Możliwość dofinansowania

Cyberbezpieczeństwo - Studia podyplomowe - Collegium Da Vinci

Numer usługi 2025/06/13/9743/2814704

8 650,00 PLN brutto
8 650,00 PLN netto
43,25 PLN brutto/h
43,25 PLN netto/h

Collegium Da Vinci z siedzibą w Poznaniu

4,5 / 5

97 ocen

zdalna w czasie rzeczywistym
Studia podyplomowe
200 h
29.11.2025 do 31.07.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Studia adresowane są dla: • absolwentów i absolwentek różnych kierunków studiów wyższych, szczególnie informatycznych i pokrewnych • pracowników i pracowniczek branży IT, chcących specjalizować się w obszarze cyberbezpieczeństwa • administratorów i administratorek systemów, programistów i programistek oraz analityków i analityczek IT • kadry zarządzającej oraz specjalistów i specjalistek bezpieczeństwa • przedstawicieli i przedstawicielek firm i organizacji odpowiedzialnych za zgodność z regulacjami (np. RODO) oraz ochronę infrastruktury cyfrowej • osób z podstawową wiedzą informatyczną (systemy operacyjne, sieci, analiza danych, chmura obliczeniowa, programowanie; znajomość platformy Azure, Microsoft 365 i Windows 10/11)
Minimalna liczba uczestników	25
Maksymalna liczba uczestników	27
Data zakończenia rekrutacji	30-09-2025
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	200
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 2024 r. poz. 1571, z późn. zm.)
Zakres uprawnień	Studia podyplomowe

Cel

Cel edukacyjny

Usługa przygotowuje do projektowania strategii bezpieczeństwa IT dla organizacji, monitorowania ruchu sieciowego i wykrywania zagrożenia w czasie rzeczywistym, analizowania incydentów bezpieczeństwa i reagowania na nie oraz przygotowywanie raportów z audytów bezpieczeństwa.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Przygotowuje raporty z audytów bezpieczeństwa	- Opracowuje raport zawierający opis stanu zabezpieczeń, wykryte luki i ocenę ryzyka, - Raportuje przejrzyście, logicznie i popiera to danymi z analizy, - Rekomenduje działania naprawcze dostosowane do potrzeb organizacji	Obserwacja w warunkach symulowanych
Projektuje strategie bezpieczeństwa IT dla organizacji	- Opracowuje strategię uwzględniając zagrożenia, specyfikę organizacji i wymagania prawne, - Proponuje rozwiązania spójne, realistyczne i możliwe do wdrożenia - Ustawia priorytety działań, podziałań odpowiedzialności i procedur reagowania	Prezentacja
Monitoruje ruch sieciowy i wykrywanie zagrożeń w czasie rzeczywistym	- Korzysta z odpowiednich narzędzi monitorujących (np. SIEM,IDS/IPS) i interpretuje dane, - Identyfikuje anomalie oraz rozpoznaje symptomy ataków, - Dokumentuje incydenty i podejmuje działania zgodne z procedurami bezpieczeństwa	Obserwacja w warunkach symulowanych

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

Studia podyplomowe

Studia podyplomowe trwają 9 miesięcy (200 godzin dydaktycznych **po 45 min.**). Zajęcia są realizowane w trakcie 10 zjazdów, w trybie sobota – niedziela (w godz. 9.00 – 17.30). Zajęcia są przeprowadzane w 100% online.

Zajęcia mają 90 godzin po 45 minut zajęć teoretycznych (wykładów) oraz 110 godzin po 45 minut zajęć praktycznych (ćwiczenia i warsztaty).

Zastrzegamy sobie możliwość zmiany formy zajęć 24 h przed rozpoczęciem danego spotkania.

W harmonogramie studiów uwzględniono przerwy między zajęciami, które trwają od 5 do 30 minut.

Studia obejmują 30 pkt ETCS.

Program

Cyberbezpieczeństwo - dziś i jutro (20 godz.) - 3 pkt ETCS

- Wstęp. Definicja cyberprzestrzeni i cyberbezpieczeństwa, aktualne trebdy na świecie
- Typy ataków hakerskich - demonstracje wraz z objaśnieniem metody ochrony
- Dobre praktyki, formy obrony przed atakami
- Rozwój kompetencji z zakresu bezpieczeństwa
- Dlaczego bezpieczeństwo to nie tylko departament

Cyberbezpieczeństwo w systemach operacyjnych (10 godz.) - 1 pkt ETCS

- Wprowadzenie do bezpieczeństwa systemów operacyjnych
- Bezpieczeństwo systemu Windows
- Bezpieczeństwo systemu Linux
- Bezpieczeństwo w systemie MacOS
- Dobre praktyki bezpieczeństwa

Informatyka śledcza (30 godz.) - 4 pkt ETCS

- Teoria (podstawy i proces informacji śledczej)
- Przegląd aktów prawnych i standardów dotyczących informacji śledczej
- Proces informatyki śledczej
- Zabezpieczanie dowodów cyfrowych
- Analiza danych cyfrowych
- Analiza sieciowa
- Analiza malware
- Informatyka śledcza w chmurze
- Śledztwa w mediach społecznościowych - OSINT
- Warsztaty - symulacja zabezpieczenia miejsca zdarzenia
- Warsztaty - analiza danych cyfrowych
- Warsztaty - analiza sieciowa i malware
- Analiza rzeczywistych przypadków śledczych

Warsztaty z CompTIA Security+ (40 godz.) -7 PKT ETCS

- Podstawowe koncepcje bezpieczeństwa
- Porównanie różnych typów zagrożeń
- Omówienie podstawowych pojęć kryptografii
- Wdrażanie zarządzania tożsamością i kontrola dostępu
- Zabezpieczanie architektury sieci korporacyjnej
- Zabezpieczanie architektury sieci w usługach chmurowych

- Omówienie koncepcji odporności
- Zarządzanie podatności
- Bezpieczeństwo sieciowe
- Ocena bezpieczeństwa punktóww końcowych
- Wdrażanie zabezpieczeńs aplikacji
- Zarządzanie incydentem i monitorowanie środowiska
- Po czym rozpoznać atak - wskaźnik kompromitacji
- Zarządzani bezpieczeństwem w organizacji poprzez polityki, standardy i procedury
- Podstawowe pojęcia związane zarządzania ryzykiem
- Ochrona danych i dbałość o ich zgodność w organizacji

Microsoft Security, Compliance and Identity Fundamentals. Przygotowanie do egzaminu (30 godz.) - 6 pkt ETCS

- Podstawowe pojęcia dotyczące bezpieczeństwa, zgodność i tożsamości
- Koncepcje i możliwości rozwiązań firmy Microsoft do zarządzania tożsamością i dostępem
- Możliwości rozwiązań zabezpieczających firmy Microsoft
- Możliwości rozwiązań Microsoft zapewniających zgodność
- Warsztat przygotowujący do egzaminu

Microsoft Security Operations Analyst (30 godz.) - 4 pkt ETCS

- Ograniczanie zagrożenia za pomocą usługi Microsoft 365 Defender
- Ograniczanie zagrożenia za pomocą usługi Microsoft Defender dla punktów końcowych
- Ograniczanie zagrożenia za pomocą usługi Microsoft Defender for Cloud
- Tworzenie zapytań dla Microsoft Sentinel przy użyciu języka Kusto Query Language
- Konfiguracja środowiska Microsoft Sentinel
- Łączenie dzienników z Microsoft Sentinel
- Wykrywanie i prowadzenie dochodzenia przy użyciu probgramu Microsoft Sentinel
- Polowanie na zagrożenia w Microsoft Sentinel

RODO (10 godz.) - 1pkt ETSC

- Wprowadzenie do RODO (GDPR) i gejo znaczenie w cyberbezpieczeństwie
- [Przetwarzanie danych osobowych i odpowiedzialność w kontekście technologicznym
- Zabezpieczenia techniczne i organizacyjne zgodnie z RODO
- Zarządzanie incydentami naruszenia danych i informatyka śledcza
- Zgodność z RODO w systemach AI i automatyzacji procesów
- Podsumowanie, sesja pytań i odpowiedzi oraz quiz sprawdzający

Bezpieczeństwo aplikacji webowych (20 godz.) - 3 pkt ETCS

- Wprowadzanie do bezpieczeństwa aplikacji webowych
- Bezpieczeństwo ruchu sieciowego (TLS.SSL, nagłówki HTTP, Same-Origin Policy i Cross-Origin Resource Sharing)
- Narzędzia (analiza ruchu sieciowego, manipulacja zapytaniami HHTP, tworzenie własnych skryptów, skanery podatności)
- Analiza podatności (atak, obrona, przykład)
  - Bezpieczeństwo API
  - Czarnoskrzynkowy test penetracyjny (CTF)

Bezpieczeństwo Copilot (10 godz.) -1 pkt ETCS

- Badanie projektu Copilot dla Microsoft 365
- Wdrażanie Copilot dla Microsoft 365
- Badanie bezpieczeństwa danych i zgodność w Copilot dla Microsoft 365
- Zarządzanie bezpiecznych dostępem użytkowników w Microsoft 365
- Zarządzanie rolami i grupami ról w Microsoft 365
- Eksploracja wywiadu zagrożeń w Microsoft Defender XDR

Zaliczenie

Warunkiem ukończenia studiów podyplomowych Cyberbezpieczeństwo jest uzyskane pozytywnego wyniku z dwóch egzaminów semestralnych. Egzaminy przewidziano na koniec każdego semestru w formie testu wyboru.

Absolwenci uzyskują, zgodne z wymogami ustawy, świadectwo ukończenia studiów podyplomowych w Collegium Da Vinci.

Harmonogram

Liczba przedmiotów/zajęć: 20

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 20 Cyberbezpieczeństwo - dziś i jutro	Jakub Tomaszewski	29-11-2025	08:00	18:00	10:00
2 z 20 Cyberbezpieczeństwo - dziś i jutro	Jakub Tomaszewski	30-11-2025	08:00	18:00	10:00
3 z 20 Cyberbezpieczeństwo w systemach operacyjnych	Marek Krupa	20-12-2025	09:00	17:30	08:30
4 z 20 Informatyka śledcza	Piotr Wichrań	21-12-2025	09:00	17:30	08:30
5 z 20 Informatyka śledcza	Piotr Wichrań	24-01-2026	09:00	17:30	08:30
6 z 20 Informatyka śledcza	Piotr Wichrań	25-01-2026	09:00	17:30	08:30
7 z 20 Warsztaty z CompTIA Security+	-	14-02-2026	09:00	17:30	08:30
8 z 20 Warsztaty z CompTIA Security+	-	15-02-2026	09:00	17:30	08:30
9 z 20 Warsztaty z CompTIA Security+	-	07-03-2026	09:00	17:30	08:30
10 z 20 Warsztaty z CompTIA Security+	-	08-03-2026	09:00	17:30	08:30

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
11 z 20 Microsoft Security, Compliance and Identity Fundamentals + przygotowanie do egzaminu	Marek Krupa	18-04-2026	09:00	17:30	08:30
12 z 20 Microsoft Security, Compliance and Identity Fundamentals + przygotowanie do egzaminu	Marek Krupa	19-04-2026	09:00	17:30	08:30
13 z 20 Microsoft Security, Compliance and Identity Fundamentals + przygotowanie do egzaminu	Marek Krupa	16-05-2026	09:00	17:30	08:30
14 z 20 Microsoft Security Operations Analyst	Marek Krupa	17-05-2026	09:00	17:30	08:30
15 z 20 Microsoft Security Operations Analyst	Marek Krupa	30-05-2026	09:00	17:30	08:30
16 z 20 Microsoft Security Operations Analyst	Marek Krupa	31-05-2026	09:00	17:30	08:30
17 z 20 RODO	Krzysztof Sługocki	20-06-2026	09:00	17:30	08:30
18 z 20 Bezpieczeństwo aplikacji webowych	Rafał Wójcik	21-06-2026	09:00	17:30	08:30
19 z 20 Bezpieczeństwo aplikacji webowych	Rafał Wójcik	04-07-2026	09:00	17:30	08:30

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
20 z 20 Bezpieczeństwo Copilot	Marek Krupa	05-07-2026	09:00	17:30	08:30

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	8 650,00 PLN
Koszt przypadający na 1 uczestnika netto	8 650,00 PLN
Koszt osobogodziny brutto	43,25 PLN
Koszt osobogodziny netto	43,25 PLN

Prowadzący

Liczba prowadzących: 5

1 z 5

Piotr Wichrań

Magister inżynier Wojskowa Akademia Techniczna w Warszawie
Informatyka Śledcza Piotr Wichrań (grudzień 1999 – obecnie)
Cyber Security and Forensics Analyst
Biegły sądowy z zakresu informatyki.
Ekspertyzy sądowe, zabezpieczanie dowodów elektronicznych, audyt bezpieczeństwa, analiza powłamaniowa.
Prowadzenie szkoleń dla firm z zakresu bezpieczeństwa IT.
Wdrażanie projektów z zakresu bezpieczeństwa IT.
Uprawnienia detektywa do przetwarzania danych osobowych zgodnie z Art. 8.1 Ustawy o usługach detektywistycznych.
Poświadczenie bezpieczeństwa dostępu do informacji oznaczonych klauzulą: ściśle tajne, tajne, poufne.
E.ON Polska IT Support Sp. z o.o. (lipiec 2023 – kwiecień 2025)
Cybersecurity Architecti.

Certyfikaty / kursy / umiejętności techniczne:
AWS Professional Solutions Architect 2020: AWS & Data Protection (Skillsoft, wydany kwi 2021, ID: 720913)
Certified Information Systems Auditor (CISA) 2019: Data Privacy & Risk (Skillsoft, wydany kwi 2021, ID: 720903)
Ethical Hacker: Host Discovery & Scanning with Nmap (Skillsoft, wydany kwi 2021, ID: 720889)
Getting Started with PowerShell (Skillsoft, wydany kwi 2021, ID: 720523)
Penetration Testing & Vulnerability Scanning (Skillsoft, wydany kwi 2021, ID: 720879)
SECOPS: Scoring with CVSS 3.0 (Skillsoft, wydany kwi 2021, ID: 728078)
Windows Exploits and Forensics: Post Exploitation (Skillsoft, wydany kwi 2021, ID: 723106)
Certified Information Systems Auditor (CISA) 2019

2 z 5

Rafał Wójcik

Wykształcenie średnie
EXATEL S.A.
Inżynier ds. Zaawansowanych Usług Bezpieczeństwa
(lipiec 2022 – obecnie)
Realizacja usług z zakresu bezpieczeństwa informacji i testów penetracyjnych.
Altkom Akademia S.A.
Trener bezpieczeństwa IT
(sierpień 2023 – obecnie)
Szkolenia z zakresu bezpieczeństwa aplikacji webowych i etycznego hackingu.
MrCertified
Instruktor ds. bezpieczeństwa IT
(październik 2021 – obecnie)
Konsultacje, tworzenie oraz prowadzenie szkoleń z zakresu cyberbezpieczeństwa.
Tester merytoryczny kursów CyberSec
(kwiecień 2021 – obecnie)
Weryfikacja kursów i materiałów edukacyjnych.
Specjalizacja:
Penetration Testing, Bug Bounty, Red Team, bezpieczeństwo aplikacji webowych, CTF, analiza podatności, programowanie w kontekście bezpieczeństwa.

Top certyfikaty (2022–2024)

OSWE – OffSec Web Expert (OffSec, luty 2024)
OSCP – Offensive Security Certified Professional (OffSec, czerwiec 2022)
Red Team Operator (Zero-Point Security, luty 2024)
eMAPT – Mobile App Penetration Tester (INE Security, maj 2024)
Platformy treningowe i laboratoria praktyczne
HackTheBox – Zephyr Pro Lab (maj 2023)
HackTheBox – Dante Pro Lab (styczeń 2023)

TryHackMe JR Penetration Tester (luty 2022)
TryHackMe Web Fundamentals, Complete Beginner, Pre Security, Offensive Pentesting, CompTIA Pentest+
Certyfikaty PentesterLab (2021–2022)
Android Badge (x2) (marzec 2021, grudzień 2022)
HTTP Badge, Yellow Badge, Essential Badge, Introduction Badge, PCAP Badge, Serialize Badge, Unix Badge, White
Badge, Blue Badge

3 z 5

Marek Krupa

Magister inżynier, absolwent Politechniki Opolskiej, Automatyka przemysłowa
Uprawnienia pedagogiczne - Uniwersytet Pedagogiczny w Krakowie
Altkom Akademia S.A. (od stycznia 2016 – obecnie)
Stanowisko: Trener Microsoft / Konsultant
Zakres obowiązków:
Prowadzenie autoryzowanych szkoleń Microsoft (Azure, Office 365, Windows Server, PowerShell, SharePoint, System Center)
Realizacja szkoleń i kursów autorskich z zakresu nowoczesnego środowiska pracy (Modern Workplace) i bezpieczeństwa IT
Konsultacje i wdrożenia w środowiskach firm prywatnych i publicznych
Uniwersytet Opolski (2016 – obecnie)
Stanowisko: Wykładowca na studiach podyplomowych
Zakres obowiązków: Prowadzenie zajęć z zakresu IT i technologii Microsoft
Sąd Rejonowy w Żorach (2017 – obecnie)
Stanowisko: Administrator Bezpieczeństwa Informacji
Zakres obowiązków: Nadzór nad bezpieczeństwem danych osobowych i systemów IT

Microsoft Certified Trainer (MCT) – aktywny od 2006 roku,

aktualny
Microsoft Certified: Azure Fundamentals
Certyfikaty techniczne Microsoft (nabyte lub utrzymywane):
MCSA (Microsoft Certified Solutions Associate)
MCSE (Microsoft Certified Solutions Expert)
MCITP (Microsoft Certified IT Professional)
MCTS (Microsoft Certified Technology Specialist)
Tytuł Microsoft MVP – dwukrotnie uhonorowany przez Microsoft (Most Valuable Professional)

4 z 5

Krzysztof Sługocki

Magister fizyki, absolwent Uniwersytetu Opolskiego
Ponad 20 lat doświadczenia jako trener, konsultant, analityk danych, informatyk i specjalista ochrony danych osobowych

Prowadzenie szkoleń i wdrożeń z zakresu zaawansowanych zastosowań Excela, AI, modeli językowych (LLM) i prawa ochrony danych osobowych (RODO)
Współpraca z firmami i instytucjami, m.in. Altkom Akademia S.A., SEMPER Centrum, J.G. Training, Europejskie Centrum Edukacji EURA, Excellent, Intellect
Specjalizacja w prowadzeniu szkoleń z wykorzystania sztucznej inteligencji (AI), modeli językowych i narzędzi analitycznych
Rozwój kompetencji miękkich: komunikacja biznesowa, negocjacje, autoprezentacja, zarządzanie czasem, ze szczególnym naciskiem na komunikację z AI i NLP

Certyfikowany Trener Biznesu (Wyższa Szkoła Bankowa,

Wrocław)
Studia podyplomowe z ochrony danych osobowych (Uniwersytet Łódzki)
Studia podyplomowe z zastosowań MS Excel w controllingu (Uniwersytet Ekonomiczny we Wrocławiu)
Data Scientist – Big Data (Akademia WSB w Dąbrowie Górniczej)
Ciągłe doskonalenie poprzez platformy Coursera, EdX, Domestika i inne
Certyfikowany Trener Biznesu (Wyższa Szkoła Bankowa, Wrocław)
Studia podyplomowe z ochrony danych osobowych (Uniwersytet Łódzki)
Studia podyplomowe z zastosowań MS Excel w controllingu (Uniwersytet Ekonomiczny we Wrocławiu)
Data Scientist – Big Data (Akademia WSB w Dąbrowie Górniczej)
Ciągłe doskonalenie poprzez platformy Coursera, EdX, Domestika i inne

5 z 5

Jakub Tomaszewski

Magister inżynier, absolwent Politechniki Poznańskiej
Altkom Akademia S.A. (wrzesień 2022 – obecnie)
Stanowisko: Trener, ekspert ds. bezpieczeństwa IT
Obowiązki:
Prowadzenie autorskich i certyfikowanych szkoleń z zakresu:
Bezpieczeństwa IT, testów penetracyjnych, Red Team
Architektury bezpieczeństwa
Security Awareness i narzędzi ofensywnych
TANUKA Sp. z o.o. (marzec 2013 – obecnie)
Stanowisko: Prezes zarządu, Konsultant ds. bezpieczeństwa IT, Tester penetracyjny
Obowiązki:
Projektowanie, wdrażanie i utrzymywanie bezpiecznego środowiska
Realizacja testów penetracyjnych i konsultacje z zakresu bezpieczeństwa
Rozwój narzędzi i usług monitorujących bezpieczeństwo

(m.in. Security Hub)
Politechnika Wrocławska (luty 2021 – obecnie)
Stanowisko: Wykładowca, mentor
Prowadzone przedmioty:
Zaawansowane testy penetracyjne
Audyt i monitorowanie sieci
Usługi bezpiecznego Internetu
Testy penetracyjne
Hackers Squad Poznań (listopad 2021 – obecnie)
Stanowisko: Mentor, współzałożyciel
Organizacja pracy i mentoring zespołu technicznego Red Team
Allegro.pl Sp. z o.o. (wrzesień 2017 – czerwiec 2022)
Stanowisko: IT Infrastructure Security Team Leader / Offensive Security Lead
Obowiązki:
Kierowanie zespołem 6 specjalistów ds. bezpieczeństwa
Symulacje Red Team, testy penetracyjne, zarządzanie incydentami
Realizacja dużych projektów: SIEM, EDR, SoC, CIS Controls, Google Cloud Security

SANS SEC-660 – Advanced Penetration Testing, Exploit Writing
SANS SEC-760 – Advanced Exploit Development for Penetrat

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Materiały dydaktyczne zamieszczane są przez wykładowców w Wirtualnej Uczelni w formie prezentacji, materiałów PDF, zdjęć oraz linków.

Warunki uczestnictwa

Warunkiem uczestnictwa jest:

- **podsiadanie dyplomu ukończonych studiów wyższych I lub II stopnia.**
- zapisanie się na studia poprzez formularz rekrutacyjny **rekrutacja.cdv.pl** (UWAGA: wypełnienie samego formularza rekrutacyjnego nie jest równoznaczne z zapisaniem się na studia)
- podpisanie umowy online oraz załączenie skanu dyplomu ukończenia studiów wyższych (lic., inż., mgr)
- **przed zapisaniem się na studia podyplomowe proszę o kontakt telefoniczny/mailowy podyplomowe@cdv.pl tel. 697 230 138.**

Informacje dodatkowe

Przed zapisaniem się na studia podyplomowe proszę o kontakt telefoniczny/mailowy **podyplomowe@cdv.pl tel. 697 230 138**.

Zapraszam na stronę internetową https://cdv.pl/studia-podyplomowe/it/akademia-programowania-w-pythonie/ ,gdzie szczegółowo przedstawiamy KADRĘ, PARTNERÓW oraz PROGRAM.

Warunki techniczne

Zajęcia realizowane zdalnie, to usługi odbywające się z wykorzystaniem połączeń on-line, realizowane w czasie rzeczywistym, w formie umożliwiającej zrealizowanie opisanego zakresu usługi, jej celów i zadeklarowanych rezultatów. Zajęcia realizowane w formie zdalnej odbywają się przy użyciu platformy GOOGLE MEET, TEAMS, ZOOM, WEBEX. Link umożliwiającego uczestnictwo w spotkaniu on-line jest ważny tylko w trakcie zaplanowanych zajęć i przesyłany za pomocą wewnętrznego systemu (Wirtualna Uczelnia) do komunikacji pomiędzy Słuchaczem studiów podyplomowych, a Collegium Da Vinci.

Minimalne wymagania sprzętowe:

- Procesor dwurdzeniowy o prędkości 2GHz (i3/i5/i7 lub odpowiednik AMD)
- Pamięć RAM: 4GB (2GB w systemach 32bit)
- Dysk twardy: 0,5 GB wolnego miejsca na dysku
- Monitor/Ekran 14” o rozdzielczości HD – 720p (dla szkoleń komputerowych 2 ekrany)
- Peryferia: Głośniki, mikrofon lub zestaw słuchawkowy, kamera internetowa

Połączenie z Internetem: Stabilne łącze szerokopasmowe (stałe lub bezprzewodowe – LTE/4G

Wspierane systemy operacyjne:

- MS Windows: Windows 10, Windows 8.1, Windows 7, Windows Server 2019, Windows Server 2016
- MacOS: Jedna z trzech najnowszych wersji systemu MacOS
- Linux: Wszystkie popularnie i aktualne dystrybucji

Przeglądarka internetowa: Aktualne wersje przeglądarek Microsoft Edge, Safari, Chrome, Opera

Kontakt

Izabella Bekas-Kwaśniewska

E-mail izabella.bekas-kwasniewska@cdv.pl

Telefon (+48) 697 230 138