Możliwość dofinansowania

Security/Warsztaty z Cyberbezpieczeństwa (AI)

Numer usługi 2026/08/07/120967/3735062

2 214,00 PLN brutto
1 800,00 PLN netto
158,14 PLN brutto/h
128,57 PLN netto/h
261,33 PLN cena rynkowa

ALTKOM AKADEMIA SPÓŁKA AKCYJNA

4,4 / 5

2 719 ocen

Usługa szkoleniowa
zdalna w czasie rzeczywistym
Zajęcia grupowe
14:00 h
12.11.2026 do 13.11.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Usługa szkoleniowa adresowana jest do kadry zarządzającej, pracowników administracyjnych oraz użytkowników komputerów i innych urządzeń z dostępem do Internetu, którzy nie są specjalistami w zakresie bezpieczeństwa IT. Oczekiwane przygotowanie uczestnika: wymagana jest ogólna wiedza informatyczna z zakresu systemów operacyjnych i zagadnień sieciowych.
Minimalna liczba uczestników	6
Maksymalna liczba uczestników	12
Data zakończenia rekrutacji	28-10-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Podstawa uzyskania wpisu do BUR	Standard Usługi Szkoleniowo-Rozwojowej PIFS SUS 2.0

Cel

Cel edukacyjny

Szkolenie przygotowuje uczestnika do rozpoznawania zagrożeń w cyberprzestrzeni i stosowania zasad bezpiecznej pracy. Uczestnik identyfikuje cyberataki i socjotechniki, dobiera działania ochronne i reakcje na incydenty oraz rozpoznaje zagrożenia związane z wykorzystaniem AI, w tym phishing, fałszywe tożsamości, obraz, głos i dane.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
WIEDZA: Uczestnik szkolenia identyfikuje podstawowe zagadnienia cyberbezpieczeństwa i najważniejsze rodzaje cyberataków.	– Rozróżnia cyberbezpieczeństwo, ryzyko, incydent i politykę bezpieczeństwa.	Test teoretyczny
	– Rozpoznaje ataki socjotechniczne oraz ataki wykorzystujące e-mail, WWW, sieci bezprzewodowe i urządzenia mobilne.	Test teoretyczny
	– Identyfikuje phishing, smishing, spear-phishing, pharming, spoofing i inne techniki ataku.	Test teoretyczny
WIEDZA: Uczestnik szkolenia identyfikuje zagrożenia związane z wykorzystaniem AI oraz podstawowe zasady bezpiecznej pracy.	– Rozpoznaje zagrożenia związane z chatbotami, phishingiem AI i wyciekiem danych.	Test teoretyczny
	– Identyfikuje wykorzystanie AI do tworzenia fałszywych tożsamości, obrazu, głosu i danych.	Test teoretyczny
	– Wskazuje zasady dotyczące haseł, dostępu, kopii zapasowych i bezpiecznego korzystania z urządzeń.	Test teoretyczny
	– Rozpoznaje symptomy ataku socjotechnicznego.	Test teoretyczny
UMIEJĘTNOŚCI: Uczestnik szkolenia dobiera sposób reakcji i zabezpieczenia w przypadku zagrożenia cyberbezpieczeństwa.	– Dobiera właściwą reakcję na próbę cyberataku.	Test teoretyczny
	– Wskazuje działania ograniczające ryzyko związane z korzystaniem z poczty, przeglądarki i urządzeń mobilnych.	Test teoretyczny
UMIEJĘTNOŚCI: Uczestnik szkolenia stosuje zasady ochrony informacji i bezpiecznego korzystania z zasobów organizacji.	– Dobiera zasady tworzenia i zarządzania hasłami oraz dostępem.	Test teoretyczny
	– Wskazuje zasady bezpiecznej pracy z urządzeniami, dokumentami i nośnikami danych.	Test teoretyczny
	– Dobiera metody obrony i detekcji wobec zagrożeń związanych z AI.	Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
KOMPETENCJE SPOŁECZNE: Uczestnik szkolenia dostrzega znaczenie odpowiedzialnego korzystania z cyberprzestrzeni i popularyzowania zasad bezpieczeństwa w organizacji.	– Wskazuje znaczenie świadomego udostępniania informacji w sieci.	Test teoretyczny
	– Dostrzega odpowiedzialność pracownika za bezpieczeństwo informacji.	Test teoretyczny
	– Wskazuje znaczenie przekazywania wiedzy o cyberbezpieczeństwie innym pracownikom.	Test teoretyczny

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem zawierają opis efektów uczenia się?

TAK

Pytanie 2. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji i zgodnie z zaplanowanymi metodami walidacji?

TAK

Pytanie 3. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

TAK

Program

Adresaci szkolenia

Usługa szkoleniowa adresowana jest do kadry zarządzającej, pracowników administracyjnych oraz użytkowników komputerów i innych urządzeń z dostępem do Internetu, którzy nie są specjalistami w zakresie bezpieczeństwa IT.

Oczekiwane przygotowanie uczestnika: wymagana jest ogólna wiedza informatyczna z zakresu systemów operacyjnych i zagadnień sieciowych.

Warunki organizacyjne

- Szkolenie realizowane jest w formule **zdalnej w czasie rzeczywistym**, z wykorzystaniem platformy wideokonferencyjnej (Zoom).
- Grupa szkoleniowa liczy maksymalnie 12 uczestników, co pozwala na interaktywną pracę (zadania praktyczne, dyskusje) w komfortowych warunkach.
- W trakcie szkolenia uczestnicy wykonują samodzielnie ćwiczenia z możliwością konsultacji z trenerem.

- Każdy uczestnik powinien dysponować własnym stanowiskiem komputerowym z dostępem do Internetu – **dostawca usługi nie zapewnia sprzętu ani pomieszczenia do udziału w szkoleniu.**
- Materiały szkoleniowe (np. prezentacje, instrukcje do laboratoriów) są udostępniane w formie elektronicznej na dedykowanej platformie Altkom Akademii (dostęp wysyłany mailowo uczestnikom przed rozpoczęciem szkolenia).
- Efekty uczenia się zostaną zweryfikowane poprzez walidację w formie testu teoretycznego, ostatniego dnia usługi tj. testu jednokrotnego wyboru (link do testu zostanie udostępniony uczestnikom w formie mailowej).

Szkolenie obejmuje:

- 2 dni pracy z trenerem
- Nadzór trenera
- Kontakt ze społecznością
- Podręcznik w wersji elektronicznej
- Środowisko laboratoryjne

Liczba godzin usługi szkoleniowej

Szkolenie liczy łącznie: **14 godzin zegarowych.** Przerwy wliczają się do czasu trwania usługi. Trener ma możliwość przesunięcia przerw, tak aby dostosować harmonogram do potrzeb uczestników.

PROGRAM SZKOLENIA

1. Wstęp
   - Co to jest cyberbezpieczeństwo – definicja cyberprzestrzeni i cyberbezpieczeństwa, dlaczego to jest ważne
   - Ryzyko i zarządzanie ryzykiem – co to jest ryzyko, podstawowe pojęcia i zasady zarządzania ryzykiem
   - Polityka bezpieczeństwa – czym jest w organizacji polityka bezpieczeństwa i jaka jest jej rola
   - Incydenty bezpieczeństwa – co należy rozumieć jako incydent bezpieczeństwa i jak z nim postępować
   - Normy i standardy bezpieczeństwa – powszechnie stosowane rozwiązania, norma ISO27001
   - – AI Act – Normy dotyczące AI
   - NIS2 i DORA oraz ECSF/NICE

2. Ataki „na człowieka” tzw. SOCJOTECHNIKA (stosowane techniki manipulacji)
   - Ataki socjotechniczne – techniki manipulacji wykorzystywane przez cyberprzestępców
   - Sposoby – pod jakimi pretekstami wyłudza się firmowe dokumenty
   - Wykrywanie – jak rozpoznać, że jest się celem ataku socjotechnicznego
   - Reakcja – jak prawidłowo reagować na ataki socjotechniczne
   - Jak i skąd atakujący zbierają dane na twój temat
   - Miejsca, w których zostawiamy swoje dane świadomie i nieświadomie – jak świadomie udostępniać informacji w sieci

3. Atak „na komputery” – demonstracje wraz z objaśnieniem metod ochrony
   - Przegląd aktualnych ataków komputerowych wykorzystywanych przez cyberprzestępców, typowe błędy zabezpieczeń wykorzystywane przez atakujących
   - Ataki przez sieci bezprzewodowe (WiFi, Bluetooth, NFC)
   - Ataki przez pocztę e-mail (fałszywe e-maile)
   - Ataki przez strony WWW – jak nie dać się zainfekować, fałszywe strony
   - Ataki przez komunikatory (Skype, Facebook)
   - Ataki przez telefon (fałszywe SMS-y, przekierowania rozmów, itp.)
   - Ataki APT, phishing, smishing, spear-phishing, pharming, spoofing, spam, spim, scam

4. Dobre praktyki związane z bezpiecznym wykorzystaniem firmowych zasobów
   - Polityka haseł, zarządzanie dostępem i tożsamością – jakie hasło jest bezpieczne, jak nim zarządzać, zasady udzielania dostępu do zasobów informacyjnych
   - Bezpieczeństwo fizyczne – urządzenia, nośniki danych, dokumenty, „czyste biurko”
   - Bezpieczna praca z urządzeniami mobilnymi (smartfon, tablet, laptop)
   - Problem aktualnego oprogramowania i kopii zapasowych
   - Bezpieczna praca z pakietem biurowym Microsoft Office
   - Bezpieczna praca z programem pocztowym
   - Bezpieczna praca z przeglądarką internetową
   - Zastosowanie technik kryptograficznych (szyfrowanie, certyfikaty)

5. Aspekty prawne
   - Odpowiedzialność pracownika przed pracodawcą za ujawnienie informacji
   - Nieautoryzowane użycie systemów komputerowych
   - Rażące zaniedbania związane z wykorzystywaniem sprzętu komputerowego
   - Dane osobowe i dane wrażliwe

6. AI – Sztuczna inteligencja w służbie oszustów:
   - Definicja i pokaz praktyczny chatbotów (np. ChatGPT)
   - Wykorzystanie chatbotów do pomocy w codziennej pracy – pokaz praktyczny
   - Zagrożenia związane z chatbotami
   - Phishing związany z AI
   - Wyciek danych / hackowanie ChatGPT
   - Fałszywe tożsamości
   - Wykorzystanie AI do generowania wizerunku
   - Wykorzystanie AI do fałszowania obrazu
   - Wykorzystanie AI do podrabiania głosu
   - Generowanie fałszywych danych
   - Podsumowanie w formie konkretnych rad metod obrony i detekcji
7. Walidacja

Harmonogram

Liczba pozycji harmonogramu: 15

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 15 Wstęp: cyberbezpieczeństwo, ryzyko, polityka bezpieczeństwa, incydenty, ISO 27001, AI Act, NIS2, DORA oraz ECSF/NICE_wykład + warsztaty	Zajęcia	Dominik Węglarz	12-11-2026	09:00	10:30	01:30
2 z 15 -	Przerwa	-	12-11-2026	10:30	10:45	00:15
3 z 15 Socjotechnika: techniki manipulacji, wyłudzanie informacji, rozpoznawanie ataku, reakcja i świadome udostępnianie danych_wykład + warsztaty	Zajęcia	Dominik Węglarz	12-11-2026	10:45	12:30	01:45
4 z 15 -	Przerwa	-	12-11-2026	12:30	13:00	00:30

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
5 z 15 Ataki na komputery: WiFi, Bluetooth, NFC, e-mail, WWW, komunikatory, telefon, APT, phishing, smishing, pharming, spoofing i scam_wykład + warsztaty	Zajęcia	Dominik Węglarz	12-11-2026	13:00	14:30	01:30
6 z 15 -	Przerwa	-	12-11-2026	14:30	14:45	00:15
7 z 15 Dobre praktyki: hasła, dostęp i tożsamość, bezpieczeństwo fizyczne i mobilne, kopie zapasowe, Office, poczta, przeglądarka i kryptografia_ wykład + warsztaty	Zajęcia	Dominik Węglarz	12-11-2026	14:45	16:00	01:15
8 z 15 Aspekty prawne: odpowiedzialność pracownika, nieautoryzowane użycie systemów, zaniedbania, dane osobowe i dane wrażliwe_wykład + warsztaty	Zajęcia	Dominik Węglarz	13-11-2026	09:00	10:30	01:30
9 z 15 -	Przerwa	-	13-11-2026	10:30	10:45	00:15

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
10 z 15 AI w służbie oszustów: chatboty, zastosowanie w pracy, zagrożenia, phishing związany z AI oraz wyciek danych_wykład + warsztaty	Zajęcia	Dominik Węglarz	13-11-2026	10:45	12:30	01:45
11 z 15 -	Przerwa	-	13-11-2026	12:30	13:00	00:30
12 z 15 AI w służbie oszustów: fałszywe tożsamości, generowanie i fałszowanie obrazu i głosu oraz generowanie fałszywych danych_wykład + warsztaty	Zajęcia	Dominik Węglarz	13-11-2026	13:00	14:30	01:30
13 z 15 -	Przerwa	-	13-11-2026	14:30	14:45	00:15
14 z 15 Podsumowanie: konkretne rady dotyczące metod obrony i detekcji zagrożeń_wykład + warsztaty	Zajęcia	Dominik Węglarz	13-11-2026	14:45	15:30	00:45
15 z 15 -	Walidacja	-	13-11-2026	15:30	16:00	00:30

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	14:00
w tym suma godzin zajęć	11:30

Rodzaj godzin	Liczba godzin
w tym suma godzin walidacji	00:30
w tym suma przerw	02:00
Suma godzin dydaktycznych bez przerw	16:00

Cennik

Jeżeli korzystasz z dofinansowania i usługa stanowi usługę kształcenia zawodowego lub przekwalifikowania zawodowego wraz z usługą lub dostawą towarów ściśle związaną z usługami kształcenia zawodowego lub przekwalifikowania zawodowego to możesz mieć możliwość skorzystania za zwolnienia z podatku VAT na podstawie art. 43 ust. 1 pkt 29 lit. c ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług, jeśli usługa w całości jest finansowana ze środków publicznych lub § 3 ust. 1 pkt 14 rozporządzenia Ministra Finansów z dnia 20 grudnia 2013 r. w sprawie zwolnień od podatku od towarów i usług oraz warunków stosowania tych zwolnień w przypadku, gdy usługa jest finansowana w co najmniej 70% ze środków publicznych.

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	2 214,00 PLN
Koszt przypadający na 1 uczestnika netto	1 800,00 PLN
Koszt osobogodziny brutto	158,14 PLN
Koszt osobogodziny netto	128,57 PLN

Liczba godzin usługi

Rodzaj godzin	Liczba godzin
Liczba godzin zegarowych usługi	14:00

Prowadzący

Liczba prowadzących: 1

1 z 1

Dominik Węglarz

Ekspert z ponad 20-letnim doświadczeniem w branży IT, specjalizujący się w infrastrukturze IT, wirtualizacji oraz bezpieczeństwie systemowym i sieciowym. Absolwent Wydziału Matematyki i Informatyki UAM w Poznaniu, posiada liczne certyfikaty międzynarodowe m.in. CEH, ECIH, CompTIA Security+, CySA+, VCP oraz VCI. Laureat nagrody EC-Council Instructor Circle of Excellence dla Europy. Jako trener Altkom Akademii prowadzi autoryzowane szkolenia z technologii VMware oraz certyfikowanych szkoleń z zakresu cyberbezpieczeństwa (CEH, ECIH, CSCU). Realizuje również autorskie kursy dotyczące bezpieczeństwa IT, wirtualizacji, ochrony danych i świadomości cyberzagrożeń (cyber awareness). W ciągu ostatnich 5 lat przeprowadził dla Altkom Akademii ponad 30 szkoleń dla prawie 1700 uczestników.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Na platformie Wirtualna Klasa Altkom Akademii udostępnione zostaną bezterminowo materiały szkoleniowe (tj. np. podręczniki/prezentacje/materiały dydaktyczne niezbędne do odbycia szkolenia/ebooki itp.), zasoby bazy wiedzy portalu oraz dodatkowe informacje od trenera. Uczestnicy zachowują bezterminowy dostęp do zasobów Mojej Akademii i materiałów szkoleniowych zgromadzonych w Wirtualnej Klasie szkolenia. Platforma do kontaktu z trenerami, grupą i całą społecznością absolwentów jest portal Moja Akademia.

Usługa prowadzona jest z wykorzystaniem metod interaktywnych i aktywizujących, w szczególności: wykładu interaktywnego, moderowanej dyskusji, pytań i odpowiedzi, analizy przypadków (case study), ćwiczeń praktycznych i laboratoryjnych, samodzielnego wykonywania zadań w środowisku testowym oraz bieżących konsultacji z trenerem.

Warunki uczestnictwa

1. Niezbędnym warunkiem uczestnictwa w szkoleniach dofinansowanych z funduszy europejskich jest założenie konta w Bazie Usług Rozwojowych, zapis na szkolenie za pośrednictwem Bazy oraz spełnienie warunków przedstawionych przez danego Operatora, dysponenta funduszy publicznych.
2. Przez uczestnictwo w usłudze rozwojowej rozumie się aktywny udział Uczestnika w szkoleniu wyłącznie przy włączonej kamerze skierowanej na osobę uczestniczącą i umożliwiającej jej identyfikację.
3. Warunkiem uznania uczestnictwa w szkoleniu jest obecność podczas co najmniej 80% czasu trwania szkolenia (lub zgodnie z warunkami określonymi w umowie z Operatorem). Uczestnik, który nie spełni tego wymagania, traktowany jest jako nieobecny.
4. Frekwencja będzie potwierdzana na podstawie raportów logowań z platformy Zoom oraz bieżącej obserwacji uczestnika przez trenera.
5. Ogólne warunki uczestnictwa w szkoleniach Altkom Akademii zamieszczone są na stronie: https://www.altkomakademia.pl/ogolne-warunki-uczestnictwa-w-szkoleniach/

Informacje dodatkowe

Po szkoleniu uczestnik otrzyma zaświadczenie o ukończeniu szkolenia. Trener podczas szkolenia będzie organizował krótkie przerwy w porozumieniu z Uczestnikami, po zakończeniu danego modułu tematycznego.

Uwaga! W przypadku, gdy liczba zapisów na szkolenie nie osiągnie minimalnej liczby Uczestników, usługa może zostać niezrealizowana.

Informacja dot. podatku VAT:

Zwolnienie z podatku VAT może mieć zastosowanie wyłącznie w przypadku spełnienia przesłanek określonych w art. 43 ust. 1 pkt 29 lit. c ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług – w przypadku finansowania usługi w całości ze środków publicznych – albo w § 3 ust. 1 pkt 14 rozporządzenia Ministra Finansów w sprawie zwolnień od podatku od towarów i usług oraz warunków stosowania tych zwolnień – w przypadku finansowania usługi w co najmniej 70% ze środków publicznych. W przypadku zastosowania zwolnienia obowiązuje cena netto, a w pozostałych przypadkach doliczany jest VAT 23%.

Warunki techniczne

Szkolenie realizowane jest w formule **zdalnej, w czasie rzeczywistym)**, z wykorzystaniem platformy wideokonferencyjnej (Zoom).

Każdy uczestnik powinien dysponować własnym stanowiskiem komputerowym z dostępem do Internetu – **dostawca usługi nie zapewnia sprzętu ani pomieszczenia do udziału w szkoleniu uczestnikom.**

Wymagania ogólne realizacji szkolenia w formule distance learning (online):

Komputer stacjonarny lub notebook wyposażony w mikrofon, głośniki i kamerę internetową z przeglądarką internetową z obsługą HTML 5. Monitor o rozdzielczości FullHD. Szerokopasmowy dostęp do Internetu o przepustowości co najmniej 25/5 (download/upload) Mb/s. W przypadku szkoleń z laboratoriami zalecamy: sprzęt wyposażony w dwa ekrany o rozdzielczości minimum HD (lub dwa komputery), kamerę internetową USB, zewnętrzne głośniki lub słuchawki.

Dla zwiększenia komfortu pracy oraz efektywności szkolenia zalecamy skorzystanie z dodatkowego ekranu. Brak dodatkowego ekranu nie jest przeciwwskazaniem do udziału w szkoleniu, ale w znaczący sposób wpływa na komfort pracy podczas zajęć.

Informacje oraz wymagania dotyczące uczestniczenia w szkoleniach w formule zdalnej dostępne na: https://www.altkomakademia.pl/distance-learning/#FAQ

Platforma komunikacji – ZOOM

Oprogramowanie – zdalny pulpit, aplikacja ZOOM

Kody dostępowe do usługi, zgodnie z regulaminem, zostaną udostępnione w karcie usługi najpóźniej 1 dzień przed szkoleniem.

Link do szkolenia jest ważny w trakcie trwania całej usługi szkoleniowej.

Kontakt

AGNIESZKA SIPURA

E-mail agnieszka.sipura@altkom.pl
Telefon (+48) 609 191 281