

REKOMENDACJA¹ NR 1/2026²

SEKTOROWEJ RADY DS. KOMPETENCJI – OCHRONA I BEZPIECZEŃSTWO MIENIA I OSÓB

Rodzaj rekomendacji³: Kompetencje kluczowe⁴

Rekomendacja została przyjęta uchwałą Rady nr 3/2026 z dnia 18.05.2026 r.

¹ Rekomendacja ma być **drogowskazem dla instytucji** przy podejmowaniu planów związanych z finansowaniem edukacji. W związku z powyższym, rekomendacja powinna obejmować całe, identyfikowane przez sektor zapotrzebowanie i rozwiązania systemowe w zakresie danego sektora.

² Numer rekomendacji wydanej przez Sektorową Radę ds. Kompetencji/rok jej wydania.

³ Rekomendacja powinna zawierać opis zidentyfikowanego zapotrzebowania na kompetencje/kwalifikacje z obszaru kompetencji kluczowych dla sektora albo kompetencji „zielonych”. W jednej rekomendacji nie powinny znajdować się rekomendacje z obydwu obszarów. Rada powinna opracować jedną rekomendację kluczową i jedną zieloną. Dokument powinien określić rodzaj rekomendacji (kluczowa/zielona).

Przez **kluczowe kompetencje** należy rozumieć takie kompetencje/kwalifikacje, w których efekty uczenia się bezpośrednio są związane z danym sektorem i jego specyfiką, np. „obsługuje maszynę do szycia typu...”, „projektuje konstrukcje budynków o nośności...”. Należy zwracać szczególną uwagę, aby kompetencja/kwalifikacja miała związek z obszarem działalności sektora i jego specyfiką. Przez **zielone kompetencje** należy rozumieć takie kompetencje/kwalifikacje, które obejmują umiejętności techniczne - wymagane do przyjęcia lub wdrożenia standardów, procesów, usług, produktów i technologii w celu ochrony środowiska i jego ekosystemów, różnorodności biologicznej oraz do zmniejszenia zużycia energii i zasobów; mogą być one specyficzne dla danego zawodu, branży lub regionu.

⁴ Należy zostawić właściwą odpowiedź, niewłaściwą wykasować.

Spis treści

I.	Opis sektora.....	8
II.	Analiza stanu sektora z punktu widzenia potrzeb kompetencyjnych, opisanych w dalszej części dokumentu.	8
III.	Zapotrzebowanie na kompetencje/kwalifikacje w sektorze.....	11
	Nazwa kompetencji nr 1: Projektowanie, instalowanie, konserwacja, eksploatacja i odbiór systemów zabezpieczeń technicznych stopni 1-4/wojskowych dokumentów normatywnych	11
	Efekt uczenia się 1: Charakteryzuje wymagania prawno-normatywne w zakresie systemów zabezpieczeń technicznych	11
	Efekt uczenia się 2: Charakteryzuje proces szacowania ryzyka bezpieczeństwa obiektów prowadzony zgodnie z wymaganiami prawno-normatywnymi	12
	Efekt uczenia się 3: Charakteryzuje systemy zabezpieczeń technicznych oraz ich zastosowanie ...	13
	Efekt uczenia się 4: Charakteryzuje zasady projektowania, instalowania, konserwacji, odbioru i eksploatacji systemów zabezpieczeń technicznych dla stopni 1-4 i wojskowych dokumentów normatywnych.....	14
	Efekt uczenia się 5: Charakteryzuje zasady projektowania infrastruktury sieciowej dla systemów zabezpieczeń technicznych	15
	Efekt uczenia się 6: Charakteryzuje podstawowe zasady cyberbezpieczeństwa w systemach zabezpieczeń technicznych	16
	Efekt uczenia się 7: Charakteryzuje podstawowe zasady kosztorysowania systemów zabezpieczeń technicznych.....	17
	Efekt uczenia się 8: Wykorzystuje narzędzia sztucznej inteligencji i uczenia maszynowego w systemach zabezpieczeń technicznych	17
	Efekt uczenia się 9: Charakteryzuje zasady zarządzania bezpieczeństwem obiektów i usług kluczowych	18
	Usługa rozwojowa wspierająca zdobycie kompetencji/kwalifikacji.....	19
	Nazwa kompetencji nr 2: Koordynacja prac instalacyjnych, konserwacyjnych i serwisowych systemów zabezpieczeń technicznych zgodnie z wymaganiami prawno-normatywnymi	23
	Efekt uczenia się 1: Identyfikuje wymagania prawno-normatywne, techniczne i organizacyjne mające zastosowanie do realizacji prac instalacyjnych, konserwacyjnych i serwisowych (naprawczych) systemów zabezpieczeń technicznych.....	23

Efekt uczenia się 2: Identyfikuje zasady planowania i organizacji prac instalacyjnych systemów zabezpieczeń technicznych	24
Efekt uczenia się 3: Identyfikuje zasady planowania i organizacji prac konserwacyjnych oraz serwisowych (naprawczych) systemów zabezpieczeń technicznych	25
Efekt uczenia się 4: Identyfikuje zasady organizacji i nadzoru nad zespołem realizującym prace instalacyjne, konserwacyjne i serwisowe systemów zabezpieczeń technicznych	26
Efekt uczenia się 5: Identyfikuje ryzyka związane z realizacją prac instalacyjnych, konserwacyjnych i serwisowych systemów zabezpieczeń technicznych oraz zasady minimalizowania wpływu tych prac na funkcjonowanie systemów	27
Efekt uczenia się 6: Identyfikuje zasady zapewnienia jakości oraz zgodności realizowanych prac instalacyjnych, konserwacyjnych i serwisowych systemów zabezpieczeń technicznych	28
Usługa rozwojowa wspierająca zdobycie kompetencji/kwalifikacji.....	28
Nazwa kompetencji nr 3: Projektowanie, instalowanie i konserwacja systemów sygnalizacji pożarowej	32
Efekt uczenia się 1: Identyfikuje wymagania prawne, normatywne oraz branżowe dotyczące projektowania, instalowania i konserwacji systemów sygnalizacji pożarowej (SSP) oraz sposoby potwierdzania kwalifikacji w tym zakresie.	32
Efekt uczenia się 2: Analizuje zagrożenie pożarowe obiektu w kontekście projektowania systemu SSP	33
Efekt uczenia się 3: Dobiera elementy systemu sygnalizacji pożarowej (SSP) do warunków technicznych i funkcjonalnych obiektu zgodnie z wybranymi wytycznymi projektowymi	33
Efekt uczenia się 4: Identyfikuje zasady opracowania dokumentacji projektowej oraz podstawowe wymagania techniczne systemu sygnalizacji pożarowej (SSP).	34
Efekt uczenia się 5: Identyfikuje zasady instalowania, uruchamiania i odbioru systemów sygnalizacji pożarowej (SSP).	35
Efekt uczenia się 6: Identyfikuje zasady eksploatacji, konserwacji oraz utrzymania sprawności systemów sygnalizacji pożarowej (SSP).	35
Efekt uczenia się 7: Identyfikuje zasady konfiguracji i przygotowania systemu sygnalizacji pożarowej (SSP) do pracy w obiekcie.	36
Usługa rozwojowa wspierająca zdobycie kompetencji/kwalifikacji.....	37
Nazwa kompetencji nr 4: Zarządzanie cyberbezpieczeństwem w systemach zabezpieczeń technicznych	41

Efekt uczenia się 1: Charakteryzuje podstawowe pojęcia z zakresu cyberbezpieczeństwa systemów zabezpieczeń technicznych	41
Efekt uczenia się 2: Identyfikuje podstawowe wymagania systemu zarządzania bezpieczeństwem informacji zgodnie z normą ISO/IEC 27001 w kontekście systemów zabezpieczeń technicznych ..	42
Efekt uczenia się 3: Identyfikuje podstawowe wymagania prawne w zakresie cyberbezpieczeństwa	42
Efekt uczenia się 4: Identyfikuje podstawowe mechanizmy techniczne funkcjonowania systemu cyberbezpieczeństwa w systemach zabezpieczeń technicznych	43
Efekt uczenia się 5: Charakteryzuje rozwiązania bezpieczeństwa sieciowego dla systemów zabezpieczeń technicznych	44
Efekt uczenia się 6: Ocenia ryzyko cyberbezpieczeństwa w systemach zabezpieczeń technicznych w oparciu o analizę aktywów, zagrożeń i podatności.	44
Efekt uczenia się 7: Analizuje zagrożenia i scenariusze ataków na systemy zabezpieczeń technicznych.....	45
Efekt uczenia się 8: Rozróżnia zdarzenia i incydenty cyberbezpieczeństwa w systemach zabezpieczeń technicznych oraz identyfikuje podstawowe zasady reagowania.	46
Efekt uczenia się 9: Identyfikuje podstawowe metody oceny bezpieczeństwa systemów zabezpieczeń technicznych.	46
Efekt uczenia się 10: Analizuje zagrożenia i incydenty cyberbezpieczeństwa w systemach zabezpieczeń technicznych oraz wykorzystuje dostępne informacje do podejmowania decyzji projektowych i eksploatacyjnych.	47
Usługa rozwojowa wspierająca zdobycie kompetencji/kwalifikacji.....	48
Nazwa kompetencji nr 5: Planowanie i organizacja wykorzystania bezzałogowych statków powietrznych w systemach ochrony obiektów	51
Efekt uczenia się 1: Charakteryzuje rolę oraz możliwości wykorzystania bezzałogowych statków powietrznych (BSP) w systemach ochrony obiektów.....	51
Efekt uczenia się 2: Charakteryzuje przepisy prawne oraz wymagania w zakresie ochrony danych osobowych związane z wykorzystaniem bezzałogowych statków powietrznych (BSP) w systemach ochrony obiektów.....	52
Efekt uczenia się 3: Charakteryzuje zasady analizy ryzyka i podatności obiektu w kontekście wykorzystania BSP jako elementu systemu ochrony	52

Efekt uczenia się 4: Charakteryzuje zasady planowania operacyjnego wykorzystania bezzałogowych statków powietrznych (BSP) w systemach ochrony obiektów	53
Efekt uczenia się 5: Charakteryzuje zasady doboru bezzałogowych statków powietrznych (BSP) oraz systemów obserwacyjnych do zadań ochronnych	54
Efekt uczenia się 6: Charakteryzuje zasady integracji bezzałogowych statków powietrznych (BSP) z systemami zabezpieczeń technicznych oraz organizacją ochrony obiektu.....	54
Usługa rozwojowa wspierająca zdobycie kompetencji/kwalifikacji.....	55
Nazwa kompetencji nr 6: Systemy wykrywania i neutralizacji bezzałogowych statków powietrznych, jako narzędzie służące do ochrony obiektów i obszarów	58
Efekt uczenia się 1: Charakteryzuje zagrożenia związane z wykorzystaniem dronów (bezzałogowych statków powietrznych – BSP) wobec obiektów chronionych oraz cechy tych dronów istotne z punktu widzenia ich wykrywania i przeciwdziałania.....	58
Efekt uczenia się 2: Charakteryzuje zasady analizy ryzyka i podatności obiektu w kontekście zagrożeń z wykorzystaniem dronów	59
Efekt uczenia się 3: Charakteryzuje technologie wykrywania i śledzenia dronów oraz ich zastosowanie w ochronie obiektów	59
Efekt uczenia się 4: Charakteryzuje zasady doboru i integracji systemu detekcji dronów z systemem bezpieczeństwa obiektu	60
Efekt uczenia się 5: Charakteryzuje zasady reagowania na incydenty z wykorzystaniem dronów w systemie bezpieczeństwa obiektu z uwzględnieniem ograniczeń prawnych i organizacyjnych	61
Efekt uczenia się 6: Charakteryzuje ramy prawne oraz zasady współdziałania z właściwymi organami i służbami w przypadku incydentów z wykorzystaniem dronów, w kontekście ochrony obiektu i bezpieczeństwa przestrzeni powietrznej	61
Usługa rozwojowa wspierająca zdobycie kompetencji/kwalifikacji.....	62
Nazwa kompetencji nr 7: Audytowanie systemów zabezpieczeń technicznych w oparciu o wytyczne PN-EN ISO/IEC 27001:2023-08	66
Efekt uczenia się 1: Charakteryzuje cele, zakres oraz strukturę systemu zarządzania bezpieczeństwem informacji (SZBI) w kontekście audytu wewnętrznego systemów zabezpieczeń technicznych.....	66
Efekt uczenia się 2: Charakteryzuje zasady prowadzenia audytu wewnętrznego zgodnie z PN-EN ISO 19011:2018-08 w kontekście systemów zabezpieczeń technicznych	67

Efekt uczenia się 3: Przygotowuje plan audytu wewnętrznego systemów zabezpieczeń technicznych zgodnie z wymaganiami PN-EN ISO 19011:2018-08	67
Efekt uczenia się 4: Prowadzi ocenę zgodności systemów zabezpieczeń technicznych z wymaganiami normatywnymi oraz wewnętrznymi kryteriami organizacji	68
Efekt uczenia się 5: Opracowuje raport z audytu systemów zabezpieczeń technicznych zgodnie z wymaganiami PN-EN ISO 19011:2018-08 oraz PN-EN ISO/IEC 27001:2023-08.....	69
Efekt uczenia się 6: Charakteryzuje zasady postępowania z niezgodnościami oraz zasady działań poaudytowych w systemach zabezpieczeń technicznych zgodnie z PN-EN ISO/IEC 27001:2023-08 oraz PN-EN ISO 19011:2018-08	69
Usługa rozwojowa wspierająca zdobycie kompetencji/kwalifikacji.....	70
Nazwa kompetencji nr 8: Zasady projektowania i eksploatacji systemów VSS/CCTV IP	74
Efekt uczenia się 1: Charakteryzuje wymagania normatywne, prawne i branżowe dotyczące projektowania i eksploatacji systemów VSS/CCTV IP	74
Efekt uczenia się 2: Charakteryzuje podstawowe zasady obrazowania w systemach VSS/CCTV IP w kontekście doboru kamery i obiektywu	75
Efekt uczenia się 3: Charakteryzuje zasady transmisji, kompresji, zapisu, przechowywania i eksportu obrazu w systemach VSS/CCTV IP w kontekście wymagań jakościowych i dowodowych.....	75
Efekt uczenia się 4: Charakteryzuje zastosowanie analityki wizyjnej, w tym rozwiązań opartych na AI, w systemach VSS/CCTV w systemach VSS/CCTV IP oraz jej zależność od jakości obrazu i architektury systemu.....	76
Efekt uczenia się 5: Charakteryzuje zasady opracowywania wymagań użytkowych (OR), weryfikacji systemu VSS/CCTV IP przed odbiorem oraz możliwości potwierdzenia jego zgodności poprzez proces oceny i certyfikacji	77
Efekt uczenia się 6: Opracowuje wstępne założenia projektowe oraz konfiguruje podstawowe parametry systemu VSS/CCTV IP w środowisku testowym	78
Usługa rozwojowa wspierająca zdobycie kompetencji/kwalifikacji.....	78
Nazwa kompetencji nr 9: Zadania i odpowiedzialność administratora i operatora Centrum Monitorowania Alarmów	82
Efekt uczenia się 1: Charakteryzuje rolę, funkcje i odpowiedzialność administratora oraz operatora Centrum Monitorowania Alarmów (CMA)	82

Efekt uczenia się 2: Charakteryzuje zasady organizacji i bieżącego funkcjonowania Centrum Monitorowania Alarmów w zakresie obsługi sygnałów alarmowych i informacji z wielu monitorowanych obiektów	83
Efekt uczenia się 3: Charakteryzuje zasady analizowania, klasyfikacji i priorytetyzacji sygnałów wpływających do Centrum Monitorowania Alarmów	83
Efekt uczenia się 4: Charakteryzuje zasady analizy obrazu oraz wykorzystania funkcji systemów monitoringu wizyjnego w pracy operatora Centrum Monitorowania Alarmów	84
Efekt uczenia się 5: Charakteryzuje zasady współpracy operacyjnej, komunikacji oraz organizacji pracy w Centrum Monitorowania Alarmów	85
Usługa rozwojowa wspierająca zdobycie kompetencji/kwalifikacji.....	86

I. Opis sektora

Sektor Ochrony i Bezpieczeństwa Mienia i Osób ma istotne znaczenie dla gospodarki i społeczeństwa, zapewniając bezpieczeństwo oraz sprawne funkcjonowanie instytucji publicznych i prywatnych. Sektor nieustannie ewoluuje, odchodząc od tradycyjnej koncepcji ochrony fizycznej na rzecz bardziej złożonych i zaawansowanych rozwiązań obejmujących m.in. nowoczesne systemy zabezpieczenia technicznego, zarządzanie kryzysowe, cyberbezpieczeństwo i ochronę infrastruktury krytycznej. Jest ściśle powiązany z niemal każdą gałęzią gospodarki, wspierając działalność od etapu projektowania inwestycji, przez instalację systemów zabezpieczeń, ochronę infrastruktury i pracowników, aż po zapewnienie ciągłości operacyjnej. Odgrywa kluczową rolę w zabezpieczaniu obiektów infrastruktury krytycznej, szczególnie w kontekście rosnących zagrożeń geopolitycznych i implementacji regulacji na poziomie UE, np. Dyrektywy CER.

Sektor łączy tradycyjne metody ochrony z nowoczesnymi technologiami i szerokim zakresem działań zarządczych oraz procedur bezpieczeństwa. Jego rozwój wiąże się z dynamicznym postępem technologicznym, w tym integracją systemów bezpieczeństwa z inteligentnymi systemami zarządzania budynkami, zastosowaniem sztucznej inteligencji i analizy big data czy rozwojem systemów monitorowania w czasie rzeczywistym, co wymaga ciągłego podnoszenia kompetencji pracowników.

II. Analiza stanu sektora z punktu widzenia potrzeb kompetencyjnych, opisanych w dalszej części dokumentu

Analiza stanu sektora:

Sektor ochrony i bezpieczeństwa mienia i osób w Polsce obejmuje (wg danych REGON, czerwiec 2024 r.) 7 595 zarejestrowanych podmiotów, zatrudniających łącznie ok. 117 743 pracowników (GUS, stan na 31.03.2024 r.), a jego przychody netto ze sprzedaży wyniosły w 2023 roku 15,8 mld zł. Tradycyjne usługi ochrony fizycznej coraz częściej uzupełniane lub zastępowane są przez zaawansowane systemy zabezpieczeń technicznych (CCTV/VSS, SSWiN, SKD, PSIM) oraz systemy sygnalizacji pożarowej (SSP). Według raportu „Branża ochrony w Polsce 2024” (Polski Związek Pracodawców Ochrona), systematycznie rośnie zainteresowanie rozwiązaniami technicznymi

umożliwiającymi wprowadzanie oszczędności przy jednoczesnym utrzymaniu wysokiej jakości usług. Raport A&S Polska z 2024 roku wskazuje, że rynek zabezpieczeń technicznych ulega dynamicznej transformacji pod wpływem automatyzacji, sztucznej inteligencji i integracji systemów, co wymaga od specjalistów nieustannego podnoszenia kwalifikacji.

Perspektywy i trendy w rozwoju sektora:

W perspektywie najbliższych 5 lat sektor będzie kształtowany przez trendy technologiczne i regulacyjne. Na poziomie europejskim implementacja Dyrektywy CER (o odporności podmiotów krytycznych) i Dyrektywy NIS 2 nakłada na podmioty krytyczne obowiązek wdrożenia zaawansowanych środków bezpieczeństwa fizycznego i cybernetycznego, generując bezpośredni popyt na kompetencje objęte niniejszą rekomendacją. Równolegle dynamicznie rozwijają się: sztuczna inteligencja w analityce wizyjnej, rozwiązania IoT w nadzorze sieciowym oraz integracja systemów zabezpieczeń z platformami PSIM i BMS. Dynamicznie rozwijającym się segmentem Sektora jest również zastosowanie bezzałogowych statków powietrznych (BSP) w ochronie obiektów. Raport Allied Market Research „Drone Surveillance Market 2023–2032” wskazuje, że zastosowanie BSP w sektorze ochrony może obniżyć koszty operacyjne przy jednoczesnym zwiększeniu skuteczności monitorowania rozległych terenów.

Wyzwania sektora:

Sektor stoi przed kilkoma istotnymi wyzwaniami. Rosnące zapotrzebowanie na kwalifikowanych pracowników zabezpieczenia technicznego, w szczególności posiadających wpis na listę, o której mowa w art. 27 ustawy o ochronie osób i mienia, przy jednoczesnym niedoborze takich kadr, stanowi jeden z kluczowych problemów branży. Pracodawcy sygnalizują, że możliwości nowoczesnych systemów są nierzadko wykorzystywane jedynie w około 15% z powodu braku odpowiedniej wiedzy operatorów i managerów bezpieczeństwa (Grzesik, Ł., Głos branży 6/2023, A&S Polska; za: Araminowicz i in., 2025, s. 129). Narastający deficyt wykwalifikowanych kadr pogłębia fakt, że niska atrakcyjność płacowa wielu stanowisk ogranicza motywację pracowników do podnoszenia kwalifikacji, a wielu pracodawców, pod presją konkurencji cenowej, ogranicza budżety szkoleniowe. Dynamiczny rozwój zagrożeń hybrydowych, cybernetycznych i dronowych wymaga natomiast stałej aktualizacji wiedzy całego środowiska branżowego.

Źródła informacji i sposób ich pozyskiwania:

Główne źródło:

Araminowicz, A., Klatta, P., Radochoński, T., Sierżyńska, M. (2025). Ochrona i Bezpieczeństwo Mienia i Osób – analiza sektora. Raport z badania. Wydanie II zaktualizowane. Kraków: MABEA sp. z o.o. https://www.techom.com/wp-content/uploads/2025/04/Raport_MABEA_TECHOM_2025.pdf

Zastosowane metody: (1) analiza danych zastanych: akty prawne, dane statystyczne, raporty i artykuły branżowe; (2) badanie jakościowe: 2 zogniskowane wywiady grupowe i panel ekspercki (łącznie 29 osób, m.in. przedstawiciele: POLALARM, Polska Izba Ochrony, Polska Izba Systemów Bezzałogowych, ABW, KGP, WOT, RCB, uczelni wyższych, przedsiębiorców sektora); (3) badanie ankietowe: 46 respondentów reprezentujących dostawców usług ochrony i zabezpieczeń technicznych, zamawiających i podmioty współpracujące z sektorem. Badanie prowadzono w dwóch etapach: sierpień–wrzesień 2024 oraz styczeń-marzec 2025.

Zdiagnozowane luki kompetencyjne (skala 1-5, gdzie 5 = „bardzo brakuje”): ewolucja zagrożeń - 4,35; postęp technologiczny - 4,07; zarządzanie bezpieczeństwem - 4,04. Jako obszary priorytetowe do dofinansowania usług rozwojowych respondenci wskazali przede wszystkim zarządzanie bezpieczeństwem (34 wskazania), ewolucję zagrożeń (33 wskazania) oraz postęp technologiczny (28 wskazań).

Dodatkowe źródła danych:

- GUS, dane o zatrudnieniu w sektorze: <https://stat.gov.pl>
- Rejestr REGON, liczba podmiotów sektora: <https://wyszukiwarkaregon.stat.gov.pl/>
- Polski Związek Pracodawców Ochrona (2024). „Branża ochrony w Polsce. Raport 2024. Kondycja, prognozy, wyzwania” https://pzpochrona.pl/wp-content/uploads/pzpo_raport_2024_final-002-1.pdf
- a&s Polska (2024). „Jaki będzie rok 2024 dla polskiego rynku security?” <https://aspolska.pl/rynek-security-czego-spodziewac-sie-w-roku-2024/>
- KPMG Polska (2024). „Barometr Cyberbezpieczeństwa 2024. Na fali, czy w labiryncie regulacji?” <https://kpmg.com/pl/pl/home/insights/2024/02/barometr-cyberbezpieczenstwa-2024.html>

- Ministerstwo Cyfryzacji (2024). „Krajobraz cyberprzestrzeni: roczne sprawozdanie o cyberbezpieczeństwie. Sprawozdanie Pełnomocnika Rządu ds. Cyberbezpieczeństwa za 2024” <https://www.gov.pl/web/cyfryzacja/krajobraz-cyberprzestrzeni-roczne-sprawozdanie-o-cyberbezpieczenstwie>
- Allied Market Research (2023). „Drone Surveillance Market by Type and Application: Global Opportunity Analysis and Industry Forecast, 2023–2032” <https://seris.pl/blog/poradnik-bezpieczenstwa/drony-w-ochronie-objektow-przyszlosc-bezpieczenstwa-infrastruktury-krytycznej-i-przemyslowej/>
- a&s Polska (2024). „RAPORT Security 50. Rok 2023 w branży security” <https://aspolska.pl/raport-security-50/>

III. Zapotrzebowanie na kompetencje/kwalifikacje w sektorze

Nazwa kompetencji nr 1: Projektowanie, instalowanie, konserwacja, eksploatacja i odbiór systemów zabezpieczeń technicznych stopni 1-4/wojskowych dokumentów normatywnych

Czy kompetencja/kwalifikacja jest włączona do Zintegrowanego Systemu Kwalifikacji?

NIE

Krótką charakterystyka kompetencji

Projektowanie, instalowanie, konserwacja, eksploatacja i odbiór systemów zabezpieczeń technicznych stopni 1-4/wojskowych dokumentów normatywnych.

Efekt uczenia się 1: Charakteryzuje wymagania prawno-normatywne w zakresie systemów zabezpieczeń technicznych

Kryteria weryfikacji:

- identyfikuje wymagania prawne, normy oraz wytyczne do ich stosowania w zakresie systemów zabezpieczeń technicznych,
- rozdziela stopnie zabezpieczenia wynikajace z norm,
- identyfikuje wymagania wojskowych dokumentów normatywnych,
- 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.

Metody walidacji:

- Ad.A. test teoretyczny
- Ad.B. test teoretyczny
- Ad.C. test teoretyczny
- Ad.D. test teoretyczny
- Ad.E. test teoretyczny
- Ad.F. test teoretyczny
- Ad.G. test teoretyczny

Efekt uczenia się 2: Charakteryzuje proces szacowania ryzyka bezpieczeństwa obiektów prowadzony zgodnie z wymaganiami prawno-normatywnymi**Kryteria weryfikacji:**

- 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.

Metody walidacji:

- Ad.A. test teoretyczny
- Ad.B. test teoretyczny
- Ad.C. test teoretyczny
- Ad.D. test teoretyczny
- Ad.E. test teoretyczny

Efekt uczenia się 3: Charakteryzuje systemy zabezpieczeń technicznych oraz ich zastosowanie

Kryteria weryfikacji:

- 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.

Metody walidacji:

- Ad.A. test teoretyczny
- Ad.B. test teoretyczny
- Ad.C. test teoretyczny
- Ad.D. test teoretyczny
- Ad.E. test teoretyczny
- Ad.F. test teoretyczny
- Ad.G. test teoretyczny
- Ad.H. test teoretyczny
- Ad.I. test teoretyczny
- Ad.J. test teoretyczny
- Ad.K. test teoretyczny

Efekt uczenia się 4: Charakteryzuje zasady projektowania, instalowania, konserwacji, odbioru i eksploatacji systemów zabezpieczeń technicznych dla stopni 1-4 i wojskowych dokumentów normatywnych

Kryteria weryfikacji:

- A. 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 zabezpieczeń technicznych,
- G. identyfikuje wymagania w zakresie wystawiania deklaracji zgodności,
- H. identyfikuje zasady oceny zgodności projektu systemów zabezpieczeń technicznych i certyfikacji zainstalowanego systemu zabezpieczeń technicznych przez upoważnioną w rozumieniu przepisów o normalizacji lub ocenie zgodności jednostkę certyfikującą,
- I. identyfikuje ścieżkę do certyfikacji zainstalowanego systemu zabezpieczeń technicznych,
- J. charakteryzuje znaczenie certyfikacji systemu zabezpieczeń technicznych po zainstalowaniu,
- K. wskazuje zasady prowadzenia dokumentacji eksploatacyjnej systemów zabezpieczeń technicznych – dla sfery cywilnej i wojskowej,
- L. oblicza bilans energetyczny dla wskazanych systemów zabezpieczeń technicznych.

Metody walidacji:

- Ad.A. test teoretyczny
- Ad.B. test teoretyczny

- Ad.C. test teoretyczny
- Ad.D. test teoretyczny
- Ad.E. test teoretyczny
- Ad.F. test teoretyczny
- Ad.G. test teoretyczny
- Ad.H. test teoretyczny
- Ad.I. test teoretyczny
- Ad.J. test teoretyczny
- Ad.K. test teoretyczny
- Ad.L. test teoretyczny

Efekt uczenia się 5: Charakteryzuje zasady projektowania infrastruktury sieciowej dla systemów zabezpieczeń technicznych

Kryteria weryfikacji:

- 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).

Metody walidacji:

- Ad.A. test teoretyczny
- Ad.B. test teoretyczny
- Ad.C. test teoretyczny
- Ad.D. test teoretyczny
- Ad.E. test teoretyczny
- Ad.F. test teoretyczny

Ad.G. test teoretyczny

Efekt uczenia się 6: Charakteryzuje podstawowe zasady cyberbezpieczeństwa w systemach zabezpieczeń technicznych

Kryteria weryfikacji:

- 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,
- J. identyfikuje dobre praktyki w zakresie cyberbezpieczeństwa systemów zabezpieczeń technicznych.

Metody walidacji:

- Ad.A. test teoretyczny
- Ad.B. test teoretyczny
- Ad.C. test teoretyczny
- Ad.D. test teoretyczny
- Ad.E. test teoretyczny
- Ad.F. test teoretyczny

- Ad.G. test teoretyczny
- Ad.H. test teoretyczny
- Ad.I. test teoretyczny
- Ad.J. test teoretyczny

Efekt uczenia się 7: Charakteryzuje podstawowe zasady kosztorysowania systemów zabezpieczeń technicznych

Kryteria weryfikacji:

- 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.

Metody walidacji:

- Ad.A. test teoretyczny
- Ad.B. test teoretyczny
- Ad.C. test teoretyczny
- Ad.D. test teoretyczny
- Ad.E. test teoretyczny

Efekt uczenia się 8: Wykorzystuje narzędzia sztucznej inteligencji i uczenia maszynowego w systemach zabezpieczeń technicznych

Kryteria weryfikacji:

- 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.

Metody walidacji:

- Ad.A. test teoretyczny
Ad.B. test teoretyczny
Ad.C. test teoretyczny
Ad.D. test teoretyczny

Efekt uczenia się 9: Charakteryzuje zasady zarządzania bezpieczeństwem obiektów i usług kluczowych

Kryteria weryfikacji:

- 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.

Metody walidacji:

- Ad.A. test teoretyczny
Ad.B. test teoretyczny
Ad.C. test teoretyczny
Ad.D. test teoretyczny
Ad.E. test teoretyczny

Szacowana skala niedoboru kompetencji/kwalifikacji

2 095

Usługa rozwojowa wspierająca zdobycie kompetencji/kwalifikacji

Standard usługi:

Usługa realizowana przez podmiot wpisany do Bazy Usług Rozwojowych, spełniający wymagania określone w Rozporządzeniu Ministra Funduszy i Polityki Regionalnej z dnia 28 lipca 2023 r. w sprawie rejestru podmiotów świadczących usługi rozwojowe (Dz.U. z 2023 r. poz. 1686), zgodnie z zasadami określonymi w Regulaminie Bazy Usług Rozwojowych oraz w niniejszej rekomendacji.

Podmiot realizujący usługę powinien być jednocześnie wpisany do Rejestru Szkół i Placówek Oświatowych jako placówka kształcenia ustawicznego, zgodnie z ustawą z dnia 14 grudnia 2016 r. – Prawo oświatowe (Dz.U. z późn. zm.), w szczególności art. 2 pkt 4 oraz art. 168.

Szkolenie realizowane jest w formie kursu pracownika zabezpieczenia technicznego, o którym mowa w art. 27 ust. 1 pkt 4 ustawy z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (Dz.U. 2025 poz. 532), i umożliwia uzyskanie wpisu na listę kwalifikowanych pracowników zabezpieczenia technicznego.

Ponadto realizacja usługi powinna uwzględniać dobre praktyki wskazane w załączniku nr 1 do Narodowego Programu Ochrony Infrastruktury Krytycznej 2023 „Standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej – dobre praktyki i rekomendacje”, zgodnie z którymi szkolenia w obszarze systemów zabezpieczeń technicznych powinny być prowadzone przez wyspecjalizowane w tym zakresie placówki kształcenia ustawicznego.

Warunki w zakresie kompetencji osób przystępujących do usługi:

- a) Posiada wykształcenie co najmniej zawodowe lub średnie.

Maksymalna liczebność grupy szkoleniowej:

30 osób – wersja zdalna w czasie rzeczywistym lub

30 osób – forma stacjonarna

Minimalny czas trwania usługi:

32 h zegarowe

Minimalne wymagania w zakresie zasobów:

- a) sala szkoleniowa spełniająca standardy jakości prowadzenia zajęć dydaktycznych, wyposażona w rzutnik multimedialny lub ekran do prezentacji materiałów szkoleniowych (dla usługi realizowanej w formie stacjonarnej lub hybrydowej),
- b) sprzęt komputerowy dla trenera wraz z oprogramowaniem umożliwiającym realizację programu szkolenia oraz prezentację materiałów dydaktycznych (dla usługi realizowanej w formie stacjonarnej lub hybrydowej),
- c) stabilne łącze internetowe umożliwiające prowadzenie zajęć w czasie rzeczywistym oraz przesyłanie materiałów szkoleniowych (dla usługi realizowanej w formie zdalnej lub hybrydowej),
- d) urządzenia umożliwiające komunikację audio-wideo w czasie rzeczywistym, w szczególności kamera oraz mikrofon dla trenera (dla usługi realizowanej w formie zdalnej lub hybrydowej),
- e) oprogramowanie umożliwiające prowadzenie zajęć w trybie zdalnym w czasie rzeczywistym, w szczególności platformę wideokonferencyjną (np. Microsoft Teams lub rozwiązanie równoważne), zapewniającą:
 - transmisję audio i wideo,
 - możliwość prezentacji materiałów szkoleniowych,
 - komunikację z uczestnikami usługi oraz zadawanie pytań w trakcie zajęć,
- f) zasób legalnych wersji dokumentów normalizacyjnych, o których mowa w art. 2 pkt 3 ustawy z dnia 12 września 2002 r. o normalizacji (Dz.U. 2015 poz. 1483), w zakresie odpowiadającym efektom uczenia się realizowanym w ramach usługi,
- g) materiały szkoleniowe dla uczestników usługi w formie elektronicznej lub papierowej.

Wymagania w zakresie kompetencji trenera:

Kompetencje określone w §6 Rozporządzenia Ministra Funduszy i Polityki Regionalnej z dnia 28 lipca 2023 r. w sprawie rejestru podmiotów świadczących usługi rozwojowe (Dz.U. z 2023 r. poz. 1686) oraz:

- a) min. **12 miesięcy** doświadczenia w zakresie odpowiadającym efektom uczenia się i kryteriom weryfikacji,

- b) doświadczenie w prowadzeniu szkoleń lub doradztwa w temacie usługi - min. **100 godzin**.

Sposób oraz metody realizacji usługi:

Szkolenie może być realizowane w formie stacjonarnej, zdalnej lub hybrydowej.

Usługa szkoleniowa powinna zostać zrealizowana z wykorzystaniem następujących metod: wykłady, prezentacje studiów przypadków (case studies), prezentacja rzeczywistych projektów z branży zabezpieczeń technicznych, demonstracje możliwości sprzętu i systemów.

Usługa musi zostać zakończona weryfikacją efektów uczenia się, zgodnie ze standardami określonymi w Rozporządzeniu Ministra Funduszy i Polityki Regionalnej z dnia 28 lipca 2023 r. w sprawie rejestru podmiotów świadczących usługi rozwojowe (Dz.U. z 2023 r. poz. 1686) oraz Rozporządzeniu Ministra Edukacji i Nauki z dnia 6 października 2023 r. w sprawie kształcenia ustawicznego w formach pozaszkolnych (Dz.U. 2023 poz. 2175), przeprowadzoną metodami: test teoretyczny (pisemny).

Potencjalni uczestnicy usług rozwojowych

Osoby odpowiedzialne lub osoby, którym przedsiębiorca zamierza powierzyć odpowiedzialność za:

- a) wykonywanie zadań pracownika zabezpieczenia technicznego w rozumieniu ustawy o ochronie osób i mienia,
- b) przygotowanie do ubiegania się o wpis na listę kwalifikowanych pracowników zabezpieczenia technicznego,
- c) projektowanie, instalowanie, konserwację oraz eksploatację systemów zabezpieczenia technicznego,
- d) nadzór nad funkcjonowaniem systemów zabezpieczeń technicznych w obiektach chronionych,
- e) zarządzanie bezpieczeństwem obiektów w części dotyczącej zabezpieczeń technicznych, w tym koordynację działań ochronnych i technicznych,
- f) opracowywanie i aktualizację planów ochrony w zakresie zabezpieczeń technicznych,
- g) realizację zadań w obszarze ochrony infrastruktury krytycznej, w tym w zakresie systemów zabezpieczeń technicznych,

- h) prowadzenie inwestycji w systemy zabezpieczeń technicznych oraz ocenę zgodności rozwiązań z wymaganiami przepisów prawa i norm branżowych,
- i) kierowanie zespołami pracowników zabezpieczenia technicznego,
- j) realizację czynności związanych z zabezpieczeniami technicznymi na rzecz jednostek podległych lub nadzorowanych przez Ministra Obrony Narodowej,
- k) pełnienie funkcji związanych z organizacją i nadzorem nad ochroną obiektów resortu obrony narodowej w części dotyczącej zabezpieczeń technicznych.

Dodatkowe uwagi

Brak

Nazwa kompetencji nr 2: Koordynacja prac instalacyjnych, konserwacyjnych i serwisowych systemów zabezpieczeń technicznych zgodnie z wymaganiami prawno-normatywnymi

Czy kompetencja/kwalifikacja jest włączona do Zintegrowanego Systemu Kwalifikacji?

NIE

Krótką charakterystyka kompetencji

Koordynacja prac instalacyjnych, konserwacyjnych i serwisowych systemów zabezpieczeń technicznych zgodnie z wymaganiami prawno-normatywnymi.

Efekt uczenia się 1: Identyfikuje wymagania prawno-normatywne, techniczne i organizacyjne mające zastosowanie do realizacji prac instalacyjnych, konserwacyjnych i serwisowych (naprawczych) systemów zabezpieczeń technicznych

Kryteria weryfikacji:

- A. charakteryzuje budowę i zasady działania różnych systemów zabezpieczeń (np. systemów dozoru wizyjnego, sygnalizacji włamania i napadu, kontroli dostępu, sygnalizacji pożaru, ochrony perymetrycznej),
- B. identyfikuje zależności i integracje pomiędzy poszczególnymi systemami zabezpieczeń technicznych oraz ich wpływ na zakres i kolejność prac,
- C. rozróżnia zakres zastosowania PN-EN 16763 oraz norm dotyczących systemów zabezpieczeń technicznych i wytycznych do ich stosowania w odniesieniu do instalowania, konserwacji i serwisu,
- D. identyfikuje wymagania wynikające ze stopni zabezpieczenia określonych w normach dla SSWiN, SKD oraz VSS/CCTV, z uwzględnieniem wytycznych do stosowania tych norm, oraz wskazuje konsekwencje przyjętego stopnia zabezpieczenia dla organizacji prac instalacyjnych, konserwacyjnych i serwisowych,
- E. wskazuje wymagania dotyczące okresu próbnego i odbioru końcowego systemów zabezpieczeń technicznych, w tym zakres weryfikacji dokumentacji powykonawczej, parametrów technicznych i poprawności działania systemu,
- F. rozróżnia zakres odpowiedzialności projektanta, wykonawcy, koordynatora prac oraz operatora obiektu w procesie zapewniania zgodności realizowanych prac z wymaganiami norm i przepisów,

- G. identyfikuje zakres odpowiedzialności koordynatora prac w zakresie nadzorowania zgodności realizowanych robót z dokumentacją wykonawczą oraz kompletności dokumentacji powykonawczej i eksploatacyjnej przed odbiorem,
- H. rozróżnia odbiór instalacyjny systemu zabezpieczeń technicznych od certyfikacji zainstalowanego systemu na zgodność z odpowiednią Polską Normą.

Metody walidacji:

- Ad.A. test teoretyczny
- Ad.B. test teoretyczny
- Ad.C. test teoretyczny
- Ad.D. test teoretyczny
- Ad.E. test teoretyczny
- Ad.F. test teoretyczny
- Ad.G. test teoretyczny
- Ad.H. test teoretyczny

Efekt uczenia się 2: Identyfikuje zasady planowania i organizacji prac instalacyjnych systemów zabezpieczeń technicznych**Kryteria weryfikacji:**

- A. rozróżnia etapy realizacji prac instalacyjnych systemów zabezpieczeń technicznych, w tym przygotowanie, instalowanie, uruchomienie, testowanie i przekazanie do odbioru,
- B. identyfikuje elementy dokumentacji projektowej/wykonawczej niezbędne do prawidłowej organizacji prac instalacyjnych,
- C. wskazuje czynniki wpływające na kolejność i harmonogram prac instalacyjnych, w tym zależności międzybranżowe oraz integrację z innymi systemami technicznymi obiektu,
- D. rozróżnia wymagania dotyczące koordynacji prac instalacyjnych w strefach ochrony oraz w obiektach o podwyższonych wymaganiach bezpieczeństwa,
- E. identyfikuje wymagania w zakresie zapewnienia bezpieczeństwa i higieny pracy oraz zabezpieczenia miejsca prowadzenia robót instalacyjnych,
- F. wskazuje działania organizacyjne minimalizujące ryzyko zakłócenia funkcjonowania istniejących systemów zabezpieczeń technicznych podczas prowadzenia prac instalacyjnych,

- G. rozróżnia sytuacje wymagające przeprowadzenia testów częściowych oraz testów funkcjonalnych przed zgłoszeniem systemu do odbioru.

Metody walidacji:

- Ad.A. test teoretyczny
- Ad.B. test teoretyczny
- Ad.C. test teoretyczny
- Ad.D. test teoretyczny
- Ad.E. test teoretyczny
- Ad.F. test teoretyczny
- Ad.G. test teoretyczny

Efekt uczenia się 3: Identyfikuje zasady planowania i organizacji prac konserwacyjnych oraz serwisowych (naprawczych) systemów zabezpieczeń technicznych**Kryteria weryfikacji:**

- A. rozróżnia konserwację planową od serwisu i naprawy systemów zabezpieczeń technicznych oraz wskazuje ich odmienne cele i zakres,
- B. identyfikuje źródła wymagań dotyczących konserwacji i serwisu systemów zabezpieczeń technicznych, w tym normy, specyfikacje techniczne, dokumentację producenta, dokumentację powykonawczą oraz postanowienia umów serwisowych,
- C. wskazuje elementy harmonogramu przeglądów technicznych i konserwacji systemów zabezpieczeń technicznych,
- D. rozróżnia sytuacje wymagające podjęcia działań serwisowych w trybie pilnym od działań planowych,
- E. identyfikuje zasady organizacji prac serwisowych w obiekcie czynnym, w tym wymagania dotyczące dostępu do systemów, nadzoru nad pracami oraz rejestrowania wykonanych czynności,
- F. wskazuje działania organizacyjne ograniczające wpływ prac konserwacyjnych i serwisowych na ciągłość działania systemów zabezpieczeń technicznych,
- G. rozróżnia obowiązki związane z dokumentowaniem przeglądów, konserwacji i napraw oraz aktualizacją dokumentacji powykonawczej po wykonanych pracach.

Metody walidacji:

- Ad.A. test teoretyczny
- Ad.B. test teoretyczny
- Ad.C. test teoretyczny
- Ad.D. test teoretyczny
- Ad.E. test teoretyczny
- Ad.F. test teoretyczny
- Ad.G. test teoretyczny

Efekt uczenia się 4: Identyfikuje zasady organizacji i nadzoru nad zespołem realizującym prace instalacyjne, konserwacyjne i serwisowe systemów zabezpieczeń technicznych**Kryteria weryfikacji:**

- A. rozróżnia role i zakres odpowiedzialności członków zespołu realizującego prace instalacyjne, konserwacyjne i serwisowe, w tym instalatora, serwisanta oraz koordynatora prac,
- B. identyfikuje wymagania dotyczące kwalifikacji i uprawnień osób wykonujących czynności instalacyjne, konserwacyjne i serwisowe systemów zabezpieczeń technicznych,
- C. wskazuje zasady przydzielania zadań w zespole z uwzględnieniem kompetencji oraz zakresu odpowiedzialności poszczególnych osób,
- D. rozróżnia sytuacje wymagające bezpośredniego nadzoru koordynatora nad realizacją prac,
- E. identyfikuje zasady raportowania postępu prac oraz dokumentowania istotnych zdarzeń w trakcie realizacji robót,
- F. wskazuje działania organizacyjne podejmowane w przypadku stwierdzenia niezgodności, błędów wykonawczych lub odstępstw od dokumentacji,
- G. rozróżnia zasady komunikacji z inwestorem, użytkownikiem obiektu oraz innymi wykonawcami w zakresie uzgodnień technicznych i organizacyjnych.

Metody walidacji:

- Ad.A. test teoretyczny
- Ad.B. test teoretyczny
- Ad.C. test teoretyczny
- Ad.D. test teoretyczny

Ad.E. test teoretyczny

Ad.F. test teoretyczny

Ad.G. test teoretyczny

Efekt uczenia się 5: Identyfikuje ryzyka związane z realizacją prac instalacyjnych, konserwacyjnych i serwisowych systemów zabezpieczeń technicznych oraz zasady minimalizowania wpływu tych prac na funkcjonowanie systemów

Kryteria weryfikacji:

- A. identyfikuje typowe ryzyka techniczne, organizacyjne i operacyjne związane z realizacją prac instalacyjnych, konserwacyjnych i serwisowych systemów zabezpieczeń technicznych,
- B. rozróżnia ryzyka wynikające z wyłączenia systemu, ograniczenia jego funkcjonalności lub ingerencji w jego konfigurację,
- C. wskazuje działania organizacyjne i techniczne ograniczające wpływ prowadzonych prac na ciągłość działania systemów zabezpieczeń technicznych,
- D. rozróżnia sytuacje wymagające zastosowania rozwiązań tymczasowych lub kompensacyjnych w okresie prowadzenia prac,
- E. identyfikuje zasady postępowania w przypadku wystąpienia incydentu podczas realizacji prac, w tym awarii, uszkodzenia elementów systemu lub nieuprawnionej ingerencji w system,
- F. wskazuje zasady dokumentowania incydentów oraz przekazywania informacji o zdarzeniach osobom odpowiedzialnym po stronie wykonawcy i użytkownika systemu,
- G. rozróżnia sytuacje wymagające wstrzymania prac ze względu na zagrożenie bezpieczeństwa lub ryzyko istotnego zakłócenia funkcjonowania systemu.

Metody walidacji:

Ad.A. test teoretyczny

Ad.B. test teoretyczny

Ad.C. test teoretyczny

Ad.D. test teoretyczny

Ad.E. test teoretyczny

Ad.F. test teoretyczny

Ad.G. test teoretyczny

Efekt uczenia się 6: Identyfikuje zasady zapewnienia jakości oraz zgodności realizowanych prac instalacyjnych, konserwacyjnych i serwisowych systemów zabezpieczeń technicznych

Kryteria weryfikacji:

- A. identyfikuje elementy podlegające kontroli jakości podczas realizacji prac instalacyjnych, konserwacyjnych i serwisowych,
- B. wskazuje etapy realizacji prac, na których powinny być prowadzone kontrole częściowe oraz weryfikacja zgodności z dokumentacją,
- C. rozróżnia rodzaje niezgodności mogących wystąpić w trakcie realizacji prac oraz wskazuje działania korygujące i zapobiegawcze,
- D. identyfikuje zasady wprowadzania zmian w trakcie realizacji prac oraz dokumentowania odstępstw od dokumentacji,
- E. wskazuje zakres dokumentów wymaganych do przekazania systemu po zakończeniu prac instalacyjnych lub serwisowych,
- F. rozróżnia odbiór instalacyjny systemu od oceny zgodności i certyfikacji oraz wskazuje działania wykonawcy w przypadku stwierdzenia niezgodności, w tym obowiązek usunięcia niezgodności i aktualizacji dokumentacji.

Metody walidacji:

- Ad.A. test teoretyczny
- Ad.B. test teoretyczny
- Ad.C. test teoretyczny
- Ad.D. test teoretyczny
- Ad.E. test teoretyczny
- Ad.F. test teoretyczny

Szacowana skala niedoboru kompetencji/kwalifikacji

1 585

Usługa rozwojowa wspierająca zdobycie kompetencji/kwalifikacji

Standard usługi:

Usługa realizowana przez podmiot wpisany do Bazy Usług Rozwojowych, spełniający wymagania określone w Rozporządzeniu Ministra Funduszy i Polityki Regionalnej z dnia

28 lipca 2023 r. w sprawie rejestru podmiotów świadczących usługi rozwojowe (Dz.U. z 2023 r. poz. 1686), zgodnie z zasadami określonymi w Regulaminie Bazy Usług Rozwojowych oraz w niniejszej rekomendacji.

Warunki w zakresie kompetencji osób przystępujących do usługi:

brak

Maksymalna liczebność grupy szkoleniowej:

30 osób – wersja zdalna w czasie rzeczywistym lub

30 osób – forma stacjonarna

Minimalny czas trwania usługi:

18 h

Minimalne wymagania w zakresie zasobów:

- a) sala szkoleniowa spełniająca standardy jakości prowadzenia zajęć dydaktycznych, wyposażona w rzutnik multimedialny lub ekran do prezentacji materiałów szkoleniowych (dla usługi realizowanej w formie stacjonarnej lub hybrydowej),
- b) sprzęt komputerowy dla trenera wraz z oprogramowaniem umożliwiającym realizację programu szkolenia oraz prezentację materiałów dydaktycznych (dla usługi realizowanej w formie stacjonarnej lub hybrydowej),
- c) stabilne łącze internetowe umożliwiające prowadzenie zajęć w czasie rzeczywistym oraz przesyłanie materiałów szkoleniowych (dla usługi realizowanej w formie zdalnej lub hybrydowej),
- d) urządzenia umożliwiające komunikację audio-wideo w czasie rzeczywistym, w szczególności kamera oraz mikrofon dla trenera (dla usługi realizowanej w formie zdalnej lub hybrydowej),
- e) oprogramowanie umożliwiające prowadzenie zajęć w trybie zdalnym w czasie rzeczywistym, w szczególności platformę wideokonferencyjną (np. Microsoft Teams lub rozwiązanie równoważne), zapewniającą:
 - transmisję audio i wideo,
 - możliwość prezentacji materiałów szkoleniowych,
 - komunikację z uczestnikami usługi oraz zadawanie pytań w trakcie zajęć,

- f) zasób legalnych wersji dokumentów normalizacyjnych, o których mowa w art. 2 pkt 3 ustawy z dnia 12 września 2002 r. o normalizacji (Dz.U. 2015 poz. 1483), w zakresie odpowiadającym efektom uczenia się realizowanym w ramach usługi,
- g) materiały szkoleniowe dla uczestników usługi w formie elektronicznej lub papierowej.

Wymagania w zakresie kompetencji trenera:

Kompetencje określone w §6 Rozporządzenia Kompetencje określone w §6 Rozporządzenia Ministra Funduszy i Polityki Regionalnej z dnia 28 lipca 2023 r. w sprawie rejestru podmiotów świadczących usługi rozwojowe (Dz.U. z 2023 r. poz. 1686) oraz:

- a) min. **12 miesięcy** doświadczenia w zakresie odpowiadającym efektom uczenia się i kryteriom weryfikacji,
- b) doświadczenie w prowadzeniu szkoleń lub doradztwa w temacie usługi - **min. 100** godzin.

Sposób oraz metody realizacji usługi:

Szkolenie może być realizowane w formie stacjonarnej, zdalnej lub hybrydowej.

Usługa szkoleniowa powinna zostać zrealizowana z wykorzystaniem następujących metod: wykłady, prezentacje studiów przypadków (case studies), analiza rzeczywistych przypadków z branży zabezpieczeń technicznych, analiza procedur.

Usługa musi zostać zakończona weryfikacją efektów uczenia się, zgodnie ze standardami określonymi w Rozporządzeniu Ministra Funduszy i Polityki Regionalnej z dnia 28 lipca 2023 r. w sprawie rejestru podmiotów świadczących usługi rozwojowe (Dz.U. z 2023 r. poz. 1686), przeprowadzoną metodami: test teoretyczny (pisemny).

Potencjalni uczestnicy usług rozwojowych

Szkolenie jest skierowane do osób odpowiedzialnych za organizację, nadzór i koordynację prac instalacyjnych, konserwacyjnych i serwisowych systemów zabezpieczeń technicznych, w szczególności do:

- a) osób pełniących funkcję koordynatora prac instalacyjnych lub serwisowych systemów zabezpieczeń technicznych,

- b) kierowników zespołów instalacyjnych i serwisowych w firmach realizujących usługi w zakresie SSWiN, SKD, VSS/CCTV oraz systemów ochrony perymetrycznej,
- c) pracowników zabezpieczenia technicznego przygotowujących się do objęcia funkcji koordynacyjnych lub nadzorczych,
- d) osób odpowiedzialnych za nadzór nad realizacją prac przez podwykonawców w obszarze systemów zabezpieczeń technicznych,
- e) przedstawicieli inwestorów lub zarządców obiektów nadzorujących realizację prac instalacyjnych i serwisowych systemów zabezpieczeń technicznych,
- f) osób odpowiedzialnych za utrzymanie techniczne systemów zabezpieczeń technicznych w obiektach o podwyższonych wymaganiach bezpieczeństwa.

Dodatkowe uwagi

Brak

Nazwa kompetencji nr 3: Projektowanie, instalowanie i konserwacja systemów sygnalizacji pożarowej

Czy kompetencja/kwalifikacja jest włączona do Zintegrowanego Systemu Kwalifikacji?

NIE

Krótką charakterystyka kompetencji

Projektowanie, instalowanie i konserwacja systemów sygnalizacji pożarowej.

Efekt uczenia się 1: Identyfikuje wymagania prawne, normatywne oraz branżowe dotyczące projektowania, instalowania i konserwacji systemów sygnalizacji pożarowej (SSP) oraz sposoby potwierdzania kwalifikacji w tym zakresie

Kryteria weryfikacji:

- A. identyfikuje akty prawne regulujące stosowanie systemów sygnalizacji pożarowej,
- B. rozróżnia wymagania wynikające z PKN-CEN/TS 54-14:2006, PKN-CEN/TS 54-14:2020-09 oraz wytycznych SITP WP-02:2021,
- C. identyfikuje zasady dopuszczania urządzeń do stosowania w ochronie przeciwpożarowej,
- D. rozróżnia projekt budowlany od projektu wykonawczego systemu SSP oraz identyfikuje zakres czynności projektowych niewymagających uprawnień budowlanych,
- E. identyfikuje rolę projektanta SSP w procesie budowlanym, w tym w zakresie współpracy z rzeczoznawcą do spraw zabezpieczeń przeciwpożarowych,
- F. rozróżnia wymagania wynikające z PKN-CEN/TS 54-14:2020-09 oraz normy PN-EN 16763:2017-04 w zakresie kompetencji i jakości świadczenia usług,
- G. identyfikuje sposoby potwierdzania kwalifikacji w obszarze SSP, w tym szkolenia specjalistyczne, certyfikację usług na zgodność z PN-EN 16763 oraz kwalifikacje włączone do Zintegrowanego Systemu Kwalifikacji.

Metody walidacji:

- Ad.A. test teoretyczny
- Ad.B. test teoretyczny
- Ad.C. test teoretyczny
- Ad.D. test teoretyczny

Ad.E. test teoretyczny

Ad.F. test teoretyczny

Ad.G. test teoretyczny

Efekt uczenia się 2: Analizuje zagrożenie pożarowe obiektu w kontekście projektowania systemu SSP

Kryteria weryfikacji:

- A. rozróżnia klasyfikację obiektów budowlanych pod względem budowlanym i pożarowym w zakresie mającym wpływ na projektowanie SSP,
- B. identyfikuje parametry obiektu wpływające na podział na strefy pożarowe, strefy dozorowe i strefy alarmowe oraz na dobór wariantu alarmowania,
- C. identyfikuje typowe zagrożenia pożarowe i warunki środowiskowe istotne dla doboru rozwiązań SSP,
- D. rozróżnia elementy scenariusza pożarowego mające wpływ na algorytmy działania SSP oraz matrycę sterowań urządzeniami przeciwpożarowymi,
- E. określa zależności pomiędzy wymaganiami ewakuacyjnymi, warunkami użytkowania obiektu i przyjętym wariantem działania SSP.

Metody walidacji:

Ad.A. test teoretyczny

Ad.B. test teoretyczny

Ad.C. test teoretyczny

Ad.D. test teoretyczny

Ad.E. test teoretyczny

Efekt uczenia się 3: Dobiera elementy systemu sygnalizacji pożarowej (SSP) do warunków technicznych i funkcjonalnych obiektu zgodnie z wybranymi wytycznymi projektowymi

Kryteria weryfikacji:

- A. rozróżnia rodzaje czujek pożarowych (dymu, temperatury, płomienia, wielosensorowe, specjalne) oraz określa zasady ich doboru w zależności od charakterystyki obiektu,

- B. identyfikuje zasady rozmieszczania czujek, ręcznych ostrzegaczy pożarowych oraz modułów sterujących i monitorujących zgodnie z wybranymi wytycznymi projektowymi,
- C. rozróżnia warianty alarmowania oraz podstawowe algorytmy działania systemu SSP w zależności od przyjętego scenariusza pożarowego,
- D. identyfikuje wpływ warunków środowiskowych (np. wentylacja, zapylenie, wysokość pomieszczeń, strefy zagrożenia wybuchem) na dobór i działanie elementów SSP,
- E. rozróżnia dobre i błędne praktyki projektowe w zakresie doboru i rozmieszczenia elementów systemu SSP.

Metody walidacji:

- Ad.A. test teoretyczny
- Ad.B. test teoretyczny
- Ad.C. test teoretyczny
- Ad.D. test teoretyczny
- Ad.E. test teoretyczny

Efekt uczenia się 4: Identyfikuje zasady opracowania dokumentacji projektowej oraz podstawowe wymagania techniczne systemu sygnalizacji pożarowej (SSP)**Kryteria weryfikacji:**

- A. rozróżnia projekt budowlany od projektu wykonawczego systemu SSP oraz identyfikuje zakres dokumentacji projektowej właściwy dla SSP,
- B. identyfikuje elementy projektu wykonawczego SSP, w tym część opisową, rysunkową oraz schematy funkcjonalne,
- C. rozróżnia wymagania dotyczące zasilania podstawowego i rezerwowego systemu SSP,
- D. identyfikuje zasady doboru okablowania oraz projektowania tras kablowych zgodnie z wymaganiami ochrony przeciwpożarowej,
- E. rozróżnia wymagania dotyczące dokumentacji powykonawczej oraz odbioru systemu SSP.

Metody walidacji:

- Ad.A. test teoretyczny

- Ad.B. test teoretyczny
- Ad.C. test teoretyczny
- Ad.D. test teoretyczny
- Ad.E. test teoretyczny

Efekt uczenia się 5: Identyfikuje zasady instalowania, uruchamiania i odbioru systemów sygnalizacji pożarowej (SSP)

Kryteria weryfikacji:

- A. rozróżnia wymagania montażowe dotyczące elementów systemu SSP, w tym okablowania, zamocowań i lokalizacji urządzeń,
- B. identyfikuje zasady koordynacji prac instalacyjnych SSP z innymi branżami budowlanymi i instalacyjnymi,
- C. rozróżnia zakres czynności uruchomieniowych oraz testów funkcjonalnych systemu SSP,
- D. identyfikuje zasady odbioru systemu SSP, w tym rolę PSP oraz wymagania dokumentacyjne,
- E. rozróżnia zakres odpowiedzialności projektanta, instalatora, kierownika robót oraz inwestora w procesie realizacji SSP.

Metody walidacji:

- Ad.A. test teoretyczny
- Ad.B. test teoretyczny
- Ad.C. test teoretyczny
- Ad.D. test teoretyczny
- Ad.E. test teoretyczny

Efekt uczenia się 6: Identyfikuje zasady eksploatacji, konserwacji oraz utrzymania sprawności systemów sygnalizacji pożarowej (SSP)

Kryteria weryfikacji:

- A. rozróżnia wymagania dotyczące przeglądów technicznych i konserwacji systemów SSP wynikające z przepisów, norm, specyfikacji technicznych oraz wytycznych branżowych,
- B. identyfikuje zakres czynności konserwacyjnych dla elementów systemu SSP, w tym central, czujek, urządzeń liniowych i zasilania,

- C. rozróżnia dokumentację eksploatacyjną systemu SSP, w tym książkę eksploatacji oraz protokoły przeglądów,
- D. identyfikuje przyczyny powstawania fałszywych alarmów oraz sposoby ich ograniczania,
- E. rozróżnia obowiązki właściciela lub zarządcy obiektu w zakresie utrzymania sprawności systemu SSP.

Metody walidacji:

- Ad.A. test teoretyczny
- Ad.B. test teoretyczny
- Ad.C. test teoretyczny
- Ad.D. test teoretyczny
- Ad.E. test teoretyczny

Efekt uczenia się 7: Identyfikuje zasady konfiguracji i przygotowania systemu sygnalizacji pożarowej (SSP) do pracy w obiekcie**Kryteria weryfikacji:**

- A. rozróżnia podstawowe funkcje centrali sygnalizacji pożarowej oraz elementów liniowych systemu SSP,
- B. identyfikuje zasady konfiguracji funkcji sterujących i monitorujących w odniesieniu do scenariusza pożarowego,
- C. rozróżnia narzędzia wspomagające konfigurację systemu SSP, w tym konfigurator i oprogramowanie producenta,
- D. identyfikuje zależności pomiędzy parametrami systemu, konfiguracją logiczną oraz wymaganiami funkcjonalnymi obiektu,
- E. rozróżnia błędy konfiguracyjne mogące wpływać na nieprawidłowe działanie systemu SSP.

Metody walidacji:

- Ad.A. test teoretyczny
- Ad.B. test teoretyczny
- Ad.C. test teoretyczny
- Ad.D. test teoretyczny
- Ad.E. test teoretyczny

Szacowana skala niedoboru kompetencji/kwalifikacji

270

Usługa rozwojowa wspierająca zdobycie kompetencji/kwalifikacji**Standard usługi:**

Usługa realizowana przez podmiot wpisany do Bazy Usług Rozwojowych, spełniający wymagania określone w Rozporządzeniu Ministra Funduszy i Polityki Regionalnej z dnia 28 lipca 2023 r. w sprawie rejestru podmiotów świadczących usługi rozwojowe (Dz.U. z 2023 r. poz. 1686), zgodnie z zasadami określonymi w Regulaminie Bazy Usług Rozwojowych oraz w niniejszej rekomendacji.

Podmiot realizujący usługę powinien być jednocześnie wpisany do Rejestru Szkół i Placówek Oświatowych jako placówka kształcenia ustawicznego, zgodnie z ustawą z dnia 14 grudnia 2016 r. – Prawo oświatowe (Dz.U. z późn. zm.), w szczególności art. 2 pkt 4 oraz art. 168.

Ponadto podmiot realizujący usługę powinien posiadać doświadczenie w prowadzeniu szkoleń lub działalności eksperckiej w obszarze systemów ochrony przeciwpożarowej oraz prowadzić działalność szkoleniową w sposób zapewniający niezależność merytoryczną od producentów i dostawców konkretnych rozwiązań technicznych. Zgodnie z dobrymi praktykami wskazanymi w załączniku nr 1 do Narodowego Programu Ochrony Infrastruktury Krytycznej 2023 „Standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej – dobre praktyki i rekomendacje”, szkolenia w zakresie projektowania, instalowania, konserwacji i eksploatacji systemów ochrony przeciwpożarowej powinny być prowadzone przez uznane na rynku, niezależne instytucje szkoleniowe.

Warunki w zakresie kompetencji osób przystępujących do usługi:

- a) Posiada wykształcenie co najmniej zawodowe lub średnie.

Maksymalna liczebność grupy szkoleniowej:

30 osób – wersja zdalna w czasie rzeczywistym lub

30 osób – forma stacjonarna

Minimalny czas trwania usługi:

32 h zegarowe

Minimalne wymagania w zakresie zasobów:

- a) sala szkoleniowa spełniająca standardy jakości prowadzenia zajęć dydaktycznych, wyposażona w rzutnik multimedialny lub ekran do prezentacji materiałów szkoleniowych (dla usługi realizowanej w formie stacjonarnej lub hybrydowej),
- b) sprzęt komputerowy dla trenera wraz z oprogramowaniem umożliwiającym realizację programu szkolenia oraz prezentację materiałów dydaktycznych (dla usługi realizowanej w formie stacjonarnej lub hybrydowej),
- c) stabilne łącze internetowe umożliwiające prowadzenie zajęć w czasie rzeczywistym oraz przesyłanie materiałów szkoleniowych (dla usługi realizowanej w formie zdalnej lub hybrydowej),
- d) urządzenia umożliwiające komunikację audio-wideo w czasie rzeczywistym, w szczególności kamera oraz mikrofon dla trenera (dla usługi realizowanej w formie zdalnej lub hybrydowej),
- e) oprogramowanie umożliwiające prowadzenie zajęć w trybie zdalnym w czasie rzeczywistym, w szczególności platformę wideokonferencyjną (np. Microsoft Teams lub rozwiązanie równoważne), zapewniającą:
 - transmisję audio i wideo,
 - możliwość prezentacji materiałów szkoleniowych,
 - komunikację z uczestnikami usługi oraz zadawanie pytań w trakcie zajęć,
- f) zasób legalnych wersji dokumentów normalizacyjnych, o których mowa w art. 2 pkt 3 ustawy z dnia 12 września 2002 r. o normalizacji (Dz.U. 2015 poz. 1483), w zakresie odpowiadającym efektom uczenia się realizowanym w ramach usługi,
- g) materiały szkoleniowe dla uczestników usługi w formie elektronicznej lub papierowej.

Wymagania w zakresie kompetencji trenera:

Kompetencje określone w §6 Rozporządzenia Ministra Funduszy i Polityki Regionalnej z dnia 28 lipca 2023 r. w sprawie rejestru podmiotów świadczących usługi rozwojowe (Dz.U. z 2023 r. poz. 1686) oraz:

- a) **minimum 12 miesięcy** doświadczenia w zakresie odpowiadającym efektom uczenia się i kryteriom weryfikacji,
- b) doświadczenie w prowadzeniu szkoleń lub doradztwa w temacie usługi - **minimum 100 godzin**.

Sposób oraz metody realizacji usługi:

Szkolenie może być realizowane w formie stacjonarnej, zdalnej lub hybrydowej.

Usługa szkoleniowa powinna zostać zrealizowana z wykorzystaniem następujących metod: wykłady, prezentacje studiów przypadków (case studies), prezentacja rzeczywistych projektów z branży systemów ochrony przeciwpożarowej, demonstracje możliwości sprzętu i systemów, prezentacja możliwości wykorzystania oprogramowania do konfiguracji central SSP (np. Aplikacja POLON Studio).

Usługa musi zostać zakończona weryfikacją efektów uczenia się, zgodnie ze standardami określonymi w Rozporządzeniu Ministra Funduszy i Polityki Regionalnej z dnia 28 lipca 2023 r. w sprawie rejestru podmiotów świadczących usługi rozwojowe (Dz.U. z 2023 r. poz. 1686) oraz Rozporządzeniu Ministra Edukacji i Nauki z dnia 6 października 2023 r. w sprawie kształcenia ustawicznego w formach pozaszkolnych (Dz.U. 2023 poz. 2175), przeprowadzoną metodami: test teoretyczny (pisemny).

Potencjalni uczestnicy usług rozwojowych

Osoby odpowiedzialne lub osoby, którym przedsiębiorca zamierza powierzyć odpowiedzialność za:

- a) projektowanie systemów sygnalizacji pożarowej i sterowania urządzeniami przeciwpożarowymi,
- b) kierowanie zespołami projektowymi instalacji SSP i sterowania urządzeniami przeciwpożarowymi,
- c) nadzór nad montażem instalacji SSP i sterowania urządzeniami przeciwpożarowymi,

- d) kierowanie zespołami montażu instalacji SSP i sterowania urządzeniami przeciwpożarowymi,
- e) kierowanie zespołami serwisującymi instalacje SSP i sterowania urządzeniami przeciwpożarowymi,
- f) eksploatację, administrowanie lub nadzór nad systemami sygnalizacji pożarowej,
- g) prowadzenie inwestycji w systemy sygnalizacji pożarowej.

Dodatkowe uwagi

Brak

Nazwa kompetencji nr 4: Zarządzanie cyberbezpieczeństwem w systemach zabezpieczeń technicznych

Czy kompetencja/kwalifikacja jest włączona do Zintegrowanego Systemu Kwalifikacji?

NIE

Krótką charakterystyką kompetencji

Zarządzanie cyberbezpieczeństwem w systemach zabezpieczeń technicznych.

Efekt uczenia się 1: Charakteryzuje podstawowe pojęcia z zakresu cyberbezpieczeństwa systemów zabezpieczeń technicznych

Kryteria weryfikacji:

- A. rozróżnia pojęcia: cyberbezpieczeństwo, bezpieczeństwo informacji, bezpieczeństwo sieciowe, ochrona danych osobowych,
- B. identyfikuje definicje pojęć: zagrożenie, podatność, ryzyko, incydent bezpieczeństwa,
- C. wskazuje różnice pomiędzy klasycznym podejściem do cyberbezpieczeństwa (IT/korporacyjnym) a cyberbezpieczeństwem systemów zabezpieczeń technicznych,
- D. przyporządkowuje przykłady zagrożeń do obszarów: poufność, integralność, dostępność (model CIA),
- E. klasyfikuje warstwy cyberbezpieczeństwa w systemach zabezpieczeń technicznych (warstwa fizyczna, sieciowa, aplikacyjna, danych).

Metody walidacji:

- Ad.A. test teoretyczny
- Ad.B. test teoretyczny
- Ad.C. test teoretyczny
- Ad.D. test teoretyczny
- Ad.E. test teoretyczny

Efekt uczenia się 2: Identyfikuje podstawowe wymagania systemu zarządzania bezpieczeństwem informacji zgodnie z normą ISO/IEC 27001 w kontekście systemów zabezpieczeń technicznych

Kryteria weryfikacji:

- A. identyfikuje główne elementy systemu zarządzania bezpieczeństwem informacji zgodnie ze strukturą normy ISO/IEC 27001,
- B. rozróżnia wymagania dotyczące polityki bezpieczeństwa informacji, analizy ryzyka oraz postępowania z ryzykiem w SZBI,
- C. wskazuje rolę polityki bezpieczeństwa informacji oraz procedur operacyjnych w systemach zabezpieczeń technicznych.

Metody walidacji:

- Ad.A. test teoretyczny
- Ad.B. test teoretyczny
- Ad.C. test teoretyczny

Efekt uczenia się 3: Identyfikuje podstawowe wymagania prawne w zakresie cyberbezpieczeństwa

Kryteria weryfikacji:

- A. wymienia kluczowe akty prawne regulujące cyberbezpieczeństwo w Polsce i Unii Europejskiej,
- B. identyfikuje wymogi dotyczące zgłaszania incydentów cyberbezpieczeństwa do właściwych organów,
- C. identyfikuje wymogi RODO w kontekście systemów zabezpieczeń technicznych przetwarzających dane osobowe,
- D. wskazuje przykładowe normy i standardy dotyczące cyberbezpieczeństwa infrastruktury krytycznej,
- E. wskazuje podstawowe obowiązki prawne administratorów systemów zabezpieczeń technicznych w zakresie Cyberbezpieczeństwa,
- F. wskazuje konsekwencje prawne naruszeń cyberbezpieczeństwa w systemach zabezpieczeń technicznych.

Metody walidacji:

- Ad.A. test teoretyczny
- Ad.B. test teoretyczny
- Ad.C. test teoretyczny
- Ad.D. test teoretyczny
- Ad.E. test teoretyczny
- Ad.F. test teoretyczny

Efekt uczenia się 4: Identyfikuje podstawowe mechanizmy techniczne funkcjonowania systemu cyberbezpieczeństwa w systemach zabezpieczeń technicznych**Kryteria weryfikacji:**

- A. identyfikuje elementy architektury cyberbezpieczeństwa w systemach zabezpieczeń technicznych,
- B. identyfikuje mechanizmy uwierzytelniania i autoryzacji stosowane w systemach zabezpieczeń technicznych,
- C. identyfikuje zasady bezpiecznej konfiguracji urządzeń i systemów zabezpieczeń technicznych,
- D. identyfikuje mechanizmy szyfrowania danych w transmisji i przechowywaniu w systemach zabezpieczeń technicznych,
- E. identyfikuje systemy logowania i monitorowania zdarzeń bezpieczeństwa (np. SIEM),
- F. identyfikuje zasady bezpiecznego zarządzania hasłami i kluczami kryptograficznymi,
- G. identyfikuje mechanizmy wykonywania kopii zapasowych i odtwarzania danych w systemach zabezpieczeń technicznych.

Metody walidacji:

- Ad.A. test teoretyczny
- Ad.B. test teoretyczny
- Ad.C. test teoretyczny
- Ad.D. test teoretyczny
- Ad.E. test teoretyczny
- Ad.F. test teoretyczny
- Ad.G. test teoretyczny

Efekt uczenia się 5: Charakteryzuje rozwiązania bezpieczeństwa sieciowego dla systemów zabezpieczeń technicznych

Kryteria weryfikacji:

- A. rozróżnia architektury bezpieczeństwa sieciowego stosowane w systemach zabezpieczeń technicznych, w tym segmentację sieci i podział na strefy bezpieczeństwa,
- B. identyfikuje funkcje zapór sieciowych (firewall) oraz systemów IDS/IPS w kontekście ochrony systemów zabezpieczeń technicznych,
- C. identyfikuje zastosowanie sieci VPN w zapewnieniu bezpiecznego zdalnego dostępu do systemów zabezpieczeń technicznych,
- D. rozróżnia podstawowe mechanizmy zabezpieczeń sieci bezprzewodowych (Wi-Fi) stosowanych w systemach zabezpieczeń technicznych,
- E. identyfikuje podstawowe mechanizmy ochrony przed atakami typu DDoS oraz innymi zagrożeniami sieciowymi,
- F. wskazuje znaczenie norm i standardów dotyczących bezpieczeństwa sieciowego w systemach zabezpieczeń technicznych (np. IEC 62443).

Metody walidacji:

- Ad.A. test teoretyczny
- Ad.B. test teoretyczny
- Ad.C. test teoretyczny
- Ad.D. test teoretyczny
- Ad.E. test teoretyczny
- Ad.F. test teoretyczny

Efekt uczenia się 6: Ocenia ryzyko cyberbezpieczeństwa w systemach zabezpieczeń technicznych w oparciu o analizę aktywów, zagrożeń i podatności

Kryteria weryfikacji:

- A. identyfikuje aktywa występujące w systemach zabezpieczeń technicznych, w tym aktywa sprzętowe, programowe, informacyjne i osobowe,
- B. rozróżnia znaczenie aktywów z punktu widzenia poufności, integralności i dostępności,

- C. identyfikuje zagrożenia oraz podatności właściwe dla systemów zabezpieczeń technicznych,
- D. rozróżnia etapy procesu zarządzania ryzykiem: identyfikacja, analiza, ocena, postępowanie z ryzykiem,
- E. określa poziom ryzyka w sposób uproszczony, adekwatny do charakteru systemu i skali zagrożenia,
- F. określa priorytet działań zabezpieczających na podstawie poziomu ryzyka.

Metody walidacji:

- Ad.A. test teoretyczny
- Ad.B. test teoretyczny
- Ad.C. test teoretyczny
- Ad.D. test teoretyczny
- Ad.E. test teoretyczny
- Ad.F. test teoretyczny

Efekt uczenia się 7: Analizuje zagrożenia i scenariusze ataków na systemy zabezpieczeń technicznych**Kryteria weryfikacji:**

- A. rozróżnia typy ataków na systemy zabezpieczeń technicznych, w tym fizyczne, sieciowe i aplikacyjne,
- B. identyfikuje wektory ataku charakterystyczne dla systemów sygnalizacji włamania i napadu, systemów telewizji dozorowej i kontroli dostępu,
- C. określa możliwe skutki ataków w odniesieniu do poufności, integralności i dostępności,
- D. klasyfikuje zagrożenia według poziomu ryzyka w odniesieniu do stopnia zabezpieczenia systemu,
- E. wskazuje działania projektowe i eksploatacyjne ograniczające skutki zidentyfikowanych zagrożeń.

Metody walidacji:

- Ad.A. test teoretyczny
- Ad.B. test teoretyczny
- Ad.C. test teoretyczny

Ad.D. test teoretyczny

Ad.E. test teoretyczny

Efekt uczenia się 8: Rozróżnia zdarzenia i incydenty cyberbezpieczeństwa w systemach zabezpieczeń technicznych oraz identyfikuje podstawowe zasady reagowania

Kryteria weryfikacji:

- A. rozróżnia zdarzenie bezpieczeństwa i incydent bezpieczeństwa w systemach zabezpieczeń technicznych,
- B. klasyfikuje incydenty według poziomu istotności i wpływu na działanie systemu,
- C. kategoryzuje incydenty według rodzaju naruszenia: poufność, integralność, dostępność,
- D. identyfikuje podstawowe etapy reagowania na incydenty cyberbezpieczeństwa w systemach zabezpieczeń technicznych,
- E. identyfikuje zasady zgłaszania incydentów,
- F. wskazuje działania minimalizujące skutki incydentu w systemach zabezpieczeń technicznych.

Metody walidacji:

- Ad.A. test teoretyczny
- Ad.B. test teoretyczny
- Ad.C. test teoretyczny
- Ad.D. test teoretyczny
- Ad.E. test teoretyczny
- Ad.F. test teoretyczny

Efekt uczenia się 9: Identyfikuje podstawowe metody oceny bezpieczeństwa systemów zabezpieczeń technicznych

Kryteria weryfikacji:

- A. rozróżnia rodzaje testów penetracyjnych: black box, white box, grey box,
- B. identyfikuje cel i zakres testów penetracyjnych w systemach zabezpieczeń technicznych,
- C. rozróżnia etapy testów penetracyjnych: rozpoznanie, analiza podatności, eksploatacja podatności, raportowanie,

- D. wskazuje przykładowe metodyki prowadzenia testów penetracyjnych (np. OWASP, PTES),
- E. identyfikuje znaczenie raportu z testów penetracyjnych w procesie doskonalenia bezpieczeństwa systemów zabezpieczeń technicznych,
- F. wskazuje podstawowe działania naprawcze wynikające z raportu z testów penetracyjnych.

Metody walidacji:

- Ad.G. test teoretyczny
- Ad.H. test teoretyczny
- Ad.I. test teoretyczny
- Ad.J. test teoretyczny
- Ad.K. test teoretyczny
- Ad.L. test teoretyczny

Efekt uczenia się 10: Analizuje zagrożenia i incydenty cyberbezpieczeństwa w systemach zabezpieczeń technicznych oraz wykorzystuje dostępne informacje do podejmowania decyzji projektowych i eksploatacyjnych**Kryteria weryfikacji:**

- A. identyfikuje aktualne typy zagrożeń cybernetycznych wpływające na systemy zabezpieczeń technicznych,
- B. rozróżnia wpływ incydentów cyberbezpieczeństwa na funkcjonowanie systemów CCTV, SSWiN i SKD,
- C. identyfikuje informacje z logów, alertów i komunikatów systemowych istotne dla oceny bezpieczeństwa systemu zabezpieczeń technicznych,
- D. wskazuje źródła informacji o podatnościach i zagrożeniach (np. komunikaty producentów, raporty branżowe, CERT, ENISA, bazy podatności),
- E. rozróżnia decyzje projektowe i eksploatacyjne ograniczające ryzyko cyberzagrożeń w systemach zabezpieczeń technicznych,
- F. identyfikuje działania zwiększające odporność systemu na zagrożenia zewnętrzne oraz nadużycia wewnętrzne.

Metody walidacji:

- Ad.A. test teoretyczny

- Ad.B. test teoretyczny
- Ad.C. test teoretyczny
- Ad.D. test teoretyczny
- Ad.E. test teoretyczny
- Ad.F. test teoretyczny

Szacowana skala niedoboru kompetencji/kwalifikacji

14 670

Usługa rozwojowa wspierająca zdobycie kompetencji/kwalifikacji**Standard usługi:**

Usługa realizowana przez podmiot wpisany do Bazy Usług Rozwojowych, spełniający wymagania określone w Rozporządzeniu Ministra Funduszy i Polityki Regionalnej z dnia 28 lipca 2023 r. w sprawie rejestru podmiotów świadczących usługi rozwojowe (Dz.U. z 2023 r. poz. 1686), zgodnie z zasadami określonymi w Regulaminie Bazy Usług Rozwojowych oraz w niniejszej rekomendacji.

Warunki w zakresie kompetencji osób przystępujących do usługi:

brak

Maksymalna liczebność grupy szkoleniowej:

30 osób – wersja zdalna w czasie rzeczywistym lub

30 osób – forma stacjonarna

Minimalny czas trwania usługi:

19 h zegarowych

Minimalne wymagania w zakresie zasobów:

- a) sala szkoleniowa spełniająca standardy jakości prowadzenia zajęć dydaktycznych, wyposażona w rzutnik multimedialny lub ekran do prezentacji materiałów szkoleniowych (dla usługi realizowanej w formie stacjonarnej lub hybrydowej),

- b) sprzęt komputerowy dla trenera wraz z oprogramowaniem umożliwiającym realizację programu szkolenia oraz prezentację materiałów dydaktycznych (dla usługi realizowanej w formie stacjonarnej lub hybrydowej),
- c) stabilne łącze internetowe umożliwiające prowadzenie zajęć w czasie rzeczywistym oraz przysyłanie materiałów szkoleniowych (dla usługi realizowanej w formie zdalnej lub hybrydowej),
- d) urządzenia umożliwiające komunikację audio-wideo w czasie rzeczywistym, w szczególności kamera oraz mikrofon dla trenera (dla usługi realizowanej w formie zdalnej lub hybrydowej),
- e) oprogramowanie umożliwiające prowadzenie zajęć w trybie zdalnym w czasie rzeczywistym, w szczególności platformę wideokonferencyjną (np. Microsoft Teams lub rozwiązanie równoważne), zapewniającą:
 - transmisję audio i wideo,
 - możliwość prezentacji materiałów szkoleniowych,
 - komunikację z uczestnikami usługi oraz zadawanie pytań w trakcie zajęć,
- f) zasób legalnych wersji dokumentów normalizacyjnych, o których mowa w art. 2 pkt 3 ustawy z dnia 12 września 2002 r. o normalizacji (Dz.U. 2015 poz. 1483), w zakresie odpowiadającym efektom uczenia się realizowanym w ramach usługi,
- g) materiały szkoleniowe dla uczestników usługi w formie elektronicznej lub papierowej.

Wymagania w zakresie kompetencji trenera:

Kompetencje określone w §6 Rozporządzenia Ministra Funduszy i Polityki Regionalnej z dnia 28 lipca 2023 r. w sprawie rejestru podmiotów świadczących usługi rozwojowe (Dz.U. z 2023 r. poz. 1686) oraz:

- a) **min. 12 miesięcy** doświadczenia w zakresie odpowiadającym efektom uczenia się i kryteriom weryfikacji,
- b) doświadczenie w prowadzeniu szkoleń lub doradztwa w temacie usługi - min. **100** godzin.

Sposób oraz metody realizacji usługi:

Szkolenie może być realizowane w formie stacjonarnej, zdalnej lub hybrydowej.

Usługa szkoleniowa powinna zostać zrealizowana z wykorzystaniem następujących metod: wykłady, prezentacje studiów przypadków (case studies), symulacje incydentów, analiza rzeczywistych przypadków z branży zabezpieczeń technicznych.

Usługa musi zostać zakończona weryfikacją efektów uczenia się, zgodnie ze standardami określonymi w Rozporządzeniu Ministra Funduszy i Polityki Regionalnej z dnia 28 lipca 2023 r. w sprawie rejestru podmiotów świadczących usługi rozwojowe (Dz.U. z 2023 r. poz. 1686), przeprowadzoną metodami: test teoretyczny (pisemny).

Potencjalni uczestnicy usług rozwojowych

- a) Projektanci, instalatorzy, administratorzy oraz integratorzy systemów zabezpieczeń technicznych, w szczególności systemów CCTV/VSS, SSWiN, SKD oraz innych systemów ochrony technicznej,
- b) Specjaliści odpowiedzialni za nadzór nad bezpieczeństwem i odpornością systemów zabezpieczeń technicznych,
- c) Osoby planujące i realizujące inwestycje w systemy zabezpieczeń technicznych po stronie inwestora lub zamawiającego, w tym definiujące wymagania bezpieczeństwa oraz nadzorujące ich wdrożenie,
- d) Specjaliści ds. bezpieczeństwa IT/OT zaangażowani w integrację systemów zabezpieczeń technicznych z infrastrukturą teleinformatyczną oraz w zapewnienie ich bezpiecznej eksploatacji,
- e) Przedstawiciele producentów i dystrybutorów rozwiązań w obszarze systemów zabezpieczeń technicznych odpowiedzialni za rozwój, wdrażanie i wsparcie technologiczne oferowanych systemów,
- f) Osoby odpowiedzialne za zarządzanie bezpieczeństwem obiektów, w tym obiektów o podwyższonych wymaganiach w zakresie ochrony.

Dodatkowe uwagi

Brak

Nazwa kompetencji nr 5: Planowanie i organizacja wykorzystania bezzałogowych statków powietrznych w systemach ochrony obiektów

Czy kompetencja/kwalifikacja jest włączona do Zintegrowanego Systemu Kwalifikacji?

NIE

Krótką charakterystyka kompetencji

Planowanie i organizacja wykorzystania bezzałogowych statków powietrznych w systemach ochrony obiektów.

Efekt uczenia się 1: Charakteryzuje rolę oraz możliwości wykorzystania bezzałogowych statków powietrznych (BSP) w systemach ochrony obiektów

Kryteria weryfikacji:

- A. identyfikuje zagrożenia i scenariusze incydentów, w których wykorzystanie BSP może zwiększyć skuteczność systemu ochrony,
- B. rozróżnia funkcje BSP w strukturze systemu zabezpieczeń technicznych (np. rozpoznanie, weryfikacja alarmu, wsparcie interwencji, monitoring obwodowy),
- C. wskazuje różnice w zastosowaniu BSP w zależności od chronionych obiektów,
- D. identyfikuje ograniczenia operacyjne i techniczne wykorzystania BSP w ochronie obiektów,
- E. wskazuje systemy zabezpieczeń technicznych, z którymi BSP mogą być integrowane (np. CCTV/VSS, SSWiN, SKD, PSIM).

Metody walidacji:

- Ad.A. test teoretyczny
- Ad.B. test teoretyczny
- Ad.C. test teoretyczny
- Ad.D. test teoretyczny
- Ad.E. test teoretyczny

Efekt uczenia się 2: Charakteryzuje przepisy prawne oraz wymagania w zakresie ochrony danych osobowych związane z wykorzystaniem bezzałogowych statków powietrznych (BSP) w systemach ochrony obiektów

Kryteria weryfikacji:

- A. identyfikuje podstawowe regulacje krajowe i unijne dotyczące wykonywania operacji BSP w działalności gospodarczej,
- B. rozróżnia kategorie operacji dronowych w kontekście zastosowań ochronnych,
- C. wskazuje wymagania dotyczące pilotów oraz obowiązki podmiotu wykorzystującego BSP,
- D. identyfikuje ograniczenia wykonywania operacji BSP w strefach o ograniczonym dostępie oraz obowiązki związane z uzyskiwaniem zezwoleń,
- E. identyfikuje podstawowe wymagania wynikające z przepisów o ochronie danych osobowych (RODO) w kontekście monitoringu realizowanego z wykorzystaniem BSP,
- F. identyfikuje ryzyka naruszenia prywatności oraz obowiązki informacyjne związane z wykorzystaniem BSP w ochronie obiektów.

Metody walidacji:

- Ad.A. test teoretyczny
- Ad.B. test teoretyczny
- Ad.C. test teoretyczny
- Ad.D. test teoretyczny
- Ad.E. test teoretyczny
- Ad.F. test teoretyczny

Efekt uczenia się 3: Charakteryzuje zasady analizy ryzyka i podatności obiektu w kontekście wykorzystania BSP jako elementu systemu ochrony

Kryteria weryfikacji:

- A. identyfikuje zagrożenia i podatności obiektu, które mogą uzasadniać zastosowanie BSP,
- B. rozróżnia sytuacje, w których BSP stanowią wsparcie systemu ochrony, od sytuacji, w których nie są rozwiązaniem optymalnym,

- C. określa czynniki wpływające na zasadność wykorzystania BSP (charakterystyka terenu, rozległość obiektu, czas reakcji, dostępność patroli naziemnych),
- D. identyfikuje ograniczenia wynikające z lokalizacji obiektu,
- E. wskazuje znaczenie analizy ryzyka w procesie włączania BSP do planu ochrony obiektu.

Metody walidacji:

- Ad.A. test teoretyczny
- Ad.B. test teoretyczny
- Ad.C. test teoretyczny
- Ad.D. test teoretyczny
- Ad.E. test teoretyczny

Efekt uczenia się 4: Charakteryzuje zasady planowania operacyjnego wykorzystania bezałogowych statków powietrznych (BSP) w systemach ochrony obiektów**Kryteria weryfikacji:**

- A. określa cele wykorzystania BSP w zależności od rodzaju zagrożenia i potrzeb ochronnych,
- B. identyfikuje czynniki wpływające na planowanie operacji BSP (np. zasięg, czas lotu, warunki atmosferyczne, ograniczenia przestrzeni powietrznej),
- C. rozróżnia planowanie operacji rutynowych (patrolowych) od operacji interwencyjnych,
- D. wskazuje znaczenie procedur awaryjnych i alternatywnych scenariuszy działania w przypadku utraty łączności lub awarii BSP,
- E. identyfikuje wymagania w zakresie dokumentowania operacji BSP zgodnie z wymogami operacyjnymi i prawnymi.

Metody walidacji:

- Ad.A. test teoretyczny
- Ad.B. test teoretyczny
- Ad.C. test teoretyczny
- Ad.D. test teoretyczny
- Ad.E. test teoretyczny

Efekt uczenia się 5: Charakteryzuje zasady doboru bezzałogowych statków powietrznych (BSP) oraz systemów obserwacyjnych do zadań ochronnych

Kryteria weryfikacji:

- A. rozróżnia rodzaje i typy BSP pod kątem zastosowań ochronnych,
- B. wskazuje parametry techniczne BSP istotne dla realizacji zadań ochronnych (np. czas lotu, zasięg operacyjny, odporność na warunki atmosferyczne, system łączności),
- C. identyfikuje rodzaje sensorów i kamer stosowanych w ochronie obiektów,
- D. określa zależność między charakterystyką obiektu a doбором platformy BSP i wyposażenia obserwacyjnego,
- E. wskazuje kryteria oceny rozwiązań BSP w kontekście bezpieczeństwa, niezawodności i integracji z systemem ochrony.

Metody walidacji:

- Ad.A. test teoretyczny
- Ad.B. test teoretyczny
- Ad.C. test teoretyczny
- Ad.D. test teoretyczny
- Ad.E. test teoretyczny

Efekt uczenia się 6: Charakteryzuje zasady integracji bezzałogowych statków powietrznych (BSP) z systemami zabezpieczeń technicznych oraz organizacją ochrony obiektu

Kryteria weryfikacji:

- A. wskazuje możliwości integracji BSP z systemami zabezpieczeń technicznych (np. CCTV/VSS, SSWiN, SKD, PSIM),
- B. rozróżnia poziomy integracji BSP: techniczny (transmisja danych, wizualizacja), operacyjny (scenariusze reakcji), organizacyjny (procedury i odpowiedzialności),
- C. identyfikuje zasady współdziałania BSP z patrolami naziemnymi (np. weryfikacja alarmu, naprowadzanie patrolu, wsparcie interwencji),
- D. wskazuje zasady przekazywania obrazu i sygnałów alarmowych z BSP do Alarmowego Centrum Odbiorczego,

- E. identyfikuje wymagania w zakresie dokumentowania zdarzeń z wykorzystaniem BSP w systemie ochrony obiektu.

Metody walidacji:

- Ad.A. test teoretyczny
- Ad.B. test teoretyczny
- Ad.C. test teoretyczny
- Ad.D. test teoretyczny
- Ad.E. test teoretyczny

Szacowana skala niedoboru kompetencji/kwalifikacji

7 491

Usługa rozwojowa wspierająca zdobycie kompetencji/kwalifikacji

Standard usługi:

Usługa realizowana przez podmiot wpisany do Bazy Usług Rozwojowych, spełniający wymagania określone w Rozporządzeniu Ministra Funduszy i Polityki Regionalnej z dnia 28 lipca 2023 r. w sprawie rejestru podmiotów świadczących usługi rozwojowe (Dz.U. z 2023 r. poz. 1686), zgodnie z zasadami określonymi w Regulaminie Bazy Usług Rozwojowych oraz w niniejszej rekomendacji.

Warunki w zakresie kompetencji osób przystępujących do usługi:

brak

Maksymalna liczebność grupy szkoleniowej:

- 30 osób – wersja zdalna w czasie rzeczywistym lub
- 30 osób – forma stacjonarna

Minimalny czas trwania usługi:

18 h zegarowe

Minimalne wymagania w zakresie zasobów:

- a) sala szkoleniowa spełniająca standardy jakości prowadzenia zajęć dydaktycznych, wyposażona w rzutnik multimedialny lub ekran do

- prezentacji materiałów szkoleniowych (dla usługi realizowanej w formie stacjonarnej lub hybrydowej),
- b) sprzęt komputerowy dla trenera wraz z oprogramowaniem umożliwiającym realizację programu szkolenia oraz prezentację materiałów dydaktycznych (dla usługi realizowanej w formie stacjonarnej lub hybrydowej),
 - c) stabilne łącze internetowe umożliwiające prowadzenie zajęć w czasie rzeczywistym oraz przysyłanie materiałów szkoleniowych (dla usługi realizowanej w formie zdalnej lub hybrydowej),
 - d) urządzenia umożliwiające komunikację audio-wideo w czasie rzeczywistym, w szczególności kamera oraz mikrofon dla trenera (dla usługi realizowanej w formie zdalnej lub hybrydowej),
 - e) oprogramowanie umożliwiające prowadzenie zajęć w trybie zdalnym w czasie rzeczywistym, w szczególności platformę wideokonferencyjną (np. Microsoft Teams lub rozwiązanie równoważne), zapewniającą:
 - transmisję audio i wideo,
 - możliwość prezentacji materiałów szkoleniowych,
 - komunikację z uczestnikami usługi oraz zadawanie pytań w trakcie zajęć,
 - f) zasób legalnych wersji dokumentów normalizacyjnych, o których mowa w art. 2 pkt 3 ustawy z dnia 12 września 2002 r. o normalizacji (Dz.U. 2015 poz. 1483), w zakresie odpowiadającym efektom uczenia się realizowanym w ramach usługi,
 - g) materiały szkoleniowe dla uczestników usługi w formie elektronicznej lub papierowej.

Wymagania w zakresie kompetencji trenera:

Kompetencje określone w §6 Rozporządzenia Ministra Funduszy i Polityki Regionalnej z dnia 28 lipca 2023 r. w sprawie rejestru podmiotów świadczących usługi rozwojowe (Dz.U. z 2023 r. poz. 1686) oraz:

- a) min. **12 miesięcy** doświadczenia w zakresie odpowiadającym efektom uczenia się i kryteriom weryfikacji,
- b) doświadczenie w prowadzeniu szkoleń lub doradztwa w temacie usługi - min. **100 godzin**.

Sposób oraz metody realizacji usługi:

Szkolenie może być realizowane w formie stacjonarnej, zdalnej lub hybrydowej.

Usługa szkoleniowa powinna zostać zrealizowana z wykorzystaniem następujących metod: wykłady, prezentacje, studiów przypadków (case studies), prezentacja rzeczywistych projektów wdrożeniowych systemów ochrony opartych na wykorzystaniu dronów.

Usługa musi zostać zakończona weryfikacją efektów uczenia się, zgodnie ze standardami określonymi w Rozporządzeniu Ministra Funduszy i Polityki Regionalnej z dnia 28 lipca 2023 r. w sprawie rejestru podmiotów świadczących usługi rozwojowe (Dz.U. z 2023 r. poz. 1686), przeprowadzoną metodami: test teoretyczny (pisemny).

Osoby odpowiedzialne lub osoby, którym przedsiębiorca zamierza powierzyć odpowiedzialność za:

- a) projektowanie systemów ochrony obiektów z wykorzystaniem bezzałogowych statków powietrznych (BSP),
- b) wdrażanie i integrację systemów BSP z systemami zabezpieczeń technicznych (SSWiN, CCTV/VSS, SKD, PSIM, BMS),
- c) planowanie i organizację operacji dronowych w strukturze systemu ochrony obiektu,
- d) opracowywanie lub aktualizację planów ochrony z uwzględnieniem komponentu BSP,
- e) nadzór nad operacjami BSP realizowanymi w działalności gospodarczej,
- f) zarządzanie bezpieczeństwem obiektów z wykorzystaniem systemów BSP,
- g) koordynację współdziałania BSP z patrolami naziemnymi oraz Alarmowym Centrum Odbiorczym (ACO),
- h) prowadzenie inwestycji i projektów wdrożeniowych w zakresie systemów ochrony opartych na wykorzystaniu BSP.

Dodatkowe uwagi

Brak

Nazwa kompetencji nr 6: Systemy wykrywania i neutralizacji bezzałogowych statków powietrznych, jako narzędzie służące do ochrony obiektów i obszarów

Czy kompetencja/kwalifikacja jest włączona do Zintegrowanego Systemu Kwalifikacji?

NIE

Krótką charakterystyka kompetencji

Systemy wykrywania i neutralizacji bezzałogowych statków powietrznych, jako narzędzie służące do ochrony obiektów i obszarów.

Efekt uczenia się 1: Charakteryzuje zagrożenia związane z wykorzystaniem dronów (bezzałogowych statków powietrznych – BSP) wobec obiektów chronionych oraz cechy tych dronów istotne z punktu widzenia ich wykrywania i przeciwdziałania

Kryteria weryfikacji:

- A. identyfikuje rodzaje zagrożeń dla bezpieczeństwa obiektów stwarzanych przez drony, w tym rozpoznanie, działania kryminalne, działania terrorystyczne, sabotaż, przemyt oraz ataki na infrastrukturę i zasoby chronione,
- B. rozróżnia podstawowe kategorie bezzałogowych statków powietrznych w kontekście ich potencjału zagrożeniowego,
- C. rozróżnia typowe scenariusze wykorzystania dronów wobec obiektu w zależności od celu działania sprawcy oraz charakteru chronionego obiektu,
- D. identyfikuje podatności obiektu na zagrożenia z wykorzystaniem dronów w zależności od typu obiektu, jego lokalizacji oraz uwarunkowań terenowych,
- E. określa potencjalne skutki incydentu z udziałem dronów dla bezpieczeństwa ludzi, mienia, infrastruktury oraz informacji,
- F. identyfikuje cechy konstrukcyjne i operacyjne dronów istotne z punktu widzenia ich wykrywania, w tym sposób sterowania i transmisji danych, profil emisji sygnałów radiowych, sygnaturę akustyczną oraz charakterystykę wizualną.

Metody walidacji:

- Ad.A. test teoretyczny
- Ad.B. test teoretyczny
- Ad.C. test teoretyczny

Ad.D. test teoretyczny

Ad.E. test teoretyczny

Ad.F. test teoretyczny

Efekt uczenia się 2: Charakteryzuje zasady analizy ryzyka i podatności obiektu w kontekście zagrożeń z wykorzystaniem dronów

Kryteria weryfikacji:

- A. identyfikuje źródła ryzyka związane z wykorzystaniem dronów wobec obiektu chronionego, w tym zagrożenia intencjonalne i nieintencjonalne,
- B. rozróżnia elementy analizy ryzyka w odniesieniu do zagrożeń dronowych, w szczególności zagrożenie, podatność, prawdopodobieństwo wystąpienia incydentu oraz potencjalne skutki,
- C. określa czynniki wpływające na poziom ryzyka w zależności od typu obiektu, jego lokalizacji, otoczenia oraz znaczenia chronionych zasobów,
- D. identyfikuje krytyczne obszary i punkty wrażliwe obiektu wymagające uwzględnienia w systemie ochrony przed dronami,
- E. wskazuje podstawowe kierunki działań ograniczających ryzyko zagrożeń związanych z wykorzystaniem dronów na poziomie organizacyjnym i technicznym.

Metody walidacji:

Ad.A. test teoretyczny

Ad.B. test teoretyczny

Ad.C. test teoretyczny

Ad.D. test teoretyczny

Ad.E. test teoretyczny

Efekt uczenia się 3: Charakteryzuje technologie wykrywania i śledzenia dronów oraz ich zastosowanie w ochronie obiektów

Kryteria weryfikacji:

- A. identyfikuje rodzaje fizycznych sygnatów wykorzystywanych w detekcji dronów,
- B. rozróżnia podstawowe metody wykrywania dronów, w tym detekcję poprzez skan częstotliwości, radary, systemy optoelektroniczne, sygnaty akustyczne,

- C. określa ograniczenia poszczególnych technologii detekcji w zależności od warunków środowiskowych i terenowych (np. zabudowa, przeszkody terenowe, zakłócenia, warunki atmosferyczne),
- D. rozróżnia wykrywanie drona od identyfikacji/klasyfikacji obiektu oraz wskazuje znaczenie redukcji fałszywych alarmów w systemach detekcji,
- E. charakteryzuje zasady działania systemów wielosensorowych (multisensorycznych) łączących różne technologie detekcji w kontekście zwiększania skuteczności wykrywania i śledzenia.

Metody walidacji:

- Ad.A. test teoretyczny
- Ad.B. test teoretyczny
- Ad.C. test teoretyczny
- Ad.D. test teoretyczny
- Ad.E. test teoretyczny

Efekt uczenia się 4: Charakteryzuje zasady doboru i integracji systemu detekcji dronów z systemem bezpieczeństwa obiektu**Kryteria weryfikacji:**

- A. określa wymagania funkcjonalne systemu detekcji dronów w zależności od profilu zagrożeń oraz charakterystyki chronionego obiektu,
- B. rozróżnia kryteria doboru technologii detekcji w zależności od ukształtowania terenu, zabudowy, stref ograniczenia lotów oraz znaczenia chronionych zasobów,
- C. identyfikuje możliwości integracji systemu detekcji dronów z istniejącymi systemami zabezpieczeń technicznych (np. CCTV/VSS, SSWiN, SKD, PSIM, Alarmowe Centrum Odbiorcze),
- D. rozróżnia poziomy integracji systemu antydronowego: techniczny (transmisja danych, wizualizacja), operacyjny (scenariusze reakcji) oraz organizacyjny (procedury i odpowiedzialności),
- E. identyfikuje ograniczenia techniczne i organizacyjne związane z wdrażaniem systemów detekcji dronów w strukturze ochrony obiektu.

Metody walidacji:

- Ad.A. test teoretyczny

- Ad.B. test teoretyczny
- Ad.C. test teoretyczny
- Ad.D. test teoretyczny
- Ad.E. test teoretyczny

Efekt uczenia się 5: Charakteryzuje zasady reagowania na incydenty z wykorzystaniem dronów w systemie bezpieczeństwa obiektu z uwzględnieniem ograniczeń prawnych i organizacyjnych

Kryteria weryfikacji:

- A. rozróżnia etapy postępowania w przypadku wykrycia nieautoryzowanego drona nad obiektem (identyfikacja, ocena zagrożenia, uruchomienie procedur, dokumentowanie zdarzenia),
- B. identyfikuje podstawowe działania możliwe do podjęcia przez personel ochrony w ramach obowiązujących przepisów i procedur wewnętrznych,
- C. rozróżnia działania organizacyjne, techniczne oraz działania wymagające zaangażowania właściwych służb publicznych,
- D. identyfikuje ryzyka związane z zastosowaniem środków przeciwdziałania dronom, w tym ryzyko odpowiedzialności prawnej i szkód ubocznych,
- E. określa zasady dokumentowania incydentu dronowego w systemie bezpieczeństwa obiektu.

Metody walidacji:

- Ad.A. test teoretyczny
- Ad.B. test teoretyczny
- Ad.C. test teoretyczny
- Ad.D. test teoretyczny
- Ad.E. test teoretyczny

Efekt uczenia się 6: Charakteryzuje ramy prawne oraz zasady współdziałania z właściwymi organami i służbami w przypadku incydentów z wykorzystaniem dronów, w kontekście ochrony obiektu i bezpieczeństwa przestrzeni powietrznej

Kryteria weryfikacji:

- A. identyfikuje kluczowe obszary regulacyjne mające znaczenie dla ochrony obiektów przed zagrożeniami dronowymi, w tym zasady wykonywania operacji z użyciem

dronów, ograniczenia w przestrzeni powietrznej oraz zasady reagowania na incydenty,

- B. rozróżnia role i odpowiedzialności podmiotu zarządzającego bezpieczeństwem obiektu oraz podmiotów publicznych właściwych w sprawach bezpieczeństwa przestrzeni powietrznej i reagowania na incydenty,
- C. identyfikuje zasady zgłaszania incydentu z wykorzystaniem drona do właściwych organów oraz zakres informacji istotnych w procesie zgłoszenia,
- D. określa zasady zabezpieczania materiału dowodowego i dokumentowania incydentu z wykorzystaniem drona na potrzeby dalszych czynności wyjaśniających prowadzonych przez uprawnione organy,
- E. identyfikuje wymagania dotyczące ochrony danych osobowych i prywatności w kontekście działań obserwacyjnych i detekcyjnych związanych z incydentami dronowymi.

Metody walidacji:

- Ad.A. test teoretyczny
- Ad.B. test teoretyczny
- Ad.C. test teoretyczny
- Ad.D. test teoretyczny
- Ad.E. test teoretyczny

Szacowana skala niedoboru kompetencji/kwalifikacji

6 000

Usługa rozwojowa wspierająca zdobycie kompetencji/kwalifikacji

Standard usługi:

Usługa realizowana przez podmiot wpisany do Bazy Usług Rozwojowych, spełniający wymagania określone w Rozporządzeniu Ministra Funduszy i Polityki Regionalnej z dnia 28 lipca 2023 r. w sprawie rejestru podmiotów świadczących usługi rozwojowe (Dz.U. z 2023 r. poz. 1686), zgodnie z zasadami określonymi w Regulaminie Bazy Usług Rozwojowych oraz w niniejszej rekomendacji.

Warunki w zakresie kompetencji osób przystępujących do usługi:

brak

Maksymalna liczebność grupy szkoleniowej:

30 osób – wersja zdalna w czasie rzeczywistym lub

30 osób – forma stacjonarna

Minimalny czas trwania usługi:

19h zegarowych

Minimalne wymagania w zakresie zasobów:

- a) sala szkoleniowa spełniająca standardy jakości prowadzenia zajęć dydaktycznych, wyposażona w rzutnik multimedialny lub ekran do prezentacji materiałów szkoleniowych (dla usługi realizowanej w formie stacjonarnej lub hybrydowej),
- b) sprzęt komputerowy dla trenera wraz z oprogramowaniem umożliwiającym realizację programu szkolenia oraz prezentację materiałów dydaktycznych (dla usługi realizowanej w formie stacjonarnej lub hybrydowej),
- c) stabilne łącze internetowe umożliwiające prowadzenie zajęć w czasie rzeczywistym oraz przesyłanie materiałów szkoleniowych (dla usługi realizowanej w formie zdalnej lub hybrydowej),
- d) urządzenia umożliwiające komunikację audio-video w czasie rzeczywistym, w szczególności kamera oraz mikrofon dla trenera (dla usługi realizowanej w formie zdalnej lub hybrydowej),
- e) oprogramowanie umożliwiające prowadzenie zajęć w trybie zdalnym w czasie rzeczywistym, w szczególności platformę wideokonferencyjną (np. Microsoft Teams lub rozwiązanie równoważne), zapewniającą:
 - transmisję audio i wideo,
 - możliwość prezentacji materiałów szkoleniowych,
 - komunikację z uczestnikami usługi oraz zadawanie pytań w trakcie zajęć,
- f) zasób legalnych wersji dokumentów normalizacyjnych, o których mowa w art. 2 pkt 3 ustawy z dnia 12 września 2002 r. o normalizacji (Dz.U. 2015 poz. 1483), w zakresie odpowiadającym efektom uczenia się realizowanym w ramach usługi,
- g) materiały szkoleniowe dla uczestników usługi w formie elektronicznej lub papierowej.

Wymagania w zakresie kompetencji trenera:

Kompetencje określone w §6 Rozporządzenia Ministra Funduszy i Polityki Regionalnej z dnia 28 lipca 2023 r. w sprawie rejestru podmiotów świadczących usługi rozwojowe (Dz.U. z 2023 r. poz. 1686) oraz:

- a) min. **12 miesięcy** doświadczenia w zakresie odpowiadającym efektom uczenia się i kryteriom weryfikacji,
- b) doświadczenie w prowadzeniu szkoleń lub doradztwa w temacie usługi - min. **100** godzin.

Sposób oraz metody realizacji usługi:

Szkolenie może być realizowane w formie stacjonarnej, zdalnej lub hybrydowej.

Usługa szkoleniowa powinna zostać zrealizowana z wykorzystaniem następujących metod: wykłady, prezentacje studiów przypadków (case studies), analiza rzeczywistych przypadków z branży bezpieczeństwa.

Usługa musi zostać zakończona weryfikacją efektów uczenia się, zgodnie ze standardami określonymi w Rozporządzeniu Ministra Funduszy i Polityki Regionalnej z dnia 28 lipca 2023 r. w sprawie rejestru podmiotów świadczących usługi rozwojowe (Dz.U. z 2023 r. poz. 1686): test teoretyczny (pisemny).

Potencjalni uczestnicy usług rozwojowych

Osoby odpowiedzialne lub osoby, którym przedsiębiorca zamierza powierzyć odpowiedzialność za:

- a) projektowanie i aktualizację systemów ochrony obiektów z uwzględnieniem zagrożeń dronowych,
- b) planowanie i wdrażanie systemów detekcji dronów oraz ich integrację z systemami zabezpieczeń technicznych (CCTV/VSS, SSWiN, SKD, PSIM, systemy monitoringu),
- c) opracowywanie lub aktualizację planów ochrony obiektów w części dotyczącej zagrożeń z powietrza,
- d) analizę ryzyka i ocenę podatności obiektu w kontekście zagrożeń dronowych,
- e) nadzór nad funkcjonowaniem systemów detekcji dronów oraz ocenę ich skuteczności,

- f) organizację reagowania na incydenty dronowe w strukturze systemu bezpieczeństwa obiektu,
- g) koordynację współdziałania z właściwymi organami i służbami w przypadku incydentów dronowych,
- h) prowadzenie inwestycji i postępowań zakupowych w zakresie systemów detekcji i przeciwdziałania zagrożeniom dronowym.

Dodatkowe uwagi

Brak

Nazwa kompetencji nr 7: Audytowanie systemów zabezpieczeń technicznych w oparciu o wytyczne PN-EN ISO/IEC 27001:2023-08

Czy kompetencja/kwalifikacja jest włączona do Zintegrowanego Systemu Kwalifikacji?

NIE

Krótką charakterystyka kompetencji

Audytowanie systemów zabezpieczeń technicznych w oparciu o wytyczne PN-EN ISO/IEC 27001:2023-08.

Efekt uczenia się 1: Charakteryzuje cele, zakres oraz strukturę systemu zarządzania bezpieczeństwem informacji (SZBI) w kontekście audytu wewnętrznego systemów zabezpieczeń technicznych

Kryteria weryfikacji:

- A. określa zakres systemu zarządzania bezpieczeństwem informacji w odniesieniu do informacji w każdej formie (elektronicznej, papierowej, ustnej),
- B. identyfikuje główne cele wdrożenia SZBI, w tym zapewnienie poufności, integralności i dostępności informacji,
- C. rozróżnia wymagania normy PN-EN ISO/IEC 27001 od wytycznych normy PN-EN ISO/IEC 27002,
- D. określa cel i znaczenie procesu szacowania ryzyka w SZBI, w tym identyfikację zagrożeń, podatności i ryzyka rezydualnego,
- E. identyfikuje związek pomiędzy zarządzaniem incydentami bezpieczeństwa informacji a procesem doskonalenia SZBI,
- F. określa powiązanie wymagań SZBI z obszarem ciągłości działania usług i zabezpieczeń technicznych.

Metody walidacji:

- Ad.A. test teoretyczny
- Ad.B. test teoretyczny
- Ad.C. test teoretyczny
- Ad.D. test teoretyczny
- Ad.E. test teoretyczny
- Ad.F. test teoretyczny

Efekt uczenia się 2: Charakteryzuje zasady prowadzenia audytu wewnętrznego zgodnie z PN-EN ISO 19011:2018-08 w kontekście systemów zabezpieczeń technicznych

Kryteria weryfikacji:

- A. rozróżnia audyt pierwszej, drugiej i trzeciej strony oraz określa rolę audytu wewnętrznego w organizacji,
- B. identyfikuje podstawowe zasady audytowania, w tym bezstronność, obiektywizm, poufność, kompetencję oraz podejście oparte na dowodach,
- C. określa znaczenie listy pytań kontrolnych jako narzędzia wspierającego audyt, stosowanego jako wytyczne, a nie zamknięty katalog pytań,
- D. rozróżnia cel audytu wewnętrznego od działań prowadzonych wyłącznie w celu wykazania zgodności wobec stron zewnętrznych,
- E. identyfikuje kompetencje i cechy osobowe wymagane od audytora wewnętrznego.

Metody walidacji:

- Ad.A. test teoretyczny
- Ad.B. test teoretyczny
- Ad.C. test teoretyczny
- Ad.D. test teoretyczny
- Ad.E. test teoretyczny

Efekt uczenia się 3: Przygotowuje plan audytu wewnętrznego systemów zabezpieczeń technicznych zgodnie z wymaganiami PN-EN ISO 19011:2018-08

Kryteria weryfikacji:

- A. wymienia elementy planu audytu, w tym cel, zakres, kryteria, zespół audytowy oraz harmonogram,
- B. określa znaczenie jednoznacznego ustalenia zakresu i kryteriów audytu przed jego rozpoczęciem,
- C. identyfikuje dokumenty i źródła informacji wykorzystywane przy planowaniu audytu (np. polityka bezpieczeństwa, procedury, Deklaracja Stosowania, wyniki analizy ryzyka, raporty z poprzednich audytów),
- D. rozróżnia program audytów od planu pojedynczego audytu,

- E. identyfikuje czynniki ryzyka i obszary o podwyższonym znaczeniu dla bezpieczeństwa informacji i zabezpieczeń technicznych, które należy uwzględnić przy planowaniu audytu.

Metody walidacji:

- Ad.A. test teoretyczny
- Ad.B. test teoretyczny
- Ad.C. test teoretyczny
- Ad.D. test teoretyczny
- Ad.E. test teoretyczny

Efekt uczenia się 4: Prowadzi ocenę zgodności systemów zabezpieczeń technicznych z wymaganiami normatywnymi oraz wewnętrznymi kryteriami organizacji

Kryteria weryfikacji:

- A. identyfikuje i gromadzi dowody audytowe w oparciu o dokumentację, zapisy systemowe, obserwacje oraz wywiady z personelem,
- B. rozróżnia dowód audytowy od opinii oraz odnosi zebrane dowody do ustalonych kryteriów audytu,
- C. kwalifikuje ustalenia audytowe jako zgodność, niezgodność lub obserwację (potencjał doskonalenia),
- D. formułuje niezgodność w sposób jednoznaczny, wskazując wymaganie, stan faktyczny oraz dowód,
- E. identyfikuje luki w zabezpieczeniach technicznych w odniesieniu do analizy ryzyka oraz wymagań Załącznika A normy PN-EN ISO/IEC 27001,
- F. ocenia znaczenie incydentów bezpieczeństwa informacji oraz zapisów systemowych jako źródeł dowodów audytowych.

Metody walidacji:

- Ad.A. test teoretyczny
- Ad.B. test teoretyczny
- Ad.C. test teoretyczny
- Ad.D. test teoretyczny
- Ad.E. test teoretyczny
- Ad.F. test teoretyczny

Efekt uczenia się 5: Opracowuje raport z audytu systemów zabezpieczeń technicznych zgodnie z wymaganiami PN-EN ISO 19011:2018-08 oraz PN-EN ISO/IEC 27001:2023-08

Kryteria weryfikacji:

- A. określa elementy raportu z audytu, w tym cel, zakres, kryteria audytu, skład zespołu audytowego oraz podsumowanie ustaleń,
- B. formułuje ustalenia audytowe w oparciu o dowody, wskazując odniesienie do konkretnego wymagania normatywnego lub wewnętrznego,
- C. rozróżnia opis faktu od interpretacji oraz unika subiektywnych ocen w treści raportu,
- D. zapisuje niezgodność w sposób jednoznaczny, wskazując wymaganie, stan faktyczny oraz dowód audytowy,
- E. identyfikuje rolę raportu jako podstawy do podjęcia działań korygujących oraz doskonalenia systemu zabezpieczeń technicznych.

Metody walidacji:

- Ad.A. test teoretyczny
- Ad.B. test teoretyczny
- Ad.C. test teoretyczny
- Ad.D. test teoretyczny
- Ad.E. test teoretyczny

Efekt uczenia się 6: Charakteryzuje zasady postępowania z niezgodnościami oraz zasady działań po audytowych w systemach zabezpieczeń technicznych zgodnie z PN-EN ISO/IEC 27001:2023-08 oraz PN-EN ISO 19011:2018-08

Kryteria weryfikacji:

- A. określa wymagane przez PN-EN ISO/IEC 27001 działania w przypadku wystąpienia niezgodności, w tym reakcję na niezgodność, skorygowanie, ocenę potrzeby eliminowania przyczyn, wdrożenie działań, przegląd skuteczności oraz ewentualne zmiany w SZBI,
- B. identyfikuje wymagania dotyczące udokumentowanych informacji jako dowodów: charakteru niezgodności i działań podjętych w następstwie oraz wyników działań korygujących,

- C. określa zasady działań po audytowych zgodnie z PN-EN ISO 19011, w tym monitorowanie statusu działań podejmowanych przez audytowanego oraz weryfikację zakończenia i skuteczności tych działań,
- D. rozróżnia możliwe formy weryfikacji działań po audytowych (np. weryfikacja na miejscu, przegląd dokumentacji, ocena podczas kolejnego audytu) oraz wskazuje ich zastosowanie w praktyce audytu wewnętrznego,
- E. identyfikuje rolę działań po audytowych w procesie ciągłego doskonalenia systemu zabezpieczeń technicznych.

Metody walidacji:

- Ad.A. test teoretyczny
- Ad.B. test teoretyczny
- Ad.C. test teoretyczny
- Ad.D. test teoretyczny
- Ad.E. test teoretyczny

Szacowana skala niedoboru kompetencji/kwalifikacji

21 134

Usługa rozwojowa wspierająca zdobycie kompetencji/kwalifikacji

Standard usługi:

Usługa realizowana przez podmiot wpisany do Bazy Usług Rozwojowych, spełniający wymagania określone w Rozporządzeniu Ministra Funduszy i Polityki Regionalnej z dnia 28 lipca 2023 r. w sprawie rejestru podmiotów świadczących usługi rozwojowe (Dz.U. z 2023 r. poz. 1686), zgodnie z zasadami określonymi w Regulaminie Bazy Usług Rozwojowych oraz w niniejszej rekomendacji.

Warunki w zakresie kompetencji osób przystępujących do usługi:

Zalecane jest uprzednie ukończenie kursu pracownika zabezpieczenia technicznego w zakresie projektowania, instalowania, konserwacji, odbioru i eksploatacji systemów zabezpieczeń technicznych stopni 1-4/wojskowych dokumentów normatywnych.

Maksymalna liczebność grupy szkoleniowej:

- 30 osób – wersja zdalna w czasie rzeczywistym lub
- 30 osób – forma stacjonarna

Minimalny czas trwania usługi:

14 h

Minimalne wymagania w zakresie zasobów:

- a) sala szkoleniowa spełniająca standardy jakości prowadzenia zajęć dydaktycznych, wyposażona w rzutnik multimedialny lub ekran do prezentacji materiałów szkoleniowych (dla usługi realizowanej w formie stacjonarnej lub hybrydowej),
- b) sprzęt komputerowy dla trenera wraz z oprogramowaniem umożliwiającym realizację programu szkolenia oraz prezentację materiałów dydaktycznych (dla usługi realizowanej w formie stacjonarnej lub hybrydowej),
- c) stabilne łącze internetowe umożliwiające prowadzenie zajęć w czasie rzeczywistym oraz przesyłanie materiałów szkoleniowych (dla usługi realizowanej w formie zdalnej lub hybrydowej),
- d) urządzenia umożliwiające komunikację audio-wideo w czasie rzeczywistym, w szczególności kamera oraz mikrofon dla trenera (dla usługi realizowanej w formie zdalnej lub hybrydowej),
- e) oprogramowanie umożliwiające prowadzenie zajęć w trybie zdalnym w czasie rzeczywistym, w szczególności platformę wideokonferencyjną (np. Microsoft Teams lub rozwiązanie równoważne), zapewniającą:
 - transmisję audio i wideo,
 - możliwość prezentacji materiałów szkoleniowych,
 - komunikację z uczestnikami usługi oraz zadawanie pytań w trakcie zajęć,
- f) zasób legalnych wersji dokumentów normalizacyjnych, o których mowa w art. 2 pkt 3 ustawy z dnia 12 września 2002 r. o normalizacji (Dz.U. 2015 poz. 1483), w zakresie odpowiadającym efektom uczenia się realizowanym w ramach usługi,
- g) materiały szkoleniowe dla uczestników usługi w formie elektronicznej lub papierowej.

Wymagania w zakresie kompetencji trenera:

Kompetencje określone w §6 Rozporządzenia Ministra Funduszy i Polityki Regionalnej z dnia 28 lipca 2023 r. w sprawie rejestru podmiotów świadczących usługi rozwojowe (Dz.U. z 2023 r. poz. 1686) oraz:

- a) **min. 24 miesiące** doświadczenia w zakresie audytowania, projektowania, instalacji lub eksploatacji systemów zabezpieczenia technicznego obiektów,
- b) znajomość wymagań normy PN-EN ISO/IEC 27001 oraz norm szczegółowych dotyczących systemów zabezpieczenia technicznego,
- c) doświadczenie w prowadzeniu szkoleń lub doradztwa w temacie usługi - min. **100** godzin.

Sposób oraz metody realizacji usługi:

Szkolenie może być realizowane w formie stacjonarnej, zdalnej lub hybrydowej.

Usługa szkoleniowa powinna zostać zrealizowana z wykorzystaniem następujących metod: wykłady, warsztaty na bazie case studies, analiza rzeczywistych przypadków z branży zabezpieczeń technicznych.

Usługa musi zostać zakończona weryfikacją efektów uczenia się, zgodnie ze standardami określonymi w Rozporządzeniu Ministra Funduszy i Polityki Regionalnej z dnia 28 lipca 2023 r. w sprawie rejestru podmiotów świadczących usługi rozwojowe (Dz.U. z 2023 r. poz. 1686): test teoretyczny.

Potencjalni uczestnicy usług rozwojowych

Osoby odpowiedzialne lub osoby, którym przedsiębiorca zamierza powierzyć odpowiedzialność za:

- a) prowadzenie audytów wewnętrznych systemów zabezpieczeń technicznych w organizacji,
- b) ocenę zgodności systemów zabezpieczeń technicznych z wymaganiami norm PN-EN ISO/IEC 27001 oraz wewnętrznymi regulacjami organizacji,
- c) nadzór nad funkcjonowaniem systemów CCTV/VSS, SSWiN, SKD oraz innych systemów zabezpieczeń technicznych w kontekście wymagań bezpieczeństwa informacji,
- d) monitorowanie skuteczności zabezpieczeń technicznych oraz realizację działań po audytowych i doskonalących,
- e) planowanie i koordynację audytów wewnętrznych w obszarze bezpieczeństwa informacji i zabezpieczeń technicznych,
- f) przygotowanie organizacji do audytów zewnętrznych, w tym audytów certyfikacyjnych.

Dodatkowe uwagi

Brak

Nazwa kompetencji nr 8: Zasady projektowania i eksploatacji systemów VSS/CCTV IP

Czy kompetencja/kwalifikacja jest włączona do Zintegrowanego Systemu Kwalifikacji?

NIE

Krótką charakterystyką kompetencji

Zasady projektowania i eksploatacji systemów VSS/CCTV IP.

Efekt uczenia się 1: Charakteryzuje wymagania normatywne, prawne i branżowe dotyczące projektowania i eksploatacji systemów VSS/CCTV IP

Kryteria weryfikacji:

- A. wskazuje zakres i znaczenie normy PN-EN 62676 w kontekście projektowania systemów VSS/CCTV,
- B. identyfikuje zasady klasyfikacji jakości obrazu oraz podstawowe metody weryfikacji jakości obrazu zgodnie z PN-EN 62676,
- C. rozróżnia cele funkcjonalne dozoru obrazu (detekcja, obserwacja, rozpoznanie, identyfikacja) wykorzystywane do określania wymagań użytkowych systemu,
- D. identyfikuje podstawowe obowiązki wynikające z przepisów o ochronie danych osobowych (RODO) w kontekście systemów telewizji dozorowej,
- E. rozróżnia role i odpowiedzialności uczestników procesu projektowania, instalowania i eksploatacji systemu VSS/CCTV,
- F. identyfikuje wymagania związane z procesem certyfikacji na zgodność z normą PN-EN 16763,
- G. identyfikuje wymagania związane z procesem certyfikacji zainstalowanych systemów na zgodność z PN-EN 62676-1.

Metody walidacji:

- Ad.A. test teoretyczny
- Ad.B. test teoretyczny
- Ad.C. test teoretyczny
- Ad.D. test teoretyczny
- Ad.E. test teoretyczny
- Ad.F. test teoretyczny

Ad.G. test teoretyczny

Efekt uczenia się 2: Charakteryzuje podstawowe zasady obrazowania w systemach VSS/CCTV IP w kontekście doboru kamery i obiektywu

Kryteria weryfikacji:

- A. rozróżnia wpływ ogniskowej obiektywu na kąt/pole widzenia oraz wielkość odwzorowania obserwowanego obiektu w kadrze,
- B. określa wpływ przysłony i czasu migawki na jasność obrazu oraz odwzorowanie obiektów w ruchu,
- C. rozróżnia pojęcia głębi ostrości i ostrości obrazu oraz wskazuje czynniki wpływające na ich uzyskanie w praktyce instalacyjnej,
- D. identyfikuje wpływ warunków oświetleniowych, w tym pracy w trybie dzień/noc oraz z wykorzystaniem podczerwieni (IR), na jakość obrazu i widoczność szczegółów,
- E. wskazuje czynniki doboru punktu kamerowego (kamera + obiektyw) istotne dla wymagań użytkowych, w tym wymagania dla niskiego oświetlenia oraz wysokiego kontrastu.

Metody walidacji:

- Ad.A. test teoretyczny
- Ad.B. test teoretyczny
- Ad.C. test teoretyczny
- Ad.D. test teoretyczny
- Ad.E. test teoretyczny

Efekt uczenia się 3: Charakteryzuje zasady transmisji, kompresji, zapisu, przechowywania i eksportu obrazu w systemach VSS/CCTV IP w kontekście wymagań jakościowych i dowodowych

Kryteria weryfikacji:

- A. rozróżnia wpływ parametrów strumienia wizyjnego (rozdzielczość, liczba klatek na sekundę, bitrate, poziom kompresji) na jakość obrazu w trybie podglądu, zapisu i eksportu,
- B. określa zależność pomiędzy czasem retencji nagrań a wymaganą pojemnością systemu rejestracji,

- C. identyfikuje wymagane elementy zapisu wizyjnego istotne z punktu widzenia wymogów PN-EN 62676-4, w szczególności oznaczenie czasu, daty i identyfikatora kamery,
- D. rozróżnia zasady eksportu materiału wizyjnego zapewniające integralność zapisu oraz możliwość jego odtworzenia przez uprawnione podmioty,
- E. identyfikuje podstawowe mechanizmy zabezpieczenia zapisu i archiwizacji nagrań (kontrola dostępu, kopie zapasowe, redundancja),
- F. określa zależność pomiędzy konfiguracją systemu (parametry zapisu, kompresja, retencja) a przydatnością nagrań jako materiału dowodowego.

Metody walidacji:

- Ad.A. test teoretyczny
- Ad.B. test teoretyczny
- Ad.C. test teoretyczny
- Ad.D. test teoretyczny
- Ad.E. test teoretyczny
- Ad.F. test teoretyczny

Efekt uczenia się 4: Charakteryzuje zastosowanie analityki wizyjnej, w tym rozwiązań opartych na AI, w systemach VSS/CCTV w systemach VSS/CCTV IP oraz jej zależność od jakości obrazu i architektury systemu

Kryteria weryfikacji:

- A. rozróżnia podstawowe funkcje analityki wizyjnej stosowane w systemach VSS/CCTV (np. detekcja zdarzeń, klasyfikacja obiektów, rozpoznawanie tablic rejestracyjnych, zliczanie osób, analiza zachowań),
- B. określa zależność pomiędzy jakością obrazu (rozdzielczość, liczba klatek, kompresja, warunki oświetleniowe) a skutecznością działania analityki wizyjnej,
- C. identyfikuje wpływ lokalizacji przetwarzania analityki (kamera/edge, rejestrator, serwer/VMS) na wydajność i stabilność systemu,
- D. rozróżnia architekturę scentralizowaną i rozproszoną w kontekście realizacji funkcji analitycznych,
- E. identyfikuje ograniczenia techniczne systemu (zasoby obliczeniowe, przepustowość sieci, pojemność zapisu) wpływające na działanie funkcji analitycznych.

Metody walidacji:

- Ad.A. test teoretyczny
- Ad.B. test teoretyczny
- Ad.C. test teoretyczny
- Ad.D. test teoretyczny
- Ad.E. test teoretyczny

Efekt uczenia się 5: Charakteryzuje zasady opracowywania wymagań użytkowych (OR), weryfikacji systemu VSS/CCTV IP przed odbiorem oraz możliwości potwierdzenia jego zgodności poprzez proces oceny i certyfikacji

Kryteria weryfikacji:

- A. identyfikuje podstawowe elementy wymagań użytkowych (OR) dla systemu VSS/CCTV, w tym cel systemu, obszar dozoru, wymagany poziom funkcjonalny oraz wymagania dotyczące zapisu i retencji,
- B. rozróżnia etapy weryfikacji systemu przed odbiorem, w tym testy funkcjonalne, testy jakości obrazu oraz testy integralności zapisu,
- C. określa zależność pomiędzy wymaganiami użytkowymi a zakresem testów akceptacyjnych systemu,
- D. identyfikuje znaczenie dokumentacji powykonawczej oraz zapisów systemowych w procesie odbioru i eksploatacji systemu,
- E. wskazuje rolę użytkownika końcowego oraz instalatora w procesie weryfikacji i odbioru systemu,
- F. identyfikuje zasady potwierdzania zgodności zainstalowanego systemu VSS/CCTV z wymaganiami normatywnymi poprzez proces oceny zgodności dokumentacji wykonawczej (projektu) i certyfikacji systemu VSS/CCTV po zainstalowaniu realizowany przez uprawnioną jednostkę certyfikującą.

Metody walidacji:

- Ad.A. test teoretyczny
- Ad.B. test teoretyczny
- Ad.C. test teoretyczny
- Ad.D. test teoretyczny
- Ad.E. test teoretyczny
- Ad.F. test teoretyczny

Efekt uczenia się 6: Opracowuje wstępne założenia projektowe oraz konfiguruje podstawowe parametry systemu VSS/CCTV IP w środowisku testowym

Kryteria weryfikacji:

- A. określa wymagania funkcjonalne dla systemu VSS/CCTV na podstawie przedstawionych potrzeb użytkownika (obszar dozoru, cel systemu, podstawowe wymagania jakościowe),
- B. dobiera podstawowe elementy systemu (kamera, sposób transmisji, rejestracja, zasilanie) adekwatne do przyjętych założeń projektowych,
- C. konfiguruje parametry sieciowe kamery i rejestratora (adres IP, maska, brama, dostęp użytkowników),
- D. ustawia podstawowe parametry obrazu i strumienia wizyjnego,
- E. weryfikuje poprawność działania systemu po konfiguracji (podgląd, zapis, dostęp użytkownika).

Metody walidacji:

- Ad.A. Zadanie praktyczne realizowane w środowisku testowym systemu VSS/CCTV IP (z możliwością wykorzystania zdalnego dostępu do tego systemu)
- Ad.B. Zadanie praktyczne realizowane w środowisku testowym systemu VSS/CCTV IP (z możliwością wykorzystania zdalnego dostępu do tego systemu)
- Ad.C. Zadanie praktyczne realizowane w środowisku testowym systemu VSS/CCTV IP (z możliwością wykorzystania zdalnego dostępu do tego systemu)
- Ad.D. Zadanie praktyczne realizowane w środowisku testowym systemu VSS/CCTV IP (z możliwością wykorzystania zdalnego dostępu do tego systemu)
- Ad.E. Zadanie praktyczne realizowane w środowisku testowym systemu VSS/CCTV IP (z możliwością wykorzystania zdalnego dostępu do tego systemu)

Szacowana skala niedoboru kompetencji/kwalifikacji

1 410

Usługa rozwojowa wspierająca zdobycie kompetencji/kwalifikacji

Standard usługi:

Usługa realizowana przez podmiot wpisany do Bazy Usług Rozwojowych, spełniający wymagania określone w Rozporządzeniu Ministra Funduszy i Polityki Regionalnej z dnia

28 lipca 2023 r. w sprawie rejestru podmiotów świadczących usługi rozwojowe (Dz.U. z 2023 r. poz. 1686), zgodnie z zasadami określonymi w Regulaminie Bazy Usług Rozwojowych oraz w niniejszej rekomendacji.

Warunki w zakresie kompetencji osób przystępujących do usługi:

brak

Maksymalna liczebność grupy szkoleniowej:

30 osób – wersja zdalna w czasie rzeczywistym lub

30 osób – forma stacjonarna

Minimalny czas trwania usługi:

21 h zegarowych

Minimalne wymagania w zakresie zasobów:

- a) sala szkoleniowa spełniająca standardy jakości prowadzenia zajęć dydaktycznych, wyposażona w rzutnik multimedialny lub ekran do prezentacji materiałów szkoleniowych (dla usługi realizowanej w formie stacjonarnej lub hybrydowej),
- b) sprzęt komputerowy dla trenera wraz z oprogramowaniem umożliwiającym realizację programu szkolenia oraz prezentację materiałów dydaktycznych (dla usługi realizowanej w formie stacjonarnej lub hybrydowej),
- c) stabilne łącze internetowe umożliwiające prowadzenie zajęć w czasie rzeczywistym oraz przysyłanie materiałów szkoleniowych (dla usługi realizowanej w formie zdalnej lub hybrydowej),
- d) urządzenia umożliwiające komunikację audio-wideo w czasie rzeczywistym, w szczególności kamera oraz mikrofon dla trenera (dla usługi realizowanej w formie zdalnej lub hybrydowej),
- e) oprogramowanie umożliwiające prowadzenie zajęć w trybie zdalnym w czasie rzeczywistym, w szczególności platformę wideokonferencyjną (np. Microsoft Teams lub rozwiązanie równoważne), zapewniającą:
 - transmisję audio i wideo,
 - możliwość prezentacji materiałów szkoleniowych,
 - komunikację z uczestnikami usługi oraz zadawanie pytań w trakcie zajęć,

- f) oprogramowanie dla trenera i uczestników umożliwiające konfigurację podstawowych parametrów VSS/CCTV IP,
- g) zasób legalnych wersji dokumentów normalizacyjnych, o których mowa w art. 2 pkt 3 ustawy z dnia 12 września 2002 r. o normalizacji (Dz.U. 2015 poz. 1483), w zakresie odpowiadającym efektom uczenia się realizowanym w ramach usługi,
- h) materiały szkoleniowe dla uczestników usługi w formie elektronicznej lub papierowej.

Wymagania w zakresie kompetencji trenera:

Kompetencje określone w §6 Rozporządzenia Ministra Funduszy i Polityki Regionalnej z dnia 28 lipca 2023 r. w sprawie rejestru podmiotów świadczących usługi rozwojowe (Dz.U. z 2023 r. poz. 1686) oraz:

- a) **min. 12 miesięcy** doświadczenia w zakresie odpowiadającym efektom uczenia się i kryteriom weryfikacji,
- b) doświadczenie w prowadzeniu szkoleń lub doradztwa w temacie usługi - min. **100** godzin.

Sposób oraz metody realizacji usługi:

Szkolenie może być realizowane w formie stacjonarnej, zdalnej lub hybrydowej.

Usługa szkoleniowa powinna zostać zrealizowana z wykorzystaniem następujących metod: wykłady, prezentacja case studies, analiza rzeczywistych przypadków z branży bezpieczeństwa, warsztaty praktyczne z wykorzystaniem systemu VSS/CCTV.

Usługa musi zostać zakończona weryfikacją efektów uczenia się, zgodnie ze standardami określonymi w Rozporządzeniu, przeprowadzoną metodami: test teoretyczny (pisemny), zadanie praktyczne realizowane w środowisku testowym systemu VSS/CCTV IP (z możliwością wykorzystania zdalnego dostępu do tego systemu).

Potencjalni uczestnicy usług rozwojowych

Osoby odpowiedzialne lub osoby, którym przedsiębiorca zamierza powierzyć odpowiedzialność za:

- a) opracowywanie założeń technicznych dla systemów VSS/CCTV IP,

- b) dobór urządzeń oraz parametrów technicznych systemów telewizji dozorowej,
- c) instalowanie, konfigurację i uruchamianie systemów VSS/CCTV IP,
- d) eksploatację, administrację i nadzór nad systemami telewizji dozorowej,
- e) planowanie i realizację inwestycji w systemy VSS/CCTV po stronie inwestora lub zamawiającego,
- f) integrację systemów VSS/CCTV z infrastrukturą teleinformatyczną oraz innymi systemami zabezpieczeń technicznych,
- g) ocenę zgodności systemów VSS/CCTV z obowiązującymi normami i wymaganiami prawnymi,
- h) zarządzanie bezpieczeństwem obiektów z wykorzystaniem systemów telewizji dozorowej.

Dodatkowe uwagi

Brak

Nazwa kompetencji nr 9: Zadania i odpowiedzialność administratora i operatora Centrum Monitorowania Alarmów

Czy kompetencja/kwalifikacja jest włączona do Zintegrowanego Systemu Kwalifikacji?

NIE

Krótką charakterystyka kompetencji

Zadania i odpowiedzialność administratora i operatora Centrum Monitorowania Alarmów.

Efekt uczenia się 1: Charakteryzuje rolę, funkcje i odpowiedzialność administratora oraz operatora Centrum Monitorowania Alarmów (CMA)

Kryteria weryfikacji:

- A. identyfikuje wymagania prawne i normatywne dotyczące prowadzenia usług Centrum Monitorowania Alarmów przez przedsiębiorcę posiadającego koncesję na wykonywanie działalności gospodarczej w zakresie usług ochrony osób i mienia,
- B. określa wymagania organizacyjne i techniczne dotyczące funkcjonowania CMA, w tym zapewnienie ciągłości działania i niezawodności systemu,
- C. rozróżnia zakres odpowiedzialności administratora CMA oraz operatora stanowiska operatorskiego,
- D. identyfikuje rodzaje systemów zabezpieczeń technicznych połączonych z CMA,
- E. rozróżnia sygnały wpływające do CMA z wielu monitorowanych obiektów,
- F. wskazuje zasady współpracy CMA z klientami, ochroną fizyczną (w tym SUFO), służbami publicznymi oraz służbami technicznymi operatora systemu.

Metody walidacji:

- Ad.A. test teoretyczny
- Ad.B. test teoretyczny
- Ad.C. test teoretyczny
- Ad.D. test teoretyczny
- Ad.E. test teoretyczny
- Ad.F. test teoretyczny

Efekt uczenia się 2: Charakteryzuje zasady organizacji i bieżącego funkcjonowania Centrum Monitorowania Alarmów w zakresie obsługi sygnałów alarmowych i informacji z wielu monitorowanych obiektów

Kryteria weryfikacji:

- A. identyfikuje zasady tworzenia i aktualizacji bazy danych monitorowanych obiektów oraz przypisanych do nich procedur,
- B. rozróżnia rodzaje torów transmisji wykorzystywanych do przesyłania sygnałów do CMA,
- C. określa zasady priorytetyzacji i kolejności obsługi zdarzeń wpływających do CMA,
- D. identyfikuje zasady przekazywania obsługi zdarzeń pomiędzy stanowiskami operatorskimi,
- E. wskazuje podstawowe wymagania w zakresie dokumentowania czynności operatora (np. wpisy w książce służby, rejestr zdarzeń).

Metody walidacji:

- Ad.A. test teoretyczny
- Ad.B. test teoretyczny
- Ad.C. test teoretyczny
- Ad.D. test teoretyczny
- Ad.E. test teoretyczny

Efekt uczenia się 3: Charakteryzuje zasady analizowania, klasyfikacji i priorytetyzacji sygnałów wpływających do Centrum Monitorowania Alarmów

Kryteria weryfikacji:

- A. rozróżnia typy i rodzaje sygnałów zagrożeń wpływających do CMA (np. alarmy włamaniowe, pożarowe, techniczne, sygnały z systemów kontroli dostępu, monitoring wizyjny),
- B. określa zasady klasyfikacji zdarzeń według ich rodzaju i poziomu istotności,
- C. wskazuje zasady ustalania priorytetu obsługi zdarzeń w zależności od charakteru zagrożenia i wymagań klienta,
- D. identyfikuje zakres informacji niezbędnych do podjęcia decyzji o dalszym postępowaniu (np. lokalizacja, typ systemu, historia zdarzeń),

- E. wskazuje znaczenie dokumentowania przebiegu obsługi zdarzenia w rejestrach CMA.

Metody walidacji:

- Ad.A. test teoretyczny
- Ad.B. test teoretyczny
- Ad.C. test teoretyczny
- Ad.D. test teoretyczny
- Ad.E. test teoretyczny

Efekt uczenia się 4: Charakteryzuje zasady analizy obrazu oraz wykorzystania funkcji systemów monitoringu wizyjnego w pracy operatora Centrum Monitorowania Alarmów**Kryteria weryfikacji:**

- A. identyfikuje czynniki wpływające na jakość obrazu w systemach monitoringu wizyjnego (np. warunki oświetleniowe, warunki atmosferyczne, ustawienia kamery),
- B. rozróżnia sytuacje wymagające weryfikacji wizualnej alarmu od zdarzeń niewymagających analizy obrazu,
- C. wskazuje podstawowe funkcje systemów monitoringu wizyjnego wspomagające pracę operatora (np. podgląd na żywo, odtwarzanie nagrań, powiększenie obrazu, funkcje analityczne),
- D. rozróżnia alarmy generowane automatycznie przez systemy analityki wideo od alarmów pochodzących z innych systemów zabezpieczeń technicznych,
- E. identyfikuje ograniczenia interpretacji obrazu oraz znaczenie zachowania ostrożności przy podejmowaniu decyzji na podstawie materiału wizyjnego.

Metody walidacji:

- Ad.A. test teoretyczny
- Ad.B. test teoretyczny
- Ad.C. test teoretyczny
- Ad.D. test teoretyczny
- Ad.E. test teoretyczny

Efekt uczenia się 5: Charakteryzuje zasady współpracy operacyjnej, komunikacji oraz organizacji pracy w Centrum Monitorowania Alarmów

Kryteria weryfikacji:

- A. identyfikuje zasady współpracy operatora monitoringu z Policją, Strażą Pożarną i innymi służbami odpowiedzialnymi za zapewnienie porządku publicznego,
- B. wskazuje zasady przekazywania informacji do ochrony fizycznej (w tym SUFO) oraz do służb odpowiedzialnych za zapewnienie porządku publicznego w przypadku wystąpienia zdarzenia,
- C. wskazuje zakres informacji pochodzących z systemów monitorowania alarmów (w tym systemów telewizji dozorowej i innych) niezbędnych do podjęcia interwencji przez ochronę fizyczną (np. lokalizacja zdarzenia, opis sytuacji, liczba intruzów),
- D. identyfikuje przykładowe procedury postępowania w odniesieniu do wymagań klienta, przepisów prawa i standardów branżowych,
- E. identyfikuje zasady archiwizacji zdarzeń i udostępniania materiałów jako potencjalnych dowodów właściwym organom,
- F. wskazuje metody skutecznej komunikacji interpersonalnej,
- G. identyfikuje podstawowe zasady organizacji stanowiska pracy operatora dotyczące bezpieczeństwa i higieny pracy, ergonomii i czynników wpływających na koncentrację.

Metody walidacji:

- Ad.A. test teoretyczny
- Ad.B. test teoretyczny
- Ad.C. test teoretyczny
- Ad.D. test teoretyczny
- Ad.E. test teoretyczny
- Ad.F. test teoretyczny
- Ad.G. test teoretyczny

Szacowana skala niedoboru kompetencji/kwalifikacji

3 170

Usługa rozwojowa wspierająca zdobycie kompetencji/kwalifikacji

Standard usługi:

Usługa realizowana przez podmiot wpisany do Bazy Usług Rozwojowych, spełniający wymagania określone w Rozporządzeniu Ministra Funduszy i Polityki Regionalnej z dnia 28 lipca 2023 r. w sprawie rejestru podmiotów świadczących usługi rozwojowe (Dz.U. z 2023 r. poz. 1686), zgodnie z zasadami określonymi w Regulaminie Bazy Usług Rozwojowych oraz w niniejszej rekomendacji.

Warunki w zakresie kompetencji osób przystępujących do usługi:

brak

Maksymalna liczebność grupy szkoleniowej:

30 osób – wersja zdalna w czasie rzeczywistym lub

30 osób – forma stacjonarna

Minimalny czas trwania usługi:

7 h zegarowych

Minimalne wymagania w zakresie zasobów:

- a) sala szkoleniowa spełniająca standardy jakości prowadzenia zajęć dydaktycznych, wyposażona w rzutnik multimedialny lub ekran do prezentacji materiałów szkoleniowych (dla usługi realizowanej w formie stacjonarnej lub hybrydowej),
- b) sprzęt komputerowy dla trenera wraz z oprogramowaniem umożliwiającym realizację programu szkolenia oraz prezentację materiałów dydaktycznych (dla usługi realizowanej w formie stacjonarnej lub hybrydowej),
- c) stabilne łącze internetowe umożliwiające prowadzenie zajęć w czasie rzeczywistym oraz przesyłanie materiałów szkoleniowych (dla usługi realizowanej w formie zdalnej lub hybrydowej),
- d) urządzenia umożliwiające komunikację audio-wideo w czasie rzeczywistym, w szczególności kamera oraz mikrofon dla trenera (dla usługi realizowanej w formie zdalnej lub hybrydowej),

- e) oprogramowanie umożliwiające prowadzenie zajęć w trybie zdalnym w czasie rzeczywistym, w szczególności platformę wideokonferencyjną (np. Microsoft Teams lub rozwiązanie równoważne), zapewniającą:
 - transmisję audio i wideo,
 - możliwość prezentacji materiałów szkoleniowych,
 - komunikację z uczestnikami usługi oraz zadawanie pytań w trakcie zajęć,
- f) zasób legalnych wersji dokumentów normalizacyjnych, o których mowa w art. 2 pkt 3 ustawy z dnia 12 września 2002 r. o normalizacji (Dz.U. 2015 poz. 1483), w zakresie odpowiadającym efektom uczenia się realizowanym w ramach usługi,
- g) materiały szkoleniowe dla uczestników usługi w formie elektronicznej lub papierowej.

Wymagania w zakresie kompetencji trenera:

Kompetencje określone w §6 Rozporządzenia Ministra Funduszy i Polityki Regionalnej z dnia 28 lipca 2023 r. w sprawie rejestru podmiotów świadczących usługi rozwojowe (Dz.U. z 2023 r. poz. 1686) oraz:

- h) **min. 12 miesięcy** doświadczenia w zakresie odpowiadającym efektom uczenia się i kryteriom weryfikacji,
- i) doświadczenie w prowadzeniu szkoleń lub doradztwa w temacie usługi - min. **100** godzin.

Sposób oraz metody realizacji usługi:

Szkolenie może być realizowane w formie stacjonarnej, zdalnej lub hybrydowej.

Usługa szkoleniowa powinna zostać zrealizowana z wykorzystaniem następujących metod: wykłady, prezentacje studiów przypadków (case studies), symulacje incydentów, analiza rzeczywistych przypadków z branży zabezpieczeń technicznych.

Usługa musi zostać zakończona weryfikacją efektów uczenia się, zgodnie ze standardami określonymi w Rozporządzeniu Ministra Funduszy i Polityki Regionalnej z dnia 28 lipca 2023 r. w sprawie rejestru podmiotów świadczących usługi rozwojowe (Dz.U. z 2023 r. poz. 1686), przeprowadzoną metodami: test teoretyczny (pisemny).

Potencjalni uczestnicy usług rozwojowych

- a) pełnienie funkcji administratora lub operatora w Centrum Monitorowania Alarmów (CMA),
- b) nadzór nad funkcjonowaniem CMA,
- c) współpracę z ochroną fizyczną (w tym SUFO) oraz służbami odpowiedzialnymi za zapewnienie porządku publicznego,
- d) prowadzenie dokumentacji operacyjnej CMA oraz zapewnienie zgodności działań z wymaganiami klienta, przepisami prawa i standardami branżowymi,
- e) nadzór nad organizacją stanowiska operatorskiego, w tym zapewnienie ciągłości działania i właściwych warunków pracy.

Dodatkowe uwagi

Brak