



DOFINANSOWANIE PARP / BAZA USŁUG ROZWOJOWYCH

Odporność na zagrożenia hybrydowe dla firm gospodarki morskiej

Szkolenie budujące świadomość dla podmiotów sektora morskiego, operatorów portów i morskiej infrastruktury krytycznej — przygotowujące kadrę do rozpoznawania realnych zagrożeń hybrydowych mających miejsce dziś na Bałtyku.

Dlaczego to dotyczy Waszej firmy już dziś

Bałtyk jest dziś największym morskim teatrem działań hybrydowych prowadzonych przez Rosję na świecie. Infrastruktura energetyczna, porty i szlaki żeglugowe całego regionu są w coraz większym stopniu narażone na działania sabotażowe, szpiegowskie i cybernetyczne — a skala tego zjawiska rośnie z roku na rok.

LUKA, KTÓREJ NIKT ZA WAS NIE WYPEŁNI

Polskie służby państwowe nie przygotowują dziś firm gospodarki morskiej pod kątem zabezpieczenia przed działalnością szpiegowską i sabotażem — nie ma programu, szkolenia ani wytycznych, które przygotowywałyby kadrę operatorów portów, infrastruktury energetycznej czy armatorów do rozpoznawania tych zagrożeń. To szkolenie wypełnia właśnie tę powstałą lukę — konkretną, praktyczną wiedzę opartą na realnych, udokumentowanych incydentach z Bałtyku.

13+

uszkodzeń podmorskich gazociągów i kabli na Bałtyku w latach 2022–2025 (Nord Stream, Balticconnector, Estlink 2 i kolejne kable telekomunikacyjne)

~700

tankowców „floty cieni” objętych sankcjami UE, Wielkiej Brytanii i USA za ryzykowną żeglugę na granicy prawa

122 tys.

lotów, które zgłosiły zakłócenia sygnału GNSS nad Bałtykiem tylko między styczniem a kwietniem 2025 r.

INFRASTRUKTURA ENERGETYCZNA I TELEKOMUNIKACYJNA

W latach 2023–2025 doszło na Bałtyku do szeregu incydentów uszkodzenia podwodnych gazociągów, kabli energetycznych i telekomunikacyjnych za pomocą kotwic ciągniętych po dnie. Rosja regularnie wykorzystuje do mapowania infrastruktury krytycznej okręty hydrograficzne oraz jednostki „floty cieni”. Dodatkowo operatorzy tej infrastruktury na co dzień mierzą się z cyberatakami oraz zgłuszaniem i fałszowaniem sygnałów GNSS, co przy inwestycjach offshore — wymagających dokładności montażu liczonej w centymetrach — generuje realne koszty liczone w dziesiątkach tysięcy euro za pojedynczy epizod zakłóceń.

PORTY BAŁTYCKIE

Jednym z głównych wyzwań dla portów jest szpiegostwo wojskowe i gospodarcze: wzrost ruchu jednostek powiązanych z Rosją (badawczych, rybackich, hydrograficznych), nasilone fotografowanie terminali i nabrzeży oraz nieautoryzowane loty dronów nad portami i terminalami paliwowymi. Problemem pozostają też zmasowane, nawet codzienne ataki cybernetyczne na systemy operacyjne portów i operatorów terminali — najczęściej DDoS oraz ransomware wymierzone w systemy zarządzania ruchem statków i suwnicami.

„FLOTA CIENI” I ŻEGLUGA

Tankowce tzw. floty cieni charakteryzują się manipulowaniem systemem AIS, przeładunkami „burta w burtę” na otwartym morzu, zatrudnianiem niedoświadczonych załóg oraz niechęcią do współpracy z nawigatorami państw UE. Jednostki te są podejrzewane nie tylko o łamanie reżimu sankcyjnego, lecz także o działalność szpiegowską z użyciem sensorów pokładowych oraz pełnienie funkcji platform startowych dla dronów.

BEZPIECZEŃSTWO ŻEGLUGI POWIETRZNEJ

Rosyjskie zgłuszanie i fałszowanie sygnału GNSS (jamming/spoofing) zmusza samoloty pasażerskie do zwiększania odstępów, co ogranicza przepustowość sektorów lotniczych nad Bałtykiem nawet o 40%. Loty rosyjskich samolotów wojskowych bez włączonych transponderów wymuszają regularne poderwania dyżurnych par myśliwców NATO, obniżając przewidywalność całego systemu ruchu lotniczego w regionie — co przekłada się także na logistykę firm związanych z transportem morskim i lotniczym.

JEDYNE SZKOLENIE, KTÓRE NIE JEST O PRZEPISACH

To szkolenie celowo nie jest zbudowane wokół dyrektyw, checklist compliance ani wymogów regulacyjnych — tego typu materiały łatwo znaleźć gdzie indziej, a przepisy z definicji nigdy nie nadążają za zmieniającymi się zagrożeniami i nigdy ich nie wyprzedzają. Uczymy tego, czego nie da się wyczytać z żadnej ustawy: **aktualnej sytuacji wywiadowczej na Bałtyku, obecnych i prognozowanych wektorów zagrożeń oraz tego, co realnie może się wydarzyć w najbliższej przyszłości** — na podstawie własnych, bieżąco prowadzonych analiz MS&S, a nie ogólnodostępnych komunikatów.

NASZA ANALIZA, NIE TYLKO NASZA OPINIA

Nasz raport wywiadowczy V/2025 o statku „floty cieni” MV SUN stał się głównym studium przypadku raportu „Bezpieczeństwo Bałtyku — od rozpoznania sytuacji do skoordynowanej reakcji” (Fundacja Impulse Institute i ICEYE, wrzesień 2026, Raport 1/2026), przygotowanego przez kmdr dr hab. Rafała Andrzeja Miętkiewicza, prof. AMW, oraz Zuzannę Nowak, przy partnerstwie Polskiej Grupy Zbrojeniowej, ORLEN i Polskiej Agencji Kosmicznej (POLSA). To, czego uczymy na tym szkoleniu, nie jest teorią — to metoda, która już trafiła do jednego z najważniejszych opracowań o bezpieczeństwie Bałtyku w Polsce.

Co obejmuje program

Program łączy szkolenie z zakresu świadomości sytuacyjnej z elementami doradczymi, pozwalającymi realnie wzmocnić odporność firmy na zagrożenia hybrydowe — praktycznie, a nie tylko „na papierze”.

MODUŁ	CO OBEJMUJE
Diagnoza zagrożeń	Analiza podatności firmy na zagrożenia hybrydowe właściwe dla jej segmentu (port, terminal energetyczny, armator, operator MFW) w oparciu o aktualne dane wywiadowcze i incydenty regionalne.
Szkolenie kadry	Budowanie świadomości sytuacyjnej wśród pracowników, kadry bezpieczeństwa i kierowniczej — rozpoznawanie działań wywiadowczych, sabotażowych i socjotechnicznych.
Procedury i reagowanie	Wsparcie w wypracowaniu prostych, praktycznych procedur zgłaszania i reagowania na incydenty — dostosowanych do realiów i skali firmy.
Architektura bezpieczeństwa	Rekomendacje dot. doboru środków ochrony fizycznej, technicznej i proceduralnej, w tym rozwiązań ograniczających ryzyko związane z poddostawcami i kontrahentami.

PROGRAM SZKOLENIA — MODUŁY TEMATYCZNE

- 1

Aktualne zagrożenia dla infrastruktury i żeglugi na Bałtyku
Rosyjska aktywność wywiadowcza i sabotażowa 2022–2026: uszkodzenia kabli i gazociągów, incydenty portowe, przypadki udokumentowane przez MS&S.
- 2

„Flota cieni” i ryzyko poddostawców
Mechanizmy działania floty cieni, ryzyko wynikające z łańcucha kontrahentów i poddostawców (na przykładzie realnych incydentów), rekomendowane środki weryfikacji.
- 3

Werbunek agenturalny i działalność wywiadowcza
Wzorce działania rosyjskiego wywiadu wobec osób zaangażowanych w budowę i obsługę strategicznych inwestycji morskich — rozpoznawanie prób pozyskania.
- 4

Cyberbezpieczeństwo i zakłócenia GNSS
Ataki DDoS i ransomware na systemy operacyjne portów i terminali, zagłuszanie i fałszowanie sygnałów nawigacyjnych — wpływ na operacje i koszty.
- 5

Budowanie świadomości sytuacyjnej i odporności organizacyjnej
Praktyczne wskazówki: jak rozpoznawać wczesne sygnały zagrożeń, budować nawyk zgłaszania incydentów i wzmacniać codzienną czujność zespołu — w oparciu o realne studia przypadków.

Finansowanie ze środków UE — PARP / Baza Usług Rozwojowych

Szkolenie może zostać zrealizowane w ramach **Bazy Usług Rozwojowych (BUR)** — ogólnopolskiego systemu prowadzonego przez Polską Agencję Rozwoju Przedsiębiorczości (PARP), finansowanego z programu Fundusze Europejskie dla Rozwoju Społecznego 2021–2027 oraz szesnastu programów regionalnych. To najprostsza droga dofinansowania tego typu szkolenia dla firm sektora MŚP i ich pracowników.

- Poziom dofinansowania:** 70–80% kosztu usługi — dokładny poziom i zasady ustala właściwy dla siedziby firmy Operator regionalny.
- Kto może skorzystać:** mikro, małe i średnie przedsiębiorstwa oraz ich pracownicy (w tym osoby samozatrudnione); zasady dla dużych podmiotów zależą od konkretnego naboru regionalnego.
- Mechanizm:** firma rejestruje się w BUR (uslugirozwojowe.parp.gov.pl), wybiera właściwego terytorialnie Operatora (Podmiotowy System Finansowania) i zgłasza udział w szkoleniu przed jego rozpoczęciem — wsparcie ma zwykle formę refundacji lub bonu rozwojowego.
- Warunek po naszej stronie:** szkolenie musi być dostępne w katalogu BUR jako zarejestrowana usługa rozwojowa (karta usługi) — MS&S przygotowuje i zgłasza kartę usługi dla tego programu, dopasowaną do wymogów konkretnego naboru.

JAK TO WYGLĄDA W PRAKTYCE

Poradamy dobrać właściwego Operatora regionalnego i przygotowujemy komplet materiałów potrzebnych do zgłoszenia (program, karta usługi, wycena). Warunki naboru (poziom dofinansowania, limity, terminy) różnią się między województwami i zmieniają się z każdą edycją — ostateczne potwierdzenie kwalifikowalności i dostępnej puli środków należy uzyskać u właściwego Operatora PSF przed rozpoczęciem szkolenia.

Warunki realizacji

DLA KOGO

- Operatorzy portów morskich i terminali (LNG, paliwowe, kontenerowe)
- Operatorzy morskich farm wiatrowych i infrastruktury energetycznej
- Armatorzy i zarządcy statków
- Kadra kierownicza i działy bezpieczeństwa/compliance

FORMA

- Szkolenie zamknięte w siedzibie klienta lub w MS&S (Szczecin)
- Łączny wymiar: 5 godzin dydaktycznych (jeden dzień szkoleniowy)
- Każdy uczestnik otrzymuje międzynarodowy certyfikat przeszkolenia z zakresu zagrożeń wywiadowczych i hybrydowych dla podmiotów gospodarki morskiej
- Możliwość rozszerzenia o audyt i rekomendacje wdrożeniowe
- Materiały dostosowane do specyfiki segmentu klienta

ORIENTACYJNA WYCENA

1000 zł / uczestnik (szkolenie otwarte) · wycena indywidualna dla szkolenia zamkniętego i pakietu doradczego

Ostateczna wycena zależy od zakresu (szkolenie / szkolenie + warsztat sytuacyjny / pakiet doradczy) oraz liczby uczestników.

WARIANT DOFINANSOWANIA (BUR)	KOSZT DLA FIRMY / UCZESTNIKA	DOFINANSOWANIE UE
70%	300 zł (wkład własny)	700 zł
80%	200 zł (wkład własny)	800 zł

Wyliczenie orientacyjne, dla ceny bazowej 1000 zł/uczestnika. Faktyczny poziom dofinansowania (70-80%) potwierdza właściwy dla siedziby firmy Operator regionalny BUR.



Prowadzący: Sebastian Kalitowski, kmdr ppor. rez.

Ekspert bezpieczeństwa morskiego, służył w jednostce Formoza jako dowódca grupy specjalnej pływonurków oraz w wywiadzie wojskowym jako oficer operacyjny HUMINT. Od 2007 roku zajmuje się komercyjnym wywiadem morskim i zagrożeniami asymetrycznymi na Bałtyku, ekspert Państwowej Komisji Badania Wypadków Morskich (PKBWM).

To wiedza od oficera operacyjnego wywiadu morskiego, której nie dowiesz się z analiz ani na konferencjach.



MARITIME SAFETY & SECURITY

Wspieramy bezpieczeństwo morskie od 2007 roku

www.maritime-security.eu



„Caret periculo, qui etiam cum est tutus, cavet” Publilius



SAMI

Security Association for
the Maritime Industry
www.seasecurity.org

