



## 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

📄 Studia podyplomowe

📖 zdalna w czasie rzeczywistym

🕒 182:00 h

📅 11.10.2025 do 03.06.2026

★★★★★ 4,6 / 5

620 ocen

## Informacje podstawowe

<b>Kategoria</b>	Informatyka i telekomunikacja / Bezpieczeństwo IT
<b>Identyfikatory projektów</b>	Małopolski Pociąg do kariery
<b>Grupa docelowa usługi</b>	<p>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.</p> <p>Usługa również adresowana dla Uczestników Projektu "Małopolski pociąg do kariery - sezon 1" i/lub dla Uczestników Projektu "Nowy start w Małopolsce z EURESem"</p>
<b>Minimalna liczba uczestników</b>	18
<b>Maksymalna liczba uczestników</b>	35
<b>Data zakończenia rekrutacji</b>	07-10-2025
<b>Forma prowadzenia usługi</b>	zdalna w czasie rzeczywistym
<b>Liczba godzin usługi</b>	182
<b>Podstawa uzyskania wpisu do BUR</b>	art. 163 ust. 1 ustawy z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce (t. j. Dz. U. z 2024 r. poz. 1571, z późn. zm.)

# 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
Definiuje istotę i funkcję cyberbezpieczeństwa w organizacjach systemu bezpieczeństwa, podstawowe zasady organizowania i funkcjonowania systemu cyberbezpieczeństwa	Wymienia zagrożenia dla systemów operacyjnych, podatności na cyberataki	Wywiad swobodny
	Omawia zasady bezpieczeństwa systemu Linux i Windows	Wywiad swobodny
	Wyjaśnia czym jest szyfrowanie i deszyfrowanie danych.	Wywiad swobodny
	Wyjaśnia znaczenie podstawowych narzędzi wbudowanych w systemie Kali Linux	Wywiad swobodny
	Wyjaśnia pojęcia dotyczące cyberbezpieczeństwa, zasad postępowania w przypadku zagrożeń oraz omawia uwarunkowania formalno-prawne.	Wywiad ustrukturyzowany
Charakteryzuje współczesne koncepcje cyberbezpieczeństwa	Wyjaśnia czym są testy penetracyjne oraz w jakim celu są wykorzystywane	Wywiad swobodny
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.	Wyjaśnia czym jest socjotechnika i jak może wpływać na podejmowanie decyzji	Wywiad swobodny
	Przedstawia znaczenie analizy ryzyka dla ochrony zasobów informacyjnych	Prezentacja

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Projektuje i dobiera właściwe metody analizy ryzyka do rozwiązywania problemów dotyczących cyberbezpieczeństwa i podejmowania decyzji	Przygotowuje plan audytu bezpieczeństwa w organizacji ze wskazaniem ról i odpowiedzialności	Wywiad swobodny
	Wyjaśnia funkcjonowanie podstawowych narzędzi monitoringu sieci: SNMP, NetFlow, SPAN, VSPAN, RSPAN	Prezentacja
Charakteryzuje podstawowe pojęcia formalnoprawne charakterystyczne dla obszaru cyberbezpieczeństwa	Wymienia konsekwencje braku stosowania polityki bezpieczeństwa w organizacji, niewłaściwego reagowania na incydenty i zagrożenia	Prezentacja
Analizuje zjawiska i zagrożenia cyberbezpieczeństwa oraz dokonuje twórczej prezentacji i interpretacji	Wymienia czynniki mające wpływające na stan zagrożenia bezpieczeństwa organizacji	Wywiad swobodny
	Wyjaśnia wykorzystanie języka Python i sztucznej inteligencji do automatyzacji działań w cyberbezpieczeństwie	Debata swobodna
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
Charakteryzuje pojęcia, prawidłowości i problemy cyberbezpieczeństwa w zakresie danych osobowych.	Wyjaśnia czym jest bezpieczeństwo informacji wg ISO 27001:2022	Prezentacja
	Klasyfikuje zasoby informacyjne, tworzy opisy i instrukcje dotyczące dokumentacji oraz możliwych incydentów	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

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

TAK

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

TAK

## Program

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

Program studiów podyplomowych:

PRZEDMIOT	LICZBA GODZIN	ZAGADNIENIA
Cisco CyberOPS Associate	12 godz. zajęcia teoretyczne 14 godz. zajęcia praktyczne	<p>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.</p> <p>Eksperymenty związane z bezpieczeństwem infrastruktury.</p> <p>Analiza, monitorowanie i zarządzanie zachowaniem systemów Windows oraz Linux.</p> <p>Metody i narzędzia wykorzystywane w kontekście zagadnień związanych z bezpieczeństwem sieci, systemów oraz infrastruktury.</p> <p>Badanie profilu cyberataków, bezpieczeństwo systemu Windows i Linux.</p> <p>Badanie aplikacji i usług sieciowych pod kątem podatności na ataki, szyfrowanie i deszyfrowanie danych, narzędzia monitoringu sieci.</p> <p>Podstawowe zagrożenia dla systemów operacyjnych oraz kierunki rozwoju bezpieczeństwa komputerowego.</p> <p>Metody poprawy bezpieczeństwa serwerów WEB oraz DNS.</p> <p>Technologie bezpiecznej administracji Linux oraz Windows.</p> <p>Analiza logów systemowych i bezpieczeństwa aktywnej zawartości.</p> <p>Wdrażanie metod bezpieczeństwa urządzeń końcowych poprzez wykorzystanie narzędzi administrowania grupowego.</p>

<p>Wprowadzenie do systemu Kali Linux</p>	<p>8 godz. zajęcia teoretyczne</p> <p>8 godz. zajęcia praktyczne</p>	<p>Podstawy etycznego hackingu, wskazówki prawne, identyfikacja złośliwych aktorów, podstawowa terminologia związana z cyberbezpieczeństwem, tworzenie planu bitwy testu penetracyjnego, platforma Cyber Kill Chain.</p> <p>Krótki historyczny przegląd, filozofia systemu.</p> <p>Specyfika dystrybucji , przeznaczenie, różnice względem innych dystrybucji Linuxa.</p> <p>Przygotowania oraz konfiguracja bezpiecznego laboratorium testowego do przeprowadzania rzeczywistych ataków i testów penetracyjnych.</p> <p>Tworzenie maszyn wirtualnych , przy użyciu hipernadzorcy typu drugiego VirtualBox.</p> <p>Instalacja Kali Linux ,wybór wersji, metody instalacji, konfiguracja podstawowa.</p> <p>Omówienie podstawowych narzędzi wbudowanych w systemie Kali Linux.</p> <p>Praca w wierszu poleceń i z plikami, terminal Tmux oraz Tilix.</p> <p>Zarządzanie systemem Kali Linux.</p> <p>Wykrywanie hostów w sieci za pomocą arping, fping, hping3, nmap, icmp, netdiscover, metasploit.</p> <p>Technologia bind shell, reverse shell, tworzenie zdalnej powłoki.</p> <p>Pakiet SET (Social-Engineer Toolkit), tworzenie ładunków , ataki , tworzenie stron phishingowych, kodów QR oraz urządzeń infekujących.</p> <p>Wprowadzenie do Metasploit-Framework, tworzenie i kodowanie ładunków z wykorzystaniem msfvenom, ataki MYSQL, ataki na system android oraz windows 10.</p>
<p>Cisco Ethical Hacker</p>	<p>8 godz. zajęcia teoretyczne</p> <p>8 godz. zajęcia praktyczne</p>	<p>Poznanie znaczenia oraz metodologii i ram etycznego hakowania wraz z testami penetracyjnymi.</p> <p>Tworzenie wstępnych dokumentów testów penetracyjnych.</p> <p>Tworzenie zakresu i planu testów penetracyjnych, który uwzględni wymagania organizacyjne dotyczące usług.</p> <p>Wykonywanie działań związanych z gromadzeniem informacji i skanowaniem podatności.</p> <p>Socjotechnika.</p> <p>Wykorzystywanie luk w zabezpieczeniach sieci, aplikacji internetowych, urządzeń IoT oraz urządzeń mobilnych.</p> <p>Poznanie działań wykonywanych po przeprowadzeniu eksploatacji celu.</p> <p>Tworzenie raportów z testów.</p> <p>Klasyfikacja narzędzi pentestingowych według przypadków użycia.</p>

System bezpieczeństwa informacji	8 godz. zajęcia teoretyczne 8 godz. zajęcia praktyczne	<p>Wymagania prawne w zakresie bezpieczeństwa informacji – przegląd</p> <p>Bezpieczeństwo informacji wg ISO 27001:2022 jako proces – opis modelem żółwia</p> <p>Przegląd wymagań normy ISO 27001 w układzie HLS (ang. High Level Standard)</p> <p>Wykaz aktywów w organizacji – praktyczne ujęcie</p> <p>Analiza ryzyka dla zasobów informacyjnych – praktyczne ujęcie</p> <p>Klasyfikacja zasobów informacyjnych – rodzaj informacji, oznakowanie, maskowanie</p> <p>Incydenty i postępowanie – klasyfikacja incydentu, zbieranie dokumentacji, śledztwo</p> <p>Ochrona budynku i pomieszczeń</p> <p>Tworzenie opisów i instrukcji do omawianych zagadnień</p> <p>Case study w grupach</p>
Cisco Network Security	12 godz. zajęcia teoretyczne 14 godz. zajęcia praktyczne	<p>Wyjaśnienie bezpieczeństwa sieci, różnych rodzajów zagrożeń i ataków wraz z narzędziami i procedurami łagodzącymi skutki najpopularniejszych ataków sieciowych.</p> <p>Konfiguracja bezpiecznego dostępu administracyjnego oraz autoryzacji poleceń przy użyciu poziomów uprawnień i CLI opartego na rolach.</p> <p>Wdrożenie bezpiecznego zarządzania i monitorowania urządzeń sieciowych.</p> <p>Konfiguracja AAA oraz list kontroli dostępu.</p> <p>Zapoznanie się ze sprzętowymi oraz aplikacyjnymi zaporami sieciowymi.</p> <p>Zapoznanie się z sieciowymi systemami zapobiegania włamaniom.</p> <p>Bezpieczeństwo urządzeń końcowych oraz warstwy 2.</p> <p>Usługi kryptograficzne.</p> <p>Sieci VPN oraz ich konfiguracja.</p> <p>Praktyczne wykorzystanie sprzętowego firewalla ASA.</p> <p>Opisanie różnych technik i narzędzi wykorzystywanych do testowania bezpieczeństwa sieci.</p>
Audyt i monitorowanie cyberbezpieczeństwa	8 godz. zajęcia teoretyczne 8 godz. zajęcia praktyczne	<p>Rodzaje audytu bezpieczeństwa oraz sposoby jego przeprowadzania.</p> <p>Monitorowanie systemów i sieci komputerowych.</p> <p>Metodologiczne i formalno-prawne podstawy audytu systemu informacyjnego, w tym treści opartych o standard ISO27000.</p>

AI w cyberbezpieczeństwie	8 godz. zajęcia teoretyczne 12 godz. zajęcia praktyczne	<p>Podstawowe pojęcia z zakresu sztucznej inteligencji.</p> <p>Etapy budowy modeli AI i ML.</p> <p>Sposoby oceny jakości działania modelu.</p> <p>Podatności systemów sztucznej inteligencji i sposoby ich zabezpieczania.</p> <p>Sposoby wykorzystania języka Python i sztucznej inteligencji do automatyzacji działań w cyberbezpieczeństwie.</p> <p>Wpływ nadchodzących regulacji AI w kontekście cyberbezpieczeństwa.</p>
Bezpieczeństwo chmury publicznej AWS	6 godz. zajęcia teoretyczne 10 godz. zajęcia praktyczne	<p>Bezpieczeństwo pracy z chmurą publiczną AWS.</p> <p>Zabezpieczenie konta oraz bezpieczna praca w środowisku złożonym z wielu kont.</p> <p>Podstawy zasad bezpieczeństwa przy pracy z serwisami AWS.</p> <p>Zasady przechowywania i transportu danych w chmurze publicznej.</p> <p>Aspekt zarządzania kosztami.</p>
Praktyczne wykorzystanie Kali Linux	8 godz. zajęcia teoretyczne 8 godz. zajęcia praktyczne	<p>Zaawansowane testy penetracyjne, eskalacja uprawnień, kradzież tokenów i podszywanie się, zacieranie śladów, kodowanie i eksfiltracja danych, posteksploatacja.</p> <p>Profilowanie systemów operacyjnych.</p> <p>Sniffing w praktyce, ettercap, on-patch attack.</p> <p>Ataki na sieci bezprzewodowe, tworzenie złośliwych punktów dostępowych, włamywanie się do sieci WPA, WPA2.</p> <p>Konfiguracja karty sieciowej Alfa AWUS036NH, praca w trybie monitora.</p> <p>OSINT (Open-Source Intelligence) wprowadzenie, zbieranie informacji o celu. Narzędzia: maltego, spiderfoot, the harvester, sherlock, recon-ng.</p> <p>OSINT Framework.</p> <p>Google Hacking Database (GHDB) - Exploit-DB.</p> <p>Luki w zabezpieczeniach systemów operacyjnych.</p> <p>Badanie podatności systemów operacyjnych.</p> <p>Skanery Nessus, OpenVAS.</p> <p>Nmap Scripting Engine (NSE).</p> <p>Skanery aplikacji WWW.</p> <p>Open Web Application Security Project (OWASP).</p> <p>Burp Suite – badanie podatności aplikacji internetowych.</p>

Reagowanie na incydenty oraz informatyka śledcza	6 godz. zajęcia teoretyczne	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.
	8 godz. zajęcia praktyczne	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, umożliwiającą uzyskanie 30 punktów ECTS.

Dni zajęć dydaktycznych: sobota, niedziela w godz. 08.00 - 17.05. (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 zależą od decyzji poszczególnych wykładowców pod warunkiem zrealizowania ilości godzin dydaktycznych przewidzianych w harmonogramie. Przykładowo: 08.55-12.30 (4 godz. dyd. + 35 min przerwa); 08.00-11.30 (4 godz. dyd. + 30 min przerwa); 13.35-17.07 (4 godz. dyd. +30 min przerwa); 12.40-16.10 (4 godz. dyd + 30 min przerwa); 08.00-10.30 (3 godz. dyd. + 20 min. przerwa). Sumaryczna liczba godzin usługi zawiera 182 godziny dydaktyczne (45 minut) i przerwy.

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. Po pozytywnym zdaniu egzaminu końcowego uzyskuje świadectwo ukończenia studiów podyplomowych.

## Harmonogram

Liczba pozycji harmonogramu: 51

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
<b>1 z 51</b> Wprowadzenie do systemu Kali Linux, 4 godz. dydaktyczne	Krzysztof Trąbiński	11-10-2025	08:55	12:30	03:35
<b>2 z 51</b> Cisco Ethical Hacker, 4 godz. dydaktyczne	dr Inż. Janusz Korniak	11-10-2025	13:35	17:05	03:30

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
<b>3 z 51</b> Cisco CyberOPS Associate, 3 godz. dydaktyczne	Kamil Dembowski	12-10-2025	08:00	10:35	02:35
<b>4 z 51</b> Cisco CyberOPS Associate, 3 godz. dydaktyczne	Kamil Dembowski	12-10-2025	11:45	14:20	02:35
<b>5 z 51</b> Wprowadzenie do systemu Kali Linux, 4 godz. dydaktyczne	Krzysztof Trąbiński	25-10-2025	08:00	11:30	03:30
<b>6 z 51</b> Cisco Ethical Hacker, 4 godz. dydaktyczne	dr Inż. Janusz Korniak	25-10-2025	12:40	16:10	03:30
<b>7 z 51</b> Cisco CyberOPS Associate, 3 godz. dydaktyczne	Kamil Dembowski	26-10-2025	08:00	10:35	02:35
<b>8 z 51</b> Cisco CyberOPS Associate, 3 godz. dydaktyczne	Kamil Dembowski	26-10-2025	11:45	14:20	02:35
<b>9 z 51</b> Cisco Ethical Hacker, 4 godz. dydaktyczne	dr Inż. Janusz Korniak	15-11-2025	08:00	11:30	03:30
<b>10 z 51</b> Wprowadzenie do systemu Kali Linux, 4 godz. dydaktyczne	Krzysztof Trąbiński	15-11-2025	12:40	16:10	03:30
<b>11 z 51</b> System bezpieczeństwa informacji, 4 godz. dydaktyczne	Aleksander Kulesz	16-11-2025	08:00	11:30	03:30

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
<b>12 z 51</b> Cisco CyberOPS Associate, 4 godz. dydaktyczne	Kamil Dembowski	16-11-2025	12:40	16:10	03:30
<b>13 z 51</b> System bezpieczeństwa informacji, 4 godz. dydaktyczne	Aleksander Kulesz	29-11-2025	08:00	11:30	03:30
<b>14 z 51</b> Wprowadzenie do systemu Kali Linux, 4 godz. dydaktyczne	Krzysztof Trąbiński	29-11-2025	12:40	16:10	03:30
<b>15 z 51</b> Cisco Ethical Hacker, 4 godz. dydaktyczne	dr Inż. Janusz Korniak	30-11-2025	08:00	11:30	03:30
<b>16 z 51</b> Cisco CyberOPS Associate, 4 godz. dydaktyczne	Kamil Dembowski	30-11-2025	12:40	16:10	03:30
<b>17 z 51</b> Cisco CyberOPS Associate, 3 godz. dydaktyczne	Kamil Dembowski	13-12-2025	08:00	10:35	02:35
<b>18 z 51</b> Cisco CyberOPS Associate, 3 godz. dydaktyczne	Kamil Dembowski	13-12-2025	11:45	14:20	02:35
<b>19 z 51</b> System bezpieczeństwa informacji, 4 godz. dydaktyczne	Aleksander Kulesz	14-12-2025	08:00	11:30	03:30
<b>20 z 51</b> System bezpieczeństwa informacji, 4 godz. dydaktyczne	Aleksander Kulesz	17-01-2026	08:00	11:30	03:30

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
<b>21 z 51</b> Audyt i monitorowanie cyberbezpieczeństwa, 4 godz. dydaktyczne	dr Edward Szczypka	31-01-2026	08:00	11:30	03:30
<b>22 z 51</b> Cisco Network Security, 4 godz. dydaktyczne	Mateusz Liput	31-01-2026	12:40	16:10	03:30
<b>23 z 51</b> Audyt i monitorowanie cyberbezpieczeństwa, 4 godz. dydaktyczne	dr Edward Szczypka	01-02-2026	08:00	11:30	03:30
<b>24 z 51</b> Cisco Network Security, 4 godz. dydaktyczne	Mateusz Liput	01-02-2026	12:40	16:10	03:30
<b>25 z 51</b> Audyt i monitorowanie cyberbezpieczeństwa, 4 godz. dydaktyczne	dr Edward Szczypka	14-02-2026	08:00	11:30	03:30
<b>26 z 51</b> Cisco Network Security, 4 godz. dydaktyczne	Mateusz Liput	14-02-2026	12:40	16:10	03:30
<b>27 z 51</b> Audyt i monitorowanie cyberbezpieczeństwa, 4 godz. dydaktyczne	dr Edward Szczypka	15-02-2026	08:00	11:30	03:30
<b>28 z 51</b> Cisco Network Security, 4 godz. dydaktyczne	Mateusz Liput	15-02-2026	12:40	16:10	03:30
<b>29 z 51</b> Bezpieczeństwo chmury publicznej AWS, 4 godz. dydaktyczne	Łukasz Chłap	07-03-2026	08:00	11:30	03:30

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
<b>30 z 51</b> AI w cyberbezpieczeństwie, 4 godz. dydaktyczne	Jan Kaczmarczyk	07-03-2026	12:40	16:10	03:30
<b>31 z 51</b> Bezpieczeństwo chmury publicznej AWS, 2 godz. dydaktyczne	Łukasz Chłap	08-03-2026	08:00	09:40	01:40
<b>32 z 51</b> Bezpieczeństwo chmury publicznej AWS, 2 godz. dydaktyczne	Łukasz Chłap	08-03-2026	09:50	11:30	01:40
<b>33 z 51</b> AI w cyberbezpieczeństwie, 4 godz. dydaktyczne	Jan Kaczmarczyk	08-03-2026	12:40	16:10	03:30
<b>34 z 51</b> AI w cyberbezpieczeństwie, 4 godz. dydaktyczne	Jan Kaczmarczyk	21-03-2026	08:00	11:30	03:30
<b>35 z 51</b> Cisco Network Security, 4 godz. dydaktyczne	Mateusz Liput	21-03-2026	12:40	16:10	03:30
<b>36 z 51</b> Cisco Network Security, 4 godz. dydaktyczne	Mateusz Liput	22-03-2026	08:00	11:30	03:30
<b>37 z 51</b> AI w cyberbezpieczeństwie, 4 godz. dydaktyczne	Jan Kaczmarczyk	22-03-2026	12:40	16:10	03:30
<b>38 z 51</b> Bezpieczeństwo chmury publicznej AWS, 4 godz. dydaktyczne	Łukasz Chłap	11-04-2026	08:00	11:30	03:30

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
<b>39 z 51</b> Cisco Network Security, 2 godz. dydaktyczne	Mateusz Liput	11-04-2026	12:40	14:20	01:40
<b>40 z 51</b> Bezpieczeństwo chmury publicznej AWS, 4 godz. dydaktyczne	Łukasz Chłap	12-04-2026	08:00	11:30	03:30
<b>41 z 51</b> Praktyczne wykorzystanie Kali Linux, 4 godz. dydaktyczne	Krzysztof Trąbiński	12-04-2026	12:40	16:10	03:30
<b>42 z 51</b> AI w cyberbezpieczeństwie, 4 godz. dydaktyczne	Jan Kaczmarczyk	25-04-2026	08:00	11:30	03:30
<b>43 z 51</b> Praktyczne wykorzystanie Kali Linux, 4 godz. dydaktyczne	Krzysztof Trąbiński	25-04-2026	12:40	16:10	03:30
<b>44 z 51</b> Praktyczne wykorzystanie Kali Linux, 4 godz. dydaktyczne	Krzysztof Trąbiński	26-04-2026	08:00	11:30	03:30
<b>45 z 51</b> Reagowanie na incydenty oraz informatyka śledcza, 4 godz. dydaktyczne	Kamil Boroszko	26-04-2026	12:40	16:10	03:30
<b>46 z 51</b> Praktyczne wykorzystanie Kali Linux, 4 godz. dydaktyczne	Krzysztof Trąbiński	16-05-2026	08:00	11:30	03:30

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
47 z 51 Reagowanie na incydenty oraz informatyka śledcza, 2 godz. dydaktyczne	Kamil Boroszko	16-05-2026	12:40	14:20	01:40
48 z 51 Reagowanie na incydenty oraz informatyka śledcza, 2 godz. dydaktyczne	Kamil Boroszko	16-05-2026	14:30	16:10	01:40
49 z 51 Reagowanie na incydenty oraz informatyka śledcza, 3 godz. dydaktyczne	Kamil Boroszko	17-05-2026	08:00	10:35	02:35
50 z 51 Reagowanie na incydenty oraz informatyka śledcza, 3 godz. dydaktyczne	Kamil Boroszko	17-05-2026	11:45	14:20	02:35
51 z 51 Walidacja - egzamin końcowy	-	03-06-2026	09:00	13:00	04:00

## 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: 11



1 z 11

## Kamil Dembowski

Absolwent Wyższej Szkoły Informatyki i Zarządzania z siedzibą w Rzeszowie na kierunkach licencjackim (Informatyka i Ekonometria) oraz magisterskim (Informatyka Stosowana – Infrastruktura i Usługi Sieciowe Cisco). Trener w programie Akademii Sieciowej Cisco z zakresu szkoleń: IT Essentials, CCNA, Network Security, Cybersecurity Operations. Autoryzowany „Instructor Trainer” w programie Akademii Sieciowej Cisco dla szkoleń: IT Essentials, CCNA, Network Security. Posiada branżową certyfikację CCNA.

Nauczyciel akademicki w Wyższej Szkole Informatyki i Zarządzania oraz wieloletni współpracownik Cisco jako instruktor dla Centrum Szkolenia Instruktorów przy WSiLiZ w Rzeszowie. W latach 2022-2024 prowadził zajęcia dydaktyczne na studiach I i II stopnia oraz studiach podyplomowych z zakresu: systemy i sieci komputerowe, cyberbezpieczeństwo systemów informatycznych. Wykładowca posiada wiedzę i umiejętności nabyte w ostatnich 5 latach, związane z zakresem prowadzonych zajęć dydaktycznych.



2 z 11

## 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 2020-2025 prowadził zajęcia dydaktyczne na studiach I i II stopnia oraz studiach podyplomowych: Systemy i sieci komputerowe.

Wykładowca posiada wiedzę i umiejętności nabyte w ostatnich 5 latach, związane z zakresem prowadzonych zajęć dydaktycznych.



3 z 11

## 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.

Wykładowca posiada wiedzę i umiejętności nabyte w ostatnich 5 latach, związane z zakresem prowadzonych zajęć dydaktycznych.



4 z 11

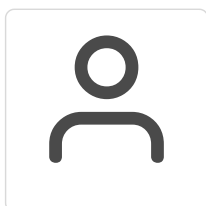
## Aleksander Kulesz

Absolwent Politechniki Łódzkiej, Wydziału Budowy Maszyn z ukończonym stopniem inżyniera mechanika w roku 2001. W roku 2016 ukończył Akademię Techniczno-Humanistyczną w Bielsku-Białej ze stopniem magistra inżyniera Zarządzania Produkcją Wydziału Budowy Maszyn. Od ponad 20 lat związany zawodowo z zarządzaniem jakością na stanowiskach od samodzielnego pracownika ds. jakości, poprzez inżyniera procesu i jakości, lidera zarządzania dostawcami a skończywszy na kierowniku i pełnomocniku ds. zintegrowanych systemów zarządzania jakością i środowiskiem.

Auditor wiodący systemu bezpieczeństwa informacji wg normy ISO 27001, certyfikowany auditor procesu wg podręcznika VDA 6.3 oraz wewnętrzny auditor systemu zarządzania jakością wg IATF 16949. Trener systemów zarządzania jakością w branży ogólnoprzemysłowej, motoryzacyjnej i lotniczej.

Poza pracą w zakresie jakości zajmuje się projektowaniem i wdrażaniem oprogramowania / aplikacji jako usprawnienia w funkcjonowaniu organizacji. Współpracuje z WSH w Wrocławiu, WSiLiZ w Rzeszowie oraz UE w Katowicach prowadząc zajęcia związane z zarządzaniem jakością począwszy od budowy systemów, procesów jak i zastosowaniem narzędzi jakości takich jak APQP, PPAP, FMEA, SPC, MSA oraz odpowiedników wydań podręczników VDA.

Wykładowca posiada wiedzę i umiejętności nabyte w ostatnich 5 latach, związane z zakresem prowadzonych zajęć dydaktycznych.



5 z 11

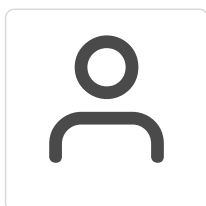
## Krzysztof Trąbiński

Absolwent Akademii Pomorskiej w Słupsku na kierunkach licencjackim (Matematyka z Informatyką) oraz magisterskim (Matematyka). Absolwent studiów podyplomowych w Wyższej Szkole Informatyki i Zarządzania z siedzibą w Rzeszowie na kierunku Systemy i Sieci Komputerowe. Absolwent European IT Security Certification Academy EITCA/IS (European Information Technologies Certification Academy, Information Technologies, Brussels, UE) z zakresu sieci komputerowych, systemów operacyjnych oraz cyberbezpieczeństwa.

Certyfikowany instruktor Akademii Sieciowej Cisco z zakresu szkoleń: CCNA, CCNP, Network Security, Cybersecurity Operations, DevNet Associate, IoT Security. Certyfikowany technik wsparcia Cisco z zakresu CCST Networking, CCST Cybersecurity. Certyfikowany specjalista IBM Cybersecurity Analyst oraz Palo Alto Networks Cybersecurity Academy. Uczestnik Sekurak Academy oraz Hack the Box Academy. Uczestnik wielu kursów oraz szkoleń w Eksperckim Centrum Szkolenia Cyberbezpieczeństwa. Posiada branżową certyfikację CCST Networking, CCST Cybersecurity, EITCA/IS.

Posiada duże doświadczenie oraz wiedzę z zakresu technologii sieciowych Cisco na poziomie CCNA, CCNP oraz cybersecurity. Zajmuje się obsługą incydentów oraz zagrożeń z zakresu cyberbezpieczeństwa. Szkoli przyszłych administratorów sieci teleinformatycznych.

Wykładowca posiada wiedzę i umiejętności nabyte w ostatnich 5 latach, związane z zakresem prowadzonych zajęć dydaktycznych.



6 z 11

## Przemysław Szczurek

Absolwent Uniwersytetu Ekonomicznego w Krakowie. Z branżą IT związany od ponad 15 lat. Obecnie pełni funkcję Senior Managera ds. Bezpieczeństwa Informacji w TUV NORD Polska, gdzie odpowiada za rozwój i sprzedaż usług związanych z normami: ISO 27001, ISO 20000, ISO 22301 oraz tematyką ODO, Cyberbezpieczeństwa i TISAX.

Posiada certyfikaty: Audytora Wiodącego ISO 27001, ISO 20000, Audytora Wewnętrznego ISO 22301, Incident Response Managera i Inspektora Ochrony Danych. Jest egzaminatorem dla Audytorów Wiodących ISO 27001 akredytowanym przez PCA. Prelegent na wielu Konferencjach i wykładowca na Wyższych Uczelniach. Jako trener TUV NORD i wykładowca akademicki duży nacisk stawia na świadomość kadry.

Wykładowca posiada wiedzę i umiejętności nabyte w ostatnich 5 latach, związane z zakresem prowadzonych zajęć dydaktycznych.



7 z 11

### Jan Kaczmarczyk

Specjalista kompleksowo zajmujący się przeciwdziałaniem przestępstwom finansowym certyfikowany przez ACAMS. Pasjonat OSINTu i analizy danych. Pracuje w bankowości jako walidator modeli.

Wykładowca posiada wiedzę i umiejętności nabyte w ostatnich 5 latach, związane z zakresem prowadzonych zajęć dydaktycznych.



8 z 11

### Łukasz Chłap

Absolwent Wyższej Szkoły Informatyki i Zarządzania z siedzibą w Rzeszowie. Administrator Windows, VMware. Pracował w IBM, Atos, Aon. Od 2015 roku związany z chmurą publiczną AWS. Obecnie jako samodzielny DevOps wspiera startup z sektora Big Data.

Wykładowca posiada wiedzę i umiejętności nabyte w ostatnich 5 latach, związane z zakresem prowadzonych zajęć dydaktycznych.



9 z 11

### Kamil Boroszko

Prowadzi zajęcia dydaktyczne na studiach pierwszego, drugiego stopnia i studiach podyplomowych. Ekspert z zakresu informatyki śledczej i reagowania na incydenty. Współpracownik Katedry Inteligentnych Systemów i Sieci WSliZ.

Wykładowca posiada wiedzę i umiejętności nabyte w ostatnich 5 latach, związane z zakresem prowadzonych zajęć dydaktycznych.



10 z 11

### dr inż. Janusz Kolbusz

Absolwent Politechniki Rzeszowskiej. Od roku 1998 pracuje w Wyższej Szkole Informatyki i Zarządzania. Stopień doktora nauk technicznych z zakresu dyscypliny naukowej telekomunikacja uzyskał w roku 2010 na Wydziale Elektroniki i Telekomunikacji Uniwersytetu Technologiczno – Przyrodniczym w Bydgoszczy. Zainteresowania naukowe obejmują zagadnienia rozległych sieci optycznych, lokalnych sieci komputerowych i jakości usług.

Egzaminator ECDL: Core, Advanced, e-Obywatel. Instruktor Akademii Cisco: CCNA, Information Technology Essentials I i II, Fundamentals of Wireless LANs, CCNA Security.

Prowadzi zajęcia z zakresu: podstaw informatyki, sieci komputerowych, systemów operacyjnych, automatyki i robotyki. Autor ponad 20 artykułów naukowych o zasięgu krajowym i międzynarodowym.

Wykładowca posiada wiedzę i umiejętności nabyte w ostatnich 5 latach, związane z zakresem studiów podyplomowych.

11 z 11

### dr Edward Szczypka



Doktor nauk matematycznych w informatyce, pracownik naukowo-dydaktyczny Wydziału Matematyki i Informatyki UJ. Członek Rady Pracodawców oraz Rady Programowej kursów Blue Team.

Ekspert współpracujący z e-Detektywi Sp. z o.o., biegły sądowy, prelegent konferencji z zakresu bezpieczeństwa i informatyki śledczej, lider projektów dla przemysłu.

## 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.

Usługa jest zwolniona z VAT na podstawie art. 43 ust. 1 pkt 26b ustawa o podatku VAT.

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

## 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](mailto:bcieszynski@wsiz.edu.pl)

**Telefon** (+48) 178 661 518