



J.G.Training  
JADWIGA GWÓŹDŹ

★★★★☆ 4,3 / 5

157 ocen

## Cyberbezpieczeństwo w pracy biurowej – jak chronić siebie i organizację w erze cyfrowych zagrożeń

Numer usługi 2026/01/19/26471/3268527

📍 zdalna w czasie rzeczywistym

🏠 Usługa szkoleniowa

🕒 6 h

📅 27.02.2026 do 27.02.2026

971,70 PLN brutto

790,00 PLN netto

161,95 PLN brutto/h

131,67 PLN netto/h

## Informacje podstawowe

|                                        |                                                                                                                                                                                                                                                                 |
|----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Kategoria</b>                       | Prawo i administracja / Ochrona informacji niejawnych                                                                                                                                                                                                           |
| <b>Grupa docelowa usługi</b>           | <ul style="list-style-type: none"><li>• Pracownicy sektora publicznego, samorządu i administracji publicznej</li><li>• Pracownicy biurowi</li><li>• Specjaliści niższego i wyższego szczebla</li></ul> <p>Wiedza wstępna oraz doświadczenie nie są wymagane</p> |
| <b>Minimalna liczba uczestników</b>    | 5                                                                                                                                                                                                                                                               |
| <b>Maksymalna liczba uczestników</b>   | 30                                                                                                                                                                                                                                                              |
| <b>Data zakończenia rekrutacji</b>     | 20-02-2026                                                                                                                                                                                                                                                      |
| <b>Forma prowadzenia usługi</b>        | zdalna w czasie rzeczywistym                                                                                                                                                                                                                                    |
| <b>Liczba godzin usługi</b>            | 6                                                                                                                                                                                                                                                               |
| <b>Podstawa uzyskania wpisu do BUR</b> | Standard Usługi Szkoleniowo-Rozwojowej PIFS SUS 2.0                                                                                                                                                                                                             |

## Cel

### Cel edukacyjny

Usługa „Cyberbezpieczeństwo w pracy biurowej – jak chronić siebie i organizację w erze cyfrowych zagrożeń” przygotowuje do identyfikowania zagrożeń cybernetycznych, bezpiecznego korzystania z poczty elektronicznej, sieci i urządzeń mobilnych oraz stosowania zasad ochrony danych i cyberhigieny w pracy biurowej i poza nią.

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

| Efekty uczenia się                                                   | Kryteria weryfikacji                                                      | Metoda walidacji                                      |
|----------------------------------------------------------------------|---------------------------------------------------------------------------|-------------------------------------------------------|
| Identyfikuje podstawowe rodzaje cyberzagrożeń biurowych.             | Wskazuje poprawne definicje phishingu, malware i ataku socjotechnicznego. | Test teoretyczny z wynikiem generowanym automatycznie |
| Klasyfikuje zasady bezpiecznego korzystania z poczty, sieci i haseł. | Wybiera poprawne działania zwiększające bezpieczeństwo haseł.             | Test teoretyczny z wynikiem generowanym automatycznie |
|                                                                      | Wskazuje bezpieczne zachowania przy korzystaniu z Wi-Fi i e-mail.         | Test teoretyczny z wynikiem generowanym automatycznie |

## Kwalifikacje

### Kompetencje

Usługa prowadzi do nabycia kompetencji.

#### Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji zawiera opis efektów uczenia się?

TAK

Pytanie 2. Czy dokument potwierdza, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji?

TAK

Pytanie 3. Czy dokument potwierdza zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

TAK

## Program

1. Wprowadzenie tematu szkolenia – rola cyberbezpieczeństwa w szybko zmieniającym się świecie

- Definicja cyberbezpieczeństwa
- Rola cyberbezpieczeństwa w szybko zmieniającym się świecie
- Rodzaje zagrożeń

1. Identyfikowanie ataków cyfrowych

- „Pomyśl zanim klikniesz” – rodzaje ataków hackerskich skierowane na pracowników biurowych
- Kampanie Phishingowe
- Przykłady z życia – zasady i wskazówki

1. Podstawy cyberbezpieczeństwa podczas podróży służbowych

- Przykłady ataków na urządzenia mobilne, m.in. wiadomość o dopłacie do przesyłki czyli rodzaj ataku w czasie rzeczywistym
- Jak bezpiecznie przysyłać dane wrażliwe
- Bezpieczne korzystanie z sieci bezprzewodowych – WI-FI. Rodzaje ataków z wykorzystaniem na sieci bezprzewodowe

1. Bezpieczne korzystanie z poczty elektronicznej – zasady i wskazówki

- Sprawdzanie i analiza wiadomości email

- Czym są linki skrócone i jak je rozwinąć
- Jak szyfrować pliki

#### 1. Bezpieczeństwo haseł

- Budowa haseł
- Mnemotechniki
- Przechowywanie haseł
- Bezpieczniejsze metody logowania
- Praktyczne wskazówki dla użytkowników

#### 1. Bankowość elektroniczna – kierunki i trendy autoryzacji transakcji

#### 2. Profil zaufany a kwalifikowany podpis cyfrowy

#### 3. Przykłady kradzieży danych oraz wycieku

- Do czego cyberprzestępcy mogą wykorzystać nasze dane
- Do czego może doprowadzić zgubiony pendrive, tj. kradzież tożsamości
- Czym jest „Cebulka”, czyli handel danymi w sieci

#### 1. Podśluchy w XXI wieku – prezentacja gadżetów umożliwiających podsłuch, nagrywanie obrazu czy odczyt kart bankomatowych, czyli na co zwrócić uwagę, aby nie zostać nagrany przez petenta

#### 2. Skutki cyberataku. Reputacja przychodzi piechotą, a odjeżdża Ferrari, czyli straty wynikające z udanego ataku na organizacje – przykłady z życia

#### 3. Gdzie szukać informacji związanych z bezpieczeństwem w sieci w celu zminimalizowania ryzyka ataku

#### 4. Cyberhigiena w sieci, czyli zbiór zasad i reguł postępowania dla pracowników biurowych zarówno w życiu zawodowym jak i prywatnym

#### 5. Dyskusje, odpowiedzi na pytania uczestników, podsumowanie szkolenia

#### 6. Walidacja

Usługa jest realizowana w godzinach zegarowych. W harmonogramie nie wyszczególniono przerw. Przerwy łącznie wyniosą 60 minut.

## Harmonogram

Liczba przedmiotów/zajęć: 2

| Przedmiot / temat zajęć                                                                                            | Prowadzący | Data realizacji zajęć | Godzina rozpoczęcia | Godzina zakończenia | Liczba godzin |
|--------------------------------------------------------------------------------------------------------------------|------------|-----------------------|---------------------|---------------------|---------------|
| <div>1 z 2</div> Cyberbezpieczeństwo w pracy biurowej – jak chronić siebie i organizację w erze cyfrowych zagrożeń | wykładowca | 27-02-2026            | 10:00               | 15:50               | 05:50         |
| <div>2 z 2</div> Walidacja                                                                                         | -          | 27-02-2026            | 15:50               | 16:00               | 00:10         |

## Cennik

### Cennik

| Rodzaj ceny | Cena |
|-------------|------|
|-------------|------|

|                                           |            |
|-------------------------------------------|------------|
| Koszt przypadający na 1 uczestnika brutto | 971,70 PLN |
| Koszt przypadający na 1 uczestnika netto  | 790,00 PLN |
| Koszt osobogodziny brutto                 | 161,95 PLN |
| Koszt osobogodziny netto                  | 131,67 PLN |

## Prowadzący

Liczba prowadzących: 1



1 z 1

### wykładowca

Specjalista ds. ochrony informacji niejawnych, biznesowych oraz osobowych od 2020 roku.

Pełnił rolę Inspektora Ochrony Danych Osobowych oraz funkcję Pełnomocnika Prezesa Zarządu ds. Ochrony Informacji Niejawnych. Były kurator zawodowy.

Ekspert szkolony przez Agencję Bezpieczeństwa Wewnętrznego w zakresie ochrony informacji niejawnych NATO, Unii Europejskiej, Europejskiej Agencji Kosmicznej oraz ochrony informacji niejawnych w systemach teleinformatycznych.

Wykładowca na szkoleniach i warsztatach. Prelegent na konferencjach i kongresach. Autor licznych artykułów branżowych.

Zdobył doświadczenie w ostatnich 5 latach

## Informacje dodatkowe

### Informacje o materiałach dla uczestników usługi

Uczestnicy online – materiały w wersji elektronicznej (pliki udostępnione dzień po szkoleniu).

### Informacje dodatkowe

W przypadku dofinansowania usługi w minimum 70% ze środków publicznych zostanie zastosowane zwolnienie z VAT. Podstawa zwolnienia z VAT: Usługa podlega zwolnieniu z podatku od towarów i usług na podstawie §3 pkt 1,14 rozporządzenia Ministra Finansów z 20 grudnia 2013 roku w sprawie zwolnień od podatku od towarów i usług oraz warunków stosowania tych zwolnień (t. jedn.Dz. U. z 2020 r., po. 1983.).

## Warunki techniczne

Szkolenie odbywa się na platformie ZOOM. Niezbędnymi wymaganiami sprzętowymi jest komputer z dostępem do Internetu. Minimalna prędkość łącz sieciowego to 512 KB/sek. Nie jest konieczna instalacja na komputerze specjalnego oprogramowania - wystarczy aktualna wersja przeglądarki Google Chrome bądź Mozilla Firefox. Linki do połączenia na szkolenie są ważne jedynie w czasie jego trwania.

Pozostałe wymagania: Procesor dwurdzeniowy 2GHz lub lepszy (zalecany czterordzeniowy); 2GB pamięci RAM (zalecane 4GB lub więcej); System operacyjny taki jak Windows 8 (zalecany Windows 10), Mac OS wersja 10.13 (zalecana najnowsza wersja), Linux, Chrome OS. Łącze internetowe o minimalnej przepustowości do zapewnienia transmisji dźwięku 512Kb/s, zalecane min. 2 Mb/s oraz min. 1 Mb/s do zapewnienia transmisji łącznie dźwięku i wizji, zalecane min. 2,5 Mb/s.

## Kontakt



**Katarzyna Jędrzejewska**

**E-mail** [szkolenia@jgt.pl](mailto:szkolenia@jgt.pl)

**Telefon** (+48) 228 455 253