Możliwość dofinansowania

Studia podyplomowe "Cyberbezpieczeństwo systemów informatycznych"

Numer usługi 2024/06/25/14073/2196980

6 200,00 PLN brutto
6 200,00 PLN netto
34,07 PLN brutto/h
34,07 PLN netto/h

WYŻSZA SZKOŁA INFORMATYKI I ZARZĄDZANIA Z SIEDZIBĄ W RZESZOWIE

★★★★½

zdalna w czasie rzeczywistym
Studia podyplomowe
182 h
26.10.2024 do 30.06.2025

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
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.
Minimalna liczba uczestników	18
Maksymalna liczba uczestników	35
Data zakończenia rekrutacji	21-10-2024
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

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

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

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?

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?

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

Program

Program studiów podyplomowych obejmuje następujace zagadnienia:

Programowe i sprzętowe środki bezpieczeństwa

Rozwiązania techniczne i organizacyjne w zarządzaniu bezpieczeństwem informacyjnym.

Budowa, potencjalne sposoby wykorzystania platform sprzętowych i potencjalne słabości systemów bezpieczeństwa.

Narzędzia monitorowania potencjalnych zagrożeń dla systemów i sieci.

Metody szyfrowania komunikacji.

Wykrywanie zagrożeń i podatności.

Przeprowadzanie ataków na łamanie haseł.

Metody bezpiecznego połączenia z hostem zdalnym.

Umacnianie ochrony systemu Linux.

Analiza sieci w systemie Linux.

Struktura, usługi, metody zarządzania komponentami infrastruktury klucza publicznego.

Zasady działania podpisu elektronicznego.

Wykorzystanie podpisu elektronicznego oraz infrastruktury klucza publicznego w praktyce biznesowej.

Metody szyfrowania tekstów jawnych, integralności danych cyfrowych, funkcji hashujących, przykłady wykorzystania funkcji skrótu.

Sposoby wykorzystania urzędów certyfikujących do zarządzania usługami infrastruktury kluczy jawnych.

Wstęp do systemu Linux

Znajomość aplikacji open source w miejscu pracy w odniesieniu do ich odpowiedników o zamkniętym kodzie źródłowym.

Podstawowe pojęcia dotyczące sprzętu, procesów, programów i komponentów systemu operacyjnego Linux.

Praca w wierszu poleceń i z plikami.

Tworzenie i przywracanie skompresowanych kopii zapasowych i archiwów.

Bezpieczeństwo systemu, użytkownicy/grupy i uprawnienia do plików w katalogach publicznych i prywatnych.

Tworzenie i uruchamianie prostych skryptów.

FOSS, różne społeczności i licencje.

Zastosowanie dystrybucji Linux w cyberbezpieczeństwie.

Ochrona danych osobowych w systemach informacyjnych

Zagrożenia wynikające z nieprawidłowej ochrony danych osobowych oraz prywatności użytkownika.

Prywatność danych użytkownika w kontekście wykorzystania ich w systemach informatycznych oraz serwisach internetowych.

Zagadnienia prawne ochrony danych osobowych.

Technologiczne rozwiązania ochrony danych, analiza danych w spoczynku oraz danych w transporcie.

Dokumenty polityki ochrony danych osobowych oraz danych wykorzystywanych przez systemy informatyczne.

Case studies z rzeczywistych wycieków danych.

Prawne podstawy bezpieczeństwa informacyjnego

Kontekst prawny i proceduralny bezpieczeństwa informacyjnego.

Znaczenie konieczności ochrony informacji niejawnych.

Akty prawne regulujące zagadnienia bezpieczeństwa i ochrony informacji.

Krajowy System Cyberbezpieczeństwa.

Laboratorium cyberbezpieczeństwa cz. I

Projektowanie złożonych systemów informatycznych z uwzględnieniem występujących zależności pomiędzy komponentami systemu.

Metody i narzędzia wykorzystywane do zwiększania poziomu bezpieczeństwa.

Metody zabezpieczeń stosowanych na urządzeniach sieciowych z uwzględnieniem możliwych zagrożeń bezpieczeństwa.

Projektowanie i testowanie mechanizmów ochronnych oraz ich synergia z poszczególnymi komponentami całego systemu informatycznego i informacyjnego.

Podatności sieci komputerowej na ataki, metody uwierzytelniania, zabezpieczanie urządzeń sieciowych, filtrowanie ruchu oraz ograniczanie ataków na sieć, wykorzystanie elementów kryptografii do autentykacji i zapewnienia integralności danych, konfiguracja sieci VPN.

Elementy kryptografii symetrycznej i asymetrycznej wykorzystywane w podpisie elektronicznym i infrastrukturze klucza publicznego.

Polityki bezpieczeństwa – projektowanie i wdrożenie

Polityka bezpieczeństwa oraz metodyki jej tworzenia.

Obszary polityki bezpieczeństwa w firmie, bezpieczeństwo fizyczne i autentykacja oraz bezpieczeństwo usług.

Praktyczne metody przygotowania polityki bezpieczeństwa dla przedsiębiorstw o różnym profilu funkcjonowania.

Sposoby obsługi polityki bezpieczeństwa, zasady niezawodnej pracy jak i uzgodnienia, wdrożenia i konserwacji przygotowanego dokumentu.

Dokumenty normatywne oraz zasoby pomocne w opracowaniu polityki bezpieczeństwa.

Reagowanie na incydenty i 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.

Audyt 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.

Laboratorium cyberbezpieczeństwa cz. II

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.

Studia trwają 2 semestry, umożliwiają uzyskanie 30 punktów ECTS. Zajęcia realizowane są w formie zdalnej z wykorzystaniem infrastruktury uczelni. Zajęcia odbywają są średnio co 2 tygodnie w soboty i niedziele, średnio 6 - 8 godzin dziennie (godzina dydaktyczna - 45 minut).

Absolwent studiów podyplomowych uzyskuje świadectwo ukończenie studiów podyplomowych.

Harmonogram

Liczba przedmiotów/zajęć: 0

Przedmiot / temat zajęć	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
Brak wyników.				

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	6 200,00 PLN
Koszt przypadający na 1 uczestnika netto	6 200,00 PLN

Koszt osobogodziny brutto	34,07 PLN
Koszt osobogodziny netto	34,07 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.
Prowadzi zajęcia dydaktyczne na studiach I i II stopnia oraz studiach podyplomowych.

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.

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, kodeks pracy w formie wydrukowanej, 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

Zajęcia odbywają się w soboty-niedziele co 2 tygodnie po około 6-8h lekcyjnych każdego dnia w formie stacjonarnej i zdalnej. Zajęcia zdalne realizowane są z wykorzystaniem platformy Cisco Webex.

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.

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