AGENCJA BEZPIECZEŃSTWA WEWNĘTRZNEGO

2024–2025

Wybrane aktywności

SPIS TREŚCI

Drodzy Państwo!

Przekazuję Państwu raport podsumowujący wybrane aktywności z ostatnich dwóch lat działalności Agencji Bezpieczeństwa Wewnętrznego. To był wymagający czas. Czas realnych zagrożeń, trudnych decyzji i intensywnej służby na rzecz bezpieczeństwa państwa.

ABW jest największą służbą specjalną w Polsce o najszerszym zakresie odpowiedzialności. Zwalczamy zagrożenia godzące w bezpieczeństwo wewnętrzne i chronimy porządek konstytucyjny. Rozpoznajemy i zwalczamy szpiegostwo, terroryzm, korupcję i proliferację broni masowego rażenia. Odpowiadamy za ochronę informacji niejawnych, bezpieczeństwo systemów teleinformatycznych administracji publicznej i infrastruktury krytycznej oraz obszar kryptografii. Naszą misją jest bezpieczeństwo Rzeczypospolitej.

Obejmując pod koniec 2023 r. kierowanie Agencją, przyjąłem odpowiedzialność za skuteczną realizację tej misji. Wiedziałem, że ABW musi działać zdecydowanie, sprawnie i blisko miejsc, w których pojawiają się zagrożenia. Dlatego w lipcu 2024 r. odtworzyliśmy 10 delegatur ABW. Rozbudowujemy strukturę terenową o wydziały i sekcje zamiejscowe, zwłaszcza na ścianie wschodniej. Działania te przyniosły wymierne efekty. Zwiększyliśmy zdolność do rozpoznawania zagrożeń i szybkiej reakcji.

Minione dwa lata to także większe nakłady budżetowe na rozwój Agencji. Inwestujemy w nowoczesne rozwiązania, ale przede wszystkim w ludzi. To funkcjonariusze i pracownicy są fundamentem skuteczności ABW. Ich doświadczenie, odpowiedzialność i gotowość do działania przesądzają o naszej sile. Dlatego podnoszenie ich kwalifikacji, poprawa warunków pracy oraz zatrzymanie odpływu doświadczonej kadry, a także pozyskiwanie nowych funkcjonariuszy i pracowników to nadal jedne z naszych priorytetów.

Najpoważniejszym wyzwaniem pozostaje aktywność dywersyjna wymierzona w Polskę, inspirowana i organizowana przez rosyjskie służby specjalne. To zagrożenie było (i jest) realne i bezpośrednie. Wymaga pełnej mobilizacji. Dzięki determinacji, profesjonalizmowi i zaangażowaniu funkcjonariuszy ABW udało się zapobiec licznym aktom dywersji wymierzonym w obiekty

wojskowe, infrastrukturę krytyczną, obiekty użyteczności publicznej oraz miejsca związane z organizacją wsparcia dla walczącej Ukrainy. Tam, gdzie zapobieżenie aktom dywersji okazało się niemożliwe, Agencja skutecznie identyfikowała, ścigała oraz doprowadzała do skazania sprawców i organizatorów.

Zwalczanie zagrożeń dywersyjnych nie zwolniło ABW z realizacji zadań związanych z ochroną kontrwywiadowczą przed wrogimi działaniami wywiadowczymi rosyjskich i białoruskich służb specjalnych (oraz ich proxy). Przeciwdziałaliśmy zagrożeniom terrorystycznym i ekstremistycznym. Chroniliśmy ekonomiczne interesy państwa. Wzmacnialiśmy bezpieczeństwo cyberprzestrzeni poprzez ochronę kluczowych systemów teleinformatycznych oraz monitorowanie aktywności wrogich grup odpowiedzialnych za incydenty w tym obszarze.

Przygotowaliśmy raport poświęcony dwóm ostatnim latom naszej działalności. Ma on szczególne znaczenie, ponieważ oznacza powrót ABW do publicznego przedstawiania rezultatów swojej aktywności. Ostatnia tego rodzaju publikacja ukazała się w 2014 r. Uważam, że takie opracowanie jest potrzebne – służy budowaniu wiedzy o zadaniach Agencji, wzmacnia zaufanie do instytucji państwa i pozwala, w zakresie możliwym do ujawnienia, pokazać skalę wyzwań związanych z bezpieczeństwem Rzeczypospolitej. Dlatego traktuję prezentowanie takich sprawozdań jako ważne zobowiązanie i będę dążył do tego, aby stały się one ponownie trwałym elementem komunikacji ABW.

W tym miejscu nie mogę nie wspomnieć o współdziałaniu ABW z partnerskimi zagranicznymi służbami specjalnymi oraz organami i strukturami naszego państwa, których zaangażowanie i odpowiedzialność współtworzyły opisane tutaj efekty. Szczególne podziękowania kieruję do: Kancelarii Prezesa Rady Ministrów, Służby Kontrwywiadu Wojskowego, Agencji Wywiadu, Służby Wywiadu Wojskowego, Centralnego Biura Antykorupcyjnego, Prokuratury, Policji, Straży Granicznej oraz Krajowej Administracji Skarbowej. Dziękuję i zachęcam do lektury.

płk Rafał Syrysko
Szef Agencji Bezpieczeństwa Wewnętrznego

ABW W PIGUŁCE

Chronimy Polskę przed zagrożeniami dla jej bezpieczeństwa

FILARY

- KONTRWYWIAD
- ZWALCZANIE TERRORYZMU
- OCHRONA STRATEGICZNYCH INTERESÓW RP
- CYBERBEZPIECZEŃSTWO
- OCHRONA INFORMACJI NIEJAWNYCH

TARCZA

dla tajemnic państwa

- BEZPIECZEŃSTWO OSOBOWE
- BEZPIECZEŃSTWO PRZEMYSŁOWE
- BEZPIECZEŃSTWO TELEINFORMATYCZNE
- KRAJOWA WŁADZA BEZPIECZEŃSTWA

JAK DZIAŁAMY

DZIAŁANIA OPERACYJNE
pozyskiwanie danych o osobach i zdarzeniach

ŚLEDZTWA
wykrywanie przestępstw i ściganie sprawców

ANALIZA I PROGNOZA
tworzenie raportów wspierających decyzje państwowe

ROLA OPINIODAWCZA

- **KONCESJE:** weryfikacja podmiotów ubiegających się o pozwolenie na produkcję uzbrojenia
- **OBRÓT SPECJALNY:** kontrola handlu bronią, amunicją i technologiami wojskowymi
- **KARTA POLAKA I MIGRACJA:** opiniowanie wniosków o osiedlenie się obcokrajowców

NADZÓR I KONTROLA

- **CYWILNA KONTROLA:** działanie pod nadzorem Premiera lub Ministra Koordynatora Służb Specjalnych
- **MECHANIZMY KONTROLNE:** podleganie kontroli Sejmu RP, sądów, prokuratury, NIK oraz Rzecznika Praw Obywatelskich

ABW W PIGUŁCE

Zadania

Priorytetem działalności Agencji Bezpieczeństwa Wewnętrznego jest ochrona stabilności państwa oraz zapewnienie nienaruszalności terytorium i porządku konstytucyjnego. W dobie ewoluujących zagrożeń asymetrycznych i hybrydowych Agencja pełni rolę kluczowej bariery chroniącej suwerenność RP.

Do priorytetowych obszarów aktywności ABW należy wczesne **rozpoznawanie** oraz **skuteczna neutralizacja zagrożeń** o charakterze wywiadowczym i terrorystycznym. Agencja sprawuje również systemowy **nadzór nad bezpieczeństwem** informacji niejawnych, dbając o ich poufność w obiegu krajowym i międzynarodowym. W odpowiedzi na współczesne wyzwania technologiczne i ekonomiczne ABW aktywnie chroni polską cyberprzestrzeń przed atakami ukierunkowanymi na instytucje publiczne oraz zabezpiecza strategiczne interesy gospodarcze kraju, monitorując sektory kluczowe dla funkcjonowania obywateli. Pełny zakres kompetencji oraz szczegółowy katalog realizowanych zadań definiuje **art. 5 ust. 1 Ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu**.

Uprawnienia

Realizując ustawową misję ochrony bezpieczeństwa wewnętrznego państwa, Agencja wykorzystuje zintegrowany system narzędzi operacyjnych, procesowych i analitycznych. Funkcjonariusze ABW prowadzą **czynności operacyjno-rozpoznawcze** oraz **dochodzeniowo-śledcze**, które uzupełniane są pogłębioną pracą **analityczno-informacyjną**. Istotnym elementem aktywności Agencji jest również udział w procedurach administracyjnych i opiniodawczych oraz sprawowanie nadzoru i wykonywanie **czynności kontrolnych** w ramach systemu ochrony tajemnic państwowych.

Czynności operacyjno-rozpoznawcze

Czynności operacyjno-rozpoznawcze to przewidziane prawem **działania umożliwiające pozyskiwanie danych o osobach, miejscach lub zdarzeniach**.

Uzyskiwane w ten sposób informacje służą do rozpoznawania, wykrywania i neutralizowania zagrożeń dla bezpieczeństwa państwa oraz wykrywania przestępstw i ścigania ich sprawców w ramach postępowań karnych.

W realizacji swoich zadań Agencja Bezpieczeństwa Wewnętrznego przede wszystkim korzysta z pomocy obywateli. Ustawa gwarantuje przy tym pełną ochronę ich tożsamości oraz zapewnia, że dane osób współpracujących z Agencją nigdy nie zostaną ujawnione.

Agencja posiada uprawnienia m.in. do prowadzenia obserwacji osób oraz rejestracji obrazu i dźwięku w miejscach publicznych. W sytuacji, w której inne czynności operacyjno-rozpoznawcze okazują się nieskuteczne, oraz w przypadkach szczególnie groźnych przestępstw Agencja może skorzystać z takich środków specjalnych, jak: kontrola operacyjna (np. kontrola korespondencji, podsłuch), niejawne nabycie lub przejęcie przedmiotów pochodzących z przestępstwa (zakup kontrolowany), niejawne nadzorowanie wytwarzania przedmiotów przestępstwa, ich przemieszczania i przechowywania oraz obrotu nimi (przesyłka niejawnie kontrolowana).

Czynności dochodzeniowo-śledcze

Wyposażeni w szerokie **uprawnienia procesowe** funkcjonariusze Agencji Bezpieczeństwa Wewnętrznego koncentrują się na identyfikacji i zwalczaniu najpoważniejszych przestępstw, które bezpośrednio zagrażają stabilności państwa oraz fundamentom jego porządku konstytucyjnego. Ścigają także sprawców tych przestępstw. W tym zakresie funkcjonariusze ABW mogą wykonywać czynności o charakterze procesowym, do których zalicza się: **zatrzymywanie, przeszukiwanie** i **legitymowanie osób, stosowanie środków przymusu bezpośredniego** i **kontroli osobistej** oraz **przeszukiwanie pomieszczeń**.

Czynności analityczno-informacyjne

Agencja Bezpieczeństwa Wewnętrznego **pozyskuje oraz przetwarza informacje istotne dla ochrony bezpieczeństwa wewnętrznego państwa** i **jego porządku konstytucyjnego**. Przekazuje je Prezydentowi RP, Prezesowi Rady Ministrów, a także – jeśli informacje te dotyczą spraw objętych zakresem działania właściwego ministra – członkom Rady Ministrów.

Opracowania analityczno-informacyjne ABW powstają na podstawie wiedzy uzyskanej z rozpoznania operacyjnego, ustaleń o charakterze dochodzeniowo-śledczym, a także danych pochodzących ze źródeł ogólnodostępnych. Ich celem jest szacowanie ryzyka oraz zapobieganie negatywnym skutkom zjawisk i wydarzeń, co przekłada się na **wspieranie procesów decyzyjnych organów państwa**.

Czynności kontrolne w ramach systemu ochrony informacji niejawnych

Zadania realizowane przez Agencję Bezpieczeństwa Wewnętrznego na podstawie Ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych mają charakter systemowy i w dużej mierze prewencyjny. Ich celem jest **minimalizowanie zagrożeń w obszarze ochrony tajemnic państwowych**. Agencja koncentruje się na budowie szczelnych mechanizmów zapobiegania przypadkom ujawniania informacji niejawnych podmiotom do tego nieuprawnionym, a w sytuacjach naruszenia procedur – na precyzyjnej identyfikacji osób odpowiedzialnych.

Nadzór Agencji Bezpieczeństwa Wewnętrznego nad systemem ochrony informacji niejawnych oparty jest na czterech kluczowych filarach:

- **bezpieczeństwo osobowe** – procesy weryfikacji wiarygodności osób ubiegających się o dostęp do tajemnic prawnie chronionych (badanie rękojmi zachowania tajemnicy) oraz specjalistyczne szkolenia dotyczące tych kwestii;
- **bezpieczeństwo przemysłowe** – procedury weryfikacyjne wobec podmiotów gospodarczych ubiegających się o wydanie świadectwa bezpieczeństwa przemysłowego;
- **bezpieczeństwo fizyczne** – definiowanie standardów ochrony technicznej oraz nadzór nad infrastrukturą służącą do przetwarzania informacji niejawnych;
- **bezpieczeństwo teleinformatyczne** – procesy certyfikacji urządzeń oraz akredytacja systemów przetwarzających dane niejawne.

Szef Agencji Bezpieczeństwa Wewnętrznego pełni funkcję KRAJOWEJ WŁADZY BEZPIECZEŃSTWA w relacjach międzynarodowych. W ramach tych kompetencji odpowiada za implementację ujednoliconych standardów i środków ochrony informacji niejawnych, co gwarantuje spójny poziom bezpieczeństwa danych wymienianych z partnerami zagranicznymi oraz strukturami NATO i UE.

W wymiarze krajowym Agencja sprawuje nadzór nad przestrzeganiem przepisów o ochronie informacji niejawnych we wszystkich cywilnych organach władzy publicznej, jednostkach samorządu terytorialnego i w przedsiębiorstwach. Aktywność ta obejmuje też profesjonalizację kadr poprzez szkolenia pełnomocników ochrony oraz operacyjne reagowanie na incydenty naruszenia bezpieczeństwa.

Procedury opiniodawcze i administracyjne

Na podstawie przepisów odrębnych od ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu na wniosek właściwych organów administracji państwowej oraz indywidualnych podmiotów gospodarczych **ABW uczestniczy w realizacji ponad 40 rodzajów procedur, których celem jest wydanie opinii** dotyczących m.in.:

- udzielenia obcokrajowcom zezwolenia na osiedlenie się na terytorium Polski;
- przyznania koncesji na wytwarzanie broni i amunicji oraz obrót nimi;
- wydania zezwolenia na międzynarodowy obrót sprzętem wojskowym i uzbrojeniem;
- przyznania Karty Polaka.

Nadzór i kontrola

Nadzór nad działalnością ABW sprawuje Prezes Rady Ministrów lub wyznaczony przez niego członek Rady Ministrów – **Minister Koordynator Służb Specjalnych**. **Organem opiniodawczo-doradczym** w sprawach koordynowania działań służb specjalnych w Polsce jest także **Kolegium do Spraw Służb Specjalnych**, działające przy Radzie Ministrów. **Działalność Agencji podlega kontroli** m.in. ze strony Sejmu RP, Prokuratora Generalnego, sądów, Najwyższej Izby Kontroli czy Rzecznika Praw Obywatelskich.

KONTRWYWIAD

Kontrwywiad ABW zidentyfikował i zneutralizował wiele wrogich operacji obcych służb wywiadowczych. Jedynie część informacji o naszej aktywności mogła zostać przekazana opinii publicznej. Dotyczyło to głównie przypadków procesowej waloryzacji efektów intensywnej pracy pionu kontrwywiadu.

Większość naszych przedsięwzięć – z uwagi na tajność realizowanych czynności – została spożytkowana w inny sposób. Skutkiem działań cywilnego kontrwywiadu było m.in. powstrzymanie konkretnych operacji obcych służb wywiadowczych, również z wykorzystaniem trybów administracyjnych (takich jak zakazy wjazdu, wydalenia z terytorium RP, nieudzielanie lub cofnięcie akredytacji przedstawicielom obcych państw), czy przesyłanie informacji i rekomendacji dla władz centralnych RP.

Lata 2024–2025 charakteryzowały się wzmożoną i rosnącą aktywnością przede wszystkim rosyjskich oraz ściśle z nimi kooperujących białoruskich służb specjalnych, a także służb chińskich.

Główne kierunki działań

Federacja Rosyjska

W przypadku Polski **przedsięwzięcia rosyjskich służb specjalnych** koncentrowały się na:

- **dyskredytowaniu RP** na arenie międzynarodowej;
- **podważaniu zaufania** społecznego do państwa i jego instytucji;
- **budowaniu prorosyjskiej narracji**;
- **podsycaniu nastrojów** antysystemowych, antyeuropejskich i antynatowskich;
- **polaryzacji i zastraszaniu** społeczeństwa;
- **wykorzystywaniu** historycznych **antagonizmów** narodowościowych, głównie w relacjach polsko-ukraińskich.

Lata 2024–2025 to **okres intensywnych działań operacyjnych Federacji Rosyjskiej wymierzonych w Polskę** oraz **inne państwa członkowskie UE i NATO**. Długofalowym celem FR pozostaje dezintegracja struktur euroatlantyckich, izolacja wybranych państw oraz doprowadzenie do ich wewnętrznej destabilizacji społeczno-politycznej i gospodarczej.

Od 2022 r. Rosja znajduje się w stanie niewypowiedzianej wojny ze światem Zachodu, a **rosyjski wywiad** coraz częściej stosuje metody charakterystyczne dla wojsk specjalnych (**rozpoznanie i dywersja**). Swoje **przedsięwzięcia realizuje** on **w sposób planowy i skoordynowany**. Jednocześnie służby specjalne FR starają się przenosić na terytorium RP doświadczenia z działań hybrydowych realizowanych przed 2022 r. w Ukrainie, wykorzystując podobny *modus operandi*.

Należy podkreślić, że w minionych dwóch latach wywiad FR prowadził w Polsce rozpoznanie na masową skalę m.in. pod kątem przygotowań do przeprowadzenia aktów dywersji. Celem rosyjskich ataków były nie tylko obiekty wojskowe i infrastruktura krytyczna, ale również sklepy wielkopowierzchniowe i inne miejsca użyteczności publicznej. **Rosyjskie służby specjalne**, eskalując swoje działania, **akceptowały wystąpienie ofiar śmiertelnych**.

Szczególnie widoczne było to w przypadku przedsięwzięć, które mogły doprowadzić do katastrof lotniczych lub kolejowych.

Rosyjskie służby stale modyfikują sposoby działania i rozwijają narzędzia wykorzystywane w operacjach hybrydowych. Do realizacji zadań rozpoznawczych i dywersyjnych wykorzystują osoby, które poszukują łatwego zarobku. Rekrutują je m.in. za pośrednictwem komunikatorów internetowych, zamieszczając ogłoszenia, w których oferują możliwość szybkiego wzbogacenia się w zamian za wykonanie określonych zadań, często pozornie niezwiązanych z działalnością wywiadowczą. Komunikacja pomiędzy zleceniodawcami a zleceniobiorcami odbywa się głównie online, a rozliczenia dokonywane są w kryptowalutach.

W 2025 r. ABW uruchomiła chatbota **@ABW_STOPdywersji_bot** na komunikatorze Telegram. Narzędzie to pozwala na zgłaszanie przypadków nawiązania kontaktów przez obce służby, zwłaszcza ofert dotyczących przeprowadzenia aktów dywersji, a także innych działań, np. rozpoznania obiektów. Chatbot jest obsługiwany w kilku językach: polskim, angielskim, ukraińskim i rosyjskim.

Rosyjskie operacje dywersyjne organizowane są głównie przez wyspecjalizowane komórki GRU i FSB, przy czym GRU dotychczas skupiała się na celach związanych z sektorem wojskowości, natomiast FSB – na pozamilitarnej infrastrukturze krytycznej oraz cywilnych obiektach użyteczności publicznej. Z uwagi na **totalny charakter rosyjskich działań hybrydowych** w latach 2024–2025 podział ten był nieostry. W praktyce obie służby prowadziły operacje w stosunku do obiektów wojskowych i cywilnych, w zależności od posiadanych możliwości operacyjnych.

W latach 2024–2025 kontrwywiad ABW obserwował „profesjonalizację" rosyjskich działań dywersyjnych. O ile jeszcze w 2023 r. służby FR opierały swoje przedsięwzięcia głównie na tzw. jednorazowej agenturze, *ad hoc* pozyskiwanej za pośrednictwem internetu, o tyle w kolejnych latach większy nacisk położono na tworzenie złożonych komórek dywersyjnych (sieciowych), opartych na hermetycznych strukturach przestępczości zorganizowanej. Rosjanie preferują przy tym osoby z doświadczeniem nabytym w strukturach siłowych (np. byłych żołnierzy, milicjantów, najemników z Grupy Wagnera).

Rosyjskie służby zintensyfikowały też prowadzone na terytorium FR szkolenia, których celem jest profesjonalne przygotowanie agentury do działań terrorystycznych (posługiwanie się bronią i materiałami wybuchowymi). W jej skład wchodzą głównie cudzoziemcy.

ABW jest zaangażowana w zabezpieczenie obecności wojsk sojuszniczych na terytorium RP. W lipcu 2024 r. funkcjonariusze Agencji doprowadzili do odzyskania i zwrotu komponentów specjalistycznego systemu łączności NATO, które zostały wcześniej utracone na terytorium państw europejskich. Agencja prowadziła w tej sprawie współpracę m.in. z Biurem Bezpieczeństwa NATO.

W sierpniu 2024 r. doszło do największej wymiany więźniów pomiędzy USA a Rosją od czasu zakończenia Zimnej Wojny. Polska miała swój udział w tej sojuszniczej operacji. ABW oraz inne polskie służby odpowiadały w swoim zakresie za zabezpieczenie jej prawidłowego przebiegu. Uwolniono 16 dziennikarzy i opozycjonistów, a stronie rosyjskiej przekazano 8 osób, wśród których był Pavel Rubtsov vel Pablo Gonzales Yague, zatrzymany w 2022 r. przez ABW oficer GRU operujący w Europie pod przykryciem dziennikarskim.

W latach 2024–2025 służby specjalne FR prowadziły również tradycyjne operacje wywiadowcze, które były neutralizowane przez ABW. Polegały one na pozyskiwaniu źródeł z dostępem do informacji wrażliwych i wpływaniu na procesy decyzyjne organów RP. **Wzmożona czujność funkcjonariuszy i wzrost społecznej świadomości zagrożeń** w Polsce skutecznie ograniczały wywiadowi rosyjskiemu możliwości nawiązywania kontaktów operacyjnych z obywatelami RP, zmuszając rezydentury do ogniskowania swoich zainteresowań na środowiskach rosyjskojęzycznych oraz prorosyjskich.

W obszarze zainteresowania wywiadu Federacji Rosyjskiej pozostawali rosyjscy opozycjoniści (najliczniejsze tego typu środowisko w Europie), w stosunku do których służby tego kraju prowadziły rozpoznanie, operacje wpływu oraz działania kinetyczne. Kontrwywiad ABW, we współpracy z innymi jednostkami, zapobiegł m.in. próbom zamachów na życie i zdrowie ustalonych antyputinowskich aktywistów.

Odpowiedzią na aktywność Rosjan były **decyzje polskich władz o zamknięciu konsulatów generalnych FR** w: **Poznaniu** (listopad 2024 r.), **Krakowie** (czerwiec 2025 r.) i **Gdańsku** (listopad 2025 r.), które zostały podjęte w odpowiedzi na akty dywersji zainspirowane i przeprowadzone na terytorium Polski przez rosyjskie służby specjalne.

Republika Białorusi

Polska pozostaje dla białoruskiego wywiadu niezmiennie priorytetowym celem operacyjnym. W latach 2024–2025 najważniejszym zadaniem służb specjalnych RB była ochrona reżimu, dlatego też ich aktywność koncentrowała się na infiltracji i dezintegracji licznych białoruskich środowisk opozycyjnych funkcjonujących w Polsce.

Białoruski wywiad, zwłaszcza wojskowy, ściśle współpracuje ze swoim odpowiednikiem w Rosji. **Swoista symbioza służb obu państw** uległa dalszemu pogłębieniu w związku z inwazją rosyjską na Ukrainę i ograniczeniem możliwości prowadzenia działań na terytorium RP z klasycznych pozycji przykrycia. Wywiad wojskowy RB również podejmuje intensywne działania rozpoznawcze wobec obiektów Sił Zbrojnych RP i sojuszniczych oraz infrastruktury krytycznej.

Białoruskie służby specjalne prowadzą masowe werbunki na terytorium swojego kraju, a następnie starają się **przenosić swoich agentów** do Polski. Przedsięwzięcia te charakteryzują się różnym stopniem profesjonalizmu. W ostatnich dwóch latach odnotowaliśmy **wzrost opresyjnych działań podejmowanych przez białoruskich oficerów** wobec obywateli RB typowanych do werbunku (szantaż, przymus bezpośredni).

Przejawem wrogiej aktywności służb specjalnych RB są też **próby indagowania i pozyskiwania do współpracy polskich obywateli** regularnie podróżujących na Białoruś i operacyjna **infiltracja mniejszości polskiej** w tym kraju.

Chińska Republika Ludowa

W ostatnich latach Chiny postawiły na ekspansję ekonomiczną w naszym regionie, dążąc do uzyskania coraz większego wpływu na gospodarkę oraz politykę. Polska poddawana jest presji i lobbingowi ze strony Państwa Środka, co realizowane jest również z rosnącym zaangażowaniem wywiadu ChRL.

Chiny charakteryzują się głęboką **synergią polityki, gospodarki, środków masowego przekazu, nauki i służb specjalnych**. Efekt ten był widoczny również w działaniach podejmowanych przez chiński wywiad, który z jednej strony lobbował na rzecz interesów gospodarczych ChRL, w tym konkretnych chińskich podmiotów, z drugiej zaś wykorzystywał te przedsiębiorstwa do prowadzenia działań wywiadowczych.

Wraz ze wzrostem chińskiej aktywności w Polsce służby wywiadowcze tego kraju dążą do **kreowania pozytywnego wizerunku ChRL**, wykorzystując w tym celu rodzime środki masowego przekazu oraz podejmując próby docierania do polskich mass mediów.

W obszarze zainteresowania wywiadu Państwa Środka pozostaje także chińska diaspora. Charakter tego zainteresowania jest dwojaki: pasywny (kontrola potencjalnych działań opozycyjnych w stosunku do chińskich władz) i aktywny (wykorzystanie członków diaspory do działań wywiadowczych).

Wywiad chiński kontynuuje zainicjowane przed laty masowe i prowadzone w skali globalnej **działania werbunkowe z wykorzystaniem internetu**, w tym portali społecznościowych. Także w ostatnich dwóch latach oficerowie wywiadu pod pozorem dobrze płatnych zleceń podejmowali próby pozyskiwania do współpracy ekspertów, naukowców, urzędników oraz osób związanych z resortami siłowymi.

Na szczególną uwagę w kontekście toczącej się wojny w Ukrainie i zagrożeń bezpieczeństwa RP zasługuje pogłębiająca się wieloaspektowa współpraca chińsko-rosyjska, w tym kooperacja w obszarze wojny informacyjnej, a także rosnąca obecność i wpływy polityczno-gospodarcze ChRL na Białorusi.

FAKTY I LICZBY

W latach 2024–2025 Agencja Bezpieczeństwa Wewnętrznego realizowała intensywne działania nakierowane na neutralizację wrogiej aktywności wywiadowczej na terytorium RP. W tym okresie prowadzono łącznie **ponad 60 postępowań przygotowawczych** (śledztw) **dotyczących przestępstwa szpiegostwa**, z czego aż 48 zainicjowano w 2025 r., co dowodzi bezprecedensowego wzrostu zagrożeń oraz wysokiej skuteczności służby. W sprawach prowadzonych od momentu wybuchu pełnoskalowej agresji przeciwko Ukrainie statusem podejrzanego objęte zostało **91 osób**. Skuteczność procesowa Agencji zaowocowała postawieniem **zarzutów** z art. 130 Kodeksu karnego **(szpiegostwo) 82 osobom**, z czego **62 zostały zatrzymane**.

Równolegle ABW zapewniała obsługę informacyjną najwyższych organów państwa, opracowując i dystrybuując w latach 2024–2025 **ponad 430 analiz i informacji** dotyczących aktualnych zagrożeń wywiadowczych.

TARCZA RP

Bezprecedensowa liczba śledztw i zatrzymań

91 PODEJRZANYCH
objętych działaniami od początku pełnoskalowej agresji na Ukrainę

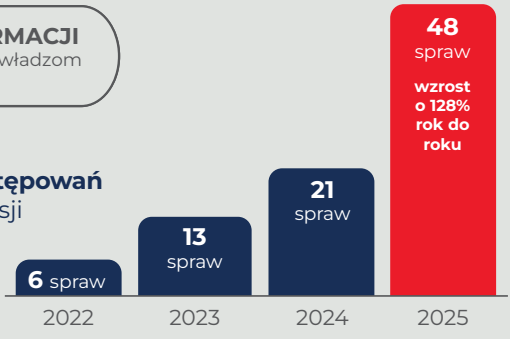
82 OSOBY Z ZARZUTAMI
usłyszały zarzut szpiegostwa (art. 130 kk)

62 ZATRZYMANIA
skuteczna eliminacja agentów z przestrzeni publicznej

430+ ANALIZ I INFORMACJI
przekazanych najwyższym władzom państwa

Począwszy od lat 90. ub. wieku wszczynano **maksymalnie 5 postępowań rocznie**. Od momentu inwazji Rosji na Ukrainę ich liczba systematycznie wzrasta.

W latach 2024–2025 wszczęto **69 śledztw** – to tyle, co łącznie w latach 1991–2023.



Przykładowe rezultaty działań ABW:

- styczeń 2024 r. – **akt oskarżenia** przeciwko ob. RP Januszowi N., uplasowanemu w środowisku polskich i europejskich parlamentarzystów, podejrzanemu o szpiegostwo na rzecz rosyjskich służb specjalnych
- maj 2024 r. – **akt oskarżenia** przeciwko ob. Ukrainy Oleksandrowi D., podejrzanemu m.in. o podżeganie do szpiegostwa
- maj 2024 r. – **zatrzymanie** ob. Polski Kamila K. oraz dwóch ob. Białorusi Stepana K. i Andreia B., dokonujących podpaleń na zlecenie służb specjalnych Federacji Rosyjskiej
- czerwiec 2024 r. – **akt oskarżenia** przeciwko dwóm ob. FR Andreiowi G. i Alexeyowi T., podejrzanym o udział w działalności obcego wywiadu
- listopad 2024 r. – **zatrzymanie** ob. Białorusi Yaraslaua S., podejrzewanego o usiłowanie podpalenia obiektu w Gdańsku
- marzec 2025 r. – **zatrzymanie** ob. Ukrainy Sergieja P., który prowadził rozpoznanie obiektów wojskowych na terytorium Polski
- czerwiec 2025 r. – **akt oskarżenia** w śledztwie ABW przeciwko ob. Ukrainy Kristinie S., której zarzucono planowanie działań sabotażowych i współudział w spowodowaniu bezpośredniego niebezpieczeństwa eksplozji materiałów wybuchowych
- lipiec 2025 r. – **zatrzymanie** Anuara B., który pod przykryciem dyplomatycznym w jednym z państw europejskich prowadził działalność wywiadowczą godzącą w bezpieczeństwo RP i wojskowych struktur sojuszniczych NATO
- sierpień 2025 r. – **akt oskarżenia** w śledztwie ABW przeciwko 6 podejrzanym należącym do zorganizowanej grupy przestępczej, zajmującej się m.in. organizacją i dokonywaniem aktów dywersyjnych na terytorium RP
- wrzesień 2025 r. – **akt oskarżenia** przeciwko Tomaszowi L., któremu zarzucono m.in. szpiegostwo na rzecz rosyjskiego wywiadu cywilnego
- październik 2025 r. – **akt oskarżenia** przeciwko ob. FR Igorovi R. oraz Irinie R., podejrzanym o spowodowanie bezpośredniego niebezpieczeństwa eksplozji materiałów wybuchowych oraz udział w działaniach obcego wywiadu na szkodę RP

ZWALCZANIE TERRORYZMU

W zakresie przeciwdziałania zagrożeniom terrorystycznym w latach 2024–2025 Agencja Bezpieczeństwa Wewnętrznego analizowała ryzyka wynikające m.in. z wojny w Ukrainie, sytuacji na Bliskim Wschodzie oraz działań hybrydowych podejmowanych przez stronę rosyjską i białoruską.

W kwietniu 2024 r. na wniosek Szefa ABW został deportowany z Polski ob. Tadżykistanu – członek organizacji terrorystycznej Państwo Islamskie.

Zadaniem ABW był też **monitoring aktywności organizacji terrorystycznych**, w tym weryfikowanie informacji o działaniach podejmowanych przez sympatyków tego rodzaju ugrupowań. W naszym kraju wielu z nich pochodzi m.in. z Azji Centralnej.

W Polsce obowiązują cztery stopnie alarmowe (ALFA, BRAVO, CHARLIE, DELTA) oraz ich odpowiedniki w cyberprzestrzeni (CRP), wprowadzane w przypadku zagrożeń terrorystycznych. Kluczową rolę w tym procesie odgrywa Szef ABW, który przedstawia stosowne rekomendacje Prezesowi Rady Ministrów.

Od 2022 r. na terytorium Polski oraz w odniesieniu do polskiej infrastruktury energetycznej mieszczącej się poza granicami RP obowiązuje drugi stopień alarmowy BRAVO. Z uwagi na odnotowane przypadki aktów dywersji na infrastrukturę kolejową 19 listopada 2025 r. wprowadzony został trzeci stopień alarmowy CHARLIE dla linii kolejowych zarządzanych przez PKP Polskie Linie Kolejowe S.A. i PKP Linia Hutnicza Szerokotorowa Sp. z o.o.

Główne kierunki działań

Terroryzm islamski

W Polsce ryzyka związane z terroryzmem islamskim – w porównaniu z państwami Europy Zachodniej – nadal utrzymują się na stosunkowo niskim poziomie. Dzięki pracy ABW **ujawniono** jednak pojedyncze **przypadki radykalizacji na gruncie fundamentalizmu islamskiego**, zarówno wśród polskich obywateli, jak i cudzoziemców przebywających w RP.

Znaczące zagrożenia wynikały z **nielegalnego przepływu cudzoziemców** na granicy z Republiką Białorusi i **działań hybrydowych** tego państwa powiązanych z migracją. Taka aktywność ułatwia przedostanie się do Polski obcokrajowców, którzy mogą zagrażać bezpieczeństwu RP. Należy podkreślić, że **ujawniane przypadki nielegalnego wjazdu lub pobytu na terytorium RP dotyczą w istotnej mierze obywateli krajów podwyższonego ryzyka terrorystycznego**.

W listopadzie 2025 r. funkcjonariusze ABW zatrzymali 19-letniego ob. RP w związku z podejrzeniem przygotowywania ataku terrorystycznego na terytorium naszego kraju.

Niepokojącym trendem jest wzrost zainteresowania propagandą terrorystyczną (np. Państwa Islamskiego) **wśród bardzo młodych osób**. W skrajnych przypadkach może to prowadzić do przygotowań do zamachu, napaści fizycznych czy prób konstruowania ładunków wybuchowych.

Ekstremizm

ABW monitoruje aktywność środowisk ekstremistycznych, struktur antysystemowych i grup dopuszczających przemoc jako środek uzyskiwania celów politycznych i neutralizuje związane z tym zagrożenia.

Ruchy skrajne i antypaństwowe

Agencja obserwuje widoczny **wzrost aktywności grup o podłożu skrajnie prawicowym** oraz utrzymującą się **aktywność grup o profilu antypaństwowym/antysystemowym**. W obu przypadkach wykorzystuje się **media społecznościowe** do celów propagandowych i autopromocji. Algorytmy rekomendacji stosowane na tych platformach **sprzyjają polaryzacji i utrwalaniu skrajnych postaw**. Rozpowszechniana **negatywna narracja** uderza m.in. w organy i instytucje państwowe, strategiczne dla Polski sojusze międzynarodowe (jak Unia Europejska czy NATO), cudzoziemców i przeciwników ideologicznych, co ma prowadzić do **pogłębiania** w społeczeństwie **kryzysu zaufania do demokratycznych zasad funkcjonowania państwa**.

Równolegle **wzrasta liczba incydentów z udziałem skrajnie lewicowych środowisk proekologicznych**. W ramach nagłaśniania swoich postulatów ich przedstawiciele dopuszczają się dewastacji mienia oraz zakłócania porządku publicznego i funkcjonowania obiektów infrastruktury krytycznej, w tym odpowiedzialnych za dostawy energii.

W listopadzie 2024 r. funkcjonariusze ABW zatrzymali ob. Niemiec, członka organizacji terrorystycznej zaklasyfikowanej do kategorii zbrojnego ekstremizmu prawicowego o charakterze neonazistowskim.

Polaryzacja społeczeństwa

Rozpowszechnianie skrajnych treści zwiększa podziały w społeczeństwie, co sprawia, że staje się ono mniej odporne na działania destabilizujące. Narracja liderów oraz kluczowych aktywistów ruchów o charakterze antypaństwowym często koreluje z wyrażaniem poparcia dla polityki reżimów Federacji Rosyjskiej i Republiki Białorusi. **Podatność jednostek** na tego typu operacje informacyjno-psychologiczne (**manipulację** i **dezinformację**) ułatwia **radykalizację ich postaw**.

W efekcie część osób zaczyna bardziej ufać narracji i wzorcom działania promowanym przez Rosję i Białoruś, uznając je błędnie za źródło porządku, siły i bezpieczeństwa.

Radykalizacja młodych

W ocenie ABW **radykalizacja osób nieletnich i** młodych **dorosłych** niesie za sobą ryzyko **zachowań przemocowych**. Katalizatorem tego procesu jest ekspozycja na skrajne treści **dystrybuowane w internecie** – ze szczególnym uwzględnieniem **komunikatorów i platform społecznościowych**, w tym forów dla graczy, zapewniających **użytkownikom duży stopień anonimowości**.

W maju 2025 r. funkcjonariusze ABW zatrzymali 17-letniego mieszkańca woj. podkarpackiego, który przygotowywał zamach w celu wsparcia polityki organizacji radykalnych dżihadystów Państwa Islamskiego ISIS.

W kwietniu i czerwcu 2025 r. funkcjonariusze ABW zatrzymali trzech 19-latków z Olsztyna, którzy planowali przeprowadzenie zamachu terrorystycznego m.in. na jedną z lokalnych szkół.

Skrajne zachowania młodzieży rzadko są uwarunkowane konkretną ideologią. Częściej **wynikają z fascynacji przemocą**, w tym masowymi morderstwami oraz brutalną aktywnością struktur terrorystycznych.

Choć większość zradykalizowanych jednostek ogranicza swoją aktywność do sfery wirtualnej, działając w przestrzeni internetowej, ABW ustaliła już pojedyncze przypadki podejmowania bezpośrednich przygotowań do przeprowadzenia ataków terrorystycznych.

Ochrona infrastruktury krytycznej

Agencja Bezpieczeństwa Wewnętrznego realizuje **intensywne działania antyterrorystyczne służące ochronie infrastruktury krytycznej** oraz innych obszarów, obiektów lub urządzeń podlegających obowiązkowej ochronie. Realizując te zadania formułuje i przekazuje **liczne rekomendacje** oraz **zalecenia prewencyjne**. Dotyczą one m.in. ochrony obiektów wchodzących w skład następujących systemów:

- zaopatrzenia w energię, surowce energetyczne i paliwa,
- łączności oraz sieci teleinformatycznych,
- finansów, transportu i ochrony zdrowia.

Proliferacja broni

ABW **prowadzi** ciągłą i wszechstronną **weryfikację sygnałów** dotyczących **prób nielegalnego obrotu bronią, jej komponentami, sprzętem wojskowym** oraz **produktami podwójnego zastosowania, klasyfikowanymi jako towary o znaczeniu strategicznym.** Szczególnym obszarem zainteresowania Agencji pozostaje identyfikacja i przeciwdziałanie ewentualnemu zaangażowaniu podmiotów zarejestrowanych w Polsce w transfery uzbrojenia i technologii o charakterze militarnym na rzecz odbiorców ze strefy wschodniej. Działania te skupiają się w dużej mierze na wykrywaniu powiązań kapitałowo-osobowych, które mogą służyć omijaniu międzynarodowych sankcji oraz nieuprawnionemu wspieraniu struktur powiązanych z tamtejszymi reżimami politycznymi.

Działalność Centrum Antyterrorystycznego

Centrum Antyterrorystyczne ABW od momentu powołania (2008 r.) pełni rolę *fusion centre* – struktury koordynującej obieg informacji o zagrożeniach terrorystycznych. Stanowi efektywną platformę współpracy polskich służb specjalnych i policyjnych, pozwalającą nie tylko na monitorowanie zagrożeń, lecz także umożliwiającą szybkie i skuteczne reagowanie na nie.

Centrum opiera swoją aktywność na współdziałaniu zagranicznych i krajowych służb bezpieczeństwa, a przede wszystkim integrowaniu wiedzy, jaką dysponują. Funkcjonariusze, żołnierze i pracownicy polskich podmiotów przeciwdziałających zagrożeniom terrorystycznym (Policji, SG, SOP, AW, SWW, SKW, KAS, ABW) pełnią służbę całodobowo przez 7 dni w tygodniu, na bieżąco weryfikując otrzymywane informacje. Możliwość korzystania przez nich z baz danych macierzystych służb przyspiesza proces pozyskiwania informacji, pozwalając zarazem na ich doraźną weryfikację i rozszerzenie.

FAKTY I LICZBY

W latach 2024–2025 Agencja Bezpieczeństwa Wewnętrznego realizowała intensywne działania nakierowane na neutralizację zagrożeń terrorystycznych oraz wzmacnianie odporności państwa. W tym obszarze prowadziła łącznie **19 postępowań przygotowawczych** (śledztw), przy czym liczba tych działań wzrosła **w 2025 r.**, kiedy to zainicjowano **7 nowych** spraw.

Kluczowym elementem antyterrorystycznej ochrony kraju była sprawna wymiana informacji operacyjnych – CAT ABW przekazała do podmiotów systemu ochrony antyterrorystycznej **blisko 700 raportów operacyjnych zawierających sygnały o potencjalnych zagrożeniach**.

ABW poddała weryfikacji i zaopiniowała **ok. 5,5 tys. wniosków dotyczących wydania zezwoleń** na międzynarodowy obrót towarami, technologiami i usługami o znaczeniu strategicznym.

Agencja sporządziła **ponad 880 opinii związanych z procedurami koncesyjnymi** podmiotów prowadzących działalność w obszarze wytwarzania materiałów wybuchowych, broni, amunicji, wyrobów i technologii o przeznaczeniu wojskowym lub policyjnym, a także handlu nimi.

Równolegle ABW pełniła funkcję eksperckiego zaplecza dla decydentów. W latach 2024–2025 przygotowała i przekazała uprawnionym odbiorcom **178 opracowań analitycznych** dotyczących zagrożeń terrorystycznych.

Przykładowe rezultaty działań ABW:

- luty 2024 r. – **zatrzymanie** ob. FR Alviego A., powiązanego z Państwem Islamskim
- kwiecień 2024 r. – **wyrok skazujący** na 2 lata więzienia dla obywatela RP Rafała K., członka organizacji terrorystycznej, który planował przeprowadzenie zamachu terrorystycznego
- lipiec 2025 r. – **przedstawienie** ob. Kolumbii Andrésowi C. **zarzutów** dotyczących dokonania na terytorium Polski czynu o charakterze terrorystycznym
- listopad 2025 r. – **zatrzymanie** obywatela RP Mateusza W., podejrzewanego o przygotowania do zamachu, w którym planował wykorzystać materiały wybuchowe

TARCZA RP

Aktywne przeciwdziałanie
i osłona antyterrorystyczna

IDENTYFIKUJEMY

blisko **700** raportów operacyjnych o potencjalnych zagrożeniach przekazanych do służb i instytucji

ŚCIGAMY

19 prowadzonych postępowań karnych w sprawach o terroryzm (w tym **7** wszczętych w 2025 r.)

OSTRZEGAMY

178 specjalistycznych opracowań o wektorach zagrożeń terrorystycznych trafiło do decydentów

CHRONIMY

skuteczne neutralizowanie ryzyk i osłona antyterrorystyczna kraju

WERYFIKUJEMY

ok. **5,5 tys.** wniosków dotyczących wydania zezwoleń na międzynarodowy obrót towarami, technologiami i usługami

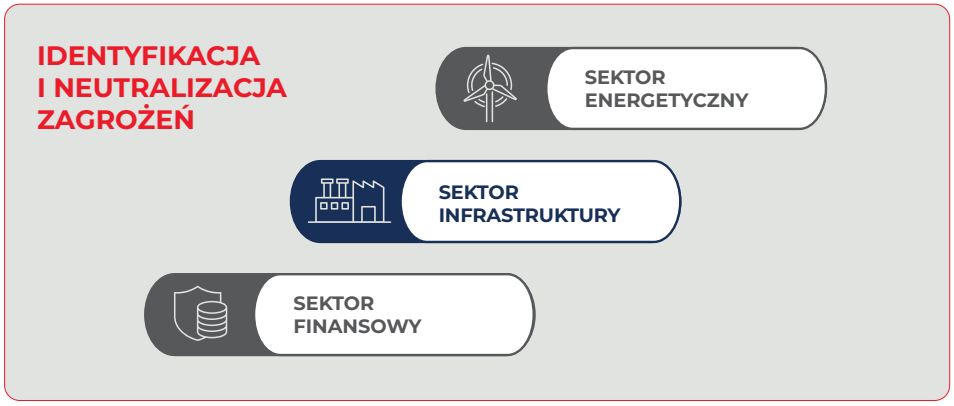
OPINIUJEMY

ponad **880** opinii związanych z procedurami koncesyjnymi

OCHRONA STRATEGICZNYCH INTERESÓW GOSPODARCZYCH

ABW w ramach realizacji ustawowych zadań związanych z ochroną ekonomicznych interesów państwa rozpoznaje i przeciwdziała szerokiemu spektrum zagrożeń. Aktywność w tym zakresie skupia się na analizie ryzyk wynikających z sytuacji geopolitycznej, która oddziałuje wielopłaszczyznowo na polską gospodarkę. W tym obszarze Agencja prowadzi działania ukierunkowane na **identyfikację i neutralizację zagrożeń dla funkcjonowania kluczowych sektorów gospodarki**, zwłaszcza **energetycznego**, **infrastrukturalnego** oraz **finansowego**. Rozpoznaniem objęta jest w szczególności działalność istotnych podmiotów kontrolowanych przez Skarb Państwa, m.in. w zakresie potencjalnych nieprawidłowości w obszarze zarządczym i operacyjnym. Agencja monitoruje także realizację strategicznych dla interesów RP projektów rozwojowych. Aktywność ta prowadzona jest wielokierunkowo i ma na celu ograniczenie możliwych ryzyk związanych m.in. z próbami destabilizacji tych przedsięwzięć, zwłaszcza przez aktorów zewnętrznych, jak również rozpoznawanie ewentualnych nieprawidłowości w ich realizacji, w tym pod kątem wiarygodności kontrahentów i wykonawców.

Główne kierunki działań



Strategiczne sektory gospodarki

Sektor energetyczny

W latach 2024–2025 aktywność Agencji związana z sektorem energetycznym koncentrowała się na ochronie kluczowych przedsięwzięć, których realizacja istotnie wzmocni bezpieczeństwo RP. Szczególnym zainteresowaniem objęta została **budowa pierwszej polskiej elektrowni jądrowej** oraz towarzyszących jej inwestycji, w tym rozbudowa sieci przesyłowej energii elektrycznej umożliwiająca jej wprowadzenie do krajowego systemu elektroenergetycznego. Monitoringiem objęto też **projekty związane z rozbudową infrastruktury LNG w Świnoujściu, budową morskich farm wiatrowych, terminala FSRU w Gdańsku oraz innych źródeł wytwórczych**, zapewniających zbilansowanie systemu energetycznego RP.

W latach 2024–2025 Agencja realizowała wiele działań procesowych w ramach śledztw dotyczących nieprawidłowości w koncernie Orlen S.A. W ich toku prowadzono zarówno czynności wobec wskazanych przez prokuratora osób oraz podmiotów, jak również działania ukierunkowane na zebranie dodatkowego materiału dowodowego.

Sektor infrastruktury

W obszarze infrastruktury Agencja monitorowała m.in. przebieg procesów inwestycyjnych, w tym zwłaszcza przygotowań do budowy Portu Polska, który będzie hubem transportowym, integrującym lotnictwo, kolej oraz drogi. Aktywność ABW koncentrowała się także na przedsięwzięciach rozwojowych oraz restrukturyzacyjnych spółek Skarbu Państwa w tym obszarze. Dodatkowo Agencja identyfikowała próby zaangażowania kapitału zagranicznego w polskie spółki sektorów lotniczego, kolejowego i IT oraz ograniczała wynikające z tego ryzyka. ABW definiowała też zagrożenia dla obiektów infrastruktury strategicznej w celu zapewnienia stabilnego funkcjonowania państwa, jego gospodarki i bezpieczeństwa narodowego.

Sektor finansowy

Istotnym obszarem aktywności Agencji w latach 2024–2025 było również zwalczanie przestępstw, których skutki odczuwalne były w postaci znacznego uszczuplenia wpływów budżetowych, a także szkód majątkowych w mieniu Skarbu Państwa. W tym zakresie ABW realizowała rozpoznanie grup przestępczych zajmujących się m.in. rzeczywistym lub fikcyjnym obrotem towarowym bez uiszczania należności podatkowych. Agencja koncentrowała się również na wykrywaniu i ujawnianiu nieprawidłowości w udzielaniu dotacji z programów celowych oraz gospodarowaniu środkami finansowymi otrzymywanymi z UE, w tym identyfikacji mechanizmów przestępstw popełnianych w trakcie przyznawania, wydatkowania oraz rozliczania funduszy.

ABW realizowała powierzone przez Prokuraturę czynności w śledztwie dotyczącym nieprawidłowości w wydatkowaniu środków finansowych z Funduszu Sprawiedliwości. Zatrzymane przez funkcjonariuszy osoby usłyszały zarzuty przekroczenia uprawnień, niedopełnienia obowiązków, przywłaszczenia mienia wielkiej wartości oraz prania pieniędzy.

ABW zwalcza także działalność międzynarodowych zorganizowanych struktur przestępczych (w szczególności grup euroazjatyckich i rosyjskojęzycznych) w kontekście generowanych przez nie zagrożeń dla bezpieczeństwa

fiskalnego i finansowego państwa oraz innych sektorów gospodarki. Opisywane struktury przestępcze stanowią jedno z kluczowych narzędzi rosyjskich służb specjalnych do destabilizacji sytuacji wewnętrznej w Polsce oraz UE, w tym istotne wsparcie działań hybrydowych FR. Równolegle ww. grupy mogą być wykorzystywane do wypracowywania i obsługi nowych dróg obchodzenia międzynarodowych sankcji oraz udostępniania kanałów transferowania środków pieniężnych do FR.

Nowe technologie – kryptoaktywa

Wiele wyzwań dla ochrony przez ABW bezpieczeństwa ekonomicznego państwa w ostatnim okresie generują także **nowe technologie, w tym związane z kryptoaktywami**. Dynamiczny rozwój rynku walut wirtualnych sprawił, że przestały one pełnić wyłącznie funkcję nowoczesnych instrumentów płatniczo-inwestycyjnych. Aktualnie stanowią zaawansowane narzędzie w działalności przestępczej, uderzającej bezpośrednio w interesy gospodarcze oraz bezpieczeństwo publiczne kraju. Wykorzystanie kryptoaktywów do celów nielegalnych obejmuje szerokie spektrum czynów zabronionych, wśród których kluczowe znaczenie mają transfer oraz pranie kapitału pochodzącego z przestępstw, oszustwa i wyłudzenia o charakterze masowym (fałszywe platformy inwestycyjne, piramidy finansowe), korupcja, finansowanie terroryzmu.

ABW zidentyfikowała proceder wykorzystywania technologii blockchain przez rosyjskie służby specjalne. Pozwala ona obcym ośrodkom wywiadowczym na omijanie międzynarodowych reżimów sankcyjnych oraz zapewnia anonimowe finansowanie wrogich operacji dywersyjno-sabotażowych na terytorium państw NATO. Z rozpoznania Agencji wynika także, że rozliczenia w tych aktywach wykorzystywane są w procederze sterowanej, nielegalnej migracji na granicy RB–RP.

Osłona antykorupcyjna

Do priorytetowych działań ABW należy również przeciwdziałanie zagrożeniom w ramach tzw. osłony antykorupcyjnej. Jej celem jest **identyfikacja i neutralizacja nieprawidłowości przy realizacji przedsięwzięć o kluczowym**

znaczeniu dla bezpieczeństwa i interesów ekonomicznych państwa. Agencja zgodnie z Wytycznymi Prezesa Rady Ministrów w sprawie funkcjonowania osłony antykorupcyjnej monitoruje projekty z obszaru energetyki, sektora paliwowego, sektora finansowego oraz infrastruktury drogowej, kolejowej i lotniczej. W ramach realizacji osłony antykorupcyjnej ABW analizuje ryzyka korupcyjne, sprawdza osoby i podmioty w zakresie ich wiarygodności, jak również monitoruje procedury w obszarze ewentualnych zmów cenowych czy konfliktów interesów.

Na **koniec 2024 r.** osłoną antykorupcyjną ABW objęte były **23 przedsięwzięcia**, natomiast na **koniec 2025 r.** Agencja osłaniała już **36 przedsięwzięć**.

Sankcje gospodarcze

ABW odgrywa także istotną rolę w realizowaniu krajowej i międzynarodowej polityki sankcyjnej związanej z konfliktem zbrojnym w Ukrainie. Jednym z priorytetowych zadań Agencji w tym obszarze jest identyfikowanie podmiotów, które dysponują środkami finansowymi, funduszami oraz zasobami gospodarczymi wspierającymi agresję Federacji Rosyjskiej bądź naruszają prawa człowieka lub stosują represje wobec społeczeństwa obywatelskiego w Rosji i na Białorusi. Działania w tym zakresie realizowane są na podstawie Ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (tzw. ustawy sankcyjnej). W ostatnich dwóch latach ABW koncentrowała się ponadto na rozpoznawaniu struktur zaangażowanych w omijanie międzynarodowych oraz krajowych sankcji (zarówno w wymiarze sektorowym, jak i indywidualnym).

W latach 2024–2025 Agencja skierowała do Ministra Spraw Wewnętrznych i Administracji **wnioski o objęcie środkami ograniczającymi** wobec **kolejnych 15 podmiotów gospodarczych**.

FAKTY I LICZBY

W obszarze zwalczania zagrożeń godzących w kluczowe interesy gospodarcze Rzeczypospolitej Polskiej Agencja Bezpieczeństwa Wewnętrznego prowadziła łącznie **180 śledztw**, z czego **50 wszczęto w 2025 r.**

W latach 2024–2025 **ABW weryfikowała kandydatów przewidzianych do objęcia najwyższych stanowisk w administracji publicznej oraz spółkach Skarbu Państwa**. W ramach tych procedur osłonowo-weryfikacyjnych **sprawdzono 820 osób**.

W latach 2024–2025 ABW przygotowała i przekazała uprawnionym odbiorcom **446 opracowań analitycznych, informacji i opinii** dotyczących ochrony strategicznych interesów gospodarczych Polski.

TARCZA RP

Osłona ekonomiczna
i kadrowa państwa

ŚCIGAMY

dynamiczny wzrost aktywności śledczej w 2025 r. jako odpowiedź na współczesne zagrożenia ekonomiczne

WERYFIKUJEMY

820 sprawdzonych kandydatów na najwyższe stanowiska państwowe oraz funkcje w spółkach Skarbu Państwa

CHRONIMY

skuteczna eliminacja ryzyk personalnych i operacyjnych w strategicznych sektorach gospodarki

REAGUJEMY

180 postępowań przygotowawczych w sprawach o kluczowym znaczeniu gospodarczym (w tym **50** wszczętych w 2025 r.)

Przykładowe rezultaty działań ABW:

- marzec–lipiec 2024 r. – **realizacja czynności procesowych** w siedzibie Orlen S.A. w Płocku, które umożliwiły zgromadzenie materiału dowodowego dot. ustalania cen paliw oraz interwencyjnego wytłaczania przez spółkę zapasów oleju napędowego i benzyny. Działania osób odpowiedzialnych doprowadziły do powstania szkody majątkowej w spółce w wysokości **ok. 4 mld zł**
- październik 2024 r. – **zatrzymanie** 5 osób w związku z nieprawidłowościami w wydatkowaniu środków z Funduszu Sprawiedliwości. Przedstawiono im zarzuty dotyczące nadużycia funkcji, przywłaszczenia i prania pieniędzy. Łączna skala strat Skarbu Państwa szacowana jest na co najmniej **kilkaset mln zł**
- listopad 2024 r. – **zatrzymanie** ob. Niemiec Marka A., któremu zostały przedstawione zarzuty dotyczące wywozu na terytorium Federacji Rosyjskiej towarów podwójnego zastosowania
- kwiecień 2025 r. – wspólne działania funkcjonariuszy ABW, KAS, CBŚP i CBZC doprowadziły do **zatrzymania** 4 osób – członków zorganizowanej grupy przestępczej, która trudniła się wyłudzaniem podatku VAT, doprowadzając do powstania po stronie Skarbu Państwa strat szacowanych na **ponad 38 mln zł**
- czerwiec 2025 r. – **zatrzymanie** Michała R., byłego członka zarządu Orlen S.A. odpowiedzialnego za nadzór nad spółką Orlen Trading Switzerland GmbH z siedzibą w Szwajcarii, w związku z działaniem na szkodę spółki w celu osiągnięcia korzyści majątkowej poprzez niewłaściwy nadzór nad środkami finansowymi przekazywanymi do OTS oraz zawieranie kontraktów na dostawę ropy. Śledczy szacują stratę na **ok. 1,5 mld zł**
- czerwiec 2025 r. – **zatrzymanie** dwojga ob. RP, Marka D.T. i Magdaleny D.T., poszukiwanych europejskim nakazem aresztowania w związku z wyrządzeniem szkody w mieniu PGE GiEK S.A. w wysokości blisko **21 mln zł**
- wrzesień 2025 r. – wspólne działania ABW i CBŚP doprowadziły do **zatrzymania** liderów zorganizowanej grupy przestępczej o zasięgu międzynarodowym, Marka M. ps. „Oczko", Daniela S. oraz Marcina K. Grupa zajmowała się m.in. przemytem narkotyków z Europy Zachodniej do Polski oraz nielegalnym wytwarzaniem i wprowadzaniem do obrotu wyrobów tytoniowych na terytorium RP. Straty Skarbu Państwa oszacowano na kwotę nie mniejszą niż **9 mln zł**
- grudzień 2025 r. – **akt oskarżenia** m.in. przeciwko Joannie S., twórczyni piramidy finansowej, reprezentującej Galleri New Form. Zarzuty dotyczą doprowadzenia osób pokrzywdzonych do niekorzystnego rozporządzenia mieniem w łącznej kwocie nie mniejszej niż **300 mln zł**

OCHRONA CYBERPRZESTRZENI RP

Agencja Bezpieczeństwa Wewnętrznego realizuje **intensywne działania operacyjno-techniczne nakierowane na neutralizację zagrożeń cyberprzestrzeni Rzeczypospolitej Polskiej**. Przedsięwzięcia te stanowią fundament osłony systemów teleinformatycznych administracji państwowej, zabezpieczenia integralności procesów wyborczych, a także ochrony innych podmiotów o krytycznym znaczeniu dla ciągłości funkcjonowania państwa.

Kluczowym ogniwem w krajowym systemie cyberbezpieczeństwa pozostaje funkcjonujący w strukturach ABW **Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego – CSIRT GOV**. Na poziomie krajowym odpowiada on za koordynację procesów ochronnych dedykowanych organom administracji publicznej oraz operatorom infrastruktury krytycznej.

W spektrum statutowych zadań zespołu mieści się **rozpoznawanie zagrożeń**, **reagowanie na ataki hakerskie**, eksperckie **wspieranie podmiotów** w obsłudze incydentów oraz **wdrażanie** wielopoziomowych **działań prewencyjnych i profilaktycznych**.

Bezpieczeństwo cyberprzestrzeni RP

Agencja Bezpieczeństwa Wewnętrznego odnotowuje **podwyższony poziom zagrożenia w polskiej cyberprzestrzeni**, co znajduje bezpośrednie odzwierciedlenie w utrzymywaniu podwyższonych **stopni alarmowych CRP** na terytorium całego kraju. Polska – z uwagi na swoje strategiczne położenie oraz status członka NATO i Unii Europejskiej – jest jednym z kluczowych celów dla cyberofensywnych grup powiązanych z obcymi ośrodkami rządowymi (tzw. *state-sponsored*), a także ugrupowań cyberprzestępczych oraz struktur haktywistycznych. Współcześnie **ataki teleinformatyczne** utraciły swój incydentalny charakter, stając się integralnym **elementem** wielowymiarowych **działań hybrydowych**. Ich **celem** jest nie tylko **kradzież danych**. Coraz częściej są one ukierunkowane na realizację agresywnych **kampanii dezinformacyjnych** oraz **destabilizację** struktur i procesów decyzyjnych **państwa**.

Klasycznym przykładem działań hybrydowych było przejęcie w maju 2024 r. konta pracowniczego w Polskiej Agencji Prasowej. Incydent ten posłużył zewnętrznym aktorom do opublikowania fałszywej depeszy informującej o rzekomym ogłoszeniu w Polsce mobilizacji. Autorzy fałszywego komunikatu sprecyzowali, że powołaniami do wojska zostaną objęte konkretne grupy zawodowe, m.in. górnicy oraz kierowcy kategorii C i D.

Dezinformacja

Kampanie dezinformacyjne prowadzone przez aktorów państwowych i pozapaństwowych **stanowią jedno z największych wyzwań bezpieczeństwa wewnętrznego**, zwłaszcza w kontekście rosyjskich działań hybrydowych.

Obecnie niemal **każdy wrażliwy społecznie temat** lub wydarzenie jest natychmiast **przedmiotem aktywności** tzw. internetowych **trolli** i **botów**, które rozpowszechniają fałszywe narracje. Działania te ukierunkowane są przede wszystkim na **zwiększenie polaryzacji społeczeństwa** oraz **podważenie zaufania polskich obywateli do instytucji państwowych i struktur międzynarodowych**.

Kampanie dezinformacyjne o charakterze wrogim są coraz częściej wspierane przez **działania grup cyberofensywnych**.

Kampanie socjotechniczne

Kampanie socjotechniczne pozostają jednym z najbardziej powszechnych i skutecznych narzędzi w arsenale cyberprzestępców. Trzeba zaznaczyć, że przyjmują one coraz bardziej wyrafinowane formy. Atakujący wciąż rozwijają i modyfikują klasyczne metody phishingowe. Obok tradycyjnych wiadomości e-mail z **niebezpiecznymi linkami** coraz częściej stosowane są **złośliwe kody QR**. Aby skutecznie ominąć czujność odbiorców, agresorzy podszywają się pod zaufane podmioty komercyjne oraz instytucje państwowe. Szczególnie niebezpiecznym zjawiskiem jest wykorzystywanie w tym celu **przejętych skrzynek pocztowych** administracji centralnej i lokalnej, a także **wizerunków firm, organizacji i instytucji publicznych**. Tego typu działania mają w efekcie wywoływać u odbiorców wiadomości fałszywe poczucie bezpieczeństwa.

Z punktu widzenia analizy technicznej istotnym wyzwaniem dla systemów bezpieczeństwa jest zmiana sposobu dystrybucji złośliwego oprogramowania. Sprawcy masowo migrują swoje zasoby (fałszywe formularze, zainfekowane dokumenty) do legalnie działających, publicznych chmur obliczeniowych. Taki model działania pozwala im na ukrycie ruchu wewnątrz zaufanych domen, co drastycznie obniża skuteczność standardowych reguł blokowania i systemów wczesnego ostrzegania.

QR phishing

Zagrożenie typu **quishing** (QR phishing) bazuje na popularności i coraz większej powszechności kodów QR oraz zaufaniu, jakim użytkownicy obdarzają tę technologię. Z perspektywy cyberbezpieczeństwa kluczową cechą quishingu jest zdolność do **ukrywania niebezpiecznego hiperłącza** przed automatycznymi systemami zabezpieczeń, skanującymi treść wiadomości. Pozwala to agresorom na skuteczne dostarczenie złośliwego ładunku z pominięciem mechanizmów bezpieczeństwa. Dystrybucja złośliwych kodów QR odbywa się dwutorowo:

- **w domenie cyfrowej** – wiadomości najczęściej trafiają do ofiar ataków poprzez masową lub celowaną wysyłkę za pośrednictwem komunikatorów internetowych i portali społecznościowych;
- **w przestrzeni zurbanizowanej** – poprzez fizyczne naklejanie fałszywych kodów QR w miejscach ogólnodostępnych, na legalnie istniejącej infrastrukturze miejskiej (np. parkometrach, biletomatach).

Ten hybrydowy model działania drastycznie zwiększa prawdopodobieństwo uśpienia czujności ofiary.

Ataki na infrastrukturę

Agencja Bezpieczeństwa Wewnętrznego odnotowuje stały **wzrost liczby ataków teleinformatycznych wymierzonych w łańcuchy dostaw**, **obiekty infrastruktury krytycznej** oraz **przemysłowe systemy sterowania infrastrukturą komunalną** (m.in. w oczyszczalniach ścieków, zakładach uzdatniania wody czy spalarniach odpadów). Poprzez uderzenia wymierzone w kontrahentów cyberprzestępcy starają się zdobyć dane dotyczące umów, dokumentację projektową oraz poświadczenia uwierzytelniające, umożliwiające dostęp do systemów klientów końcowych. Pozyskane w ten sposób zasoby pośrednio lub bezpośrednio służą do budowy bazy wiedzy o architekturze i funkcjonowaniu kluczowych obiektów na terytorium kraju.

Aktywność wymierzona w infrastrukturę komunalną była szczególnie intensywnie prowadzona przez grupy haktywistyczne. Podejmując próby ingerencji w działanie tego typu obiektów, wykorzystywano rażącą podatność w obszarze niewłaściwej polityki haseł oraz niezabezpieczone panele zarządzania urządzeniami, dostępne bezpośrednio w publicznej sieci internet.

W 2025 r. odnotowano m.in. incydenty naruszenia bezpieczeństwa **stacji uzdatniania wody** w miejscowościach: Jabłonna Lacka, Szczytno, Małdyty, Tolkmicko, Sierakowo. Atakujący, uzyskując w niektórych przypadkach dostęp do przemysłowych systemów sterowania, mieli **możliwość zmiany parametrów technicznych urządzeń**, co stwarzało bezpośrednie ryzyko dla ciągłości ich funkcjonowania, a co za tym idzie – dla procesów zaopatrzenia ludności.

Grupy APT

Wraz z obserwowanym wzrostem ogólnej liczby ataków teleinformatycznych ABW odnotowuje systematyczną profesjonalizację **działań grup APT** (ang. *advanced persistent threat*). Są to sponsorowani przez rządy wrogich państw, wysoce wyspecjalizowani aktorzy realizujący zaawansowane i długofalowe operacje szpiegowskie oraz dywersyjne. Wśród ugrupowań wykazujących szczególną aktywność w zakresie ataków w cyberprzestrzeni możemy wskazać m.in. rosyjskie APT28 (Fancy Bear), APT29 (Midnight Blizzard) oraz powiązaną z białoruskim aparatem państwowym grupę UNC1151. Są to zespoły specjalistów działające na zlecenie podmiotów państwowych (w tym głównie wschodnich służb specjalnych), których nadrzędnym celem pozostaje **pozyskiwanie strategicznych danych wywiadowczych, cyberszpiegostwo, prowadzenie operacji wpływu oraz realizacja wieloobszarowych kampanii dezinformacyjnych.**

W sierpniu 2024 r. Polska Agencja Antydopingowa (POLADA) padła ofiarą poważnego ataku hakerskiego, w wyniku którego skradziono i opublikowano w sieci dane wrażliwe, w tym dokumenty medyczne oraz wyniki kontroli antydopingowych polskich sportowców.

Hakerzy stale doskonalą i modyfikują metody prowadzenia ataków, dążąc do niezauważalnej eksfiltracji danych z pominięciem mechanizmów detekcji i obrony stosowanych na urządzeniach ofiary (takich jak systemy antywirusowe). Wykorzystują przy tym najczęściej luki oraz podatności w użytkowanym oprogramowaniu i sprzęcie.

System wczesnego ostrzegania ARAKIS GOV

Dokonana przez ABW analiza danych pochodzących z funkcjonującego w Polsce systemu wczesnego ostrzegania o zagrożeniach w internecie ARAKIS GOV dowodzi, że **lata 2024–2025** charakteryzowały się bezprecedensową **intensyfikacją działań obronnych w cyberprzestrzeni RP.**

Agresorzy nie tylko operują zaawansowanymi technologicznie narzędziami, lecz przede wszystkim **celują bezpośrednio w najsłabsze ogniwo systemów bezpieczeństwa – czynnik ludzki (użytkowników)**. W obliczu tak dynamicznej ewolucji zagrożeń kluczowym zagadnieniem ochrony polskiej cyberprzestrzeni stało się wdrażanie i stosowanie wielowarstwowej strategii cyberbezpieczeństwa. Obejmuje ona zarówno permanentny monitoring infrastruktury, cykliczne procedury audytowe, jak i systemową edukację użytkowników.

W omawianym okresie Agencja zidentyfikowała **w cyberprzestrzeni wzmożoną aktywność** obcych ośrodków wywiadowczych, ze szczególnym uwzględnieniem **służb specjalnych Federacji Rosyjskiej**.

Skalę działań odzwierciedlają statystyki prowadzonego przez Szefa ABW zespołu CSIRT GOV, który odnotował **ponad 40 tys. zgłoszeń** o potencjalnych incydentach teleinformatycznych. Ponadto w 2025 r. system ARAKIS GOV wykazał **18-procentowy wzrost liczby zdarzeń w ujęciu rok do roku**, co przełożyło się na rekordową liczbę **ponad 5,5 mln alarmów bezpieczeństwa**.

ARAKIS GOV to system wczesnego ostrzegania o zagrożeniach w internecie, który powstał na potrzeby wsparcia ochrony zasobów teleinformatycznych podmiotów administracji państwowej oraz operatorów infrastruktury krytycznej. System ten agreguje i przetwarza dane noszące znamiona potencjalnego ataku bądź złośliwego ruchu sieciowego, które koreluje z danymi już posiadanymi celem identyfikacji takich wskaźników, jak m.in. unikalne adresy IP, porty, sygnatury czasowe oraz typy i metodologie zagrożeń.

TARCZA RP

Cyberbezpieczeństwo
i walka z dezinformacją

KAMPANIE DEZINFORMACYJNE

Rozpowszechnianie fałszywych narracji
Cel: polaryzacja i podważanie zaufania do instytucji

KAMPANIE SOCJOTECHNICZNE

Stosowanie phishingu, quishingu
Cel: wyłudzenie poufnych informacji

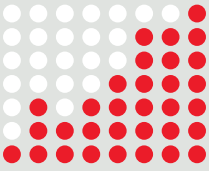
ARCHITEKTURA ZAGROŻEŃ

ATAKI NA STACJE UZDATNIANIA WODY

Cel: zakłócanie codziennego funkcjonowania państwa i wywoływanie poczucia destabilizacji

GRUPY APT

Celowane ataki grup rządowych (APT28, APT29, UNC1151)
Cel: szpiegostwo i eksfiltracja danych



ALERT!!!

Utrzymuje się **podwyższony stopień alarmowy CRP**:

- **ponad 40 tys.** zgłoszeń o potencjalnych incydentach
- **18-procentowy wzrost** liczby zdarzeń (rok do roku)
- rekordowa liczba **ponad 5,5 mln alarmów**

OCHRONA INFORMACJI NIEJAWNYCH

Agencja Bezpieczeństwa Wewnętrznego sprawuje **nadzór nad funkcjonowaniem systemu ochrony informacji niejawnych**. Skuteczność i szczelność tego mechanizmu determinowana jest ścisłą synergią rozwiązań organizacyjnych, technicznych i prawnych. Istotnym filarem jego stabilności pozostaje także sprawna koordynacja działań pomiędzy wyspecjalizowanymi instytucjami odpowiedzialnymi za bezpieczeństwo państwa. Działania ABW w tym zakresie obejmują nie tylko kontrolę przestrzegania procedur dostępu do tajemnic prawnie chronionych, ale również certyfikację systemów teleinformatycznych oraz audyty przedsiębiorców ubiegających się o świadectwa bezpieczeństwa przemysłowego.

ABW zainicjowała prace nad nowelizacją ustawy o ochronie informacji niejawnych o przepisy dotyczące stanów nadzwyczajnych, w szczególności konfliktu zbrojnego. Celem nowelizacji jest wprowadzenie przepisów zapewniających sprawne działanie w sytuacjach zagrożeń wojennych.

W każdym systemie informacyjnym nadal **najsłabszym ogniwem pozostaje człowiek**. Naruszenia przepisów mogą wynikać zarówno z jego **umyślnych działań**, do których należy zaliczyć

szpiegostwo czy **sabotaż**, jak i z **nieumyślnych błędów**, będących często skutkiem rutyny, braku świadomości zagrożeń bądź zewnętrznej presji. Ponadto do nieuprawnionego pozyskania, modyfikacji lub ujawnienia informacji o kluczowym znaczeniu dla bezpieczeństwa państwa może prowadzić szybko **postępująca cyfryzacja**, umożliwiająca przetwarzanie informacji niejawnych w systemach, które stają się częstym obiektem cyberataków.

Przypadek byłego sędziego Tomasza Szmydta, podejrzanego o szpiegostwo, który w maju 2024 r. uciekł na Białoruś i uzyskał tam azyl polityczny, był dla ABW impulsem do zainicjowania prac nad zmianą przepisów regulujących dostęp do informacji niejawnych dla sędziów i prokuratorów wykonujących obowiązki związane z dostępem do tego rodzaju informacji. Proponowane zmiany uzyskały poparcie działającego przy Prezesie Rady Ministrów Kolegium do Spraw Służb Specjalnych.

W latach 2024–2025 Agencja Bezpieczeństwa Wewnętrznego w ramach realizacji ustawowych procedur weryfikacyjnych wydała blisko **23 tys. poświadczeń bezpieczeństwa**. Dokumenty te uprawniają do dostępu do informacji niejawnych o klauzuli krajowej oraz tajemnic organizacji międzynarodowych. Rygorystyczne kryteria oceny rękojmi zachowania tajemnicy sprawiły, że w tym samym okresie odmówiono wydania poświadczenia prawie **200 osobom**, a **ponad 100 osób** otrzymało decyzję o cofnięciu nadanych wcześniej uprawnień.

Realizując zadania z zakresu ochrony informacji niejawnych w sferze gospodarczej, Agencja Bezpieczeństwa Wewnętrznego wydała ponad **550 świadectw bezpieczeństwa przemysłowego**. Dokumenty te potwierdzają zdolność przedsiębiorców do zapewnienia wymaganych standardów ochrony informacji niejawnych. W wyniku rygorystycznych postępowań weryfikacyjnych w tym samym okresie **8 podmiotom odmówiono** wydania takiego świadectwa, a **6 przedsiębiorców** otrzymało decyzję o cofnięciu wcześniej przyznanych uprawnień w tym zakresie. We wskazanych wyżej latach w zakresie ochrony informacji niejawnych w obszarze zainteresowania i nadzoru ABW pozostawali przedsiębiorcy dysponujący ok. 2200 świadectwami bezpieczeństwa przemysłowego.

Agencja Bezpieczeństwa Wewnętrznego realizuje również ustawowe zadania w obszarze bezpieczeństwa teleinformatycznego. W związku z tym we wskazanym okresie wydano **ponad 1 tys. świadectw akredytacji** systemów przeznaczonych do przetwarzania informacji niejawnych. Procedury te miały na celu potwierdzenie, że poddane weryfikacji środowiska spełniają rygorystyczne kryteria ochrony kryptograficznej, elektromagnetycznej oraz fizycznej, gwarantując nienaruszalność i poufność danych państwowych.

W ramach ustawowego nadzoru nad systemem ochrony informacji niejawnych ABW wszczęła łącznie **blisko 80 kontroli** w instytucjach publicznych oraz podmiotach komercyjnych. Zdecydowaną większość z nich stanowiły **zaplanowane audyty systemowe**, których było **ponad 70**. Równolegle, reagując na zidentyfikowane ryzyka i sygnały o potencjalnych uchybieniach, Agencja zainicjowała **4 procedury kontrolne w trybie doraźnym**.

TARCZA RP

Ochrona informacji niejawnych

ABW **nadzoruje** szczelność systemu poprzez certyfikację, audyty i koordynację służb.

STATYSTYKI

BEZPIECZEŃSTWO OSOBOWE

- **23 tys.** wydanych poświadczeń bezpieczeństwa
- blisko **200** odmów wydania poświadczenia
- ponad **100** cofniętych uprawnień

BEZPIECZEŃSTWO PRZEMYSŁOWE

- ponad **550** świadectw dla przedsiębiorców
- **8** odmów wydania świadectwa
- **6** cofniętych uprawnień

SYSTEMY TELEINFORMATYCZNE

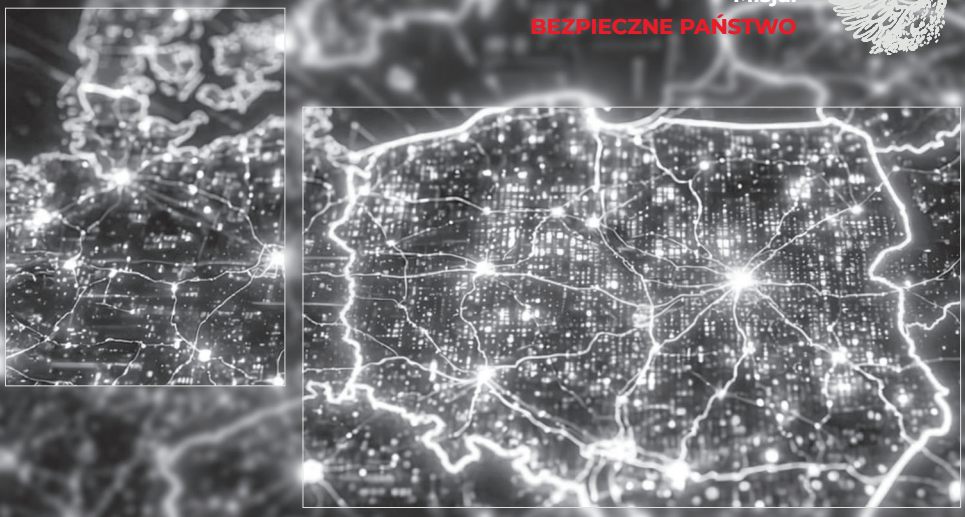
- ponad **1 tys.** wydanych świadectw akredytacji dla systemów IT
- **3** filary ochrony

KONTROLE BEZPIECZEŃSTWA SYSTEMÓW IT

80 przeprowadzonych kontroli

Ponad **70** audytów systemów (działania planowe i prewencyjne)

4 kontrole doraźne (szybka reakcja na zidentyfikowane ryzyka i błędy)



WSPÓŁPRACA MIĘDZYNARODOWA

Agencja Bezpieczeństwa Wewnętrznego prowadzi **intensywną współpracę międzynarodową**. Obejmuje ona partnerów z całego świata, przy czym kluczowe znaczenie mają relacje z państwami europejskimi i sojusznikami transatlantyckimi, w tym szczególnie z partnerami z NATO, UE i Ukrainy.

Współpraca ta pozwala na wspólną **analizę zagrożeń, wymianę informacji i doświadczeń** oraz wzmacnia skuteczność działań ABW i przyczynia się do zwiększenia bezpieczeństwa Polski.

Katalog partnerów zagranicznych ABW obejmuje w szczególności:

- **zagraniczne służby specjalne** (kontrwywiadowcze i wywiadowcze);
- **organy bezpieczeństwa i ochrony porządku publicznego** innych państw;
- akredytowane w Polsce **przedstawicielstwa dyplomatyczne**;
- **organizacje i instytucje** międzynarodowe;
- **fora współpracy** służb specjalnych.

Agencja Bezpieczeństwa Wewnętrznego utrzymuje stałe relacje z **blisko 100 podmiotami z ponad 50 państw**. Kluczowe obszary współdziałania koncentrują się na **przeciwdziałaniu obcej aktywności wywiadowczej, zwalczaniu terroryzmu, ochronie strategicznych interesów ekonomicznych RP,** monitorowaniu **niekontrolowanej migracji** oraz **zagrożeń w cyberprzestrzeni**.

Intensywność tej współpracy znajduje odzwierciedlenie w statystykach. W latach 2024–2025 przedstawiciele ABW uczestniczyli w **ponad 3 tys.** spotkań eksperckich w kraju i za granicą. W tym samym okresie w ramach współpracy z zagranicznymi służbami partnerskimi oraz organizacjami międzynarodowymi Agencja przekazała i odebrała **ponad 76 tys. informacji**.

Obserwowany od kilku lat systematyczny wzrost dynamiki i zakresu współpracy międzynarodowej stanowi bezpośrednią odpowiedź na ewolucję globalnych zagrożeń.

DZIAŁANIA OPERACYJNO-TECHNICZNE

Jednym z priorytetów Agencji Bezpieczeństwa Wewnętrznego jest rozwój potencjału operacyjno-technicznego. Jest to szczególnie istotne w warunkach dynamicznego rozwoju technologii i stale ewoluujących zagrożeń, które wymagają od służby ciągłego dostosowywania narzędzi i metod działania. Skuteczność w tym obszarze zależy bowiem nie tylko od inwestycji w nowoczesne rozwiązania techniczne, lecz także od rozwoju kadr oraz unikalnych, specjalistycznych kompetencji.

Działania podejmowane w latach 2024–2025 w obszarze wsparcia technicznego obejmowały realizację **ponad 520 tys. ustaleń telekomunikacyjnych**, w tym:

- **ponad 177 tys.** ustaleń abonenckich,
- **ponad 290 tys.** ustaleń bilingowych,
- **ponad 54 tys.** lokalizacji końcowych urządzeń mobilnych.

W raportowanym okresie Agencja zrealizowała także **ponad 850 wniosków o zastosowanie kontroli operacyjnej**.

Ponadto w ramach osłony kontrwywiadowczej organów państwa i samorządu w latach 2024–2025 przeprowadzono **ponad 200 specjalistycznych badań antypodsłuchowych**, realizowanych na wniosek uprawnionych podmiotów zewnętrznych.

Kontrola operacyjna

Bezpieczeństwo obywateli wymaga skutecznych działań, ale zawsze w granicach i na podstawie prawa. Kontrola operacyjna stanowi dla ABW niezwykle ważne narzędzie pracy operacyjnej, ponieważ wrogie przedsięwzięcia obcych państw i organizacji odbywają się przy zachowaniu głębokiej konspiracji, nastawionej na ochronę bezprawnych działań. Często jest to jedyny środek pozwalający na zdobycie informacji umożliwiających rozpoznanie struktur i mechanizmów przestępczych, a w konsekwencji podjęcie skutecznych działań zapobiegawczych. Uprawnienie to wykorzystywane jest tylko w ściśle określonych przypadkach – wtedy, gdy inne metody nie wystarczają, a zagrożenie jest realne. Stosowanie kontroli operacyjnej każdorazowo odbywa się na podstawie szczegółowych regulacji prawnych, gwarantujących, aby nie dochodziło do nadmiernej i nieproporcjonalnej ingerencji w prawa i wolności obywatelskie.

PREWENCJA I EDUKACJA

W obliczu nowych zagrożeń dla bezpieczeństwa wewnętrznego Polski nie wystarczy już tylko reagować na niebezpieczne sytuacje. Równie ważne jest budowanie świadomości i postaw, które pomagają im zapobiegać. Dlatego **Agencja Bezpieczeństwa Wewnętrznego kładzie szczególny nacisk na pozyskiwanie i upowszechnianie wiedzy o zagrożeniach hybrydowych oraz asymetrycznych.** Stałe podnoszenie kompetencji odbiorców w zakresie identyfikacji działań obcych służb oraz metod werbunku i dezinformacji pomaga ograniczać ryzyko zagrożeń wywiadowczych i terrorystycznych. Prewencja stanowi dla Agencji nieodzowny element osłony kontrwywiadowczej kraju.

Szkolenia

W latach 2024–2025 Agencja Bezpieczeństwa Wewnętrznego realizowała intensywne działania szkoleniowe, nakierowane na wzmacnianie odporności instytucjonalnej oraz podnoszenie kompetencji kadr administracji publicznej i sektora strategicznego. W tym okresie przeprowadzono **ponad 3 tys. szkoleń stacjonarnych**, obejmujących zagadnienia dotyczące kluczowych obszarów bezpieczeństwa państwa, takie jak:

- **profilaktyka kontrwywiadowcza,**
- **profilaktyka antyterrorystyczna,**
- **zjawisko radykalizacji,**
- **symbolika ekstremistyczna,**
- **bezpieczeństwo informacyjne, w tym ochrona informacji niejawnych,**
- **cyberbezpieczeństwo.**

Procesem edukacyjnym objęto łącznie **ponad 70 tys. pracowników z kilkuset podmiotów**, w tym kluczowych organów konstytucyjnych (Kancelarii Prezydenta RP, Kancelarii Prezesa Rady Ministrów, Kancelarii Sejmu, Kancelarii Senatu), ministerstw, a także instytucji o znaczeniu strategicznym (m.in. Instytutu Pamięci Narodowej, Urzędu Lotnictwa Cywilnego, Generalnej Dyrekcji Dróg Krajowych i Autostrad, Polskich Elektrowni Jądrowych).

Równolegle ABW rozwijała kanały edukacji zdalnej, **wydając** – od momentu uruchomienia w maju 2021 r. – **ponad 1,1 mln dostępów do dedykowanej platformy e-learningowej ABW**:

https://learning.tpcoe.gov.pl/

Szkolenia skierowane były do **urzędników administracji państwowej,** a także **pracowników spółek Skarbu Państwa, ośrodków naukowo-badawczych** oraz **instytucji i podmiotów gospodarczych o istotnym znaczeniu z punktu widzenia zabezpieczenia podstawowych interesów RP**.

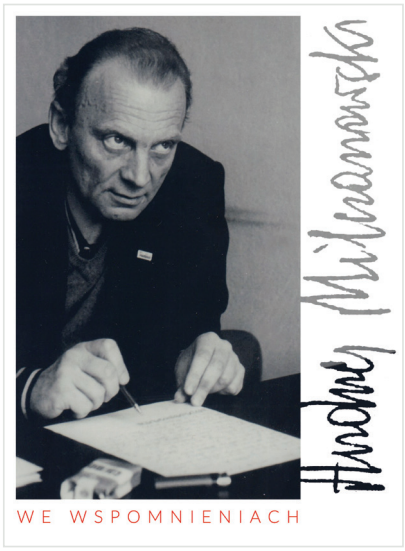
Odrębny, specjalistyczny filar stałej aktywności ABW stanowią **szkolenia dla inspektorów bezpieczeństwa teleinformatycznego** oraz **administratorów systemów**. Działania te realizowane są zarówno w instytucjach państwowych (sektor publiczny), jak i prywatnych podmiotach gospodarczych. Ich celem

jest zapewnienie poprawności i ciągłości funkcjonowania systemów oraz sieci wchodzących w skład krytycznej infrastruktury teleinformatycznej kraju, aby chronić bezpieczeństwo przetwarzanych w nich informacji.

Publikacje

Istotnym elementem zaplecza analityczno-badawczego Agencji Bezpieczeństwa Wewnętrznego jest działalność wydawnicza, realizowana poprzez edycję 2 czasopism naukowych. Od 2009 r. Agencja publikuje **„Przegląd Bezpieczeństwa Wewnętrznego”**, a od 2022 r. – „**Terroryzm – studia, analizy, prewencja”**. Oba periodyki stanowią forum wymiany myśli w obszarze szeroko rozumianego bezpieczeństwa wewnętrznego oraz ewoluujących zagrożeń o charakterze terrorystycznym. Dobór tematów poruszanych na łamach tych wydawnictw jest ściśle skorelowany z ustawowymi zadaniami Agencji, zapewniając merytoryczne wsparcie dla procesów decyzyjnych i operacyjnych. Do grona autorów artykułów należą uznani specjaliści, w tym funkcjonariusze ABW i innych służb mundurowych RP, przedstawiciele środowisk akademickich oraz eksperci zaangażowani w ochroną interesów narodowych.

W latach 2024–2025 ABW opublikowała 4 numery „Przeglądu Bezpieczeństwa Wewnętrznego” oraz 5 numerów „Terroryzmu”, w tym jedno wydanie specjalne.



W 2025 r. Agencja wydała również publikację *Andrzej Milczanowski we wspomnieniach*, dla upamiętnienia pełniącego dwukrotnie funkcję Szefa Urzędu Ochrony Państwa Śp. Andrzeja Milczanowskiego.

35-lecie cywilnych służb specjalnych

W 2025 r. ABW obchodziła 35. rocznicę powstania cywilnych służb specjalnych w wolnej Polsce, licząc od daty utworzenia Urzędu Ochrony Państwa w 1990 r. Zorganizowana z tej okazji w Pałacu Rzeczypospolitej uroczystość stanowiła okazję do mianowania funkcjonariuszy Agencji na pierwszy stopień oficerski oraz wręczenia listów gratulacyjnych przez Prezesa Rady Ministrów Pana Donalda Tuska.

DOBRE PRAKTYKI

Bezpieczeństwo informacji niejawnych oraz fizyczna ochrona obiektów zależą od sprawnego połączenia procedur systemowych z czujnością personelu. Każdy pracownik administracji publicznej i sektora strategicznego musi identyfikować się jako **potencjalny obiekt zainteresowania zagranicznych służb specjalnych**, które operują w sposób ciągły i wielokierunkowy. W odpowiedzi na te wyzwania w niniejszym rozdziale przygotowano zbiór fundamentalnych zasad bezpieczeństwa. Ich celem jest dostarczenie praktycznych wskazówek, które pozwolą na skuteczną identyfikację zagrożeń wywiadowczych i terrorystycznych oraz wdrożenie optymalnych schematów reagowania w codziennej służbie i pracy.

Pamiętaj! Możesz mieć wiedzę, którą interesują się obce służby specjalne. Współczesne środowisko bezpieczeństwa wymaga od osób przetwarzających informacje niejawne i wrażliwe szczególnej czujności oraz znajomości technik manipulacji stosowanych przez adwersarzy. **Obce ośrodki wywiadowcze wykorzystują** w swoich działaniach szerokie **spektrum narzędzi, metod i środków** – od psychotechnik manipulacji w świecie realnym, po zaawansowane operacje w cyberprzestrzeni – zmierzając do pozyskania danych kluczowych dla bezpieczeństwa RP. Równie istotna pozostaje gotowość do podjęcia natychmiastowych działań w przypadku wystąpienia zdarzeń o charakterze terrorystycznym.

Zestawienie zamieszczone na kolejnych stronach to kompendium wiedzy na temat pożądanych postaw i procedur – jasne wytyczne dotyczące tego, **jakich zachowań unikać oraz w jaki sposób efektywnie reagować** na zidentyfikowane zagrożenia.

Profilaktyka kontrwywiadowcza

Zalecane działania 😊

- **Włącz „filtr informacyjny”:** zachowaj czujność, gdy ktoś zbyt wnikliwie wypytuje cię o sprawy wrażliwe lub szczegóły zawodowe.
- **Monitoruj nietypowe zainteresowanie:** zwracaj uwagę na osoby, które wykazują nadmierną ciekawość twoimi uprawnieniami, dostępami do systemów czy specyfiką twojej pracy.
- **Stosuj zasadę ograniczonego zaufania:** każdą niespodziewaną przysługę czy pomoc od osób postronnych traktuj jako sygnał ostrzegawczy i potencjalny mechanizm budowania zależności.
- **Dziel się wiedzą oszczędnie:** ograniczaj przekazywanie informacji służbowych do niezbędnego minimum – nadmiar wiedzy w niepowołanych rękach to realne zagrożenie.
- **Bądź „cieniem” swojego sprzętu:** podczas podróży służbowych trzymaj dokumenty, laptopa i telefon pod stałym, osobistym nadzorem.
- **Dbaj o higienę relacji:** zachowaj zdrowy rozsądek i unikaj dwuznacznych sytuacji, które w przyszłości mogłyby stać się fundamentem do szantażu lub manipulacji.
- **Reaguj natychmiast:** jeśli dostrzeżesz jakiekolwiek sygnały zainteresowania ze strony obcych służb specjalnych, niezwłocznie skontaktuj się z Agencją Bezpieczeństwa Wewnętrznego.

Zachowania niepożądane 😵

- **Nie ulegaj „efektowi nowości”:** kategorycznie nie ujawniaj informacji wrażliwych nowo poznanym osobom, bez względu na to, jak godne zaufania się wydają.
- **Nie wchodź w układy „coś za coś”:** nigdy nie przyjmuj pomocy ani prezentów w zamian za udostępnienie kontaktów służbowych lub pozornie błahych informacji.
- **Nie bądź kurierem nieznajomych:** podczas wyjazdów zagranicznych nigdy nie przewoź paczek i nie przyjmuj upominków od nowo poznanych osób – to klasyczna metoda kompromitacji i werbunku.

Ochrona informacji

Zalecane działania 😊

- **Zapewnij ciągłość ochrony:** aktywnie chroń dokumenty niejawne oraz nośniki danych wrażliwych przed utratą, przypadkowym zniszczeniem lub wglądem osób nieuprawnionych.
- **Dbaj o trwałą utylizację danych:** zanim wyrzucisz dokumenty zawierające dane osobowe (np. PESEL, adres), poddaj je fizycznemu zniszczeniu w niszczarce. Skrawki papieru bywają cennym źródłem informacji dla osób trzecich.
- **Weryfikuj punkty powielania:** ograniczaj drukowanie i kopiowanie dokumentacji wrażliwej w ogólnodostępnych punktach usługowych, gdzie pamięć urządzeń nie gwarantuje poufności.
- **Sprawuj nadzór w przestrzeni publicznej:** poza miejscem pracy utrzymuj stałą, osobistą kontrolę nad posiadanymi dokumentami zawierającymi informacje wrażliwe.
- **Korzystaj z autoryzowanych narzędzi:** przetwarzaj informacje niejawne wyłącznie w dedykowanych i certyfikowanych do tego celu systemach teleinformatycznych.

Zachowania niepożądane 😵

- **Nie omawiaj spraw służbowych w miejscach publicznych:** Unikaj prowadzenia rozmów o charakterze wrażliwym w kawiarniach, środkach transportu czy windach, gdzie ryzyko podsłuchania jest wysokie.
- **Nie eksponuj treści dokumentów:** powstrzymaj się od czytania materiałów wrażliwych w pociągu, autobusie czy samolocie. Osoby postronne mogą bez trudu zapoznać się z ich zawartością.
- **Nie lekceważ wersji roboczych:** nie traktuj notatek ani brudnopisów jako materiałów nieistotnych. Często zawierają one kluczowe dane, które wymagają takiej samej ochrony jak finalne dokumenty.

Cyberhigiena

Zalecane działania 😊

- **Chroń swoją tożsamość cyfrową:** ograniczaj publikowanie danych personalnych do niezbędnego minimum.
- **Dbaj o aktualizacje:** regularnie aktualizuj system operacyjny oraz aplikacje na komputerze i smartfonie.
- **Weryfikuj źródła oprogramowania:** instaluj aplikacje i programy wyłącznie z legalnych, zaufanych platform oraz oficjalnych sklepów.
- **Separuj dostęp do urządzeń:** jeśli z twojego komputera korzystają inne osoby, skonfiguruj dla nich oddzielne profile użytkowników.
- **Stosuj zaawansowane zabezpieczenia dostępowe:** twórz długie, unikatowe i złożone hasła, wszędzie tam, gdzie to możliwe, aktywuj uwierzytelnianie wieloskładnikowe.
- **Świadomie zarządzaj hasłami:** regularnie odświeżaj swoje klucze dostępowe i nie stosuj tego samego hasła do różnych usług i aplikacji.
- **Zabezpieczaj kluczowe dane:** regularnie twórz kopie zapasowe najważniejszych plików i stosuj szyfrowanie danych.
- **Bądź nieufnym odbiorcą:** zawsze sprawdzaj adres nadawcy, poprawność linków oraz zawartość załączników przed ich otwarciem.
- **Kieruj się zasadą ograniczonego zaufania:** nigdy nie ufaj domyślnie, zawsze weryfikuj każde żądanie lub nietypową wiadomość.

Zachowania niepożądane 😵

- **Nie podłączaj obcych nośników danych:** nigdy nie wpinaj do swoich urządzeń znalezionych lub nieznanych pendrive'ów i dysków.
- **Nie udostępniaj haseł i skanów dokumentów:** nie przesyłaj haseł dostępowych ani skanów dowodu tożsamości drogą elektroniczną.
- **Nie działaj pod wpływem impulsu:** nie ulegaj presji „pilnej sprawy" ani silnym emocjom towarzyszącym wiadomościom.
- **Unikaj transakcji poza oficjalnymi systemami:** podczas zakupów online nigdy nie realizuj płatności ani nie prowadź rozmów poza oficjalną platformą sklepu lub portalu aukcyjnego.

Zagrożenia terrorystyczne

Zalecane działania 😊

- **Dbaj o orientację w terenie:** zapoznaj się z planami ewakuacji w miejscach, w których bywasz regularnie (biuro, galeria handlowa, dworzec). Wiedza o wyjściach awaryjnych to klucz do szybkiej reakcji.
- **Zachowaj świadomość sytuacyjną:** aktywnie obserwuj otoczenie i zwracaj uwagę na zachowania nienaturalne albo budzące twój niepokój.
- **Identyfikuj przedmioty bez nadzoru:** zwracaj szczególną uwagę na porzucone w miejscach publicznych paczki, torby czy plecaki.
- **Postaw na szybką i bezpieczną ewakuację:** w razie wystąpienia zagrożenia niezwłocznie opuść niebezpieczną strefę, o ile istnieje taka możliwość.
- **Stosuj procedurę ukrycia:** jeśli bezpieczna ewakuacja jest niemożliwa, znajdź schronienie, zabarykaduj się i wycisz urządzenia elektroniczne.
- **Alarmuj służby ratunkowe:** gdy znajdziesz się w bezpiecznym miejscu, natychmiast zadzwoń pod numer alarmowy 112 i przekaż zwięzłe informacje o sytuacji.
- **Podejmij obronę w ostateczności:** jeśli nie masz możliwości ucieczki ani ukrycia, a twoje życie jest bezpośrednio zagrożone, podejmij próbę obrony dostępnymi środkami.

Zachowania niepożądane 😨

- **Unikaj zbliżania się do źródła zagrożenia:** nigdy nie podchodź do miejsca zdarzenia, aby zaspokoić ciekawość lub sprawdzić, co się dzieje. Każda sekunda zwłoki zwiększa ryzyko.
- **Nie lekceważ sygnałów ostrzegawczych:** nie bagatelizuj podejrzanych sytuacji ani anomalii w przestrzeni publicznej. Lepiej zgłosić fałszywy alarm, niż przeoczyć realne niebezpieczeństwo.

Struktura terenowa ABW

CENTRALA ABW W WARSZAWIE

Adres: ul. Rakowiecka 2A, 00-993 Warszawa
email: poczta@abw.gov.pl

DYŻURNY OFICER OPERACYJNY ABW:
tel. 22 585-82-21, fax 22 585-84-88

www.abw.gov.pl

© Copyright by ABW

Warszawa 2026

Przeznaczone do bezpłatnego rozpowszechniania.

Powołując się na raport lub cytując jego fragmenty, należy podać źródło.