



Europejska Agencja
Rozwoju Mirosław
Kopik

★★★★★ 5,0 / 5

3 796 ocen

AKADEMIA KSIĘGOWOŚCI 2. Praca, sprzedaż usług, bezpieczeństwo i obsługa klienta oraz niezbędna wiedza w księgowości - szkolenie

Numer usługi 2026/01/26/27209/3285255

📍 zdalna w czasie rzeczywistym

🏠 Usługa szkoleniowa

🕒 10 h

📅 01.04.2026 do 01.04.2026

2 320,00 PLN brutto

2 320,00 PLN netto

232,00 PLN brutto/h

232,00 PLN netto/h

Informacje podstawowe

Kategoria

Biznes / Sprzedaż

Grupa docelowa usługi

Właściciele firm, menadżerowie, specjaliści ds. księgowości, osoby planujące rozpocząć pracę w działach księgowości; osoby, które niedawno rozpoczęły pracę w księgowości; księgowi i samodzielni księgowi, pracownicy biur rachunkowych, osoby prowadzące podatkową KPiR lub współpracujące z podmiotami prowadzącymi KPiR, przedsiębiorcy oraz osoby odpowiedzialne za nadzór nad księgowością, osoby zajmujące się rozliczeniami finansowo-księgowymi w mikro, małych i średnich przedsiębiorstwach, osoby odpowiedzialne za obsługę klienta w podmiotach świadczących usługi księgowe, osoby wykonujące zadania związane ze sprzedażą usług księgowych oraz kontaktem z klientem; osoby, które chcą zgłębić i zaktualizować wiedzę z zakresu rozpoznawania cybernetycznych zagrożeń w sektorze księgowym; osoby, które chcą przekwalifikować się; osoby, które chcą doskonalić umiejętności zawodowe i społeczne, aby zapobiec utracie zatrudnienia; osoby poszukujące nowych możliwości zawodowych w obszarze księgowości.

Minimalna liczba uczestników

6

Maksymalna liczba uczestników

24

Data zakończenia rekrutacji

31-03-2026

Forma prowadzenia usługi

zdalna w czasie rzeczywistym

Liczba godzin usługi

10

Podstawa uzyskania wpisu do BUR

Standard Usługi Szkoleniowo-Rozwojowej PIFS SUS 2.0

Cel

Cel edukacyjny

Usługa przygotowuje do: rozpoznawania cybernetycznych zagrożeń w sektorze księgowym; stosowania zasad bezpiecznych transakcji online, bezpiecznego przeglądania księgowych zasobów Internetu, ochrony przed złośliwym oprogramowaniem i atakami poprzez przeglądarkę, unikania ataków phishingowych, do stosowania bezpiecznych płatności elektronicznych, ochrony danych klientów w handlu elektronicznym, świadomego zabezpieczania danych, stosowania praktycznych rozwiązań w pracy w biurze rachunkowym.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Rozpoznaje zagrożenia cybernetyczne w sektorze księgowości.	Opisuje zasady bezpiecznej transakcji online.	Test teoretyczny
	Definiuje zagrożenia cybernetyczne w sektorze księgowości.	Test teoretyczny
	Wybiera bezpieczne narzędzia i rozszerzenia do przeglądarki.	Test teoretyczny
	Opisuje bezpieczne sposoby przeglądania księgowych zasobów Internetu.	Test teoretyczny
Skutecznie chroni się przed złośliwym oprogramowaniem i atakami poprzez przeglądarkę.	Określa sposoby ochrony przed złośliwym oprogramowaniem i atakami phishingowymi.	Test teoretyczny
	Opisuje sposób weryfikacji tożsamości klienta.	Test teoretyczny
	Opisuje bezpieczne stosowanie płatności elektronicznych.	Test teoretyczny
Chroni dane klienta w obiegu elektronicznym	Opisuje sposoby ochrony danych klienta.	Test teoretyczny
Jest świadomy odpowiedzialności związanej z bezpieczeństwem danych finansowych i osobowych klientów.	Zachowuje bezpieczeństwo praktyk cyfrowych w pracy księgowego i biura rachunkowego.	Test teoretyczny
	Stosuje zasady ostrożności i rzetelności w pracy z systemami informatycznymi.	Test teoretyczny

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

Szkolenie adresowane jest do osób chcących lepiej wykorzystywać w swej pracy najnowszą wiedzę z zakresu księgowości, rozpoznawać zagrożenia cybernetyczne w sektorze księgowym; poznać i stosować zasady bezpiecznych transakcji online, bezpiecznego przeglądania księgowych zasobów Internetu, poznać i wykorzystywać sposoby ochrony przed złośliwym oprogramowaniem i atakami poprzez przeglądarkę, unikać ataków phishingowych, stosować bezpieczne płatności elektroniczne, skutecznie chronić dane klientów w handlu elektronicznym, stosować praktyczne rozwiązania z tego zakresu w pracy w biurze rachunkowym.

Usługa jest realizowana w godzinach dydaktycznych, przerwy w usłudze są wliczone w czas usługi.

Szkolenie prowadzone jest w grupie od 6 do 24 osób, a warunki organizacyjne są zawsze dostosowywane do liczby osób na szkoleniu. Podczas szkolenia odbywa się zarówno praca zbiorowa (np. mini-wykład), jak i praca indywidualna (np. ćwiczenia indywidualne), w zależności od potrzeb.

Na szkoleniu część teoretyczna zajmuje około 20-25% czasu szkolenia, część praktyczna to 75-80% czasu szkolenia. W przypadku szkolenia realizowanego podczas 10 godzin dydaktycznych, około 2 godzin dydaktycznych to część teoretyczna, pozostały czas to zajęcia praktyczne.

W trakcie usługi rozwojowej prowadzona jest weryfikacja postępów z wykorzystaniem testów, quizów. Zadania zawsze są omawiane i podsumowywane albo indywidualnie, albo grupowo.

Walidacja jest prowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria weryfikacji. Zapewniona jest rozdzielnosc procesów kształcenia i walidacji. Metoda walidacji to test porównawczy (pre i post test).

Przywitanie, kontrakt z uczestnikami. Pre-test.

Moduł 1. Wprowadzenie do Cyberbezpieczeństwa w finansach. Definicja cyberbezpieczeństwa i jego kluczowe znaczenie dla sektora finansowego. Bezpieczne zarządzanie hasłami i Dostępem w biurze rachunkowym. Zarządzanie Ryzykiem Cyberbezpieczeństwa w Dziale Księgowości. Zarządzanie Incydentami Cyberbezpieczeństwa.

Metody pracy: Wykład. Prezentacja multimedialna. Wyjaśnianie.

Moduł 2. Tożsamość Cyfrowa. Znaczenie tożsamości cyfrowej dla sektora finansowego i handlowego. Strategie monitorowania aktywności w sieci w kontekście zapewniania bezpieczeństwa finansowego. Narzędzia i strategie zapewniające prywatność i bezpieczeństwo podczas korzystania z Internetu w sektorze finansowym. Praktyczne wskazówki dotyczące bezpiecznego surfowania w sieci w kontekście działań finansowych.

Metody pracy: Wykład interaktywny. Prezentacja multimedialna.

Moduł 3. Incydenty związane z cyberbezpieczeństwem w dziale księgowości i finansach - przykłady. Phishing, Vishing, socjotechnika. Ransomware. Studium przypadków związanych z phishingiem w biurze rachunkowym. Praktyczne wskazówki dotyczące identyfikacji i unikania zagrożeń phishingowych.

Metody pracy: Wykład. Prezentacja multimedialna. Wyjaśnianie.

Moduł 4. Bezpieczeństwo danych finansowych. Kopie zapasowe. Znaczenie regularnych kopii bezpieczeństwa danych finansowych dla zapewnienia ciągłości działania. Strategie tworzenia, przechowywania i przywracania kopii zapasowych danych księgowych. Techniki automatyzacji procesów tworzenia kopii zapasowych w celu zminimalizowania ryzyka utraty danych.

Metody pracy: Wykład. Prezentacja multimedialna. Wyjaśnianie.

Zakończenie i ewaluacja szkolenia. Post-test.

Harmonogram

Liczba przedmiotów/zajęć: 9

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 9 Przywitanie kontrakt z uczestnikami. Pre-test.	-	01-04-2026	07:15	07:35	00:20
2 z 9 Moduł 1.	Dawid Koziorowski	01-04-2026	07:35	09:05	01:30
3 z 9 Przerwa	Dawid Koziorowski	01-04-2026	09:05	09:20	00:15
4 z 9 Moduł 2.	Dawid Koziorowski	01-04-2026	09:20	10:50	01:30
5 z 9 Przerwa	Dawid Koziorowski	01-04-2026	10:50	11:05	00:15
6 z 9 Moduł 3.	Dawid Koziorowski	01-04-2026	11:05	12:35	01:30
7 z 9 Przerwa obiadowa	Dawid Koziorowski	01-04-2026	12:35	13:05	00:30
8 z 9 Moduł 4.	Dawid Koziorowski	01-04-2026	13:05	14:35	01:30
9 z 9 Podsumowanie i ewaluacja. Post-test.	-	01-04-2026	14:35	14:45	00:10

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	2 320,00 PLN
Koszt przypadający na 1 uczestnika netto	2 320,00 PLN
Koszt osobogodziny brutto	232,00 PLN
Koszt osobogodziny netto	232,00 PLN

Prowadzący

Liczba prowadzących: 1



1 z 1

Dawid Koziorowski

Trener IT z ponad 10 letnim doświadczeniem, certyfikowany „etyczny haker” oraz instruktor EC-COUNCIL. Na co dzień zajmuje się realizacją testów penetracyjnych symulujących realne ataki hakerskie na infrastrukturę sieciowe oraz aplikacje webowe. Specjalizuje się w socjotechnice oraz działaniach typu Red Team. Jako trener realizował szkolenia z zakresu cyberbezpieczeństwa m.in. dla specjalnych (CBZC, ABW, CBA), oraz dla administracji (m.in. Krajowa Izba Skarbowa). Obszar specjalizacji: Cyberbezpieczeństwo, Osint (Biały wywiad), inżynieria społeczna, Phishing, Hacking. Założyciel i właściciel Akademii Portal – Centrum Szkoleń IT.

Wykształcenie: wyższe informatyczne, specjalizacja: Cyberbezpieczeństwo i Informatyka Śledcza

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Uczestnik szkolenia otrzyma autorskie materiały szkoleniowe (prezentacja multimedialna, skrypt itp.) drogą mailową.

Warunki uczestnictwa

Osoba zainteresowana skorzystaniem z usługi rozwojowej z dofinansowaniem musi zarejestrować się w Bazie Usług Rozwojowych oraz dokonać zapisu na usługę przed jej rozpoczęciem, z użyciem numeru ID wsparcia.

Każdy uczestnik szkolenia otrzyma link aktywacyjny do platformy szkoleniowej, aktywacja umożliwi uczestnictwo w szkoleniu.

Podczas logowania się do platformy (system prosi tylko o podanie: imienia, e-maila i hasła) w celu jednoznacznego zidentyfikowania uczestnika szkolenia wymagane jest **podanie imienia i nazwiska uczestnika**.

Lista obecności na szkoleniu będzie sporządzona na podstawie pisemnych potwierdzeń uczestników szkolenia o ich uczestnictwie w szkoleniu oraz dodatkowo na podstawie potwierdzenia obecności na czacie.

Informacje dodatkowe

Czas trwania usługi szkoleniowej to 10 godzin dydaktycznych (1 godzina dydaktyczna= 45 minut). Szkolenie jest jednodniowe, ujęte w 4 moduły. Planujemy przerwy pomiędzy modułami.

Usługa jest zwolniona z podatku VAT w przypadku, kiedy przedsiębiorstwo zwolnione jest z podatku VAT lub dofinansowanie wynosi co najmniej 70%. W innej sytuacji do ceny netto doliczany jest podatek VAT w wysokości 23%.

Podstawa: §3 ust. 1 pkt. 14 rozporządzenia Ministra Finansów z dnia 20.12.2013 r. w sprawie zwolnień od podatku od towarów i usług oraz szczegółowych warunków stosowania tych zwolnień (Dz.U. z 2018 r., poz. 701).

Warunki techniczne

Szkolenia odbywają się na platformie ClickMeeting w formie Webinaru.

Warunki techniczne niezbędne do udziału w usłudze:

Każdy komputer używany na co dzień będzie wystarczający do uczestnictwa w usłudze rozwojowej. Rekomendujemy udział w szkoleniu za pośrednictwem komputera. Tablet a zwłaszcza smartfon może być mniej praktyczny ze względu na wielkość ekranu.

1. Komputer/laptop – najlepiej, procesor Intel Core od i3 w górę, zalecane 4 GB RAM lub więcej, tablet 3 GB RAM lub smartfon.
2. Stałe łącze internetowe w dowolnej technologii – światłowod, GSM 3G lub 4G/LTE, Internet kablowy, zalecane min. 3 Mb/s w zakresie pobierania i wysyłania danych.
3. W miarę możliwości najnowszy system operacyjny: Windows 10 lub 8, 7, Vista z SP1; macOS X z macOS 10.7 lub nowszy, iOS 10 lub nowszy lub dedykowana aplikacja mobilna z AppStore lub GooglePlay, Android w wersji 4.0.4 lub nowszy w przypadku tabletów lub inne systemy operacyjne dające pewność odbioru transmisji bez zakłóceń.
4. Dowlolna przeglądarka internetowa (zalecana Chrome lub Mozilla FireFox).
5. Głośniki lub słuchawki.

W trakcie szkolenia dostęp do wizji i dźwięku mają tylko trenerzy, uczestnicy szkolenia mogą komunikować się jedynie za pomocą czatu. Link umożliwiający uczestnictwo w spotkaniu on-line ważny jest tylko w dniu szkolenia. Do każdego szkolenia przypisany jest oddzielny link. Nad sprawnym przebiegiem szkolenia będzie czuwać trener organizacyjny.

Kontakt



Mirosław Kopik

E-mail mirek.kopik@eurodotacje.pl

Telefon (+48) 505 060 800