

Załącznik do uchwały nr 6235/2026

Zarządu Województwa Opolskiego

z 7 września 2026 r.



Fundusze Europejskie
dla Opolskiego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



**Analiza dotycząca możliwych form wsparcia dla
przedsiębiorstw w ramach**

Działania 14.1 Rozwój technologii dual-use

oraz

Działania 17.1 Edukacja w budowaniu odporności instytucji

i przedsiębiorstw

Programu Fundusze Europejskie dla Opolskiego 2021-2027

Szymon Ogłaza

Zuzanna Donath-Kasiura

Zbigniew Kubalańca

Robert Węgrzyn

Antoni Konopka

Opracował Zespół w składzie:

podinspektor Marcin Wodziński – Naczelnik Wydziału Prewencji KWP Opole

mł. kpt. Marcin Melnarowicz – kierownik sekcji w Wydziale Logistyki Komendy
Wojewódzkiej PSP w Opolu

Robert Czochara – Opolskie Centrum Ratownictwa Medycznego

Bartosz Maziarz – Dyrektor Biura Bezpieczeństwa UMWO

Aneta Skawińska – Biuro Bezpieczeństwa UMWO

Opolskie Centrum Rozwoju Gospodarki, wrzesień 2026 r.

Spis treści

Wstęp.....	4
Diagnoza potrzeb i uzasadnienie zakresu wsparcia.....	6
Definicje.....	7
Zasady oceny kwalifikowalności szkoleń	8
Katalog branż przedsiębiorstw możliwych do wsparcia	10
Katalog rozwiązań proobronnych możliwych do wsparcia	12
Produkty i technologie ochrony osobistej i wsparcia działań.....	12
Rozwiązania logistyczne i mobilne.....	13
Technologie cyfrowe i organizacyjne	14
Innowacje środowiskowe i odpornościowe.....	14
Katalog obszarów szkoleniowych	15
I. Cyberbezpieczeństwo i ochrona systemów informatycznych oraz przemysłowych	15
II. Bezpieczeństwo energetyczne i odporność infrastruktury energetycznej.....	16
III. Automatyzacja, ciągłość i odporność procesów produkcyjnych	16
IV. Logistyka strategiczna i odporność łańcuchów dostaw	17
V. Systemy bezzałogowe w ochronie infrastruktury i reagowaniu kryzysowym	18
VI. Zarządzanie kryzysowe i odporność organizacji.....	19
Wnioski	20
Źródła.....	20

Wstęp

Dynamicznie zmieniające się uwarunkowania geopolityczne, wzrost znaczenia zagrożeń hybrydowych, cyberzagrożeń oraz doświadczenia wynikające z ostatnich kryzysów o charakterze zdrowotnym, energetycznym, klimatycznym i bezpieczeństwa międzynarodowego powodują konieczność budowania odporności państwa i regionów w sposób kompleksowy, obejmujący zarówno rozwój zdolności przemysłowych, jak i wzmacnianie kompetencji społeczeństwa oraz gospodarki.

Współczesne bezpieczeństwo nie jest już wyłącznie domeną sił zbrojnych i administracji publicznej. Coraz większą rolę odgrywają przedsiębiorstwa, które stanowią integralny element krajowych i regionalnych systemów bezpieczeństwa poprzez udział w strategicznych łańcuchach dostaw, utrzymanie ciągłości funkcjonowania infrastruktury krytycznej, rozwój nowoczesnych technologii oraz zapewnienie zdolności produkcyjnych niezbędnych w sytuacjach kryzysowych. Szczęólnego znaczenia nabierają technologie i rozwiązania o podwójnym zastosowaniu (dual-use), które mogą być wykorzystywane zarówno na potrzeby cywilne, jak i obronne, a także szeroko rozumiane rozwiązania pro-obronne wzmacniające odporność logistyczną, technologiczną, energetyczną, informacyjną i organizacyjną państwa.

Potrzeba aktywnego zaangażowania potencjału gospodarczego województwa opolskiego w budowanie odporności i bezpieczeństwa znajduje odzwierciedlenie w zapisach programu regionalnego *Fundusze Europejskie dla Opolskiego 2021–2027* (FEO 2021-2027). W ramach działania 14.1 *Rozwój technologii dual-use* ” przewidziano wsparcie dla przedsięwzięć służących zwiększaniu zdolności przemysłowych na rzecz gotowości cywilnej, ze szczególnym uwzględnieniem technologii podwójnego zastosowania, rozwoju działalności badawczo-rozwojowej, wdrażania innowacyjnych rozwiązań pro-obronnych oraz modernizacji potencjału produkcyjnego przedsiębiorstw. Jednocześnie działanie 17.1 *Edukacja w budowaniu odporności instytucji i przedsiębiorstw* zakłada podniesienie umiejętności i kompetencji oraz nabycie kwalifikacji niezbędnych do funkcjonowania przedsiębiorstw w odniesieniu do wzmacniania gotowości cywilnej, cyberbezpieczeństwa, przemysłu obronnego oraz technologii dual-use.

Ze względu na nowy charakter planowanych interwencji oraz brak wcześniejszych regionalnych instrumentów wsparcia realizowanych w tak szerokim zakresie tematycznym,

konieczne stało się opracowanie materiału analitycznego identyfikującego potencjalne obszary wsparcia możliwe do objęcia interwencją w ramach obydwu działań. Celem dokumentu jest stworzenie spójnych ram interpretacyjnych dla przyszłych działań wdrożeniowych oraz wskazanie branż gospodarki, rodzajów rozwiązań technologicznych i organizacyjnych oraz zakresów umiejętności, kompetencji i kwalifikacji, które mogą przyczyniać się do wzmacniania zdolności obronnych i odporności regionu.

Niniejsze opracowanie stanowi syntetyczne połączenie trzech komplementarnych katalogów przygotowanych na potrzeby programowania wsparcia w ramach FEO 2021–2027:

1. katalogu branż przedsiębiorstw mogących uczestniczyć w budowaniu zdolności obronnych i odporności regionu,
2. katalogu rozwiązań proobronnych oraz technologii o znaczeniu dla bezpieczeństwa i odporności,
3. katalogu obszarów szkoleniowych służących podniesieniu umiejętności i kompetencji oraz nabyciu kwalifikacji pracowników oraz przedsiębiorców.

Katalogi zostały opracowane przy udziale ekspertów reprezentujących instytucje odpowiedzialne za bezpieczeństwo publiczne, ochronę ludności, ratownictwo oraz zarządzanie kryzysowe w województwie opolskim, co pozwoliło na uwzględnienie zarówno uwarunkowań wynikających z dokumentów strategicznych i regulacyjnych, jak również praktycznych potrzeb systemu bezpieczeństwa regionu. W pracach uczestniczyli przedstawiciele administracji samorządowej, Policji, Państwowej Straży Pożarnej oraz ratownictwa medycznego, dysponujący doświadczeniem w zakresie gotowości cywilnej, ochrony ludności, reagowania kryzysowego oraz funkcjonowania infrastruktury krytycznej. Przedstawiony materiał ekspercki służy określeniu kierunków interwencji dla działania 14.1 oraz działania 17.1 w ramach programu regionalnego FEO 2021-2027 w zakresie wzmacniania odporności województwa opolskiego poprzez rozwój potencjału przedsiębiorstw, technologii, produktów, usług oraz kompetencji kadr, które mogą znaleźć zastosowanie zarówno w codziennym funkcjonowaniu gospodarki, jak i w sytuacjach kryzysowych, zagrożenia bezpieczeństwa lub konieczności wsparcia systemu obronnego państwa.

Diagnoza potrzeb i uzasadnienie zakresu wsparcia

Na potrzeby opracowania Opolskie Centrum Rozwoju Gospodarki przeprowadziło jakościową diagnozę funkcjonalną. Objęła ona analizę FEO 2021–2027 i SZOP, aktualnych dokumentów regionalnych, danych o gospodarce województwa oraz kierunków polityki UE w dziedzinie gotowości i przemysłu obronnego. Wykorzystano również wiedzę ekspercką i konsultacje robocze z przedstawicielami administracji samorządowej, Policji, Państwowej Straży Pożarnej i ratownictwa medycznego. Diagnoza miała charakter wdrożeniowy, a nie badania statystycznego: jej celem było rozpoznanie funkcji przedsiębiorstw, które należy wzmocnić, oraz powtarzających się potrzeb rozwojowych.

Pierwsza wersja diagnozy została poddana konsultacjom z przedsiębiorcami oraz innymi podmiotami zainteresowanymi planowanym wsparciem. Zgłoszone uwagi przeanalizowano pod kątem ich zasadności i zgodności z dokumentacją programową – uwagi zasadne uwzględniono w aktualizacji, natomiast pozostałe pozostawiono bez uwzględnienia.

Diagnoza wskazała, że przedsiębiorstwa pełnią coraz ważniejszą funkcję w utrzymaniu ciągłości dostaw, energii, transportu, łączności i procesów produkcyjnych, a także w zapewnianiu produktów i usług potrzebnych podczas zakłóceń lub kryzysu. W warunkach zagrożeń hybrydowych, cyberataków i niestabilnych łańcuchów dostaw odporność regionu zależy zarówno od zdolności przedsiębiorstw do nieprzerwanego działania, jak i od ich gotowości do adaptowania technologii i procesów do zastosowań związanych z bezpieczeństwem lub obronnością.

Województwo opolskie dysponuje zróżnicowanym potencjałem przemysłowym, technologicznym i logistycznym, powiązanych m.in. z przemysłem maszynowym i metalowym, chemią, energetyką, przetwórstwem rolno-spożywczym, technologiami materiałowymi, ICT, transportem i ochroną środowiska. Zidentyfikowana luka dotyczy przede wszystkim przełożenia istniejącego know-how na sprawdzone technologie, produkty i procesy dual-use lub proobronne, ich testowania, uruchamiania pierwszej produkcji oraz zwiększania zdolności wytwórczych. Uzasadnia to katalog branż i rozwiązań przewidziany dla Działania 14.1.

Równolegle rozpoznano potrzebę podnoszenia kompetencji pracowników i osób zarządzających. Najczęściej powtarzające się potrzeby dotyczą ochrony systemów IT i OT,

bezpieczeństwa energetycznego, elastycznej automatyzacji i utrzymania produkcji, odporności łańcuchów dostaw, operacyjnego wykorzystania systemów bezałogowych oraz zarządzania ciągłością działania i sytuacją kryzysową. Kompetencje te powinny być rozwijane w związku z rolą zawodową uczestnika i rzeczywistymi funkcjami przedsiębiorstwa, a nie jako szkolenia ogólne. Uzasadnia to sześć obszarów szkoleniowych wskazanych dla drugiego typu projektów Działania 17.1.

Wyniki diagnozy uzasadniają zastosowanie dwóch uzupełniających się ścieżek: wsparcia technologiczno-inwestycyjnego w Działaniu 14.1 oraz wsparcia kompetencyjnego w Działaniu 17.1. Katalogi zawarte w analizie mają charakter kierunkowy. Przynależność do wskazanej branży, nazwa produktu albo tytuł szkolenia nie przesądza o jednostronnie o kwalifikowalności - decydują rzeczywisty zakres przedsięwzięcia, jego zgodność z celem i warunkami danego działania.

Definicje

Technologie podwójnego zastosowania (dual-use) – technologie, produkty, procesy lub kompetencje, które mogą być wykorzystywane zarówno w działalności cywilnej, jak i w obszarze bezpieczeństwa, obronności lub ochrony ludności, w szczególności w sektorach takich jak: przemysł obronny, infrastruktura krytyczna, cyberbezpieczeństwo, energetyka, transport, łączność, produkcja zaawansowana oraz technologie cyfrowe.

Gotowość cywilna – zdolność przedsiębiorstw i ich pracowników do zapewnienia ciągłości działania, odporności na zagrożenia oraz wsparcia funkcjonowania państwa i społeczeństwa w sytuacjach kryzysowych poprzez odpowiednie kompetencje pracowników w tym w szczególności w obszarach takich jak: zarządzanie kryzysowe, bezpieczeństwo infrastruktury, logistyka, energetyka, łączność oraz cyberbezpieczeństwo. Do kompetencji związanych z gotowością cywilną zalicza się w szczególności umiejętności pozwalające na zapewnienie ciągłości działania, odporności organizacyjnej, skuteczne reagowanie na sytuacje kryzysowe oraz utrzymanie kluczowych funkcji i usług w warunkach zakłóceń lub zagrożeń.

Rozwiązania proobronne – technologie, produkty, procesy lub usługi o istotnym znaczeniu dla odporności, bezpieczeństwa, logistyki albo zdolności produkcyjnych, które nie muszą spełniać definicji produktu dual-use w reżimie kontroli eksportu.

Zasady oceny kwalifikowalności szkoleń

Drugi typ projektów możliwy do realizacji w ramach Działania 17.1, czyli „Rozwój umiejętności, kompetencji i kwalifikacji pracowników przedsiębiorstw i przedsiębiorców oraz przedsiębiorstw społecznych w dziedzinie gotowości cywilnej, w przemyśle obronnym, w tym w odniesieniu do zdolności w zakresie technologii podwójnego zastosowania oraz w dziedzinie cyberbezpieczeństwa” realizowany będzie poprzez szkolenia. Przy ocenie, czy szkolenie jest kwalifikowalne w ramach niniejszego działania stosowane będą poniższe zasady.

1. Wsparciem mogą zostać objęte wyłącznie szkolenia:
 - ujęte w niniejszym katalogu lub równoważne tematycznie,
 - bezpośrednio powiązane z technologiami dual-use / gotowością cywilną / cyberbezpieczeństwem / działalnością w sektorach strategicznych lub obronnych.
2. Ocena kwalifikowalności szkolenia dokonywana jest w pierwszej kolejności na podstawie jego zgodności z katalogiem.
3. Intytucja Ogłaszająca Nabór może odrzucić szkolenie, jeżeli jego rzeczywisty zakres nie odpowiada deklarowanemu obszarowi lub ma charakter ogólny lub niezwiązany z celami projektu.
4. Samo nazewnictwo szkolenia nie stanowi podstawy do uznania jego kwalifikowalności.
5. Wsparcie w ramach niniejszego katalogu dotyczy rozwoju kompetencji pracowników przedsiębiorstw, w kontekście ich roli zawodowej i funkcjonowania organizacji. Nie obejmuje ono działań o charakterze edukacji powszechnej, skierowanych do mieszkańców, dotyczących indywidualnego przygotowania do sytuacji kryzysowych. Szkolenia ukierunkowane wyłącznie na potrzeby życia prywatnego uczestników, niezwiązane z funkcjonowaniem przedsiębiorstwa lub wykonywaną pracą, nie są kwalifikowalne w ramach niniejszego katalogu.
6. Wsparciem nie mogą zostać objęte szkolenia:
 - charakterze ogólnym lub podstawowym, niezwiązane z katalogiem,
 - dotyczące kompetencji biurowych lub administracyjnych (np. pakiety biurowe),

- szkolenia sprzedażowe, marketingowe lub ogólne zarządcze,
- obowiązkowe szkolenia wynikające z przepisów prawa (np. BHP),
- szkolenia niezwiązane z wykorzystaniem kompetencji w obszarach: dual-use, gotowości cywilnej, cyberbezpieczeństwa, przemysłu obronnego lub sektorów strategicznych.

Katalog branż przedsiębiorstw możliwych do wsparcia

W ramach działania 14.1 *Rozwój technologii dual-use* Priorytetu 14 „Fundusze Europejskie na rzecz zdolności obronnych opolskiego” wsparcie kierowane będzie do przedsiębiorstw prowadzących działalność w branżach posiadających potencjał do rozwijania, wdrażania lub produkcji technologii, produktów i usług służących wzmocnieniu zdolności obronnych oraz odporności państwa i regionu.

Wskazane branże zostały wytypowane na podstawie analizy ich potencjalnego udziału w regionalnych i krajowych łańcuchach wartości związanych z bezpieczeństwem i obronnością, możliwości adaptacji istniejących procesów produkcyjnych do potrzeb sektora obronnego oraz zdolności do rozwijania rozwiązań zwiększających odporność infrastruktury, gospodarki i społeczeństwa na sytuacje kryzysowe, zagrożenia hybrydowe oraz zakłócenia funkcjonowania państwa.

Uwzględnione w katalogu branże obejmują zarówno sektory o wysokim potencjale technologicznym, zdolne do tworzenia rozwiązań dual-use, jak również branże dostarczające produkty i usługi niezbędne dla zapewnienia odporności państwa, ochrony ludności, zabezpieczenia działań ratowniczych oraz utrzymania ciągłości funkcjonowania gospodarki i infrastruktury w sytuacjach kryzysowych.

- 1. Technologie chemiczne**
- 2. Technologie budownictwa i drewna**
- 3. Technologie przemysłu maszynowego i metalowego**
- 4. Technologie przemysłu energetycznego (w tym OZE)**
- 5. Technologie rolno-spożywcze**
- 6. Inteligentne systemy zarządzania mobilnością**
- 7. Sektor ICT**
- 8. Gospodarka obiegu zamkniętego**
- 9. Transport i logistyka**
- 10. Produkcja materiałów i wyrobów specjalistycznych**
- 11. Technologie wodno-sanitarne i środowiskowe**

- 12. Technologie medyczne i ratownicze (w zakresie sprzętu medycznego, systemów ratowniczych, medycyny urazowej, żywności medycznej)**
- 13. Sektor bezpieczeństwa i ochrony**

Katalog rozwiązań proobronnych możliwych do wsparcia

Załącznik I rozporządzenia 2021/821¹ zawiera wyspecyfikowane technologie i towary podlegające kontroli eksportowej (np. zaawansowana elektronika, kryptografia, drony, lasery, materiały o wysokiej odporności, technologie nuklearne) - to właśnie technologie o podwójnym zastosowaniu (dual use), głównie „high-tech” o potencjalnym militarnym zastosowaniu możliwe do wsparcia.

Wykaz ten nie stanowi samodzielnego katalogu projektów kwalifikowalnych w Działaniu 14.1. Zgodnie z SZOP przedsięwzięcie dotyczące dual-use musi prowadzić do opracowania lub praktycznego wykorzystania technologii, produktu albo procesu możliwego do zastosowania zarówno cywilnie, jak i w obszarze bezpieczeństwa lub obronności.

Natomiast poniższe propozycje proobronne spoza katalogu dual-use, które będą mogły być dodatkowo wspierane, dotyczą:

- produktów „niskotechnologicznych” (odzież, żywność, plandeki PCV),
- rozwiązań logistycznych (mobilne moduły, uzdatnianie wody, kontenery),

Nie wchodzą one w zakres załącznika I, bo nie są objęte kontrolą eksportu jako technologie strategiczne. Ale w praktyce obronnej są niezbędne.

Cel szczegółowy Priorytetu 14 FEO 2021-2027 brzmi „Wzmacnianie potencjału przemysłowego w celu wspierania zdolności obronnych, przy priorytetowym traktowaniu tych o podwójnym zastosowaniu”, dlatego takie rozróżnienie (dual-use jako priorytet, a obok nich koszyk proobronnych rozwiązań wspierających odporność) jest logiczne i uzasadnione.

Produkty i technologie ochrony osobistej i wsparcia działań

- obuwie i odzież specjalistyczna/umundurowanie (np. trudnopalne, wodoodporne, odporne na warunki ekstremalne),

¹ ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2021/821 z dnia 20 maja 2021 r. ustanawiające unijny system kontroli wywozu, pośrednictwa, pomocy technicznej, tranzytu i transferu produktów podwójnego zastosowania.

- środki ochrony indywidualnej (np. hełmy lekkie, okulary balistyczne, rękawice ochronne – niekwalifikujące się jako broń, latarki taktyczne wodo-odporne/wybucho-odporne, maski tlenowe/pełno-twarzowe/przeciwpyłowe, race ratownicze do oznaczania strefy ewakuacji),
- plandeki, powłoki i zabezpieczenia pojazdów militarnych i schronów i (np. osłony ochronne, materiały maskujące, maty kompozytowe szybkiego montażu),
- systemy maskowania i kamuflażu (np. siatki, powłoki ograniczające sygnaturę w IR/UV),
- sprzęt i wyposażenie medyczne polowe (np. zestawy mobilne, przenośne USG, nowoczesne opatrunki hemostatyczne),
- mobilne zestawy higieniczne (np. prysznice polowe, toalety chemiczne, utylizacja odpadów medycznych i bytowych),
- produkcja wiązek kablowych, hydraulika siłowa,
- prefabrykowane żelbetowe moduły ochronne,
- systemy zabezpieczenia dostępu o podwyższonej odporności.

Rozwiązania logistyczne i mobilne

- specjalistyczna żywność (np. liofilizowana, przygotowywana w trudnych warunkach, innowacyjne metody przechowywania),
- mobilne moduły mieszkalne i medyczne (np. kontenery, szpitale polowe, moduły sanitarne, kuchnie polowe),
- systemy oczyszczania wody i powietrza,
- łodzie ratunkowe,
- mobilne zbiorniki na paliwo,
- mobilne źródła energii (np. generatory, magazyny energii, OZE w wersji polowej),
- zestawy do szybkiej naprawy infrastruktury (np. maty samoprzylepne do zabezpieczenia uszkodzonych dachów, rurociągów, zbiorników),

- mobilne magazyny kontenerowe oraz magazyny polowe (namioty, hale tymczasowe)

Technologie cyfrowe i organizacyjne

- symulatory VR/AR dla szkoleń ratowniczych i ewakuacyjnych.
- systemy łączności kryzysowej

WAŻNE !!!

W przypadku rozwiązań cyfrowych - oprogramowania/aplikacji/systemów, itp. z uwagi na szczegółowe wytyczne krajowe w tym zakresie oraz konieczność zapewnienia demarkacji rozwiązań, możliwe będzie wsparcie jedynie na szczeblu krajowym w ramach kierowanych programów celowych, jak np. SAFE czy PERUN.

Innowacje środowiskowe i odpornościowe

- suplementy diety i żywność dla osób chorych (np. medyczna żywność specjalnego przeznaczenia, nutraceutyki wspierające odporność).
- materiały o podwyższonej odporności (np. trudnopalne, antykorozyjne, samonaprawiające się),
- systemy recyklingu i odzysku wody/powietrza w warunkach polowych,
- systemy detekcji chemicznej i biologicznej.

WAŻNE !!!

Zakwalifikowanie produktu jako rozwiązania dual-use lub proobronnego każdorazowo wymaga oceny konkretnego rozwiązania, w szczególności jego specyfikacji technicznej, parametrów użytkowych oraz właściwości operacyjnych właściwych dla danego zastosowania, takich jak np. mobilność, autonomia energetyczna, odporność na czynniki CBRN lub możliwość dekontaminacji. Wnioskodawca powinien wykazać praktyczne zastosowanie rozwiązania w obszarze cywilnym oraz – w przypadku dual-use – również w obszarze bezpieczeństwa lub obronności, a w przypadku rozwiązania proobronnego – jego istotne znaczenie dla odporności lub logistyki. Sam typ, nazwa handlowa ani ogólne przeznaczenie produktu nie przesądzą o możliwości objęcia go wsparciem.

Jeżeli dla danego rozwiązania przepisy prawa, normy branżowe lub dokumentacja wymagają uzyskania certyfikatów, atestów, wyników badań, dopuszczeń, oznaczeń albo kodów identyfikacyjnych, w tym np. kodu NCAGE, wnioskodawca powinien wykazać możliwość spełnienia tych wymagań.

Katalog obszarów szkoleniowych

Sposób rozumienia katalogu

Poniższy katalog obejmuje sześć obszarów szkoleniowych wybranych z uwzględnieniem struktury gospodarczej województwa opolskiego. Region charakteryzuje się dominacją przemysłu przetwórczego (spożywczy, metalowy, motoryzacyjny, chemiczny), rozwijającym się sektorem OZE i elektromobilności, obecnością sektora IT/BPO oraz strategicznym położeniem logistycznym na osi autostrady A4. Dobór obszarów odzwierciedla faktyczny potencjał absorpcji kompetencji dual-use przez przedsiębiorstwa regionu.

I. Cyberbezpieczeństwo i ochrona systemów informatycznych oraz przemysłowych

Sektor IT/BPO skoncentrowany w Opolu oraz rosnąca automatyzacja w przemyśle metalowym i motoryzacyjnym generują bezpośrednie zapotrzebowanie na kompetencje z zakresu ochrony systemów IT i OT. Szkolenia z tego obszaru wpisują się w wymogi Krajowego Systemu Cyberbezpieczeństwa (KSC/NIS2) i mają bezpośrednie zastosowanie dual-use - ochrona systemów przemysłowych jest kompetencją zarówno z zakresu gotowości cywilnej, jak i w przemyśle obronnym, w tym w zakresie technologii podwójnego zastosowania.

Przykładowe szkolenia:

- Cyberbezpieczeństwo w przedsiębiorstwie - podstawy operacyjne,
- Zarządzanie bezpieczeństwem informacji (ISO/IEC 27001),
- Ochrona systemów przemysłowych (OT/ICS/SCADA) przed cyberatakami,
- Bezpieczeństwo sieci i infrastruktury IT w warunkach zakłóceń,
- Bezpieczeństwo środowisk chmurowych i usług zdalnych,
- Zarządzanie incydentami bezpieczeństwa (incident response),
- Testy penetracyjne i audyt bezpieczeństwa systemów IT,
- Ochrona danych wrażliwych i informacji strategicznych przedsiębiorstwa,
- Cyberbezpieczeństwo w systemach IoT i urządzeniach przemysłowych,
- Zarządzanie ciągłością działania systemów IT (IT disaster recovery).

II. Bezpieczeństwo energetyczne i odporność infrastruktury energetycznej

Województwo opolskie przechodzi intensywną transformację energetyczną - sektor OZE i elektromobilności był największym obszarem nowych inwestycji w regionie w 2024 r. Jednocześnie energochłonne branże (spożywcza, chemiczna, materiałów budowlanych) są szczególnie narażone na skutki przerw w dostawach energii. Kompetencje z zakresu bezpieczeństwa energetycznego mają charakter dual-use - są bezpośrednio wykorzystywane zarówno w zarządzaniu ciągłością działania przedsiębiorstwa, jak i w funkcjonowaniu infrastruktury krytycznej.

Przykładowe szkolenia:

- Zarządzanie bezpieczeństwem energetycznym przedsiębiorstwa,
- Systemy zasilania awaryjnego i redundancja energetyczna,
- Magazynowanie energii na potrzeby ciągłości działania,
- Mikrosieci i niezależne systemy zasilania w warunkach zakłóceń,
- Zarządzanie zużyciem energii w sytuacjach kryzysowych,
- Odporność infrastruktury energetycznej na zakłócenia zewnętrzne,
- Systemy monitoringu i zarządzania energią w czasie rzeczywistym,
- Inteligentne sieci energetyczne (smart grids) w kontekście bezpieczeństwa i stabilności dostaw.

III. Automatyzacja, ciągłość i odporność procesów produkcyjnych

Przemysł motoryzacyjny, metalowy i przetwórstwo spożywcze stanowią trzon gospodarki opolskiej. Przedsiębiorstwa z tych sektorów uczestniczą w rozbudowanych łańcuchach dostaw o znaczeniu strategicznym, w tym dla odbiorców z sektora publicznego i obronnego. Kompetencje z zakresu automatyzacji i odporności produkcji są typowym obszarem dual-use - umiejętność rekonfiguracji linii produkcyjnych, utrzymania procesów w trybie awaryjnym oraz wytwarzania komponentów w warunkach ograniczonych zasobów ma zastosowanie zarówno w działalności komercyjnej, jak i w realizacji kontraktów na rzecz bezpieczeństwa.

Przykładowe szkolenia:

- Obsługa i programowanie robotów przemysłowych w warunkach zmiennych i awaryjnych,
- Rekonfiguracja linii produkcyjnych i elastyczna integracja systemów automatyki,
- Systemy automatyki przemysłowej w zapewnieniu ciągłości działania,
- Tryby pracy awaryjnej systemów produkcyjnych (degraded mode operations),
- Redundancja i bezpieczeństwo systemów automatyki przemysłowej,
- Druk 3D i produkcja rozproszona w zapewnieniu ciągłości dostaw komponentów krytycznych,
- Produkcja komponentów w warunkach ograniczonej dostępności zasobów i materiałów,
- Rekonfiguracja procesów produkcyjnych w sytuacjach kryzysowych,
- Systemy monitoringu i wykrywania anomalii w procesach produkcyjnych (w tym z wykorzystaniem AI),
- Kontrola jakości w produkcji komponentów o znaczeniu strategicznym.

IV. Logistyka strategiczna i odporność łańcuchów dostaw

Województwo opolskie pełni kluczową funkcję węzła tranzytowego na osi wschód–zachód (autostrada A4 z sześcioma węzłami, bliskość autostrad A1 i dróg ekspresowych S8/S11). Przedsiębiorstwa logistyczne i produkcyjne regionu są uczestnikami łańcuchów dostaw o znaczeniu strategicznym - zarówno w łańcuchach przemysłowych, jak i w systemie zaopatrzenia na potrzeby bezpieczeństwa państwa. Kompetencje z zakresu zarządzania zakłóceniami w logistyce mają charakter dual-use i bezpośrednie zastosowanie w scenariuszach kryzysowych.

Przykładowe szkolenia:

- Zarządzanie logistyką w sytuacjach kryzysowych i zakłóceniach operacyjnych,

- Bezpieczne łańcuchy dostaw - identyfikacja ryzyk i procedury reagowania,
- Dywersyfikacja i odporność źródeł dostaw (supply chain resilience),
- Zarządzanie zakłóceniami w łańcuchach dostaw,
- Logistyka awaryjna i alternatywne kanały transportowe,
- Systemy monitorowania transportu i śledzenia towarów w sytuacjach kryzysowych,
- Logistyka infrastruktury krytycznej,
- Zastosowanie systemów UAV w monitoringu infrastruktury logistycznej i transportowej.

V. Systemy bezzałogowe w ochronie infrastruktury i reagowaniu kryzysowym

Monitoring infrastruktury krytycznej (energetycznej, transportowej, przemysłowej) z wykorzystaniem systemów UAV ma bezpośrednie zastosowanie operacyjne w przedsiębiorstwach dysponujących rozległą infrastrukturą - w szczególności w sektorze energetycznym i logistycznym. Jest to obszar o wyraźnym charakterze dual-use: te same kompetencje i systemy są wykorzystywane zarówno do inspekcji infrastruktury w warunkach normalnych, jak i do działań rozpoznawczych i reagowania kryzysowego. Do katalogu włączono wyłącznie szkolenia o zastosowaniu operacyjnym, z wyłączeniem szkoleń pilotażowych i regulacyjnych, które nie stanowią kompetencji dual-use.

Przykładowe szkolenia:

- Zastosowanie systemów UAV w reagowaniu kryzysowym i sytuacjach awaryjnych,
- Drony w ochronie i monitoringu infrastruktury krytycznej,
- Systemy UAV w inspekcji infrastruktury energetycznej i przemysłowej,
- Analiza danych z obrazowania lotniczego (UAV) na potrzeby operacyjne,
- Integracja systemów dronowych z systemami IT i zarządzania kryzysowego,

- Systemy autonomiczne i roboty mobilne w zastosowaniach operacyjnych.

VI. Zarządzanie kryzysowe i odporność organizacji

Obszar o charakterze przekrojowym, adresowany do wszystkich sektorów gospodarki regionu. Kompetencje z zakresu zarządzania kryzysowego, ciągłości działania i bezpieczeństwa operacyjnego stanowią fundament gotowości cywilnej przedsiębiorstw i są bezpośrednio powiązane z rolą przedsiębiorstw w systemie bezpieczeństwa państwa - jako operatorów infrastruktury, dostawców usług i uczestników łańcuchów dostaw. Wyłączone zostały szkolenia dotyczące indywidualnego przygotowania psychologicznego oraz działania niezwiązanego z funkcjonowaniem organizacji jako podmiotu gospodarczego.

Przykładowe szkolenia:

- Zarządzanie ryzykiem operacyjnym w przedsiębiorstwie,
- Zarządzanie ciągłością działania (Business Continuity Planning - BCP),
- Zarządzanie kryzysowe w organizacji - procedury i struktury decyzyjne,
- Ochrona infrastruktury krytycznej - rola i obowiązki przedsiębiorstwa,
- Bezpieczeństwo fizyczne i techniczne obiektów przedsiębiorstwa,
- Odporność organizacji na zagrożenia hybrydowe i dezinformację operacyjną,
- Zarządzanie zasobami przedsiębiorstwa w sytuacji kryzysowej (energia, woda, materiały, łączność),
- Organizacja pracy w warunkach ograniczonej dostępności mediów i infrastruktury,
- Procedury ewakuacji zakładu pracy i reagowania na sytuacje nadzwyczajne,
- Testowanie planów ciągłości działania - ćwiczenia i symulacje scenariuszy kryzysowych,
- Funkcjonowanie przedsiębiorstwa w warunkach zakłóceń operacyjnych i przerw w dostawach.

Dodatkowe uwagi

Analiza przedstawia podstawowe zasady, katalogi branż i rozwiązań proobronnych oraz obszarów szkoleniowych uzasadniający zakres wsparcia zaplanowanego w ramach działania 14.1 oraz w drugim typie projektów Działania 17.1.

Analiza została opracowana według stanu prawnego i programowego na 10 sierpnia 2026 r. Przy realizacji projektu należy stosować dokumenty i przepisy obowiązujące w dniu dokonywania danej czynności.

Wnioski

Przeprowadzona diagnoza potwierdza, że odporność województwa opolskiego wymaga jednoczesnego wzmacniania zdolności technologicznych i produkcyjnych przedsiębiorstw oraz kompetencji ich kadr. Najistotniejsze są rozwiązania i umiejętności służące ciągłości działania, cyberbezpieczeństwu, odpornej produkcji, energii, logistyce i zarządzaniu kryzysowemu.

Katalogi branż, rozwiązań proobronnych i obszarów szkoleniowych odpowiadają tym potrzebom, ale mają charakter kierunkowy. O możliwości wsparcia nie przesądza sama branża, nazwa produktu ani tytuł szkolenia, lecz rzeczywisty zakres przedsięwzięcia i jego zgodność z dokumentacją programową.

Działanie 14.1 i drugi typ projektów Działania 17.1 tworzą uzupełniający się model interwencji: pierwsze wspiera rozwój, testowanie i wdrażanie rozwiązań dual-use i proobronnych, drugie – kompetencje potrzebne do ich wykorzystania oraz do zwiększania gotowości cywilnej przedsiębiorstw. W Działaniu 17.1 jest realizowane poprzez PSF/BUR.

Źródła

1. [Program Fundusze Europejskie dla Opolskiego 2021–2027, wersja nr 4](#)
2. [Szczegółowy Opis Priorytetów FEO 2021–2027, SZOP.FEOP.027, obowiązujący od 28 lipca 2026 r.](#)
3. [Regionalna Strategia Innowacji Województwa Opolskiego 2030, aktualizacja z 2025 r.](#)
4. [Urząd Statystyczny w Opolu, Raport o sytuacji społeczno-gospodarczej województwa opolskiego 2026.](#)

5. [Rozporządzenie Parlamentu Europejskiego i Rady \(UE\) 2021/821 ustanawiające unijny system kontroli produktów podwójnego zastosowania – tekst skonsolidowany.](#)
6. [Rozporządzenie Rady Ministrów z dnia 17 września 2019 r. w sprawie klasyfikacji wyrobów i technologii, na których wytwarzanie lub obrót jest wymagane uzyskanie koncesji.](#)
7. [European Commission, European Defence Industrial Strategy, 5 marca 2024 r.](#)
8. [European Commission and High Representative, White Paper for European Defence – Readiness 2030, 19 marca 2025 r.](#)
9. [European Commission, EU Preparedness Union Strategy.](#)
10. [Dyrektywa Parlamentu Europejskiego i Rady \(UE\) 2022/2555 w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w Unii \(NIS2\).](#)
11. [Sprawozdanie o stanie cyberbezpieczeństwa Polski za rok 2025.](#)
12. [ENISA Threat Landscape 2025.](#)
13. [Wytyczne dotyczące realizacji projektów z udziałem środków EFS+ w regionalnych programach na lata 2021–2027.](#)
14. [Wytyczne dotyczące monitorowania postępu rzeczowego realizacji programów na lata 2021–2027 – informacje dotyczące kwalifikacji w EFS+.](#)
15. [Polska Agencja Rozwoju Przedsiębiorczości, Baza Usług Rozwojowych.](#)