Możliwość dofinansowania

Cyberbezpieczeństwo dla działów finansowo-księgowych - szkolenie zdalne w czasie rzeczywistym

Numer usługi 2026/06/26/47095/3653067

1 722,00 PLN brutto
1 400,00 PLN netto
287,00 PLN brutto/h
233,33 PLN netto/h
157,33 PLN cena rynkowa

ADN AKADEMIA spółka z ograniczoną odpowiedzialnością spółka komandytowa

4,6 / 5

387 ocen

Usługa szkoleniowa
zdalna w czasie rzeczywistym
Zajęcia grupowe
06:00 h
03.09.2026 do 03.09.2026

Informacje podstawowe

Kategoria	Finanse i bankowość / Rachunkowość/księgowość
Grupa docelowa usługi	Szkolenie skierowane jest do osób odpowiedzialnych za przetwarzanie danych finansowych, księgowych i kadrowych oraz wszystkich pracowników mających dostęp do informacji poufnych w organizacji. Adresowane jest w szczególności do pracowników działów finansowo-księgowych, głównych i samodzielnych księgowych, pracowników biur rachunkowych, specjalistów ds. kadr i płac, controllerów finansowych, dyrektorów finansowych, kierowników działów finansowo-księgowych, właścicieli i pracowników MŚP oraz osób zainteresowanych podniesieniem kompetencji w zakresie cyberbezpieczeństwa. Od uczestników wymagana jest podstawowa umiejętność obsługi komputera. Nie jest wymagana specjalistyczna wiedza z zakresu cyberbezpieczeństwa.
Minimalna liczba uczestników	7
Maksymalna liczba uczestników	30
Data zakończenia rekrutacji	02-09-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Podstawa uzyskania wpisu do BUR	Certyfikat VCC Akademia Edukacyjna

Cel

Cel edukacyjny

Celem szkolenia jest rozwój kompetencji uczestników w zakresie rozpoznawania zagrożeń cyberbezpieczeństwa oraz stosowania zasad ochrony danych i informacji w pracy działów finansowo-księgowych. Uczestnicy zdobędą wiedzę o aktualnych zagrożeniach, nauczą się identyfikować próby cyberataków, właściwie reagować na incydenty oraz stosować dobre praktyki zwiększające bezpieczeństwo danych finansowych i osobowych.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Po zakończeniu usługi uczestnik: wyjaśnia podstawowe pojęcia związane z cyberbezpieczeństwem i bezpieczeństwem informacji; charakteryzuje najczęściej występujące zagrożenia cybernetyczne dotyczące działów finansowo-księgowych; opisuje zasady ochrony danych finansowych i danych osobowych oraz podstawowe wymagania wynikające z przepisów prawa; rozpoznaje znaczenie procedur bezpieczeństwa i współpracy z działem IT w ograniczaniu ryzyka cyberzagrożeń.	Uczestnik: rozróżnia rodzaje cyberzagrożeń; wskazuje sposoby ochrony danych i systemów; omawia podstawowe zasady cyberhigieny; identyfikuje obowiązki pracownika w zakresie bezpieczeństwa informacji.	Test teoretyczny z wynikiem generowanym automatycznie
Po zakończeniu usługi uczestnik: identyfikuje podejrzane wiadomości e-mail, próby phishingu oraz inne formy socjotechniki; stosuje zasady bezpiecznej pracy z pocztą elektroniczną, urządzeniami oraz danymi finansowymi; wykorzystuje dobre praktyki dotyczące tworzenia haseł, uwierzytelniania wieloskładnikowego oraz ochrony dostępu do danych; dobiera właściwy sposób postępowania w przypadku wykrycia incydentu bezpieczeństwa;	Uczestnik: prawidłowo rozpoznaje przykłady prób phishingu; wskazuje właściwe działania ograniczające ryzyko cyberataku; dobiera odpowiednie procedury postępowania dla przedstawionych sytuacji; poprawnie analizuje studia przypadków dotyczące bezpieczeństwa informacji.	Test teoretyczny z wynikiem generowanym automatycznie

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Po zakończeniu usługi uczestnik: odpowiedzialnie stosuje zasady bezpieczeństwa informacji podczas wykonywania obowiązków zawodowych; dostrzega znaczenie przestrzegania procedur bezpieczeństwa dla ochrony organizacji; współpracuje z innymi pracownikami oraz działem IT podczas reagowania na incydenty bezpieczeństwa; wykazuje gotowość do systematycznego aktualizowania wiedzy z zakresu cyberbezpieczeństwa.	Uczestnik: aktywnie uczestniczy w analizie przypadków; proponuje właściwe działania zwiększające bezpieczeństwo informacji; uzasadnia wybór sposobu postępowania w sytuacjach zagrożenia.	Test teoretyczny z wynikiem generowanym automatycznie

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

1. Wprowadzenie do cyberbezpieczeństwa

• Definicja cyberbezpieczeństwa i bezpieczeństwa informacji

• Znaczenie ochrony danych finansowych i księgowych w organizacji

• Przegląd aktualnych zagrożeń cyfrowych dla sektora finansowo-księgowego

2. Typowe zagrożenia i ataki w finansach i księgowości

• Phishing, spearphishing, malware, ransomware – mechanizmy i przykłady

• Ataki socjotechniczne i manipulacje pracownikami

• Wycieki danych, kradzież tożsamości i wyłudzenia finansowe

• Przykłady incydentów z branży finansowej

3. Bezpieczeństwo pracy na komputerze i urządzeniach mobilnych

• Zasady cyberhigieny w codziennej pracy

• Bezpieczne korzystanie ze sprzętu służbowego i prywatnego

• Ochrona urządzeń mobilnych (smartfony, laptopy, tablety)

• Zabezpieczenie sieci bezprzewodowych (Wi-Fi, VPN)

4. Ochrona danych finansowych i osobowych

• Podstawy RODO i wymogi prawne dotyczące ochrony danych w księgowości

• Klasyfikacja i inwentaryzacja zasobów informacyjnych

• Zarządzanie dostępem do danych finansowych i kadrowych

• Szyfrowanie danych i bezpieczne przechowywanie informacji

5. Bezpieczeństwo poczty elektronicznej i komunikacji

• Rozpoznawanie podejrzanych wiadomości i załączników

• Zasady bezpiecznego korzystania z poczty elektronicznej

• Ochrona przed spamem, scamem i atakami phishingowymi

6. Zarządzanie hasłami i uwierzytelnianie

• Tworzenie i przechowywanie silnych haseł

• Uwierzytelnianie dwuskładnikowe (2FA)

• Narzędzia do zarządzania hasłami (password manager)

7. Kopie zapasowe i odzyskiwanie danych

• Znaczenie regularnych kopii zapasowych w działach finansowych

• Praktyczne zasady tworzenia i przechowywania backupów

• Procedury odzyskiwania danych po incydencie

8. Reagowanie na incydenty bezpieczeństwa

• Rozpoznawanie symptomów ataku lub naruszenia bezpieczeństwa

• Procedury zgłaszania i obsługi incydentów

• Współpraca z działem IT i zarządzanie kryzysowe

9. Dobre praktyki i polityki bezpieczeństwa w organizacji

• Tworzenie i wdrażanie polityk bezpieczeństwa informacji

• Szkolenia okresowe i podnoszenie świadomości pracowników

• Odpowiedzialność pracowników za powierzone zasoby

10. Praktyczne ćwiczenia i analiza przypadków

• Symulacje ataków phishingowych i analiza reakcji

• Studium przypadków z branży finansowej

• Warsztaty z zakresu identyfikacji i reagowania na zagrożenia

Harmonogram

Liczba pozycji harmonogramu: 10

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 10 Moduł 1. Wprowadzenie do cyberbezpieczeństwa	Zajęcia	Michał Horubała	03-09-2026	10:00	11:00	01:00
2 z 10 -	Przerwa	-	03-09-2026	11:00	11:10	00:10
3 z 10 Moduł 2. Typowe zagrożenia i ataki w finansach i księgowości	Zajęcia	Michał Horubała	03-09-2026	11:10	12:00	00:50
4 z 10 -	Przerwa	-	03-09-2026	12:00	12:10	00:10
5 z 10 Moduły 3–4. Bezpieczeństwo pracy na komputerze i urządzeniach mobilnych oraz ochrona danych finansowych i osobowych	Zajęcia	Michał Horubała	03-09-2026	12:10	13:00	00:50
6 z 10 -	Przerwa	-	03-09-2026	13:00	13:30	00:30
7 z 10 Moduły 5–6. Bezpieczeństwo poczty elektronicznej oraz zarządzanie hasłami i uwierzytelnianie	Zajęcia	Michał Horubała	03-09-2026	13:30	14:20	00:50

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
8 z 10 -	Przerwa	-	03-09-2026	14:20	14:30	00:10
9 z 10 Moduły 7–10. Kopie zapasowe i odzyskiwanie danych, reagowanie na incydenty bezpieczeństwa, dobre praktyki bezpieczeństwa oraz ćwiczenia praktyczne i analiza przypadków	Zajęcia	Michał Horubała	03-09-2026	14:30	15:45	01:15
10 z 10 -	Walidacja	Michał Horubała	03-09-2026	15:45	16:00	00:15

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	06:00
w tym suma godzin zajęć	04:45
w tym suma godzin walidacji	00:15
w tym suma przerw	01:00
Suma godzin dydaktycznych bez przerw	06:30

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 2024 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	1 722,00 PLN
Koszt przypadający na 1 uczestnika netto	1 400,00 PLN
Koszt osobogodziny brutto	287,00 PLN
Koszt osobogodziny netto	233,33 PLN

Liczba godzin usługi

Rodzaj godzin	Liczba godzin
Liczba godzin zegarowych usługi	06:00

Prowadzący

Liczba prowadzących: 1

1 z 1

Michał Horubała

.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Autorskie materiały szkoleniowe w formie elektronicznej zostaną udostępnione dzień przed terminem szkolenia

Informacje dodatkowe

- wygodna forma szkolenia - wystarczy dostęp do urządzenia z Internetem
- bierzesz udział w pełnowartościowym szkoleniu zajęcia prowadzone "na żywo"
- podczas szkolenia możesz zadawać pytania, na które dostajesz odpowiedź w czasie rzeczywistym
- otrzymujesz certyfikat wydany przez jedną z wiodących firm szkoleniowych w Polsce, uhonorowanej prestiżową nagrodą Plebiscytu Orły Polskiej Przedsiębiorczości jako Firma 20-lecia
- otrzymujesz bezpłatny dostęp do platformy szkoleniowej przez 6mcy od rozpoczęcia szkolenia

Warunki techniczne

Warunkiem uczestnictwa jest posiadanie przez uczestnika minimalnych narzędzi sprzętowych i niezbędnych warunków technicznych do udziału w usłudze. Uczestnik zainteresowany skorzystaniem z usługi z dofinansowaniem musi dokonać zapisu na usługę co najmniej 2 dni przed jej rozpoczęciem, z użyciem numeru ID wsparcia. Lista Uczestników zostanie zamknięta przez Usługodawcę na 2 dni przed rozpoczęciem usługi. Uczestnicy, którzy ukończą usługę otrzymają zaświadczenie o zakończeniu udziału w usłudze w formie elektronicznej. Warunki techniczne niezbędne do udziału w usłudze: •platforma komunikacyjna – MS Teams. •wymogi sprzętowe: komputer stacjonarny lub laptop, kamera wbudowana lub na USB, mikrofon, słuchawki lub głośniki, •system operacyjny minimum Windows XP/MacOS High Sierra, min 2 GB pamięci RAM, pamięć dysku minimum 10GB, łącze internetowe minimum 10 kb/s,•link z zaproszeniem na szkolenie zostanie przesłany drogą e-mail na 2 dni przed szkoleniem, •dołączenie do szkolenia na platformie MS Teams

Kontakt

Magdalena Czapska

E-mail magdalena.czapska@adnakademia.pl

Telefon (+48) 222 082 826