



CENTRUM  
ANDRZEJ SZOPE  
SPÓŁKA JAWNA

★★★★★ 4,8 / 5

358 ocen

## Bądź bezpieczny w sieci - cyberbezpieczeństwo w praktyce - szkolenie

Numer usługi 2026/03/05/162860/3383523

📍 Olsztyn

🏢 Usługa szkoleniowa

📅 stacjonarna

🕒 18:00 h

📅 14.05.2026 do 15.05.2026

5 000,00 PLN brutto

5 000,00 PLN netto

277,78 PLN brutto/h

277,78 PLN netto/h

261,33 PLN cena rynkowa ⓘ

## Informacje podstawowe

### Kategoria

Informatyka i telekomunikacja / Bezpieczeństwo IT

### Grupa docelowa usługi

**Szkolenie jest przeznaczone przede wszystkim dla osób chcących chronić dane firmy, rozpoznawać oszustwa np. w mediach społecznościowych oraz odpowiednio reagować na nie.**

Szkolenie skierowane jest do:

- Specjalistów ds. IT bez doświadczenia w temacie Cyberbezpieczeństwa
- Dyrektorów i menedżerów pionów IT bez doświadczenia w temacie Cyberbezpieczeństwa
- Pracowników branży IT bez doświadczenia w temacie Cyberbezpieczeństwa
- Pracowników działów nowych technologii
- Pracowników działów zarządzania ryzykiem
- Audytorów wewnętrznych
- Audytorów systemów
- Użytkowników końcowych nowych technologii
- Pracowników biurowych.
- osób chcących poznać tajniki cyberbezpieczeństwa oraz zasady ochrony swoich danych w sieci
- pracowników i/lub właścicieli pracujących z komputerem, Internetem oraz urządzeniami mobilnymi
- pracowników z sektora MSP

Minimalna liczba uczestników

1

Maksymalna liczba uczestników

10

Data zakończenia rekrutacji

13-05-2026

Forma prowadzenia usługi

stacjonarna

## 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

Szkolenie "Bądź bezpieczny w sieci - cyberbezpieczeństwo w praktyce - szkolenie" przygotowuje uczestników do samodzielnego reagowania na cyber-zagrożenia, poprzez dokonywanie prawidłowej oceny własnych zabezpieczeń oraz wykorzystanie technik i sposobów walki z hakerami.

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

| Efekty uczenia się                                                       | Kryteria weryfikacji                                                                                 | Metoda walidacji                    |
|--------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|-------------------------------------|
| Uczestnik posługuje się podstawową wiedzą w zakresie cyberbezpieczeństwa | identyfikuje metody ochrony danych cyfrowych                                                         | Test teoretyczny                    |
|                                                                          | definiuje złożone hasła dostępu do danych stosując uwierzytelnienie wieloskładnikowe                 | Test teoretyczny                    |
|                                                                          | charakteryzuje rolę cyberbezpieczeństwa w audycie                                                    | Test teoretyczny                    |
|                                                                          | definiuje system szyfrowania plików                                                                  | Test teoretyczny                    |
| Uczestnik wykorzystuje techniki i sposoby walki z cyberzagrożeniem       | określa działania złośliwego oprogramowania                                                          | Test teoretyczny                    |
|                                                                          | przeprowadza ocenę poziomu zagrożenia własnych zabezpieczeń                                          | Test teoretyczny                    |
|                                                                          |                                                                                                      | Wywiad swobodny                     |
|                                                                          | projektuje rozwiązania dot. ochrony stacji komputerowych oraz pracy na przenośnych nośnikach pamięci | Test teoretyczny                    |
|                                                                          |                                                                                                      | Obserwacja w warunkach symulowanych |
|                                                                          | charakteryzuje się umiejętnością podejmowania decyzji pod wpływem stresu                             | Test teoretyczny                    |

# Kwalifikacje

## Kompetencje

Usługa prowadzi do nabycia kompetencji.

### Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji lub wyrażnie z nim powiązane inne dokumenty związane ze wsparciem zawierają opis efektów uczenia się?

TAK

Pytanie 2. Czy dokument lub wyrażnie 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 wyrażnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

TAK

## Program

### PROGRAM

#### Bądź bezpieczny w sieci - cyberbezpieczeństwo w praktyce - szkolenie

Szkolenie składa się z 2 dni szkoleniowych po 9h godzin dydaktycznych w tym 1 godzinę walidacji w postaci zdalnej w czasie rzeczywistym(45minut).

Szkolenie składa się z 17h dydaktycznych w formie stacjonarnej oraz 1 godziny dydaktycznej w formie zdalnej w czasie rzeczywistym tj. walidacji. 17h dydaktycznych są podzielone na 10 godzin teorii i 7 godzin praktyki.

**Szkolenie jest przeznaczone przede wszystkim dla osób chcących chronić dane firmy, rozpoznawać oszustwa np. w mediach społecznościowych oraz odpowiednio reagować na nie.** Uczestnicy powinni posiadać podstawową znajomość obsługi komputera.

### Warunki organizacyjne

- Uczestnicy podczas zajęć korzystają z **komputerów zapewnionych przez organizatora szkolenia**.
- Każdy uczestnik dysponuje własnym stanowiskiem komputerowym umożliwiającym samodzielną realizację ćwiczeń i praktycznych zadań.
- Komputery wyposażone są w podstawowe oprogramowanie biurowe, przeglądarki internetowe (**Google Chrome, Mozilla Firefox lub Safari**) oraz narzędzia niezbędne do realizacji ćwiczeń praktycznych z zakresu cyberbezpieczeństwa.

Podczas szkolenia uczestnicy będą wykonywać praktyczne ćwiczenia obejmujące:

- **Analiza przypadków zagrożeń** (malware, phishing, ransomware) – uczestnicy identyfikują rodzaje zagrożeń na przykładzie rzeczywistych scenariuszy.
- **Symulacje ataków cybernetycznych** – ćwiczenia polegające na rozpoznaniu, analizie oraz reakcji na symulowane ataki hakerskie.
- **Bezpieczne zarządzanie hasłami** – tworzenie oraz zarządzanie bezpiecznymi, silnymi hasłami z wykorzystaniem praktycznych narzędzi.
- **Planowanie i symulowanie reakcji na incydenty** – praktyczne warsztaty przygotowania planu reagowania na zagrożenia cyfrowe.
- **Praktyczna ochrona przed phishingiem** – ćwiczenia rozpoznawania prób wyłudzenia danych i manipulacji socjotechnicznych.
- **Ćwiczenia szyfrowania danych** – praktyczne wdrażanie szyfrowania plików, wiadomości e-mail i komunikacji firmowej.
- **Konfiguracja podstawowych zabezpieczeń sieciowych** – zajęcia praktyczne obejmujące ustawienia bezpieczeństwa sieci firmowej i domowej.

- **Wdrażanie polityki bezpieczeństwa** – ćwiczenia obejmujące zasady tworzenia dokumentacji i procedur bezpieczeństwa w przedsiębiorstwie.
  - **Bezpieczna obsługa urządzeń mobilnych** – warsztaty dotyczące ochrony smartfonów i tabletów używanych w pracy zawodowej.
- 

Dzień I

**Moduł 1.**

Zrozumienie podstawowych zasad bezpieczeństwa

Zagrożenia w sieci i ich wpływ na firmy MSP

**Moduł 2.**

Podstawowe terminy i koncepcje (np. malware, phishing, ransomware)

Znaczenie higieny cyfrowej w kontekście biznesowym

Dzień II

**Moduł 3.**

Hasła i zarządzanie nimi, Przygotowanie planu reagowania na incydenty

Zaawansowana ochrona przed złośliwym oprogramowaniem,

Bezpieczne korzystanie z Internetu i e-maila,

**Moduł 4.**

Ochrona przed phishingiem i innymi formami socjotechniki

Podstawy bezpiecznej pracy zdalnej

Szyfrowanie danych i komunikacji

Bezpieczeństwo sieci firmowych i domowych

**Moduł 5.**

Wprowadzenie do bezpieczeństwa urządzeń mobilnych

Tworzenie i wdrażanie polityki bezpieczeństwa w firmie

Symulacje ataków cybernetycznych i reakcje

**W trakcie walidacji online korzystamy z platformy Zoom.** Każdy uczestnik otrzymuje przed szkoleniem link do platformy internetowej (na wskazany adres mailowy), na której znajdować się będzie test online. Uczestnictwo w streamingu nie wymaga żadnych, specjalnych oprogramowań: wystarczy, że komputer jest podłączony do Internetu (należy korzystać z przeglądarek: Google Chrome, Mozilla Firefox lub Safari). Link do walidacji online generowany jest przed szkoleniem i ważny jest przez cały czas trwania walidacji.

**Czas trwania szkolenia:**

Czas trwania szkolenia: 18h dydaktycznych (w tym 1h walidacji)= 13,5h zegarowe

Czas trwania 1h szkoleniowej: 45 minut.

**Walidacja:**

Podsumowaniem szkolenia jest przeprowadzenie procesu walidacji w formie testu teoretycznego przeprowadzonego w formie zdalnej w czasie rzeczywistym oraz wywiadu swobodnego i obserwacji w warunkach symulowanych również w formie zdalnej w czasie rzeczywistym.

W ramach części teoretycznej uczestnicy będą musieli wypełnić testy jedno/wielokrotnego wyboru. Warunkiem zaliczenia części teoretycznej jest uzyskanie minimum 80% prawidłowych odpowiedzi.

*Walidator nie bierze udziału w części edukacyjnej.*

Test teoretyczny, mający na celu sprawdzenie poziomu wiedzy, będzie trwał 30 minut. Będzie przeprowadzony dla wszystkich Uczestników jednocześnie. Druga walidacja odbędzie się za pomocą obserwacji w warunkach symulowanych i będzie trwała około 10 minut na jednego Uczestnika (10 uczestników x 10 minut = 100 minut), oraz ostatnia walidacja będzie wywiadem swobodnym i będzie trwała około 5 minut na jednego uczestnika ( 10 Uczestników x 5 minut = 50 minut).

*W Karcie Usługi określony jest czas trwania walidacji dla jednego uczestnika . Pozostali uczestnicy będą walidowani po zakończeniu części praktycznej usługi, co oznacza, że dodatkowy czas na walidację po szkoleniu nie wlicza się w czas trwania usługi.*

Osoba walidująca waliduje usługę po jej zakończeniu, a następnie potwierdza osiągnięcie efektów kształcenia swoim podpisem na certyfikacie.

Dokładny czas walidacji dla poszczególnych osób, będzie dostępny u Dostawcy Usług.

- Usługa rozwojowa nie jest świadczona przez podmiot pełniący funkcję Operatora lub Partnera Operatora w danym projekcie PSF lub w którymkolwiek Regionalnym Programie lub FERS albo przez podmiot powiązany z Operatorem lub Partnerem kapitałowo lub osobowo.
- Usługa rozwojowa nie jest świadczona przez podmiot będący jednocześnie podmiotem korzystającym z usług rozwojowych o zbliżonej tematyce w ramach danego projektu.
- Usługa rozwojowa nie obejmuje wzajemnego świadczenia usług w projekcie o zbliżonej tematyce przez Dostawców usług, którzy delegują na usługi siebie oraz swoich pracowników i korzystają z dofinansowania, a następnie świadczą usługi w zakresie tej samej tematyki dla Przedsiębiorcy, który wcześniej występował w roli Dostawcy tych usług.
- Cena usługi nie obejmuje kosztów niezwiązanych bezpośrednio z usługą rozwojową, w szczególności kosztów środków trwałych przekazywanych Przedsiębiorcom lub Pracownikom przedsiębiorcy, kosztów dojazdu i zakwaterowania.

W ciągu dnia szkoleniowego są wprowadzone trzy przerwy, które nie wliczają się w czas trwania usługi.

# Harmonogram

Liczba pozycji harmonogramu: 1

| Przedmiot / temat                                              | Prowadzący            | Data realizacji zajęć | Godzina rozpoczęcia | Godzina zakończenia | Liczba godzin |
|----------------------------------------------------------------|-----------------------|-----------------------|---------------------|---------------------|---------------|
| <div>1 z 1</div> Zrozumienie podstawowych zasad bezpieczeństwa | Agnieszka Poniatowska | 14-05-2026            | 08:30               | 10:00               | 01:30         |

# Cennik

## Cennik

| Rodzaj ceny                               | Cena         |
|-------------------------------------------|--------------|
| Koszt przypadający na 1 uczestnika brutto | 5 000,00 PLN |

|                                          |              |
|------------------------------------------|--------------|
| Koszt przypadający na 1 uczestnika netto | 5 000,00 PLN |
| Koszt osobogodziny brutto                | 277,78 PLN   |
| Koszt osobogodziny netto                 | 277,78 PLN   |

## Prowadzący

Liczba prowadzących: 1



1 z 1

### Agnieszka Poniatowska

od 2019 - 2023 - Trener w Centrum Szkoleniowym MS Szkolenia Marlena Sobieska - Ciesielska

#### ZAKRES SZKOLEŃ:

warsztaty umiejętności psychospołecznych  
 szkolenia trenerskie dla liderów  
 budowanie autorytetu trenera  
 szkolenie z umiejętności i technik trenerskich  
 budowanie motywacji i zarządzanie zaangażowaniem pracowników  
 szkolenia interpersonalne i kursy umiejętności osobistych  
 szkolenia z zakresu rynku pracy  
 stres, zmęczenie i wypalenie zawodowe  
 pracownik administracyjno - biurowy  
 kurs komputerowy - obsługa komputera oraz pakietu Microsoft Office: (600h)  
 Word,  
 Excel,  
 PowerPoint,  
 Access,  
 Publisher,  
 Outlook,  
 OneNote  
 Rozwiązywanie problemów  
 IT Security  
 negocjacje

## Informacje dodatkowe

### Informacje o materiałach dla uczestników usługi

Notatnik, długopis

Prezentacja w formie multimedialnej zostanie wysłana na e-mail Uczestników.

### Informacje dodatkowe

Szkolenie trwa 18 godzin dydaktyczne w tym walidacja trwa 45minut.

Szkolenie składa się z 17h dydaktycznych w formie stacjonarnej oraz 1 godziny dydaktycznej w formie zdalnej w czasie rzeczywistym tj. walidacji.

**Szkolenie odbywa się w godzinach dydaktycznych, czyli 1 godzina szkolenia równa się 45 minut.**

**W ciągu szkolenia zostały uwzględnione 3 przerwy które nie są wliczane do czasu trwania usługi.**

Koszt szkolenia nie zawiera kosztów dojazdu, wyżywienia i noclegu.

Podstawą do rozliczenia usługi jest wygenerowany z systemu raport umożliwiający identyfikację wszystkich uczestników na walidacji oraz zastosowanego narzędzia.

Uczestnik szkolenia otrzyma zaświadczenie o ukończeniu szkolenia dopiero po pozytywnym wyniku walidacji, który odbędzie się na ostatnich zajęciach. Warunkiem otrzymania zaświadczenia o ukończeniu szkolenia jest pozytywny wynik walidacji końcowej.

## Adres

ul. Maurycego Mochnackiego 10/1

10-037 Olsztyn

woj. warmińsko-mazurskie

Szkolenie będzie realizowane w firmie Centrum Nauka Jazdy

## Udogodnienia w miejscu realizacji usługi

- Klimatyzacja
- Wi-fi

## Kontakt



**KLAUDIA ZEJER**

**E-mail** k.zejer@centrum-osk.pl

**Telefon** (+48) 664 265 725