Możliwość dofinansowania

ZAKŁAD ROZWOJU TECHNICZNEJ OCHRONY MIENIA TECHOM SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

4,8 / 5

488 ocen

Kurs pracownika zabezpieczenia technicznego w zakresie projektowania, instalowania, konserwacji, odbiorów i eksploatacji technicznych systemów zabezpieczeń do stopni 1-4/wojskowych dokumentów normatywnych

Numer usługi 2026/05/29/117343/3595204

- Usługa szkoleniowa
- zdalna w czasie rzeczywistym
- Zajęcia grupowe
- 32:00 h
- 15.06.2026 do 19.06.2026

3 450,00 PLN brutto
3 450,00 PLN netto
107,81 PLN brutto/h
107,81 PLN netto/h
200,00 PLN cena rynkowa

Informacje podstawowe

Kategoria	Techniczne / Budownictwo i projektowanie
Grupa docelowa usługi	• Projektanci, instalatorzy i konserwatorzy systemów zabezpieczeń technicznych (lub innych systemów niskoprącowych, np. systemów ochrony przeciwpożarowej, automatyki) • Koordynatorzy projektów • Inwestorzy • Osoby zarządzające bezpieczeństwem obiektów • Osoby zajmujące się ochroną infrastruktury krytycznej • Administratorzy systemów zabezpieczeń technicznych • Kwalifikowani pracownicy zabezpieczenia technicznego • Inspektorzy nadzoru • Inspektorzy ochrony przeciwpożarowej • Inżynierowie i technicy pożarnictwa • Pracownicy przedsiębiorstw działających w branży budowlanej W szczególności osoby zainteresowane uzyskaniem: • wpisu na listę kwalifikowanych pracowników zabezpieczenia technicznego • możliwości realizacji usług w zakresie systemów zabezpieczeń w obiektach podległych lub nadzorowanych przez MON, a także w infrastrukturze krytycznej • certyfikatu zgodnie z PN-EN 16763 Usługi w zakresie systemów ochrony przeciwpożarowej i systemów zabezpieczeń technicznych
Minimalna liczba uczestników	2
Maksymalna liczba uczestników	30
Forma prowadzenia usługi	zdalna w czasie rzeczywistym

Cel

Cel edukacyjny

Udział w kursie pracownika zabezpieczenia technicznego w zakresie projektowania, instalowania i konserwacji technicznych systemów zabezpieczeń do stopni 1-4/wojskowych dokumentów normatywnych przygotowuje do realizacji usług w zakresie projektowania, instalowania i konserwacji systemów zabezpieczeń. Co więcej, ukończenie kursu umożliwia ubieganie się o uzyskanie wpisu na listę kwalifikowanych pracowników zabezpieczenia technicznego zgodnie z art. 27 Ustawy o ochronie osób i mienia.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Charakteryzuje wymagania prawno-normatywne w zakresie systemów zabezpieczeń technicznych	A. identyfikuje wymagania prawne, normy oraz wytyczne do ich stosowania w zakresie systemów zabezpieczeń technicznych, B. rozróżnia stopnie zabezpieczenia wynikające z norm, C. identyfikuje wymagania wojskowych dokumentów normatywnych, D. identyfikuje wymagania w zakresie audytowania systemów zabezpieczeń technicznych, E. rozróżnia audyt i certyfikację zainstalowanych systemów zabezpieczeń, F. identyfikuje wymagania związane z procesem certyfikacji na zgodność z normą PN-EN 16763, G. identyfikuje wymagania związane z procesem certyfikacji na zgodność z normami dotyczącymi urządzeń i systemów.	Test teoretyczny
Charakteryzuje proces szacowania ryzyka bezpieczeństwa obiektów prowadzony zgodnie z wymaganiami prawno-normatywnymi	A. identyfikuje proces szacowania ryzyka bezpieczeństwa obiektów, B. klasyfikuje obiekty z punktu widzenia szacowania ryzyka, C. wskazuje typowe zagrożenia i podatności dla różnego rodzaju obiektów chronionych, D. opisuje potencjalne skutki wystąpienia typowych zagrożeń, E. wskazuje środki redukcji ryzyka adekwatne do zagrożeń.	Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Charakteryzuje systemy zabezpieczeń technicznych oraz ich zastosowanie	A. rozróżnia elementy składowe systemów zabezpieczeń technicznych, ich funkcje oraz zasady działania, B. identyfikuje zasady klasyfikacji jakości obrazu zgodnie z PN-EN 62676-4, C. identyfikuje metody badawcze weryfikacji jakości obrazu zgodnie z PN-EN 62676-5, D. wskazuje metody albo systemy związane z bezpieczeństwem zapisu i backupu danych, E. identyfikuje zależności pomiędzy parametrami technicznymi i ich przełożenie na jakość nagrań i materiału dowodowego, F. charakteryzuje dobre praktyki w zakresie zapewniania niezakłóconego działania systemów zabezpieczeń technicznych zgodnie z ich przeznaczeniem (np. problem fałszywych alarmów), G. identyfikuje wymagania dotyczące systemów transmisji alarmu, H. identyfikuje standardy transmisji danych w systemach kontroli dostępu i dobre praktyki w tym zakresie, I. identyfikuje wymagania, ograniczenia i możliwości integracji z innymi systemami (np. systemami ochrony przeciwpożarowej, BMS, systemami antydronowymi, itp.), J. rozróżnia zakresy integracji pod względem technicznym i prawnym, K. wskazuje na możliwości platform PSIM.	Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Charakteryzuje zasady projektowania, instalowania, konserwacji, odbioru i eksploatacji systemów zabezpieczeń technicznych dla stopni 1-4 i wojskowych dokumentów normatywnych	wskazuje wymagania w zakresie stopni zabezpieczenia określonych w normach PN-EN 50131-1, PN-EN 60839-11-1, PN-EN 62676-1 i wytycznych do ich stosowania, B. identyfikuje wymagania PN-EN 16763 w zakresie projektowania, instalowania, konserwacji, odbioru i eksploatacji systemów zabezpieczeń technicznych, C. określa zakres czynności dla projektowania, instalowania, konserwacji, odbioru i eksploatacji systemów zabezpieczeń technicznych, uwzględniając wymagania: PN-EN 16763, odpowiednich stopni zabezpieczenia określonych w PN-EN 50131-1, PN-EN 60839-11-1, PN-EN 62676-1 i wojskowych dokumentów normatywnych, D. rozróżnia wymagania w zakresie projektowania, instalowania, konserwacji, odbioru i eksploatacji systemów zabezpieczeń technicznych dla sfery cywilnej i wojskowej, E. opisuje zasady przygotowywania dokumentacji technicznej projektowej, wykonawczej, powykonawczej, F. określa zakres dokumentacji technicznej dotyczącej systemów G. identyfikuje wymagania w zakresie wystawiania deklaracji zgodności,	Test teoretyczny
Charakteryzuje zasady projektowania infrastruktury sieciowej dla systemów zabezpieczeń technicznych	A. wyjaśnia podstawowe pojęcia związane z infrastrukturą sieciową, B. identyfikuje wymagania w zakresie sieci dla systemów zabezpieczeń technicznych, C. identyfikuje okablowanie dla systemów zabezpieczeń technicznych, D. identyfikuje wyzwania związane z łącznością bezprzewodową i proponuje sposoby ich pokonania, E. wskazuje typowe urządzenia brzegowe podłączone do sieci w systemie zabezpieczeń technicznych, F. wskazuje możliwości zastosowania rozwiązań bezprzewodowych, mobilnych i chmurowych w systemach zabezpieczeń technicznych, G. wyjaśnia zasady ochrony danych przetwarzanych przez systemy zabezpieczeń (np. danych osobowych, danych zdarzeń i archiwów).	Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Charakteryzuje podstawowe zasady cyberbezpieczeństwa w systemach zabezpieczeń technicznych	A. charakteryzuje zasady ochrony danych i informacji przetwarzanych przez systemy zabezpieczeń technicznych, B. identyfikuje zagrożenia dla systemów zabezpieczeń technicznych wynikające z cyberataków, nieautoryzowanego dostępu oraz awarii systemowych, C. identyfikuje podstawowe podatności urządzeń systemów zabezpieczeń technicznych i proponuje sposoby ich niwelowania, D. charakteryzuje wpływ środowiska wdrożeniowego systemów zabezpieczeń technicznych (np. lokalne, chmurowe, poza lokalne, hybrydowe) na poziom bezpieczeństwa systemów i danych, E. identyfikuje protokoły komunikacji oraz techniki szyfrowania danych stosowane w systemach zabezpieczeń technicznych, F. identyfikuje standardy i protokoły bezpieczeństwa sieci dla systemów zabezpieczeń technicznych, G. wskazuje podstawowe metody zapewnienia bezpieczeństwa sieci stosowane w systemach zabezpieczeń, H. identyfikuje procesy autentykacji w cyberbezpieczeństwie systemów zabezpieczeń technicznych, w tym ich rolę w ochronie przed nieautoryzowanym dostępem, podszywaniem się oraz manipulacją danymi i zdarzeniami, I. charakteryzuje wybrane wymagania z PN-EN ISO/IEC 27001,	Test teoretyczny
Charakteryzuje podstawowe zasady kosztorysowania systemów zabezpieczeń technicznych	A. identyfikuje metodykę prezentacji kosztów z branży instalacyjno-budowlanej, B. charakteryzuje połączenia nakładów materialnych i niematerialnych niezbędnych do realizacji założeń i celów wynikających z projektów różnych branż, C. identyfikuje nakłady pracy odnosząc się do wartości pieniężnej, która została przypisana do realizacji danego zadania, D. charakteryzuje możliwości wykorzystania programu Norma lub podobnego programu, E. wskazuje wybrane, znormalizowane i powtarzalne czynności, które mają określone jednostki nakładu pracochłonności.	Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Wykorzystuje narzędzia sztucznej inteligencji i uczenia maszynowego w systemach zabezpieczeń technicznych	A. wyjaśnia podstawowe pojęcia związane ze sztuczną inteligencją, B. wskazuje możliwości wykorzystania sztucznej inteligencji w systemach zabezpieczeń technicznych, C. wskazuje przykładowe narzędzia AI wykorzystywane w systemach zabezpieczeń technicznych, D. ocenia przydatność narzędzi AI dla konkretnych zastosowań w systemach zabezpieczeń technicznych.	Test teoretyczny
Charakteryzuje zasady zarządzania bezpieczeństwem obiektów i usług kluczowych	A. charakteryzuje podejście do zapewniania bezpieczeństwa w infrastrukturze krytycznej w odniesieniu do obowiązujących wymagań prawno-normatywnych, B. charakteryzuje proces planowania systemu zarządzania bezpieczeństwem obiektu lub usługi kluczowej, C. identyfikuje powiązania prawno-regulacyjne, organizacyjne, proceduralne i techniczne w zarządzaniu bezpieczeństwem obiektu lub usługi kluczowej, D. wskazuje podstawowe wymagania w zakresie uzgadniania planów ochrony, E. charakteryzuje zasady organizowania i kierowania zespołami pracowników zabezpieczenia technicznego.	Test teoretyczny

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 usługi jest skierowany do grupy docelowej i realizuje niezbędne zagadnienia.

Bloki tematyczne:

1. Aspekty prawno-normatywne

2. Analiza zagrożeń, szacowanie ryzyka.

3. Aspekty instalowania, konserwacji i projektowania systemów sygnalizacji włamania i napadu, systemów telewizji dozorowej, systemów kontroli dostępu i innych systemów technicznej ochrony osób i mienia.

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 zorganizowanie drugiego monitora, co ułatwiłoby pracę w trakcie warsztatów, ale podział ekranu powinien wystarczyć do realizacji celu szkolenia.

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

4. Usługa jest realizowana zgodnie z aktualnym regulaminem BUR oraz załącznikiem nr 2g do Regulaminu Bazy Usług Rozwojowych (BUR).

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.

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).

Zasadność odbycia kursu:

1. Zdobycie aktualnej wiedzy prawno-technicznej w zakresie: projektowania, instalowania i konserwacji technicznych systemów zabezpieczeń, szacowania ryzyka, analizy zagrożeń, procesu inwestycyjnego, rozwiązań i realizacji dla danego obiektu, formułowania wymagań wobec sprzętu – i – co obecnie jest szczególnie ważne – bezpieczeństwa samego sprzętu pod względem zbierania/ulotów danych
2. Spełnienie wymagań obowiązującej Ustawy o ochronie osób i mienia (Dz.U. 1997 nr 114 poz. 740 z późn. zm.) –
3. uzyskanie wpisu na listę kwalifikowanych pracowników zabezpieczenia technicznego
4. Uzyskanie uprawnień branżowych do projektowania, instalowania i konserwacji technicznych systemów zabezpieczeń do stopni 1-4/wojskowych dokumentów normatywnych
5. Spełnienie wymagań MON wobec usługodawców realizujących techniczne systemy zabezpieczeń w obiektach wojskowych
6. Spełnienie wymagań zamawiających z sektora obiektów podlegających obowiązkowej ochronie
7. Podwyższenie wiarygodności wobec kontrahentów
8. Znaczące podwyższenie kompetencji i dostosowanie do wymogów normy PN-EN 16763 Usługi w zakresie systemów ochrony przeciwpożarowej oraz systemów zabezpieczeń technicznych

Harmonogram

Liczba pozycji harmonogramu: 34

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 34 Wprowadzenie organizacyjne i otoczenie prawno-normatywne systemów zabezpieczeń technicznych	Zajęcia	ADAM TATAROWSKI	15-06-2026	09:00	09:45	00:45
2 z 34 System norm, wytycznych stosowania i stopni zabezpieczenia 1–4	Zajęcia	ADAM TATAROWSKI	15-06-2026	09:45	10:30	00:45
3 z 34 -	Przerwa	-	15-06-2026	10:30	10:45	00:15
4 z 34 Klasyfikacja obiektu i ustalenie kontekstu szacowania ryzyka bezpieczeństwa	Zajęcia	Andrzej Wójcik	15-06-2026	10:45	12:15	01:30
5 z 34 -	Przerwa	-	15-06-2026	12:15	12:45	00:30
6 z 34 Case study: analiza zagrożeń, szacowanie ryzyka i dobór stopnia zabezpieczenia	Zajęcia	Andrzej Wójcik	15-06-2026	12:45	14:30	01:45
7 z 34 -	Przerwa	-	15-06-2026	14:30	14:45	00:15

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
8 z 34 Karta wyników szacowania ryzyka jako wejście do projektu systemu zabezpieczeń	Zajęcia	Andrzej Wójcik	15-06-2026	14:45	15:15	00:30
9 z 34 Podstawy kosztorysowania systemów zabezpieczeń technicznych	Zajęcia	Andrzej Wójcik	15-06-2026	15:15	16:00	00:45
10 z 34 SSWiN i transmisja alarmu — budowa, działanie, stopnie zabezpieczenia	Zajęcia	Bartłomiej Kwiatkowski	16-06-2026	08:00	09:30	01:30
11 z 34 -	Przerwa	-	16-06-2026	09:30	09:45	00:15
12 z 34 Systemy kontroli dostępu — architektura, identyfikacja, nośniki	Zajęcia	Bartłomiej Kwiatkowski	16-06-2026	09:45	11:15	01:30
13 z 34 -	Przerwa	-	16-06-2026	11:15	11:45	00:30
14 z 34 SKD — bezpieczeństwo, stopnie 1–4, zastosowania i integracje	Zajęcia	Bartłomiej Kwiatkowski	16-06-2026	11:45	13:15	01:30
15 z 34 -	Przerwa	-	16-06-2026	13:15	13:30	00:15
16 z 34 VSS/CCTV — wymagania użytkowe i jakość obrazu	Zajęcia	Marcin Cholewka	16-06-2026	13:30	15:00	01:30

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
17 z 34 VSS IP — architektura, zapis, backup, dane	Zajęcia	Marcin Cholewka	17-06-2026	08:00	09:30	01:30
18 z 34 -	Przerwa	-	17-06-2026	09:30	09:45	00:15
19 z 34 Sieci, okablowanie i usługi zdalne dla systemów zabezpieczeń	Zajęcia	Marcin Cholewka	17-06-2026	09:45	11:15	01:30
20 z 34 -	Przerwa	-	17-06-2026	11:15	11:45	00:30
21 z 34 Cyberbezpieczeństwo systemów zabezpieczeń technicznych	Zajęcia	Marcin Cholewka	17-06-2026	11:45	13:15	01:30
22 z 34 -	Przerwa	-	17-06-2026	13:15	13:30	00:15
23 z 34 AI i analityka w systemach zabezpieczeń	Zajęcia	Marcin Cholewka	17-06-2026	13:30	15:00	01:30
24 z 34 PN-EN 16763 jako mapa procesu usługi i punkt wejścia do wytycznych stosowania	Zajęcia	Waldemar Konkol	18-06-2026	08:00	09:30	01:30
25 z 34 -	Przerwa	-	18-06-2026	09:30	09:45	00:15
26 z 34 Dokumentacja techniczna – zasady, zakres, cykl życia	Zajęcia	Waldemar Konkol	18-06-2026	09:45	11:15	01:30
27 z 34 -	Przerwa	-	18-06-2026	11:15	11:45	00:30

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
28 z 34 Instalowanie, uruchamianie, sprawdzanie zgodności i odbiór systemu	Zajęcia	Waldemar Konkol	18-06-2026	11:45	13:15	01:30
29 z 34 -	Przerwa	-	18-06-2026	13:15	13:30	00:15
30 z 34 Wojskowe dokumenty normatywne: ESWOF, odbiór, certyfikacja i eksploatacja	Zajęcia	Waldemar Konkol	18-06-2026	13:30	15:00	01:30
31 z 34 Zewnętrzne systemy zabezpieczeń technicznych. Problematyka projektowania, instalowania i konserwacji. Praktyczny wymiar opracowywania i uzgadniania planów ochrony	Zajęcia	Marcin Stępień	19-06-2026	08:00	09:30	01:30
32 z 34 -	Przerwa	-	19-06-2026	09:30	09:45	00:15
33 z 34 Powtórzenie ukierunkowane na kryteria weryfikacji	Zajęcia	ADAM TATAROWSKI	19-06-2026	09:45	10:15	00:30
34 z 34 -	Walidacja	-	19-06-2026	10:15	12:00	01:45

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	32:00

Rodzaj godzin	Liczba godzin
w tym suma godzin zajęć	26:00
w tym suma godzin walidacji	01:45
w tym suma przerw	04:15
Suma godzin dydaktycznych bez przerw	37:00

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto Podmiot uprawniony do zwolnienia z VAT na podstawie art. 43 ust. 1 ustawy o VAT	3 450,00 PLN
Koszt przypadający na 1 uczestnika netto	3 450,00 PLN
Koszt osobogodziny brutto	107,81 PLN
Koszt osobogodziny netto	107,81 PLN

Liczba godzin usługi

Rodzaj godzin	Liczba godzin
Liczba godzin zegarowych usługi	32:00

Prowadzący

Liczba prowadzących: 6

1 z 6

Andrzej Wójcik

Certyfikowany audytor wiodący IEC/ISO 27001 – Zarządzania bezpieczeństwem informacji dwóch organizacji BSI i ISOQAR; Trener do spraw szkolenia audytorów wewnętrznych ISO 27001 organizacji SAI Global/EFSIS Polska, BSI Management Systems Polska Sp. z o.o., KEMA Quality; * Rzeczoznawca w zakresie zabezpieczenia technicznego osób i mienia Stowarzyszenia POLALARM; Ukończone ukierunkowane na bezpieczeństwo studia podyplomowe w tym: marketing i analiza rynku security (SGH 1991), radioelektronika – Politechnika Warszawska (1994), obronność państwa

(Akademia Obrony Narodowej 1998), zarządzanie infrastrukturą IT (Wyższa Warszawska Szkoła Informatyki -2007); * Posiada Certyfikat w zakresie zarządzania usługami teleinformatycznymi wg ITIL V3 (2009), zarządzania projektami wg metodyki PRINCE 2 (2010); Pełnomocnik Ochrony Informacji Niejawnych w firmach sektora IT i budowlanym.
Posiada min. dwuletnie doświadczenie zawodowe w prowadzeniu szkoleń z obszaru projektowania, instalowania i konserwacji technicznych systemów zabezpieczeń dla wskazanej Grupy docelowej

2 z 6

ADAM TATAROWSKI

Dyrektor Szkoły Elektronicznych Systemów Zabezpieczeń TECHOM, zajmuje się organizacją profesjonalnych kursów w sektorach systemów ochrony przeciwpożarowej, systemów zabezpieczeń technicznych i ochrony informacji niejawnych. Jest autorem programu szkoleniowego osób funkcyjnych zajmujących się ochroną obiektów wojskowych. Członek Komitetów Technicznych nr 52, 264, 306 i 323 w Polskim Komitecie Normalizacyjnym. Autor tłumaczenia Normy PN-EN 16763 Usługi w zakresie systemów ochrony przeciwpożarowej i systemów zabezpieczeń technicznych. Odpowiedzialny za tłumaczenie nowej specyfikacji TS 54-14 dotyczącej stosowania systemów sygnalizacji pożarowej. Członek Grupy ds. Standaryzacji i Certyfikacji funkcjonującej w ramach Sektorowej Rady ds. Kompetencji w Budownictwie. Prezes Ogólnopolskiego Stowarzyszenia Inżynierów i Techników Zabezpieczeń Technicznych i Zarządzania Bezpieczeństwem „POLALARM”.
Posiada min. dwuletnie doświadczenie zawodowe w prowadzeniu szkoleń z obszaru projektowania, instalowania i konserwacji technicznych systemów zabezpieczeń dla wskazanej Grupy docelowej.

3 z 6

Marcin Cholewka

Specjalista z ponad 25-letnim doświadczeniem w branży IT, teleinformatyce oraz systemach bezpieczeństwa elektronicznego. Swoje kompetencje budował przez lata pracy na różnych stanowiskach — od właściciela serwisu komputerowego i współwłaściciela dostawcy internetu (ISP), przez dyspozytora z zadaniami administratora sieci, aż po stanowisko inżyniera i eksperta ds. technicznych w jednej z wiodących firm dystrybucyjnych systemów bezpieczeństwa w Polsce.

W swojej działalności zawodowej realizował szkolenia dla instalatorów, techników oraz użytkowników indywidualnych z zakresu: systemów telewizji przemysłowej (CCTV), sieci komputerowych i bezprzewodowych, konfiguracji serwerów, systemów integracji i wizualizacji oraz bezpiecznego użytkowania Internetu. Jako trener w unijnym projekcie ICEO prowadził zajęcia dla osób zagrożonych wykluczeniem cyfrowym, w tym osób starszych, a także szkolił samych szkoleniowców — co pozwoliło mu rozwinąć wysoki poziom cierpliwości, empatii i umiejętności dostosowywania przekazu do różnych grup odbiorców.

Posiada szeroką wiedzę praktyczną z zakresu projektowania i budowy sieci kablowych oraz bezprzewodowych (2,4 GHz / 5 GHz), technologii MikroTik, instalacji zasilania awaryjnego (UPS, systemy solarne), a także diagnostyki i utrzymania systemów bezpieczeństwa (CCTV, SSWiN). Przez wiele lat zarządzał zespołami techników i instalatorów, realizując złożone projekty teleinformatyczne i bezpieczeństwa elektronicznego.

4 z 6

Bartłomiej Kwiatkowski

Specjalista z ponad 16-letnim doświadczeniem w branży elektronicznych systemów zabezpieczeń fizycznych, z głęboką wiedzą ekspercką w zakresie systemów kontroli dostępu, wideodomofonów, systemów sygnalizacji włamania i napadu (SSWiN) oraz platform integracyjnych PSIM.
Wykształcenie inżynierskie zdobył na Wojskowej Akademii Technicznej na kierunku mechatronika, robotyka i automatyka, co stanowi solidną podstawę techniczną dla prowadzonej działalności szkoleniowej i eksperckiej.

Przez całą karierę zawodową związany z firmą AAT Systemy Bezpieczeństwa, gdzie przeszedł ścieżkę rozwoju od specjalisty ds. serwisu SSWiN, przez głównego specjalistę i kierownika działu technicznego, aż do stanowiska Dyrektora Działu Technicznego (Physical Security). Na tym stanowisku odpowiada za zarządzanie produktami i rozwojem w obszarze elektronicznego bezpieczeństwa fizycznego, kształtowanie kierunków rozwoju produktów oraz kierowanie i rozwijanie zespołów technicznych.

Jako wykładowca i trener branżowy posiada szeroką wiedzę praktyczną i merytoryczną z zakresu projektowania, wdrażania oraz integracji systemów bezpieczeństwa fizycznego. Specjalizuje się w systemach kontroli dostępu, wideodomofonach oraz systemach alarmowych, a jego doświadczenie obejmuje zarówno aspekty techniczne, jak i zarządcze — w tym zarządzanie produktem, zarządzanie zespołem oraz wdrażanie innowacji w obszarze security.

5 z 6

Waldemar Konkol

ppłk rezerwy, wieloletni specjalista Wydziału Ochrony i Obrony Obiektów Inspektoratu Wsparcia Sił Zbrojnych, współautor wojskowych dokumentów normatywnych regulujących system ochrony jednostek wojskowych. Doświadczony inżynier elektronik oraz specjalista w zakresie normalizacji systemów zabezpieczeń technicznych. Posiada wieloletnie doświadczenie zawodowe i dydaktyczne w prowadzeniu szkoleń, wykładów oraz zajęć specjalistycznych z zakresu systemów zabezpieczeń technicznych, ochrony obiektów oraz wymagań normatywnych i organizacyjnych dotyczących bezpieczeństwa. Audytor systemów zabezpieczeń technicznych, praktyk z doświadczeniem w ocenie, projektowaniu i wdrażaniu rozwiązań bezpieczeństwa zgodnych z obowiązującymi przepisami, normami oraz wymaganiami resortowymi

6 z 6

Marcin Stępień

Absolwent Politechniki Wrocławskiej, magister inżynier telekomunikacji, z branżą systemów bezpieczeństwa związany od roku 2006. Projektant/manager ds. systemów teletechnicznych z dużym doświadczeniem, związanym z systemami ochrony obwodowej, CCTV, SSWiN, KD, SAP oraz sieci transmisji danych, zdobytych w biurze projektowym, dziale realizacji oraz dziale sprzedaży. Obecnie kierownik Działu Systemów Bezpieczeństwa w firmie PRODUS S.A. odpowiedzialny za dystrybucję systemów bezpieczeństwa, przygotowanie koncepcji/projektów, współprace z Partnerami firmy oraz wprowadzanie do dystrybucji firmy innowacyjnych rozwiązań z zakresu teletechnicznych systemów bezpieczeństwa. Od wielu lat prowadzi szkolenia w zakresie swoich kompetencji.

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.

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.

Warunki uczestnictwa

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

Warunkiem nieobowiązkowym, ale zalecanym, jest posiadanie podstawowej wiedzy i umiejętności z zakresu elektryki, elektroniki i telekomunikacji.

UWAGA:

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

Informacje dodatkowe

Zakład Rozwoju Technicznej Ochrony Mienia TECHOM Sp. z o.o. jest zarejestrowaną placówkę oświatową pod nazwą Szkoła Elektronicznych Systemów Zabezpieczeń i posiada:

1) nr 127157 w Rejestrze Szkół i Placówek Oświatowych

2) Zaświadczenie nr 663/K/95[2] o wpisie do ewidencji szkół i placówek niepublicznych prowadzonej przez M. St. Warszawa

Po kursie uczestnicy otrzymują:

1)Zaświadczenie o ukończeniu kursu wydane zgodnie ze wzorem określonym w §22ust.4 Rozporządzenia Ministra Edukacji z dnia 19 marca 2019 r. w sprawie kształcenia ustawicznego w formach pozaszkolnych (Dz.U.2019 r. poz.652).

2)Zaświadczenie o ukończeniu usługi rozwojowej

Ukończenie kursu umożliwia absolwentowi ubieganie się o wpis na listę kwalifikowanych pracowników zabezpieczenia technicznego (zgodnie z art. 27 Ustawy o ochronie osób i mienia)

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