ZAKŁAD ROZWOJU TECHNICZNEJ OCHRONY MIENIA TECHOM SP. Z O.O.

Jednostka Certyfikująca
na Znak PN
PN-EN 16763

Al. Wyzwolenia 12, 00-570 Warszawa
tel. (22) 625-34-00, fax (22) 625-26-75
www.techom.com
techom@techom.com

Wpis do KRS Nr 0000164572
NIP: 5260011894
Regon: 010663796

KOD NCAGE **9A57H**

OFERTA KURSU

KURS PRACOWNIKA ZABEZPIECZENIA TECHNICZNEGO W ZAKRESIE PROJEKTOWANIA, INSTALOWANIA, KONSERWACJI, ODBIORU I EKSPLOATACJI SYSTEMÓW ZABEZPIECZEŃ TECHNICZNYCH STOPNI 1-4 / WOJSKOWYCH DOKUMENTÓW NORMATYWNYCH – forma stacjonarna

O KURSIE

Kurs pokazuje, jak prowadzić cały proces przygotowania i realizacji systemów zabezpieczeń technicznych – od analizy zagrożeń i szacowania ryzyka, przez określenie wymagań i stopnia zabezpieczenia oraz projektowanie, aż po instalowanie, uruchamianie, sprawdzanie, odbiór, eksploatację i konserwację systemu.

Duży nacisk położony jest na zasady przygotowywania dokumentacji technicznej: wykonawczej, powykonawczej i eksploatacyjnej – jej zakres, zawartość i rolę na kolejnych etapach procesu inwestycyjnego, również w powiązaniu z wymaganiami prawa budowlanego i szerszym kontekstem realizacji instalacji telekomunikacyjnych. Program obejmuje SSWiN, SKD, VSS/CCTV i zewnętrzne systemy perymetryczne, a także infrastrukturę sieciową, integrację systemów, kosztorysowanie, cyberbezpieczeństwo, AI, ocenę zgodności oraz wymagania dotyczące obiektów wojskowych i infrastruktury krytycznej.

ANALIZA ZAGROŻEŃ I SZACOWANIE RYZYKA » **WYMAGANIA I STOPIEŃ ZABEZPIECZENIA** » **PROJEKTOWANIE** » **INSTALOWANIE I URUCHAMIANIE** » **SPRAWDZANIE I ODBIÓR** » **EKSPLOATACJA I KONSERWACJA**

ORGANIZACJA SZKOLENIA

TERMIN	Zgodnie z ofertą na stronie.
MIEJSCE	Warszawa.
FORMA	Stacjonarna. UWAGA: zajęcia odbywają się w tym samym hotelu, w którym realizowane są opcjonalne noclegi uczestników.
CZAS TRWANIA	5 dni – 32 godziny zegarowe (łącznie z przerwami)
GODZINY ZAJĘĆ	Dzień I: od 9.00; dni II–V: od 8.00 (szczegóły w harmonogramie kursu)
CENA	3950,00 zł od osoby – zwolnione z VAT. Cena obejmuje: szkolenie, materiały dydaktyczne, test, zaświadczenie o ukończeniu kursu i Autoryzację TECHOM, całodzienny bufet kawowy, wyżywienie w ramach szkolenia.
TERMIN ZGŁOSZEŃ	Do dwóch tygodni przed rozpoczęciem szkolenia (po tym terminie zgłoszenia będą przyjmowane warunkowo).

DLA KOGO JEST TEN KURS?

Kurs jest przeznaczony dla osób, które odpowiadają – lub mają odpowiadać – za projektowanie, realizację, eksploatację albo nadzór nad systemami zabezpieczeń technicznych, a także za organizację bezpieczeństwa obiektów. W szczególności dla:

- osób przygotowujących się do wpisu na listę kwalifikowanych pracowników zabezpieczenia technicznego oraz osób, którym pracodawca zamierza powierzyć zadania pracownika zabezpieczenia technicznego;
- projektantów, instalatorów, konserwatorów i specjalistów technicznych zajmujących się SSWiN, SKD, VSS/CCTV, transmisją alarmu, systemami perymetrycznymi oraz integracją systemów zabezpieczeń;
- inwestorów, kierowników projektów, inspektorów i osób nadzorujących inwestycje, odpowiedzialnych za określanie wymagań, dobór rozwiązań, dokumentację techniczną, odbiór oraz ocenę zgodności wykonanych systemów;
- kierowników i koordynatorów bezpieczeństwa, którzy odpowiadają za techniczne środki ochrony, przygotowanie rozwiązań do planów ochrony oraz organizację pracy zespołów zabezpieczenia technicznego;
- osób odpowiedzialnych za bezpieczeństwo infrastruktury krytycznej i obiektów o podwyższonych wymaganiach ochronnych, w których zabezpieczenia techniczne łączą się z zarządzaniem ryzykiem, cyberbezpieczeństwem i ciągłością działania;
- osób realizujących lub nadzorujących zabezpieczenia techniczne w obiektach wojskowych i jednostkach resortu obrony narodowej, w tym w zakresie dokumentacji, odbioru i eksploatacji systemów.

JAKIE KORZYŚCI DAJE UKOŃCZENIE KURSU?

Uprawnienia i kompetencje	**Dokumenty po ukończeniu**
• umożliwia ubieganie się o wpis na listę kwalifikowanych pracowników zabezpieczenia technicznego w rozumieniu art. 27 ustawy o ochronie osób i mienia; • umożliwia realizację czynności w zakresie zabezpieczenia technicznego oraz projektowania systemów zabezpieczeń	• Zaświadczenie o ukończeniu kursu pracownika zabezpieczenia technicznego – wystawione zgodnie z § 23 ust. 4 rozporządzenia Ministra Edukacji i Nauki z dnia 6 października 2023 r. w sprawie kształcenia ustawicznego w formach pozaszkolnych (Dz.U. 2023 poz. 2175), bezterminowe i uznawane przez instytucje państwowe oraz sektor prywatny;

technicznych w obiektach podlegających obowiązkowej ochronie, wojskowych, a także w sektorze infrastruktury krytycznej; • potwierdza kompetencje wymagane przez wielu zamawiających, także spoza rynku regulowanego; • uzupełnia inne uprawnienia, w tym budowlane (ukończenie kursu uprawnia do realizacji projektów wykonawczych).	• Autoryzacja TECHOM – uznaniowy dokument branżowy, ważny 3 lata, wydawany reprezentantom firm/instytucji po ukończeniu kursu; potwierdza aktualność wiedzy i kompetencji w zakresie systemów zabezpieczeń technicznych i w praktyce jest często wymagany przez zamawiających, inwestorów i audytorów.

PODSTAWY PRAWNE, NORMATYWNE I BRANŻOWE

W wielu przypadkach kurs pracownika zabezpieczenia technicznego jest wymagany lub oczekiwany jako potwierdzenie przygotowania zawodowego. Znaczenie kursu wynika zarówno z przepisów, jak i z wymagań stosowanych w praktyce inwestycyjnej, wojskowej oraz w ochronie infrastruktury krytycznej:

- obiekty podlegające obowiązkowej ochronie w rozumieniu ustawy o ochronie osób i mienia – ukończenie kursu jest jedną z ustawowych podstaw potwierdzenia przygotowania zawodowego przy ubieganiu się o wpis na listę kwalifikowanych pracowników zabezpieczenia technicznego;
- obiekty wojskowe – wymagania dotyczące kwalifikacji projektantów, instalatorów i konserwatorów systemów zabezpieczeń technicznych wynikają również z właściwych wojskowych dokumentów normatywnych;
- infrastruktura krytyczna – ukończenie specjalistycznego kursu pracownika zabezpieczenia technicznego jest wskazywane w dobrych praktykach i rekomendacjach Narodowego Programu Ochrony Infrastruktury Krytycznej (Załącznik 1 do NPOIK 2023).

Kluczowe dokumenty normatywne omawiane na kursie:

PN-EN 16763 Usługi w zakresie systemów ochrony przeciwpożarowej i systemów zabezpieczeń technicznych	**PKN-CLC/TS 50131-7** Systemy alarmowe – Systemy sygnalizacji włamania i napadu – Część 7: Wytyczne stosowania
PN-EN IEC 62676-4 Systemy dozoru wizyjnego stosowane w zabezpieczeniach – Część 4: Wytyczne stosowania	**PN-EN 60839-11-2** Systemy alarmowe i elektroniczne systemy zabezpieczeń – Część 11-2: Elektroniczne systemy kontroli dostępu – Wytyczne stosowania

TEMATYKA KURSU

Kurs obejmuje cały proces przygotowania, realizacji i eksploatacji systemów zabezpieczeń technicznych – od analizy zagrożeń i szacowania ryzyka, przez określenie wymagań i dobór stopnia zabezpieczenia, projektowanie, instalowanie, uruchamianie i sprawdzanie, aż po odbiór, eksploatację i konserwację systemu. Istotnym elementem programu są zasady przygotowywania i prowadzenia dokumentacji na kolejnych etapach tego procesu – w tym dokumentacji wykonawczej, powykonawczej i eksploatacyjnej – oraz jej powiązanie z procesem inwestycyjnym i wymaganiami dotyczącymi instalacji telekomunikacyjnych. Program uzupełniają zagadnienia infrastruktury sieciowej, integracji systemów, cyberbezpieczeństwa, AI, kosztorysowania, oceny zgodności oraz zarządzania bezpieczeństwem obiektów.

Moduł 1: Analiza zagrożeń, szacowanie ryzyka i dobór stopnia zabezpieczenia

- wymagania prawne, Polskie Normy i wytyczne do ich stosowania, wojskowe dokumenty normatywne, wymagania inwestora oraz wymagania wynikające z charakteru obiektu chronionego;
- klasyfikacja obiektu z uwzględnieniem jego funkcji, chronionych aktywów, realizowanych procesów i stref ochrony;
- ustalanie kontekstu i kryteriów ryzyka oraz identyfikacja źródeł ryzyka, zagrożeń, podatności i możliwych następstw;
- określanie poziomu ryzyka oraz ocena jego akceptowalności;
- dobór sposobu postępowania z ryzykiem i środków jego redukcji;
- zasady doboru stopni zabezpieczenia 1–4 oraz środków organizacyjno-technicznych z uwzględnieniem SSWiN, SKD, VSS/CCTV i transmisji alarmu;
- współdziałanie systemów lub podsystemów o różnych stopniach zabezpieczenia, w szczególności przy podziale obiektu na strefy ochrony;
- opracowanie karty wyników szacowania ryzyka jako danych wejściowych do projektu systemu zabezpieczeń;
- case study obejmujące analizę konkretnego obiektu, szacowanie ryzyka i dobór rozwiązań zabezpieczających.

Moduł 2: SSWiN, SKD, VSS/CCTV i zewnętrzne perymetryczne systemy zabezpieczeń

- budowa, funkcje i zasady działania SSWiN, w tym zasilanie, ochrona przed sabotażem, rejestracja zdarzeń i problem fałszywych alarmów;
- stopnie zabezpieczenia 1–4 w SSWiN, dobór urządzeń do ryzyka i stref obiektu oraz systemy transmisji alarmu;
- architektura SKD: systemy offline, online, online bezprzewodowe, hybrydowe i wirtualne;
- sposoby identyfikacji użytkownika, nośniki, uprawnienia, uwierzytelnianie, szyfrowanie i bezpieczeństwo transmisji danych w SKD;
- wymagania dotyczące SKD w stopniach zabezpieczenia 1–4 oraz rodzaje przejść kontrolowanych;
- cele stosowania VSS/CCTV: obserwacja, detekcja, rozpoznanie, identyfikacja, weryfikacja alarmów i pozyskiwanie materiału dowodowego;
- dobór kamer, obiektywów, oświetlenia, lokalizacji i pola widzenia oraz zależność parametrów obrazu od użyteczności nagrań;
- architektura VSS IP, kompresja, zapis, retencja, eksport nagrań, integralność materiału, znaczniki czasu i kopie zapasowe;
- zewnętrzne perymetryczne systemy zabezpieczeń: struktura systemu, obszary, warstwy, strefy i punkty detekcji, technologie detekcji, klasy środowiskowe, stopnie ochrony własnej i odporność na fałszywe alarmy;
- współdziałanie SSWiN, SKD, VSS/CCTV i zewnętrznych perymetrycznych systemów zabezpieczeń.

Moduł 3: Infrastruktura sieciowa, integracja, cyberbezpieczeństwo i sztuczna inteligencja

- infrastruktura sieciowa systemów zabezpieczeń technicznych: Ethernet, adresacja, VLAN, PoE, QoS, multicast/unicast, przepustowość, opóźnienia i segmentacja;
- okablowanie strukturalne, punkty dystrybucyjne, zasilanie i zabezpieczenia przepięciowe;
- urządzenia brzegowe oraz rozwiązania bezprzewodowe, mobilne, chmurowe i hybrydowe;
- bezpieczne usługi zdalne oraz ochrona danych przetwarzanych w systemach zabezpieczeń;
- integracja VSS, SSWiN i SKD z VMS, BMS/PMS, PSIM i innymi systemami obiektowymi, w tym scenariusze alarmowe i weryfikacja zdarzeń;
- zagrożenia dla VMS, SKD, SSWiN, urządzeń brzegowych i sieci oraz podstawowe podatności systemów;

- uwierzytelnianie, autoryzacja, szyfrowanie, VPN, segmentacja, hardening, aktualizacje, kopie zapasowe, logowanie, monitoring podatności i reakcja na incydenty;
- wybrane wymagania PN-EN ISO/IEC 27001 w kontekście systemów zabezpieczeń technicznych;
- zastosowanie AI i uczenia maszynowego w systemach zabezpieczeń, w tym analityka obrazu, LPR, detekcja incydentów, zliczanie osób, analiza kolejek, automatyczne śledzenie i kontekstualizacja alarmów;
- warunki skutecznego stosowania analityki AI, w tym jakość obrazu, oświetlenie, scena, konfiguracja, testy i dane oraz problem wyników fałszywie pozytywnych i fałszywie negatywnych.

Moduł 4: Zasady realizacji usług w zakresie systemów zabezpieczeń technicznych – od planowania do eksploatacji i konserwacji

- PN-EN 16763 jako podstawa uporządkowania procesu usługi: planowanie, projektowanie, instalowanie, uruchamianie, sprawdzanie, przekazywanie i konserwacja;
- powiązanie PN-EN 16763 z właściwymi normami systemowymi i wytycznymi stosowania dla SSWiN, VSS/CCTV i SKD;
- zasady przygotowywania i prowadzenia dokumentacji na kolejnych etapach realizacji usługi – od planowania i projektowania po odbiór, eksploatację i konserwację;
- zakres dokumentacji technicznej systemów zabezpieczeń oraz zasady aktualizacji dokumentacji;
- organizacja prac instalacyjnych: okablowanie, trasy kablowe, oznakowanie, zasilanie i kompatybilność elektromagnetyczna;
- konfiguracja urządzeń i oprogramowania, uruchamianie oraz testowanie zgodności wykonanego systemu z projektem;
- sprawdzenia funkcjonalne, kontrole częściowe, odbiór robót ulegających zakryciu oraz identyfikacja i usuwanie niezgodności;
- odbiór i przekazanie systemu jako potwierdzenie zgodności z dokumentacją oraz wymaganiami technicznymi, normatywnymi i użytkowymi;
- bilans energetyczny i obliczanie wymaganej pojemności źródła zasilania rezerwowego;
- przygotowanie danych wyjściowych do kosztorysowania, prezentacja kosztów oraz wykorzystanie programu Norma lub podobnych narzędzi kosztorysowych.

Moduł 5: Wymagania wojskowe i dla infrastruktury krytycznej, audyt, ocena zgodności i certyfikacja

- wymagania wojskowych dokumentów normatywnych oraz różnice pomiędzy sferą cywilną i wojskową;
- Elektroniczne Systemy Wspomagające Ochronę Fizyczną, tj. ESWOF – podejście wojskowe;
- wymagania dotyczące dokumentacji technicznej powykonawczej i dokumentacji eksploatacji w sferze cywilnej (z naciskiem na infrastrukturę krytyczną) i w sferze wojskowej, w tym jej formy, liczby egzemplarzy i klauzul;
- deklaracje zgodności i certyfikaty dotyczące urządzeń oraz zainstalowanych systemów;
- wymagania wojskowe dotyczące zasilania rezerwowego i czasów podtrzymania w zależności od kategorii obiektu;
- próbne działanie, odbiór końcowy, protokół odbioru oraz zakres sprawdzeń funkcjonalnych – sfera infrastruktury krytycznej i wojskowa;
- audyt zainstalowanych systemów zabezpieczeń technicznych/ESWOF oraz znaczenie certyfikacji nowo wybudowanego systemu zabezpieczeń technicznych/ESWOF w procesie odbiorowym;
- szkolenie użytkowników, konserwacja, przeglądy, naprawy i dokumentowanie czynności eksploatacyjnych;
- rozróżnienie audytu i certyfikacji oraz podstawy audytowania według PN-EN ISO 19011;
- certyfikacja usług na zgodność z PN-EN 16763, certyfikacja urządzeń i systemów, ocena zgodności projektu oraz certyfikacja zainstalowanego systemu.

Moduł 6: Zarządzanie bezpieczeństwem obiektów i usług kluczowych

- podejście do zapewniania bezpieczeństwa infrastruktury krytycznej i usług kluczowych;
- planowanie systemu zarządzania bezpieczeństwem obiektu lub usługi kluczowej;
- powiązanie bezpieczeństwa fizycznego, technicznego, osobowego, cyberbezpieczeństwa, bezpieczeństwa prawnego i ciągłości działania;
- powiązania prawno-regulacyjne, organizacyjne, proceduralne i techniczne w zarządzaniu bezpieczeństwem;
- dokumentacja ochrony infrastruktury krytycznej oraz ramy organizacyjno-dokumentacyjne ochrony w różnych porządkach prawnych;
- plany ochrony i podstawowe wymagania dotyczące ich uzgadniania;
- organizowanie i kierowanie zespołami pracowników zabezpieczenia technicznego.

EFEKTY UCZENIA SIĘ

Absolwent kursu:

1. charakteryzuje wymagania prawno-normatywne w zakresie systemów zabezpieczeń technicznych;
2. charakteryzuje proces szacowania ryzyka bezpieczeństwa obiektów prowadzony zgodnie z wymaganiami prawno-normatywnymi;
3. charakteryzuje systemy zabezpieczeń technicznych oraz ich zastosowanie;
4. charakteryzuje zasady projektowania, instalowania, konserwacji, odbioru i eksploatacji systemów zabezpieczeń technicznych dla stopni 1-4 i wojskowych dokumentów normatywnych;
5. charakteryzuje zasady projektowania infrastruktury sieciowej dla systemów zabezpieczeń technicznych;
6. charakteryzuje podstawowe zasady cyberbezpieczeństwa w systemach zabezpieczeń technicznych;
7. charakteryzuje podstawowe zasady kosztorysowania systemów zabezpieczeń technicznych;
8. wykorzystuje narzędzia sztucznej inteligencji i uczenia maszynowego w systemach zabezpieczeń technicznych;
9. charakteryzuje zasady zarządzania bezpieczeństwem obiektów i usług kluczowych.

Walidacja: osiągnięcie efektów uczenia się jest weryfikowane podczas walidacji końcowej – test teoretyczny (pisemny).

WARUNKI UCZESTNICTWA

Wymagania formalne: ukończone 18 lat; wykształcenie co najmniej zawodowe lub średnie.
Zalecane (nieobowiązkowe): podstawowa wiedza i umiejętności z zakresu elektryki, elektroniki i telekomunikacji.

ZGŁOSZENIE NA KURS

1. Pobierz i wypełnij kartę zgłoszenia (zgodę dotyczącą przetwarzania danych osobowych podpisuje bezpośrednio uczestnik).
2. Opłać kurs – nr konta: 60 1240 6218 1111 0000 4615 3700 (instytucje państwowe i spółki Skarbu Państwa mogą dokonać opłaty po zrealizowaniu kursu).
3. Prześlij skan podpisanej karty zgłoszenia (może być podpisana podpisem kwalifikowanym lub przez ePUAP) oraz potwierdzenie przelewu na adres techom@techom.com.
4. Oczekuj potwierdzenia przyjęcia zgłoszenia i szczegółów organizacyjnych.

Kontakt: tel. 22 625 34 00, e-mail: techom@techom.com, www.techom.com.

Zajęcia prowadzą znani i cenieni w Polsce i na świecie specjaliści branżowi – praktycy, rzeczoznawcy i audytorzy, w tym eksperci uczestniczący w pracach normalizacyjnych.

Organizator kursu zastrzega sobie prawo do zmian w planie kursu zgodnie z występującymi potrzebami w tym zakresie. Ostateczny plan kursu uczestnicy otrzymają w pierwszym dniu kursu, przed jego rozpoczęciem. Organizator zastrzega również prawo do zmiany planu kursu w trakcie jego trwania.