Możliwość dofinansowania

Cyberbezpieczeństwo w pracy biurowej i technicznej – bezpieczne wykorzystanie AI i Microsoft Office

Numer usługi 2026/06/10/21247/3617509

4 320,00 PLN brutto
4 320,00 PLN netto
180,00 PLN brutto/h
180,00 PLN netto/h
261,33 PLN cena rynkowa

TOMASZ KOPCZYŃSKI "SYNERGIA"

4,4 / 5

731 ocen

Usługa szkoleniowa
zdalna w czasie rzeczywistym
Zajęcia grupowe
24:00 h
03.07.2026 do 10.07.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Szkolenie skierowane jest do pracowników wykonujących obowiązki w środowisku biurowym i technicznym, którzy w codziennej pracy korzystają z narzędzi cyfrowych, w tym pakietu Microsoft Office oraz rozwiązań opartych na sztucznej inteligencji.
Minimalna liczba uczestników	5
Maksymalna liczba uczestników	30
Data zakończenia rekrutacji	02-07-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
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

Celem szkolenia jest rozwój kompetencji uczestników w zakresie cyberbezpieczeństwa oraz bezpiecznego wykorzystania sztucznej inteligencji i narzędzi Microsoft Office w pracy biurowej i technicznej, w szczególności w obszarze ochrony danych, identyfikacji zagrożeń, bezpiecznego przetwarzania informacji oraz usprawnienia pracy z dokumentacją i analizą danych.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik identyfikuje zagrożenia cyberbezpieczeństwa w środowisku pracy biurowej i technicznej.	Rozróżnia podstawowe typy zagrożeń (phishing, malware, ransomware, socjotechnika), wskazuje źródła potencjalnych zagrożeń w środowisku pracy, określa skutki naruszenia bezpieczeństwa informacji.	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik stosuje zasady ochrony danych oraz bezpiecznego przetwarzania informacji.	Rozróżnia dane wrażliwe i dane ogólne, wskazuje zasady bezpiecznego przechowywania i udostępniania danych, dobiera właściwe metody zabezpieczania informacji (np. hasła, dostęp).	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik wykorzystuje narzędzia sztucznej inteligencji w sposób bezpieczny i świadomy.	Identyfikuje ryzyka związane z wykorzystaniem AI (np. wycieki danych), wskazuje zasady bezpiecznego korzystania z narzędzi AI, dobiera właściwy sposób użycia AI do zadań zawodowych bez ujawniania danych wrażliwych.	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik wykorzystuje narzędzia Microsoft Office zgodnie z zasadami bezpieczeństwa.	Wskazuje sposoby zabezpieczania dokumentów i plików, rozpoznaje zasady bezpiecznego udostępniania danych, identyfikuje poprawne praktyki pracy z dokumentacją i danymi.	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik stosuje dobre praktyki cyberbezpieczeństwa w codziennej pracy zawodowej.	Wskazuje właściwe działania w sytuacjach zagrożenia, rozpoznaje nieprawidłowe zachowania użytkowników, dobiera odpowiednie reakcje na incydenty bezpieczeństwa.	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

PROGRAM SZKOLENIA

Temat: Cyberbezpieczeństwo w pracy biurowej i technicznej – bezpieczne wykorzystanie AIi Microsoft Office

Wprowadzenie do cyberbezpieczeństwa w organizacji

- Znaczenie cyberbezpieczeństwa w pracy biurowej i technicznej
- Aktualne zagrożenia: phishing, malware, ransomware, socjotechnika
- Najczęstsze błędy użytkowników
- Przykłady incydentów (case study)
- Rola pracownika w systemie bezpieczeństwa

Ochrona danych i zarządzanie informacją

- Rodzaje danych (w tym dane wrażliwe i firmowe)
- Zasady bezpiecznego przetwarzania danych
- Podstawy RODO w praktyce
- Zarządzanie dostępem do danych
- Bezpieczne przechowywanie i archiwizacja informacji

Bezpieczeństwo pracy w środowisku cyfrowym

- Bezpieczne korzystanie z poczty elektronicznej
- Rozpoznawanie phishingu i prób wyłudzeń
- Bezpieczeństwo pracy zdalnej i mobilnej
- Sieci Wi-Fi i urządzenia służbowe/prywatne
- Aktualizacje systemów i oprogramowania

Bezpieczne wykorzystanie sztucznej inteligencji (AI)

- Wprowadzenie do narzędzi AI (np. ChatGPT)
- Możliwości wykorzystania AI w pracy (analizy, dokumenty, raporty)
- Ryzyka związane z AI (wycieki danych, błędy)
- Zasady bezpiecznego korzystania z AI
- Tworzenie bezpiecznych zapytań (promptów)
- Ćwiczenia praktyczne

Microsoft Excel – analiza danych i bezpieczeństwo

- Praca na danych (sortowanie, filtrowanie, podstawowe formuły)
- Identyfikacja błędów i nieprawidłowości
- Zabezpieczanie arkuszy i plików
- Bezpieczne udostępnianie danych
- Wykorzystanie AI w analizie danych

Microsoft Word i PowerPoint – bezpieczna dokumentacja i komunikacja

- Tworzenie dokumentów formalnych i technicznych (Word)
- Ochrona dokumentów (hasła, ograniczenia dostępu)
- Śledzenie zmian i współpraca zespołowa
- Tworzenie prezentacji biznesowych (PowerPoint)
- Bezpieczne udostępnianie plików
- Wykorzystanie AI w dokumentach i prezentacjach
- Ćwiczenia praktyczne

Reagowanie na incydenty i dobre praktyki

- Identyfikacja incydentów bezpieczeństwa
- Procedury reagowania i zgłaszania
- Minimalizacja skutków zagrożeń
- Dobre praktyki w codziennej pracy
- Checklisty bezpieczeństwa dla pracownika

Podsumowanie szkolenia

- Powtórzenie kluczowych zagadnień
- Najważniejsze zasady cyberbezpieczeństwa
- Sesja pytań i odpowiedzi
- Wskazówki do wdrożenia w pracy

Walidacja efektów uczenia się zostanie przeprowadzona przez trenera Łukasza Kopczyńskiego w formie:

- testu teoretycznego jednokrotnego wyboru oraz pytań typu prawda/fałsz,
- realizowanego w formie elektronicznej,
- z automatycznym generowaniem wyniku po zakończeniu testu.

Harmonogram

Liczba pozycji harmonogramu: 18

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 18 Wprowadzenie do cyberbezpieczeństwa w organizacji cz.1	Zajęcia	Łukasz Kopczyński	03-07-2026	09:00	12:00	03:00
2 z 18 -	Przerwa	-	03-07-2026	12:00	12:15	00:15
3 z 18 Wprowadzenie do cyberbezpieczeństwa w organizacji	Zajęcia	Łukasz Kopczyński	03-07-2026	12:15	13:00	00:45

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
4 z 18 Ochrona danych i zarządzanie informacją cz.1	Zajęcia	Łukasz Kopczyński	06-07-2026	09:00	12:00	03:00
5 z 18 -	Przerwa	-	06-07-2026	12:00	12:15	00:15
6 z 18 Ochrona danych i zarządzanie informacją cz.2	Zajęcia	Łukasz Kopczyński	06-07-2026	12:15	13:00	00:45
7 z 18 Bezpieczeństwo pracy w środowisku cyfrowym cz. 1	Zajęcia	Łukasz Kopczyński	07-07-2026	09:00	12:00	03:00
8 z 18 -	Przerwa	-	07-07-2026	12:00	12:15	00:15
9 z 18 Bezpieczeństwo pracy w środowisku cyfrowym cz. 2	Zajęcia	Łukasz Kopczyński	07-07-2026	12:15	13:00	00:45
10 z 18 Bezpieczne wykorzystanie sztucznej inteligencji (AI) cz.1	Zajęcia	Łukasz Kopczyński	08-07-2026	09:00	12:00	03:00
11 z 18 -	Przerwa	-	08-07-2026	12:00	12:15	00:15
12 z 18 Bezpieczne wykorzystanie sztucznej inteligencji (AI) cz.2	Zajęcia	Łukasz Kopczyński	08-07-2026	12:15	13:30	01:15
13 z 18 Reagowanie na incydenty i dobre praktyki cz.1	Zajęcia	Łukasz Kopczyński	09-07-2026	09:00	12:00	03:00

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
14 z 18 -	Przerwa	-	09-07-2026	12:00	12:15	00:15
15 z 18 Reagowanie na incydenty i dobre praktyki cz.2	Zajęcia	Łukasz Kopczyński	09-07-2026	12:15	13:30	01:15
16 z 18 Podsumowanie	Zajęcia	Łukasz Kopczyński	10-07-2026	09:00	10:30	01:30
17 z 18 -	Przerwa	-	10-07-2026	10:30	10:45	00:15
18 z 18 -	Walidacja	Łukasz Kopczyński	10-07-2026	10:45	12:00	01:15

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	24:00
w tym suma godzin zajęć	21:15
w tym suma godzin walidacji	01:15
w tym suma przerw	01:30
Suma godzin dydaktycznych bez przerw	30:00

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	4 320,00 PLN
Podmiot uprawniony do zwolnienia z VAT na podstawie art. 43 ust. 1 ustawy o VAT	
Koszt przypadający na 1 uczestnika netto	4 320,00 PLN
Koszt osobogodziny brutto	180,00 PLN

Koszt osobogodziny netto	180,00 PLN

Liczba godzin usługi

Rodzaj godzin	Liczba godzin
Liczba godzin zegarowych usługi	24:00

Prowadzący

Liczba prowadzących: 2

1 z 2

Łukasz Kopczyński

Bartosz Lewandowski – inżynier z 10-letnim doświadczeniem w IT, entuzjasta technologii budujący mosty między światem IT a osobami nietechnicznymi.
Od 2025 roku naucza firmy i organizacje praktycznego wykorzystania AI – nie pokazując szczegółów narzędzi, ale rozwiązując konkretne problemy i usprawniając codzienną pracę.
Kładzie równy nacisk na możliwości i odpowiedzialne wykorzystanie: ochronę prywatności, weryfikację treści, świadomość ograniczeń.

2 z 2

Michał Michaluk

Ekspert bezpieczeństwa IT, craftsman i praktyk bezpiecznego wdrażania sztucznej inteligencji oraz ekosystemu Microsoft Office. W ciągu ostatnich 5 lat intensywnie budował cyfrową odporność organizacji, łącząc twardą wiedzę techniczną z realiami codziennej pracy biurowej. Posiada bogate doświadczenie w projektowaniu bezpiecznych procedur i edukacji użytkowników – zarówno w dynamicznych, skrajnie zwinnych startupach wdrażających narzędzia AI na oślep, jak i w silnie zbiurokratyzowanych korporacjach obwarowanych restrykcyjnymi zasadami compliance. W swojej pracy trenera stawia na pragmatyzm, pokazując, jak nowoczesne technologie mogą wspierać biznes bez wystawiania go na cyberzagrożenia.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Uczestnicy szkolenia otrzymają komplet materiałów w formie elektronicznej, które będą dostępne do pobrania przed rozpoczęciem szkolenia oraz na bieżąco w trakcie jego trwania.

Materiały obejmują:

- **Podręcznik „Cyberbezpieczeństwo w praktyce”** – zawierający podsumowanie najważniejszych zagadnień omawianych podczas szkolenia, w tym typowe zagrożenia, dobre praktyki, checklisty oraz przykładowe scenariusze reagowania na incydenty.
- **Prezentacje multimedialne** wykorzystywane podczas zajęć – w formacie PDF.
- **Interaktywne arkusze ćwiczeń** – m.in. symulacje rozpoznawania phishingu, analiza ryzyka, tworzenie planu bezpieczeństwa.
- **Zestaw narzędzi rekomendowanych** do zwiększenia poziomu bezpieczeństwa cyfrowego (linki do aplikacji, rozszerzeń przeglądarkowych, menedżerów haseł itp.).

- **Certyfikat uczestnictwa** w formacie PDF (dla osób, które ukończą szkolenie i wezmą udział w walidacji).

Warunki techniczne

1. Komputer lub urządzenie mobilne – w przypadku urządzenia mobilnego można pobrać odpowiednią aplikację „Google Meet” ze sklepu Google Play lub AppStore.

2. Szerokopasmowe połączenie z internetem.

3. Wymagania sprzętowe - procesor dwurdzeniowy 2GHz lub lepszy (zalecany czterordzeniowy), 2GB pamięci RAM (zalecane 4GB lub więcej).

4. Mikrofon zewnętrzny lub mikrofon wbudowany w urządzeniu oraz głośniki zewnętrzne lub wbudowane w urządzeniu. Szkolenie prowadzone będzie na platformie google meets lub clickmeeting

Kontakt

WERONIKA BRZOSTOWSKA

E-mail weronika.brzostowska@synergia-pm.pl
Telefon (+48) 793 087 684