



## Cyberbezpieczeństwo w praktyce: od socjotechniki do testów infrastruktury – szkolenie prowadzi do nabycia kwalifikacji

Numer usługi 2026/05/28/145274/3592256

4 366,50 PLN brutto  
3 550,00 PLN netto  
272,91 PLN brutto/h  
221,88 PLN netto/h  
261,33 PLN cena rynkowa ⓘ

YOURSKILLUP.PL  
SPÓŁKA Z  
OGRANICZONĄ  
ODPOWIEDZIALNOŚ  
CIĄ

★★★★★ 4,8 / 5  
390 ocen

- 📍 Katowice
- 🏢 Usługa szkoleniowa
- 📄 mieszana (stacjonarna połączona z usługą zdalną w czasie rzeczywistym)
- 👥 Zajęcia grupowe
- 🕒 16:00 h
- 📅 22.08.2026 do 28.08.2026

## Informacje podstawowe

### Kategoria

Informatyka i telekomunikacja / Bezpieczeństwo IT

### Grupa docelowa usługi

**Szkolenie skierowane jest do osób dorosłych, które wykorzystują lub planują wykorzystywać narzędzia cyfrowe w pracy zawodowej lub życiu codziennym, w szczególności do:**

- pracowników administracyjnych i biurowych,
- osób pracujących w organizacjach wdrażających rozwiązania z zakresu zrównoważonego rozwoju (zielonej gospodarki),
- osób wykorzystujących technologie cyfrowe w różnych branżach,
- osób planujących rozwój kompetencji cyfrowych lub zmianę kwalifikacji zawodowych,
- osób poszukujących pracy.

**Szkolenie jest odpowiednie dla wszystkich grup zawodowych, niezależnie od branży, wieku czy poziomu zaawansowania technicznego. Nie są wymagane wcześniejsze kompetencje informatyczne - program został zaprojektowany w sposób przystępny i praktyczny.**

**Zakres szkolenia uwzględnia aktualne zagrożenia w cyberprzestrzeni, które mają wpływ zarówno na funkcjonowanie organizacji, jak i bezpieczeństwo użytkowników w życiu prywatnym, ze szczególnym uwzględnieniem środowisk wykorzystujących rozwiązania cyfrowe.**

Minimalna liczba uczestników

5

Maksymalna liczba uczestników

15

Data zakończenia rekrutacji

21-08-2026

# Cel

## Cel edukacyjny

Usługa przygotowuje uczestników do świadomego i bezpiecznego poruszania się w cyfrowym świecie. Uczestnicy nauczą się rozpoznawać i zapobiegać zagrożeniom cyfrowym, stosować zasady higieny cyfrowej, a także bezpiecznie zarządzać infrastrukturą cyfrową, uwzględniając AI, zgodnie z zasadami zrównoważonego rozwoju i zielonej transformacji.

## Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Posługuje się wiedzą dotyczącą cyberzagrożeń i ich konsekwencji.	Charakteryzuje podstawowe zagrożenia cybernetyczne (cyberprzemoc, phishing, malware, ransomware).	Test teoretyczny z wynikiem generowanym automatycznie
	Rozpoznaje dezinformację i niebezpieczne treści w sieci	Test teoretyczny z wynikiem generowanym automatycznie
	Rozumie mechanizmy działania tych zagrożeń i sposobów, w jakie mogą przenikać do systemów informatycznych Ma świadomość skutków finansowych (np. utrata pieniędzy, koszty odtworzenia danych). Rozumie konsekwencje prawne i reputacyjne (np. utrata zaufania klientów, odpowiedzialność karna lub cywilna). Rozwija krytyczne myślenie wobec informacji w sieci i potencjalnych manipulacji.	Test teoretyczny z wynikiem generowanym automatycznie

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Stosuje zasady higieny cyfrowej i bezpieczeństwa danych	Tworzy silne hasła oraz stosuje uwierzytelnianie dwuskładnikowe.	Analiza dowodów i deklaracji
	<p>Konfiguruje ustawienia prywatności w mediach społecznościowych.</p> <p>Regularnie aktualizuje systemy operacyjne, aplikacje i programy antywirusowe</p> <p>Unika korzystania z niezabezpieczonych sieci WWi-Fi</p> <p>Świadomie udostępnia informacje ogranicza publikacje danych wrażliwych w mediach społecznościowych i formularzach online.</p>	<p>Analiza dowodów i deklaracji</p> <p>Analiza dowodów i deklaracji</p>
Rozpoznaje i reaguje na cyberzagrożenia.	Analizuje przypadki phishingu i potrafi je skutecznie zidentyfikować	Analiza dowodów i deklaracji
	Zabezpiecza urządzenia przed złośliwym oprogramowaniem.	Analiza dowodów i deklaracji
	Stosuje narzędzia do ochrony danych, takie jak szyfrowanie i VPN.	Analiza dowodów i deklaracji
	<p>Dostrzega nietypowe zachowania systemu lub podejrzanych wiadomości jako potencjalne sygnały zagrożenia. Analizuje, jakie skutki może mieć dane zagrożenie dla użytkownika, organizacji czy systemu.</p> <p>Rozumie różnice między zagrożeniami niskiego i wysokiego ryzyka oraz ich wpływu na bezpieczeństwo danych.</p> <p>Przedstawia Optymalizację wykorzystanie energii w pracy zdalnej i zarządzaniu danymi</p>	<p>Analiza dowodów i deklaracji</p> <p>Test teoretyczny z wynikiem generowanym automatycznie</p>
Wdraża zasady zrównoważonego zarządzania technologią.	<p>Optymalizuje wykorzystanie energii i sprzętu, aby zmniejszyć ślad węglowy. Wybiera rozwiązania technologiczne wspierające efektywność energetyczną i ograniczające marnotrawstwo. Uwzględnia zasady recyklingu i ponownego wykorzystania urządzeń oraz komponentów.</p> <p>Poszukuje innowacyjnych rozwiązań, które łączą rozwój technologiczny z zasadami zrównoważonego rozwoju.</p> <p>Dbą o właściwą utylizację sprzętu elektronicznego zgodnie z zasadami ochrony środowiska.</p>	Test teoretyczny z wynikiem generowanym automatycznie

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
<p>Stosuje zasady prawidłowej komunikacji podczas rozwiązywania problemów związanych z cyberbezpieczeństwem.</p>	<p>Analizuje przypadki cyberzagrożeń i przedstawia rozwiązania problemów, które wynikają z pracy zespołowej oraz indywidualnej,</p>	<p>Test teoretyczny z wynikiem generowanym automatycznie</p>
	<p>Identyfikuje i przedstawia rozwiązania konflikty w zespole, które mogą wynikać z różnic w podejściu do problemów związanych z cyberbezpieczeństwem.</p> <p>Opisuje problem w sposób zrozumiały. Przekazuje kluczowe fakty i symptomy zagrożenia, aby ułatwić szybką diagnozę.</p> <p>Stosuje ustalone kanały komunikacji do raportowania zagrożeń i incydentów. Przekazuje informacje zgodnie z obowiązującymi zasadami poufności i ochrony danych.</p> <p>Zachowuje spokój i rzeczowość w sytuacjach kryzysowych, unikając paniki i dezinformacji.</p> <p>Buduje zaufanie poprzez rzetelne, etyczne i odpowiedzialne podejście do komunikacji w obszarze cyberbezpieczeństwa.</p>	<p>Test teoretyczny z wynikiem generowanym automatycznie</p> <p>Test teoretyczny z wynikiem generowanym automatycznie</p>

## Kwalifikacje

### Kwalifikacje niewłączone do ZSK

#### Uznane kwalifikacje

Pytanie 3. Czy dokument jest certyfikatem wydawanym przez międzynarodowe instytucje?

TAK

Strona internetowa Instytucji Certyfikującej: <https://my-ps.eu/dzialalnosc-miedzynarodowa/>

Strona internetowa Instytucji Walidującej: <https://my-ps.eu/dzialalnosc-miedzynarodowa/>

#### Informacje

Nazwa Podmiotu prowadzącego walidację

Fundacja My Personality Skills

Nazwa Podmiotu certyfikującego

Fundacja My Personality Skills

# Program

Usługa prowadzi do nabycia kwalifikacji : **Specjalista ds. cyberbezpieczeństwa**

Specjalista ds. cyberbezpieczeństwa, posiada kwalifikacje w zakresie zapewniania bezpieczeństwa systemów informatycznych oraz ochrony danych organizacji. Dysponuje wiedzą z zakresu analizy ryzyka. Zna zasady działania sieci komputerowych, systemów operacyjnych. Potrafi identyfikować i neutralizować zagrożenia, a także wdrażać rozwiązania zwiększające poziom cyberbezpieczeństwa. Wykorzystuje aktualne standardy i narzędzia zgodne z najlepszymi praktykami branżowymi

---

**Usługa powiązana jest z dokumentami strategicznymi**

**Szkolenie jest zgodne z:**

- **Regionalną Strategią Innowacji Województwa Śląskiego 2030**
- **Programem Rozwoju Technologii Województwa Śląskiego 2019–2030**
- zakresem **zielonych umiejętności** (ESCO – Europejska Klasyfikacja Umiejętności, Kompetencji, Kwalifikacji i Zawodów)

**Obszary technologiczne:**

- Technologie informacyjne i komunikacyjne (ICT), podobszar 4.6 Bezpieczeństwo informacji

**Warunki organizacyjne:**

**Godziny realizacji szkolenia**

1. **Szkolenie trwa 19 godzin dydaktycznych (1 godzina dydaktyczna = 45 min)** tj. 14.30 godzin zegarowych
2. Harmonogram przedstawiony jest w godzinach zegarowych (09:00–17:00) i obejmuje przerwy (łącznie 90 minut,)

- usługa obejmuje 16 godzin dydaktycznych teoretycznych i 3 godzin dydaktycznych praktycznych.
- Walidacja wliczona jest w czas trwania usługi.
- Przerwy nie zostały wliczone w czas trwania usługi (tj. 2 h dydaktyczne = 1,30 h zegarowe), natomiast ujęte zostały w harmonogramie

**Walidacja kwalifikacji**

**Na zakończenie szkolenia zostanie przeprowadzona walidacja przeprowadzona w standardzie MY PERSONALITY SKILLS® potwierdzająca:**

- **nabycie kwalifikacji : „Specjalista ds. cyberbezpieczeństwa”**

**Uwaga!** Czas oczekiwania na wydanie certyfikatu potwierdzającego nabycie kwalifikacji został wliczony w czas trwania usługi (5 dni robocze)

Certyfikat

- w pierwszej kolejności wydawany jest w wersji elektronicznej,
- w kolejnych dniach roboczych certyfikat w wersji papierowej wysyłany jest pocztą tradycyjną na adres uczestnika .

---

**Program szkolenia:**

**Dzień 1**

Moduł 1: Wprowadzenie do cyberbezpieczeństwa

- Podstawowe pojęcia i typy zagrożeń, w tym cyberprzemoc
- Rola użytkownika w ochronie danych
- Realne przypadki incydentów cybernetycznych
- Poznanie technik ataków oraz programów wykorzystywanych przez włamywaczy (przeгляд na poziomie ogólnym z uwzględnieniem pentestów )

Moduł 2A: Phishing i socjotechnika

- Mechanizmy ataków phishingowych
- Techniki manipulacji (Cialdini – 6 zasad wpływu)
- Przykłady fałszywych wiadomości (e-mail, SMS, komunikatory)

- Rozszerzenie wiedzy o narzędziach wykorzystywanych w kampaniach phishingowych (np. generatory stron, klony loginów)

#### Moduł 2B: Phishing i socjotechnika - praktyka

- Ćwiczenia rozpoznawania prób oszustwa
- Analiza przypadków i dyskusja
- Przegląd metod testowania odporności użytkowników (wariant audytu socjotechnicznego)

#### Moduł 3: Sztuczna inteligencja w cyberzagrożeniach

- Wykorzystanie AI przez cyberprzestępców (deepfake, automatyzacja)
- Przykłady użycia ChatGPT w phishingu
- Rozpoznawanie treści generowanych przez AI
- Omówienie narzędzi AI wspierających analizę incydentów i bezpieczeństwo

#### Dzień 2

- Moduł 4: Bezpieczne praktyki cyfrowe
- Tworzenie i zarządzanie silnymi hasłami
- Uwierzytelnianie dwuskładnikowe
- Bezpieczne korzystanie z sieci publicznych
- Ochrona danych osobowych i firmowych
- Rozszerzenie wiedzy na temat zabezpieczania serwerów i usług (najważniejsze zasady, bez technicznych konfiguracji)
- OSINT – podstawy i zagrożenia

#### Moduł 4B: Technologie wspierające przemysł i bezpieczeństwo informacji

- Technologie informacyjne i telekomunikacyjne w kontekście przemysłu 4.0
- Geoinformacja i jej zastosowanie w analizie ryzyka
- Bezpieczeństwo informacji w środowisku cyfrowym

#### Moduł 5: Część praktyczna – scenariusze i ćwiczenia

- Symulacja ataku phishingowego (e-mail/SMS)
- Interaktywne quizy i analiza reakcji
- Praca w grupach: rozpoznawanie zagrożeń, podejmowanie decyzji
- Omówienie wyników i rekomendacje
- Przegląd narzędzi i metod służących do testowania bezpieczeństwa sieci (skanery, analizatory, podstawowe narzędzia audytowe )
- Omówienie technik prowadzenia testów penetracyjnych infrastruktury (wariant audytu)

#### Moduł 6: Zielone i cyfrowe kompetencje – analiza i rozwój

- Zielone kompetencje według GreenComp i ESCO – analiza stanowisk pracy
- Matryca kompetencji green & digital – narzędzie rozwoju pracownika i zespołu
- Powiązanie kompetencji cyfrowych z celami zrównoważonego rozwoju

Walidacja, Egzamin końcowy

Podsumowanie i refleksja uczestników

## Harmonogram

Liczba pozycji harmonogramu: 19

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin	Forma stacjonarna
1 z 19 Wprowadzenie do cyberbezpieczeństwa_ współdziałanie ekranu, chat, rozmowa na żywo	Zajęcia	Kamila Juszczyk	22-08-2026	09:00	10:30	01:30	Tak
2 z 19 -	Przerwa	-	22-08-2026	10:30	10:40	00:10	Tak
3 z 19 Phishing i socjotechnika – teoria — współdziałanie ekranu, chat, rozmowa na żywo	Zajęcia	Kamila Juszczyk	22-08-2026	10:40	12:10	01:30	Tak
4 z 19 -	Przerwa	-	22-08-2026	12:10	12:40	00:30	Tak
5 z 19 Phishing i socjotechnika – praktyka_ współdziałanie ekranu, chat, rozmowa na żywo	Zajęcia	Kamila Juszczyk	22-08-2026	12:40	14:40	02:00	Tak
6 z 19 -	Przerwa	-	22-08-2026	14:40	14:50	00:10	Tak
7 z 19 Sztuczna inteligencja w cyberzagrozeniach_ współdziałanie ekranu, chat, rozmowa na żywo	Zajęcia	Kamila Juszczyk	22-08-2026	14:50	15:50	01:00	Tak
8 z 19 -	Przerwa	-	22-08-2026	15:50	16:00	00:10	Tak

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin	Forma stacjonarna
<b>9 z 19</b> Ciąg dalszy_Sztuczna inteligencja w cyberzagrożeniach__współdzienie ekranu, chat, rozmowa na żywo	Zajęcia	Kamila Juszczyk	22-08-2026	16:00	17:00	01:00	Tak
<b>10 z 19</b> Bezpieczne praktyki cyfrowe__współdzienie ekranu, chat, rozmowa na żywo	Zajęcia	Kamila Juszczyk	23-08-2026	09:00	10:45	01:45	Tak
<b>11 z 19</b> -	Przerwa	-	23-08-2026	10:45	10:55	00:10	Tak
<b>12 z 19</b> Technologie wspierające przemysł i bezpieczeństwo informacji__współdzienie ekranu, chat, rozmowa na żywo	Zajęcia	Kamila Juszczyk	23-08-2026	10:55	12:25	01:30	Tak
<b>13 z 19</b> -	Przerwa	-	23-08-2026	12:25	12:55	00:30	Tak
<b>14 z 19</b> Część praktyczna __scenariusze i ćwiczenia, współdzienie ekranu, chat, rozmowa na żywo	Zajęcia	Kamila Juszczyk	23-08-2026	12:55	13:55	01:00	Tak

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin	Forma stacjonarna
15 z 19 -	Przerwa	-	23-08-2026	13:55	14:05	00:10	Tak
16 z 19 Ciąg dalszy_ Część praktyczna - scenariusze i ćwiczenia, współdziałanie ekranu, chat, rozmowa na żywo	Zajęcia	Kamila Juszczyk	23-08-2026	14:05	15:05	01:00	Tak
17 z 19 Zielone i cyfrowe kompetencje – analiza i rozwój	Zajęcia	Kamila Juszczyk	23-08-2026	15:05	15:50	00:45	Tak
18 z 19 -	Przerwa	-	23-08-2026	15:50	16:00	00:10	Tak
19 z 19 -	Walidacja	-	23-08-2026	16:00	17:00	01:00	Nie

## Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	16:00
w tym suma godzin zajęć	13:00
w tym suma godzin walidacji	01:00
w tym suma przerw	02:00
Suma godzin dydaktycznych bez przerw	18:30

## 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 z 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	4 366,50 PLN
Koszt przypadający na 1 uczestnika netto	3 550,00 PLN
Koszt osobogodziny brutto	272,91 PLN
Koszt osobogodziny netto	221,88 PLN
W tym koszt walidacji brutto	36,90 PLN
W tym koszt walidacji netto	30,00 PLN
W tym koszt certyfikowania brutto	547,35 PLN
W tym koszt certyfikowania netto	445,00 PLN

## Liczba godzin usługi

Rodzaj godzin	Liczba godzin
Liczba godzin zegarowych usługi	16:00

## Prowadzący

Liczba prowadzących: 1



1 z 1

### Kamila Juszczyk

Ekspertka ds. cyberbezpieczeństwa, trenerka i edukatorka z pasją do dzielenia się wiedzą. Posiada liczne certyfikaty branżowe, w tym ISO 27001, Cyber Security Foundation, Cyber Security Specialist, OSINT, oraz MoR Foundation a także ukończony kurs ITIL i CRISC.

Interdyscyplinarne podejście łączy aspekty technologiczne z perspektywą społeczną, co czyni szkolenia kompleksowymi i praktycznymi.

Posiada 6 letnie doświadczenie, wiedzę i pasję do edukacji, by skutecznie wzmacniać cyberodporność organizacji i jednostek.

Przeprowadzone szkolenia:

W ramach realizowanych działań od 2021 roku, Trenerka przeprowadziła liczne warsztaty dla dzieci i młodzieży oraz osób dorosłych, w tym m.in :

- 200 godzin szkoleniowych w przedszkolach, szkołach podstawowych i średnich z zakresu cyberbezpieczeństwa

- 40 godzin szkoleniowych dla seniorów,

W ramach współpracy z Fundacją IT Girls:

- 6 miesięczny mentoring dla mentee, opiewający na 40 godzin spotkań, które miały na celu pomóc wejść mentee do świata technologii, w tym cyberbezpieczeństwa w ramach projektu Jump To IT.

- 16 godzin warsztat 16 godzin warsztatów w 4 edycjach programu MOCna Ja,

## Informacje dodatkowe

### Informacje o materiałach dla uczestników usługi

Prezentacja, zbiór najlepszych praktyk z zakresu cyberbezpieczeństwa, linki edukacyjne.

### Informacje dodatkowe

Po szkoleniu Uczestnicy otrzymują zaświadczenie ukończenia szkolenia.

Szkolenie kończy się egzaminem w standardzie MY PERSONALITY SKILLS® - instytucją prowadząca walidację i certyfikację jest Fundacja My Personality Skills

Usługa szkoleniowa jest zwolniona z VAT zgodnie z podstawą prawną:

§ 3 ust.1 pkt 14 Rozporządzenia Ministra Finansów z dnia 20 grudnia 2013 roku w sprawie zwolnień od podatku towarów i usług oraz warunków stosowania tych zwolnień. (Dz.U. 2025 poz. 832)

## Warunki techniczne

**Szkolenie odbędzie się na platformie ClickMeeting.**

**Jakie są wymagania sprzętowe oraz oprogramowania ?**

Wymagania, które muszą zostać spełnione:

- komputer lub laptop z dostępem do Internetu , kamerką i mikrofonem
- Procesor dwurdzeniowy 2GHz lub lepszy (zalecany czterordzeniowy);
- 2GB pamięci RAM (zalecane 4GB lub więcej);
- System operacyjny taki jak Windows 8 (zalecany Windows 11), Mac OS wersja 10.13 (zalecana najnowsza wersja), Linux, Chrome OS.

**Minimalne wymagania dotyczące parametrów łącza internetowego**

Rodzaj połączenia	Uczestnik
Dźwięk	512 kbps
Dźwięk + obraz SD	512 kbps + 1 Mbps
Dźwięk + obraz HD	512 kbps + 2 Mbps

Współdzielenie ekranu (Tryb LiteQ)	2 Mbps
Współdzielenie ekranu (Tryb HighQ)	2 – 5 Mbps
Współdzielenie ekranu (oparte na przeglądarce)	1 – 4 Mbps

Ponieważ ClickMeeting jest platformą opartą na przeglądarce, wymagane jest korzystanie z Google Chrome, Mozilla Firefox, Safari, Edge (Chromium), Yandex lub Opera. Pamiętaj, aby korzystać z najaktualniejszej oficjalnej wersji wybranej przeglądarki.

ClickMeeting współpracuje z wszystkimi wbudowanymi w laptopy kamerami oraz większością kamer internetowych.

Aby móc korzystać z usługi na urządzeniach mobilnych, konieczne może być pobranie odpowiedniej aplikacji w iTunes App Store lub Google Play Store. Do korzystania z usługi w pełnym zakresie dźwięku i obrazu, konieczne jest posiadanie kamery internetowej, mikrofonu lub zestawu słuchawkowego, lub głośników podłączonych do urządzenia i rozpoznanych przez Twoje urządzenie i nie powinny być one jednocześnie używane przez żadną inną aplikację.

Uczestnicy nie muszą tworzyć konta ClickMeeting, aby dołączyć do usługi. Zostaną zaproszeni poprzez zaproszenie e-mail z linkiem przekierowującym do pokoju szkoleniowego.

**Okres ważności linku aktywacyjnego** - od momentu rozpoczęcia szkolenia do momentu zakończenia szkolenia

**Podstawą do rozliczenia usługi jest wygenerowanie z sytemu raportu, umożliwiającego identyfikację wszystkich uczestników, oraz zastosowanego narzędzia.**

## Adres

Katowice 138A  
40-156 Katowice  
woj. śląskie

Piętro 7

## Udogodnienia w miejscu realizacji usługi

- Klimatyzacja
- Wi-fi

## Kontakt



**Alicja Wal**

**E-mail** alicja.wal@yourskillup.pl

**Telefon** (+48) 506 668 408