Możliwość dofinansowania

CYBERBEZPIECZEŃSTWO W SYSTEMACH ZABEZPIECZEŃ TECHNICZNYCH

Numer usługi 2025/06/01/117343/2785883

3 259,50 PLN brutto
2 650,00 PLN netto
116,41 PLN brutto/h
94,64 PLN netto/h

ZAKŁAD ROZWOJU TECHNICZNEJ OCHRONY MIENIA TECHOM SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

4,8 / 5

467 ocen

zdalna w czasie rzeczywistym
Usługa szkoleniowa
28 h
19.11.2025 do 21.11.2025

Informacje podstawowe

Kategoria	Techniczne / Pozostałe techniczne
Grupa docelowa usługi	**Szkolenie przeznaczone jest dla osób pełniących / przygotowywanych do pełnienia funkcji m.in.:** • projektantów, instalatorów, konserwatorów i administratorów systemów zabezpieczeń technicznych – pracowników zabezpieczenia technicznego • koordynatorów projektów systemów zabezpieczenia technicznego • osób zarządzających bezpieczeństwem obiektów • menedżerów, specjalistów, konsultantów ds. cyberbezpieczeństwa, zarzadzania bezpieczeństwem informacji • osób zajmujących się ochroną infrastruktury krytycznej • pracowników operatorów usług kluczowych oraz dostawców usług cyfrowych odpowiedzialnych za wdrożenia systemu zarzadzania bezpieczeństwem • prawników obsługujących projekty dot. cyberbezpieczeństwa • administratorów sieci • szefów sekcji ochrony obiektów, administratorów systemów alarmowych, komendantów ochrony, osób nadzorujących i użytkujących systemy zabezpieczeń w jednostkach wojskowych
Minimalna liczba uczestników	1
Maksymalna liczba uczestników	30
Data zakończenia rekrutacji	18-11-2025
Forma prowadzenia usługi	zdalna w czasie rzeczywistym

Liczba godzin usługi	28
Podstawa uzyskania wpisu do BUR	Standard Usługi Szkoleniowo-Rozwojowej PIFS SUS 2.0

Cel

Cel edukacyjny

Szkolenie w zakresie cyberbezpieczeństwa w systemach zabezpieczeń technicznych umożliwia przygotowanie teoretyczne do projektowania i instalowania systemów zabezpieczeń technicznych z uwzględnieniem aktualnej wiedzy technicznej w zakresie cyberbezpieczeństwa.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Charakteryzuje pojęcia z zakresu cyberbezpieczeństwa z naciskiem na obszar systemów zabezpieczeń technicznych	Wskazuje definicje podstawowych pojęć z zakresu cyberbezpieczeństwa oraz odnosi je do systemów zabezpieczeń technicznych	Test teoretyczny
Definiuje podstawowe wymagania dotyczące systemu zarządzania bezpieczeństwem informacji według norm ISO/IEC 27000	Wskazuje kluczowe wymagania norm ISO/IEC 27001 oraz zasady ich wdrażania w organizacji	Test teoretyczny
Definiuje podstawowe wymagania dotyczące szacowania ryzyka dla systemów zabezpieczeń technicznych	Wskazuje etapy procesu szacowania ryzyka i identyfikuje metody oceny ryzyka	Test teoretyczny
Identyfikuje i grupuje wartości aktywów	Rozróżnia rodzaje aktywów oraz przypisuje je do odpowiednich kategorii	Test teoretyczny
Kategoryzuje zagrożenia i podatności aktywów	Dobiera przykładowe zagrożenia i podatności do wybranych aktywów	Test teoretyczny
Identyfikuje i wartościuje zagrożenia oraz ataki, a także techniki wykorzystywania słabości bezpieczeństwa;	Rozróżnia rodzaje zagrożeń i przyporządkowuje je do odpowiednich kategorii ataków	Test teoretyczny
Dobiera i uzasadnia metody zarządzania incydentami bezpieczeństwa informacji	Wskazuje działania podejmowane w odpowiedzi na różne scenariusze incydentów	Test teoretyczny
Omawia zasady klasyfikacji i kwalifikacji zdarzeń jako incydentów bezpieczeństwa	Charakteryzuje kryteria kwalifikacji zdarzenia jako incydentu	Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Charakteryzuje współczesne rozwiązania bezpieczeństwa sieciowego dla systemów zabezpieczeń technicznych	Wskazuje cechy i funkcje podstawowych rozwiązań bezpieczeństwa sieciowego	Test teoretyczny
Charakteryzuje rodzaje testów penetracyjnych	Rozróżnia podstawowe rodzaje testów penetracyjnych oraz ich zastosowanie	Test teoretyczny
Definiuje podstawowe mechanizmy funkcjonowania systemu cyberbezpieczeństwa	Wskazuje zależności między elementami systemu cyberbezpieczeństwa i ich wpływem na bezpieczeństwo	Test teoretyczny
Charakteryzuje podstawowe pojęcia formalnoprawne z zakresu cyberbezpieczeństwa	Wskazuje akty prawne regulujące obszar cyberbezpieczeństwa i opisuje ich podstawowe założenia	Test teoretyczny
Analizuje zjawiska i zagrożenia cyberbezpieczeństwa oraz identyfikuje narzędzia wspomagające podejmowanie decyzji	Dobiera odpowiednie narzędzia do rodzaju zagrożenia lub potrzeby analizy	Test teoretyczny

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

Aspekty techniczno-organizacyjne:

1. Z uwagi na zdalną formułę kursu uczestnik powinien zapewnić sobie dogodne warunki odbywania kursu: samodzielne stanowisko komputerowe. Zaleca się odbywania kursu w oddzielnym pomieszczeniu, które ogranicza dystraktory zewnętrzne.

2. Zaleca się, aby uczestnicy szkolenia powtarzali materiał kursowy po każdym dniu zajęć w oparciu o udostępnione na serwerze TECHOM materiały.

3. Usługa jest realizowana w godzinach dydaktycznych.

Elementy szkoleniowe:

Kurs będzie prowadzony w czasie rzeczywistym na platformie Microsoft Teams. Wszystkie zajęcia są prowadzone z bezpośrednim kontaktem między wykładowcą, a kursantem co umożliwia użycie elementów szkoleniowych takich jak: rozmowa na żywo, chat oraz współdzielenie ekranu. Większość zajęć będzie stosowała wykład z prezentacją jako metodę nauczania.

Harmonogram

Liczba przedmiotów/zajęć: 0

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
Brak wyników.					

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	3 259,50 PLN
Koszt przypadający na 1 uczestnika netto	2 650,00 PLN
Koszt osobogodziny brutto	116,41 PLN
Koszt osobogodziny netto	94,64 PLN

Prowadzący

Liczba prowadzących: 3

1 z 3

Mateusz Zapotoczny

Mgr informatyki, po Uniwersytecie Zielonogórskim. Od 15 lat w branży IT i systemów zabezpieczeń technicznych. Posiada rozległe doświadczenie w zakresie systemów telewizji dozorowej i cyberbezpieczeństwa. Pracował na kierowniczych stanowiskach (w działach technicznych) w wiodących firmach produkujących systemy zabezpieczeń technicznych. Jako pasjonat specjalizuje się w zakresie doboru rozwiązań sprzętowych, integracji i cyberbezpieczeństwa. Jest doświadczonym szkoleniowcem, o szerokim uznaniu.

2 z 3

Łukasz Lik

Mgr inż. elektrotechniki w specjalności automatyka i technika mikroprocesorowa - Politechnika Białostocka. Doświadczony instalator i projektant systemów zabezpieczeń technicznych. Od 2016 roku jest Dyrektorem Technicznym w wiodących firmach zajmujących się produkcją i dostarczaniem nowoczesnych rozwiązań w zakresie systemów telewizji dozorowej IP. Uznany specjalista w branży bezpieczeństwa i trener z zakresu swoich kompetencji; prowadzi szkolenia od wielu lat.

3 z 3

Piotr Rogalewski

Obecny w branży zabezpieczeń technicznych od 2000 r., aktualnie w dziale technicznym największego producenta telewizji dozorowej na świecie, odpowiedzialny m.in. za bezpieczeństwo cybernetyczne Przez kilkadziesiąt lat zatrudniony u wiodących dystrybutorów i producentów (Honeywell, ADI, Samsung, Hanwha) Członek stowarzyszenia Polalarm Audytor wewnętrzny IEC/ISO 27001 Zarządzania Bezpieczeństwem Informacji (BSI) Współautor koncepcji technicznych i założeń projektowych oraz konsultant wykonawczy wielu systemów monitoringu wizyjnego dla obiektów NATO oraz obiektów infrastruktury krytycznej na terenie RP i w krajach bałtyckich Współautor koncepcji technicznej największego w Polsce miejskiego systemu monitoringu wizyjnego (Miasto Stołeczne Warszawa) oraz autor oprogramowania wykonawczego dla krosownic wizyjnych , a także dla ich późniejszej integracji z nowym systemem cyfrowym Programista C / C++, C#, Python, PHP, Visual Basic, HTML/CSS, JavaScript, jQuery z ponad 15-letnim doświadczeniem w implementacji API i SDK producentów zabezpieczeń technicznych Projektant i programista relacyjnych baz danych SQL, głównie w systemach integrujących zabezpieczenia techniczne Programista sztucznych sieci neuronowych, algorytmów uczenia maszynowego oraz modeli rozwojowych AI (Tensor Flow, Keras, OpenCV, PyTorch) Posiada min. dwuletnie doświadczenie zawodowe w prowadzeniu szkoleń z obszaru projektowania, instalowania i konserwacji technicznych systemów zabezpieczeń dla wskazanej Grupy docelowej

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Materiały z kursu będą udostępnione wszystkim uczestnikom na serwerze TECHOM - w trakcie kursu.

Materiały są przekazywane w formie prezentacji i konspektów.

Usługa realizowane będzie zgodnie ze Standardem Usług Zdalnego Uczenia się (ZUS), które stanowi Załącznik Nr 5 do Regulaminu BUR.

Usługa jest nagrywana i może być udostępniona PARP lub podmiotowi wskazanemu przez PARP, np. prowadzącemu audyt. Nagranie usługi nie jest udostępniane uczestnikom.

Kurs, poza trenerami wymienionymi powyżej, mogą prowadzić również inni trenerzy, np. w zastępstwie. Informacja o innych trenerach będzie udostępniona niezwłocznie uczestnikom oraz administracji BUR i innym podmiotom zainteresowanym.

Charakterystyka testu:

- Test jest jednokrotnego wyboru i będzie realizowany w formularzu google.
- Test jest ustandaryzowany, przygotowany przez ekspertów.
- Liczba pytań testowych zmienia się nieznacznie z kursu na kurs (przewiduje się około 20 pytań).
- Test składa się z pytań odnoszących się do wszystkich kryteriów weryfikacji, które są opisane powyżej, we właściwej rubryce.
- Test prowadzi osoba prowadząca walidację.
- Test jest prowadzony na końcu kursu.

UWAGA: Po usłudze rozwojowej przewiduje się jeden test składający się z pytań odnoszących się do wszystkich kryteriów weryfikacji (nie przewiduje się rozłącznych testów odnoszących się do różnych kryteriów weryfikacji).

Warunki uczestnictwa

Aby uczestniczyć w kursie należy posiadać wykształcenie minimum zawodowe lub średnie.

UWAGA:

Udział w usłudze rozwojowej na poziomie frekwencji nie może być mniejszej niż 80%.

Informacje dodatkowe

Po kursie uczestnicy otrzymują:

1. Bezterminowe zaświadczenia o ukończeniu szkolenia.

Usługa realizowana będzie zgodnie ze Standardem Usług Zdalnego Uczenia się (ZUS), które stanowi Załącznik Nr 5 do Regulaminu BUR

Warunki techniczne

Kurs odbywa się w formie zdalnej w czasie rzeczywistym przez aplikację **Microsoft TEAMS**, która jest darmowa.

Zalecamy ściągnięcie i zainstalowanie aplikacji na komputerze. Można też uruchomić aplikację przez przeglądarkę internetową (zalecana przeglądarka: **Google Chrome**), ale ta alternatywa jest mniej stabilna.

Niezbędne jest również posiadanie:

- **programu do przeglądania plików pdf** (warunki spełnia dowolny darmowy program)
- **programów: Word, Excel i Power Point**

Zalecane (ale nie niezbędne) jest posiadanie programu **AutoCAD** (nie ma konieczności otwierania tych plików w trakcie zajęć - są one przeznaczone do wykorzystania przez uczestników kursu w pracy zawodowej).

Zalecenia techniczne:

- Stabilne łącze internetowe (wystarcza 10 Mbit/s download oraz 2 Mbit/s upload)
- Komputer z systemem Windows 7 lub wyższym
- Uwaga: nie ma szczególnych wymagań dot. parametrów komputera - sprzętowo kwalifikuje się każdy komputer, który posiada zintegrowaną (lub nie) kartę dźwiękową, i na którym jest zainstalowany system Windows 7 lub wyższy
- Sprawne głośniki lub słuchawki (zaleca się sprawdzenie, czy sprzęt działa w aplikacji MS TEAMS przed rozpoczęciem szkolenia)
- Sprawny mikrofon oraz kamera (zaleca się sprawdzenie, czy sprzęt działa w aplikacji MS TEAMS przed rozpoczęciem szkolenia)
- Zaleca się także zorganizowanie drugiego monitora, co ułatwiłoby pracę w trakcie niektórych zajęć, ale podział ekranu powinien wystarczyć do realizacji celu szkolenia.

Link do kursu będzie udostępniony uczestnikom najpóźniej 1 dzień roboczy przed rozpoczęciem szkolenia. Link będzie aktywny dla wszystkich zapisanych na kurs. Link wygasa po zakończeniu kursu.

Kontakt

Adam Tatarowski

E-mail tatarowski@techom.com
Telefon (+48) 601 248 728