Możliwość dofinansowania

Księgowość, kadry i finanse w dobie cyberprzestępstw – kurs online

Numer usługi 2025/12/22/43371/3225993

3 062,70 PLN brutto
2 490,00 PLN netto
145,84 PLN brutto/h
118,57 PLN netto/h

Wektor Wiedzy Sp. z o.o.

4,5 / 5

3 719 ocen

Usługa szkoleniowa
zdalna w czasie rzeczywistym
21:00 h
03.09.2026 do 23.09.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	**Na kurs zapraszamy w szczególności:** • księgowych, • specjalistów ds. kadr i płac, • analityków finansowych, • osoby zarządzające firmą, • wszystkich, którzy w swojej codziennej pracy wykorzystują systemy komputerowe i zarządzają danymi.
Minimalna liczba uczestników	15
Maksymalna liczba uczestników	20
Data zakończenia rekrutacji	31-08-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	21
Podstawa uzyskania wpisu do BUR	Certyfikat systemu zarządzania jakością wg. ISO 9001:2015 (PN-EN ISO 9001:2015) - w zakresie usług szkoleniowych

Cel

Cel edukacyjny

Kurs przygotowuje do samodzielnego zarządzania ryzykiem związanym z cyberprzestępczością w obszarze księgowości, kadr i finansów poprzez praktyczne opanowanie metod identyfikacji potencjalnych zagrożeń, wdrażania

strategii zabezpieczających dane finansowe i kadrowe oraz skutecznego reagowania na incydenty związane z bezpieczeństwem informacji.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik definiuje podstawowe pojęcia z zakresu cyberbezpieczeństwa i identyfikuje najczęstsze zagrożenia cyfrowe	rozpoznaje pojęcia takie jak cyberprzestępczość, phishing oraz ransomware na podstawie definicji zawartych w pytaniach testowych	Test teoretyczny z wynikiem generowanym automatycznie
	wskazuje najczęściej występujące typy cyberataków w środowisku pracy biurowej i zdalnej	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik charakteryzuje zasady tworzenia i zarządzania bezpiecznymi hasłami	identyfikuje cechy bezpiecznego hasła, w tym długość, złożoność oraz unikalność	Test teoretyczny z wynikiem generowanym automatycznie
	wskazuje prawidłowe praktyki dotyczące zmiany, niepowtarzalności oraz przechowywania haseł	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik stosuje zasady bezpiecznej pracy zdalnej i ochrony danych firmowych	rozróżnia bezpieczne i niebezpieczne praktyki pracy zdalnej, w tym korzystanie z VPN oraz aktualizacji systemowych	Test teoretyczny z wynikiem generowanym automatycznie
	wskazuje działania minimalizujące ryzyko naruszenia bezpieczeństwa danych podczas pracy poza siedzibą organizacji	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik rozpoznaje zagrożenia wynikające z instalowania i użytkowania oprogramowania	identyfikuje bezpieczne źródła pobierania oprogramowania na podstawie opisanych sytuacji testowych	Test teoretyczny z wynikiem generowanym automatycznie
	wskazuje działania, których należy unikać w celu ograniczenia ryzyka instalacji złośliwego oprogramowania	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik wyjaśnia znaczenie procedur i narzędzi organizacyjnych w zapewnianiu bezpieczeństwa informacji	rozpoznaje rolę polityk bezpieczeństwa oraz ich wpływ na ograniczenie liczby incydentów cyberbezpieczeństwa	Test teoretyczny z wynikiem generowanym automatycznie
	identyfikuje narzędzia służące do monitorowania incydentów bezpieczeństwa, w tym systemy klasy SIEM	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

Temat 1 – Zagrożenia, ataki i incydenty cyberbezpieczeństwa w branży finansowo-kadrowej.

1. Podstawy cyberbezpieczeństwa.

• Czy w świecie cyfrowym jest bezpiecznie?

• Podstawowe narzędzia cyberbezpieczeństwa.

• Aktualność problemu bezpieczeństwa teleinformatycznego – socjotechnika

i manipulacje przestępców.

• Z czego składa się system cyberbezpieczeństwa?

• Powszechność zagrożeń.

• Co ryzykujemy zaniedbując cyberbezpieczeństwo?

2. Ataki „na człowieka” tzw. SOCJOTECHNIKA (stosowane techniki manipulacji).

• Czym jest socjotechnika?

• Dlaczego człowiek jest najsłabszym ogniwem?

• Przykłady podstępów socjotechnicznych – wyłudzenia dokumentów, loginów, haseł.

• Jak i skąd atakujący zbierają dane na twój temat?

• Miejsca, w których zostawiamy swoje dane świadomie i nieświadomie - jak świadomie udostępniać informacje w sieci?

3. Klasyfikacja zagrożeń dla sieci teleinformatycznej i ich źródeł - system i jego podatność.

• Antywirus i firewall.

• Niebezpieczeństwo ataków na firmę/instytucję.

• Co zrobić, gdy zidentyfikujemy atak?

• Podatność systemu.

• Sposoby atakowania sieci, rodzaje włamań sieciowych.

• Niebezpieczny system.

• Niebezpieczne aplikacje i źródła.

• Podatność na ataki w związku z przelewami i bankowością.

4. Monitorowanie incydentów bezpieczeństwa teleinformatycznego.

• Zbieranie danych, diagnozowanie incydentów, podejmowanie działań naprawczych.

Temat 2 – Jak się nie dać zaskoczyć cyberzagrożeniom?

1. Mechanizmy i programy ochrony przed zagrożeniami cyberbezpieczeństwa.

• Jakie emocje wykorzystują oszuści w wyłudzeniach danych i finansów?

• Keyloggery – jak działają, jak się bronić?

• Malware i Spyware.

• Zagrożenia i zabezpieczenia laptopów i dysków.

• VPN – co to i kiedy korzystać?

2. (Nie)bezpieczne płatności.

• Płatności niebezpieczne.

• Płatności bezpieczne.

• Płatności przez portale.

• Kto prosi mnie o płatność.

3. Fałszywi konsultanci.

• Jak przeprowadzane są ataki telefoniczne?

• Fałszywe załączniki.

• Fałszywe smsy.

4. Bezpieczne hasła i logowanie.

• Skuteczne organizowanie i zabezpieczanie haseł.

• Uwierzytelnianie dwuskładnikowe.

• Wrażliwe dostępy o które należy zadbać.

• Jak pracować z pocztą elektroniczną?

5. Metody i środki bezpieczeństwa – w branży finansowej.

• Bezpieczeństwo fizyczne.

• Kopie zapasowe i redundantność.

• Ochrona Danych Osobowych i zagrożenia.

• Kontrola dostępu.

• Zasady ochrony urządzeń mobilnych.

• Polityka stosowania rozwiązań kryptograficznych i szyfrowanie informacji -

przedsięwzięcia organizacyjne.

• Zarządzanie uprawnieniami użytkowników systemów informatycznych, kontrola dostępu.

6. 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.

Temat 3 – Jak zorganizować cyberbezpieczeństwo w kadrach i księgowości?

1. Cyberprzestępczość - najpowszechniejsze rodzaje ataków i zagrożeń – praktyczne case study przypadków.

• Phishing i inne odmiany ataków socjotechnicznych.

• Pozostałe zagrożenia dla bezpieczeństwa sieci teleinformatycznej.

• Cracking.

• Sniffing.

• Metoda salami.

• Fałszywe powiadomienia z mediów społecznościowych.

• Oszustwo na „nigeryjskiego księcia”.

• Skimming.

2. Organizacja bezpiecznej sieci teleinformatycznej i bezpieczeństwa informacji – rozwiązania systemowe i wymagania prawne w Polsce.

• Rozporządzenie DORA: Wymagania dla instytucji finansowych.

• Norma ISO 27001:2017 i ISO 27002:2022.

• Rozporządzenie o Ochronie Danych Osobowych (RODO).

• Kary i odpowiedzialność za cyberprzestępstwa.

• Prawa ofiar cyberataków.

3. 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”.

• Bezpieczeństwo danych osobowych kadrowych.

• 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).

4. Edukacja i Budowanie świadomości.

• Budowanie kultury cyberbezpieczeństwa w organizacji.

• Edukacja użytkowników końcowych: praktyczne porady.

• Dobre praktyki w korzystaniu z firmowych zasobów.

• Organizacja bezpiecznego środowiska pracy: polityka czystego biurka, zarządzanie hasłami.

• Praktyczne ćwiczenia i quizy w celu utrwalenia wiedzy.

5.Test walidacyjny

Link to testu online zostanie wysłany po zakończonych zajęciach. Test przygotowała osoba prowadząca walidację niniejszego kursu. Test zawiera pytania do których należy wybrać jedną odpowiedź spośród trzech propozycji. Wynik testu jest automatycznie wyliczany w pliku google.

Po uzyskaniu wyniku pozytywnego, Uczestnik otrzyma zaświadczenie o ukończeniu kursu.

Usługa jest realizowana w godzinach dydaktycznych 45 minut. Każdego dnia zaplanowano przerwy: 10:30-10:45, a później 12:30-13:00.

Przerwy nie wliczają się w liczbę godzin usługi (7 x 45 minut dydaktycznych + 45 minut przerwy).

Każdy temat realizowany jest w trybie 2 godziny zajęć teoretycznych i 5 godzin zajęć praktycznych.

Na kurs zapraszamy w szczególności:

- księgowych,
- specjalistów ds. kadr i płac,
- analityków finansowych,
- osoby zarządzające firmą,
- wszystkich, którzy w swojej codziennej pracy wykorzystują systemy komputerowe i zarządzają danymi.

Kurs przeprowadzany będzie w formie online, bez podziału na grupy. Uczestnicy mają możliwość korzystania zarówno z kamerki jak i mikrofonu. Taką chęć mogą zgłaszać na bieżąco poprzez kliknięcie ikonki „dłoń". Pytania można również zadawać za pomocą czatu.

Harmonogram

Liczba pozycji harmonogramu: 16

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 16 Zagrożenia, ataki i incydenty cyberbezpieczeństwa w branży finansowo kadrowej.	Daniel Lampart	03-09-2026	09:00	10:30	01:30
2 z 16 Przerwa	Daniel Lampart	03-09-2026	10:30	10:45	00:15

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
3 z 16 Zagrożenia, ataki i incydenty cyberbezpieczeństwa w branży finansowo kadrowej.	Daniel Lampart	03-09-2026	10:45	12:30	01:45
4 z 16 Przerwa	Daniel Lampart	03-09-2026	12:30	13:00	00:30
5 z 16 Zagrożenia, ataki i incydenty cyberbezpieczeństwa w branży finansowo kadrowej.	Daniel Lampart	03-09-2026	13:00	15:00	02:00
6 z 16 Jak się nie dać zaskoczyć cyberzagrożeniom?	Daniel Lampart	17-09-2026	09:00	10:30	01:30
7 z 16 Przerwa	Daniel Lampart	17-09-2026	10:30	10:45	00:15
8 z 16 Jak się nie dać zaskoczyć cyberzagrożeniom?	Daniel Lampart	17-09-2026	10:45	12:30	01:45
9 z 16 Przerwa	Daniel Lampart	17-09-2026	12:30	13:00	00:30
10 z 16 Jak się nie dać zaskoczyć cyberzagrożeniom?	Daniel Lampart	17-09-2026	13:00	15:00	02:00
11 z 16 Jak zorganizować cyberbezpieczeństwo w kadrach i księgowości?	Daniel Lampart	23-09-2026	09:00	10:30	01:30
12 z 16 Przerwa	Daniel Lampart	23-09-2026	10:30	10:45	00:15
13 z 16 Jak zorganizować cyberbezpieczeństwo w kadrach i księgowości?	Daniel Lampart	23-09-2026	10:45	12:30	01:45

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
14 z 16 Przerwa	Daniel Lampart	23-09-2026	12:30	13:00	00:30
15 z 16 Jak zorganizować cyberbezpieczeństwo w kadrach i księgowości?	Daniel Lampart	23-09-2026	13:00	13:45	00:45
16 z 16 Test walidacyjny	Daniel Lampart	23-09-2026	13:45	15:00	01:15

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	3 062,70 PLN
Koszt przypadający na 1 uczestnika netto	2 490,00 PLN
Koszt osobogodziny brutto	145,84 PLN
Koszt osobogodziny netto	118,57 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Daniel Lampart

Trener, konsultant, licencjonowany audytor wiodący norm ISO 9001 (zarządzanie jakością) oraz 27001(bezpieczeństwo informacji), Ekspert w cyberbezpieczeństwa i ochrony danych osobowych, podnoszenia efektywności i wydajności biznesowej, wdrożeniowiec systemów zarządzania jakością oraz bezpieczeństwa informacji. Inspektor Ochrony danych Osobowych w wielu firmach prywatnych i jednostkach publicznych w Polsce. Doświadczenie zawodowe zdobywał na stanowiskach Security Oficera, Information Security Managera, Inspektora Ochrony Danych Osobowych, Audytora wiodącego systemów zarządzania jakością, bezpieczeństwem informacji i cyberbezpieczeństwa. Ponad 200 zrealizowanych wdrożeń systemów bezpieczeństwa informacji. Od 2015 roku auditor wiodący Normy ISO 27001 oraz 27701 realizujący Audyty certyfikacyjne dla międzynarodowych jednostek certyfikujących m.in. QS Zurich, ICVC, DeuZert GmbH, SCK Cert. Jako trener pro aktywnie realizuje rocznie dziesiątki szkoleń w zakresie ochrony danych osobowych, zarządzania procesami, cyberbezpieczeństwa oraz bezpieczeństwa informacji dla branży handlowej, przemysłowej,

medycznej, urzędów państwowych oraz wymiaru sprawiedliwości, przygotowuje również do pełnienia funkcji Inspektora Ochrony Danych Osobowych.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Uczestnik usługi otrzyma komplet materiałów szkoleniowych w formie PDF, przygotowany przez prowadzących:

- Skrypt

- dostęp do nagrania szkolenia na okres 21 dni.

Warunki uczestnictwa

Umiejętność pracy z komputerem, znajomość środowiska Windows, Internet

Informacje dodatkowe

Cena bez VAT dla opłacających szkolenie, w co najmniej 70% ze środków publicznych.

Zwolnienie z art. 43 ust. 1 pkt 29 lit. C ustawy o VAT lub paragraf 3 ust. 1 pkt. 14 Rozporządzenia Ministra Finansów w sprawie zwolnień VAT oraz warunków stosowania tych zwolnień.

Zapraszamy do odwiedzenia naszej strony internetowej: https://wektorwiedzy.pl/

Warunki techniczne

Szkolenie bedzie prowadzone za pośrednictwem Platformy ClickMeeting.

Szkolenia na ClickMeeting nie wymagają instalowania żadnego programu, są transmitowane przez przeglądarkę. Bardzo ważne jest, żeby była ona zaktualizowana do najnowszej wersji (jeśli nie będzie aktualna, podczas testu nie pojawi się zielony “✓”). W razie potrzeby istnieje też możliwość pobrania aplikacji mobilnej i uczestniczenia w szkoleniu poprzez smartfon lub tablet.

Wymagania techniczne: procesor 2-rdzeniowy 2 GHz; 2 GB pamięci RAM; system operacyjny Windows 8 lub nowszy, MAC OS wersja 10.13; przeglądarka internetowa Google Chrome, Mozilla Firefox lub Safari; stałe łącze internetowe o prędkości 1,5 Mbps.

Konieczne jest posiadanie kamerki internetowej, umożliwiającej przeprowadzenie monitoringu realizacji usług szkoleniowych.

Najbezpieczniejszą opcją jest połączenie internetowe za pomocą kabla sieciowego. Gdy nie ma takiej możliwości i pozostaje korzystanie z WiFi, warto na czas szkolenia umieścić komputer jak najbliżej routera i zadbać, aby inni użytkownicy tej samej sieci WiFi ograniczyli w tym czasie aktywności mocno obciążające sieć (np. oglądanie filmów, rozmowy wideo lub pobieranie dużych plików). Jeśli jest taka możliwość zachęcamy do przetestowania połączenia w domu oraz miejscu pracy i uczestniczenia w szkoleniu z tego miejsca, w którym będzie lepszy Internet.

Jak dołączyć do spotkania: https://youtu.be/ZFWhNh2KHro, https://knowledge.clickmeeting.com/pl/infographic/jak-dolaczyc-do-wydarzenia-instrukcja-dla-uczestnika/

Link umożliwiający uczestnictwo w kursie ważny jest od dnia poprzedzającego rozpoczęcie kursu do zakończenia zajęć.

Kontakt

Anna Wilk

E-mail a.wilk@wektorwiedzy.pl
Telefon (+48) 17 2831 004