwy 2.

Usługi kryptograficzne.

Sieci VPN oraz ich konfiguracja.

Praktyczne wykorzystanie sprzętowego firewalla ASA.

Opisanie różnych technik i narzędzi wykorzystywanych do testowania

bezpieczeństwa sieci.

Audyt i monitorowanie cyberbezpieczeństwa

Rodzaje audytu bezpieczeństwa oraz sposoby jego przeprowadzania.

Monitorowanie systemów i sieci komputerowych.

Metodologiczne i formalno-prawne podstawy audytu systemu informacyjnego, w tym treści opartych o standard ISO27000.

Metody i środki skanowania systemów IT, sieci komputerowych.

Funkcjonowanie podstawowych narzędzi monitoringu sieci: SNMP, NetFlow, SPAN, VSPAN, RSPAN.

AI w Cyberbezpieczeństwie

Podstawowe pojęcia z zakresu sztucznej inteligencji.

Etapy budowy modeli AI i ML.

Sposoby oceny jakości działania modelu.

Podatności systemów sztucznej inteligencji i sposoby ich zabezpieczania.

Sposoby wykorzystania języka Python i sztucznej inteligencji do automatyzacji działań w cyberbezpieczeństwie.

Wpływ nadchodzących regulacji AI w kontekście cyberbezpieczeństwa.

1. Bezpieczeństwo chmury publicznej AWS

Bezpieczeństwo pracy z chmurą publiczną AWS.

Zabezpieczenie konta oraz bezpieczna praca w środowisku złożonym z wielu kont.

Podstawy zasad bezpieczeństwa przy pracy z serwisami AWS.

Zasady przechowywania i transportu danych w chmurze publicznej.

Aspekt zarządzania kosztami.

Praktyczne wykorzystanie Kali Linux

Zaawansowane testy penetracyjne, eskalacja uprawnień, kradzież tokenów i podszywanie

się, zacieranie śladów, kodowanie i eksfiltracja danych, postekploatacja.

Profilowanie systemów operacyjnych.

Sniffing w praktyce, ettercap, on-patch attack.

Ataki na sieci bezprzewodowe, tworzenie złośliwych punktów dostępowych, włamywanie się

do sieci WPA, WPA2.

Konfiguracja karty sieciowej Alfa AWUS036NH, praca w trybie monitora.

OSINT (Open-Source Intelligence) wprowadzenie, zbieranie informacje o celu. Narzędzia:

maltego, spiderfoot, the harvester, sherlock, recon-ng.

OSINT Framework.

Google Hacking Database (GHDB) - Exploit-DB.

Luki w zabezpieczeniach systemów operacyjnych.

Badanie podatności systemów operacyjnych.

Skanery Nessus, OpenVAS.

Nmap Scripting Engine (NSE).

Skanery aplikacji WWW.

Open Web Application Security Project (OWASP).

Burp Suite – badanie podatności aplikacji internetowych.

Reagowanie na incydenty oraz informatyka śledcza

Incydenty w kontekście bezpieczeństwa informatycznego, metod wykrywania oraz reagowania na nie.

Proces pracy ze zdarzeniami oraz wybrane typy ataków i możliwe wektory ataku.

Sposoby przeprowadzania analizy incydentu w kontekście wyciągnięcia wniosków i opracowania strategii powrotu do normalnego działania systemu informacyjnego.

Analiza dowodowa w zakresie wykrytych incydentów bezpieczeństwa.

Sposoby analizy systemów plików, zasobów sprzętowych komputera oraz ruchu sieciowego.

Metody zbierania cyfrowych danych dowodowych na temat stwierdzonych incydentów bezpieczeństwa.

Case study - przeprowadzenie procesu reakcji na incydenty.

Czas trwania studiów: 2 semestry, 182 godziny zajęć w formie zdalnej w czasie rzeczywistym, umożliwiają uzyskanie 30 punktów ECTS.

Dni zajęć dydaktycznych: sobota, niedziela w godz. 08.00 - 16.10. (godzina dydaktyczna - 45 minut). Zajęcia zdalne prowadzone są w czasie rzeczywistym z wykorzystaniem platformy Cisco Webex.

Zajęcia na studiach prowadzone są w formie wykładów, ćwiczeń, warsztatów, case study.

Zajęcia dydaktyczne realizowane są w blokach kilkugodzinnych. Każdy blok zajęć zawiera określoną liczbę godzin dydaktycznych (45 minut) wpisaną w harmonogramie i przerwy. Przerwy nie są wliczane do czasu zajęć dydaktycznych i zalezą od decyzji poszczególnych wykładowców pod warunkiem zrealizowania ilości godzin dydaktycznych przewidzianych w harmonogramie.

Wykładowcami studiów podyplomowych są pracownicy uczelni zajmujący się tematyką cyberbezpieczeństwa oraz pracownicy innych instytucji i organizacji posiadający doświadczenie z zakresu cyberbezpieczeństwa.

Zajęcia prowadzone są w sposób interaktywny, angażujący słuchaczy do wykonywania zadań, ćwiczeń i projektów oraz symulowania konkretnych sytuacji zagrożenia cyberatakiem oraz zapobiegania takim zdarzeniom.

Walidacja: słuchacz studiów podyplomowych uzyskuje zaliczenie lub ocenę po zakończeniu każdego przedmiotu. Po zakończeniu zajęć dydaktycznych, uzyskaniu zaliczeń z wszystkich przedmiotów dopuszczany jest do egzaminu końcowego. Czas egzaminu nie wlicza się do liczby godzin dydaktycznych. Po pozytywnym zdaniu egzaminu końcowego uzyskuje świadectwo ukończenia studiów podyplomowych.

Harmonogram

Liczba przedmiotów/zajęć: 1

Przedmiot / temat zajęć	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 1 Walidacja - egzamin końcowy	30-06-2026	09:00	09:45	00:45

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	6 800,00 PLN
Koszt przypadający na 1 uczestnika netto	6 800,00 PLN
Koszt osobogodziny brutto	37,36 PLN
Koszt osobogodziny netto	37,36 PLN

Prowadzący

Liczba prowadzących: 2

1 z 2

dr Inż. Janusz Korniak

Doktor nauk technicznych (Akademia Rolniczo–Techniczna w Bydgoszczy, rok 2005), absolwent studiów magisterskich Politechniki Rzeszowskiej.

Ukończył szkolenia z zakresu sieci komputerowych w Centrach Szkoleniowych Akademii Cisco w Budapest Polytechnic, University of Central England, Advance Technology Consortium – Romania oraz Cisco Learning Institute. Instruktor Akademii Cisco i trener instruktorów. Prowadzi szkolenia CCNA, CCNP, CCNA Security, CCNA Cybersecurity Operations, IoT Fundamentals.
W latach 2019-2024 prowadził zajęcia dydaktyczne na studiach I i II stopnia oraz studiach podyplomowych: Systemy i sieci komputerowe.

2 z 2

Mateusz Liput

Magister informatyki (Wyższa Szkoła Informatyki i Zarządzania w Rzeszowie, Wydział Informatyki Stosowanej, rok 2019).
Ukończył następujące szkolenia akademii CISCO: Cisco Certified Network Associate (CCNA), CCNA Security, Partner: NDG Linux Essentials. Posiada uprawnienia instruktorskie dla kursów z zakresu DevOps: ETW – Experimenting with REST APIs using Webex Teams, ETW – Network Programmability with Cisco APIC-EM, ETW – Model Driven Programmability; z zakresu sieci komputerowych: CCNA R&S: Routing and Switching Essentials, CCNA R&S: Introduction to Networks, CCNAv7 SRWE (Switching, Routing and Wireless Essentials), CCNAv7 ENSA (Enterprise Networking, Security and Automation), z zakresu Internetu Rzeczy: Introduction to IoT, IoT Fundamentals: Connecting Things, IoT Fundamentals: Big Data; z zakresu cyberbezpieczeństwa: Cybersecurity Essentials, Network Security, CyberOps Associate. Zdobyte certyfikaty branżowe: PCEP – Certified Entry-Level Python Programmer, PCAP – Certified Associate in Python Programming. Wyróżnienia: Cisco Instructor Excellence Expert 2022, Cisco 5 Years of Service.
Prowadzi zajęcia dydaktyczne na studiach I i II stopnia oraz studiach podyplomowych od 2022 roku.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Zapewniamy uczestnikom studiów dostęp do materiałów przekazywanych przez wykładowców poszczególnych przedmiotów drogą elektroniczną oraz na platformie Moodle. Słuchacze otrzymują: prezentacje przygotowane przez wykładowców, skrypty, inne materiały opisowe przygotowane przez wykładowców, zestawy ćwiczeń.

Warunki uczestnictwa

Osoby z wykształceniem wyższym (I lub II stopnia). Rejestracja https://podyplomowe.wsiz.pl/rekrutacja/

Rejestracja na studia podyplomowe odbywa się w formie elektronicznej. Aby zarezerwować miejsce na studiach podyplomowych konieczne jest złożenie kompletu wymaganych dokumentów rekrutacyjnych. Zgłoszenie na studia tylko przez Bazę Usług Rozwojowych nie gwarantuje miejsca w grupie.

Informacje dodatkowe

Czesne za studia wpisane w karcie usługi nie obejmuje opłaty rekrutacyjnej w wysokości 50 zł. Opłatę rekrutacyjną należy wnieść w chwili rejestracji na studia przez system rekrutacyjny uczelni.

Usługa skierowana również do Uczestników Projektu MP.

Szczegółowy harmonogram zajęć dydaktycznych zostanie wprowadzony do karty usługi co najmniej 2 tygodnie przed terminem rozpoczęcia usługi.

Warunki techniczne

Zajęcia zdalne prowadzone są z użyciem platformy Cisco Webex. Słuchacz loguje się do platformy Cisco Webex ze swojego konta w Wirtualnej Uczelni. Słuchacz, aby skorzystać z zajęć online musi posiadać stanowisko pracy spełniające poniższe minimalne wymagania:

Komputer/laptop/ z zainstalowanym systemem:

Windows

• Windows 10 lub nowszym

Mac OS

- 10.15 lub nowszym

Urządzenia mobilne:

iOS

- 16 i nowsze

iPadOS

- 16 i nowsze

Android

- 10 i nowsze

Minimalna przepustowość połączenia internetowego:

· Download 4 Mb/s

· Upload 4 MB/s

Niezbędne oprogramowanie umożliwiające uczestnikom dostęp do prezentowanych treści i materiałów

- Przeglądarka internetowa (według wyboru słuchacza)

Kontakt

Bartłomiej Cieszyński

E-mail bcieszynski@wsiz.edu.pl
Telefon (+48) 178 661 518