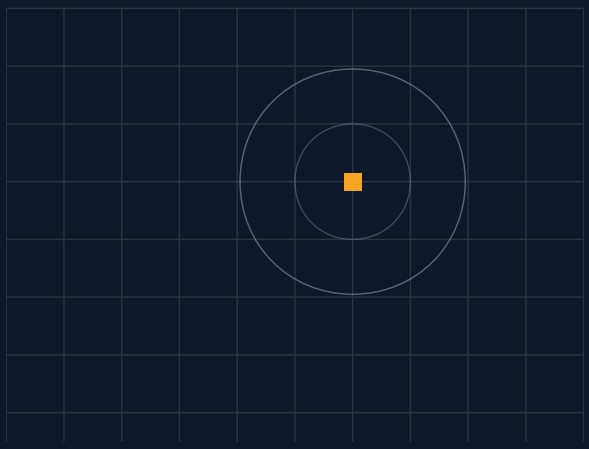
MATTHEW
HALABA.

stan na 24 października 2026 r.



Bezpieczeństwo osobiste i ochrona informacji w przestrzeni publicznej

Przewodnik szkoleniowy w warunkach zagrożeń hybrydowych

OPRACOWANIE
Matthew Halaba

> halaba.online

Spis treści

	Wstęp	3
	Kontekst zagrożeń 2025–2026	8
1	Podstawy bezpieczeństwa osobistego	15
2	Wybór lokalu i miejsca spotkania	21
3	Ocena otoczenia przed wejściem	27
4	Rozpoznawanie możliwego śledzenia i niepożądanej uwagi	31
5	Bezpieczne planowanie tras i przemieszczania się	41
6	Procedura weryfikacji niepokojącej sytuacji	46
7	Ochrona rozmów i informacji w lokalach publicznych	53
8	Bezpieczeństwo cyfrowe podczas spotkań i podróży	60
9	Bezpieczeństwo podczas spotkań z nieznanymi osobami	70
10	Rutyny, nawyki i ograniczanie przewidywalności	75
11	Postępowanie w sytuacjach kryzysowych	79
12	Przykłady i scenariusze praktyczne	84
13	Checklisty do wykorzystania w praktyce	93
14	Biznes z Ukrainą, w Ukrainie i na rzecz Ukrainy	97
15	OPSEC dla osób pracujących z wojskiem, dla wojska i w infrastrukturze krytycznej	105
	Aneksy	115

Wstęp

Ten przewodnik uczy, jak spotykać się, rozmawiać i przemieszczać w przestrzeni publicznej tak, żeby nie wystawiać siebie, rozmówców ani powierzonych informacji na niepotrzebne ryzyko. Powstał w październiku 2026 roku, w okresie, w którym polskie służby notują najwięcej spraw szpiegowskich i dywersyjnych od początku lat dziewięćdziesiątych. Nie zakłada jednak, że każdy czytelnik jest celem. Zakłada, że każdy powinien umieć to ocenić.

Najważniejsze zasady na jednej stronie

Cały przewodnik da się sprowadzić do dwunastu zasad. Pozostałe rozdziały wyjaśniają, jak je stosować w konkretnych sytuacjach.

1. Oceniaj zachowania i okoliczności, nigdy wygląd, język ani pochodzenie.
2. Pojedyncze zdarzenie zwykle nie pozwala ustalić intencji; powtarzalność zwiększa wagę sygnału, ale poważny sygnał wymaga reakcji od razu.
3. Najpierw oceń, czy zagrożenie jest bezpośrednie; jeśli tak, oddal się w stronę ludzi i dzwoń pod 112, bez konfrontacji.
4. Jeśli zagrożenie nie jest bezpośrednie, nazwij obserwację bez ocen i rozważ zwyczajne wyjaśnienia, zanim zareagujesz.
5. W przestrzeni publicznej omawiaj tylko informacje dopuszczone do ujawnienia; usunięcie nazwisk, dat i miejsc nie wystarcza do zachowania poufności.
6. Dokumenty w teczce, ekran do ściany, telefon ekranem w dół, blokada przy każdym odejściu od stołu.
7. Plan podróży i godzinę kontrolną zna zaufana osoba; zmiany przekazujesz na bieżąco.
8. Nie publikujesz lokalizacji w czasie rzeczywistym ani zdjęć z obiektów, transportów i ćwiczeń.
9. Nietypowa oferta od niezweryfikowanego zleceniodawcy, dotycząca fotografowania infrastruktury, rozpoznania trasy lub przekazania paczki, może być próbą werbunku. Szczególnie ostrożny bądź, gdy zleceniodawca ukrywa tożsamość, żąda tajemnicy albo zadanie dotyczy zabezpieczeń. Przy podejrzeniu nie wykonujesz zadania, zachowujesz korespondencję i zgłaszasz sprawę do ABW.
10. Zmianę rachunku bankowego partnera zawsze potwierdzasz telefonicznie na znany wcześniej numer.
11. Każdy incydent zapisujesz po fakcie, oddzielając fakty od ocen, i zgłaszasz właściwej osobie lub instytucji.
12. Środki ostrożności dobierasz do realnego ryzyka; stałe poczucie zagrożenia męczy i pogarsza decyzje.

Dla kogo jest ten dokument

Przewodnik jest przeznaczony dla osób, które z racji pracy mają dostęp do informacji cennych dla kogoś z zewnątrz albo bywają w miejscach, które ktoś może chcieć rozpoznać. W praktyce to szeroka grupa:

- członkowie zarządów, rad nadzorczych i kadra kierownicza,
- konsultanci, audytorzy, prawnicy i doradcy pracujący na danych klientów,
- dziennikarze i researcherzy, w tym osoby prowadzące rozmowy ze źródłami,
- uczestnicy negocjacji i rozmów biznesowych,
- specjaliści ds. bezpieczeństwa, ochrony informacji i ciągłości działania,
- pracownicy firm logistycznych, energetycznych, obronnych, telekomunikacyjnych i technologicznych,
- osoby zaangażowane w organizację lub transport pomocy dla Ukrainy,
- pracownicy samorządów i instytucji odpowiedzialnych za odporność lokalnych społeczności.

Część materiału przyda się każdemu dorosłemu. Rozdział o nietypowych ofertach „łatwego zarobku" warto przekazać także członkom rodziny, w tym nastolatkom, bo to właśnie młodzi ludzie bywają celem takich propozycji.

Czego ten przewodnik nie robi

Nie zastępuje procedur obowiązujących w twojej organizacji, instrukcji pełnomocnika ds. ochrony informacji niejawnych ani porady prawnej. Jeśli pracujesz z informacjami niejawnymi w rozumieniu ustawy z 5 sierpnia 2010 r. o ochronie informacji niejawnych, przepisy i wewnętrzne regulacje mają pierwszeństwo przed wszystkim, co tu przeczytasz.

Nie opisuje też profesjonalnych technik obserwacji, wykrywania obserwacji ani badań antypodsłuchowych. Ich legalność zależy od sposobu działania i okoliczności, a stosowane bez odpowiednich kompetencji mogą naruszać prawa innych osób albo zwiększać ryzyko. Opisane tu działania są legalne, nie wymagają specjalistycznego wyposażenia i mieszczą się w zwykłej ostrożności, jakiej można oczekiwać od odpowiedzialnego profesjonalisty.

Nie obiecuje wreszcie anonimowości ani pełnego bezpieczeństwa. Żaden zestaw nawyków ich nie zapewnia. Dobre praktyki obniżają prawdopodobieństwo incydentu i ograniczają jego skutki. To wszystko, i to w zupełności wystarcza, żeby się nimi zajmować.

Zasady, na których opiera się przewodnik

1. **Proporcjonalność.** Środki ostrożności dobiera się do rzeczywistego ryzyka. Rozmowa o terminie dostawy biurek nie wymaga tych samych zabezpieczeń co rozmowa o harmonogramie transportu sprzętu wojskowego.
2. **Legalność.** Wszystko, co robisz w ramach własnej ochrony, musi mieścić się w prawie. Nie śledzisz, nie zatrzymujesz, nie przeszukujesz, nie publikujesz wizerunku osób, które wydały ci się podejrzane.
3. Życie i zdrowie przed informacjami i mieniem. Dokumenty, laptop i telefon da się odtworzyć albo zablokować. Ciebie nie.
4. **Unikanie konfrontacji.** Przy uzasadnionym niepokoju oddalasz się, informujesz, zapisujesz fakty. Nie rozstrzygasz sytuacji samodzielnie.
5. **Fakty przed interpretacjami.** Notujesz, co widzisz i słyszysz, a ocenę zostawiasz na później albo osobom, które mają do tego uprawnienia.

6. **Naturalność.** Ostrożność, której nie widać, działa lepiej niż ostentacyjna podejrzliwość. Nerwowe rozglądanie się przyciąga uwagę i pogarsza jakość decyzji.

Jak odróżniamy fakty od ocen

W rozdziale o kontekście zagrożeń i w scenariuszach stosujemy trzy poziomy pewności. Te same kategorie przydają się później, gdy sam opisujesz niepokojące zdarzenie.

Poziom	Co oznacza	Przykład sformułowania
Ustalone	Zdarzenie potwierdzone przez organ państwa, prokuraturę, sąd lub kilka niezależnych źródeł	„Prokuratura przedstawiła zarzuty…"
Prawdopodobne	Wynika z analiz instytucji badawczych lub wypowiedzi przedstawicieli służb, bez pełnego potwierdzenia procesowego	„Według raportu ICCT i GLOBSEC…"
Możliwe	Hipoteza, którą warto brać pod uwagę, ale której nie da się dziś udowodnić	„Nie można wykluczyć, że…"

Poziom pewności opisuje samo zdarzenie. Status procesowy i przypisanie sprawstwa oznaczamy osobno, bo „potwierdzono zatrzymanie" nie znaczy „potwierdzono winę i zleceniodawcę". Dlatego tabela incydentów w rozdziale o kontekście zapisuje osobno, co potwierdzono, i według kogo przypisano sprawstwo, a osoby bez prawomocnego rozstrzygnięcia nazywamy podejrzanymi lub zatrzymanymi.

Co opisujesz	Jak to oznaczamy
Zdarzenie	Potwierdzono pożar, uszkodzenie, zatrzymanie
Status procesowy	Zarzuty, akt oskarżenia, wyrok nieprawomocny, wyrok prawomocny
Przypisanie sprawstwa	Według prokuratury, według służb, ustalone w wyroku

Tam, gdzie informacja zależy od daty, miejsca, aktualnych przepisów albo procedur konkretnej organizacji, dokument wskazuje konieczność sprawdzenia jej przed szkoleniem, podróżą lub zastosowaniem w organizacji.

Jak korzystać z dokumentu

Rozdziały 1–3 dotyczą przygotowania: jak myśleć o ryzyku, gdzie się spotykać, jak ocenić miejsce przed wejściem. Rozdziały 4 i 6 opisują sytuacje, w których coś zaczyna budzić niepokój, i dają schemat postępowania, a rozdział 5 dotyczy planowania tras i przemieszczania się. Rozdziały 7–9 skupiają się na ochronie rozmów, urządzeń i kontaktów z nieznajomymi. Rozdziały 10–11 dotyczą nawyków i sytuacji kryzysowych. Rozdział 12 zawiera osiem scenariuszy do omówienia na szkoleniu, a rozdział 13 zbiera krótkie listy kontrolne do wydrukowania. Rozdział 14 zawiera zalecenia dla firm i organizacji pracujących z Ukrainą, w Ukrainie i na jej rzecz, a rozdział 15 opisuje OPSEC dla osób pracujących z wojskiem, dla wojska i w infrastrukturze krytycznej. Aneksy zawierają podstawy prawne, kontakty, wzór notatki z incydentu, wykaz źródeł z datą weryfikacji, program trzygodzinnego szkolenia i pytania kontrolne z odpowiedziami. Rysunki są ponumerowane. Szkice oznaczone jako poglądowe nie przedstawiają rzeczywistych miejsc, a przykłady z danymi fikcyjnymi nie dotyczą prawdziwych osób.

Trener prowadzący zajęcia może pracować na scenariuszach od razu, odsyłając uczestników do rozdziałów, z których wynika rozwiązanie. Osoba ucząca się samodzielnie powinna przeczytać najpierw rozdział o kontekście i rozdział 1, potem wybrać te części, które odpowiadają jej codziennym obowiązkom.

Słowniczek pojęć

Pojęcie	Znaczenie w tym przewodniku
Świadomość sytuacyjna	Spokojna, bieżąca orientacja w tym, co dzieje się wokół: kto jest obok, którędy można wyjść, co odbiega od normy. Nie oznacza ciągłej czujności na maksymalnym poziomie.
Linia bazowa (norma miejsca)	Typowy obraz danego miejsca o danej porze: ruch, hałas, zachowania ludzi. Odstępstwa od linii bazowej są punktem wyjścia do oceny, a nie dowodem.
OPSEC	Ochrona informacji o działaniach i planach (ang. operational security). Polega na ustaleniu, które pozornie drobne informacje (godziny, trasy, nazwiska, zdjęcia) pozwalają komuś złożyć obraz całości, i na ograniczeniu ich wycieku.
Informacja wrażliwa	Każda informacja, której ujawnienie może zaszkodzić tobie, organizacji, kontrahentom albo bezpieczeństwu publicznemu, nawet jeśli formalnie nie jest niejawna: dane osobowe, harmonogramy, lokalizacje, warunki umów, plany inwestycji.
Informacja niejawna	Informacja, której nieuprawnione ujawnienie spowodowałoby lub mogłoby spowodować szkody dla Rzeczypospolitej Polskiej albo byłoby niekorzystne z punktu widzenia jej interesów, także w trakcie jej opracowywania i niezależnie od formy (art. 1 ust. 1 ustawy o ochronie informacji niejawnych). Brak oznaczenia na dokumencie lub ustna forma przekazania nie oznaczają, że informacja nie podlega ochronie; wątpliwości wyjaśniasz z pełnomocnikiem do spraw ochrony informacji niejawnych. Taka informacja rządzi się odrębnymi przepisami i nie powinna być przedmiotem rozmów w lokalu publicznym w żadnej formie.
Infrastruktura krytyczna	Systemy i obiekty niezbędne do funkcjonowania państwa i obywateli, m.in. energetyka, paliwa, łączność, transport, woda, finanse, ochrona zdrowia.
Działania hybrydowe	Działania państwa lub podmiotów przez nie inspirowanych poniżej progu otwartej wojny: dezinformacja, cyberataki, sabotaż, presja migracyjna, zastraszanie.
Dywersja i sabotaż	W języku potocznym celowe niszczenie lub zakłócanie działania obiektów i usług. W prawie karnym te pojęcia pojawiają się m.in. w art. 130 Kodeksu karnego.
Jednorazowy wykonawca	Osoba werbowana zwykle przez internet do pojedynczego zadania za niewielką zapłatę, często nieświadoma, na czyje zlecenie działa. W literaturze anglojęzycznej: disposable agent, gig-economy operative.

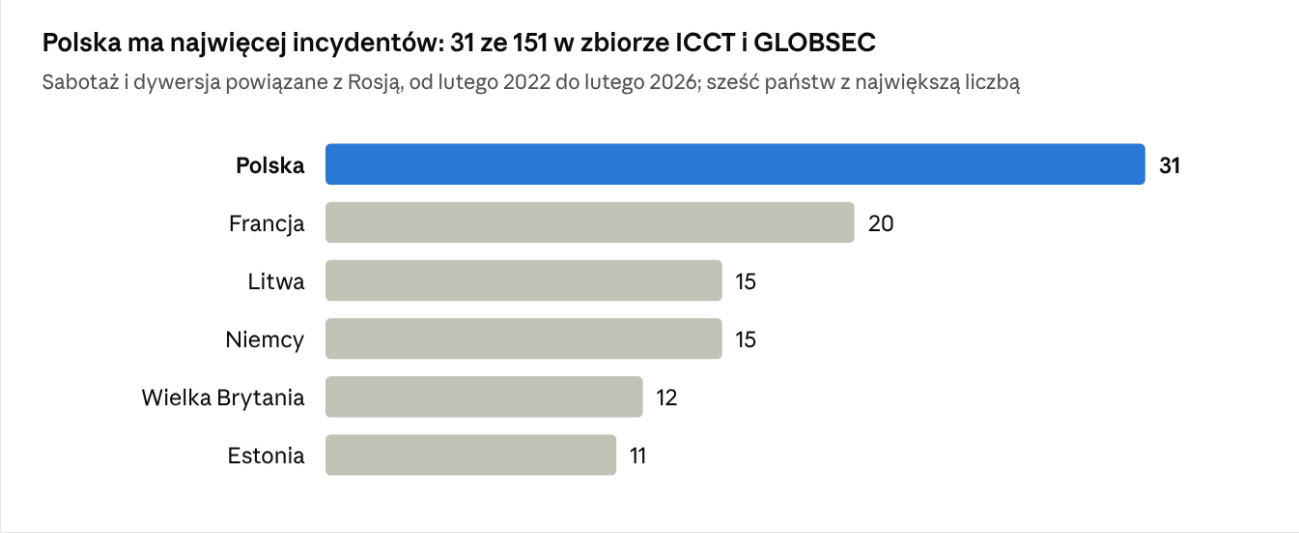
Pojęcie	Znaczenie w tym przewodniku
Socjotechnika	Wpływanie na ludzi tak, żeby sami ujawnili informacje lub wykonali działanie korzystne dla atakującego: pośpiech, autorytet, sympatia, poczucie winy, ciekawość.
Phishing i quishing	Wyłudzanie danych lub instalowanie złośliwego oprogramowania przez fałszywe wiadomości (phishing) albo podmienione kody QR (quishing).
Spoofing	Podszywanie się pod cudzy numer telefonu, nazwę nadawcy SMS-a albo adres e-mail tak, żeby wiadomość lub połączenie wyglądały na pochodzące od banku, urzędu albo znanej osoby.
Deepfake	Obraz, nagranie wideo lub głos wygenerowane albo przerobione przez narzędzia sztucznej inteligencji tak, żeby przypominały prawdziwą osobę.
Uwierzytelnianie wieloskładnikowe (MFA)	Logowanie wymagające więcej niż hasła, np. kodu z aplikacji albo fizycznego klucza bezpieczeństwa.
Klucz sprzętowy	Fizyczne urządzenie (np. w standardzie FIDO2) potwierdzające logowanie. Odporne na większość ataków phishingowych.
Metadane	Dane o danych: kto, kiedy, skąd, do kogo. Zdjęcie może zawierać współrzędne GPS, a kalendarz sam w sobie zdradza rytm pracy.
Stopnie alarmowe	Cztery stopnie (ALFA, BRAVO, CHARLIE, DELTA) oraz odpowiedniki dla cyberprzestrzeni (CRP) wprowadzane zarządzeniem Prezesa Rady Ministrów, a w sprawach niecierpiących zwłoki przez ministra spraw wewnętrznych, na podstawie ustawy z 10 czerwca 2016 r. o działaniach antyterrorystycznych.
Bezpieczne miejsce publiczne	Miejsce, w którym są inni ludzie, oświetlenie, personel i możliwość wezwania pomocy: recepcja hotelu, apteka, stacja paliw, komisariat, czynny sklep.

Kontekst zagrożeń 2025–2026

W zbiorze ICCT i GLOBSEC, który obejmuje zidentyfikowane przypadki z okresu od lutego 2022 do lutego 2026 roku, Polska ma najwięcej odnotowanych incydentów sabotażu i dywersji powiązanych z Rosją: 31. W 2025 roku liczba wszczętych u nas śledztw szpiegowskich wzrosła do 48, czyli ponad dwukrotnie wobec roku poprzedniego. Ten rozdział porządkuje to, co wiadomo publicznie według stanu na 24 października 2026 roku, i wyjaśnia, co z tego wynika dla osoby, która nie pracuje w służbach, ale bywa w miejscach i posiada informacje, którymi ktoś może się interesować.

Skala zjawiska w liczbach

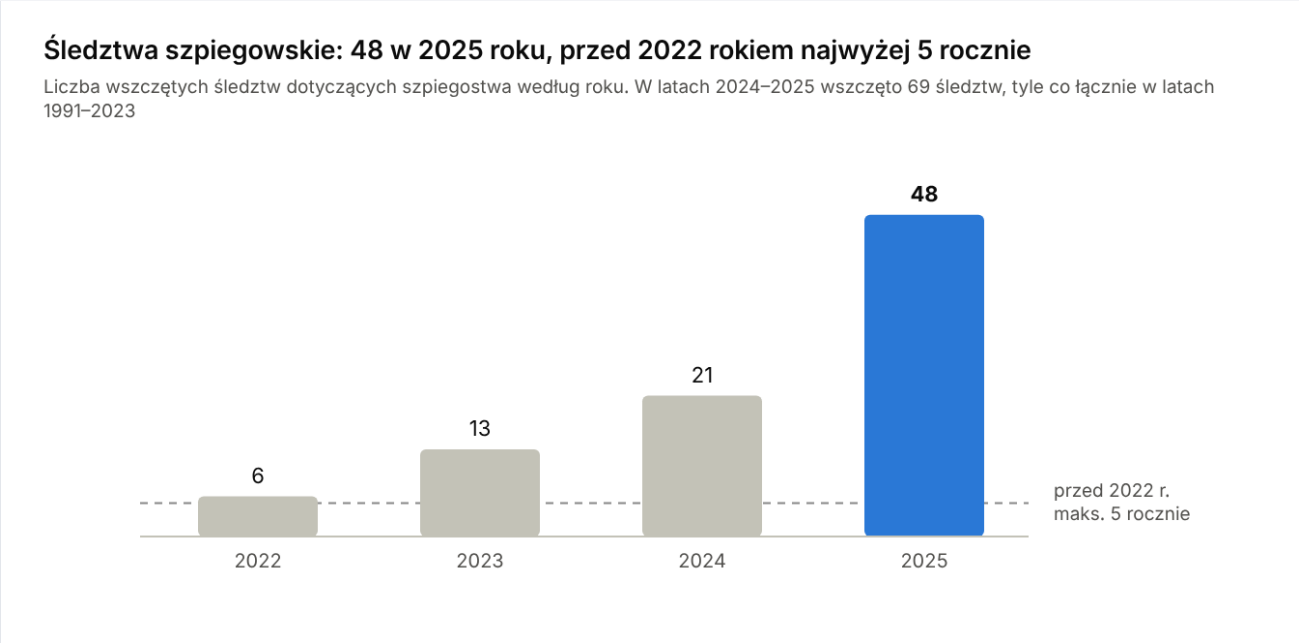
Najpełniejszym jawnym zestawieniem incydentów w Europie jest zbiór danych prowadzony przez International Centre for Counter-Terrorism (ICCT) w Hadze i słowacki think tank GLOBSEC. Pierwszy wspólny raport, opublikowany 30 września 2025 roku, opisał ponad 110 ataków i prób ataków powiązanych z Rosją od lutego 2022 roku. Aktualizacja z 23 lutego 2026 roku dodała 41 przypadków i podniosła tę liczbę do 151 incydentów do lutego 2026 roku.



Rys. 1. Sześć państw z największą liczbą incydentów sabotażu i dywersji powiązanych z Rosją, luty 2022 – luty 2026 · źródło: ICCT i GLOBSEC, aktualizacja z 23 lutego 2026 r.

Autorzy zastrzegają, że to dolna granica. Wiele incydentów staje się publicznych dopiero po zakończeniu śledztw, a atrybucja bywa trudna. Dla porównania: według tego samego opracowania niemieckie organy bezpieczeństwa odnotowały w samym 2025 roku 320 podejrzeń prób sabotażu, choć sprawców ustalono w niewielu z nich.

Polskie dane pochodzą z pierwszego od 2014 roku jawnego raportu Agencji Bezpieczeństwa Wewnętrznego, „Agencja Bezpieczeństwa Wewnętrznego 2024–2025. Wybrane aktywności”, opublikowanego w maju 2026 roku. Od lat dziewięćdziesiątych wszczynano maksymalnie pięć śledztw szpiegowskich rocznie. Po rosyjskiej inwazji na Ukrainę ta liczba rośnie co roku.



Rys. 2. Śledztwa szpiegowskie wszczęte w latach 2022–2025 · źródło: raport ABW „Agencja Bezpieczeństwa Wewnętrznego 2024–2025. Wybrane aktywności”

Według ABW w latach 2024–2025 wszczęto 69 takich śledztw, czyli tyle, ile łącznie w latach 1991–2023. Od początku pełnoskalowej agresji status podejrzanego otrzymało 91 osób, zarzuty z art. 130 Kodeksu karnego usłyszały 82 osoby, a 62 zostały zatrzymane. Raport nie rozstrzyga, w jakim stopniu wzrost wynika z większej aktywności obcych służb, a w jakim ze skuteczniejszego wykrywania. Rozsądnie jest przyjąć, że działają oba czynniki.

Główne incydenty w Polsce i w regionie

Poniższe zestawienie obejmuje zdarzenia, które mają znaczenie dla praktyki opisanej w przewodniku. Najnowsze są na górze.

Data	Zdarzenie	Co potwierdzono / status sprawy
23 IX 2026	Wieczorem dwóch zamaskowanych mężczyzn pokonało ogrodzenie naziemnej stacji łączności satelitarnej Starlink w Woli Krobowskiej (gm. Grójec), oblało łatwopalną cieczą i podpaliło urządzenia zasilania i sterowania. Śledztwo prowadzone jest m.in. w kierunku sabotażu na rzecz obcego wywiadu i przestępstwa o charakterze terrorystycznym. 7 X prokurator przedstawił zarzuty dwóm obywatelom Turcji, zatrzymanym 12 X 2026 w Niemczech. Według ABW atak poprzedziło rozpoznanie: osoba wcześniej sprawdzona przez zleceniodawcę przesyłała mu przez Telegram zdjęcia i nagrania, a potem dostała polecenie rozpoznania terenu stacji i jej zabezpieczeń; według RMF FM to obywatel Ukrainy, aresztowany 30 IX. W Niemczech zatrzymano też 24-letnią obywatelkę Turcji, która według RMF FM miała przywieźć podejrzanych. (InfoSecurity24 za ABW, RMF24)	Potwierdzono pożar, zarzuty i zatrzymania; zlecenie rosyjskich służb według rządu i prokuratury; śledztwo w toku
13 VIII 2026	Premier poinformował o zatrzymaniu 7 VIII 29-letniego obywatela Rosji, który według służb, zwerbowany przez rosyjski wywiad, przygotowywał w Warszawie zabójstwo osoby mającej obywatelstwo USA i Ukrainy. (Notes from Poland)	Potwierdzono zatrzymanie i zarzuty; zlecenie rosyjskich służb według premiera
4 VIII 2026	Lotnisko Lipsk/Halle w Niemczech: przy ukraińskim samolocie transportowym An znaleziono drona z ładunkiem wybuchowym i zapalnikiem. Niemieckie MSW mówi o możliwym ataku hybrydowym. (LIGA.net za Die Zeit)	Potwierdzono znalezienie drona; możliwy atak hybrydowy według niemieckiego MSW
15–16 XI 2025	Wysadzenie toru na linii Warszawa–Lublin w pobliżu miejscowości Mika oraz uszkodzenie sieci trakcyjnej w rejonie Puław (Gołąb). Rząd wskazał dwóch obywateli Ukrainy współpracujących z rosyjskimi służbami, którzy uciekli na Białoruś. Trzeciemu obywatelowi Ukrainy prokuratura zarzuciła pomocnictwo: według śledczych we wrześniu 2025 zawiózł jednego z podejrzanych w rejon przyszłych ataków, żeby ten mógł rozpoznać teren. 19 XI 2025 wprowadzono stopień alarmowy CHARLIE dla linii kolejowych PKP PLK i PKP LHS. (Eska)	Potwierdzono uszkodzenia; podejrzanych i ich powiązania ze służbami Rosji wskazał rząd; zarzut pomocnictwa i areszt wobec trzeciej osoby
X 2025	Polsko-rumuńska operacja przeciw planowi nadania przez firmę kurierską paczek z ładunkami, które miały zapalić się lub wybuchnąć w transporcie przez Polskę i Rumunię do Ukrainy. W Polsce zatrzymano 21-letniego obywatela Ukrainy, w Rumunii dwóch kolejnych, którzy zostawili paczki w oddziale firmy kurierskiej w Bukareszcie. (Reuters, ICCT)	Potwierdzono zatrzymania; plan według śledczych
9–10 IX 2025	Według ministra obrony od 11 do 20 rosyjskich dronów naruszyło polską przestrzeń powietrzną podczas ataku na Ukrainę. Pierwsze zestrzelenia, czasowe zamknięcie lotnisk w Warszawie, Modlinie, Rzeszowie i Lublinie.	Potwierdzono naruszenie przestrzeni powietrznej i zestrzelenia; liczba dronów według ministra obrony
III 2024 – II 2025	Grupa pięciu osób (obywatele Ukrainy i Białorusi) fotografowała i przekazywała zdjęcia infrastruktury krytycznej oraz rozwieszała plakaty i malowała graffiti na zlecenie rosyjskich służb, m.in. w Rzeszowie, Warszawie i Łodzi. (ICCT)	Zarzuty; zlecenie rosyjskich służb według śledczych

Data	Zdarzenie	Co potwierdzono / status sprawy
12 V 2024	Pożar centrum handlowego Marywilska 44 w Warszawie, w którym działało ponad 1400 sklepów i punktów usługowych. W maju 2025 premier i prokuratura poinformowali, że było to podpalenie na zlecenie rosyjskich służb. Jedna z osób miała za zadanie nagrać pożar i działania służb; film trafił na rosyjskie strony propagandowe. (Notes from Poland)	Potwierdzono pożar; podpalenie na zlecenie rosyjskich służb według rządu i prokuratury; zarzuty
VII 2024	Paczki z ukrytymi urządzeniami zapalającymi zapaliły się w centrach logistycznych DHL w Lipsku i Birmingham. Polska prokuratura zatrzymała osoby podejrzane o udział w tej operacji, którą zachodnie służby wiązały z testowaniem kanału przerzutu na samoloty cargo.	Potwierdzono pożary paczek i zatrzymania podejrzanych; powiązanie z testem kanału przerzutu według zachodnich służb

W odpowiedzi na akty dywersji Polska cofnęła zgody na działanie konsulatów generalnych Rosji. Placówki zakończyły działalność w Poznaniu (listopad 2024), Krakowie (czerwiec 2025) i Gdańsku (grudzień 2025; decyzję ogłoszono w listopadzie, po sabotażu na kolei).



Rys. 3. Wybrane zdarzenia z lat 2024–2026 omawiane w przewodniku · opracowanie na podstawie źródeł z tabeli powyżej i aneksu D

Jak wygląda werbunek jednorazowych wykonawców

Najbardziej praktyczna dla czytelnika część wiedzy dotyczy sposobu, w jaki obce służby pozyskują ludzi do prostych zadań. Opisy z raportu ABW, opracowania ICCT i GLOBSEC, białej księgi Polskiego Instytutu Spraw Międzynarodowych (PISM) z maja 2026 roku oraz śledztw dziennikarskich są w tej sprawie zbieżne.

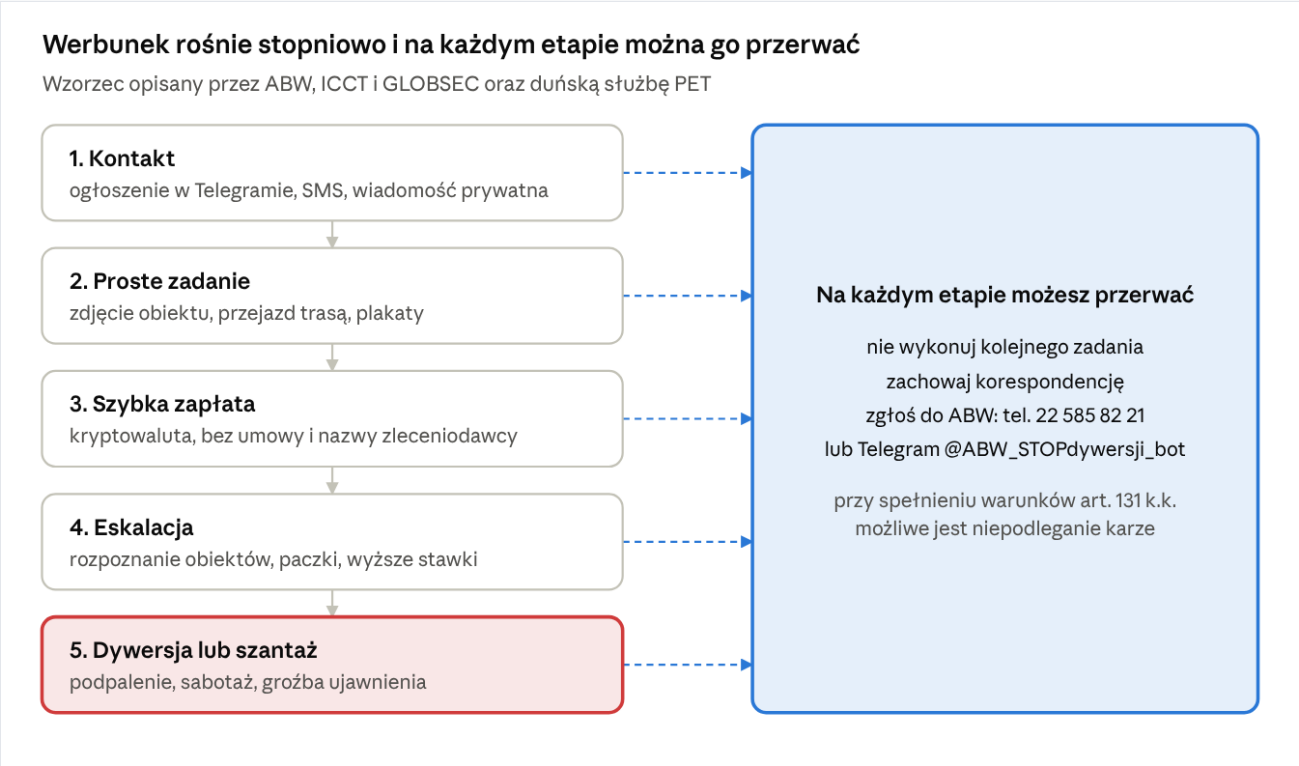
Kanał kontaktu. Ogłoszenia i wiadomości pojawiają się w komunikatorach, przede wszystkim w Telegramie, oraz w mediach społecznościowych, w tym w serwisach popularnych wśród młodzieży. Według ABW komunikacja między zleceniodawcą a wykonawcą odbywa się głównie online, a rozliczenia w kryptowalutach. We wrześniu 2026 roku opisywano także SMS-y z ofertą „pracy zdalnej" za nawet 35 euro za godzinę. Link prowadził do konta w Telegramie podszywającego się pod rekrutera, a Michał Marek, ekspert od dezinformacji, ocenił, że w ten sposób rosyjskie i białoruskie służby mogą szukać ludzi do prostych zadań (Spider's Web).

Forma zadania. Pierwsze zlecenia wyglądają niewinnie: zrób zdjęcie budynku, przejedź się trasą i opisz, co widzisz, naklej plakaty, namaluj napis, odbierz i przekaż paczkę, nagraj film z określonego miejsca o określonej godzinie. Duńska służba bezpieczeństwa PET opisuje ten sam wzorzec: zaczyna się od rozpoznania i fotografowania potencjalnych celów, potem przychodzą zadania sabotażowe (Kyiv Post).

Eskalacja. ICCT i GLOBSEC nazywają to zasadą podwójnej eskalacji: najpierw drobne zadania za małe kwoty, potem coraz poważniejsze zlecenia za coraz wyższe stawki, aż do podpaleń i ładunków wybuchowych.

Kto jest werbowany. Według ICCT i GLOBSEC około 95 procent ze 172 zidentyfikowanych sprawców to zwykli cywile bez formalnych związków z rosyjskimi służbami. Głównym motywem są pieniądze. 11 osób miało mniej niż 18 lat (najmłodsza 16), kolejne 14 miało od 18 do 21 lat. Około jednej czwartej było wcześniej karanych. Mniej więcej połowa nie mieszkała w kraju ataku, tylko przyjechała na jedno zadanie za kilkaset euro. Według białej księgi PISM z 29 maja 2026 roku o rosyjskim sabotażu w państwach Rady Państw Morza Bałtyckiego, w sprawach, w których ustalono motywację, czynnik finansowy występował w około 96 procentach, ideologiczny w około 15, a ponad połowa zwerbowanych nie była w pełni świadoma, że działa na rzecz obcego wywiadu (INE za PISM).

Grupa, nie samotnik. Wbrew obiegowemu obrazowi samotnego „agenta na jedno zadanie" około 90 procent sprawców działało z przynajmniej jedną inną osobą.



Rys. 4. Etapy werbunku jednorazowych wykonawców i wyjście na każdym etapie

Schemat pokazuje, że nie ma momentu, w którym jest „za późno" na zgłoszenie. Im wcześniej ktoś przerwie, tym mniejsze ryzyko dla niego samego i dla innych.

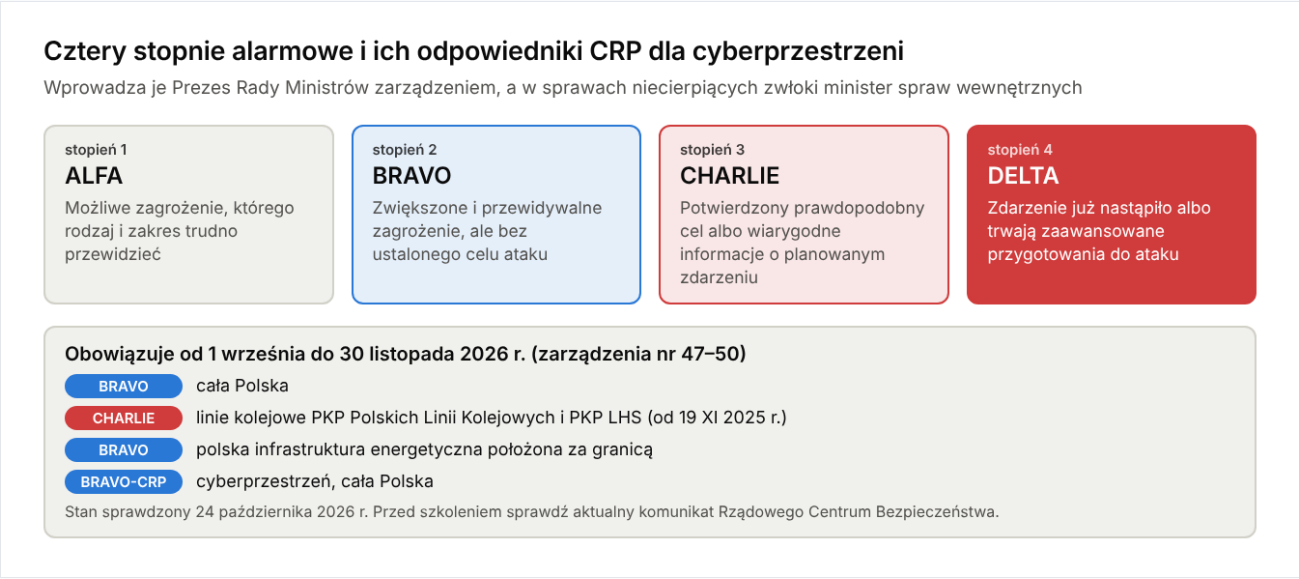
Zmiana modelu w latach 2024–2026

ABW opisuje „profesjonalizację" rosyjskich działań. W 2023 roku przeważali jednorazowi wykonawcy pozyskiwani ad hoc przez internet. W latach 2024–2025 większy nacisk położono na złożone komórki oparte na hermetycznych strukturach przestępczości zorganizowanej, z preferencją dla osób z doświadczeniem w formacjach siłowych. Rosja intensyfikuje też szkolenia na własnym terytorium. Agencja wprost stwierdza, że rosyjskie służby akceptowały możliwość ofiar śmiertelnych, zwłaszcza przy przedsięwzięciach, które mogły doprowadzić do katastrof lotniczych lub kolejowych, a celem były także sklepy wielkopowierzchniowe i inne miejsca użyteczności publicznej.

Nie oznacza to, że werbunek przez komunikatory zniknął. Oba modele działają równolegle: masowy, tani nabór do prostych zadań i mniejsze, lepiej przygotowane grupy do zadań poważniejszych. Przypadek stacji Starlink pokazuje element wspólny dla obu: według ABW podpalenie poprzedziło rozpoznanie terenu i zabezpieczeń stacji, a zdjęcia i nagrania trafiały do zleceniodawcy przez Telegram (InfoSecurity24). Policja sprawdzała też w okolicy mężczyzn, których później powiązano ze sprawą, choć wtedy nie było podstaw do ich zatrzymania. Rozpoznanie poprzedzające działanie zostawia ślady, które czasem dostrzegają zwykli ludzie.

Stopnie alarmowe

Według stanu na 24 października 2026 roku obowiązują: drugi stopień alarmowy BRAVO na całym terytorium Polski, drugi stopień alarmowy CRP (BRAVO-CRP) dotyczący cyberprzestrzeni, również na całym terytorium, trzeci stopień CHARLIE na liniach kolejowych zarządzanych przez PKP PLK i PKP LHS oraz BRAVO wobec polskiej infrastruktury energetycznej położonej za granicą. CHARLIE na kolei wprowadzono 19 listopada 2025 roku, po aktach sabotażu z 15–16 listopada. Obecne zarządzenia Prezesa Rady Ministrów nr 47–50 obowiązują od 1 września do 30 listopada 2026 roku (komunikat RCB z 26 sierpnia 2026 roku). Zakres i terminy sprawdzaj przed szkoleniem w aktualnych komunikatach Rządowego Centrum Bezpieczeństwa.



Rys. 5. Stopnie alarmowe i stan obowiązujący od 1 września do 30 listopada 2026 r. · źródła: ustawa o działaniach antyterrorystycznych (art. 15–16), komunikat RCB z 26 sierpnia 2026 r.

Dla przeciętnej osoby stopień alarmowy oznacza przede wszystkim więcej kontroli na dworcach, lotniskach i przy obiektach infrastruktury oraz większą wrażliwość służb na nietypowe zachowania w ich pobliżu. Fotografowanie torowisk, stacji transformatorowych czy terminali w okresie CHARLIE może skończyć się legitymowaniem, nawet jeśli robisz to w dobrej wierze.

Co z tego wynika dla czytelnika

Z powyższych danych nie wynika, że każdy pracownik firmy logistycznej czy energetycznej jest celem obcych służb. Wynika z nich pięć realnych obszarów ryzyka, które dotyczą zwykłych ludzi:

Obszar ryzyka	Na czym polega	Gdzie w przewodniku
Kontakt werbunkowy	Ty, ktoś z rodziny lub współpracownik dostajecie ofertę „łatwego zarobku" za zdjęcie, przejazd, paczkę.	Rozdziały 4, 9, scenariusz 7
Źródło informacji	Twoje rozmowy, zdjęcia, kalendarz i publikacje pozwalają komuś odtworzyć harmonogramy, trasy, lokalizacje i nazwiska.	Rozdziały 7, 8, 10
Bliskość celu	Pracujesz lub spotykasz się w pobliżu centrów logistycznych, węzłów kolejowych, obiektów energetycznych, punktów zbiórki pomocy.	Rozdziały 2, 3, 5, scenariusz 8
Ataki cyfrowe	Phishing, quishing, przejęcie kont i urządzeń, w tym podczas podróży.	Rozdział 8
Dezinformacja	Fałszywe komunikaty o mobilizacji, atakach czy ewakuacji wywołujące chaos albo skłaniające do nieprzemyślanych działań.	Rozdziały 6, 11

Odpowiedzią na te ryzyka nie jest podejrzliwość wobec wszystkich, a zwłaszcza wobec całych grup narodowościowych. Wśród sprawców i podejrzanych opisanych przez ICCT są m.in. obywatele Ukrainy, Białorusi, Mołdawii, Serbii, Bułgarii i Kolumbii oraz osoby z podwójnym, rosyjskim i unijnym obywatelstwem, a w sprawach opisanych w tym przewodniku także obywatele Polski, Rosji i Turcji. Wśród ofiar są też ukraińscy uchodźcy werbowani pod presją. Ocena dotyczy zachowań i okoliczności, nigdy pochodzenia.

ABW zauważa, że wzrost społecznej świadomości zagrożeń ograniczył rosyjskiemu wywiadowi możliwości nawiązywania kontaktów z obywatelami RP. Nie oznacza to jednak, że nadmierna podejrzliwość jest właściwa: osoba zmęczona ciągłym alarmem może przestawać rozróżniać sygnały, które naprawdę coś znaczą.

1.

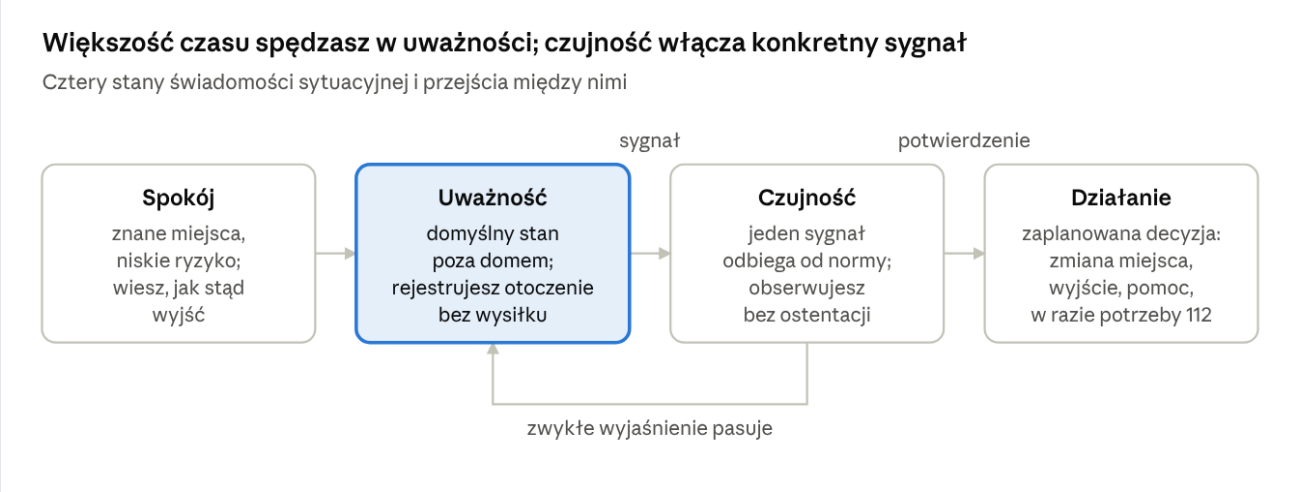
Podstawy bezpieczeństwa osobistego

Bezpieczeństwo osobiste w przestrzeni publicznej opiera się na trzech umiejętnościach: spokojnej orientacji w otoczeniu, realistycznej ocenie ryzyka i przygotowanym z wyprzedzeniem planie na wypadek, gdyby coś poszło nie tak. Żadna z nich nie wymaga specjalistycznego wyposażenia ani szkolenia. Wymaga natomiast nawyku, który buduje się tygodniami, a nie w dniu ważnego spotkania.

1.1. Czym jest świadomość sytuacyjna

Świadomość sytuacyjna to bieżąca, w dużej mierze automatyczna orientacja w tym, co dzieje się wokół ciebie. Obejmuje trzy rzeczy: dostrzeżenie elementów otoczenia, zrozumienie ich znaczenia i przewidzenie, jak sytuacja może się rozwinąć w najbliższych minutach. Kierowca, który widzi piłkę toczącą się na jezdnię i odruchowo zwalnia, bo za piłką może wybiec dziecko, wykazuje się właśnie świadomością sytuacyjną.

W praktyce bezpieczeństwa osobistego nie chodzi o permanentną czujność. Człowiek nie jest w stanie przez wiele godzin utrzymywać wysokiej koncentracji na otoczeniu. Po kilkudziesięciu minutach uwaga słabnie, a zmęczenie prowadzi do gorszych decyzji niż spokojna nieuwaga. Dlatego w tym przewodniku posługujemy się prostym modelem czterech stanów, między którymi przechodzi się płynnie w zależności od sytuacji.



Rys. 6. Cztery stany świadomości sytuacyjnej i przejścia między nimi

Najczęstszym błędem nie jest brak czujności, tylko przebywanie w stanie „odcięcia", poniżej spokoju: słuchawki w obu uszach, wzrok w ekranie, brak wiedzy, gdzie jest wyjście. Drugim częstym błędem jest skakanie od razu do czujności przy każdym drobiazgu, co wyczerpuje i sprawia, że po godzinie przestajesz zauważać cokolwiek.

1.2. Jak rozwijać świadomość sytuacyjną bez nadmiernej podejrzliwości

Świadomość sytuacyjną rozwija się przez ćwiczenie spostrzegania, a nie przez czytanie o zagrożeniach. Poniższe nawyki można wdrażać stopniowo, po jednym tygodniowo.

Określanie normy miejsca. Wchodząc do nowego miejsca, poświęć kilkanaście sekund na odpowiedź na pytanie, jak wygląda tu „zwykle". Czy ludzie rozmawiają głośno, czy cicho? Czy przychodzą i wychodzą szybko, czy siedzą godzinami? Czy obsługa jest widoczna? Ta linia bazowa jest punktem odniesienia. Bez niej każde zachowanie wydaje się albo całkowicie normalne, albo podejrzane.

Znajomość wyjść. Za każdym razem, gdy siadasz w lokalu, sali konferencyjnej czy poczekalni, ustal dostępną drogę wyjścia oraz alternatywną, jeśli istnieje, najlepiej inną niż ta, którą wszedłeś. Nie zakładaj, że każde widoczne drzwi są dostępnym wyjściem ewakuacyjnym. Ludzie w sytuacji zagrożenia instynktownie kierują się do wejścia, przez które przyszli, nawet jeśli jest dalej i zatłoczone.

Telefon niżej, wzrok wyżej. Korzystaj z telefonu, ale co jakiś czas podnoś wzrok. Jeśli masz słuchawki, w miejscach publicznych noś jedną albo używaj trybu, który przepuszcza dźwięki otoczenia.

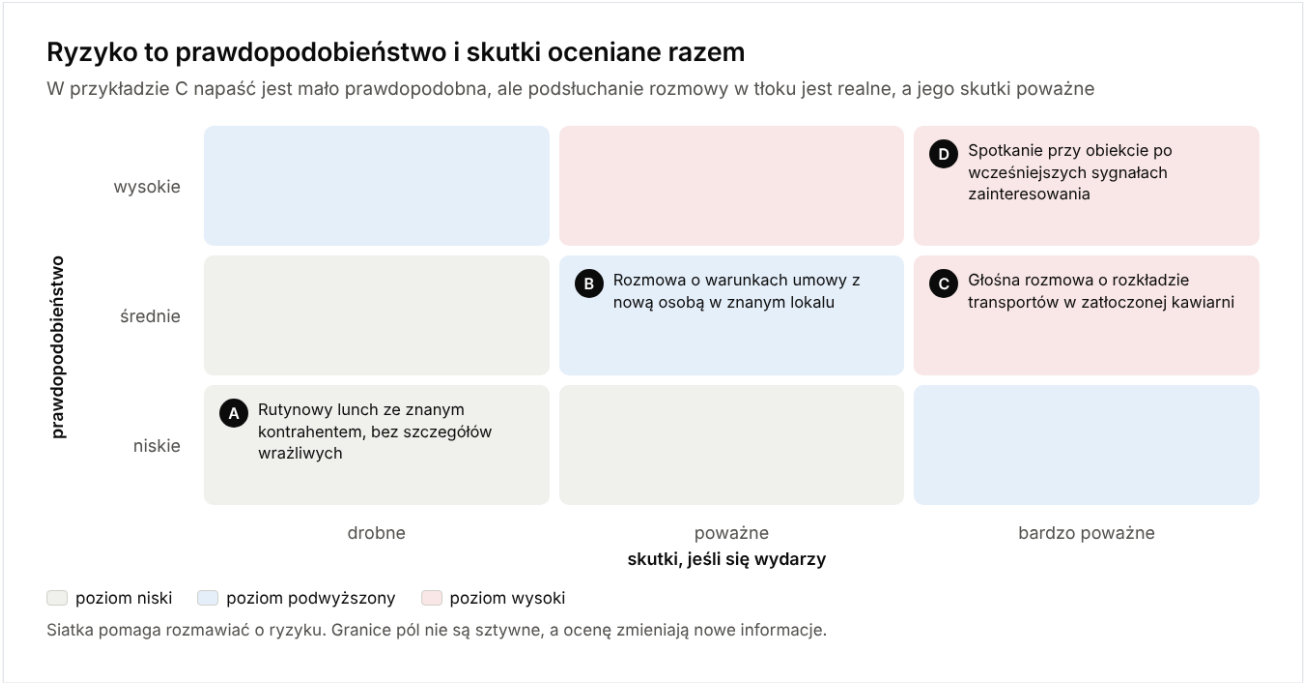
Ćwiczenie odtwarzania. Po wyjściu z kawiarni, sklepu czy pociągu spróbuj w myślach odtworzyć, kto siedział najbliżej, ile było wyjść, co miała na sobie osoba przy kasie. Na początku przypomnisz sobie niewiele. Po kilku tygodniach zauważysz, że rejestrujesz więcej bez wysiłku.

Nazywanie zamiast oceniania. Kiedy coś zwróci twoją uwagę, nazwij to opisowo („mężczyzna stoi przy wejściu od kwadransa i nie korzysta z telefonu"), a nie oceniająco („podejrzany typ"). Opis pozostawia miejsce na niewinne wyjaśnienie i jest użyteczny, gdybyś musiał komuś przekazać informację. Ocena zamyka myślenie.

Sprawdzanie niewinnych wyjaśnień. Jeśli sytuacja nie wygląda na bezpośrednie zagrożenie, dla każdej obserwacji, która cię zaniepokoiła, postaraj się znaleźć co najmniej dwa zwyczajne wyjaśnienia. Przy bezpośrednim zagrożeniu najpierw się oddalasz i wzywasz pomoc, a wyjaśnienia rozważasz dopiero w bezpiecznym miejscu. Mężczyzna przy wejściu może czekać na kogoś, może być pracownikiem ochrony w cywilu, może mieć przerwę w pracy. Jeśli zwyczajne wyjaśnienia przestają pasować do kolejnych obserwacji, dopiero wtedy masz powód do większej uwagi.

1.3. Ocena ryzyka zależna od kontekstu

Ryzyko to połączenie dwóch rzeczy: prawdopodobieństwa, że coś niepożądanego się wydarzy, i skutków, jeśli się wydarzy. Spotkanie w zatłoczonej kawiarni na rynku dużego miasta ma niskie prawdopodobieństwo napaści, ale jeśli rozmawiasz tam głośno o rozkładzie transportów, skutki podsłuchania mogą być poważne. Ocena ryzyka polega na uczciwym przyjrzeniu się obu stronom.



Rys. 7. Siatka ryzyka z przykładami spotkań · schemat poglądowy

Przed każdym spotkaniem lub wyjazdem, który wykracza poza codzienną rutynę, warto przejść przez kilka pytań. Zajmuje to dwie, trzy minuty.

Czynnik	Pytania pomocnicze	Co podnosi ryzyko
Miejsce	Czy znam to miejsce? Jaka jest okolica? Czy w pobliżu są obiekty, którymi ktoś może się interesować?	Nieznana okolica, odludzie, sąsiedztwo węzłów logistycznych, kolejowych, energetycznych, punktów zbiórki pomocy.
Czas	O której się spotykamy? Jak będę wracać?	Późna pora, słabe oświetlenie, ostatnie połączenie komunikacji.
Charakter spotkania	Czy to rutynowe spotkanie, czy coś nietypowego? Kto je zainicjował?	Spotkanie zaproponowane przez nieznaną osobę, z presją czasu, z nietypowym uzasadnieniem.
Wrażliwość informacji	Co będziemy omawiać? Co stałoby się, gdyby ktoś to usłyszał lub sfotografował?	Harmonogramy, trasy, lokalizacje, dane osobowe, warunki umów, informacje o zabezpieczeniach.
Profil uczestników	Czy ktoś z nas jest osobą publiczną? Czy nasza branża lub projekt budzi zainteresowanie?	Obronność, energetyka, logistyka, telekomunikacja, wsparcie Ukrainy, media śledcze.
Bieżąca sytuacja	Czy obowiązuje podwyższony stopień alarmowy? Czy w okolicy były ostatnio incydenty?	Wyższy stopień alarmowy, świeże incydenty, napięcie społeczne, duże wydarzenia publiczne.

Na tej podstawie można przyporządkować spotkanie lub podróż do jednego z trzech poziomów. Poziomy nie są sztywnymi kategoriami. To narzędzie, które pomaga dobrać środki do potrzeb i uniknąć zarówno lekceważenia, jak i przesady.

Poziom	Typowe sytuacje	Rozsądne środki
Niski	Rutynowe spotkanie ze znanym kontrahentem w znanym miejscu, bez omawiania szczegółów wrażliwych.	Zwykła uważność, blokada ekranu, rozsądna głośność rozmowy.
Podwyższony	Spotkanie z nową osobą, rozmowa o warunkach umowy lub danych klienta, podróż służbowa w nowe miejsce.	Weryfikacja rozmówcy, wybór lokalu z prywatnością akustyczną, informacja dla zaufanej osoby, ograniczenie szczegółów w rozmowie.
Wysoki	Rozmowa o harmonogramach transportów, lokalizacjach magazynów, zabezpieczeniach obiektów, projektach obronnych lub wsparciu Ukrainy; spotkanie w pobliżu takich obiektów; wcześniejsze sygnały niepożądanego zainteresowania.	Przeniesienie rozmowy do pomieszczenia kontrolowanego przez organizację, plan dojazdu i powrotu, godzina kontrolna z zaufaną osobą, minimalizacja dokumentów i urządzeń zabieranych na spotkanie, konsultacja z działem bezpieczeństwa.

Jeśli ocena wskazuje na poziom wysoki, pierwsze pytanie powinno brzmieć, czy rozmowa w ogóle musi odbyć się w miejscu publicznym. W większości przypadków odpowiedź jest negatywna, a najlepszym środkiem ostrożności jest zmiana formy: sala w siedzibie organizacji, zabezpieczone połączenie wideo z ustalonymi zasadami albo podział rozmowy na część ogólną w lokalu i część szczegółową w biurze.

1.4. Zwykłe zachowania i sygnały ostrzegawcze

Większość rzeczy, które w pierwszej chwili wydają się dziwne, ma zwyczajne wyjaśnienie. Ludzie fotografują budynki, bo są turystami, studentami architektury, rzeczoznawcami albo pracują dla dewelopera. Ktoś długo siedzi z laptopem, bo pracuje zdalnie. Ktoś pojawia się w tym samym miejscu dwa dni z rzędu, bo mieszka lub pracuje w okolicy. Celem tego podrozdziału nie jest nauczenie podejrzliwości, tylko pokazanie, które cechy zachowań zasługują na uwagę.

Sygnały ostrzegawcze rzadko są pojedynczymi zachowaniami. Zwykle są to zestawienia okoliczności, które razem przestają mieć sensowne wyjaśnienie. Pomocne są cztery kategorie:

Niezgodność z miejscem i rolą. Zachowanie nie pasuje do tego, co ludzie zwykle robią w danym miejscu. Klient kawiarni, który nie zamawia, nie pracuje, nie czeka na nikogo, a jedynie obserwuje wejście. Osoba w stroju roboczym, która nie wykonuje żadnej pracy, tylko fotografuje ogrodzenie i kamery.

Powtarzalność w czasie i przestrzeni. Ta sama osoba lub ten sam pojazd pojawia się w kilku miejscach związanych z tobą, w różnym czasie i w miejscach od siebie oddalonych. Pojedyncze spotkanie zwykle nie pozwala ustalić intencji drugiej osoby. Kilka niezależnych spotkań w różnych częściach miasta w ciągu tygodnia zasługuje na odnotowanie. Powtarzalność zwiększa wagę sygnału, ale nie jest warunkiem reakcji: obserwacja, która sama wskazuje na poważne zagrożenie, uzasadnia działanie lub zgłoszenie od razu.

Zainteresowanie tobą, twoimi rzeczami lub informacjami. Ktoś zbyt wnikliwie wypytuje o twoją pracę, dostęp do systemów czy harmonogram. Ktoś przysuwa się, żeby zobaczyć ekran. Ktoś zwraca uwagę na twoją teczkę albo na to, gdzie odkładasz telefon.

Zachowania przygotowawcze wobec obiektu. Fotografowanie lub filmowanie wejść, zabezpieczeń, kamer, bram wjazdowych i rozkładów ruchu zamiast fasady czy krajobrazu. Spacerowanie wzdłuż ogrodzenia bez celu. Notowanie godzin zmiany ochrony. Wypytywanie pracowników o godziny pracy, liczbę osób, dostawy. Te zachowania mają znaczenie zwłaszcza przy obiektach logistycznych, kolejowych i energetycznych.

Zwykle niewinne	Zasługuje na uwagę, zwłaszcza w zestawieniu z innymi sygnałami
Ktoś fotografuje zabytkowy dworzec	Ktoś fotografuje nastawnię, rozjazdy, kable lub szafy zasilające i odchodzi, gdy pojawia się ochrona
Ktoś siedzi długo z laptopem w kawiarni	Ktoś siedzi długo, nie korzysta z laptopa, a odwraca się w stronę twojego stolika za każdym razem, gdy zaczynasz mówić
Ta sama osoba w twoim osiedlowym sklepie dwa razy w tygodniu	Ta sama osoba w sklepie, potem przy twoim biurze, potem na dworcu w innym mieście
Ktoś pyta, gdzie pracujesz	Ktoś po krótkiej znajomości pyta o twoje uprawnienia, systemy, harmonogramy dostaw albo prosi o „drobną przysługę" związaną z pracą
Kurier pyta o drogę do magazynu	Osoba bez związku z firmą pyta pracowników o godziny zmian, liczbę ochroniarzy i rozkład kamer

Zwróć uwagę, że w prawej kolumnie nie ma żadnych cech wyglądu, wieku, języka ani pochodzenia. Ocena dotyczy zachowań i okoliczności. Podejrzliwość wobec osób z powodu ich narodowości jest niesprawiedliwa i nieskuteczna: sprawcy opisani w rozdziale o kontekście pochodzili z kilkunastu państw, w tym z Polski.

1.5. Spokój i zdolność podejmowania decyzji

W sytuacji niepokoju organizm reaguje stresem: przyspiesza tętno, zawęża się pole widzenia, myślenie upraszcza się do kilku opcji. Ta reakcja bywa przydatna przy bezpośrednim zagrożeniu, ale przeszkadza w trzeźwej ocenie niejasnych sygnałów. Kilka praktycznych sposobów pomaga utrzymać zdolność decyzyjną.

Oddech. Kilka wolnych oddechów z wydłużonym wydechem obniża pobudzenie w ciągu kilkudziesięciu sekund. Tak działa fizjologia oddychania.

Decyzje podjęte wcześniej. Najtrudniej podejmuje się decyzje pod presją, dlatego najważniejsze warto podjąć zawczasu, w formie prostych reguł „jeśli..., to...". Na przykład: „jeśli ktoś przy sąsiednim stoliku wyraźnie przysłuchuje się rozmowie, zmieniamy temat na ogólny i kończymy szczegóły w biurze" albo „jeśli po spotkaniu zobaczę tę samą osobę przy samochodzie, nie wsiadam, tylko idę do recepcji hotelu". Reguły ustalone wcześniej uruchamiają się prawie automatycznie.

Naturalne zachowanie. Ostentacyjne rozglądanie się, nerwowe sprawdzanie telefonu i nagłe zmiany kierunku przyciągają uwagę. Jeśli coś cię niepokoi, zachowuj się tak, jak zachowałbyś się, gdybyś po prostu zmienił plany: dokończ kawę, zapłać, wyjdź spokojnie. Ta rada dotyczy sytuacji bez bezpośredniego zagrożenia. Przy przemocy, pożarze lub innym nagłym niebezpieczeństwie nie zwlekasz po to, żeby zachować pozory normalności.

Konsultacja zamiast samotnej analizy. Gdy masz wątpliwości, porozmawiaj z kimś zaufanym lub z działem bezpieczeństwa. Opowiedzenie sytuacji drugiej osobie często samo w sobie porządkuje myślenie.

1.6. Plan działania na wypadek zagrożenia lub nagłej zmiany sytuacji

Plan nie musi być dokumentem. Przy niskim ryzyku wystarczy, że wiesz, jak stąd wyjść i do kogo zadzwonić. Przy podwyższonym i wysokim ryzyku warto mieć przemyślane kilka elementów, najlepiej zapisanych w notatce, którą łatwo odnaleźć.

Element planu	Na czym polega	Przykład
Zaufana osoba	Ktoś, kto wie, gdzie jesteś, z kim i do kiedy.	Współpracownik, członek rodziny, dyżurny działu bezpieczeństwa.
Godzina kontrolna	Ustalony moment, w którym dajesz znać, że wszystko w porządku. Brak sygnału uruchamia ustaloną reakcję.	„Napiszę do 20:30. Jeśli nie napiszę, dzwonisz. Jeśli nie odbieram dwa razy, dzwonisz do działu bezpieczeństwa."
Umówiony sygnał	Neutralne zdanie, które znaczy „potrzebuję pomocy" albo „nie mogę mówić swobodnie".	„Czy podlałeś już kwiaty?" w rozmowie telefonicznej.
Bezpieczne miejsca	Dwa, trzy punkty w pobliżu, w których są ludzie i personel.	Recepcja hotelu, apteka całodobowa, stacja paliw, komisariat.
Trasa i alternatywa	Sposób dotarcia i powrotu oraz wariant zapasowy.	Taksówka z aplikacji, a w razie problemów tramwaj do centrum.
Zasoby	Naładowany telefon, powerbank, karta płatnicza i niewielka ilość gotówki, dokument tożsamości.	Bateria powyżej 50 procent przed wyjściem z biura.
Kontakty alarmowe	Numer 112 oraz numery działu bezpieczeństwa i zaufanej osoby zapamiętane lub zapisane poza telefonem.	Kartka w portfelu z dwoma numerami.
Granice	Z góry ustalone sytuacje, w których kończysz spotkanie lub rezygnujesz z wyjazdu.	Zmiana miejsca spotkania w ostatniej chwili bez wyjaśnienia, prośba o przyjście samemu.

Plan sprawdza się wtedy, gdy jest prosty. Jeśli masz go w głowie w formie kilku zdań, zadziała. Jeśli wymaga zaglądania do instrukcji, w stresie prawdopodobnie zostanie pominięty.

Na koniec uwaga o rodzinie i bliskich. Osoby, z którymi mieszkasz, nie muszą znać szczegółów twojej pracy, ale powinny wiedzieć, jak się z tobą skontaktować, kogo powiadomić, jeśli nie wrócisz o ustalonej porze, i jak zareagować, gdyby ktoś obcy wypytywał je o ciebie. Tej ostatniej kwestii poświęcony jest rozdział 10.

2.

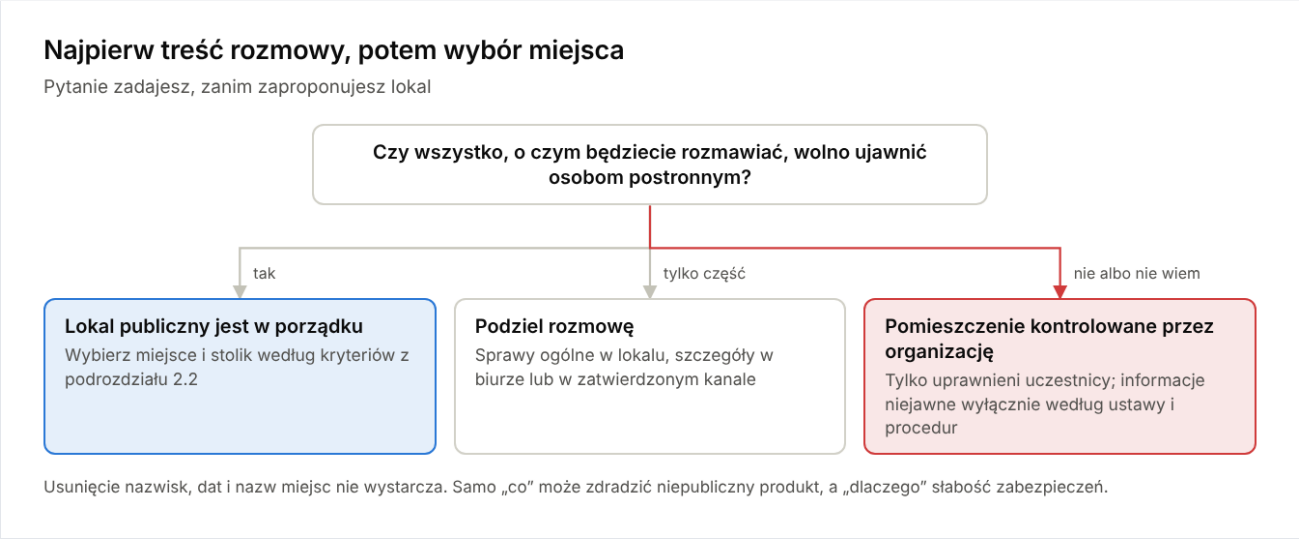
Wybór lokalu i miejsca spotkania

Największy wpływ na poufność rozmowy w przestrzeni publicznej ma decyzja podjęta przed spotkaniem: gdzie się spotkać. Dobrze wybrany lokal sprawia, że wiele środków ostrożności staje się zbędnych. Źle wybrany sprawia, że żadne środki nie pomogą. Ten rozdział opisuje kryteria wyboru, typowe błędy i miejsca, w których ryzyko rośnie z powodu sąsiedztwa.

2.1. Najpierw pytanie, czy lokal publiczny to właściwe miejsce

Zanim wybierzesz restaurację, odpowiedz sobie, co będzie przedmiotem rozmowy. Jeśli omawiane będą informacje niejawne, szczegóły zabezpieczeń obiektów, dokładne harmonogramy transportów albo dane osobowe wielu osób, żaden lokal publiczny nie zapewni wystarczającej ochrony. Właściwym miejscem jest pomieszczenie kontrolowane przez twoją organizację lub organizację rozmówcy.

Lokal publiczny dobrze sprawdza się w rozmowach wstępnych, w budowaniu relacji, w omawianiu kierunków współpracy i spraw, których ujawnienie byłoby niezręczne, ale nie szkodliwe. Dobrym kompromisem jest podział: ogólna część w lokalu, szczegóły w biurze lub w zabezpieczonym kanale.



Rys. 8. Decyzja o miejscu rozmowy zaczyna się od jej treści

2.2. Kryteria oceny lokalu

Poniższe kryteria dotyczą każdego rodzaju miejsca. Żadne nie jest rozstrzygające samo w sobie. Lokal idealny pod każdym względem zdarza się rzadko, dlatego chodzi o świadomy wybór kompromisu.

Natężenie ruchu i hałasu. Umiarkowany gwar jest sprzymierzeńcem poufności, bo maskuje rozmowę przed osobami siedzącymi kilka stolików dalej. Cisza działa odwrotnie: w pustej kawiarni każde słowo słychać w całym pomieszczeniu. Bardzo głośna muzyka też nie pomaga, bo zmusza rozmówców do podnoszenia głosu i nachylania się, a to przyciąga uwagę.

Prywatność akustyczna. Liczy się odległość od sąsiednich stolików, obecność przegród, kształt sali i miejsce, w którym zwykle stoi obsługa. Stoliki ustawione gęsto wzdłuż jednej ściany oznaczają, że osoba obok słyszy praktycznie wszystko. Loże z wysokimi oparciami poprawiają sytuację, ale nie eliminują jej, bo dźwięk przenosi się nad oparciem.

Rozmieszczenie stolików i ruch obsługi. Stolik przy przejściu do kuchni lub toalety oznacza, że co chwilę ktoś przechodzi obok i może zerknąć na stół. Stolik przy barze oznacza, że barman słyszy fragmenty rozmowy przez cały czas.

Widoczność wejść i wyjść. Dobrze jest siedzieć tak, żeby widzieć wejście i mieć dostęp do drugiego wyjścia. Nie chodzi o filmową czujność, tylko o to, żebyś zauważył, kto wchodzi, i mógł spokojnie wyjść, gdyby zaszła potrzeba.

Oświetlenie. Dobre oświetlenie wnętrza i otoczenia lokalu ułatwia orientację i zniechęca do drobnej przestępczości. Wieczorem ma znaczenie także oświetlenie drogi do parkingu lub przystanku.

Monitoring w lokalu. Kamery nad kasą lub salą rejestrują obraz, czasem w wysokiej rozdzielczości. Ekran laptopa i rozłożone dokumenty mogą zostać utrwalone na nagraniu, do którego dostęp ma personel, firma ochroniarska i potencjalnie osoby nieuprawnione. Usiądź tak, żeby ekran i dokumenty były zwrócone do ściany, a nie w stronę kamery.

Przechowywanie rzeczy. Sprawdź, czy przy stoliku jest miejsce na torbę i laptopa tak, żeby pozostawały w zasięgu ręki. Szatnia jest wygodna, ale oznacza, że kurtka z telefonem lub kluczami jest poza twoją kontrolą. Wieszaki przy wejściu są najgorszą opcją.

Ryzyko pozostawienia rzeczy bez nadzoru. Każde wyjście do toalety to moment, w którym na stole zostają dokumenty i urządzenia. Jeśli spotykasz się w dwie osoby, ustalcie, że jedna zawsze zostaje przy stole, a dokumenty wędrują do torby przed każdym odejściem.

Rezerwacja i ślady w systemach. Rezerwacja na nazwisko z numerem telefonu i opisem „spotkanie zarządu firmy X w sprawie projektu Y" zostawia informację w systemie lokalu i w skrzynce mailowej. Rezerwuj na imię, bez nazwy firmy i celu spotkania.

Wi-Fi lokalu. Darmowa sieć jest wygodna, a poprawnie działające szyfrowanie (HTTPS) chroni w niej treść komunikacji. Głównym ryzykiem są fałszywe strony logowania, a to, czy wolno w niej pracować na danych służbowych, określa polityka organizacji. Szczegóły w rozdziale 8.

Dojazd i powrót. Dostępność komunikacji, parking w widocznym i oświetlonym miejscu, możliwość zamówienia taksówki pod drzwi. Spotkanie, po którym musisz iść kilkaset metrów pustą ulicą do samochodu, ma słabszy punkt na końcu.

2.3. Porównanie typów miejsc

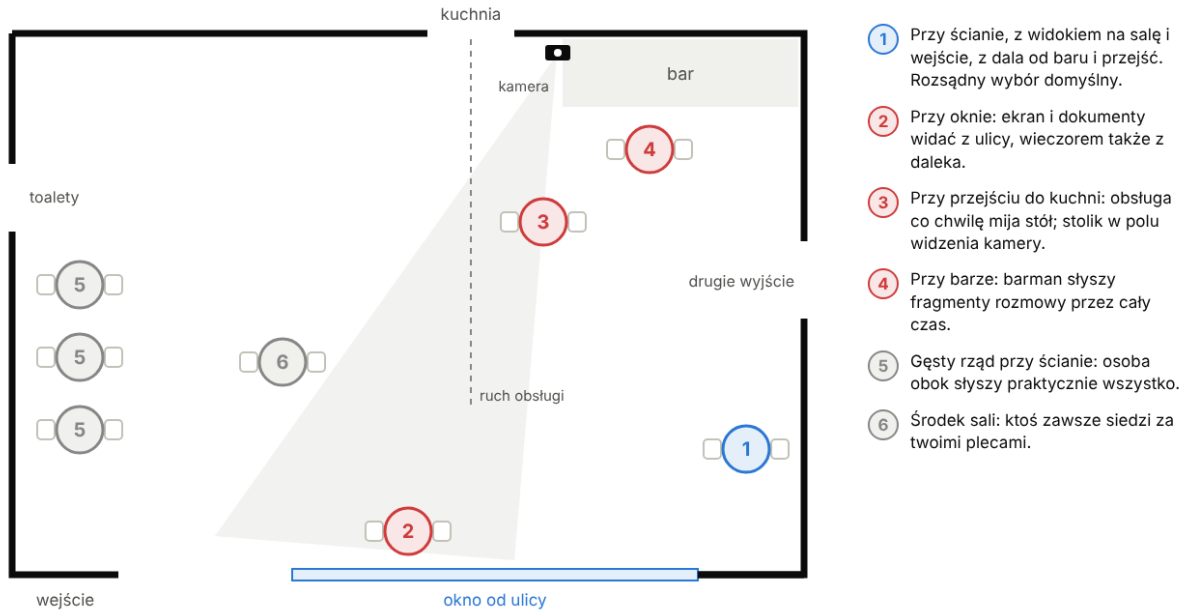
Miejsce	Mocne strony	Słabe strony	Dobre dla poziomu ryzyka
Restauracja w porze lunchu	Naturalny gwar, długi czas spotkania nie budzi zdziwienia, obsługa i inni goście.	Gęste stoliki, częste wizyty kelnera, rezerwacja na nazwisko.	Niski, podwyższony przy dobrym stoliku
Kawiarnia sieciowa	Anonimowość, rotacja gości, łatwość zmiany miejsca.	Często ciasno, dużo osób pracujących na laptopach w zasięgu słuchu, kamery.	Niski
Lobby hotelowe	Duża przestrzeń, rozstawione fotele, obecność recepcji i ochrony, możliwość wynajęcia sali na godzinę.	Ruch osób z bagażami, możliwość długiego przebywania bez zwracania uwagi także dla obserwatorów.	Niski i podwyższony
Sala konferencyjna wynajęta na godziny (hotel, centrum biznesowe)	Zamknięte drzwi, kontrola nad tym, kto wchodzi.	Dane w systemie rezerwacji, cienkie ściany w niektórych obiektach, czasem obecność technika.	Podwyższony
Coworking	Infrastruktura biurowa, często budki do rozmów.	Wielu ludzi pracujących w tej samej branży, budki nie zawsze są dźwiękoszczelne, wspólne drukarki.	Niski i podwyższony
Spacer w parku	Brak kamer lokalu, łatwo ocenić, kto jest w pobliżu.	Pogoda, brak miejsca na dokumenty, wieczorem słabe oświetlenie, w odludnych miejscach ryzyko dla bezpieczeństwa fizycznego.	Rozmowy bez dokumentów, w dzień
Samochód	Prywatność od osób postronnych.	Brak świadków przy spotkaniu z nową osobą, nie wiadomo, co jest w pojeździe, trudność wyjścia.	Tylko ze znanymi osobami
Pociąg, samolot, poczekalnia	Wygodne, bo i tak spędzasz tam czas.	Rozmowy i ekrany widoczne dla wielu osób, brak możliwości zmiany miejsca.	Nie do rozmów o sprawach wrażliwych

2.4. Stolik przy ścianie, sala obok, róg sali: kiedy to ma sens

Stolik przy ścianie z widokiem na salę ma kilka zalet. Nikt nie siedzi za twoimi plecami i nie widzi ekranu ani dokumentów. Widzisz wejście. Liczba osób w zasięgu słuchu jest mniejsza, bo z jednej strony jest ściana. To rozsądny domyślny wybór.

Gdzie usiąść: ten sam lokal, różne poziomy prywatności

Szkic poglądowy. Szary klin to pole widzenia kamery nad barem, linia przerywana to trasa obsługi z kuchni



Rys. 9. Wybór stolika a prywatność rozmowy · szkic poglądowy sali

Są jednak sytuacje, w których pozorna dyskrecja wprowadza w błąd.

Osobna sala lub gabinet. Daje poczucie prywatności, ale w pustym, cichym pomieszczeniu głos niesie się przez drzwi i przepierzenia. Kelner wchodzi bez pukania. Rezerwacja osobnej sali jest zwykle imienna i bardziej zapamiętywana przez personel. Osobna sala ma sens, gdy jest naprawdę oddzielona od reszty lokalu i gdy rozmowa toczy się normalnym, spokojnym tonem.

Róg sali przy cienkiej ściance. Lekka przegroda może nie zapewniać wystarczającej izolacyjności akustycznej; nie zakładaj poufności bez oceny pomieszczenia. Za przegrodą może siedzieć osoba, której nie widzisz.

Pusty lokal. Brak innych gości wydaje się bezpieczny, a w praktyce oznacza, że personel słyszy wszystko, a każda osoba, która wejdzie, będzie siedziała blisko.

Stolik przy oknie. Dobrze widać ulicę, ale z ulicy dobrze widać ciebie i stół. Laptop zwrócony ekranem do okna jest czytelny dla przechodniów, a w niektórych warunkach oświetlenia także z większej odległości.

Ogródek letni. Hałas uliczny maskuje rozmowę, ale ludzie przechodzą tuż obok stolików, a torba na krześle obok jest łatwym łupem.

2.5. Zmienność miejsc

Jeśli regularnie spotykasz się z tymi samymi osobami w sprawach o podwyższonej wrażliwości, unikaj jednego stałego lokalu. Nie chodzi o ciągłe zmiany, tylko o to, żeby twoja obecność w danym miejscu o danej porze nie była przewidywalna dla osób z zewnątrz. Rotacja kilku sprawdzonych miejsc wystarczy. Więcej o przewidywalności w rozdziale 10.

2.6. Lokale w pobliżu obiektów infrastruktury, logistyki i pomocy dla Ukrainy

Lokale położone blisko centrów logistycznych, węzłów kolejowych, lotnisk cargo, rozdzielni i elektrowni, terminali paliwowych, jednostek wojskowych czy magazynów pomocy humanitarnej wymagają dodatkowej rozwagi z kilku powodów.

Po pierwsze, takie miejsca są naturalnym punktem obserwacyjnym. Według ABW rosyjskie służby prowadziły w Polsce rozpoznanie obiektów na masową skalę, a zadania jednorazowych wykonawców często polegały na fotografowaniu i opisywaniu ruchu. Kawiarnia z widokiem na bramę magazynu jest wygodnym miejscem dla kogoś, kto liczy ciężarówki.

Po drugie, w takich lokalach bywają pracownicy obiektu. Rozmowy przy kawie o tym, kiedy przyjeżdża następny transport, ile osób jest na zmianie i co się psuje w systemie zabezpieczeń, są tam słyszalne dla każdego.

Po trzecie, przy podwyższonych stopniach alarmowych służby i ochrona obiektów zwracają większą uwagę na osoby przebywające w pobliżu. Twoje zachowanie, nawet niewinne, może zostać zauważone i zweryfikowane. To nie jest powód do niepokoju, ale argument za tym, żeby nie fotografować obiektu i nie rozkładać na stole planów logistycznych.

Praktyczne zalecenia:

- nie wybieraj lokalu z widokiem na obiekt, o którym rozmawiasz, ani lokalu, w którym bywają jego pracownicy,
- jeśli pracujesz w takim obiekcie, nie omawiaj spraw służbowych w pobliskich lokalach, sklepach i na przystankach,
- zalecenie ostrożnościowe: nie fotografuj obiektu, nawet przypadkowo, i nie publikuj zdjęć zrobionych w jego pobliżu z oznaczeniem lokalizacji,
- zwróć uwagę, czy w lokalu nie ma osób, które przez dłuższy czas obserwują wjazd, notują lub fotografują ruch, a jeśli takie zachowanie powtarza się, poinformuj ochronę obiektu lub zgłoś to zgodnie z rozdziałem 6,
- przy spotkaniach z kontrahentami z branży logistycznej czy energetycznej wybierz miejsce oddalone od obiektów, nawet jeśli to mniej wygodne.

2.7. Lista kontrolna oceny lokalu przed spotkaniem

Poniższą listę można przejść w pamięci w kilka minut albo, przy spotkaniach o wysokim poziomie ryzyka, sprawdzić lokal dzień wcześniej.

- ☐ Rodzaj rozmowy pasuje do miejsca publicznego (lub szczegóły przeniesiemy do biura).
- ☐ Znam lokal lub sprawdziłem jego układ (zdjęcia, plan, wcześniejsza wizyta).
- ☐ W porze spotkania panuje umiarkowany gwar, nie cisza ani bardzo głośna muzyka.
- ☐ Jest stolik z dala od przejść, baru i wejścia do kuchni, z widokiem na wejście.
- ☐ Ekran i dokumenty da się ustawić tyłem do kamer, okien i przejść.
- ☐ Rzeczy zmieszczą się w zasięgu ręki, bez oddawania do szatni.
- ☐ Znam drogę wyjścia i alternatywną, jeśli istnieje.
- ☐ Rezerwacja (jeśli potrzebna) jest na imię, bez nazwy firmy i celu spotkania.
- ☐ Dojazd i powrót są proste, parking lub przystanek są oświetlone.

- ☐ Lokal nie sąsiaduje z obiektem, o którym będziemy rozmawiać, i nie jest miejscem, w którym bywają jego pracownicy.
- ☐ Nie korzystam z tego samego lokalu przy każdym spotkaniu z tą osobą w sprawach wrażliwych.
- ☐ Wiem, dokąd pójdę, jeśli lokal okaże się nieodpowiedni (lokal zapasowy).

3.

Ocena otoczenia przed wejściem

Wstępna ocena miejsca trwa od kilku minut przy rutynowym spotkaniu do kwadransa przy spotkaniu o wysokim poziomie ryzyka. Opiera się wyłącznie na informacjach publicznie dostępnych i na tym, co widzisz, podchodząc do lokalu. Jej celem jest wyłapanie oczywistych problemów, zanim usiądziesz przy stole, a nie przeprowadzenie dochodzenia.

3.1. Przygotowanie zdalne

Większość informacji o miejscu można zebrać przed wyjściem z biura. To, co sprawdzasz, zależy od poziomu ryzyka.

Co sprawdzić	Gdzie	Po co
Dokładny adres i położenie wejścia	Mapy internetowe, widok ulicy, strona lokalu	Żeby nie szukać wejścia na miejscu i nie krążyć po okolicy.
Godziny otwarcia i typowy tłok w porze spotkania	Strona lokalu, informacje o popularności w mapach	Żeby nie trafić na pustą salę ani na tłum.
Dojazd, parking, przystanki	Mapy, rozkłady jazdy	Żeby zaplanować powrót, zwłaszcza wieczorem.
Najbliższe bezpieczne miejsca	Mapy	Recepcja hotelu, apteka, stacja paliw, komisariat, szpitalny oddział ratunkowy.
Wydarzenia w okolicy	Lokalne media, strona urzędu miasta, komunikaty policji	Demonstracje, mecze, imprezy masowe, utrudnienia drogowe, zamknięte ulice.
Sąsiedztwo obiektów infrastruktury	Mapy	Węzły kolejowe, centra logistyczne, obiekty wojskowe i energetyczne w pobliżu (rozdział 2.6).
Aktualne alerty	Alerty RCB, komunikaty wojewody, stopień alarmowy	Żeby wiedzieć, czy w regionie obowiązują szczególne środki.

Korzystanie z map, widoku ulicy i publicznych stron jest w pełni legalne. Nie fotografuj natomiast obiektów oznaczonych znakiem zakazu fotografowania (szczegóły w aneksie A) i nie wykonuj nagrań okolicy obiektów infrastruktury tylko po to, żeby „zobaczyć, jak tam jest". Nawet przy niewinnych intencjach takie zachowanie może zostać odebrane jako rozpoznanie i wymagać wyjaśnienia, zwłaszcza gdy dotyczy zabezpieczeń lub elementów technicznych obiektu.

Z tego samego powodu nie używaj dronów do oglądania okolicy przed spotkaniem. Loty w pobliżu infrastruktury krytycznej, lotnisk i obiektów wojskowych podlegają ograniczeniom, a samo pojawienie się drona nad takim obiektem w obecnej sytuacji uruchamia reakcję służb.

3.2. Podejście do miejsca

Przyjdź kilka minut przed czasem. Daje to możliwość spokojnego wyboru stolika i przyjrzenia się okolicy bez pośpiechu. Osoba, która wpada spóźniona, zajmuje pierwsze wolne miejsce i od razu wyciąga dokumenty, nie ma żadnej przestrzeni na ocenę.

Podchodząc do lokalu, zwróć uwagę na kilka rzeczy. Nie wymaga to zatrzymywania się ani rozglądania. Wystarczy, że idziesz z podniesionym wzrokiem.

- Jak wygląda ruch pieszych i samochodów. Czy odpowiada porze dnia i charakterowi ulicy.
- Czy wejście jest dobrze oświetlone i widoczne z ulicy.
- Czy przy wejściu nie ma zbiegowiska, awantury, osób, które zaczepiają przechodniów.
- Czy na zewnątrz jest wyraźna obecność służb lub ochrony, która może sugerować wcześniejszy incydent.
- Jak wygląda droga, którą będziesz wracać, zwłaszcza jeśli to będzie po zmroku.

Po wejściu poświęć kilkanaście sekund na określenie normy miejsca (rozdział 1.2): jak głośno jest, ile osób siedzi, gdzie stoi obsługa, gdzie są kamery, gdzie jest wyjście oraz alternatywna droga opuszczenia miejsca, jeśli istnieje. Następnie wybierz stolik według kryteriów z rozdziału 2.

3.3. Rozsądna obserwacja i doszukiwanie się zagrożeń

Granica między rozsądną obserwacją a doszukiwaniem się zagrożeń przebiega w dwóch miejscach. Pierwsze to cel: obserwujesz po to, żeby podjąć decyzję (czy tu zostać, gdzie usiąść), a nie po to, żeby udowodnić sobie, że coś jest nie tak. Drugie to zachowanie: rozsądna obserwacja jest niewidoczna dla innych, doszukiwanie się zagrożeń zwykle widać.

Rozsądna obserwacja	Doszukiwanie się zagrożeń
Zauważasz wyjścia i układ sali przy wejściu.	Co minutę odwracasz się w stronę drzwi.
Rejestrujesz, że ktoś przy sąsiednim stoliku nie rozmawia i nie pracuje.	Uznajesz go za obserwatora i zaczynasz go fotografować.
Zmieniasz stolik, bo obok jest za blisko.	Wypytujesz kelnera, kim jest osoba przy oknie.
Odnotowujesz w pamięci samochód z pracującym silnikiem przed lokalem.	Spisujesz numery wszystkich samochodów na ulicy.
Po spotkaniu zapisujesz kilka faktów, jeśli coś się powtórzyło.	Prowadzisz rejestr wszystkich osób, które widziałeś w ciągu dnia.
Pytasz rozmówcę, czy nie woli usiąść gdzie indziej.	Wyjaśniasz rozmówcy, że „chyba ktoś nas obserwuje", bez żadnych podstaw.

W prawej kolumnie są zachowania, które mają trzy wady. Przyciągają uwagę do ciebie. Mogą naruszać prawa innych osób, np. prawo do wizerunku. Wreszcie wyczerpują cię i pogarszają jakość decyzji w sytuacji, gdy pojawi się rzeczywisty sygnał.

3.4. Kiedy zmienić miejsce

Zmiana miejsca jest normalnym, codziennym zachowaniem. Ludzie przesiadają się, bo jest przeciąg, bo jest za głośno, bo stolik się chwieje. Nikt nie oczekuje wyjaśnień. Warto korzystać z tej swobody, zamiast tłumaczyć sobie, że „jakoś to będzie".

Zmień stolik, gdy:

- przy sąsiednim stoliku siedzi ktoś na tyle blisko, że słyszy rozmowę, a lokal ma wolne miejsca dalej,
- twoje miejsce jest pod kamerą, przy oknie lub przy przejściu i nie da się ustawić ekranu i dokumentów bezpiecznie,
- po wejściu zauważysz, że przy stoliku obok usiadła osoba, która wcześniej pojawiła się w innym miejscu związanym z tobą.

Zmień lokal, gdy:

- jest znacznie bardziej zatłoczony lub znacznie bardziej pusty, niż zakładałeś, i nie ma dobrego miejsca,
- przed wejściem lub w środku trwa awantura, interwencja, impreza zamknięta,
- lokal okazał się położony bezpośrednio przy obiekcie, o którym będziecie rozmawiać,
- coś w zachowaniu personelu lub innych gości budzi twój konkretny niepokój, którego nie potrafisz rozwiać.

Najprostszym sposobem jest zaproponowanie rozmówcy wcześniej przygotowanego lokalu zapasowego: „Tu jest dziś głośno, obok jest spokojniejsza kawiarnia, przejdziemy?". Nie trzeba podawać innego powodu.

3.5. Kiedy zrezygnować ze spotkania

Rezygnacja ze spotkania jest decyzją poważniejszą, ale czasem właściwą. Rozważ ją, gdy:

- rozmówca w ostatniej chwili zmienia miejsce na mniej publiczne (mieszkanie, samochód, odludny parking, teren zamkniętego obiektu) bez przekonującego uzasadnienia,
- jesteś proszony o przyjście samemu, bez telefonu, bez informowania kogokolwiek,
- w drodze lub przy lokalu zauważasz sygnały, które razem z wcześniejszymi obserwacjami tworzą spójny, niepokojący obraz,
- w okolicy trwa incydent bezpieczeństwa (alarm bombowy, akcja służb, pożar),
- czujesz, że nie jesteś w stanie prowadzić rozmowy spokojnie i z kontrolą nad tym, co mówisz.

Rezygnację najlepiej zakomunikować krótko i neutralnie, bez wchodzenia w szczegóły: „Coś mi wypadło, przełóżmy na przyszły tydzień, zaproponuję termin". Nie musisz uzasadniać decyzji podyktowanej bezpieczeństwem. Jeśli rezygnacja wynika z niepokojących sygnałów, potraktuj ją jako początek procedury z rozdziału 6: oddal się do bezpiecznego miejsca, poinformuj zaufaną osobę, zapisz fakty.

3.6. Spotkania w miejscach wskazanych przez rozmówcę

Gdy miejsce wybiera druga strona, a ty go nie znasz, zastosuj przygotowanie zdalne z tabeli w podrozdziale 3.1. Zwróć uwagę zwłaszcza na:

- czy miejsce w ogóle istnieje i jest czynne o tej porze,
- czy to rzeczywiście lokal publiczny, a nie np. biuro firmy, której nie znasz, lub mieszkanie,

- czy wybór miejsca ma sensowne uzasadnienie (blisko biura rozmówcy, po drodze, znany lokal),
- czy miejsce nie jest położone przy obiekcie, o którym będziecie rozmawiać.

Jeśli coś budzi wątpliwości, zaproponuj własne miejsce. Zwykle nikt nie ma nic przeciwko, a niechęć do zmiany jest sama w sobie informacją. Więcej o spotkaniach z nieznanymi osobami w rozdziale 9.

4.

Rozpoznawanie możliwego śledzenia i niepożądanej uwagi

Pojedyncze spotkanie tej samej osoby w dwóch miejscach niczego nie dowodzi, a część sytuacji, które w pierwszej chwili wyglądają na obserwację, ma zwyczajne wyjaśnienie. Ten rozdział uczy, jak oceniać takie sytuacje w szerszym kontekście, jak dokumentować fakty i jak reagować tak, żeby nie eskalować sytuacji i nie narażać siebie. Nie uczy natomiast technik wykrywania ani „gubienia" obserwacji. To domena służb i wyspecjalizowanych zespołów ochrony, a amatorskie próby w tym zakresie są nieskuteczne i mogą być niebezpieczne.

4.1. Spektrum niepożądanej uwagi

Niepożądana uwaga ma różne źródła i różną wagę. Rozpoznanie, z czym masz do czynienia, pomaga dobrać reakcję.

Rodzaj	Typowe przejawy	Typowa reakcja
Ciekawość, nietakt	Ktoś zerka na ekran w pociągu, przysłuchuje się rozmowie z nudów.	Zmiana miejsca, ograniczenie szczegółów.
Nachalność, natręctwo	Ktoś nawiązuje rozmowę, której nie chcesz, wraca, dosiada się.	Uprzejma, stanowcza odmowa, zmiana miejsca, w razie potrzeby obsługa lub ochrona lokalu.
Uporczywe nękanie	Ta sama osoba pojawia się wielokrotnie w miejscach związanych z twoim życiem, kontaktuje się wbrew twojej woli.	Dokumentowanie, zgłoszenie na policję. Uporczywe nękanie jest przestępstwem z art. 190a Kodeksu karnego.
Zbieranie informacji o tobie lub twojej pracy	Pytania o projekty, dostęp, harmonogramy, współpracowników; próby zbliżenia się do rozmów i dokumentów.	Ograniczenie informacji, zgłoszenie do działu bezpieczeństwa, a przy sygnałach działania obcych służb do ABW.
Rozpoznanie obiektu	Fotografowanie zabezpieczeń, wjazdów, kamer; notowanie ruchu; wypytywanie pracowników.	Zgłoszenie ochronie obiektu, przy infrastrukturze krytycznej także policji lub ABW.
Kontakt werbunkowy	Oferta zarobku za proste zadanie, prośba o przysługę związaną z pracą.	Brak odpowiedzi na zlecenie, zabezpieczenie korespondencji, zgłoszenie (podrozdział 4.9).

Zwróć uwagę, że tylko część tych sytuacji ma związek z obcymi służbami. Znacznie częściej źródłem niepożądanej uwagi są konkurencja biznesowa, wierzyciele, byli partnerzy, dziennikarze, przestępcy szukający okazji. Reakcja na wszystkie jest podobna: nie konfrontujesz, dokumentujesz, informujesz właściwy podmiot.

4.2. Dlaczego zbieg okoliczności nie jest dowodem

Ludzie mają rutyny. Mieszkają, pracują i robią zakupy w tych samych okolicach co ty. Jeśli codziennie o 8:15 wsiadasz do tego samego tramwaju, to codziennie o 8:15 widzisz te same twarze. Jeśli w porze lunchu chodzisz do dwóch, trzech lokali w okolicy biura, to w tych samych lokalach jedzą ludzie z sąsiednich biurowców. Spotkanie tej samej osoby kilka razy w tygodniu w takim kontekście jest statystycznie oczekiwane.

Do tego dochodzą dwa mechanizmy psychologiczne. Pierwszy to skłonność do potwierdzania: gdy raz zaczniesz podejrzewać, że ktoś cię obserwuje, każda kolejna obserwacja wydaje się to potwierdzać, a te, które nie pasują, umykają uwadze. Drugi to dostrzeganie wzorów tam, gdzie ich nie ma: mózg szuka porządku w przypadkowych zdarzeniach. Oba są naturalne i oba prowadzą do błędnych wniosków, jeśli nie przeciwdziała się im świadomie.

Praktyczne zabezpieczenia przed tymi błędami:

- zapisuj obserwacje na bieżąco, zamiast odtwarzać je z pamięci po kilku dniach, bo pamięć dopasowuje się do hipotezy,
- dla każdej obserwacji szukaj zwyczajnych wyjaśnień (rozdział 1.2),
- zapisuj także sytuacje, w których spodziewałeś się kogoś zobaczyć, a go nie było,
- przed wyciągnięciem wniosków porozmawiaj z kimś, kto spojrzy na fakty z dystansu.

4.3. Ocena powtarzalności w szerszym kontekście

Sygnał staje się istotny, gdy powtarzalności nie da się wyjaśnić wspólną rutyną. Pomocne są cztery pytania.

Czy miejsca są ze sobą powiązane tylko przez ciebie? Ta sama osoba w twoim biurowcu i w lokalu obok to normalne. Ta sama osoba w twoim biurowcu, na dworcu w innym mieście, w którym byłeś na spotkaniu, i pod twoim domem to coś innego.

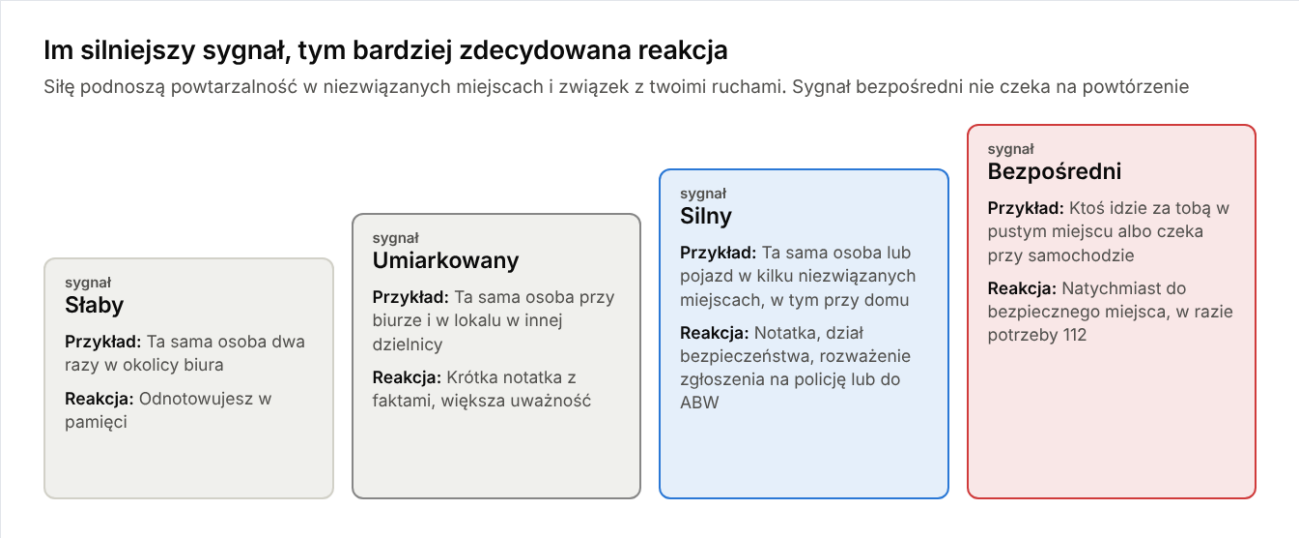
Czy odstępy czasu i przestrzeni są nietypowe? Kilka spotkań w ciągu jednego dnia w różnych dzielnicach albo w różnych miastach w ciągu tygodnia trudno wyjaśnić przypadkiem.

Czy zachowanie osoby jest związane z twoim zachowaniem? Na przykład ktoś wychodzi z lokalu chwilę po tobie, zatrzymuje się, gdy ty się zatrzymujesz, albo przestaje rozmawiać przez telefon, gdy ty zaczynasz mówić. Pojedyncza taka sytuacja może być przypadkiem. Kilka w różnych miejscach zasługuje na uwagę.

Czy jest związek z czymś, co robisz zawodowo? Pojawienie się tej samej osoby w okolicy kilku spotkań dotyczących tego samego wrażliwego projektu waży więcej niż spotkania przy codziennych sprawach.

Siła sygnału	Przykład	Co robisz
Słaby	Ta sama osoba dwa razy w okolicy biura.	Nic poza odnotowaniem w pamięci.

Siła sygnału	Przykład	Co robisz
Umiarkowany	Ta sama osoba w okolicy biura i w lokalu w innej dzielnicy, w którym byłeś na spotkaniu.	Krótka notatka z faktami, większa uważność w kolejnych dniach.
Silny	Ta sama osoba lub pojazd w kilku niezwiązanych miejscach w ciągu kilku dni, w tym w pobliżu domu lub wrażliwego spotkania; albo zachowanie wyraźnie związane z twoimi ruchami.	Notatka, rozmowa z działem bezpieczeństwa lub zaufaną osobą, rozważenie zgłoszenia na policję lub do ABW.
Bezpośredni	Ktoś idzie za tobą w pustym miejscu, zbliża się agresywnie, czeka przy samochodzie lub drzwiach.	Natychmiastowe przejście do bezpiecznego miejsca publicznego, w razie potrzeby 112.



Rys. 10. Siła sygnału i odpowiadająca jej reakcja · na podstawie tabeli w podrozdziale 4.3

4.4. Jak prowadzić notatki

Notatka ma utrwalić fakty, zanim pamięć je zniekształci. Ma być krótka, rzeczowa i sporządzona po odzyskaniu bezpieczeństwa, nie w trakcie sytuacji. Wzór w aneksie C.

Co zapisywać:

- datę, godzinę (możliwie dokładnie) i miejsce,
- opis osoby: cechy trwałe, które trudno zmienić (wzrost, budowa ciała, sposób poruszania się, znaki szczególne), a dopiero potem ubiór,
- opis pojazdu, jeśli występuje: rodzaj, kolor, marka, numer rejestracyjny, jeśli zauważyłeś go bez wysiłku,
- co dokładnie dana osoba robiła, opisowo, bez interpretacji,
- gdzie byłeś ty i co robiłeś,
- czy byli świadkowie i kto to był,
- co zrobiłeś w reakcji.

Czego unikać:

- spekulacji i ocen („na pewno agent", „wyglądał podejrzanie"),

- fotografowania osób z bliska, zwłaszcza w sposób jawny i prowokujący, oraz publikowania ich wizerunku w internecie (rozpowszechnianie wizerunku wymaga odrębnej oceny prawnej i może zaszkodzić niewinnemu człowiekowi),
- chodzenia za osobą, żeby „sprawdzić", dokąd idzie,
- przechowywania notatek w miejscu, do którego dostęp mają osoby postronne, w tym w ogólnodostępnych folderach i prywatnych chmurach.

Jeśli zdjęcie lub nagranie powstało przypadkiem, w bezpiecznych okolicznościach, nie kasuj go, ale też nie rozpowszechniaj. Przekaż je organowi, któremu zgłaszasz sprawę.

Przykład notatki: fakty osobno, oceny osobno

Wzór z aneksu C wypełniony na podstawie scenariusza 3 (dane fikcyjne). Opis zaczyna się od cech trwałych, a dopiero potem od ubioru

FAKTY

Sporządzono	piątek, 19:40, w domu
Zdarzenie	piątek ok. 11:20–11:30, hala kas dworca w mieście, do którego pojechałem na spotkanie
Co robiłem	stałem w kolejce do kasy, sam
Co zauważyłem	mężczyzna stał ok. 3 m ode mnie przy automacie biletowym, nie kupił biletu; wyszedł z hali około minuty po mnie
Cechy trwałe	ok. 185 cm, szczupły, krótkie ciemne włosy, lekko utyka na prawą nogę
Ubiór, przedmioty	czerwona kurtka, szary plecak
Wcześniej	pon. ok. 7:30, stacja paliw obok magazynu, patrzył na bramę; śr. ok. 19:00, kawiarnia na moim osiedlu
Reakcja	przeszedłem do poczekalni z ochroną, o 11:35 zadzwoniłem do działu bezpieczeństwa

OCENY

Moja ocena	to prawdopodobnie ta sama osoba; jej zamiarów nie znam
Poziom pewności	prawdopodobne (cechy trwałe pasują w dwóch z trzech obserwacji)
Zwyczajne wyjaśnienia	mieszka na moim osiedlu i pracuje przy magazynie; podróż przypadkowa; pomyłka, bo czerwona kurtka to cecha częsta
Propozycja	omówić z działem bezpieczeństwa; poprosić ochronę magazynu o uwagę na bramę

Czego tu nie ma: „na pewno agent", „wyglądał podejrzanie", zdjęć zrobionych z bliska, domysłów w miejscu luk w pamięci.

Rys. 11. Przykład notatki z incydentu wypełnionej według wzoru z aneksu C · dane fikcyjne

4.5. Reakcja bez eskalacji

Celem reakcji jest odzyskanie bezpieczeństwa i kontroli, a nie ustalenie, kim jest obserwujący. Zasady:

Nie dawaj znać, że coś zauważyłeś. Nie wpatruj się, nie fotografuj ostentacyjnie, nie zatrzymuj się nagle, żeby „zobaczyć, co zrobi". Jeśli to przypadek, nic nie tracisz. Jeśli nie, nie prowokujesz.

Kieruj się do miejsc z ludźmi. Recepcja hotelu, czynny sklep, apteka, stacja paliw, biurowiec z ochroną. W takich miejscach możesz spokojnie ocenić sytuację, zadzwonić i poczekać.

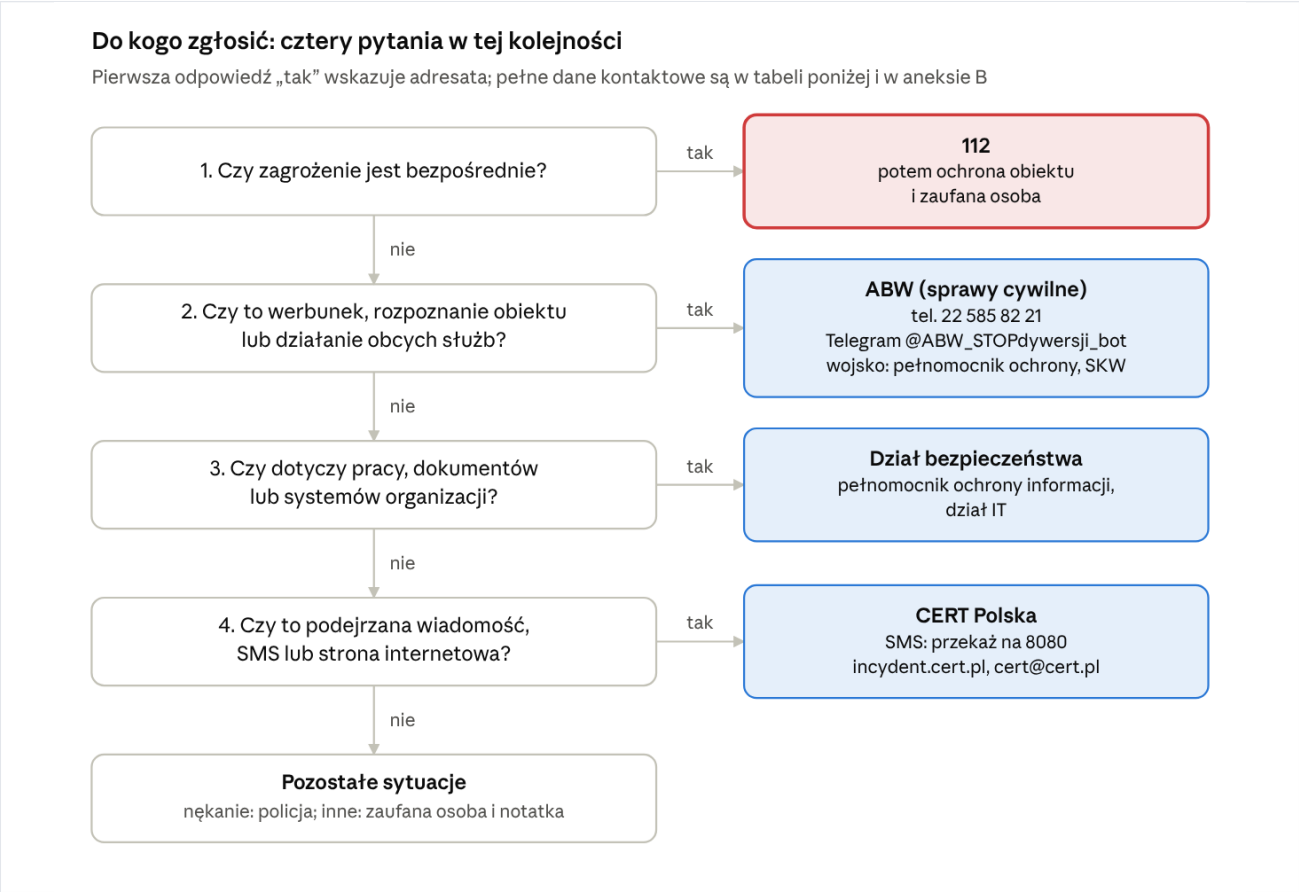
Nie prowadź do domu ani do miejsc wrażliwych. Jeśli masz silne podejrzenie, że ktoś za tobą idzie, nie wracaj do domu, do biura projektu ani do samochodu, dopóki sytuacja się nie wyjaśni.

Zmień plan w sposób naturalny. Wejdź do sklepu, zrób zakupy, zamów taksówkę z miejsca publicznego. Nie wykonuj gwałtownych manewrów, nie biegaj, nie jedź samochodem w sposób niebezpieczny. Ta rada dotyczy niejasnego podejrzenia. Gdy grozi ci bezpośrednie niebezpieczeństwo, oddalasz się tak szybko, jak trzeba, i dzwonisz pod 112.

Poinformuj kogoś. Zadzwoń do zaufanej osoby lub działu bezpieczeństwa i powiedz, gdzie jesteś i co się dzieje. Sama rozmowa telefoniczna w widoczny sposób bywa czynnikiem odstraszającym.

Przy bezpośrednim zagrożeniu dzwoń pod 112. Nie czekaj, aż sytuacja stanie się „wystarczająco poważna". Dyspozytor oceni, czy potrzebna jest interwencja.

4.6. Kogo i kiedy informować



Rys. 12. Kolejność pytań przy wyborze adresata zgłoszenia

Gdy sytuacja pasuje do kilku pytań, zgłaszasz do pierwszego adresata, a pozostałych informujesz po nim. Przy zagrożeniu bezpośrednim zawsze zaczynasz od 112. Osoba, która przyjmuje zgłoszenie w organizacji, korzysta z karty w aneksie C.

Sytuacja	Kogo informujesz	Jak
Bezpośrednie zagrożenie życia, zdrowia lub mienia	Policja, pogotowie	Numer alarmowy 112
Niepokojąca sytuacja w lokalu, hotelu, biurowcu	Obsługa, ochrona obiektu	Osobiście, dyskretnie
Sygnały niepożądanego zainteresowania tobą w związku z pracą	Dział bezpieczeństwa, pełnomocnik ds. ochrony informacji, przełożony	Zgodnie z procedurą organizacji
Uporczywe pojawianie się tej samej osoby w twoim życiu prywatnym	Policja	Zgłoszenie w komisariacie, z notatkami

Sytuacja	Kogo informujesz	Jak
Próba werbunku, oferta wykonania zdjęć obiektów lub innych zadań na rzecz nieznanego zleceniodawcy, sygnały działania obcych służb	ABW	Dyżurny oficer operacyjny ABW, tel. 22 585 82 21; chatbot @ABW_STOPdywersji_bot w Telegramie; delegatury ABW (aneks B)
Osoba fotografująca lub obserwująca obiekt infrastruktury krytycznej w sposób wskazujący na rozpoznanie	Ochrona obiektu, policja (112), ABW	Natychmiast, jeśli zdarzenie trwa
Sprawy związane z wojskiem, jednostkami wojskowymi, przemysłem zbrojeniowym pracującym dla wojska	Pełnomocnik ochrony informacji w organizacji, właściwe służby (w tym Służba Kontrwywiadu Wojskowego)	Zgodnie z procedurą organizacji

Zgłoszenie do ABW nie wymaga pewności. Agencja sama ocenia zasadność zgłoszeń. Twoim zadaniem jest przekazanie faktów, a nie przeprowadzenie analizy.

4.7. Dlaczego nie konfrontować

Samodzielna konfrontacja z osobą, którą podejrzewasz o obserwację lub działanie na rzecz obcych służb, jest złym pomysłem z kilku powodów.

Ryzyko dla ciebie. Nie wiesz, z kim masz do czynienia ani jak zareaguje. Osoba przyłapana na czymś nielegalnym może zachować się agresywnie. Według ICCT i GLOBSEC około jedna czwarta sprawców opisanych w ich zbiorze danych była wcześniej karana, w tym za przestępstwa z użyciem przemocy.

Ryzyko pomyłki. Możesz się mylić. Publiczne oskarżenie niewinnego człowieka jest dla niego krzywdzące, a dla ciebie może skończyć się odpowiedzialnością cywilną lub karną.

Ryzyko dla sprawy. Jeśli rzeczywiście trafiłeś na element większego działania, konfrontacja ostrzega sprawców i może utrudnić pracę służb, które być może już się nimi zajmują.

Ryzyko prawne. Przytrzymanie, przeszukanie, odebranie telefonu, zablokowanie drogi to działania, które łatwo przekraczają granice prawa. Kodeks postępowania karnego pozwala każdemu ująć osobę na gorącym uczynku przestępstwa lub w pościgu podjętym bezpośrednio po jego popełnieniu, ale tylko wtedy, gdy zachodzi obawa ukrycia się tej osoby albo nie można ustalić jej tożsamości; osobę ujętą trzeba niezwłocznie oddać Policji (art. 243 k.p.k.). Mimo to w praktyce bezpieczeństwa osobistego nie rekomendujemy korzystania z tego uprawnienia. Wiąże się z ryzykiem fizycznym i prawnym, którego nie da się dobrze ocenić w kilka sekund.

Wyjątkiem jest sytuacja, w której ktoś bezpośrednio sięga po twoje rzeczy, np. próbuje zabrać laptop ze stołu. Naturalne zabezpieczenie swojej własności (przytrzymanie torby, głośne zwrócenie uwagi) jest czymś innym niż konfrontacja z podejrzewanym obserwatorem.

4.8. Bezpieczny protokół przy uzasadnionej obawie

Gdy sygnał ma siłę co najmniej umiarkowaną, postępuj według poniższej kolejności. Pełny schemat decyzyjny znajduje się w rozdziale 6.

1. Zachowaj spokój i naturalne zachowanie. Nie dawaj znać, że coś zauważyłeś.
2. Oceń, czy zagrożenie jest bezpośrednie. Jeśli tak, przejdź do bezpiecznego miejsca i dzwoń pod 112.

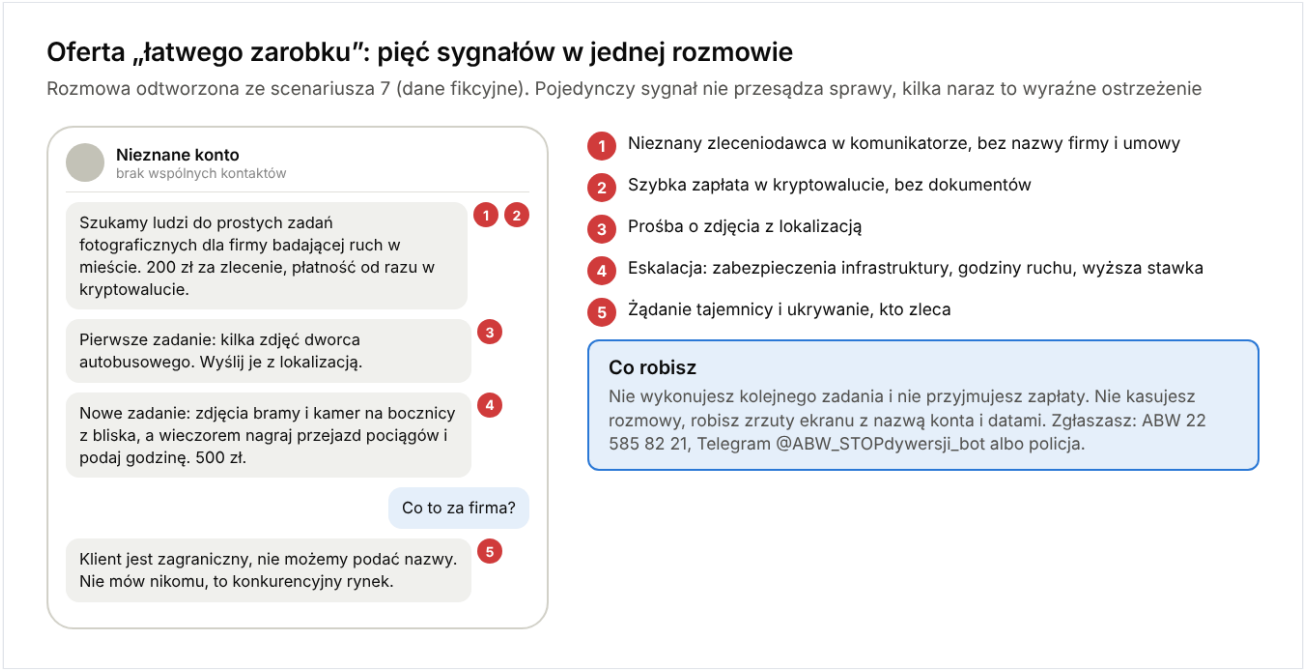
3. Jeśli nie jest bezpośrednie, zakończ lub przenieś to, co robisz (spotkanie, rozmowę, pracę na laptopie) w sposób niewzbudzający uwagi.
4. Udaj się do bezpiecznego miejsca publicznego.
5. Poinformuj zaufaną osobę lub dział bezpieczeństwa: gdzie jesteś, co zaobserwowałeś, co zamierzasz zrobić.
6. Nie wracaj bezpośrednio do domu ani do miejsc wrażliwych, dopóki nie ocenisz sytuacji razem z kimś drugim.
7. Po odzyskaniu bezpieczeństwa sporządź notatkę według wzoru z aneksu C.
8. Przy sygnałach związanych z pracą zgłoś sprawę w organizacji. Przy sygnałach działania obcych służb zgłoś ją do ABW.
9. W kolejnych dniach zachowaj większą uważność i notuj kolejne obserwacje, ale nie zmieniaj gwałtownie całego trybu życia bez konsultacji.

4.9. Elementy szczególne w latach 2025–2026

Sygnały związane z werbunkiem jednorazowych wykonawców

Na podstawie opisów ABW, ICCT i GLOBSEC oraz przypadków opisanych w mediach można wskazać cechy ofert, które powinny wzbudzić czujność. Pojedyncza cecha nie przesądza sprawy. Kilka naraz to wyraźny sygnał.

- oferta przychodzi od nieznanej osoby przez komunikator (najczęściej Telegram), media społecznościowe lub SMS, często w formie „pracy zdalnej” lub „łatwego zarobku”,
- wynagrodzenie jest nieproporcjonalnie wysokie do prostoty zadania, a pierwsza wpłata przychodzi szybko, zanim wykonasz cokolwiek istotnego,
- zapłata ma nastąpić w kryptowalutach lub przez pośredników, bez umowy i bez danych zleceniodawcy,
- zadanie polega na fotografowaniu lub filmowaniu obiektów (dworce, tory, mosty, magazyny, stacje paliw, jednostki wojskowe, rozdzielnie, siedziby firm), opisywaniu ruchu, przejechaniu określoną trasą, naklejeniu plakatów, namalowaniu napisu, odebraniu lub przekazaniu paczki, nagraniu filmu w określonym miejscu i czasie,
- zleceniodawca prosi o włączenie udostępniania lokalizacji, o zdjęcia z metadanymi albo o nagranie dowodu wykonania zadania,
- zadania stopniowo stają się poważniejsze, a odmowa spotyka się z presją, szantażem lub groźbą ujawnienia wcześniejszych zleceń,
- oferta jest przedstawiana młodym osobom jako gra, wyzwanie albo zadanie „dla społeczności”.



Rys. 13. Oferta „łatwego zarobku" z zaznaczonymi sygnałami ostrzegawczymi · rozmowa odtworzona ze scenariusza 7, dane fikcyjne

Jak reagować:

- nie wykonuj żadnego zadania, nawet „próbnego", i nie przyjmuj płatności,
- nie wdawaj się w dyskusję, nie próbuj „wyciągnąć" informacji od zleceniodawcy,
- nie kasuj korespondencji: zrób zrzuty ekranu z widoczną nazwą konta, datą i treścią,
- zgłoś sprawę do ABW (chatbot @ABW_STOPdywersji_bot, dyżurny 22 585 82 21) lub na policję,
- jeśli oferta przyszła SMS-em, możesz ją także przekazać do CERT Polska na numer 8080,
- porozmawiaj o takich ofertach z bliskimi, zwłaszcza z nastolatkami i osobami w trudnej sytuacji finansowej.

Jeśli ktoś z twojego otoczenia już wykonał takie zadanie, najważniejsze jest, żeby jak najszybciej się zgłosił. Polskie prawo przewiduje surowe kary za działanie na rzecz obcego wywiadu, a karalne jest także samo zgłoszenie gotowości do takiego działania i gromadzenie dla niego informacji (art. 130 § 3 Kodeksu karnego, od 6 miesięcy do 8 lat pozbawienia wolności).

Art. 131 Kodeksu karnego przewiduje w określonych przypadkach niepodleganie karze, ale tylko po spełnieniu wszystkich ustawowych warunków. Przy czynach z art. 130 § 3 sprawca musi dobrowolnie poniechać dalszej działalności, podjąć istotne starania zmierzające do zapobieżenia popełnieniu zamierzonego czynu i ujawnić organowi ścigania wszystkie istotne okoliczności (art. 131 § 2). Przy usiłowaniu cięższych postaci szpiegostwa przepis wymaga dobrowolnego poniechania dalszej działalności i ujawnienia wszystkich istotnych okoliczności (art. 131 § 1; nowelizacja Kodeksu karnego, Dz.U. 2023 poz. 1834). Zgłoszenie się nie daje więc automatycznej gwarancji niepodlegania karze. Konkretną sytuację ocenia prawnik, dlatego od razu skorzystaj z pomocy adwokata lub radcy prawnego.

Osoby fotografujące obiekty infrastruktury lub logistyki

Fotografowanie budynków i krajobrazu jest legalne i powszechne. Zakaz określony w art. 616a ustawy o obronie Ojczyzny dotyczy oznaczonych obiektów zajmowanych przez jednostki wojskowe lub służby specjalne oraz wskazanych w przepisie ruchomości i wizerunków osób, z ustawowymi wyjątkami. Opis

dotyczy tego zakazu, a nie wszystkich możliwych ograniczeń. Utrwalanie obrazu i jego rozpowszechnianie wymagają odrębnej oceny prawnej (aneks A). Dlatego sam fakt, że ktoś robi zdjęcie dworca czy mostu, nie jest powodem do reakcji.

Uwagę powinno zwrócić zestawienie kilku okoliczności: fotografowanie elementów technicznych i zabezpieczeń zamiast całości (szafy zasilające, rozjazdy, kable, bramy, kamery, ogrodzenia), robienie zdjęć w sposób ukryty, długie przebywanie przy obiekcie bez widocznego celu, notowanie godzin ruchu, oddalanie się na widok ochrony lub patrolu, powroty w kolejnych dniach. W opisanej w rozdziale o kontekście sprawie stacji Starlink atak według ABW poprzedziło rozpoznanie terenu i zabezpieczeń, dokumentowane zdjęciami i nagraniami wysyłanymi zleceniodawcy.

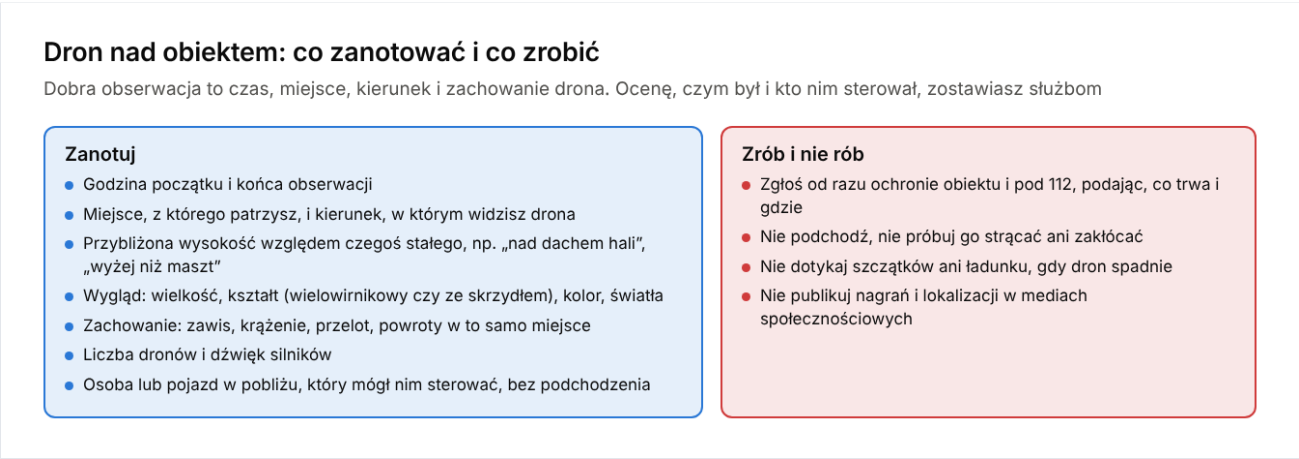
Jeśli widzisz takie zachowanie, nie podchodź i nie pytaj, co ta osoba robi. Odnotuj czas, miejsce i opis, a jeśli zdarzenie trwa przy obiekcie infrastruktury krytycznej lub kolejowej, poinformuj ochronę obiektu albo zadzwoń pod 112. Gdy masz podstawy sądzić, że to działanie powtarzające się, zgłoś je także do ABW.

Drony nad obiektami i w pobliżu spotkań

We wrześniu 2025 roku rosyjskie drony naruszyły polską przestrzeń powietrzną, a w sierpniu 2026 roku przy ukraińskim samolocie na lotnisku Lipsk/Halle znaleziono drona z ładunkiem wybuchowym (rozdział o kontekście). Dron nad miastem może jednak należeć do operatora wykonującego zwykły lot: filmowanie, inspekcję, pomiary. O tym, czy lot był zgodny z prawem i kto sterował dronem, rozstrzygają służby. Twoim zadaniem jest dobra obserwacja i szybkie zgłoszenie, gdy dron krąży nad obiektem infrastruktury, jednostką wojskową, magazynem albo nad miejscem wrażliwego spotkania.

Zgłaszasz ochronie obiektu i pod numer 112. Nie próbujesz drona strącić, zakłócić ani przechwycić. Znowelizowana w 2026 roku ustawa o zarządzaniu kryzysowym pozwala na niszczenie, unieruchamianie lub przejmowanie kontroli nad dronami stanowiącymi zagrożenie, ale robią to wyłącznie uprawnione formacje i osoby (podrozdział 15.9). Jeśli dron spadnie, nie dotykaj go ani ładunku, odejdź na bezpieczną odległość i wezwij pomoc.

Jeśli sam latasz dronem, przed lotem sprawdź strefy geograficzne i ograniczenia na mapie DroneMap Polskiej Agencji Żeglugi Powietrznej (dronemap.pansa.pl). Mapa ma charakter informacyjny i pokazuje stan z chwili sprawdzenia, a strefy mogą zostać aktywowane w każdej chwili (Dla Pilota). Lot nad cudzym obiektem po to, żeby „sprawdzić okolicę" przed spotkaniem, jest złym pomysłem z powodów opisanych w podrozdziale 3.1.



Rys. 14. Obserwacja drona nad obiektem: co zanotować i co zrobić

Powtarzające się pojawianie tych samych osób w pobliżu wrażliwych spotkań

Jeśli uczestniczysz w cyklu spotkań dotyczących projektu z obszaru logistyki, energetyki, obronności lub wsparcia Ukrainy, a w okolicy kilku z nich, w różnych miejscach, zauważasz tę samą osobę lub pojazd, potraktuj to jako sygnał co najmniej umiarkowany. Zapisz obserwacje, porównaj je z obserwacjami innych uczestników i przekaż działowi bezpieczeństwa. Do czasu wyjaśnienia rozważ zmianę formy spotkań: przeniesienie ich do pomieszczeń kontrolowanych przez organizację, ograniczenie liczby uczestników, rezygnację z publicznych kalendarzy i rezerwacji.

5.

Bezpieczne planowanie tras i przemieszczania się

Droga na spotkanie i powrót również wymagają uwzględnienia w ocenie ryzyka: na parkingu, w pustym przejściu, w taksówce, w hotelowym korytarzu. Planowanie trasy nie polega na ciągłym zmienianiu dróg, tylko na tym, żeby wiedzieć, którędy jedziesz, jak wrócisz, co zrobisz, gdy plan się posypie, i komu o tym mówisz.

5.1. Zasady ogólne

Każda podróż poza codzienną rutyną powinna mieć trasę podstawową i alternatywną. Alternatywa nie musi być rozpisana szczegółowo. Wystarczy, że wiesz, czym wrócisz, jeśli nie przyjedzie taksówka, odwołają pociąg albo ulica będzie zamknięta.

Przy wyborze trasy bierz pod uwagę:

- porę dnia i oświetlenie (ta sama trasa w południe i o 23:00 to dwie różne trasy),
- dostępność pomocy (czynne sklepy, stacje paliw, hotele, komisariaty po drodze),
- natężenie ruchu pieszego i samochodowego,
- znane utrudnienia, wydarzenia, roboty drogowe,
- długość odcinków, na których jesteś sam (np. droga od przystanku do hotelu).

Najprostsza zasada brzmi: po zmroku wybieraj trasę dłuższą, ale ruchliwą i oświetloną, zamiast krótszej i pustej.

5.2. Przemieszczanie się pieszo

- Idź ulicami oświetlonymi i uczęszczanymi. Skróty przez parki, podwórka i przejścia podziemne zostaw na dzień.
- Idź środkiem chodnika, z dala od bram i zaparkowanych samochodów.
- Trzymaj torbę z dokumentami i laptopem po stronie od budynków, nie od jezdni.
- Nie idź z wzrokiem w telefonie. Jeśli musisz sprawdzić drogę, zatrzymaj się w oświetlonym miejscu, plecami do ściany lub witryny.
- Słuchawki w jednym uchu albo w trybie przepuszczania dźwięków otoczenia.
- Jeśli nie znasz okolicy, sprawdź trasę przed wyjściem, żeby nie zatrzymywać się co chwilę.
- Pytaj o drogę w sklepie, hotelu, aptece, a nie przypadkowe osoby na pustej ulicy.

- Jeśli coś cię niepokoi, wejdź do najbliższego czynnego lokalu. Nie musisz niczego kupować.

5.3. Samochód

Parkowanie. Wybieraj miejsca oświetlone, monitorowane i bliskie wejściu. Nie zostawiaj w samochodzie niczego na widoku, zwłaszcza teczek, laptopów i dokumentów firmowych. Unikaj miejsc parkingowych oznaczonych nazwiskiem lub stanowiskiem („prezes", „dyrektor"), bo ułatwiają identyfikację pojazdu i harmonogramu.

Przed wejściem do samochodu. Podchodź z kluczem w ręku, rozejrzyj się wokół pojazdu. Po wejściu od razu zamknij drzwi. Nie siedź na parkingu z telefonem przez kilka minut z otwartymi drzwiami. Jeśli przy samochodzie stoi ktoś, kogo zachowanie cię niepokoi, nie podchodź: wróć do budynku i poproś o pomoc ochronę.

W trakcie jazdy. W korku zostawiaj odstęp, który pozwala wyjechać z kolejki. Jeśli ktoś próbuje cię zatrzymać w nietypowych okolicznościach, na przykład sygnałami ręką na pustej drodze albo wymuszoną stłuczką w odludnym miejscu, nie zatrzymuj się na odludnym odcinku; kieruj się do ruchliwego, oświetlonego miejsca i zadzwoń pod 112. Policja może zatrzymywać pojazdy do kontroli. Niezastosowanie się do polecenia zatrzymania może stanowić wykroczenie albo, po spełnieniu warunków art. 178b Kodeksu karnego, przestępstwo. Jeżeli masz uzasadnione wątpliwości co do tożsamości osób prowadzących kontrolę, zachowaj ostrożność: zatrzymaj się w bezpiecznym, widocznym miejscu, zachowaj dystans i w razie potrzeby zweryfikuj sytuację niezależnym kanałem. Nie traktuj tych wątpliwości jako automatycznego pozwolenia na zignorowanie prawidłowo wydanego polecenia zatrzymania. Poza obszarem zabudowanym kontrolę może przeprowadzić umundurowany policjant, a sygnał „Policja. Jedź za mną" wyświetlany przez nieoznakowany radiowóz jest poleceniem, które należy wykonać. Jeśli poza terenem zabudowanym próbuje cię zatrzymać nieumundurowana osoba z nieoznakowanego samochodu, zadzwoń pod 112, aby zweryfikować pojazd, i kieruj się spokojnie do najbliższego obszaru zabudowanego lub komisariatu.

Samochody wynajęte i służbowe. System multimedialny wynajętego samochodu po sparowaniu z telefonem zapisuje często książkę kontaktów, historię połączeń i nawigacji. Przed oddaniem auta usuń sparowany telefon i historię celów nawigacji. Do ładowania używaj własnej ładowarki samochodowej, nie gniazda USB systemu multimedialnego. Samochody służbowe z systemem telematycznym rejestrują trasy. To ma sens z punktu widzenia zarządzania flotą, ale oznacza, że dane o twoich przejazdach są przechowywane przez firmę i dostawcę usługi.

Osoby postronne. Nie zabieraj autostopowiczów i nie podwoź osób poznanych przypadkowo, zwłaszcza z okolic obiektów, w których pracujesz.

5.4. Transport publiczny i taksówki

W pociągu, autobusie i tramwaju:

- wieczorem siadaj w wagonie lub części pojazdu, w której są inni pasażerowie, najlepiej w pobliżu obsługi,
- nie prowadź rozmów służbowych, ani na żywo, ani przez telefon,
- nie pracuj na dokumentach wrażliwych, nawet z filtrem prywatności na ekranie,
- trzymaj bagaż z dokumentami przy sobie, nie na półce za plecami,
- nie zasypiaj z telefonem w dłoni i laptopem na stoliku.

Taksówki i przejazdy z aplikacji:

- zamawiaj przez aplikację lub telefonicznie, nie zatrzymuj przypadkowych pojazdów,
- przed wejściem sprawdź numer rejestracyjny i imię kierowcy podane w aplikacji,
- poproś, żeby kierowca podał twoje imię, zamiast samemu się przedstawiać,
- korzystaj z funkcji udostępnienia przejazdu zaufanej osobie,
- nie wykonuj w taksówce rozmów służbowych i nie mów kierowcy więcej, niż trzeba („do hotelu", nie „na spotkanie z zarządem spółki X"),
- przy wysiadaniu sprawdź, czy niczego nie zostawiłeś na siedzeniu.

5.5. Ograniczanie niepotrzebnego ujawniania planów podróży

Plany podróży wyciekają głównie przez rzeczy, które wydają się niewinne. Przegląd najczęstszych źródeł:

Źródło	Co ujawnia	Jak ograniczyć
Kalendarz współdzielony lub publiczny	Miejsce, czas, uczestników, temat spotkania	Udostępniaj tylko informację „zajęty", szczegóły w prywatnych wpisach.
Automatyczna odpowiedź w poczcie	Że cię nie ma, gdzie jesteś i do kiedy	Krótka treść bez miejsca i celu podróży: „Odpowiem po 15 listopada".
Media społecznościowe	Lokalizację w czasie rzeczywistym, hotel, towarzystwo	Publikuj po powrocie, bez oznaczania lokalizacji i bez zdjęć kart pokładowych.
Zdjęcie karty pokładowej	Kod kreskowy zawiera nazwisko i numer rezerwacji, czasem więcej	Nie publikuj, a papierowe karty niszcz po podróży.
Przywieszka bagażowa	Adres domowy	Adres służbowy lub sam numer telefonu i e-mail.
Aplikacje sportowe z publicznymi profilami	Trasy biegania wokół hotelu i domu, godziny	Profil prywatny, strefy prywatności wokół domu i hotelu.
Rozmowy w biurze i w lokalach	Plany całego zespołu	Szczegóły podróży tylko dla osób, które ich potrzebują.
Zamówienia i rezerwacje	Dane w systemach hoteli, linii lotniczych, firm transportowych	Rezerwacje przez dział podróży, bez zbędnych uwag i danych.

W przypadku podróży o wysokim poziomie ryzyka, np. wyjazdów do Ukrainy, na wschodnie pogranicze lub w związku z transportami pomocy, plan podróży powinien znać wąski krąg osób, a w komunikacji wewnętrznej warto stosować ogólne sformułowania zamiast nazw miejsc i godzin.

5.6. Udostępnianie planu zaufanej osobie

Przy podwyższonym i wysokim ryzyku plan podróży powinna znać co najmniej jedna zaufana osoba. Plan powinien obejmować:

- trasę i środki transportu, z numerami lotów lub pociągów,
- miejsca noclegu z adresem i telefonem,
- spotkania (z kim, gdzie, o której), w formie, która nie ujawnia więcej niż potrzeba,
- godziny kontrolne i sposób kontaktu (rozdział 1.6),

- umówiony sygnał oznaczający problem,
- dane kontaktowe działu bezpieczeństwa i najbliższej placówki dyplomatycznej przy podróżach zagranicznych.

Przekazuj plan bezpiecznym kanałem (szyfrowany komunikator, służbowa poczta), a nie w otwartej grupie czy na tablicy w biurze. Udostępnianie lokalizacji w czasie rzeczywistym jest przydatne na czas konkretnej podróży, ale nie powinno być włączone na stałe, bo tworzy pełną historię twoich ruchów u osoby trzeciej i u dostawcy usługi.

5.7. Gdy plan się posypie: zgubienie się, utrata telefonu, zmiana planów

Zgubienie się. Zatrzymaj się w bezpiecznym miejscu publicznym, nie na środku pustej ulicy. Sprawdź mapę offline (warto mieć ją pobraną przed podróżą) albo zapytaj obsługę sklepu lub hotelu. Jeśli jest późno i okolica wydaje się niebezpieczna, zamów taksówkę do miejsca, które znasz.

Utrata telefonu. Telefon jest dziś mapą, portfelem, kluczem do kont i listą kontaktów. Dlatego w podróży o podwyższonym ryzyku warto mieć przy sobie kartkę z dwoma, trzema numerami telefonów (zaufana osoba, dział bezpieczeństwa, hotel), niewielką ilość gotówki i kartę płatniczą noszoną oddzielnie od telefonu. Procedura blokowania urządzenia i kont jest opisana w podrozdziale 8.9, a postępowanie przy kradzieży i napaści w podrozdziałach 11.1 i 11.3.

Zmiana planów. Każda istotna zmiana (inny hotel, odwołane spotkanie, inne połączenie powrotne) powinna trafić do zaufanej osoby. Najczęstszy problem z godzinami kontrolnymi polega na tym, że plan się zmienia, a nikt o tym nie wie, więc brak sygnału albo wywołuje niepotrzebny alarm, albo, co gorsze, przestaje być traktowany poważnie.

5.8. Legalna kontrola bezpieczeństwa trasy przed podróżą

Przed wyjazdem warto sprawdzić publicznie dostępne źródła:

Źródło	Co zawiera
Rządowe Centrum Bezpieczeństwa (gov.pl/rcb), alerty RCB	Ostrzeżenia, obowiązujące stopnie alarmowe, komunikaty kryzysowe.
Komunikaty wojewodów i policji	Utrudnienia, imprezy masowe, zamknięte obszary.
Informacje przewoźników i zarządców infrastruktury	Utrudnienia na kolei, zmiany rozkładów, zamknięte odcinki dróg.
Prognozy i ostrzeżenia IMGW	Zjawiska pogodowe, które mogą wpłynąć na podróż.
MSZ, strona „Informacje dla podróżujących" (gov.pl/web/dyplomacja)	Ostrzeżenia dla podróżnych, informacje o kraju, kontakty do placówek.
System Odyseusz (MSZ)	Rejestracja podróży zagranicznej, dzięki której konsul może się z tobą skontaktować w sytuacji kryzysowej. W 2026 roku rejestracja stała się dostępna także w aplikacji mObywatel.

Przy podróżach zagranicznych sprawdź także przepisy kraju docelowego dotyczące fotografowania obiektów, kontroli urządzeń elektronicznych na granicy i wwozu sprzętu szyfrującego. Różnią się one znacząco między państwami.

5.9. Rejony infrastruktury krytycznej, centrów logistycznych i tras pomocy

Przemieszczanie się w okolicach węzłów kolejowych, terminali, centrów logistycznych, lotnisk cargo, obiektów energetycznych i punktów przeładunku pomocy dla Ukrainy wymaga kilku dodatkowych zasad. Ich celem jest uniknięcie sytuacji, w której narażasz siebie albo zostajesz uznany za osobę prowadzącą rozpoznanie.

Dla wszystkich:

- nie zatrzymuj się bez potrzeby przy ogrodzeniach i bramach obiektów i nie parkuj tam na dłużej,
- nie fotografuj i nie filmuj elementów technicznych, wjazdów ani zabezpieczeń, także przez okno samochodu lub pociągu,
- miej przy sobie dokument tożsamości i bądź przygotowany na legitymowanie, zwłaszcza w okresach podwyższonych stopni alarmowych,
- nie wchodź na tory i tereny kolejowe poza wyznaczonymi przejściami,
- jeśli zauważysz uszkodzenie toru, przedmiot na torach, otwartą szafę zasilającą lub podejrzane działania przy infrastrukturze kolejowej, zadzwoń pod 112 i podaj jak najdokładniejsze miejsce; na przejazdach kolejowo-drogowych PKP PLK umieszcza żółte naklejki z indywidualnym, dziewięciocyfrowym numerem przejazdu, numerem 112 i numerami do zgłaszania awarii; podanie tego numeru dyspozytorowi pozwala od razu zlokalizować miejsce.

Dla kierowców i pracowników obsługujących transporty, w tym pomocy dla Ukrainy:

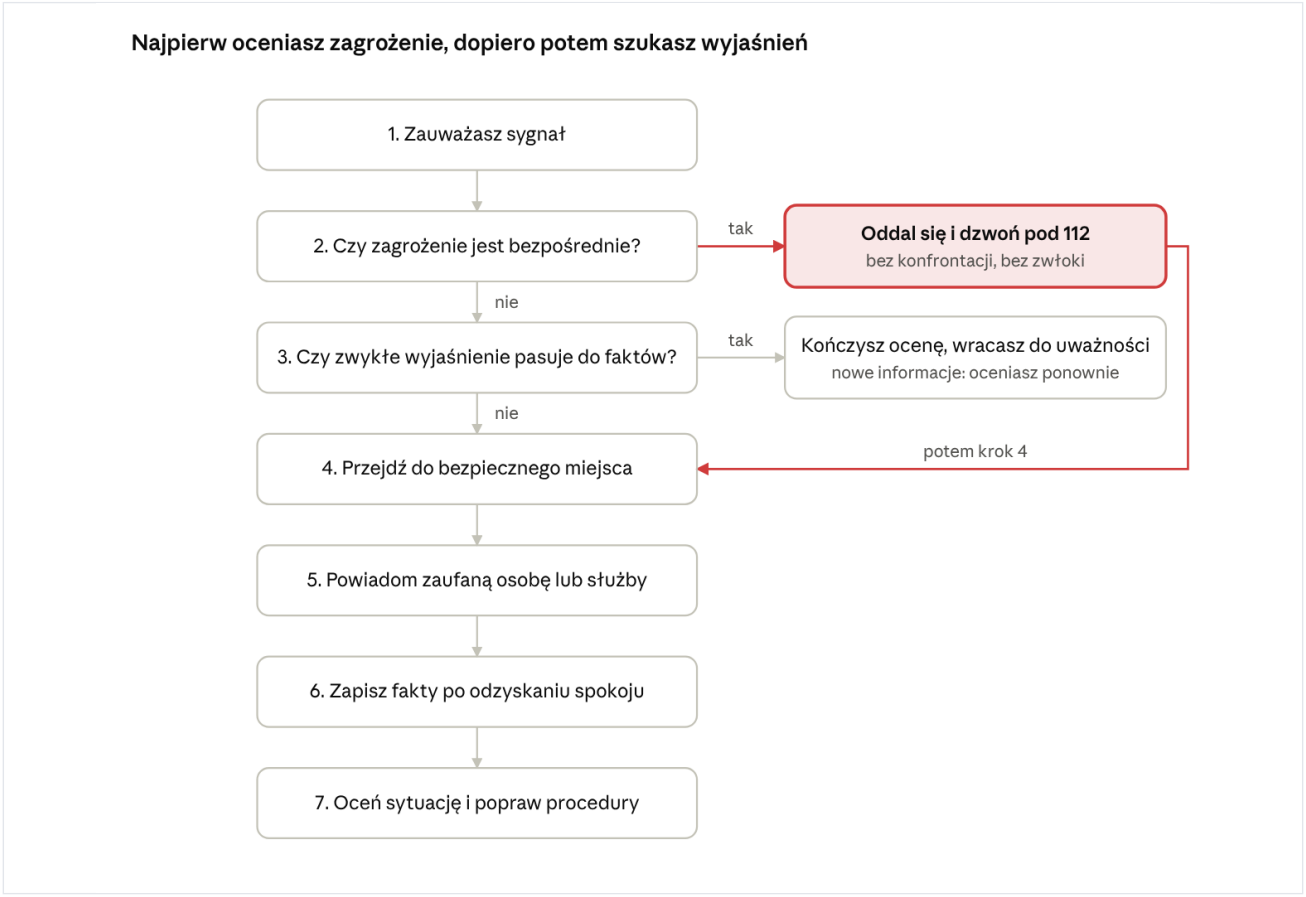
- nie publikuj tras, godzin wyjazdu, miejsc postojów, zdjęć ładunku ani zdjęć z bazy,
- planuj postoje w miejscach monitorowanych i ruchliwych, a nie na pustych zatokach przy drodze,
- po postoju obejdź pojazd i sprawdź, czy nie ma oczywistych zmian: otwartych klap, uszkodzeń, przedmiotów, których wcześniej nie było; jeśli zauważysz nieznany przedmiot przy pojeździe lub pod nim, nie dotykaj go, odejdź na bezpieczną odległość i dzwoń pod 112,
- nie przyjmuj „pomocy" ani paczek do przewiezienia od przypadkowych osób na parkingach i stacjach,
- zgłaszaj dyspozytorowi i ochronie osoby, które wypytują o ładunek, cel podróży lub godziny,
- przy powtarzających się sygnałach zainteresowania twoim pojazdem lub trasą informuj dział bezpieczeństwa, a ten rozważy zgłoszenie do ABW.

Te zasady nie mają tworzyć atmosfery zagrożenia. Ogromna większość przejazdów odbywa się bez żadnych incydentów. Mają sprawić, że gdy coś odbiega od normy, zostanie to zauważone i przekazane właściwym osobom.

6.

Procedura weryfikacji niepokojącej sytuacji

Każda niepokojąca sytuacja, niezależnie od tego, czy dotyczy obserwacji, nietypowej oferty, przedmiotu pozostawionego bez nadzoru czy dziwnego zachowania rozmówcy, przechodzi przez te same siedem kroków. Najpierw oceniasz, czy zagrożenie jest bezpośrednie. Jeśli tak, oddal się i wezwij pomoc. Jeśli zagrożenie nie jest bezpośrednie, spokojnie oceń kontekst. Wyjaśnienie musi odpowiadać dostępnym faktom i nie mogą pozostawać istotne sygnały zagrożenia. Procedura pozwala zakończyć ocenę po wyjaśnieniu sytuacji albo przejść do działań ochronnych i zgłoszenia. Przy bezpośrednim zagrożeniu rozważanie alternatywnych wyjaśnień nie może opóźniać oddalenia się ani wezwania pomocy. Celem procedury jest zastąpienie improwizacji pod presją prostą kolejnością działań, którą można przećwiczyć wcześniej.



Rys. 15. Schemat postępowania przy niepokojącej sytuacji: 7 kroków, 2 rozgałęzienia

Schemat czyta się od góry. Odpowiedź „tak" w kroku 2 oznacza, że najpierw oddalasz się i dzwonisz pod 112, a dopiero potem przechodzisz do kroków 4–7. Odpowiedź „tak" w kroku 3 kończy ocenę, jeśli zwyczajne wyjaśnienie jest zgodne z faktami; nowe informacje mogą uzasadniać ponowną ocenę.

6.1. Krok 1: zauważenie sygnału

Cel. Uświadomić sobie, że coś odbiega od normy miejsca, i przejść ze stanu uważności do czujności, bez okazywania tego na zewnątrz.

Zalecane działania:

- nazwij w myślach, co dokładnie zauważyłeś, opisowo i bez oceny („kobieta przy sąsiednim stoliku od 20 minut nie dotknęła kawy i trzyma telefon ekranem w naszą stronę"),
- zanotuj w pamięci godzinę i miejsce,
- nie zmieniaj gwałtownie zachowania: nie odwracaj się, nie przerywaj rozmowy w pół zdania,
- jeśli jesteś z kimś, nie informuj go od razu na głos; możesz użyć umówionego sygnału lub zakończyć wątek.

Najczęstsze błędy:

- zignorowanie sygnału, bo „na pewno nic", bez chwili zastanowienia,
- natychmiastowe uznanie sygnału za dowód zagrożenia,
- ostentacyjne przyglądanie się osobie lub przedmiotowi.

Warunek zakończenia. Masz jasny, opisowy obraz tego, co zauważyłeś, i przechodzisz do oceny, czy zagrożenie jest bezpośrednie.

6.2. Krok 2: ocena bezpośredniego zagrożenia

Cel. Rozstrzygnąć, czy masz czas na spokojne działanie, czy musisz natychmiast odejść. To pierwsze pytanie po zauważeniu sygnału, zanim zaczniesz szukać wyjaśnień.

Zagrożenie jest bezpośrednie, gdy:

- ktoś zachowuje się agresywnie wobec ciebie lub innych, grozi, ma w ręku przedmiot mogący służyć jako broń,
- ktoś idzie za tobą w pustym miejscu, blokuje ci drogę, czeka przy twoim samochodzie lub drzwiach,
- zauważasz przedmiot, który wygląda na niebezpieczny (wystające przewody, dym, zapach chemikaliów, płyn wyciekający z pakunku), albo pakunek pozostawiony w miejscu, w którym nie powinien się znaleźć, bez możliwości ustalenia właściciela,
- w lokalu lub w okolicy wybucha panika, pożar, słychać huk lub strzały,
- ktoś usiłuje zabrać twoje rzeczy lub zmusić cię do pójścia z nim.

Zalecane działania przy zagrożeniu bezpośrednim:

- oddal się w stronę ludzi i wyjścia, nie w stronę źródła zagrożenia,
- zostaw rzeczy, jeśli ich zabranie wymaga czasu lub zbliżenia się do zagrożenia,
- gdy jesteś w bezpiecznym miejscu, dzwoń pod 112 i podaj: co się dzieje, gdzie (adres, charakterystyczne punkty), ile osób jest zagrożonych, czy są ranni,
- przy przedmiocie podejrzanym nie dotykaj go, nie przesuwaj, nie fotografuj z bliska i nie używaj telefonu w jego bezpośrednim pobliżu; poinformuj obsługę i oddal się,
- przy zagrożeniu terrorystycznym ABW zaleca kolejno: ewakuację, jeśli jest możliwa; ukrycie się z wyciszeniem telefonu, jeśli ewakuacja jest niemożliwa; wezwanie pomocy pod 112 z bezpiecznego miejsca; obronę dostępnymi środkami tylko w ostateczności, gdy życie jest bezpośrednio zagrożone, a nie ma możliwości ucieczki ani ukrycia.

Najczęstsze błędy:

- zbliżanie się do zdarzenia z ciekawości lub żeby nagrać film,
- czekanie, aż ktoś inny zadzwoni po pomoc,
- wracanie po rzeczy,
- konfrontacja z osobą agresywną.

Warunek zakończenia. Jeśli zagrożenie nie jest bezpośrednie, przechodzisz spokojnie do kroku 3. Jeśli jest bezpośrednie, pomijasz krok 3 i przechodzisz do kroku 4 dopiero wtedy, gdy jesteś w bezpiecznym miejscu i pomoc została wezwana.

6.3. Krok 3: spokojna ocena kontekstu

Cel. Gdy zagrożenie nie jest bezpośrednie, sprawdzić, czy obserwacja ma zwyczajne wyjaśnienie, zanim podejmiesz dalsze działania.

Zalecane działania:

- znajdź co najmniej dwa niewinne wyjaśnienia (osoba czeka na kogoś, pracuje, jest pracownikiem lokalu, ochroniarzem w cywilu, turystą),
- zapytaj siebie, czy to pierwszy raz, czy element powtarzającego się wzoru (rozdział 4.3),
- zastanów się, czy twoja sytuacja (temat rozmowy, miejsce, branża) czyni zainteresowanie bardziej prawdopodobnym,
- jeśli przedmiot pozostał bez nadzoru, rozejrzyj się, czy właściciel nie jest w pobliżu (przy stoliku, w kolejce, w toalecie),
- daj sytuacji kilka minut: wiele niejasności rozwiązuje się samo (osoba spotyka znajomego, właściciel torby wraca).

Najczęstsze błędy:

- ocena oparta na wyglądzie, języku lub pochodzeniu osoby, a nie na jej zachowaniu,
- pomijanie wyjaśnień, które nie pasują do hipotezy o zagrożeniu,
- podejmowanie działań (fotografowanie, pytanie obsługi, wychodzenie w pośpiechu), zanim ocena się zakończy, jeśli zagrożenie nie jest bezpośrednie.

Warunek zakończenia. Jeśli zwyczajne wyjaśnienie jest zgodne z dostępnymi faktami i nie pozostają istotne sygnały zagrożenia, kończysz ocenę na tym etapie, wracasz do stanu uważności i zachowujesz obserwację w pamięci. Nowe informacje mogą uzasadniać ponowną ocenę. Jeśli żadne wyjaśnienie nie pasuje albo sygnał się powtarza, przechodzisz do kroku 4.

6.4. Krok 4: wybór bezpiecznego miejsca publicznego

Cel. Znaleźć się w otoczeniu, które ogranicza ryzyko i pozwala na spokojne dalsze działania.

Zalecane działania:

- zakończ lub przerwij spotkanie w naturalny sposób („przepraszam, muszę lecieć, odezwę się jutro”),
- zabierz dokumenty i urządzenia, jeśli możesz to zrobić bez zwłoki,
- przejdź do miejsca z ludźmi, oświetleniem i personelem: recepcja hotelu, czynny sklep, apteka, stacja paliw, biurowiec z ochroną, komisariat,
- nie idź do samochodu, domu ani biura projektu, jeśli podejrzewasz, że ktoś może za tobą iść,
- jeśli jesteś z kimś, zostańcie razem.

Najczęstsze błędy:

- wybór miejsca, które wydaje się ukryte, ale jest odludne (zaułek, pusty parking, klatka schodowa),
- tłumaczenie się rozmówcy z powodów wyjścia, co przedłuża sytuację,
- pozostanie w lokalu „żeby zobaczyć, co będzie”.

Warunek zakończenia. Jesteś w miejscu, w którym czujesz się bezpiecznie i możesz spokojnie rozmawiać przez telefon.

6.5. Krok 5: powiadomienie zaufanej osoby lub służb

Cel. Przekazać informację osobie, która może pomóc, i nie zostawać z sytuacją samemu.

Zalecane działania:

- zadzwoń do zaufanej osoby lub dyżurnego działu bezpieczeństwa; powiedz, gdzie jesteś, co zaobserwowałeś i co zamierzasz zrobić,
- ustalcie wspólnie, czy sprawa wymaga zgłoszenia: na policję (zagrożenie, nękanie), do ochrony obiektu, do ABW (sygnały działania obcych służb, rozpoznanie infrastruktury, próba werbunku), do pełnomocnika ochrony informacji (możliwe ujawnienie informacji),
- ustalcie, jak wrócisz (taksówka zamówiona z miejsca, w którym jesteś; ktoś po ciebie przyjedzie),
- ustalcie godzinę, o której dasz znać, że jesteś w domu lub w hotelu.

Najczęstsze błędy:

- rezygnacja z powiadomienia, bo „nie chcę robić zamieszania”,
- relacjonowanie wydarzeń w otwartych grupach komunikatora lub w mediach społecznościowych,
- przekazywanie interpretacji zamiast faktów („śledzi mnie agent”) zamiast („trzeci raz w tym tygodniu widzę tego samego mężczyznę w różnych miejscach”).

Warunek zakończenia. Ktoś zaufany wie o sytuacji, a decyzja o ewentualnym zgłoszeniu jest podjęta.

6.6. Krok 6: zapisanie faktów po odzyskaniu bezpieczeństwa

Cel. Utrwalić obserwacje, zanim pamięć je zniekształci, w formie przydatnej dla ciebie, organizacji i ewentualnie służb.

Zalecane działania:

- sporządź notatkę według wzoru z aneksu C możliwie szybko, najlepiej tego samego dnia,
- oddziel fakty (co widziałeś i słyszałeś) od ocen (co o tym myślisz) i zaznacz poziom pewności,
- dołącz posiadane materiały (zrzuty ekranu korespondencji, przypadkowe zdjęcia, bilety, potwierdzenia płatności z godziną),
- przechowuj notatkę w zatwierdzonym repozytorium z dostępem ograniczonym do uprawnionych osób, nie w ogólnodostępnych folderach ani prywatnych chmurach.

Najczęstsze błędy:

- odkładanie notatki na później i odtwarzanie wydarzeń po kilku dniach,
- uzupełnianie luk w pamięci domysłami,
- usuwanie korespondencji lub zdjęć „żeby nie mieć kłopotów”.

Warunek zakończenia. Notatka jest gotowa i przekazana tam, gdzie powinna trafić.

6.7. Krok 7: ocena i ewentualna zmiana procedur

Cel. Wyciągnąć wnioski, żeby podobna sytuacja w przyszłości była mniej prawdopodobna albo lepiej obsłużona.

Zalecane działania:

- po kilku dniach przeczytaj notatkę jeszcze raz i sprawdź, czy ocena się nie zmieniła,
- zastanów się, co ułatwiło sytuację (przewidywalne miejsce spotkań, publiczny kalendarz, rozmowa w złym miejscu) i co można zmienić,

- w organizacji: wpisz zdarzenie do rejestru incydentów, przeanalizuj je w gronie osób odpowiedzialnych za bezpieczeństwo, sprawdź, czy inni pracownicy nie zgłaszali podobnych obserwacji,
- zaktualizuj plan (rozdział 1.6) i listy kontrolne (rozdział 13),
- jeśli sytuacja była trudna emocjonalnie, porozmawiaj o niej z kimś bliskim lub skorzystaj z pomocy psychologicznej oferowanej przez pracodawcę.

Najczęstsze błędy:

- reakcja przesadna: zmiana całego trybu życia po jednym niejasnym zdarzeniu,
- reakcja niedostateczna: uznanie sprawy za zamkniętą bez żadnych wniosków,
- brak informacji zwrotnej dla osoby, która zgłosiła zdarzenie w organizacji, co zniechęca do zgłaszania w przyszłości.

Warunek zakończenia. Wiesz, co zmieniasz (albo świadomie postanawiasz niczego nie zmieniać), a organizacja ma informację o zdarzeniu.

6.8. Niepokojące komunikaty i dezinformacja

Schemat dotyczy także sytuacji, w których sygnałem jest informacja, a nie zachowanie: SMS o rzekomej ewakuacji, wiadomość o „ataku" w twojej okolicy, komunikat o mobilizacji. W maju 2024 roku przejęte konto w Polskiej Agencji Prasowej posłużyło do opublikowania fałszywej depeszy o mobilizacji, a ABW opisuje to jako klasyczny przykład działań hybrydowych.

W takiej sytuacji krok 3 polega na sprawdzeniu informacji w co najmniej jednym oficjalnym źródle: alertach RCB, stronach gov.pl, komunikatach policji i wojewody. Do czasu weryfikacji nie przesyłaj komunikatu dalej. Jeśli informacja okaże się fałszywa, możesz zgłosić ją do CERT Polska, a SMS przekazać na numer 8080.

6.9. Jak ćwiczyć procedurę

Procedura, którą zna się tylko z lektury, w stresie nie zadziała. Najprostsze sposoby ćwiczenia:

- omówienie scenariuszy z rozdziału 12 na szkoleniu zespołu, krok po kroku, z pytaniem, co uczestnicy zrobiliby na każdym etapie,
- krótkie ćwiczenia „na sucho" przed ważnym wyjazdem: „gdzie jest bezpieczne miejsce, do kogo dzwonię, jaki jest nasz umówiony sygnał",
- przegląd rzeczywistych zgłoszeń w organizacji, z zachowaniem poufności osób, które je zgłosiły.

Ćwiczenie stołowe w 45 minut. Najprostszą formą ćwiczenia zespołowego jest omówienie jednego scenariusza z podziałem na etapy. Prowadzący ujawnia kolejne informacje dopiero wtedy, gdy uczestnicy podejmą decyzję na poprzednim etapie, tak jak dzieje się to w rzeczywistości.

Czas	Co robi prowadzący	Co ćwiczą uczestnicy
0–5 min	Przedstawia cel i zasady: nie ma złych odpowiedzi, liczy się uzasadnienie decyzji.	Podział ról: kto prowadzi notatkę, kto pilnuje czasu.
5–15 min	Czyta samą sytuację ze scenariusza, np. 12.3 albo 12.8, bez sygnałów i rozwiązania.	Kroki 1–3: opis obserwacji bez ocen, ocena, czy zagrożenie jest bezpośrednie, zwyczajne wyjaśnienia.

Czas	Co robi prowadzący	Co ćwiczą uczestnicy
15–25 min	Dodaje nową informację, np. „ta sama osoba pojawia się trzeci raz" albo „ktoś pyta w barze o godziny wyjazdów".	Kroki 4–5: bezpieczne miejsce, kogo powiadomić i jakim kanałem.
25–35 min	Prosi o notatkę według wzoru z aneksu C.	Krok 6: oddzielenie faktów od ocen, poziom pewności.
35–45 min	Omawia rozwiązanie z rozdziału 12 i porównuje je z decyzjami zespołu.	Krok 7: co zmieniamy w procedurach i listach kontrolnych.

Po ćwiczeniu zapisz dwa, trzy wnioski i wróć do nich przy kolejnym przeglądzie procedur. Pytania kontrolne do sprawdzenia wiedzy uczestników zawiera aneks F, a program całego szkolenia aneks E.

7.

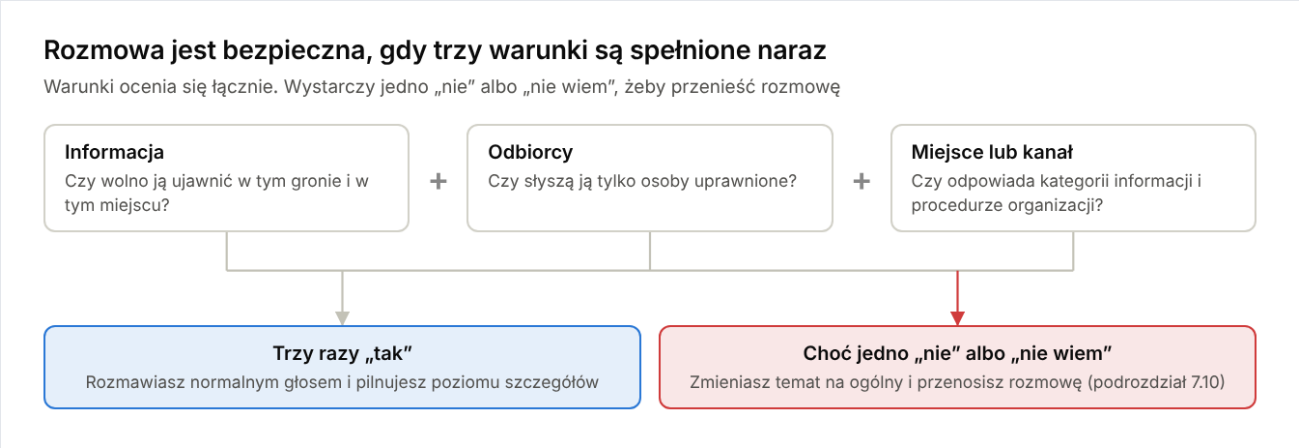
Ochrona rozmów i informacji w lokalach publicznych

Najczęstszą drogą wycieku informacji w przestrzeni publicznej nie jest technika, tylko ludzki głos, rozłożony na stole dokument i ekran widoczny dla osoby obok. ABW w swoim raporcie wprost zaleca, żeby nie omawiać spraw służbowych w kawiarniach, środkach transportu i windach oraz nie czytać materiałów wrażliwych w pociągu czy samolocie. Ten rozdział rozwija te zalecenia w praktyczne nawyki.

7.1. Dopasowanie miejsca do wrażliwości rozmowy

Rodzaj informacji	Przykłady	Gdzie omawiać
Ogólne, publiczne	Kierunki współpracy, informacje z publicznych raportów, ogólne doświadczenia branżowe	Dowolny lokal
Wewnętrzne	Organizacja pracy, wewnętrzne problemy, opinie o kontrahentach, niepubliczne plany biznesowe	W miejscu i kanale dopuszczonym przez organizację. W lokalu publicznym wyłącznie zakres wyraźnie dopuszczony do ujawnienia.
Poufne	Warunki umów, ceny, dane klientów, dane osobowe, wyniki audytów, plany inwestycyjne	W odpowiednim pomieszczeniu kontrolowanym przez organizację lub zatwierdzonym kanale, wyłącznie z uprawnionymi osobami. W lokalu publicznym nie omawiaj treści poufnych.
Wrażliwe dla bezpieczeństwa	Harmonogramy i trasy transportów, lokalizacje magazynów, zabezpieczenia obiektów, dane o infrastrukturze, informacje o projektach obronnych, logistyka pomocy dla Ukrainy	Wyłącznie w pomieszczeniach kontrolowanych i bezpiecznych kanałach
Niejawne	Informacje niejawne w rozumieniu ustawy, także bez widocznej klauzuli	Wyłącznie zgodnie z ustawą o ochronie informacji niejawnych, nigdy w lokalu

Z tabeli wynika prosta reguła: w przestrzeni publicznej omawiasz wyłącznie informacje dopuszczone do ujawnienia. Nie zakładaj, że usunięcie nazwisk, dat i lokalizacji wystarcza do zachowania poufności, bo samo „co" może ujawnić niepubliczny produkt, a „dlaczego" słabość zabezpieczeń albo problem organizacji. Informacje chronione omawiasz w odpowiednim pomieszczeniu i tylko z uprawnionymi uczestnikami, a nie w dowolnym open space czy wynajętej sali.



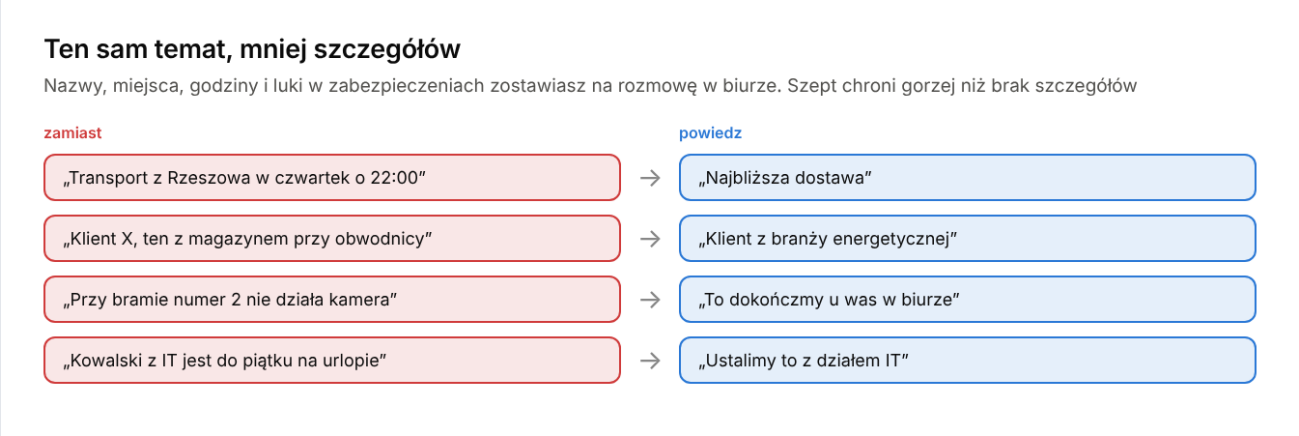
Rys. 16. Trzy warunki bezpiecznej rozmowy oceniane łącznie

7.2. Głośność i poziom szczegółów

Mów normalnym, spokojnym głosem. Szept i nachylanie się nad stołem przyciągają uwagę bardziej niż zwykła rozmowa, a szeptu i tak słychać więcej, niż się wydaje. Najskuteczniejszym zabezpieczeniem nie jest ściszanie głosu, tylko ograniczenie szczegółów.

Praktyczne zasady:

- nie wymieniaj nazwisk osób trzecich, nazw obiektów, adresów, numerów rejestracyjnych, kwot i dat, jeśli nie są niezbędne,
- zamiast „transport z Rzeszowa w czwartek o 22:00" mów „najbliższa dostawa",
- zamiast nazwy klienta mów „klient z branży energetycznej", o ile to wystarcza do zrozumienia,
- nie stosuj wymyślnych nazw kodowych tylko na potrzeby rozmowy w lokalu; jeśli organizacja używa nazw projektów, pamiętaj, że powtarzana nazwa projektu także staje się informacją,
- gdy rozmowa schodzi na szczegóły, umów się na ich omówienie w biurze lub bezpiecznym kanałem,
- zwracaj uwagę na rozmówcę: jeśli zaczyna mówić za dużo, delikatnie zmień temat („to dokończmy u was w biurze").



Rys. 17. Ten sam temat bez szczegółów operacyjnych · przykłady zdań, dane fikcyjne

Pamiętaj też o rozmowach telefonicznych prowadzonych w lokalu. Osoba obok słyszy tylko twoją część rozmowy, ale to często wystarcza, żeby odtworzyć sens. Rozmowy z głośnikiem w miejscach publicznych są niedopuszczalne przy jakiejkolwiek sprawie służbowej.

7.3. Hasła, dane dostępowe i informacje personalne

Niektórych informacji nie podaje się w lokalu publicznym w żadnej formie, nawet rozmówcy, któremu ufasz:

- haseł, kodów PIN, kodów jednorazowych i odpowiedzi na pytania bezpieczeństwa,
- loginów do systemów, adresów paneli administracyjnych, numerów VPN,
- danych z dokumentów tożsamości, numerów PESEL, numerów kont,
- danych osobowych pracowników i klientów, zwłaszcza adresów domowych i danych o zdrowiu,
- informacji o tym, kto ma dostęp do czego i kiedy jest nieobecny.

Dane dostępowe przekazuje się kanałami do tego przeznaczonymi (menedżer haseł, procedura IT), a nie ustnie przy stole. Jeśli ktoś w lokalu prosi cię o podanie hasła, kodu lub danych dostępowych, nawet w dobrej wierze, odmów i zaproponuj właściwą drogę.

Organizacje przetwarzające dane osobowe mają obowiązek stosować odpowiednie środki techniczne i organizacyjne, żeby je chronić (art. 32 RODO). Rozmowa o danych klientów przy kawiarnianym stoliku może być naruszeniem tego obowiązku.

7.4. Notatki i dokumenty

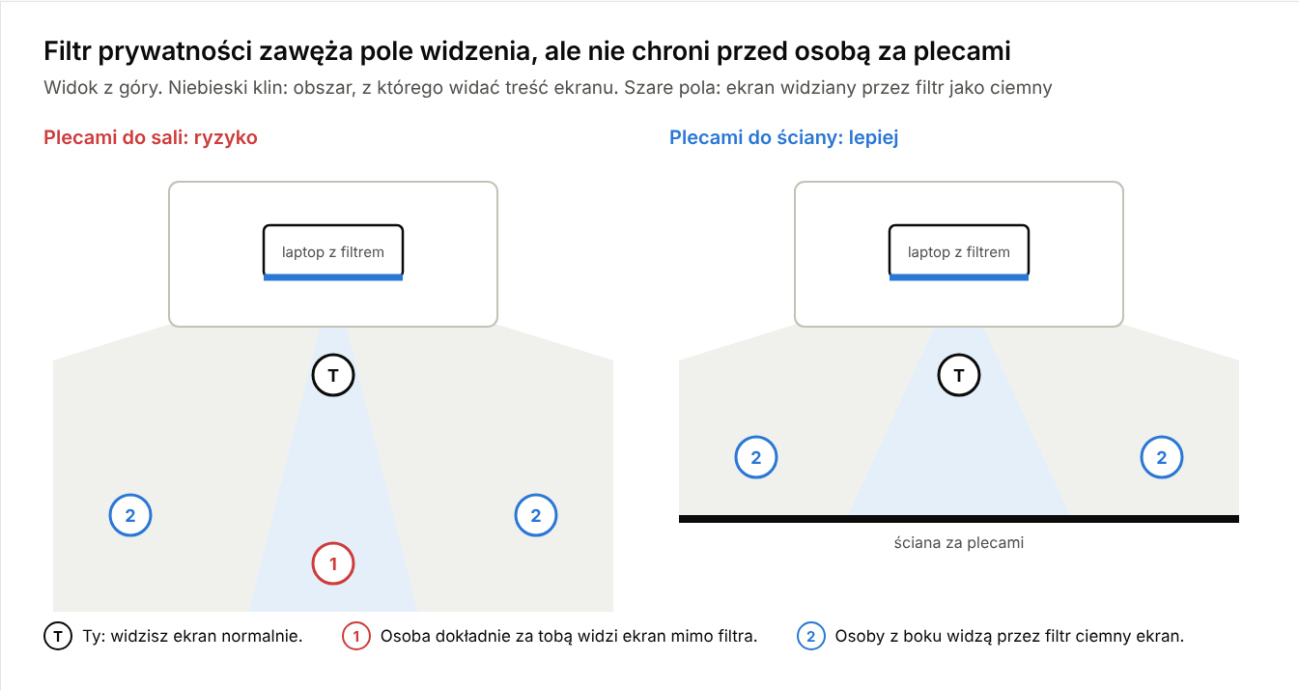
Zabieraj na spotkanie tylko te dokumenty, które są naprawdę potrzebne. Każda dodatkowa kartka to dodatkowe ryzyko zgubienia, sfotografowania lub zapomnienia na stole.

- Noś dokumenty w zamykanej teczce lub torbie, nie luzem w ręku.
- Okładka nie powinna zdradzać zawartości. Napis „poufne" na teczce przyciąga uwagę.
- Nie rozkładaj dokumentów na całym stole. Wyjmuj tylko stronę, o której rozmawiacie, i chowaj ją po omówieniu.
- Przed każdym odejściem od stołu dokumenty wracają do teczki.
- Notuj w zeszycie, który zabierasz, a nie na luźnych kartkach, serwetkach czy podkładkach.

- Pamiętaj, że wersje robocze i notatki zawierają często tyle samo informacji co dokument końcowy i wymagają takiej samej ochrony.

7.5. Ekrany laptopów, tabletów i telefonów

- Używaj filtra prywatności na ekranie laptopa. Ogranicza on widoczność pod kątem, choć nie chroni przed osobą siedzącą dokładnie za tobą.
- Ustaw laptop tak, aby treść ekranu była niewidoczna dla osób w przejściu, przy sąsiednich stolikach, za oknem oraz dla kamer. Dobierz pozycję siedzenia do układu pomieszczenia.
- Ustaw automatyczną blokadę ekranu po krótkim czasie bezczynności i przed każdym odejściem ręcznie blokuj sesję (skrót klawiszowy). Samego zamknięcia klapy nie traktuj jako potwierdzenia blokady, dopóki nie sprawdzisz ustawień urządzenia.
- Wyłącz podgląd treści powiadomień na ekranie blokady telefonu i komputera. Nagłówek wiadomości z kodem czy nazwą klienta jest widoczny dla każdego.
- Zegarki i opaski wyświetlające powiadomienia też pokazują ich treść osobie obok.
- Nie prezentuj materiałów rozmówcy na ekranie zwróconym do sali. Jeśli musisz coś pokazać, odwróć laptop tak, żeby ekran widziały tylko osoby przy stole.



Rys. 18. Filtr prywatności a pozycja przy stoliku · widok z góry, schemat poglądowy

7.6. Ryzyko podsłuchu: realne zagrożenia i mity

W lokalu wybranym przez ciebie najbardziej realnym „podsłuchem" są ludzie przy sąsiednich stolikach i personel. Na drugim miejscu jest sam rozmówca: każdy uczestnik rozmowy może ją nagrać, więc mów tak, jakby to, co mówisz, mogło zostać utrwalone. Na trzecim miejscu są urządzenia elektroniczne: twoje i rozmówcy.

Twierdzenie	Ocena
„Każdy telefon cały czas podsłuchuje rozmowy”	Mit w tej formie. Przeciętny telefon nie przesyła stale nagrań rozmów. Natomiast telefon zainfekowany oprogramowaniem szpiegującym może to robić, a osoby szczególnie interesujące dla obcych służb mogą być celem takich ataków.
„Wyłączenie telefonu wystarcza”	Częściowo. Wyłączony telefon z aktualnym systemem jest znacznie mniej ryzykowny niż włączony. Przy rozmowach najbardziej wrażliwych organizacje stosują zasadę zostawiania telefonów poza salą.
„W lokalu na pewno są ukryte mikrofony”	Mało prawdopodobne w lokalu, który wybrałeś sam, losowo spośród kilku. Bardziej prawdopodobne w lokalu wskazanym przez nieznaną stronę i w miejscach, w których spotykasz się regularnie.
„Asystent głosowy w sali hotelowej nagrywa”	Urządzenia z asystentem głosowym nasłuchują słowa aktywującego i mogą przypadkowo nagrać fragmenty rozmowy. W pokojach i salach z takimi urządzeniami warto je wyłączyć lub nie prowadzić tam rozmów wrażliwych.
„Szyfrowany komunikator chroni rozmowę przy stole”	Nie. Chroni treść przesyłaną przez sieć, nie to, co mówisz na głos.

Z tego zestawienia wynika praktyczna hierarchia: najpierw wybór miejsca i ograniczenie szczegółów, potem higiena urządzeń (rozdział 8), a dopiero na końcu, w organizacjach o wysokim profilu ryzyka, profesjonalne sprawdzanie pomieszczeń. Takie badania antypodsłuchowe wykonują wyspecjalizowane firmy, a dla organów państwa i samorządu także ABW, która w latach 2024–2025 przeprowadziła ponad 200 takich badań.

7.7. Fotografowanie dokumentów i przypadkowe nagrywanie

Współczesny lokal publiczny jest pełen kamer: monitoring, telefony gości, selfie, nagrania do mediów społecznościowych, transmisje na żywo. Skutki są dwojakie.

Celowe fotografowanie. Ktoś przechodzący obok stołu albo siedzący przy sąsiednim stoliku może sfotografować dokument lub ekran w ułamku sekundy, nie zwracając niczyjej uwagi. Jedyną skuteczną ochroną jest niewystawianie dokumentów i ekranów na widok.

Przypadkowe utrwalenie. Selfie zrobione przy sąsiednim stoliku może mieć w tle ciebie, twojego rozmówcę i rozłożone dokumenty, a następnie trafić do internetu z oznaczeniem lokalizacji i godziny. To samo dotyczy nagrań z wydarzeń branżowych, konferencji i targów. Jeśli spotkanie ma charakter poufny, sam fakt, że się odbyło, może być informacją wrażliwą.

Praktyczne wnioski: dokumenty w teczce, ekran do ściany, spotkania poufne z dala od miejsc, w których odbywają się wydarzenia nagrywane i transmitowane.

7.8. Postępowanie z dokumentami i materiałami po spotkaniu

Po spotkaniu, zanim wstaniesz od stołu:

- sprawdź stół, krzesła i podłogę: kartki, długopis z logo projektu, wizytówki, pendrive, kabel, ładowarka,

- zabierz wszystkie notatki, także te, które wydają się bezwartościowe,
- nie wyrzucaj dokumentów ani notatek do kosza w lokalu, hotelu czy na dworcu.

Po powrocie do biura lub domu:

- niszcz dokumenty zawierające dane osobowe i informacje wrażliwe w niszczarce; ABW zwraca uwagę, że skrawki papieru bywają cennym źródłem informacji dla osób trzecich,
- nie drukuj i nie kopiuj dokumentów wrażliwych w ogólnodostępnych punktach usługowych ani w hotelowych centrach biznesowych, bo urządzenia mogą przechowywać kopie w pamięci, a wydruki zostają na tacy,
- w salach konferencyjnych zmaż tablice i zabierz kartki z flipcharta,
- jeśli w wyjątkowej sytuacji korzystałeś z cudzego komputera lub drukarki, zgłoś to działowi IT i zmień hasła do kont, na które się logowałeś; wylogowanie i usunięcie pobranych plików nie potwierdzają, że urządzenie było bezpieczne.

7.9. Ślady w systemach rezerwacyjnych, wiadomościach i kalendarzach

Informacje o spotkaniu zostają w wielu miejscach, zanim jeszcze się odbędzie: w kalendarzu, w zaproszeniu, w rezerwacji, w wiadomościach organizacyjnych. Każde z tych miejsc może zostać przejęte, przeczytane przez osobę nieuprawnioną albo przekazane dalej.

Gdzie zostaje ślad	Ryzyko	Dobra praktyka
Tytuł i opis wydarzenia w kalendarzu	Widoczny dla osób z dostępem do kalendarza, asystentów, systemów integrujących kalendarz	Neutralny tytuł („Spotkanie”), szczegóły tylko w notatkach prywatnych
Lista uczestników zaproszenia	Ujawnia, kto z kim się spotyka	Zapraszaj tylko niezbędne osoby, pozostałe informuj osobno
Rezerwacja w lokalu	Nazwisko, telefon, liczba osób, uwagi	Rezerwacja na imię, bez nazwy firmy i celu
Potwierdzenia SMS i e-mail od lokalu	Kopia rezerwacji na telefonie	Porządkuj zgodnie z zasadami retencji; zachowaj, jeśli doszło do incydentu
Wiadomości organizacyjne w komunikatorach	Miejsce, godzina, temat, czasem zdjęcia dokumentów	Ograniczaj treść do niezbędnego minimum, używaj kanałów zatwierdzonych przez organizację
Publiczne linki do wideokonferencji	Możliwość dołączenia osoby nieuprawnionej	Poczekalnia, hasło, weryfikacja uczestników
Podziękowania po spotkaniu	„Dziękuję za spotkanie w X w sprawie transportu Y”	Krótkie podziękowanie bez szczegółów

Zbędne wiadomości usuwasz zgodnie z zasadami retencji organizacji. Nie usuwasz materiałów związanych z incydentem, podejrzeniem przestępstwa, sporem ani obowiązkiem zachowania dokumentacji, bo ograniczanie śladów nie oznacza natychmiastowego kasowania wszystkiego.

7.10. Przenoszenie rozmów do zabezpieczonych pomieszczeń

Gdy rozmowa w lokalu schodzi na szczegóły spraw poufnych albo dotyka spraw z dwóch najniższych wierszy tabeli w podrozdziale 7.1, właściwą reakcją jest jej przeniesienie. Nie trzeba tego uzasadniać obawami o bezpieczeństwo. Wystarczy: „To ważne, dokończmy jutro u nas, przygotuję materiały".

Organizacje, które regularnie prowadzą rozmowy o sprawach wrażliwych, powinny zapewnić pracownikom:

- sale do rozmów bez okien wychodzących na ulicę lub z odpowiednim zabezpieczeniem, z dala od przestrzeni ogólnodostępnych,
- zasady dotyczące wnoszenia telefonów i urządzeń z mikrofonami na spotkania o najwyższej wrażliwości,
- bezpieczny kanał do rozmów zdalnych z ustalonymi zasadami,
- procedurę rezerwacji sal, która nie ujawnia tematu spotkania osobom postronnym.

Dzięki temu przeniesienie rozmowy nie jest kłopotliwe i pracownicy nie mają pokusy, żeby „szybko omówić to przy kawie".

8.

Bezpieczeństwo cyfrowe podczas spotkań i podróży

Telefon i laptop zabrane na spotkanie lub w podróż zawierają zwykle więcej informacji niż wszystkie dokumenty w teczce: pocztę, kalendarz, kontakty, zdjęcia, dostęp do systemów firmy. Według raportu ABW zespół CSIRT GOV odnotował w latach 2024–2025 ponad 40 tys. zgłoszeń o potencjalnych incydentach, a system ARAKIS GOV w samym 2025 roku ponad 5,5 mln alarmów bezpieczeństwa. Agencja podkreśla, że najsłabszym ogniwem pozostaje człowiek. Ten rozdział opisuje nawyki, które ograniczają ryzyko poza biurem, i oddziela realne zagrożenia od mitów.

8.1. Zasady ogólne

- Aktualizuj system i aplikacje na bieżąco. Aktualizacje ograniczają ryzyko wykorzystania znanych, załatanych podatności.
- Zabieraj tylko te urządzenia, które są potrzebne. Laptop zostawiony w biurze nie zginie w pociągu.
- Oddzielaj sprawy służbowe od prywatnych: osobne konta, a przy wyższym ryzyku osobne urządzenia.
- Instaluj aplikacje wyłącznie z oficjalnych sklepów i zaufanych źródeł.
- Traktuj każdą nieoczekiwaną prośbę (o kod, o kliknięcie, o „pilne" działanie) jako wymagającą weryfikacji innym kanałem.

8.2. Publiczne Wi-Fi

Sieci w kawiarniach, hotelach, pociągach i na lotniskach są wygodne, ale nie masz kontroli nad tym, kto nimi zarządza i kto jeszcze jest do nich podłączony. Realne ryzyka to:

- fałszywe punkty dostępowe o nazwie łudząco podobnej do sieci lokalu, przez które przechodzi cały twój ruch,
- fałszywe strony logowania do sieci, które wyłudzają dane (np. „zaloguj się kontem firmowym, żeby uzyskać dostęp"),
- przechwytywanie ruchu nieszyfrowanego (coraz rzadsze, ale wciąż możliwe w starszych aplikacjach i usługach),
- widoczność twojego urządzenia dla innych w tej samej sieci, jeśli udostępnianie plików jest włączone.

Poprawnie działające szyfrowanie połączeń (HTTPS) chroni treść komunikacji także w publicznej sieci, nawet gdy punkt dostępowy jest fałszywy. Największym realnym ryzykiem pozostaje phishing, czyli przekierowanie na fałszywą stronę logowania, dlatego liczy się adres strony w pasku przeglądarki, a nie sama kłódka (CERT Polska, grudzień 2025). Firmowy VPN i własny hotspot mogą być wymagane przez politykę organizacji, ale VPN nie czyni niezaufanego urządzenia bezpiecznym.

Zalecenia:

- jeśli wymaga tego polityka organizacji, do pracy służbowej używaj firmowego VPN albo udostępniania internetu z własnego telefonu,
- wyłącz automatyczne łączenie ze znanymi sieciami i usuwaj z listy sieci, z których korzystałeś jednorazowo,
- wyłącz udostępnianie plików i drukarek w ustawieniach sieci publicznej,
- nigdy nie podawaj danych logowania do kont firmowych na stronie logowania do sieci lokalu,
- nie ignoruj ostrzeżeń przeglądarki o certyfikatach, sprawdzaj domenę przed zalogowaniem i nie instaluj oprogramowania ani certyfikatów, których żąda strona dostępowa sieci; do paneli administracyjnych i systemów o podwyższonych uprawnieniach łącz się tak, jak określa polityka organizacji.

8.3. Telefon i laptop poza biurem

Blokada i szyfrowanie. Ustaw blokadę ekranu z kodem co najmniej sześciocyfrowym lub hasłem, a nie wzorem rysowanym palcem, który łatwo podejrzeć. Włącz szyfrowanie dysku w laptopie (np. BitLocker w systemie Windows, FileVault w macOS). Nowoczesne telefony są szyfrowane domyślnie, o ile mają ustawioną blokadę.

Biometria. Odcisk palca i rozpoznawanie twarzy są wygodne i dobrze chronią przed przypadkowym znalazcą. Trzeba jednak pamiętać, że łatwiej wymusić przyłożenie palca niż podanie kodu. W sytuacjach podwyższonego ryzyka warto znać skrót, który chwilowo wyłącza biometrię i wymaga kodu.

Nazwa urządzenia. Telefony i laptopy rozgłaszają swoją nazwę przez Bluetooth i w sieciach Wi-Fi. Nazwa „iPhone Jana Kowalskiego" albo „Laptop-Dyrektor-Logistyki" informuje każdego w zasięgu, kto jest w pobliżu. Zmień nazwę na neutralną.

Bluetooth i udostępnianie. Wyłącz funkcje szybkiego udostępniania plików (np. AirDrop, Quick Share) lub ustaw je na „tylko kontakty". Wyłączaj Bluetooth, gdy nie jest potrzebny.

Nadzór fizyczny. ABW zaleca, żeby podczas podróży służbowych trzymać dokumenty, laptopa i telefon pod stałym, osobistym nadzorem. Nie zostawiaj laptopa w pokoju hotelowym bez zabezpieczenia, jeśli zawiera dane wrażliwe, ani w samochodzie, ani na stole w lokalu, gdy idziesz do toalety.

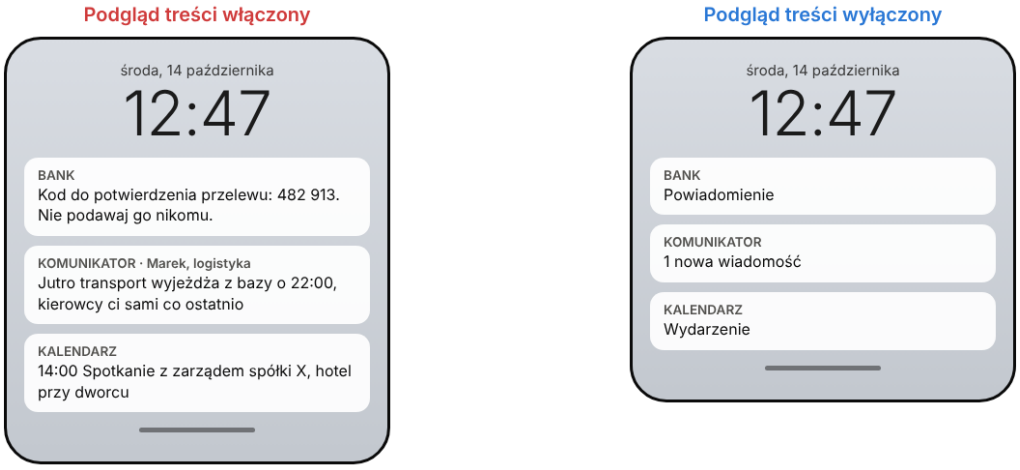
8.4. Powiadomienia

Powiadomienia są jednym z najczęściej pomijanych kanałów wycieku. Kod jednorazowy z banku, nazwa nadawcy, początek wiadomości o „jutrzejszym transporcie" pojawiają się na ekranie leżącego na stole telefonu, na zegarku i na ekranie laptopa podczas prezentacji.

- Wyłącz podgląd treści powiadomień na ekranie blokady.
- Przed prezentacją lub udostępnianiem ekranu włącz tryb „nie przeszkadzać".
- Kładź telefon ekranem do dołu albo trzymaj go w kieszeni.
- Na zegarku ogranicz powiadomienia do tych, które naprawdę muszą tam trafiać.

Ekran blokady zdradza tyle, ile pokazuje powiadomienie

Telefon leżący na stole w lokalu. Z lewej podgląd treści włączony, z prawej wyłączony (dane fikcyjne)

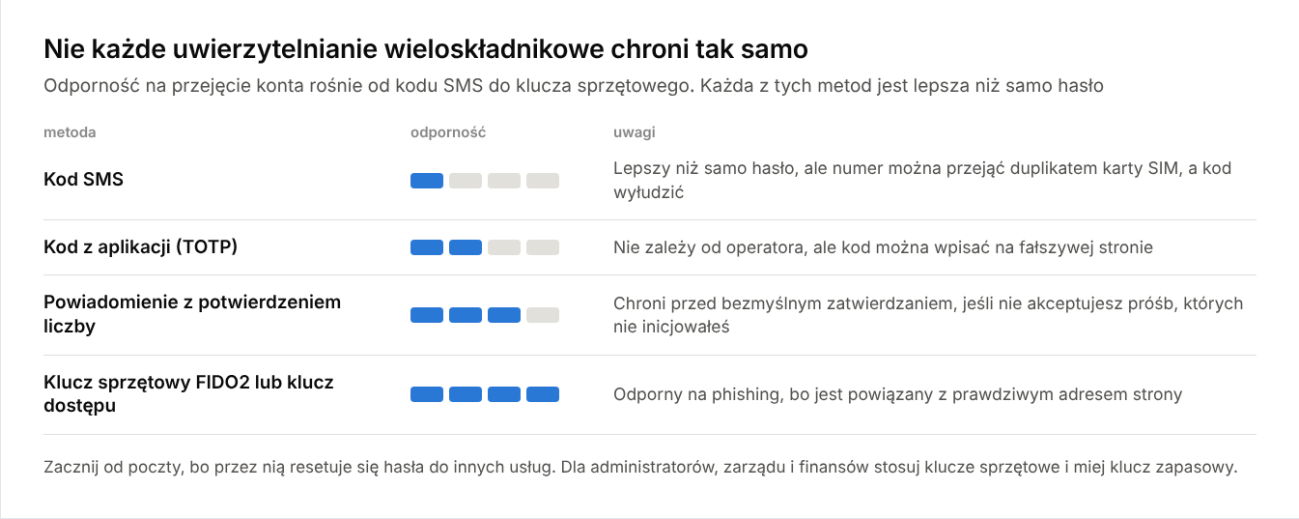


Rys. 19. Powiadomienia na ekranie blokady: podgląd treści włączony i wyłączony · dane fikcyjne

8.5. Uwierzytelnianie wieloskładnikowe i klucze sprzętowe

Uwierzytelnianie wieloskładnikowe (MFA) sprawia, że samo hasło nie wystarcza do zalogowania. To jedno z najskuteczniejszych zabezpieczeń kont, ale jego metody różnią się odpornością.

Metoda	Odporność	Uwagi
Kod SMS	Podstawowa	Lepszy niż samo hasło, ale podatny na przejęcie numeru (duplikat karty SIM) i na phishing.
Kod z aplikacji (TOTP)	Średnia	Nie zależy od operatora, ale kod można wyłudzić na fałszywej stronie.
Powiadomienie push z potwierdzeniem liczby	Średnia do wysokiej	Chroni przed bezmyślnym zatwierdzaniem, pod warunkiem, że nie zatwierdzasz próśb, których nie inicjowałeś.
Klucz sprzętowy FIDO2 lub klucz dostępu (passkey)	Wysoka	Odporny na phishing, bo jest powiązany z prawdziwym adresem strony. Warto mieć klucz zapasowy przechowywany w bezpiecznym miejscu.



Rys. 20. Metody uwierzytelniania wieloskładnikowego według odporności na przejęcie konta

Zasady praktyczne:

- włącz MFA na wszystkich kontach, które na to pozwalają, w pierwszej kolejności na poczcie, bo przez nią resetuje się hasła do innych usług,
- dla kont najważniejszych dla organizacji (administratorzy, zarząd, finanse) stosuj klucze sprzętowe,
- nigdy nie przekazuj nikomu kodu jednorazowego, także osobie podającej się za pracownika banku, IT czy służb,
- jeśli dostajesz serię próśb o zatwierdzenie logowania, których nie inicjowałeś, nie zatwierdzaj żadnej i zgłoś to do IT; może to wskazywać na próbę nieuprawnionego logowania, w tym z użyciem przejętego hasła.

8.6. Lokalizacja i metadane

Twoje urządzenia nieustannie wytwarzają informacje o tym, gdzie jesteś. Część z nich trafia do aplikacji, część do zdjęć, część do usług, z których korzystasz.

- Przejrzyj uprawnienia aplikacji do lokalizacji i zostaw je tylko tym, które naprawdę ich potrzebują (mapy, taksówki), najlepiej w trybie „tylko podczas używania".
- Wyłącz zapisywanie historii lokalizacji w koncie Google lub Apple, jeśli nie jest ci potrzebne.
- Zdjęcia z telefonu zawierają zwykle metadane EXIF, w tym współrzędne GPS i czas. Niektóre komunikatory usuwają je przy wysyłaniu, ale poczta elektroniczna i chmury zwykle nie. Przed udostępnieniem zdjęcia na zewnątrz usuń metadane lub wyłącz zapisywanie lokalizacji w aparacie.
- Patrz na tło zdjęć: identyfikator na smyczy, ekran laptopa, tablica z harmonogramem, okno z widokiem na charakterystyczny budynek, plan obiektu na ścianie.
- Aplikacje sportowe z publicznymi profilami potrafią ujawnić miejsce zamieszkania, hotel i codzienny rytm. Ustaw profil jako prywatny i stwórz strefy prywatności wokół domu.
- Udostępnianie lokalizacji rodzinie lub zespołowi włączaj na czas konkretnej podróży, nie na stałe.
- Telefony z aktualnym systemem ostrzegają o nieznanych lokalizatorach Bluetooth (np. typu AirTag) przemieszczających się z tobą. Nie ignoruj takiego ostrzeżenia. Jeśli znajdziesz w swoich rzeczach lub w samochodzie nieznany lokalizator, nie niszcz go, tylko zgłoś sprawę na policję.

8.7. Nieznane kable, ładowarki, nośniki i kody QR

Ładowanie z cudzych portów USB. Publiczne porty USB (lotniska, pociągi, hotele) mogą teoretycznie służyć do przesyłania danych, a nie tylko zasilania. Udokumentowanych ataków tego typu na szeroką skalę jest niewiele, ale ochrona jest prosta: używaj własnej ładowarki podłączonej do gniazdka elektrycznego albo własnego powerbanku. Przy ładowaniu z obcego portu możesz użyć adaptera blokującego transmisję danych.

Kable i ładowarki od nieznajomych. Kabel wyglądający jak zwykły przewód może zawierać elektronikę. Nie używaj kabli pozostawionych w salach konferencyjnych, otrzymanych od przypadkowych osób ani gadżetów rozdawanych bez wyraźnego źródła.

Pendrive'y i dyski. ABW zaleca, żeby nigdy nie wpinać do swoich urządzeń znalezionych lub nieznanych nośników. Dotyczy to także nośników otrzymanych na konferencjach i targach. Jeśli musisz przyjąć materiały na nośniku, przekaż je do sprawdzenia działowi IT.

Kody QR. ABW opisuje rosnące zagrożenie tzw. quishingiem: fałszywe kody QR rozsyłane w wiadomościach i naklejane w przestrzeni publicznej, np. na parkometrach i biletomatach. Przed otwarciem strony z kodu QR sprawdź pełny adres. Do płatności za parking i bilety używaj oficjalnych aplikacji, a nie kodów naklejonych na urządzeniach.

8.8. Ochrona kont, sesji i kopii zapasowych

- Używaj menedżera haseł i unikalnego, długiego hasła dla każdej usługi.
- Regularnie przeglądaj listę aktywnych sesji i zalogowanych urządzeń w najważniejszych kontach (poczta, chmura, media społecznościowe, komunikatory) i kończ te, których nie rozpoznajesz.
- Nie używaj niezaufanych komputerów (centrum biznesowe, sala konferencyjna) do kont służbowych i informacji wrażliwych. Wylogowanie i usunięcie pobranych plików nie potwierdzają, że urządzenie było bezpieczne, dlatego po wyjątkowym użyciu zmień hasła i poinformuj dział IT.
- Sprawdź, które urządzenia mają dostęp do twojego komunikatora w wersji przeglądarkowej lub desktopowej. Sparowanie komunikatora z obcym komputerem to prosty sposób na odczytywanie korespondencji.
- Twórz regularne kopie zapasowe najważniejszych danych, szyfrowane i chronione MFA.
- Nie przesyłaj haseł ani skanów dokumentów tożsamości pocztą elektroniczną ani komunikatorami.

8.9. Procedura przy utracie urządzenia

Utrata telefonu lub laptopa jest najczęściej zwykłą kradzieżą lub zgubieniem, ale skutki dla bezpieczeństwa informacji zależą od szybkości reakcji. Poniższa kolejność zakłada, że urządzenie służbowe lub prywatne zawiera dostęp do kont służbowych. Kolejność szczegółowych działań zależy od okoliczności i procedury organizacji. Wskazane etapy nie oznaczają zgody na zwlekanie z zabezpieczeniem urządzenia, numeru telefonu lub kont.

Kiedy	Działanie
Niezwłocznie po stwierdzeniu utraty	Z zaufanego urządzenia uruchom dostępną zdalną blokadę i powiadom dział IT lub bezpieczeństwa. Nie odkładaj kontaktu z operatorem i bankiem, jeśli zagrożone są karta SIM lub usługi finansowe. Nie jedź samodzielnie pod adres wskazany przez usługę lokalizacji.

Kiedy	Działanie
Bez zbędnej zwłoki, zgodnie z procedurą	Zabezpiecz konta: zakończ sesje na utraconym urządzeniu, zmień hasła zgodnie z oceną ryzyka i zaleceniami IT oraz sprawdź ustawienia odzyskiwania dostępu i przekierowania poczty. Działaj z innego, zaufanego urządzenia.
W porozumieniu z IT	Zdalne wymazanie danych to decyzja podejmowana w porozumieniu z działem IT, z uwzględnieniem ryzyka ujawnienia informacji i możliwości zabezpieczenia śladów. Wykonanie oraz wpływ wymazania na dalsze lokalizowanie zależą od urządzenia, systemu i dostępności połączenia. Samo wysłanie polecenia nie oznacza potwierdzenia jego wykonania. Nie usuwaj pochopnie urządzenia z konta producenta.
Tego samego dnia	Zgłoś kradzież lub zgubienie na policji, podając numer IMEI telefonu lub numer seryjny laptopa.
Jeśli zginęły też dokumenty	Zgłoś utratę dowodu osobistego i zastrzeż numer PESEL w aplikacji lub serwisie mObywatel albo w urzędzie gminy.
W kolejnych dniach	Uprzedź kontakty, że ktoś może podszywać się pod ciebie. Obserwuj powiadomienia o nietypowych logowaniach i operacjach.



Rys. 21. Kolejność działań po utracie telefonu lub laptopa · na podstawie tabeli w podrozdziale 8.9

Zastrzeżenie numeru PESEL jest bezpłatne i można je cofnąć w dowolnym momencie. Od 1 czerwca 2024 roku banki i inne instytucje mają obowiązek sprawdzać, czy numer jest zastrzeżony, przed zawarciem m.in. umowy kredytu (informacja samorządowa za Ministerstwem Cyfryzacji). Wiele osób utrzymuje numer zastrzeżony na stałe i cofa zastrzeżenie tylko na czas załatwiania konkretnej sprawy.

8.10. Podejrzenie naruszenia

Sygnały, że konto lub urządzenie mogło zostać przejęte: nieznane logowania, wiadomości wysłane bez twojej wiedzy, zmienione ustawienia przekierowań, prośby o zatwierdzenie logowania, których nie inicjowałeś, nagła utrata dostępu do konta, nietypowe zachowanie urządzenia połączone z innymi sygnałami.

Co robić:

- nie wpadaj w panikę i nie wymazuj urządzenia samodzielnie, bo to niszczy ślady potrzebne do ustalenia, co się stało,
- odłącz urządzenie od sieci, jeśli dział IT tak zaleci,
- z innego, zaufanego urządzenia zmień hasła i zakończ sesje,

- zgłoś incydent do działu IT lub bezpieczeństwa,
- incydenty niezwiązane z organizacją, która ma własny zespół reagowania, możesz zgłosić do CERT Polska przez formularz na stronie incydent.cert.pl lub na adres cert@cert.pl; podejrzane SMS-y przekazuj na numer 8080,
- jeśli podejrzewasz, że atak ma związek z działaniem obcych służb (np. celowany phishing w związku z twoim projektem obronnym), poinformuj także pełnomocnika ochrony informacji lub ABW.

8.11. Rekrutacja i rozpoznanie przez komunikatory i media społecznościowe

Twoja obecność w internecie to dla kogoś z zewnątrz pierwsze źródło informacji o tym, czy warto się tobą zainteresować. Profil zawodowy z opisem „kierownik transportów sprzętu na wschód, terminal X, zespół 12 osób" podpowiada, gdzie jesteś, do czego masz dostęp i kogo znasz.

Ograniczanie widoczności:

- w profilach zawodowych opisuj kompetencje, a nie szczegóły obiektów, projektów i klientów,
- nie publikuj zdjęć z wnętrza obiektów, identyfikatorów, ekranów, tablic, planów, pojazdów z numerami,
- ogranicz widoczność listy kontaktów i grup, do których należysz,
- nie potwierdzaj publicznie udziału w spotkaniach i wyjazdach o charakterze wrażliwym.

Rozpoznawanie podejrzanych kontaktów. ABW opisuje masowe działania werbunkowe prowadzone przez internet, w tym przez portale społecznościowe, przy czym oficerowie wywiadu pod pozorem dobrze płatnych zleceń próbowali pozyskiwać ekspertów, naukowców, urzędników i osoby związane z resortami siłowymi. Uważaj na:

- „rekruterów" i „firmy doradcze", które oferują wysokie honoraria za krótkie raporty, konsultacje lub analizy dotyczące twojej branży,
- prośby o materiały „tylko do wglądu", o opis organizacji pracy czy o kontakty do innych osób,
- profile bez historii, z idealnymi zdjęciami, z siecią kontaktów zbudowaną w krótkim czasie,
- zaproszenia do zamkniętych grup w komunikatorach z „ofertami pracy",
- kontakt, który szybko przechodzi z oficjalnej platformy do prywatnego komunikatora.

Weryfikuj takie kontakty niezależnym kanałem (oficjalna strona firmy, telefon do recepcji, rejestr KRS) i informuj o nich dział bezpieczeństwa. Przy podejrzeniu działania obcych służb zgłoś sprawę do ABW. Zasady reakcji na oferty „łatwego zarobku" opisuje rozdział 4.9.

8.12. Podróże zagraniczne

Przy wyjazdach do państw o podwyższonym ryzyku warto stosować kilka dodatkowych zasad, zwykle określonych w procedurach organizacji:

- urządzenia „podróżne" z minimalną ilością danych i dostępem tylko do niezbędnych kont, zamiast codziennego laptopa i telefonu,
- świadomość, że w niektórych państwach służby graniczne mogą żądać odblokowania urządzeń,
- unikanie hotelowych komputerów, drukarek i sejfów jako miejsca przechowywania danych wrażliwych,
- po powrocie przegląd urządzeń przez dział IT, jeśli były poza twoją kontrolą (np. zabrane do kontroli).

8.13. Realne zagrożenia i mity

Twierdzenie	Ocena
„Mam silne hasło, więc MFA nie jest potrzebne"	Fałsz. Hasła wyciekają z baz innych usług i są wyłudzane. MFA chroni nawet po wycieku hasła.
„Tryb incognito ukrywa mnie w sieci"	Fałsz. Ukrywa historię na urządzeniu, nie ruch przed dostawcą sieci ani stronami.
„VPN czyni mnie anonimowym"	Fałsz w tej formie. Szyfruje ruch do serwera VPN, co ogranicza podgląd w sieci lokalnej, ale nie zapewnia anonimowości i nie czyni niezaufanego urządzenia bezpiecznym.
„Każdy publiczny port USB kradnie dane"	Przesada. Ryzyko istnieje, a tani i prosty środek (własna ładowarka) wyraźnie je ogranicza.
„Telefon wyłączony nie wysyła lokalizacji"	Zwykle prawda dla telefonu naprawdę wyłączonego, choć niektóre modele obsługują lokalizowanie także w trybie niskiego zasilania. Przy rozmowach najbardziej wrażliwych telefon zostaje poza salą.
„Phishing łatwo rozpoznać po błędach"	Fałsz. Wiadomości są coraz lepiej przygotowane, wysyłane z przejętych skrzynek instytucji i opatrzone prawdziwymi logotypami, co ABW opisuje jako rosnący problem.
„Nikt nie będzie się mną interesował"	Nie wiadomo. Atak nie musi być wymierzony w ciebie osobiście. Twoje konto może być drogą do organizacji, klienta albo osoby, z którą się kontaktujesz.

8.14. Narzędzia AI, transkrypcje i asystenci spotkań

Przed użyciem narzędzia AI ustal, czy przetwarzanie odbywa się lokalnie, w infrastrukturze organizacji czy u zewnętrznego dostawcy. Sprawdź zasady przechowywania danych, dostępu do nich i ewentualnego wykorzystania treści do trenowania modeli. Nie zakładaj, że samo oznaczenie usługi jako „AI" przesądza o którymkolwiek z tych elementów. Gdy narzędzie przetwarza dane osobowe, obowiązują przepisy o ich ochronie (UODO, Sztuczna inteligencja). Wygoda narzędzia nie zmienia zasad ochrony informacji.

Zasady organizacyjne:

- nie przesyłasz dokumentów służbowych do chatbotów, których organizacja nie zatwierdziła,
- przed uruchomieniem transkrypcji lub nagrania uczestnicy znają zasady: kto ma dostęp do zapisu, gdzie jest przechowywany i jak długo,
- na początku wideokonferencji sprawdzasz listę uczestników, w tym boty i asystentów, które dołączyły automatycznie,
- ustalasz, dokąd trafiają nagrania, streszczenia i załączniki, zanim rozmowa zejdzie na sprawy wrażliwe,
- wygenerowanego streszczenia nie traktujesz jako wiernego zapisu, dopóki ktoś z uczestników go nie sprawdzi.

Narzędzia AI, w tym automatyczną transkrypcję, stosujesz tylko w zakresie dopuszczonym dla danej kategorii informacji, zgodnie z przepisami i procedurami organizacji.

8.15. Podszywanie się pod instytucje, fałszywe połączenia i deepfake

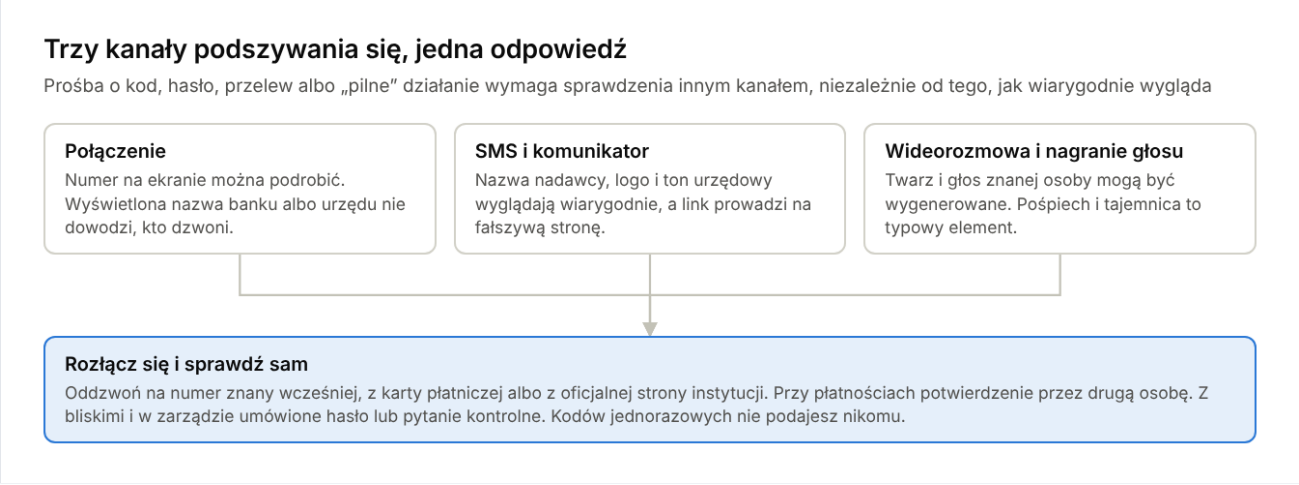
Atakujący coraz częściej nie łamią zabezpieczeń technicznych, tylko podszywają się pod kogoś, komu ufasz: bank, urząd, dział IT, przełożonego, partnera biznesowego. Numer wyświetlany przy połączeniu i nazwę nadawcy SMS-a da się podrobić. Od 25 września 2023 roku obowiązuje ustawa z 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej. Operatorzy muszą na jej podstawie blokować SMS-y wyłudzające dane według wzorców przekazywanych przez CSIRT NASK, a połączenia z prawdopodobnie podrobionym numerem blokować albo ukrywać numer dzwoniącego. Ustawa nadała też rangę ustawową liście ostrzeżeń przed niebezpiecznymi domenami, a za nadużycia w komunikacji elektronicznej grozi kara od 3 miesięcy do 5 lat pozbawienia wolności (e-prawnik.pl, Rzeczpospolita). Filtry operatorów nie wychwycą jednak każdej próby, dlatego decyduje twoja reakcja.

Nowym elementem są nagrania i wideorozmowy wygenerowane przez sztuczną inteligencję. Na początku 2024 roku pracownik działu finansów firmy Arup w Hongkongu wykonał 15 przelewów na łączną kwotę 200 mln dolarów hongkońskich, czyli około 25,6 mln dolarów amerykańskich, po wideorozmowie, w której dyrektor finansowy i inni współpracownicy byli w rzeczywistości wygenerowanymi postaciami. Firma potwierdziła, że użyto fałszywych głosów i obrazów (CNN).

Zasady:

- prośbę o kod, hasło, przelew, zmianę danych albo „pilne" działanie sprawdzasz innym kanałem: rozłączasz się i oddzwaniasz na numer znany wcześniej, wydrukowany na karcie płatniczej albo podany na oficjalnej stronie instytucji,
- nie oddzwaniasz na numer podany w wiadomości i nie otwierasz linku z SMS-a „od banku" czy „od urzędu"; do serwisu wchodzisz, wpisując adres samodzielnie,
- przy płatnościach i zmianach rachunków stosujesz zasadę dwóch osób, także wtedy, gdy polecenie wydaje przełożony w wideorozmowie (podrozdział 14.4),
- z bliskimi i w zarządzie umawiacie hasło lub pytanie kontrolne na wypadek telefonu z prośbą o pieniądze albo pilną decyzję,
- pośpiech, prośba o tajemnicę i przeniesienie rozmowy do prywatnego komunikatora to sygnały ostrzegawcze, nawet gdy obraz i głos wyglądają wiarygodnie,
- podejrzane SMS-y przekazujesz na numer 8080, a niebezpieczne strony zgłaszasz do CERT Polska przez incydent.cert.pl.

Bank nie poprosi cię o podanie kodu jednorazowego, a policja i inne służby nie zlecają obywatelom przelewów „na bezpieczne konto" ani zadań przez komunikator. Jeśli rozmowa zmierza w tę stronę, przerywasz ją bez względu na to, kim przedstawia się rozmówca.



Rys. 22. Kanały podszywania się i jedna zasada reakcji

9.

Bezpieczeństwo podczas spotkań z nieznanymi osobami

Spotkanie z osobą, której nie znasz osobiście, to codzienność w biznesie, dziennikarstwie i doradztwie. Prawie zawsze jest dokładnie tym, czym się wydaje. Zasady z tego rozdziału nie mają podważać zaufania do nowych kontaktów, tylko sprawić, że pierwsze spotkanie odbywa się na twoich warunkach, a ewentualna próba manipulacji zostanie zauważona wcześnie.

9.1. Weryfikacja tożsamości i uzasadnienia spotkania

Zanim zgodzisz się na spotkanie, ustal dwie rzeczy: czy osoba jest tym, za kogo się podaje, i czy powód spotkania ma sens.

Weryfikacja tożsamości:

- sprawdź firmę lub instytucję w niezależnym źródle: oficjalna strona, rejestr KRS lub CEIDG, publiczne informacje o zarządzie,
- zadzwoń do firmy na numer ze strony internetowej lub rejestru, a nie na numer podany w wiadomości, i zapytaj, czy dana osoba tam pracuje i czy kontaktowała się w twojej sprawie,
- zwróć uwagę na domenę poczty: adres z darmowej skrzynki albo domena różniąca się jedną literą od prawdziwej to sygnał ostrzegawczy,
- sprawdź historię profilu zawodowego: kiedy powstał, ile ma kontaktów, czy ma rekomendacje od realnych osób, czy zdjęcie nie pojawia się w innych miejscach pod innym nazwiskiem,
- jeśli osoba powołuje się na wspólnego znajomego, zapytaj tego znajomego bezpośrednio.

Osoby podające się za funkcjonariuszy. Funkcjonariusz powinien mieć legitymację służbową. Sprawdź dane i w razie wątpliwości zweryfikuj tożsamość przez oficjalny kanał danej służby. W razie wątpliwości możesz zweryfikować tożsamość, dzwoniąc do jednostki na numer z oficjalnej strony (dla ABW: dyżurny oficer operacyjny, aneks B). Nie korzystaj z numeru podanego przez rozmówcę.

Weryfikacja uzasadnienia:

- czy temat spotkania odpowiada twojej roli i temu, czym zajmuje się rozmówca,
- czy forma kontaktu jest typowa dla tej branży,
- czy jest presja czasu („musimy się spotkać jeszcze dziś"), której nie da się wyjaśnić,
- czy rozmówca unika podania szczegółów przed spotkaniem albo nalega na rozmowę wyłącznie w cztery oczy.

9.2. Wybór miejsca i czasu

Przy pierwszym spotkaniu z nieznaną osobą:

- ty proponujesz miejsce albo akceptujesz tylko miejsce publiczne, które znasz,
- spotkanie odbywa się w dzień lub wczesnym wieczorem,
- miejsce nie jest położone przy obiekcie, którego dotyczy twoja praca,
- nie spotykasz się w swoim domu, w mieszkaniu rozmówcy, w samochodzie ani w pomieszczeniach firmy, której nie znasz,
- z góry określasz czas trwania („mam godzinę"),
- przy podwyższonym ryzyku przychodzisz z drugą osobą z organizacji.

9.3. Informowanie zaufanej osoby

O spotkaniu z nieznaną osobą powinien wiedzieć ktoś zaufany: z kim się spotykasz (imię, nazwisko, firma, dane kontaktowe), gdzie i o której, kiedy planujesz skończyć. Ustal godzinę kontrolną i umówiony sygnał (rozdział 1.6). Po spotkaniu daj znać, że wszystko jest w porządku, i krótko przekaż wrażenia, jeśli coś cię zaniepokoiło.

9.4. Przekazywanie dokumentów i urządzeń

- Przekazuj tylko dokumenty jawne lub takie, których przekazanie jest uzgodnione z organizacją. Wersje robocze i notatki zostają u ciebie.
- Nie przekazuj oryginałów. Jeśli coś musi zostać przekazane, przekaż kopię lub wersję elektroniczną oficjalnym kanałem.
- Nie przyjmuj pendrive'ów, dysków ani innych nośników do odczytania na miejscu. Jeśli rozmówca chce przekazać materiały, poproś o przesłanie ich na służbowy adres, gdzie przejdą kontrolę bezpieczeństwa.
- Nie pozwalaj nikomu „na chwilę" skorzystać ze swojego laptopa lub telefonu i nie podłączaj urządzeń rozmówcy do swoich.
- Nie przyjmuj paczek ani przesyłek do przekazania komuś innemu. ABW wymienia przewożenie paczek i przyjmowanie upominków od nowo poznanych osób jako klasyczną metodę kompromitacji i werbunku.
- Prezenty przyjmuj tylko zgodnie z polityką organizacji. Zasada wzajemności (otrzymałem, więc wypada się odwdzięczyć) jest jednym z najstarszych mechanizmów budowania zależności.
- Płać za siebie. Wspólny rachunek opłacony przez rozmówcę jest drobiazgiem, ale przy kolejnych spotkaniach tworzy nierównowagę.

9.5. Presja psychologiczna, wymuszanie informacji i manipulacja

Próby wydobycia informacji rzadko przyjmują formę bezpośredniego pytania o tajemnicę. Częściej są to rozmowy, które wydają się zwyczajne, a mimo to prowadzą do ujawnienia szczegółów. W literaturze kontrwywiadowczej nazywa się to wyciąganiem informacji (ang. elicitation). Poniższe techniki są dobrze znane i warto umieć je rozpoznać.

Technika	Jak brzmi	Jak odpowiedzieć
Fałszywe stwierdzenie	„Słyszałem, że te transporty idą zawsze w nocy przez Hrubieszów." Liczy się na odruch korygowania.	Nie potwierdzaj i nie poprawiaj: „Nie wiem, nie zajmuję się tym".
Pochlebstwo kompetencji	„Pan jest jedyną osobą, która naprawdę rozumie, jak działa ten system."	Podziękuj i nie rozwijaj tematu.
Udawana niewiedza	„Nie znam się na tym, jak to w ogóle wygląda u was od środka?"	Odpowiedz ogólnie, odeślij do publicznych materiałów.
Pytanie hipotetyczne	„Gdyby ktoś chciał to zakłócić, gdzie byłby najsłabszy punkt?"	Nie spekuluj o słabych punktach, nawet hipotetycznie.
Wymiana „poufności"	Rozmówca zdradza coś rzekomo tajnego i czeka na rewanż.	Nie odwzajemniaj. Zanotuj, co ci powiedział.
Stopniowanie próśb	Najpierw publiczny raport, potem wewnętrzna prezentacja, potem „tylko jeden plik".	Granica jest na pierwszej rzeczy niejawnej dla otoczenia.
Pośpiech	„Potrzebuję tego na jutro, inaczej projekt upadnie."	Pilność nie zmienia zasad. „Prześlę przez dział, w trybie standardowym."
Autorytet	„Dyrektor X już się zgodził, to tylko formalność."	Zweryfikuj bezpośrednio u dyrektora.
Tajemnica i wyjątkowość	„Niech to zostanie między nami, nie mów nikomu w firmie."	To silny sygnał ostrzegawczy. Poinformuj dział bezpieczeństwa.
Poczucie winy i sympatia	„Pomagamy Ukrainie, a ty utrudniasz."	Cel nie uzasadnia omijania procedur. Wskaż właściwą drogę.
Alkohol i swobodna atmosfera	Rozmowy „po godzinach", długie kolacje, imprezy.	Pij mniej niż rozmówca albo wcale. Nie rozmawiaj o pracy po alkoholu.

Ogólna zasada brzmi: im bardziej rozmowa dotyczy twojego dostępu, uprawnień, harmonogramów, słabości organizacji i ludzi z twojego otoczenia, tym bardziej powinieneś przesunąć ją na poziom ogólny lub zakończyć.

ABW zaleca także higienę relacji: unikanie dwuznacznych sytuacji, które w przyszłości mogłyby stać się podstawą szantażu. Nie chodzi o moralizowanie, tylko o to, żeby nikt nie miał w ręku czegoś, czym mógłby cię naciskać.

9.6. Bezpieczne zakończenie spotkania

- Określ czas spotkania na początku. Zakończenie po godzinie nie wymaga wtedy wyjaśnień.
- Używaj neutralnych formuł: „Dziękuję, muszę już iść, wrócę z odpowiedzią do piątku".
- Nie zgadzaj się na odprowadzenie do samochodu, podwiezienie ani wspólne wyjście „w tę samą stronę", jeśli tego nie chcesz.
- Nie mów, dokąd idziesz po spotkaniu.
- Po wyjściu daj znać zaufanej osobie i zapisz najważniejsze ustalenia oraz sygnały, które zwróciły twoją uwagę.

9.7. Gdy rozmówca narusza granice

Naruszeniem granic jest każde zachowanie, które wykracza poza normalną rozmowę biznesową: dotyk, którego nie chcesz, groźby, sugestie szantażu, ujawnienie, że rozmówca zna szczegóły twojego życia prywatnego, nalegania po twojej odmowie, próba zabrania ci dokumentów lub telefonu, informacja, że rozmowa jest nagrywana bez twojej zgody, próba zatrzymania cię przy stole.

Co robisz:

1. Kończysz spotkanie krótko i stanowczo, bez dyskusji: „Kończymy na tym".
2. Wstajesz i idziesz w stronę obsługi, wyjścia, ludzi. Przy agresji lub groźbie dzwonisz pod 112.
3. Nie wdajesz się w kłótnię ani w tłumaczenia.
4. Po odzyskaniu bezpieczeństwa informujesz zaufaną osobę i dział bezpieczeństwa.
5. Sporządzasz notatkę z możliwie dokładnym zapisem słów rozmówcy.
6. Przy groźbach, szantażu lub próbie wymuszenia informacji zgłaszasz sprawę na policję, a przy sygnałach działania obcych służb do ABW.

9.8. Profesjonalne sposoby odmowy

Odmowa udzielenia informacji nie musi być niegrzeczna i nie wymaga uzasadnienia. Kilka formuł, które dobrze sprawdzają się w praktyce:

- „Tego nie mogę omawiać, ale chętnie powiem, co jest w naszym publicznym raporcie."
- „To pytanie do naszego działu komunikacji, przekażę kontakt."
- „Nie zajmuję się tym obszarem, więc nie chcę wprowadzać w błąd."
- „Takie rzeczy przekazujemy wyłącznie w ramach umowy i przez dział prawny."
- „Wolałbym zostać przy ogólnych sprawach, szczegóły omówimy, jak podpiszemy porozumienie o poufności."
- „Nie przyjmuję prezentów, takie mamy zasady, ale dziękuję za gest."
- „Nie mogę tego przekazać dalej bez zgody przełożonego."

Powtarzaj tę samą formułę, jeśli rozmówca naciska. Zmienianie uzasadnień zachęca do szukania luk.

9.9. Kontakty inicjowane przez nieznane osoby w kontekście 2025–2026

Ze względu na skalę opisaną w rozdziale o kontekście, szczególną ostrożność należy zachować wobec nieoczekiwanych kontaktów, które łączą propozycję współpracy, łatwego zarobku albo pomocy z zainteresowaniem logistyką, energetyką, obronnością lub wsparciem Ukrainy. Przykładowe wzorce:

Kontakt	Na co zwrócić uwagę
„Fundacja" lub „wolontariusz" oferuje pomoc w transporcie darów i pyta o trasy, terminy, miejsca załadunku	Czy organizacja istnieje w rejestrze, ma historię działalności, czy pytania nie wykraczają poza to, co potrzebne do współpracy.
„Dziennikarz" zagranicznego medium pyta o lokalizacje magazynów lub obiektów	Czy redakcja potwierdza współpracę z tą osobą, czy pytania dotyczą informacji, których dziennikarz nie mógłby opublikować.

Kontakt	Na co zwrócić uwagę
„Student" lub „badacz" prosi o dane techniczne do pracy o odporności infrastruktury	Czy uczelnia i promotor istnieją, czy zakres danych jest proporcjonalny do celu, czy prośba przyszła oficjalną drogą.
„Firma doradcza" oferuje wysokie honorarium za krótki raport o branży	Czy firma istnieje i ma klientów, czy płaci za informacje, które nie są publiczne, czy kontakt szybko przechodzi do prywatnego komunikatora.
Nowy znajomy z siłowni, kursu, portalu randkowego szybko interesuje się twoją pracą	Czy zainteresowanie jest proporcjonalne do znajomości, czy wraca do tych samych tematów.
Osoba z pozoru przypadkowa prosi o „drobną przysługę" związaną z pracą: wpuszczenie na teren, wydruk, zdjęcie, przekazanie paczki	Każda taka prośba wymaga odmowy i zgłoszenia, niezależnie od tego, jak niewinnie brzmi.

W każdym z tych przypadków dobra reakcja jest podobna: przekazuj tylko informacje publiczne, kieruj rozmówcę do oficjalnych kanałów organizacji, weryfikuj jego tożsamość niezależną drogą i informuj dział bezpieczeństwa. Jeśli sygnały wskazują na możliwe działanie obcych służb, zgłoś sprawę do ABW, nawet jeśli nie masz pewności. Zgłoszenie przekazuje fakty instytucji, która potrafi je ocenić, i nikogo nie oskarża.

10.

Rutyny, nawyki i ograniczanie przewidywalności

Przewidywalność jest dla osoby z zewnątrz najtańszym źródłem informacji. Jeśli wiadomo, że codziennie o 7:40 wychodzisz z domu, o 12:30 jesz lunch w tej samej restauracji, a w czwartki wieczorem biegasz tą samą trasą, nie trzeba nikogo śledzić, żeby wiedzieć, gdzie będziesz. Rutyny mają jednak także dobrą stronę: porządkują dzień, zmniejszają zmęczenie decyzjami i utrwalają bezpieczne nawyki. Celem tego rozdziału nie jest walka z rutyną, tylko świadome decydowanie, które jej elementy są widoczne dla innych.

10.1. Co ujawnia przewidywalność

Element rutyny	Co z niego wynika dla obserwatora
Stałe godziny wyjścia z domu i powrotu	Kiedy dom jest pusty, kiedy można cię spotkać przed drzwiami.
Ten sam lokal na lunch lub spotkania	Gdzie usiąść, żeby słuchać twoich rozmów.
Stała trasa biegania lub spaceru z psem	Gdzie jesteś sam, w jakich godzinach.
Miejsce parkingowe z nazwiskiem lub stanowiskiem	Który samochód jest twój, kiedy przyjeżdżasz i odjeżdżasz.
Publiczny kalendarz, automatyczne odpowiedzi	Kiedy jesteś w podróży, z kim się spotykasz.
Regularne publikacje w mediach społecznościowych	Gdzie bywasz, z kim, jak wygląda twój dom, jakie masz zwyczaje.
Zdjęcia dzieci w mundurkach szkolnych, z treningów	Gdzie i kiedy można je znaleźć.

Żaden z tych elementów osobno nie stanowi zagrożenia. Problem pojawia się wtedy, gdy kilka z nich jest jednocześnie łatwo dostępnych dla osób spoza kręgu, który powinien je znać.



Rys. 23. Jak drobne, jawne informacje składają się w obraz dnia · przykłady z tabeli w podrozdziale 10.1

10.2. Ograniczanie publicznego ujawniania informacji

Harmonogramy i stałe godziny. Kalendarz współdzielony z osobami spoza najbliższego zespołu powinien pokazywać tylko „zajęty". Asystenci i sekretariaty powinni mieć jasną zasadę, że nie podają szczegółów harmonogramu osobom dzwoniącym z zewnątrz („pani dyrektor jest dziś nieobecna" zamiast „pani dyrektor jest dziś w Rzeszowie na spotkaniu z X").

Miejsca i trasy. Nie musisz codziennie zmieniać trasy do pracy, ale nie ma powodu, żeby była ona publicznie dostępna. Publikuj zdjęcia z miejsc po wyjściu z nich, nie w trakcie, i bez oznaczania lokalizacji.

Podróże. Szczegóły podróży znają tylko osoby, które ich potrzebują (rozdział 5.5). Po powrocie możesz opowiedzieć, gdzie byłeś. W trakcie wyjazdu lepiej się z tym wstrzymać. Opóźnienie nie zwalnia jednak z oceny, co z wyjazdu nadal wymaga ochrony.

Współpracownicy. Strony internetowe firm często zawierają pełne listy pracowników z rolami i zdjęciami. To ułatwia kontakt klientom, ale też dobór celów do socjotechniki. Organizacja powinna świadomie zdecydować, które role muszą być publiczne, a które nie. Sam pracownik nie powinien publikować składu zespołu, zdjęć z wnętrza biura ani informacji o tym, kto odpowiada za jakie systemy.

Rodzina. Zdjęcia dzieci, ich imiona, szkoła, zajęcia dodatkowe, miejsce wakacji to informacje, które w niepowołanych rękach mogą posłużyć do nacisku. Nie oznacza to, że trzeba zniknąć z sieci. Wystarczy profil prywatny, rozsądny dobór odbiorców i unikanie zdjęć, na których widać szkołę, adres czy tablice rejestracyjne.

Miejsce zamieszkania. Adres domowy nie powinien pojawiać się w miejscach publicznych: na przywieszkach bagażowych, w podpisach mailowych, w ogłoszeniach sprzedaży. Jeśli prowadzisz jednoosobową działalność gospodarczą, sprawdź, czy w publicznym rejestrze CEIDG nie widnieje twój adres domowy jako adres wykonywania działalności, i rozważ zmianę na adres biura lub adres do doręczeń. Zdjęcia domu i ulicy publikowane w sieci pozwalają ustalić lokalizację nawet bez podania adresu.

10.3. Proporcjonalność do poziomu ryzyka

Środki ograniczające przewidywalność powinny odpowiadać rzeczywistemu ryzyku. Osoba, która nigdy nie zetknęła się z niepożądanym zainteresowaniem i nie zajmuje się sprawami wrażliwymi, nie potrzebuje tych samych nawyków co członek zarządu spółki obronnej po serii niepokojących sygnałów.

Profil	Kto	Rozsądne nawyki
Podstawowy	Większość pracowników, także w firmach z branż wrażliwych	Prywatne profile w mediach społecznościowych, publikowanie po fakcie, neutralne automatyczne odpowiedzi, brak szczegółów pracy w sieci.
Podwyższony	Kadra kierownicza, osoby z dostępem do informacji o obiektach, transportach, projektach obronnych; dziennikarze śledczy; osoby publiczne	Jak wyżej, plus: brak nazwisk na miejscach parkingowych, ograniczony dostęp do kalendarza, rotacja kilku miejsc spotkań, plan podróży znany zaufanej osobie, przegląd śladu cyfrowego co kwartał.
Wysoki	Osoby, wobec których odnotowano sygnały niepożądanego zainteresowania; osoby wskazane przez dział bezpieczeństwa	Jak wyżej, plus: indywidualny plan ustalony z działem bezpieczeństwa lub profesjonalną ochroną, zmienność godzin i tras w uzasadnionym zakresie, procedury dla rodziny, konsultacja ze służbami.

10.4. Dlaczego nie warto popadać w nadmierną podejrzliwość ani ciągle zmieniać tras

W poradnikach bezpieczeństwa często pojawia się zalecenie, żeby stale zmieniać trasy i godziny. Dla większości ludzi jest to rada nietrafiona z kilku powodów.

Ciągłe zmiany są męczące i trudno je utrzymać dłużej niż kilka tygodni. Potem człowiek wraca do starych nawyków, często z poczuciem, że „i tak się nie da".

Nietypowe trasy bywają mniej bezpieczne niż zwykłe: przebiegają przez nieznane okolice, słabiej oświetlone ulice, miejsca, w których trudniej o pomoc.

Widoczne zmiany przyciągają uwagę. Osoba, która codziennie robi coś inaczej, jest dla otoczenia bardziej interesująca niż osoba, która po prostu żyje.

Ciągła czujność obciąża psychicznie ciebie i rodzinę, a zmęczenie obniża jakość decyzji w sytuacji, gdy pojawi się rzeczywisty sygnał.

Zamiast ciągłych zmian lepiej sprawdza się zasada niewielkiej zmienności i dyskrecji: kilka sprawdzonych tras i lokali używanych zamiennie, brak publicznych informacji o tym, który z nich wybierzesz dziś, oraz gotowość do bardziej zdecydowanych zmian, jeśli pojawią się konkretne sygnały.

10.5. Rodzina i bliscy

Bliscy nie muszą znać szczegółów twojej pracy, a w wielu przypadkach nie powinni. Warto jednak ustalić z nimi kilka prostych zasad.

- Nie podajemy osobom dzwoniącym lub piszącym z zewnątrz informacji o tym, gdzie jesteś, kiedy wracasz i czym się zajmujesz, nawet jeśli przedstawiają się jako współpracownicy. Odpowiedź „przekażę, żeby oddzwonił" wystarcza.
- Jeśli ktoś obcy wypytuje o ciebie sąsiadów, dzieci w szkole, nauczycieli lub opiekunów, chcesz o tym wiedzieć. Uprzedź szkołę, że nikt poza wskazanymi osobami nie odbiera dzieci i nie otrzymuje informacji o nich.
- Umówcie się na sygnał w rozmowie telefonicznej oznaczający „nie mogę mówić swobodnie" lub „potrzebuję pomocy".
- Wszyscy dorośli domownicy znają numer 112 i numer zaufanej osoby z twojej pracy.

Osobny temat to młodzież. Według ICCT i GLOBSEC co siódmy z udokumentowanych sprawców w Europie miał poniżej 22 lat, a najmłodszy 16. Werbunek odbywa się w serwisach i komunikatorach popularnych wśród młodych, czasem w formie gry lub wyzwania. Porozmawiaj z nastolatkami w rodzinie o tym, że oferty zapłaty za zdjęcie dworca, przejazd trasą, naklejenie plakatów czy dostarczenie paczki mogą być początkiem werbunku, że udział w takich zadaniach może być przestępstwem także wtedy, gdy wykonawca nie wie, dla kogo pracuje, i że w razie kontaktu najważniejsze jest powiedzenie o tym dorosłemu i zgłoszenie sprawy, a nie ukrywanie jej ze wstydu.

10.6. Kwartalny przegląd własnego śladu

Raz na kwartał poświęć pół godziny na sprawdzenie, co o tobie widać z zewnątrz:

1. Wyszukaj swoje imię i nazwisko w wyszukiwarce, także w połączeniu z nazwą firmy i miastem.
2. Sprawdź ustawienia prywatności w mediach społecznościowych i listę osób, które widzą twoje publikacje.
3. Przejrzyj zdjęcia, na których jesteś oznaczony, i usuń oznaczenia, które ujawniają za dużo.
4. Sprawdź uprawnienia aplikacji do lokalizacji, mikrofonu i kontaktów.
5. Przejrzyj aktywne sesje i urządzenia w najważniejszych kontach.
6. Sprawdź, czy twój adres e-mail nie pojawił się w znanych wyciekach danych (np. w serwisach informujących o wyciekach), i zmień hasła tam, gdzie to potrzebne.
7. Zastanów się, czy w ostatnich miesiącach nie zmieniło się coś w twojej pracy, co wymaga podniesienia profilu ostrożności.

Taki przegląd jest szybki, a jego efekt kumuluje się w czasie. Po kilku kwartałach twój publiczny obraz zawiera to, co chcesz pokazać, a nie przypadkowy zbiór informacji z ostatnich lat.

11.

Postępowanie w sytuacjach kryzysowych

W sytuacji kryzysowej kolejność priorytetów jest zawsze ta sama: życie i zdrowie, oddalenie się od zagrożenia, wezwanie pomocy, unikanie konfrontacji, a dopiero potem informacje i mienie. Ten rozdział zawiera krótkie procedury dla najczęstszych sytuacji. Są celowo proste, bo w stresie pamięta się tylko proste rzeczy.

11.1. Zestawienie sytuacji i pierwszych działań

Sytuacja	Pierwsze działanie	Drugie działanie	Trzecie działanie
Bezpośrednie zagrożenie fizyczne	Oddal się w stronę ludzi i wyjścia	112 z bezpiecznego miejsca	Zaufana osoba, notatka
Agresywne zachowanie rozmówcy lub osoby obok	Zwiększ dystans, mów spokojnie	Obsługa lub ochrona lokalu	Wyjście, w razie potrzeby 112
Utrata telefonu lub laptopa	Zdalna blokada urządzenia	Dział IT, zastrzeżenie SIM	Zmiana haseł, policja (rozdział 8.9)
Utrata dokumentów	Zgłoszenie utraty dowodu, zastrzeżenie PESEL	Bank, jeśli zginęły karty	Dział bezpieczeństwa, jeśli zginęły dokumenty firmowe
Podejrzenie ujawnienia informacji poufnych	Przerwanie dalszego ujawniania	Dział bezpieczeństwa, inspektor ochrony danych	Notatka z faktami
Utrata kontaktu z osobą towarzyszącą	Telefon, oczekiwanie w umówionym miejscu	Obsługa miejsca, organizator	Zaufana osoba, policja
Pożar, alarm, panika w lokalu	Polecenia personelu, najbliższe wyjście	Oddalenie się od budynku	112, jeśli nikt nie zadzwonił
Podejrzany przedmiot	Nie dotykaj, poinformuj obsługę	Oddal się	112

11.2. Jak wezwać pomoc

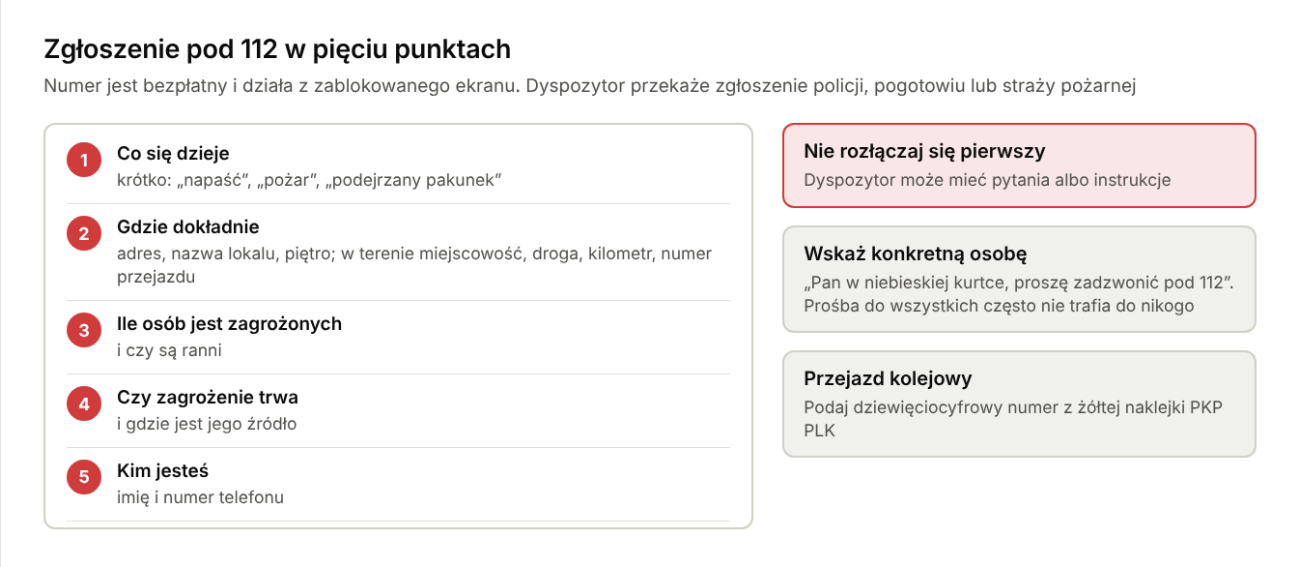
Numer alarmowy 112 jest bezpłatny, działa także bez środków na koncie, a połączenie można wykonać z zablokowanego ekranu telefonu. Dyspozytor przekaże zgłoszenie policji, pogotowiu lub straży pożarnej.

Co powiedzieć:

1. Co się dzieje (krótko: „napaść", „pożar", „mężczyzna z nożem", „podejrzany pakunek").
2. Gdzie dokładnie (adres, nazwa lokalu, piętro, charakterystyczne punkty; w terenie: najbliższa miejscowość, droga, kilometr, numer przejazdu kolejowego).
3. Ile osób jest zagrożonych i czy są ranni.
4. Czy zagrożenie trwa i gdzie jest jego źródło.
5. Twoje imię i numer telefonu.

Nie rozłączaj się pierwszy. Dyspozytor może mieć dodatkowe pytania lub instrukcje.

Jeśli wzywasz pomocy, a wokół są ludzie, zwracaj się do konkretnej osoby: „Pan w niebieskiej kurtce, proszę zadzwonić pod 112". Prośba skierowana do wszystkich często nie trafia do nikogo, bo każdy zakłada, że zadzwoni ktoś inny.



Rys. 24. Pięć informacji dla dyspozytora numeru 112

11.3. Bezpośrednie zagrożenie fizyczne

Napaść, rabunek, groźba z użyciem przedmiotu niebezpiecznego.

- Jeśli napastnik żąda rzeczy (telefon, portfel, torba), oddaj je. Dokumenty i dane da się zabezpieczyć zdalnie (rozdział 8.9). Ciebie nie da się odtworzyć.
- Oddal się w stronę ludzi, światła, czynnych lokali. Głośne wołanie o pomoc zwraca uwagę i często zniechęca napastnika.
- Nie ścigaj sprawcy.
- Z bezpiecznego miejsca dzwoń pod 112.
- Zapamiętaj możliwie dużo szczegółów (wygląd, kierunek ucieczki, pojazd) i zapisz je po odzyskaniu spokoju.

Kodeks karny pozwala na obronę konieczną przed bezpośrednim, bezprawnym zamachem (art. 25 k.k.). W praktyce bezpieczeństwa osobistego obrona fizyczna jest ostatecznością, gdy nie ma możliwości ucieczki, a życie lub zdrowie jest bezpośrednio zagrożone. ABW w swoich zaleceniach dotyczących zagrożeń terrorystycznych ujmuje to tak samo: najpierw ewakuacja, potem ukrycie, potem alarm, a obrona dostępnymi środkami dopiero w ostateczności.

11.4. Agresywne zachowanie

Agresja słowna lub zachowanie zapowiadające przemoc (w lokalu, na ulicy, w trakcie spotkania).

- Zwiększ dystans. Wstań, cofnij się, postaw między sobą a tą osobą stół lub krzesło, nie wykonując gwałtownych ruchów.
- Mów spokojnie, cicho, krótkimi zdaniami. Nie odpowiadaj na obelgi i prowokacje.
- Nie dotykaj tej osoby, nie wskazuj jej palcem, nie stój naprzeciw na wyciągnięcie ręki.
- Nie odwracaj się plecami w momencie największego napięcia. Odejdź, gdy sytuacja na chwilę się uspokoi.
- Daj sygnał obsłudze lub ochronie lokalu.
- Jeśli agresja przechodzi w groźby lub przemoc, wyjdź i dzwoń pod 112.

11.5. Utrata dokumentów

Dowód osobisty i paszport. Zgłoś utratę dowodu osobistego w dowolnym urzędzie gminy lub przez serwis mObywatel, a paszportu w urzędzie wojewódzkim lub placówce konsularnej za granicą. Zgłoszenie utraty dowodu osobistego powoduje, że dokument zostaje unieważniony. Unieważnienie dowodu osobistego z powodu utraty powoduje także zastrzeżenie numeru PESEL z urzędu. Sprawdź jego status w aplikacji mObywatel i w razie potrzeby zastrzeż go samodzielnie w mObywatelu lub w urzędzie gminy.

Karty płatnicze. Zastrzeż je natychmiast przez aplikację banku lub infolinię.

Dokumenty służbowe. Poinformuj dział bezpieczeństwa niezwłocznie, nawet jeśli uważasz, że dokumenty nie zawierały niczego istotnego. Ocena skutków należy do organizacji. Utrata dokumentów zawierających informacje niejawne wymaga natychmiastowego zawiadomienia pełnomocnika ds. ochrony informacji niejawnych zgodnie z procedurą obowiązującą w twojej jednostce.

Identyfikator służbowy i karta dostępu. Zgłoś utratę, żeby karta została zablokowana. Identyfikator z nazwą firmy, twoim zdjęciem i stanowiskiem to dla osoby z zewnątrz cenny przedmiot.

11.6. Podejrzenie ujawnienia informacji poufnych

Przykłady: zostawiłeś dokumenty w lokalu i wróciłeś po nie po godzinie, wysłałeś wiadomość do niewłaściwej osoby, ktoś sfotografował ekran, rozmowę o szczegółach transportu słyszała osoba obok, która zachowywała się nietypowo.

1. Przerwij dalsze ujawnianie: zabierz dokumenty, zamknij laptop, zakończ rozmowę, poproś adresata pomyłkowej wiadomości o jej usunięcie.
2. Poinformuj dział bezpieczeństwa i przełożonego. Nie ukrywaj zdarzenia ze wstydu: szybka informacja pozwala ograniczyć skutki, a ukrywanie zwykle je pogłębia.
3. Jeśli ujawnione mogły zostać dane osobowe, niezwłocznie poinformuj inspektora ochrony danych. Administrator ocenia naruszenie i zgłasza je Prezesowi Urzędu Ochrony Danych Osobowych bez zbędnej zwłoki, w miarę możliwości nie później niż w ciągu 72 godzin od jego stwierdzenia, chyba że jest mało prawdopodobne, by skutkowało ono ryzykiem naruszenia praw lub wolności osób fizycznych (art. 33 RODO). Ty zgłaszasz zdarzenie wewnątrz organizacji niezwłocznie, nie czekając na upływ tego terminu.
4. Sporządź notatkę: co, kiedy, gdzie, kto mógł mieć dostęp, jakie działania już podjąłeś.
5. Przy informacjach niejawnych postępuj wyłącznie według procedury pełnomocnika ochrony.

6. Jeśli okoliczności wskazują, że ujawnienie nie było przypadkowe (ktoś celowo przysłuchiwał się, fotografował, wypytywał), organizacja powinna rozważyć zgłoszenie do ABW.



Rys. 25. Sześć kroków po podejrzeniu ujawnienia informacji · na podstawie podrozdziału 11.6

11.7. Utrata kontaktu z osobą towarzyszącą

Przed każdym wyjściem w grupie, zwłaszcza w nieznane miejsce, ustalcie punkt spotkania na wypadek rozdzielenia się (wejście do hotelu, recepcja, konkretny sklep) i godzinę, po której zaczynacie szukać pomocy.

Gdy tracisz kontakt:

1. Zadzwoń i napisz. Brak odpowiedzi w pierwszych minutach jest zwykle wynikiem rozładowanego telefonu, hałasu lub braku zasięgu.
2. Udaj się do umówionego punktu i czekaj tam przez ustalony czas.
3. Zapytaj obsługę miejsca, w którym ostatnio byliście, czy ktoś nie widział tej osoby.
4. Po upływie ustalonego czasu poinformuj zaufaną osobę lub dział bezpieczeństwa organizacji.
5. Jeśli masz obawy o bezpieczeństwo tej osoby, zgłoś sprawę na policję. Nie ma zasady, że zaginięcie osoby dorosłej można zgłosić dopiero po 24 godzinach.

11.8. Nagła zmiana sytuacji w lokalu

Pożar, alarm, zadymienie. Wykonuj polecenia personelu. Kieruj się do najbliższego wyjścia, niekoniecznie tego, którym wszedłeś. Nie korzystaj z windy. W zadymieniu poruszaj się nisko, przy ścianie. Po wyjściu oddal się od budynku i nie wracaj po rzeczy.

Panika i tłok. W tłumie trzymaj ręce przed klatką piersiową, żeby mieć miejsce do oddychania, i staraj się przemieszczać ukośnie do kierunku ruchu tłumu, w stronę jego krawędzi. Nie zatrzymuj się, żeby podnieść rzeczy.

Podejrzany przedmiot lub pakunek. Nie dotykaj go, nie przesuwaj, nie zaglądaj do środka. Poinformuj obsługę. Oddal się. Nie używaj telefonu w bezpośrednim sąsiedztwie przedmiotu. Dzwoń pod 112 z bezpiecznej odległości, jeśli obsługa tego nie zrobiła.

Zasłabnięcie lub uraz u kogoś obok. Wezwij pomoc (112), udziel pierwszej pomocy w zakresie, jaki potrafisz, poproś personel o apteczkę i informację, czy w lokalu jest defibrylator AED.

11.9. Konieczność szybkiego opuszczenia miejsca

- Zabierz to, co masz przy sobie lub w zasięgu ręki: telefon, dokument, portfel. Laptop i teczkę tylko wtedy, gdy nie wymaga to zwłoki.
- Idź do wyjścia, które znasz (rozdział 1.2), spokojnym, ale zdecydowanym krokiem.
- Po wyjściu oddal się od wejścia. Gromadzenie się tuż przed budynkiem utrudnia pracę służb i w niektórych sytuacjach może być niebezpieczne.
- Udaj się do bezpiecznego miejsca publicznego i stamtąd poinformuj zaufaną osobę.
- Jeśli wyszedłeś w trakcie spotkania bez wyjaśnień, wyślij rozmówcy później krótką wiadomość. Nie musisz podawać powodu.

11.10. Po zdarzeniu

Sytuacja kryzysowa nie kończy się w momencie, gdy jesteś bezpieczny.

- Sporządź notatkę według wzoru z aneksu C, możliwie szybko.
- Poinformuj pracodawcę, jeśli zdarzenie miało związek z pracą lub mogło dotyczyć informacji służbowych.
- Zachowaj dowody: zrzuty ekranu, zdjęcia uszkodzeń, potwierdzenia zgłoszeń, numery spraw nadane przez policję.
- Zadbaj o siebie. Reakcje stresowe po trudnym zdarzeniu (problemy ze snem, rozdrażnienie, natrętne wspomnienia) są normalne i zwykle mijają w ciągu kilku tygodni. Jeśli nie mijają, skorzystaj z pomocy psychologicznej, w tym z programów oferowanych przez pracodawcę.
- Wróć do kroku 7 procedury z rozdziału 6: co można zmienić, żeby podobna sytuacja była mniej prawdopodobna.

12.

Przykłady i scenariusze praktyczne

Osiem poniższych scenariuszy służy do omawiania na szkoleniach i do samodzielnej analizy. Są fikcyjne, ale zbudowane z elementów, które występują w rzeczywistych zdarzeniach opisanych w rozdziale o kontekście i w materiałach ABW. Każdy ma tę samą strukturę: sytuacja, sygnały ostrzegawcze, możliwe wyjaśnienia, zalecane działania, błędy do uniknięcia i wnioski. Prowadzący szkolenie może przeczytać uczestnikom samą sytuację i poprosić o samodzielne przejście przez schemat z rozdziału 6, zanim omówi resztę.

12.1. Scenariusz 1: spotkanie biznesowe w zatłoczonej restauracji

Sytuacja. Anna jest dyrektorką zakupów w firmie dystrybuującej paliwa. Umówiła się na lunch z przedstawicielem nowego dostawcy w popularnej restauracji w centrum miasta. Lokal jest pełny, stoliki stoją gęsto. Przedstawiciel dostawcy mówi głośno i chętnie: opowiada o wolumenach, które jego firma dostarcza do „waszego terminalu pod miastem", i pyta, jak często są tam dostawy. W pewnym momencie prosi Annę, żeby pokazała mu na laptopie projekt umowy, „bo chce sprawdzić jedną liczbę". Przy sąsiednim stoliku od początku spotkania siedzi sam mężczyzna z zamkniętym laptopem. Nie je, telefon trzyma pionowo na stoliku, aparatem w stronę Anny.

Sygnały ostrzegawcze:

- rozmowa schodzi na lokalizację terminalu i częstotliwość dostaw, czyli informacje operacyjne,
- prośba o otwarcie dokumentu w miejscu publicznym,
- osoba przy sąsiednim stoliku zachowuje się niezgodnie z normą miejsca (nie je, nie pracuje, telefon ustawiony w stronę rozmówców).

Możliwe wyjaśnienia:

- przedstawiciel dostawcy jest po prostu niedoświadczony i nie zdaje sobie sprawy, że w lokalu nie omawia się takich szczegółów,
- mężczyzna czeka na kogoś, oparł telefon o szklankę, żeby oglądać wiadomości,
- telefon może nagrywać albo nie, z tej odległości nie da się tego ustalić.

Zalecane działania:

- przenieść rozmowę na poziom ogólny: „Szczegóły logistyczne omówimy w biurze, przygotuję zestawienie",
- odmówić otwarcia umowy: „Wyślę panu fragment mailem po spotkaniu",
- jeśli w lokalu jest wolny stolik w lepszym miejscu, zaproponować przesiadkę bez wyjaśniania powodu,

- po spotkaniu ocenić sygnał: pojedyncza obserwacja mężczyzny przy stoliku to sygnał słaby, wystarczy zapamiętać,
- przy kolejnym spotkaniu z tym dostawcą wybrać salę w biurze.

Błędy do uniknięcia:

- pokazanie umowy na ekranie „na chwilę",
- głośne zwrócenie uwagi mężczyźnie lub fotografowanie go,
- kontynuowanie rozmowy o terminalu, bo „przecież to nasz przyszły partner".

Wnioski. Większe ryzyko niż nieznajomy przy sąsiednim stoliku stanowił w tej sytuacji sposób prowadzenia rozmowy. Wybór lokalu z gęstymi stolikami i dopuszczenie do rozmowy o szczegółach operacyjnych sprawiły, że informacje były dostępne dla każdego w promieniu kilku metrów. Rozwiązaniem jest dyscyplina tematu, a nie podejrzliwość wobec otoczenia.

12.2. Scenariusz 2: rozmowa o poufnym projekcie w kawiarni

Sytuacja. Dwaj inżynierowie z firmy telekomunikacyjnej, Piotr i Tomasz, pracują nad ofertą w przetargu na zabezpieczenie stacji bazowych. Po spotkaniu u klienta idą do kawiarni obok biura i omawiają, które lokalizacje mają najsłabsze ogrodzenia i gdzie nie działa monitoring. Kobieta przy stoliku obok prosi ich, żeby popilnowali jej laptopa, gdy pójdzie do toalety. Po powrocie dziękuje, zagaja rozmowę, pyta, gdzie pracują, i mówi: „Słyszałam, że te stacje w ogóle nie są chronione, ktoś może tam wejść, kiedy chce, prawda?".

Sygnały ostrzegawcze:

- inżynierowie sami ujawnili informacje o słabych punktach zabezpieczeń w miejscu publicznym,
- nieznajoma nawiązuje kontakt przez drobną przysługę, a potem przechodzi do pytań o pracę,
- pytanie ma formę fałszywego stwierdzenia, które zachęca do korekty i podania szczegółów.

Możliwe wyjaśnienia:

- kobieta usłyszała fragment rozmowy i jest po prostu ciekawa,
- jest dziennikarką lub pracuje dla konkurencji,
- jej zainteresowanie ma inne źródło, którego nie da się ustalić.

Zalecane działania:

- nie potwierdzać i nie korygować: „Nie wiem, nie zajmujemy się tym, pracujemy w sprzedaży",
- uprzejmie zakończyć rozmowę i wyjść,
- po powrocie do biura poinformować dział bezpieczeństwa o zdarzeniu, łącznie z tym, co sami powiedzieli przy stoliku,
- sporządzić krótką notatkę z opisem kobiety, godziną i treścią pytań,
- organizacja oceni, czy informacja o słabych punktach mogła wyciec, i czy zdarzenie zgłosić dalej; przy obiektach infrastruktury krytycznej rozważy zgłoszenie do ABW.

Błędy do uniknięcia:

- prostowanie fałszywego stwierdzenia („Nie no, część jest chroniona, tylko te pod..."),
- ukrywanie przed działem bezpieczeństwa tego, o czym rozmawiali, ze strachu przed konsekwencjami,

- wypytywanie kobiety, dla kogo pracuje, albo robienie jej zdjęć.

Wnioski. Najpoważniejszy błąd popełniono, zanim pojawiła się nieznajoma: rozmowa o słabych punktach zabezpieczeń nie powinna była się odbyć w kawiarni. Nieznajoma mogła być zupełnie niewinna, ale informacja, którą usłyszała, i tak wyszła poza organizację. Zgłoszenie własnego błędu jest w takiej sytuacji najcenniejszym działaniem, bo pozwala organizacji zareagować.

12.3. Scenariusz 3: powtarzające się spotkania z tą samą osobą

Sytuacja. Marek jest kierownikiem magazynu, z którego wysyłana jest pomoc humanitarna do Ukrainy. W poniedziałek rano, tankując na stacji obok magazynu, zauważa mężczyznę w charakterystycznej czerwonej kurtce, który stoi przy dystrybutorze bez samochodu i patrzy na bramę magazynu. W środę wieczorem widzi tego samego mężczyznę w kawiarni na swoim osiedlu, dwadzieścia kilometrów od magazynu. W piątek, w innym mieście, na dworcu, gdzie Marek przyjechał na spotkanie z przewoźnikiem, mężczyzna stoi kilka metrów od niego przy kasach.

Sygnały ostrzegawcze:

- trzy obserwacje w trzech niezwiązanych miejscach w ciągu tygodnia, w tym w pobliżu domu i na wyjeździe służbowym,
- pierwsza obserwacja dotyczy zachowania wobec obiektu (obserwowanie bramy bez widocznego celu),
- miejsca łączy tylko osoba Marka i jego praca.

Możliwe wyjaśnienia:

- mężczyzna mieszka na tym samym osiedlu i pracuje w okolicy magazynu, a w piątek przypadkiem podróżował,
- Marek pomylił osoby: czerwona kurtka to cecha łatwo zmienna i powszechna,
- mężczyzna rzeczywiście interesuje się magazynem lub Markiem.

Zalecane działania:

- nie dawać znać, że coś zauważył, nie podchodzić, nie pytać,
- sporządzić notatkę z każdą obserwacją, z naciskiem na cechy trwałe (wzrost, budowa, twarz, sposób poruszania się), a nie na kurtkę,
- na dworcu przejść w miejsce z ludźmi i ochroną, poinformować zaufaną osobę, gdzie jest,
- po powrocie omówić sytuację z działem bezpieczeństwa firmy; to sygnał silny, więc dział rozważy zgłoszenie na policję lub do ABW,
- przez kolejne dni zachować większą uważność, ustalić z rodziną zasady (rozdział 10.5), nie zmieniać gwałtownie całego trybu życia bez konsultacji,
- poprosić ochronę magazynu o zwrócenie uwagi na osoby obserwujące bramę.

Błędy do uniknięcia:

- opublikowanie zdjęcia mężczyzny w mediach społecznościowych z pytaniem „kto to jest?", co narusza jego prawa i może ostrzec sprawcę, jeśli rzeczywiście nim jest,
- chodzenie za mężczyzną, żeby sprawdzić, dokąd idzie,
- konfrontacja w kawiarni na osiedlu,
- zbagatelizowanie sprawy, bo „to pewnie przypadek", bez żadnej notatki.

Wnioski. Pojedyncze spotkanie zwykle nie pozwala ustalić intencji, ale trzy w niezwiązanych miejscach, w tym jedno przy obiekcie, to wzór, który warto przekazać profesjonalistom. Notatki prowadzone na bieżąco, z cechami trudnymi do zmiany, są dla służb znacznie cenniejsze niż ogólne wrażenie. Marek nie musi rozstrzygać, czy jest obserwowany. Ma przekazać fakty tym, którzy potrafią to ocenić.

12.4. Scenariusz 4: utrata telefonu podczas podróży służbowej

Sytuacja. Katarzyna jest konsultantką prowadzącą audyt w spółce energetycznej. Wraca pociągiem z kilkudniowego wyjazdu. Po wyjściu z dworca orientuje się, że telefon został w przedziale. Na telefonie jest poczta służbowa, komunikator z kanałami projektowymi i kilkanaście zdjęć dokumentów audytowych, które zrobiła „na szybko" w trakcie wyjazdu. Telefon jest zablokowany sześciocyfrowym kodem, ale powiadomienia wyświetlają treść na ekranie blokady.

Sygnały ostrzegawcze:

- na urządzeniu znajdują się informacje klienta, w tym zdjęcia dokumentów,
- podgląd powiadomień pozwala odczytać fragmenty wiadomości bez odblokowania telefonu,
- czas działa na niekorzyść.

Możliwe wyjaśnienia:

- telefon zostanie znaleziony przez obsługę pociągu i oddany do biura rzeczy znalezionych,
- telefon zabrał inny pasażer w złej wierze,
- żadna z tych możliwości nie zmienia procedury.

Zalecane działania:

- z laptopa lub telefonu współpracownika zablokować urządzenie i sprawdzić jego lokalizację w usłudze producenta,
- zadzwonić do przewoźnika i biura rzeczy znalezionych na dworcu docelowym,
- powiadomić dział IT swojej firmy i zastrzec kartę SIM u operatora,
- z zaufanego urządzenia zmienić hasło do poczty i komunikatora oraz zakończyć sesje na zgubionym telefonie,
- w porozumieniu z IT podjąć decyzję o zdalnym wymazaniu danych, jeśli telefon nie zostanie odnaleziony w krótkim czasie,
- poinformować przełożonego i ocenić, czy utrata zdjęć dokumentów wymaga powiadomienia klienta zgodnie z umową o poufności, a jeśli dokumenty zawierały dane osobowe, poinformować inspektora ochrony danych (rozdział 11.6),
- zgłosić utratę na policji z numerem IMEI, jeśli telefon nie wróci.

Błędy do uniknięcia:

- odkładanie reakcji do następnego dnia „bo może się znajdzie",
- samodzielny wyjazd pod adres wskazany przez usługę lokalizacji,
- publikowanie w mediach społecznościowych prośby o zwrot telefonu z podaniem swojego numeru i nazwy firmy,
- ukrywanie przed pracodawcą i klientem, że na telefonie były zdjęcia dokumentów.

Wnioski. Utrata telefonu była przypadkiem, ale jej skutki wynikają z wcześniejszych nawyków: zdjęć dokumentów robionych telefonem prywatnym lub służbowym bez szyfrowanego folderu i włączonego podglądu powiadomień. Ochronę ustawia się przed podróżą (rozdział 8), a procedura po utracie ogranicza szkody tylko wtedy, gdy jest uruchomiona natychmiast.

12.5. Scenariusz 5: podejrzenie nieuprawnionego dostępu do dokumentów

Sytuacja. Jacek, prawnik doradzający spółce z branży obronnej, przyjeżdża na dwudniowe negocjacje i nocuje w hotelu. Wieczorem po kolacji wraca do pokoju i ma wrażenie, że teczka z dokumentami leży inaczej, niż ją zostawił: klapa jest otwarta, a kartki z harmonogramem dostaw, które leżały na wierzchu, są teraz na dole. Laptop jest zamknięty, ale przy włączeniu system informuje o nieudanej próbie logowania godzinę wcześniej. Na drzwiach wisiała zawieszka „nie przeszkadzać".

Sygnały ostrzegawcze:

- zmiana ułożenia dokumentów mimo zawieszki „nie przeszkadzać",
- zapis systemowy o nieudanej próbie logowania w czasie nieobecności,
- dokumenty dotyczą harmonogramu dostaw dla branży obronnej.

Możliwe wyjaśnienia:

- obsługa hotelu weszła mimo zawieszki (np. uzupełnić minibar) i przesunęła rzeczy,
- Jacek sam przełożył dokumenty i tego nie pamięta,
- nieudane logowanie to efekt przypadkowego naciśnięcia klawiszy przy przenoszeniu laptopa przez obsługę,
- ktoś rzeczywiście próbował zapoznać się z dokumentami lub danymi.

Zalecane działania:

- nie ruszać dalej dokumentów i laptopa poza tym, co konieczne, żeby niczego nie zatrzeć,
- zrobić zdjęcia ułożenia rzeczy i zrzut ekranu komunikatu o próbie logowania,
- zapytać recepcję, czy ktoś z obsługi wchodził do pokoju i w jakim celu, bez oskarżeń,
- niezwłocznie poinformować dział bezpieczeństwa klienta i swojej kancelarii, a przy informacjach niejawnych pełnomocnika ochrony,
- traktować dokumenty jako potencjalnie ujawnione: organizacja oceni skutki i ewentualnie zmieni harmonogram,
- do czasu sprawdzenia przez dział IT nie używać laptopa do pracy na danych wrażliwych,
- w przyszłości nie zostawiać dokumentów wrażliwych w pokoju hotelowym; jeśli to konieczne, używać zamykanej walizki i nie pozostawiać laptopa włączonego ani w trybie uśpienia.

Błędy do uniknięcia:

- oskarżanie pracownika obsługi przed ustaleniem faktów,
- przemilczenie sprawy, bo „pewnie mi się wydawało",
- dalsza praca na laptopie, jakby nic się nie stało,
- samodzielne „śledztwo" w hotelu, przeglądanie nagrań, wypytywanie gości.

Wnioski. Nie wszystkie wątpliwości da się rozstrzygnąć, ale skutki da się ograniczyć. Organizacja, która wie o zdarzeniu, może zmienić harmonogram lub procedury. Organizacja, która nie wie, działa dalej na podstawie informacji, które mogły zostać ujawnione. Najskuteczniejszą ochroną było niezostawianie dokumentów w pokoju, co ABW ujmuje w zaleceniu, by być „cieniem" swojego sprzętu w podróży.

12.6. Scenariusz 6: konieczność zmiany planów z powodów bezpieczeństwa

Sytuacja. Zespół czterech osób z firmy logistycznej ma jechać pociągiem na całodniowe warsztaty z kontrahentem w hotelu położonym obok dużego węzła kolejowego na wschodzie kraju. Wieczorem dzień przed wyjazdem pojawiają się komunikaty o uszkodzeniu linii kolejowej w regionie i trwającej akcji służb, a rano przewoźnik informuje o odwołanych pociągach. W mediach społecznościowych krążą sprzeczne informacje, w tym o „kolejnych wybuchach" i „ewakuacji miasta". Kontrahent proponuje, żeby zespół dojechał samochodami i spotkał się „gdzieś na parkingu przy obwodnicy, bo w hotelu będzie zamieszanie".

Sygnały ostrzegawcze:

- trwający incydent w pobliżu miejsca spotkania,
- informacje z niezweryfikowanych źródeł, które mogą być dezinformacją,
- propozycja zmiany miejsca na mniej publiczne, w ostatniej chwili.

Możliwe wyjaśnienia:

- incydent może być awarią techniczną, a nie sabotażem,
- kontrahent chce po prostu pomóc i nie przemyślał propozycji,
- doniesienia o „kolejnych wybuchach" są plotką lub celową dezinformacją.

Zalecane działania:

- sprawdzić informacje w oficjalnych źródłach (komunikaty policji, wojewody, RCB, przewoźnika), zanim podejmie się decyzję,
- nie przesyłać dalej niezweryfikowanych doniesień,
- przełożyć warsztaty albo przenieść je do formy zdalnej, zamiast improwizować spotkanie na parkingu,
- przekazać kontrahentowi decyzję krótko i neutralnie: „Ze względu na sytuację przekładamy, zaproponujemy nowy termin",
- poinformować dział bezpieczeństwa o zmianie planów i o propozycji spotkania na parkingu, jeśli wydała się nietypowa,
- przy nowym terminie ponownie ocenić ryzyko (rozdział 1.3) i rozważyć inne miejsce.

Błędy do uniknięcia:

- jazda „na wszelki wypadek" w rejon trwającej akcji służb,
- spotkanie w przypadkowym, odludnym miejscu tylko dlatego, że plan się posypał,
- publikowanie w mediach społecznościowych relacji z drogi i zdjęć utrudnień,
- podejmowanie decyzji na podstawie jednej wiadomości z komunikatora.

Wnioski. Zmianę planów z powodów bezpieczeństwa warto traktować jak każdą inną decyzję organizacyjną i podejmować ją bez wahania oraz bez szczegółowych tłumaczeń. W sytuacji incydentu największym ryzykiem bywa improwizacja: nowe, nieznane miejsce, pośpiech i informacje z niesprawdzonych źródeł.

12.7. Scenariusz 7: oferta „łatwego zarobku” przez komunikator

Sytuacja. Oskar ma 19 lat, studiuje i dorabia jako kurier rowerowy. Na Telegramie dostaje wiadomość od nieznanego konta: „Szukamy ludzi do prostych zadań fotograficznych dla firmy badającej ruch w mieście. 200 zł za zlecenie, płatność od razu w kryptowalucie”. Pierwsze zadanie polega na zrobieniu kilku zdjęć dworca autobusowego i wysłaniu ich z lokalizacją. Oskar je wykonuje i dostaje przelew. Tydzień później przychodzi kolejne: sfotografować z bliska bramę i kamery na terenie bocznicy kolejowej, a wieczorem nagrać przejazd pociągów towarowych i podać godzinę. Stawka rośnie do 500 zł. Na pytanie, jaka to firma, Oskar dostaje odpowiedź: „Klient jest zagraniczny, nie możemy podać nazwy. Nie mów nikomu, to konkurencyjny rynek”.

Sygnały ostrzegawcze:

- nieznany zleceniodawca w komunikatorze, bez nazwy firmy i umowy,
- płatność w kryptowalucie, szybka i bez dokumentów,
- zadania dotyczące fotografowania infrastruktury kolejowej i jej zabezpieczeń oraz rejestrowania ruchu,
- prośba o lokalizację i godziny,
- eskalacja zadań i stawek,
- wymóg zachowania tajemnicy.

Możliwe wyjaśnienia:

- istnieją legalne serwisy zleceń fotograficznych (np. audyty witryn sklepów), ale działają jako firmy z regulaminem, umową i rozliczeniem podatkowym, a ich zadania nie dotyczą zabezpieczeń infrastruktury,
- w opisanej konfiguracji żadne niewinne wyjaśnienie nie pasuje do wszystkich sygnałów.

Zalecane działania:

- natychmiast przerwać współpracę i nie wykonywać żadnego kolejnego zadania,
- nie kasować korespondencji: zrobić zrzuty ekranu z nazwą konta, datami, treścią zleceń i potwierdzeniami płatności,
- porozmawiać z zaufaną osobą dorosłą (rodzic, wykładowca, starszy znajomy),
- zgłosić sprawę do ABW przez chatbot @ABW_STOPdywersji_bot lub dyżurnego (22 585 82 21) albo na policji,
- skonsultować się z adwokatem lub radcą prawnym, bo wykonanie pierwszego zadania może mieć znaczenie prawne; art. 131 Kodeksu karnego przewiduje niepodleganie karze tylko po spełnieniu wszystkich ustawowych warunków (rozdział 4.9), a samo zgłoszenie nie daje takiej gwarancji,
- nie informować zleceniodawcy o zgłoszeniu.

Błędy do uniknięcia:

- wykonanie „jeszcze jednego” zadania, żeby odebrać pieniądze, a dopiero potem zgłosić,
- usunięcie aplikacji i korespondencji ze strachu,
- grożenie zleceniodawcy policją lub próby „przejęcia” rozmowy, żeby coś o nim ustalić,
- przekonanie, że skoro nie wiedział, dla kogo pracuje, to nic mu nie grozi; za fotografowanie obiektów na zlecenie obcego wywiadu i zgłoszenie gotowości do współpracy grozi odpowiedzialność karna, a o tym, czy niewiedza ją wyłącza, rozstrzyga sąd na podstawie wszystkich okoliczności.

Wnioski. Ten scenariusz odpowiada mechanizmowi opisanemu przez ABW, ICCT i GLOBSEC oraz duńską PET: proste zadanie, szybka zapłata, stopniowa eskalacja. Ofiara takiego werbunku nie musi być naiwna, wystarczy, że potrzebuje pieniędzy i nie zna kontekstu. Dlatego rozmowa o takich ofertach z młodymi ludźmi w rodzinie i w zespole jest jednym z najskuteczniejszych działań profilaktycznych, a szybkie zgłoszenie jest najlepszym wyjściem także dla osoby, która już dała się wciągnąć.

12.8. Scenariusz 8: przemieszczanie się w pobliżu infrastruktury logistycznej i obiektów wsparcia Ukrainy

Sytuacja. Ewa koordynuje transporty pomocy dla Ukrainy. Czeka w samochodzie na parkingu przy terminalu przeładunkowym na kierowców, którzy mają odebrać ładunek. Zauważa mężczyznę, który powoli idzie wzdłuż ogrodzenia terminalu z papierową torbą w ręku, zatrzymuje się przy szafach zasilających i kamerze, robi telefonem kilka zdjęć, a gdy na końcu ogrodzenia pojawia się samochód ochrony, odchodzi w stronę pobliskiego sadu. Godzinę później w przydrożnym barze, gdzie Ewa kupuje kawę, nieznany mężczyzna, inny niż ten przy ogrodzeniu, zagaduje ją, czy „to te transporty na Ukrainę" i o której zwykle wyjeżdżają.

Sygnały ostrzegawcze:

- fotografowanie elementów technicznych i zabezpieczeń (szafy zasilające, kamera), a nie obiektu jako całości,
- oddalenie się na widok ochrony,
- spacer wzdłuż ogrodzenia bez widocznego celu, połączony z fotografowaniem zabezpieczeń, co przypomina opisane przez ABW rozpoznanie przed podpaleniem stacji Starlink we wrześniu 2026 roku,
- odrębne pytanie o godziny wyjazdów transportów od nieznanej osoby.

Możliwe wyjaśnienia:

- mężczyzna przy ogrodzeniu to pracownik firmy serwisowej, który dokumentuje usterkę, albo okoliczny mieszkaniec idący do sadu,
- osoba w barze jest po prostu ciekawa, bo widzi charakterystyczne samochody,
- obie sytuacje mogą nie mieć ze sobą żadnego związku.

Zalecane działania:

- nie podchodzić do mężczyzny przy ogrodzeniu i nie pytać, co robi,
- zapamiętać czas, miejsce, opis osoby i kierunek, w którym odszedł,
- niezwłocznie poinformować ochronę terminalu, a jeśli zachowanie przy obiekcie trwa lub wygląda na przygotowanie do działania, zadzwonić pod 112,
- w barze nie odpowiadać na pytanie o godziny: „Nie wiem, ja tylko czekam na znajomego",
- poinformować dyspozytora i dział bezpieczeństwa organizacji o obu sytuacjach, z zaznaczeniem, że nie wiadomo, czy są powiązane,
- sporządzić notatkę; dział bezpieczeństwa oceni, czy zgłosić sprawę do ABW,
- nie publikować niczego o zdarzeniu w mediach społecznościowych ani w otwartych grupach wolontariuszy.

Błędy do uniknięcia:

- konfrontacja z mężczyzną przy ogrodzeniu albo pójście za nim do sadu,

- nagrywanie go z bliska i publikowanie filmu z apelem o identyfikację,
- uznanie, że „to sprawa ochrony terminalu, nie moja", i niezgłoszenie obserwacji,
- podanie w barze godzin wyjazdu, „bo to przecież nic tajnego".

Wnioski. Rozpoznanie obiektu przed atakiem zostawia ślady, które widzą zwykli ludzie: kierowcy, okoliczni mieszkańcy, pracownicy pobliskich firm. Według ABW wzrost społecznej świadomości zagrożeń realnie ograniczył możliwości rosyjskich służb. Ewa nie musi wiedzieć, czy obserwowała rozpoznanie, czy pracownika serwisu. Jej rolą jest zauważyć, nie konfrontować się i przekazać fakty dalej, a przy tym nie ujawnić informacji, o które ktoś inny ją wypytywał.

13.

Checklisty do wykorzystania w praktyce

Poniższe listy zbierają najważniejsze działania z całego przewodnika w formie, którą można wydrukować, zapisać w telefonie lub przejść w pamięci w ciągu dwóch, trzech minut. Nie wymagają specjalistycznego wyposażenia. Punkty oznaczone w nawiasie „(H)" dotyczą aktualnego kontekstu zagrożeń hybrydowych i mają szczególne znaczenie dla osób pracujących w logistyce, energetyce, obronności, telekomunikacji lub przy wsparciu Ukrainy.

13.1. Przed wyjściem na spotkanie

- ☐ Wiem, z kim się spotykam, i sprawdziłem tożsamość nowego rozmówcy w niezależnym źródle.
- ☐ Oceniłem poziom ryzyka: niski, podwyższony czy wysoki (rozdział 1.3).
- ☐ Rozmowa pasuje do miejsca publicznego; szczegóły wrażliwe przenoszę do biura lub bezpiecznego kanału.
- ☐ Wybrałem lokal według kryteriów z rozdziału 2 i mam lokal zapasowy.
- ☐ Lokal nie sąsiaduje z obiektem, o którym będziemy rozmawiać (H).
- ☐ Zabieram tylko niezbędne dokumenty, w zamykanej teczce.
- ☐ Laptop ma filtr prywatności, aktualny system i blokadę ekranu.
- ☐ Podgląd powiadomień na ekranie blokady jest wyłączony.
- ☐ Telefon jest naładowany, mam powerbank.
- ☐ Zaufana osoba wie, gdzie i z kim jestem oraz do której godziny.
- ☐ Mamy ustaloną godzinę kontrolną i umówiony sygnał.
- ☐ Wiem, jak wrócę, i mam wariant zapasowy.
- ☐ Rezerwacja (jeśli była) jest na imię, bez nazwy firmy i celu.
- ☐ Wpis w kalendarzu ma neutralny tytuł.

13.2. Przed wejściem do lokalu

- ☐ Przyszedłem kilka minut wcześniej.
- ☐ Okolica i wejście wyglądają zwyczajnie, bez zbiegowiska, awantury, akcji służb.
- ☐ Po wejściu określiłem normę miejsca: hałas, liczba gości, obsługa, kamery.

- ☐ Znam drogę wyjścia i alternatywną, jeśli istnieje.
- ☐ Wybrałem stolik z dala od przejść, baru i kuchni, z widokiem na wejście.
- ☐ Ekran i dokumenty mogę ustawić tyłem do kamer, okien i sali.
- ☐ Rzeczy mam w zasięgu ręki.
- ☐ Jeśli miejsce jest nieodpowiednie, przechodzę do lokalu zapasowego bez tłumaczenia się.

13.3. Przed rozpoczęciem rozmowy w miejscu publicznym

- ☐ Potwierdziliśmy, że zakres rozmowy jest dopuszczony do ujawnienia w miejscu publicznym.
- ☐ Przy sąsiednich stolikach nikt nie siedzi w zasięgu normalnego głosu albo przenieśliśmy się.
- ☐ Ustaliliśmy z rozmówcą, że w lokalu mówimy ogólnie, a szczegóły omawiamy w biurze.
- ☐ Nie podajemy nazwisk, adresów, numerów, kwot, dat i tras, jeśli nie są niezbędne.
- ☐ Nie omawiamy harmonogramów transportów, lokalizacji magazynów ani zabezpieczeń obiektów (H).
- ☐ Nie przekazujemy haseł, kodów ani danych dostępowych.
- ☐ Telefony leżą ekranem w dół lub są w kieszeni; przy rozmowie wysokiego ryzyka zostały poza salą.
- ☐ Dokumenty wyjmujemy pojedynczo i chowamy po omówieniu.
- ☐ Przed odejściem od stołu wszystko wraca do teczki, a ekran jest zablokowany.

13.4. Podczas podróży

- ☐ Plan podróży zna zaufana osoba; zmiany przekazuję na bieżąco.
- ☐ Udostępnianie lokalizacji jest włączone tylko na czas podróży.
- ☐ Nie publikuję lokalizacji ani zdjęć z podróży w trakcie wyjazdu.
- ☐ Nie pracuję na dokumentach wrażliwych w pociągu, samolocie i poczekalni.
- ☐ Nie prowadzę rozmów służbowych w taksówce i transporcie publicznym.
- ☐ Laptop, telefon i dokumenty są pod moim stałym nadzorem; nie zostawiam ich w pokoju hotelowym, jeśli zawierają dane wrażliwe.
- ☐ Łączę się zgodnie z polityką organizacji (firmowy VPN lub własny hotspot, jeśli są wymagane) i nie ignoruję ostrzeżeń o certyfikatach.
- ☐ Ładuję urządzenia własną ładowarką z gniazdka.
- ☐ Nie podłączam obcych nośników i kabli.
- ☐ Sprawdzam adres strony przed otwarciem kodu QR; płacę przez oficjalne aplikacje.
- ☐ Mam kartkę z dwoma, trzema numerami telefonów i niewielką ilość gotówki oddzielnie od telefonu.
- ☐ Nie fotografuję infrastruktury kolejowej, energetycznej i obiektów wojskowych, także z okna pojazdu (H).
- ☐ Mam przy sobie dokument tożsamości na wypadek legitymowania w rejonach objętych podwyższonym stopniem alarmowym (H).
- ☐ Przy podróży zagranicznej zarejestrowałem wyjazd w systemie Odyseusz (także w aplikacji mObywatel) i sprawdziłem ostrzeżenia MSZ.

13.5. Po zauważeniu niepokojącego zdarzenia

- ☐ Najpierw sprawdzam, czy zagrożenie jest bezpośrednie: jeśli tak, od razu oddalam się w stronę ludzi i dzwonię pod 112.
- ☐ Jeśli zagrożenie nie jest bezpośrednie, zachowuję spokój i naturalne zachowanie, nie daję znać, że coś zauważyłem.
- ☐ Nazwałem obserwację opisowo, bez oceny.
- ☐ Rozważyłem zwyczajne wyjaśnienia i dobrałem proporcjonalną reakcję.
- ☐ Nie konfrontuję się, nie fotografuję ostentacyjnie, nie idę za nikim.
- ☐ Przeszedłem do bezpiecznego miejsca publicznego.
- ☐ Poinformowałem zaufaną osobę lub dział bezpieczeństwa.
- ☐ Nie wracam bezpośrednio do domu ani do miejsc wrażliwych, dopóki nie ocenię sytuacji z drugą osobą.
- ☐ Przy ofercie „łatwego zarobku" niczego nie wykonuję, nie kasuję korespondencji, robię zrzuty ekranu i zgłaszam do ABW (H).
- ☐ Przy osobie fotografującej zabezpieczenia obiektu infrastruktury informuję ochronę obiektu lub dzwonię pod 112 (H).

13.6. Po zakończeniu spotkania

- ☐ Sprawdziłem stół, krzesła i podłogę: dokumenty, notatki, nośniki, ładowarki.
- ☐ Nie wyrzuciłem żadnych notatek w lokalu.
- ☐ Dałem znać zaufanej osobie, że spotkanie się skończyło.
- ☐ Nie dałem się odprowadzić ani podwieźć, jeśli tego nie chciałem.
- ☐ Zapisałem najważniejsze ustalenia oraz sygnały, które zwróciły moją uwagę.
- ☐ Wysłałem podziękowanie bez szczegółów spotkania.
- ☐ Zbędne wiadomości organizacyjne porządkuję zgodnie z zasadami retencji organizacji; nie usuwam niczego, co wiąże się z incydentem, podejrzeniem przestępstwa lub sporem.
- ☐ Dokumenty do zniszczenia trafiły do niszczarki, nie do kosza.
- ☐ Jeśli rozmówca wypytywał o harmonogramy, dostęp lub zabezpieczenia, poinformowałem dział bezpieczeństwa (H).

13.7. Po incydencie bezpieczeństwa

- ☐ Jestem bezpieczny, a osoby towarzyszące są ze mną lub w kontakcie.
- ☐ Pomoc została wezwana, jeśli była potrzebna; znam numer sprawy nadany przez policję.
- ☐ Przy utracie urządzenia: blokada zdalna, dział IT, zastrzeżenie SIM, zmiana haseł, zakończenie sesji.
- ☐ Przy utracie dokumentów: zgłoszenie utraty dowodu, zastrzeżenie PESEL, zastrzeżenie kart.
- ☐ Przy możliwym ujawnieniu informacji: dział bezpieczeństwa, inspektor ochrony danych, przy informacjach niejawnych pełnomocnik ochrony.
- ☐ Sporządziłem notatkę według wzoru z aneksu C, z podziałem na fakty i oceny.
- ☐ Zabezpieczyłem dowody: zrzuty ekranu, zdjęcia, potwierdzenia.

- ☐ Przy sygnałach działania obcych służb zgłosiłem sprawę do ABW lub przekazałem ją do działu bezpieczeństwa z taką rekomendacją (H).
- ☐ Zdarzenie trafiło do rejestru incydentów organizacji.
- ☐ Po kilku dniach przejrzałem notatkę i ustaliłem, co zmieniam w swoich nawykach i procedurach.
- ☐ Zadbałem o siebie; jeśli stres się utrzymuje, korzystam z pomocy psychologicznej.

13.8. Karta kieszonkowa

Najkrótsza wersja przewodnika, do wydrukowania na odwrocie wizytówki lub zapisania w notatce w telefonie:

Sytuacja	Zasada
Wybór miejsca	W lokalu tylko to, co wolno ujawnić. Szczegóły w biurze lub w zatwierdzonym kanale.
Coś mnie niepokoi	Najpierw oceń, czy zagrożenie jest bezpośrednie (jeśli tak: oddal się, 112). Jeśli nie, opisz obserwację i rozważ zwyczajne wyjaśnienia.
Zagrożenie bezpośrednie	Oddal się do ludzi, dzwoń 112, nie konfrontuj się.
Ktoś pyta za dużo	Ogólnie, grzecznie, ta sama formuła odmowy.
Oferta łatwego zarobku	Nie wykonuj, nie kasuj, zrób zrzuty ekranu, zgłoś: ABW 22 585 82 21 lub @ABW_STOPdywersji_bot.
Zgubiony telefon	Blokada zdalna, IT, SIM, hasła. Natychmiast.
Po wszystkim	Notatka: fakty osobno, oceny osobno.

14.

Biznes z Ukrainą, w Ukrainie i na rzecz Ukrainy

Firmy i organizacje, które handlują z Ukrainą, pracują na jej terytorium albo dostarczają jej sprzęt, usługi i pomoc, są dziś w grupie podwyższonego ryzyka. Według ICCT i GLOBSEC wsparcie dla Ukrainy jest najważniejszym czynnikiem, od którego zależy wybór celów rosyjskich ataków w Europie. ABW wymienia miejsca związane z organizacją wsparcia dla Ukrainy obok obiektów wojskowych i infrastruktury krytycznej. Duńska służba PET poinformowała 7 października 2026 roku, że Rosja przeszła do ataków sabotażowych na duńskie firmy zbrojeniowe dostarczające sprzęt Ukrainie, bo szersze działania nie zniechęciły Zachodu do pomocy, a teraz celem są podmioty mające „bezpośredni wpływ na front", czyli produkcja uzbrojenia (Kyiv Post za Reuters). Ten rozdział zbiera zalecenia z całego przewodnika w wersji dla tej grupy i dodaje kwestie, które dotyczą tylko jej.

14.1. Trzy profile, trzy rodzaje ryzyka

Profil	Kto	Główne ryzyka
Praca na rzecz Ukrainy z Polski	Producenci sprzętu i komponentów (w tym dronów), firmy logistyczne i spedycyjne, magazyny, przewoźnicy, dostawcy energetyki i telekomunikacji, firmy IT	Rozpoznanie i sabotaż obiektów, werbunek pracowników i podwykonawców, wycieki harmonogramów i tras, cyberataki, dezinformacja wymierzona w firmę
Interesy w Ukrainie	Firmy z biurami, zakładami, projektami odbudowy, inwestorzy, konsultanci, audytorzy, dziennikarze	Zagrożenie fizyczne (ataki rakietowe i dronowe), przepisy stanu wojennego, kontrahenci powiązani z Rosją, przejęte konta partnerów, utrata łączności
Pomoc i wolontariat	Fundacje, zbiórki, konwoje, punkty przeładunkowe, grupy wolontariuszy	Ujawnianie lokalizacji i tras w mediach społecznościowych, przenikanie do grup osób o fałszywej tożsamości, oszustwa, wykorzystanie emocji do manipulacji

Wiele organizacji łączy dwa albo trzy profile. Warto to nazwać wprost w ocenie ryzyka (rozdział 1.3), bo od profilu zależy, które z poniższych podrozdziałów są najważniejsze.

14.2. Firma w Polsce pracująca na rzecz Ukrainy

Z perspektywy zleceniodawcy sabotażu twoja firma jest celem wtedy, gdy wiadomo, że pracuje dla Ukrainy, gdzie są jej obiekty i kiedy coś z nich wyjeżdża. Ograniczanie tych trzech informacji jest podstawą ochrony.

Komunikacja publiczna. Sukces kontraktu z ukraińskim partnerem kusi, żeby się nim pochwalić. Przy dostawach o znaczeniu obronnym lub infrastrukturalnym rozważ, czy komunikat musi zawierać nazwę zakładu, zdjęcia hali, liczby, terminy i nazwiska kierowników projektu. Zdjęcia produktu na tle charakterystycznej hali i wpis pracownika „dziś wyjechał kolejny transport" pozwalają ustalić lokalizację i rytm wysyłek. 15 kwietnia 2026 roku rosyjskie Ministerstwo Obrony opublikowało listę zakładów produkujących drony i ich komponenty w kilkunastu państwach, w tym w Polsce, z adresami, a Dmitrij Miedwiediew nazwał ją listą potencjalnych celów dla rosyjskich sił zbrojnych. Firmy z tego sektora powinny szczególnie uważnie dobierać to, co publikują.

Pracownicy, podwykonawcy, agencje pracy. Jednorazowi wykonawcy są werbowani także spośród osób, które mają naturalny dostęp do obiektów: pracowników tymczasowych, kierowców, ochroniarzy, sprzątających, serwisantów. Uzgodnij z agencjami i podwykonawcami zasady weryfikacji osób kierowanych na teren obiektów, przyznawaj dostęp tylko do niezbędnych stref i odbieraj go natychmiast po zakończeniu pracy.

Świadomość załogi. Przeprowadź krótkie szkolenie z rozdziału 4.9 dla całej załogi, w tym dla pracowników zmianowych i magazynowych, w językach, którymi posługują się pracownicy. Chatbot ABW działa w językach polskim, angielskim, ukraińskim i rosyjskim. ABW prowadzi też szkolenia z profilaktyki kontrwywiadowczej dla podmiotów o znaczeniu strategicznym i udostępnia platformę e-learningową.

Ochrona fizyczna. Przegląd ogrodzeń, oświetlenia, kamer i stref, w których stoją szafy zasilające, generatory, zbiorniki i materiały łatwopalne. Przypadek stacji Starlink z września 2026 roku pokazał, że atak może polegać na pokonaniu ogrodzenia i podpaleniu szafy elektrycznej. Ochrona powinna wiedzieć, że osoby fotografujące te elementy albo spacerujące wzdłuż ogrodzenia należy odnotować i zgłosić (rozdział 4.9).

Gotowość na dezinformację. ABW wskazuje, że rosyjskie służby wykorzystują historyczne antagonizmy, głównie polsko-ukraińskie, i podsycają nastroje polaryzujące. Firma pracująca dla Ukrainy może stać się bohaterem fałszywych informacji (o rzekomych wypadkach, skażeniach, zwolnieniach, „wywożeniu polskiego sprzętu"). Przygotuj osobę odpowiedzialną za szybkie dementi, listę oficjalnych kanałów i zasadę, że pracownicy nie komentują takich doniesień w mediach społecznościowych.

Kontakt ze służbami. Ustal, kto w firmie kontaktuje się z ABW, policją i ochroną obiektów w razie zdarzenia, i przekaż te dane wszystkim kierownikom zmian.

14.3. Partnerzy i kontrahenci: weryfikacja

Współpraca z Ukrainą to często szybkie decyzje, nowi pośrednicy i łańcuchy dostaw przebiegające przez kilka państw. To ułatwia działanie podmiotom, które chcą uzyskać informacje, towary lub pieniądze pod fałszywym pretekstem.

Przed nawiązaniem współpracy:

- sprawdź kontrahenta w oficjalnym ukraińskim rejestrze podmiotów i w komercyjnych bazach danych o firmach, z uwzględnieniem historii zmian właścicieli i zarządu,
- ustal beneficjenta rzeczywistego i sprawdź, czy w strukturze nie ma osób lub spółek powiązanych z Rosją lub Białorusią,
- zweryfikuj kontrahenta i jego właścicieli na unijnych listach sankcyjnych oraz na polskiej liście prowadzonej przez MSWiA na podstawie ustawy z 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę,

- przy towarach podwójnego zastosowania i uzbrojeniu upewnij się, że masz wymagane zezwolenia i że znasz ostatecznego odbiorcę; ABW opiniuje tysiące wniosków o zezwolenia na obrót towarami strategicznymi i ściga ich wywóz do Rosji przez państwa trzecie,
- zweryfikuj osobę kontaktową niezależnym kanałem (rozdział 9.1), zwłaszcza gdy kontakt przyszedł przez pośrednika lub komunikator.

Sygnały ostrzegawcze w relacji z kontrahentem: nalegania na dostawę przez dodatkowe państwo bez uzasadnienia, zmiana odbiorcy w ostatniej chwili, płatność od podmiotu trzeciego, zainteresowanie szczegółami technicznymi i harmonogramami wykraczające poza potrzeby zamówienia, prośby o dokumentację „do wglądu" przed podpisaniem umowy.

14.4. Płatności, faktury i przejęte konta partnerów

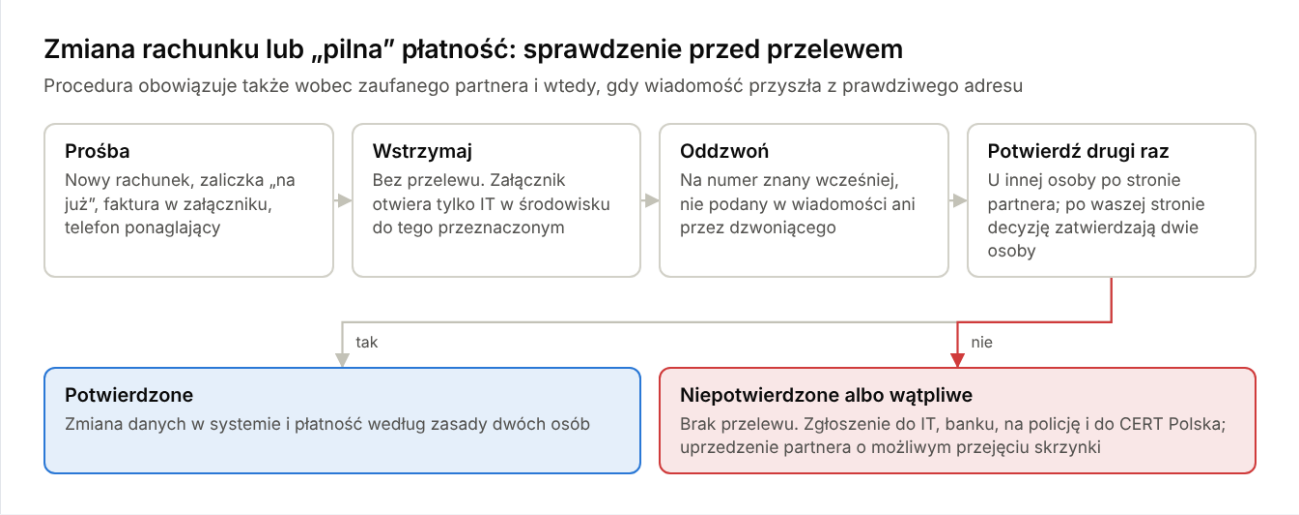
Oszustwa polegające na podszywaniu się pod kontrahenta (zmiana numeru rachunku w fakturze, „pilna" płatność zaliczki, nowy adres e-mail „z powodu ataku na serwer") są szczególnie skuteczne w relacjach z partnerami działającymi w warunkach wojny, bo przerwy w łączności i zmiany organizacyjne wydają się naturalne.

Zasady:

- każdą zmianę rachunku bankowego potwierdzaj telefonicznie na numer znany wcześniej, nie podany w tej samej wiadomości,
- przy płatnościach powyżej ustalonego progu stosuj zasadę dwóch osób,
- ustal z partnerem z góry, jakim kanałem potwierdzacie zmiany danych,
- traktuj z ostrożnością załączniki i linki od partnera, jeśli wiadomość jest nietypowa, nawet gdy przychodzi z prawdziwego adresu.

Ostatni punkt wymaga wyjaśnienia. Ukraiński zespół CERT-UA wielokrotnie opisywał kampanie, w których atakujący wysyłali wiadomości z przejętych skrzynek prawdziwych instytucji, a nawet podszywali się pod samo CERT-UA i SBU, żeby skłonić odbiorców do instalacji oprogramowania zdalnego dostępu (The Hacker News, przegląd komunikatów CERT-UA). W styczniu 2026 roku CERT-UA opisało wykorzystanie przez rosyjską grupę APT28 luki w pakiecie Microsoft Office do ataków na instytucje ukraińskie, a te same dokumenty i infrastruktura pojawiły się w atakach na organizacje w UE (SOC Prime za CERT-UA). Wniosek praktyczny: aktualizuj oprogramowanie bez zwłoki i nie zakładaj, że wiadomość jest bezpieczna tylko dlatego, że nadawca jest prawdziwy.

Do tego dochodzą wideorozmowy i nagrania głosu wygenerowane przez sztuczną inteligencję (podrozdział 8.15). Głos albo twarz znajomego dyrektora po stronie partnera nie zastępuje procedury: zmianę rachunku i pilną płatność potwierdzasz na numer znany wcześniej, u drugiej osoby po stronie partnera, a po swojej stronie decyzję zatwierdzają dwie osoby.



Rys. 26. Weryfikacja zmiany rachunku lub pilnej płatności

14.5. Komunikacja i dane we współpracy z partnerami z Ukrainy

- Do rozmów i przesyłania dokumentów używaj komunikatorów z szyfrowaniem end-to-end i kanałów zatwierdzonych przez organizację. Nie używaj usług, których dostawcy podlegają jurysdykcji rosyjskiej.
- Udostępniaj dokumenty partnerom z ograniczonym czasem dostępu i tylko osobom wskazanym z nazwiska. Regularnie przeglądaj, kto ma dostęp do wspólnych folderów.
- Uwzględnij, że urządzenia partnerów w Ukrainie mogą zostać zniszczone, zgubione lub przejęte w wyniku działań wojennych. Nie przesyłaj im więcej, niż potrzebują.
- Ustal kanał zapasowy na wypadek przerw w dostawach prądu i łączności oraz zasadę, ile czasu bez kontaktu jest normalne, zanim uruchamiacie procedurę z rozdziału 11.7.
- Nie opisuj w korespondencji tras, terminów i miejsc załadunku dokładniej, niż wymaga tego realizacja zlecenia.

14.6. Podróże służbowe do Ukrainy

MSZ utrzymuje dla Ukrainy najwyższy, czwarty poziom ostrzeżenia: odradza wszelkie podróże ze względu na działania zbrojne i zaleca obywatelom polskim przebywającym w Ukrainie rozważenie niezwłocznego opuszczenia kraju (serwis Odyseusz, MSZ). Ostrzeżenie dotyczy także podróży służbowych. Decyzja o wyjeździe powinna więc zapadać na poziomie organizacji, po ocenie ryzyka i z pełną świadomością, że możliwości pomocy konsularnej są ograniczone.

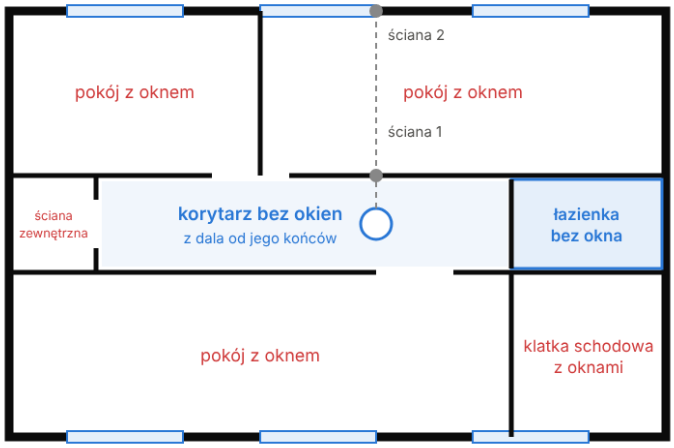
Jeśli wyjazd jest konieczny:

- zarejestruj podróż w systemie Odyseusz (także w aplikacji mObywatel) i zapisz numery dyżurne ambasady i konsulatów RP w telefonie oraz na kartce,
- miej ważny paszport; według MSZ dowód osobisty nie uprawnia do przekroczenia granicy,
- sprawdź ubezpieczenie: Europejska Karta Ubezpieczenia Zdrowotnego nie działa w Ukrainie, a wiele polis wyłącza szkody związane z działaniami wojennymi, więc potrzebne jest ubezpieczenie obejmujące ryzyko wojenne,
- przygotuj plan podróży, godziny kontrolne i plan wyjazdu awaryjnego z zaufaną osobą w Polsce (rozdziały 1.6 i 5.6),

- zainstaluj oficjalną aplikację ostrzegającą o alarmach lotniczych dla regionu pobytu i pobierz mapy offline, bo nawigacja satelitarna i internet mobilny mogą działać zawodnie,
- w każdym miejscu noclegu i spotkania ustal, gdzie jest najbliższy schron, i przy ogłoszeniu alarmu udawaj się tam bez zwłoki; jeśli schronu nie ma, wybierz pomieszczenie bez okien, oddzielone od zewnątrz co najmniej dwiema ścianami,
- licz się z tym, że w trakcie alarmu pociąg lub autobus może się zatrzymać, a pasażerowie muszą udać się w bezpieczne miejsce,
- miej zawsze przy sobie dokument tożsamości i stosuj się do poleceń patroli i punktów kontrolnych; przed wyjazdem sprawdź w oficjalnych źródłach ukraińskich aktualny okres obowiązywania stanu wojennego oraz związane z nim ograniczenia,
- sprawdź lokalne godziny policyjne, które różnią się między regionami, i planuj spotkania tak, żeby wracać przed ich rozpoczęciem,
- zabierz urządzenia „podróżne" z minimalną ilością danych (rozdział 8.12),
- uwzględnij przy planowaniu spotkań, że mężczyźni w wieku poborowym, obywatele Ukrainy, podlegają ograniczeniom wyjazdu z kraju, więc spotkania z niektórymi partnerami możliwe są tylko na miejscu lub zdalnie.

Alarm lotniczy, a schronu nie ma: zasada dwóch ścian

Szkic poglądowy mieszkania lub piętra hotelu. Między tobą a zewnętrzem powinny być co najmniej dwie ściany



- Pierwszy wybór: schron lub ukrycie. Ustal, gdzie jest, zaraz po przyjeździe do hotelu i w każdym miejscu spotkania.
- Jeśli schronu nie ma albo nie zdążysz: pomieszczenie bez okien, oddzielone od zewnątrz co najmniej dwiema ścianami, np. korytarz lub łazienka.
- Unikaj pomieszczeń z oknami, ścian zewnętrznych, balkonów i przeszklonych klatek schodowych.

Rys. 27. Zasada dwóch ścian przy alarmie lotniczym · szkic poglądowy

14.7. Czego nie fotografować i nie publikować w Ukrainie

Ukraiński Kodeks karny w art. 114-2 przewiduje karę pozbawienia wolności za nieuprawnione rozpowszechnianie w czasie stanu wojennego informacji o rozmieszczeniu i przemieszczaniu się sił zbrojnych, o dostawach międzynarodowej pomocy wojskowej i o uzbrojeniu. SBU interpretuje to szeroko: zabronione jest publikowanie nagrań pracy obrony przeciwlotniczej, skutków ataków na obiekty wojskowe i infrastrukturę krytyczną oraz przemieszczania się sprzętu i żołnierzy. Według SBU od początku 2026 roku do połowy października skazano za takie publikacje 75 osób (Interfax-Ukraina). SBU podkreśla, że takie materiały pomagają przeciwnikowi przygotowywać i korygować kolejne ataki.

Praktyczne zasady na czas pobytu:

- nie fotografuj i nie filmuj obrony przeciwlotniczej, pocisków, dronów na niebie, miejsc trafień, punktów kontrolnych, pojazdów i obiektów wojskowych, infrastruktury energetycznej,
- nie publikuj niczego z lokalizacją w czasie pobytu; zdjęcia z podróży publikuj po powrocie i po sprawdzeniu tła,
- nie przesyłaj zdjęć zniszczeń znajomym „żeby pokazali, jak tu jest", bo trafiają dalej,
- uważaj na tło zdjęć ze spotkań biznesowych: widok z okna hotelu może pokazywać obiekt, którego lokalizacja nie powinna być ujawniana.

Te same zasady warto stosować w Polsce wobec transportów pomocy wojskowej i humanitarnej (rozdział 5.9).

14.8. Werbunek po obu stronach granicy

Rosyjskie służby werbują wykonawców także w samej Ukrainie, a stosowane tam metody przenikają do Polski, gdzie mieszka i pracuje duża społeczność ukraińska. SBU podała na początku sierpnia 2026 roku, że od początku roku Rosja podjęła w Ukrainie ponad 300 prób sabotażu i zamachów; SBU i policja ujawniły 249 takich spraw, a 84 zapobiegły (Interfax-Ukraina). Według SBU werbownik podszywa się pod pracodawcę, wolontariusza, funkcjonariusza lub korzysta z portali randkowych, a pierwsze zadania to dostarczenie paczki, zrobienie zdjęcia obiektu lub zakup określonych materiałów w sklepie budowlanym.

Szczególnie groźny jest schemat, przed którym SBU i ukraińska policja ostrzegły w lipcu 2026 roku: werbownik podaje się za śledczego SBU lub policjanta, wysyła przez komunikator sfałszowane wezwanie w sfabrykowanej sprawie (np. o rzekomy zakup leków w rosyjskich sklepach internetowych), ofiarę wybiera na podstawie danych wykradzionych z handlu internetowego i w zamian za „umorzenie sprawy" zleca zadania, od obserwacji po sabotaż (Euromaidan Press). ICCT i GLOBSEC opisują z kolei nacisk na uchodźców z terenów okupowanych przez osoby, które znali przed wojną i które pozostały pod rosyjską kontrolą.

Co z tego wynika dla pracodawców i partnerów:

- poinformuj pracowników z Ukrainy, w ich języku, o tych schematach i o tym, że prawdziwe służby nie zlecają obywatelom zadań przez komunikator,
- wskaż kanały zgłoszeń: w Polsce ABW (chatbot w języku ukraińskim), a w sprawach dotyczących Ukrainy SBU (bezpłatna infolinia 1516, chatbot t.me/spaly_fsb_bot),
- zapewnij, że zgłoszenie próby nacisku nie będzie powodem zwolnienia ani podejrzeń wobec pracownika; ofiary szantażu często milczą ze strachu przed utratą pracy i statusu pobytowego,
- nie traktuj pracowników z Ukrainy jako grupy podejrzanej; są w tej sytuacji przede wszystkim celem, a ich czujność bywa najlepszym źródłem sygnałów.

14.9. Wolontariat i organizacje pomocowe

Organizacje pomocowe działają zwykle szybko, otwarcie i z dużym zaufaniem do nowych osób. To ich siła i jednocześnie słaby punkt.

- Publikując apele i relacje, nie podawaj miejsc załadunku, magazynów, tras, godzin wyjazdu ani zdjęć z numerami rejestracyjnymi pojazdów.

- Weryfikuj nowych wolontariuszy i darczyńców oferujących nietypową pomoc (transport, magazyn, „kontakty na granicy"), zwłaszcza gdy szybko pytają o szczegóły logistyczne.
- Prowadź otwarte grupy w komunikatorach tylko do spraw ogólnych; szczegóły logistyczne omawiaj w zamkniętej grupie zweryfikowanych osób.
- Nie przyjmuj paczek od nieznanych osób do przewiezienia „przy okazji" konwoju.
- Wyznacz osobę odpowiedzialną za zgłaszanie niepokojących sytuacji do ABW i policji.

14.10. Scenariusz 9: „pilna zmiana rachunku" od ukraińskiego partnera

Sytuacja. Dział finansów polskiego dostawcy generatorów dla ukraińskich szpitali dostaje wiadomość z prawdziwego adresu wieloletniego partnera z Kijowa. Partner pisze, że po ataku na ich bank muszą „pilnie" zmienić rachunek i prosi o przelew zaliczki na nowe konto w państwie trzecim. W załączniku jest „zaktualizowana faktura" w pliku Office. Kilka minut później dzwoni ktoś przedstawiający się jako dyrektor finansowy partnera i ponagla.

Sygnały ostrzegawcze: zmiana rachunku, rachunek w innym państwie, presja czasu, załącznik w formacie, który może zawierać złośliwy kod, telefon z numeru niezweryfikowanego.

Możliwe wyjaśnienia: partner rzeczywiście ma problem z bankiem; skrzynka partnera została przejęta; obie rzeczy jednocześnie.

Zalecane działania: nie otwierać załącznika poza środowiskiem sprawdzonym przez IT, wstrzymać płatność, oddzwonić do partnera na wcześniej znany numer, potwierdzić zmianę z inną osobą po jego stronie, poinformować dział IT o możliwym przejęciu skrzynki partnera, a po potwierdzeniu oszustwa zgłosić sprawę na policję, do banku i do CERT Polska oraz uprzedzić partnera.

Błędy do uniknięcia: przelew „bo to sprawdzony partner i ratujemy szpitale", oddzwonienie na numer podany w wiadomości, otwarcie faktury na komputerze z dostępem do systemów płatniczych.

Wnioski. Emocjonalny kontekst pomocy Ukrainie jest wykorzystywany do skrócenia procedur. Procedury weryfikacji płatności powinny obowiązywać bez wyjątków, także wtedy, gdy cel jest szczytny, a partner zaufany.

14.11. Lista kontrolna dla organizacji pracujących z Ukrainą i na jej rzecz

- ☐ Ocena ryzyka uwzględnia nasz profil (praca dla Ukrainy z Polski, interesy w Ukrainie, pomoc).
- ☐ Komunikacja publiczna nie ujawnia lokalizacji obiektów, rytmu wysyłek, tras ani nazwisk kierowników projektów.
- ☐ Pracownicy, w tym zmianowi i tymczasowi, przeszli szkolenie o werbunku w zrozumiałym dla nich języku.
- ☐ Agencje pracy i podwykonawcy stosują uzgodnione zasady weryfikacji osób wchodzących na teren obiektów.
- ☐ Ochrona wie, że fotografowanie zabezpieczeń i spacery wzdłuż ogrodzenia należy odnotować i zgłosić.
- ☐ Szafy zasilające, generatory i materiały łatwopalne są zabezpieczone i objęte monitoringiem.
- ☐ Kontrahenci są sprawdzeni w rejestrach, pod kątem beneficjenta rzeczywistego i list sankcyjnych.
- ☐ Towary podwójnego zastosowania mają wymagane zezwolenia, a ostateczny odbiorca jest znany.

- ☐ Zmiany rachunków bankowych potwierdzamy telefonicznie na znany numer, a duże płatności zatwierdzają dwie osoby.
- ☐ Oprogramowanie jest aktualizowane bez zwłoki; załączniki od partnerów przechodzą kontrolę.
- ☐ Mamy kanał zapasowy łączności z partnerami w Ukrainie i ustaloną procedurę na wypadek utraty kontaktu.
- ☐ Wyjazdy do Ukrainy zatwierdza organizacja po ocenie ryzyka; podróżni mają ubezpieczenie obejmujące ryzyko wojenne, rejestrację w Odyseuszu i plan awaryjny.
- ☐ Podróżni znają zakaz fotografowania i publikowania materiałów o obronie i skutkach ataków w Ukrainie.
- ☐ Pracownicy z Ukrainy wiedzą, jak zgłosić próbę nacisku w Polsce (ABW) i w Ukrainie (SBU 1516), i wiedzą, że zgłoszenie nie zaszkodzi ich zatrudnieniu.
- ☐ Mamy przygotowaną reakcję na dezinformację wymierzoną w firmę.
- ☐ Wiemy, kto w organizacji kontaktuje się z ABW, policją i ochroną obiektów.

15.

OPSEC dla osób pracujących z wojskiem, dla wojska i w infrastrukturze krytycznej

Osoby związane z wojskiem i infrastrukturą krytyczną rzadko ujawniają tajemnice wprost. Znacznie częściej ujawniają drobne, jawne informacje, które ktoś z zewnątrz składa w obraz całości: trasę porannego biegu wokół jednostki, zdjęcie z przysięgi z widocznym oznaczeniem, wpis żony „mąż na poligonie do piątku", ogłoszenie firmy o naborze kierowców do konkretnej bazy, portfolio podwykonawcy z fotografiami instalacji. ABW pisze, że rosyjski wywiad prowadził w latach 2024–2025 w Polsce rozpoznanie na masową skalę, także pod kątem przygotowań do aktów dywersji, a obiekty wojskowe i infrastruktura krytyczna były ich głównymi celami. Ten rozdział opisuje OPSEC (ochronę informacji o działaniach i planach) w praktyce codziennej. Nie zastępuje przepisów, rozkazów ani wewnętrznych instrukcji, które w tych środowiskach mają zawsze pierwszeństwo.

15.1. Dla kogo jest ten rozdział

Grupa	Przykłady	Najczęstsze źródła wycieku
Żołnierze i pracownicy resortu obrony	Żołnierze zawodowi, WOT, żołnierze dobrowolnej zasadniczej służby, rezerwiści na ćwiczeniach, pracownicy cywilni wojska	Smartfony i zegarki, media społecznościowe, aplikacje sportowe, rozmowy poza jednostką, rodzina
Przemysł obronny i podwykonawcy	Producenci uzbrojenia i komponentów, firmy serwisowe, IT, budowlane, transportowe, cateringowe i porządkowe pracujące dla wojska	Portfolio i marketing, ogłoszenia o pracę, profile zawodowe pracowników, przetargi, korespondencja z podwykonawcami
Infrastruktura krytyczna	Energetyka, paliwa, gaz, woda i ścieki, telekomunikacja, transport, ochrona zdrowia, finanse, administracja	Dokumentacja techniczna poza systemami firmy, zdalny dostęp, słabe hasła, rozmowy branżowe, fotografie obiektów
Rodziny i bliscy	Partnerzy, dzieci, rodzice osób z powyższych grup	Media społecznościowe, rozmowy z obcymi, publikacje o wyjazdach i nieobecnościach

15.2. OPSEC jako proces w pięciu krokach

Klasyczny model OPSEC, stosowany w wojsku i administracji wielu państw NATO, składa się z pięciu kroków. Warto go znać także poza wojskiem, bo porządkuje myślenie o tym, co chronić i dlaczego.



Rys. 28. Pięć kroków OPSEC w układzie cyklu

Krok	Pytanie	Przykład dla operatora stacji uzdatniania wody	Przykład dla żołnierza
1. Informacje krytyczne	Jakie informacje o nas są cenne dla przeciwnika?	Lokalizacja i schemat pompowni, dostęp zdalny, dostawca systemu sterowania, godziny pracy zmiany	Termin wyjazdu na ćwiczenia, skład pododdziału, rozmieszczenie sprzętu
2. Zagrożenia	Kto może chcieć je zdobyć i jakimi metodami?	Obce służby, haktywiści, przestępcy; skanowanie internetu, socjotechnika, rozpoznanie terenu	Obce służby i ich jednorazowi wykonawcy; OSINT, werbunek, obserwacja
3. Podatności	Którędy te informacje mogą wyciec?	Panel sterowania dostępny z internetu, hasło domyślne, rozmowy na branżowej grupie	Strava, zdjęcia z ćwiczeń, wpisy rodziny, rozmowy w pociągu
4. Ryzyko	Co się stanie, jeśli wycieką, i jak bardzo jest to prawdopodobne?	Możliwość zmiany parametrów uzdatniania, przerwa w dostawach wody	Przygotowanie ataku lub prowokacji, nacisk na żołnierza lub rodzinę
5. Środki	Co realnie możemy zrobić?	Odcięcie paneli od internetu, MFA, szkolenie zespołu	Ustawienia prywatności, zasady dla rodziny, dyscyplina w rozmowach

Proces nie kończy się na piątym kroku. Wraca się do pierwszego przy każdej zmianie: nowym projekcie, nowym obiekcie, nowym podwykonawcy, nowym zagrożeniu.

15.3. Informacje krytyczne i wskaźniki pośrednie

Informacją krytyczną jest każda informacja, która ujawnia zamiar, zdolność, słabość lub rytm działania, także wtedy, gdy dokument nie ma klauzuli. Poniżej najczęstsze kategorie.

Kategoria	Przykłady informacji, których nie należy ujawniać poza krąg uprawnionych
Harmonogramy	Terminy wyjazdów, ćwiczeń, dostaw, przeglądów, wyłączeń, zmian warty i ochrony
Lokalizacje	Rozmieszczenie sprzętu, magazynów, punktów przeładunku, tymczasowych miejsc postoju
Zdolności i braki	Awarie, braki kadrowe, braki sprzętu, opóźnienia dostaw, luki w zabezpieczeniach

Kategoria	Przykłady informacji, których nie należy ujawniać poza krąg uprawnionych
Ludzie	Kto ma dostęp do czego, kto jest na urlopie, nazwiska i dane rodzin, przepustki
Procedury	Sposób kontroli dostępu, procedury reagowania, czasy reakcji ochrony
Technika	Systemy, wersje oprogramowania, dostawcy, konfiguracje, schematy sieci i instalacji
Łańcuch dostaw	Kto dostarcza, skąd, kiedy, jakim transportem

Wskaźniki pośrednie to jawne ślady, z których można wywnioskować informacje krytyczne. Przykłady:

- ogłoszenie o pracę „pilnie 30 kierowców z uprawnieniami ADR do realizacji kontraktu dla jednostki w X od przyszłego miesiąca”,
- dokumentacja przetargowa ze szczegółowymi rzutami, schematami i lokalizacjami urządzeń,
- nagły wzrost zamówień jedzenia, noclegów i transportu w okolicy obiektu,
- zdjęcie zespołu na tle hali z widocznym sprzętem i tablicą z harmonogramem,
- wpis w profilu zawodowym „wdrożyłem system X w Y obiektach energetycznych operatora Z”,
- zmiana zdjęcia profilowego na zdjęcie w mundurze z nowej lokalizacji.

Sam wskaźnik nie jest tajemnicą, a często nie da się go ukryć. Chodzi o to, żeby nie dokładać do niego szczegółów, które zamieniają przypuszczenie w pewność.

15.4. Smartfony, zegarki i aplikacje

W resorcie obrony zasady wnoszenia i używania urządzeń rejestrujących obraz i dźwięk określa decyzja nr 77/MON z 9 czerwca 2020 r., która uzależnia możliwość korzystania z urządzeń prywatnych i służbowych od klasy strefy ochronnej (Defence24). Szczegółowe zasady w danej jednostce wynikają z rozkazów i instrukcji, których należy przestrzegać bez wyjątków. Poniższe zalecenia dotyczą czasu poza strefami i życia prywatnego.

Aplikacje sportowe i lokalizacyjne. Publiczne profile w aplikacjach do rejestrowania treningów wielokrotnie pozwalały ustalić położenie baz i trasy żołnierzy. Na początku 2018 roku analitycy zauważyli, że opublikowana przez Stravę globalna mapa cieplna ujawnia lokalizacje i trasy wokół baz wojskowych w kilku państwach. W 2025 roku w interpelacji poselskiej nr 8712 opisano, że te same mechanizmy pozwalały identyfikować trasy żołnierzy polskich i sojuszniczych w pobliżu baz w Polsce (Sejm, interpelacja 8712). Sky News zidentyfikowało ponad 1300 użytkowników udostępniających treningi z amerykańskich baz na Bliskim Wschodzie, mimo zakazów dowództwa (TVP Info).

Zalecenia:

- ustaw profile w aplikacjach sportowych jako prywatne i wyłącz udział w publicznych mapach cieplnych i rankingach odcinków,
- nie rejestruj treningów na terenie jednostek i obiektów ani w ich bezpośrednim otoczeniu; strefa prywatności wokół domu nie chroni obiektu,
- wyłącz historię lokalizacji w kontach Google i Apple,
- nie oznaczaj lokalizacji na zdjęciach i nie publikuj ich w czasie rzeczywistym,
- sprawdzaj uprawnienia aplikacji do lokalizacji, mikrofonu i aparatu (rozdział 8.6).

Grupy w komunikatorach. Nieformalne grupy pododdziału, zmiany czy zespołu projektowego w prywatnych komunikatorach są wygodne, ale gromadzą w jednym miejscu harmonogramy, zdjęcia i nazwiska. Jeden przejęty telefon albo jeden członek grupy, który przestał w niej być lojalny, wystarcza do wycieku. Takie grupy powinny służyć wyłącznie sprawom organizacyjnym niewrażliwym, a wszystko inne trafia do kanałów zatwierdzonych przez organizację.

Zegarki i opaski. Synchronizują dane z chmurą producenta, często z lokalizacją. Na teren stref, w których obowiązują ograniczenia, nie wnoś ich wbrew zasadom, a poza nimi stosuj te same ustawienia prywatności co w telefonie.

15.5. Media społecznościowe, życie prywatne i podatność na nacisk

Zasady publikowania:

- nie publikuj zdjęć z jednostki, z ćwiczeń, ze sprzętem, z dokumentami, z tablicami i ekranami w tle,
- nie publikuj informacji o wyjazdach i nieobecnościach przed ich zakończeniem, a po zakończeniu oceniaj treść, tło i metadane, bo opóźnienie publikacji nie jest zgodą na ujawnienie informacji,
- nie wskazuj w profilu numeru jednostki, stanowiska, specjalności ani obiektu, w którym pracujesz, jeśli nie jest to niezbędne,
- uważaj na oznaczenia na mundurze i odzieży roboczej widoczne na zdjęciach,
- nie wchodź w publiczne dyskusje o sprzęcie, brakach i incydentach w swojej formacji lub firmie.

Podatność na nacisk. ABW zaleca higienę relacji, czyli unikanie sytuacji, które mogłyby stać się podstawą szantażu, i ostrożność wobec nieoczekiwanych przysług i prezentów (rozdział 9). ICCT i GLOBSEC wskazują, że zwerbowani sprawcy często byli w trudnej sytuacji finansowej, zadłużeni lub uzależnieni. SBU opisuje werbunek przez portale randkowe. Oznacza to, że problemy z długami, hazardem czy uzależnieniem są sprawą prywatną, a zarazem punktem, który ktoś z zewnątrz może wykorzystać. Najlepszą ochroną jest wczesne szukanie pomocy, także w ramach programów wsparcia oferowanych przez pracodawcę lub resort, zanim problem stanie się dźwignią w cudzych rękach.

Randki i nowe znajomości. Nowa znajomość, która szybko kieruje rozmowę na twoją pracę, jednostkę, dostęp do systemów, wyjazdy lub kolegów, wymaga ostrożności (rozdział 9.9). Nie musi to oznaczać złych intencji, ale granica dyskrecji powinna być taka sama jak wobec każdego obcego.

15.6. Kontakty, podróże i werbunek

ABW opisuje kilka wzorców, które dotyczą bezpośrednio tej grupy:

- rosyjskie służby przy tworzeniu komórek dywersyjnych preferują osoby z doświadczeniem w strukturach siłowych (byłych żołnierzy, funkcjonariuszy, najemników),
- białoruskie służby próbują indagować i pozyskiwać polskich obywateli regularnie podróżujących na Białoruś,
- chiński wywiad pod pozorem dobrze płatnych zleceń próbował pozyskiwać ekspertów, naukowców, urzędników i osoby związane z resortami siłowymi,
- w maju 2026 roku ABW zatrzymała trzech obywateli Polski, którzy według Agencji byli przygotowywani do zadań dywersyjnych i sabotażowych na rzecz obcego wywiadu (Eska).

Zasady praktyczne:

- osoby z poświadczeniem bezpieczeństwa i dostępem do informacji niejawnych postępują zgodnie z procedurami swojej jednostki dotyczącymi zgłaszania kontaktów, podróży zagranicznych i zmian w sytuacji osobistej; w razie wątpliwości pytają pełnomocnika ds. ochrony informacji niejawnych,
- podróże do państw o podwyższonym ryzyku (Rosja, Białoruś, a także inne państwa wskazane przez organizację) planujesz w porozumieniu z przełożonym lub pełnomocnikiem i po powrocie informujesz o nietypowych kontaktach i kontrolach,
- każdą ofertę płatnej konsultacji, raportu, wykładu lub „analizy rynku" od nieznanego podmiotu, która dotyczy twojej specjalności wojskowej lub branży krytycznej, traktujesz jako sygnał do weryfikacji i zgłoszenia (rozdziały 8.11 i 9.9),
- nie zgadzasz się na żadne „drobne przysługi" związane z dostępem: wpuszczenie na teren, wypożyczenie przepustki, zrobienie zdjęcia, wydruk dokumentu, przekazanie paczki.

15.7. Rozmowy w miejscach publicznych w pobliżu jednostek i obiektów

Zasady z rozdziałów 2 i 7 obowiązują tu ze szczególną mocą. Lokale, sklepy, stacje paliw i przystanki przy jednostkach wojskowych i dużych obiektach infrastruktury są miejscami, w których bywają ich pracownicy, a więc także miejscami, w których łatwo podsłuchać rozmowę o tym, co dzieje się za ogrodzeniem. O sprawach służbowych wymagających ochrony rozmawiasz wyłącznie w dozwolonych miejscach i kanałach. W pociągach i autobusach wiozących żołnierzy na urlop lub z urlopu nie omawiasz, skąd jedziesz, dokąd wracasz i co się dzieje w pododdziale.

15.8. Dostawcy i podwykonawcy wojska i infrastruktury krytycznej

Firmy pracujące dla wojska i operatorów infrastruktury często są słabszym ogniwem niż sam zleceniodawca, bo mają mniej rygorystyczne procedury, a ich pracownicy bywają w wielu obiektach. Nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa wdrażająca dyrektywę NIS2 przenosi część wymagań bezpieczeństwa na łańcuch dostaw, więc podwykonawcy podmiotów kluczowych i ważnych muszą liczyć się z wymaganiami kontraktowymi (Rzeczpospolita).

Najczęstsze wycieki po stronie dostawców i sposoby ich ograniczenia:

Wyciek	Jak ograniczyć
Portfolio na stronie i w ofertach („zrealizowaliśmy instalację w jednostce X", zdjęcia z obiektu)	Uzgodnienie ze zleceniodawcą, co wolno publikować; ogólne opisy bez nazw obiektów i zdjęć z wnętrza
Ogłoszenia o pracę z nazwą obiektu, terminem i skalą	Ogólne opisy lokalizacji i projektu, szczegóły na rozmowie z kandydatem
Profile zawodowe pracowników z listą obiektów i systemów	Zasady dla pracowników dotyczące opisu doświadczenia
Samochody firmowe z logo parkujące przy obiektach	Świadomość, że obecność pojazdu jest informacją; unikanie zdjęć i publikacji z wyjazdów
Dokumentacja techniczna na prywatnych skrzynkach i w prywatnych chmurach	Zakaz przetwarzania dokumentacji poza systemami firmy; kontrola dostępu i jego odbieranie po zakończeniu projektu
Zdalny dostęp serwisowy do systemów klienta	Dostęp tylko na czas zlecenia, przez kanał kontrolowany przez klienta, z MFA i rejestracją sesji

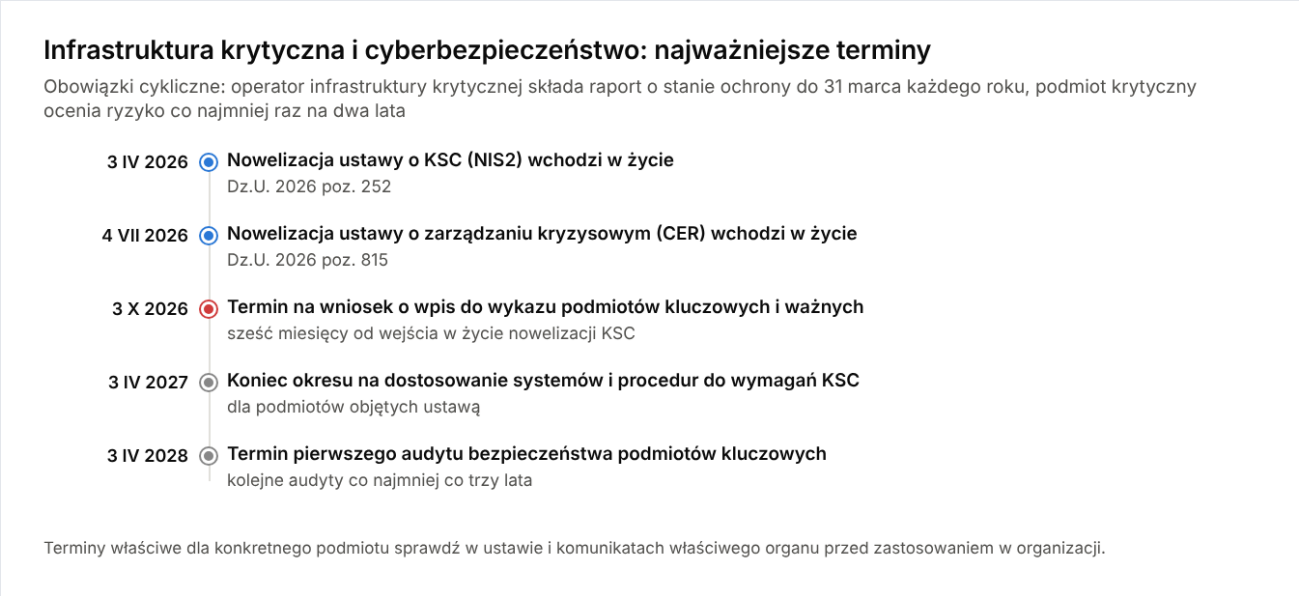
Wyciek	Jak ograniczyć
Wymiana plików z podwykonawcami niższego szczebla	Ograniczanie przekazywanych informacji do niezbędnych; umowy o poufności; weryfikacja podwykonawców

15.9. Infrastruktura krytyczna: ramy prawne i praktyka

W 2026 roku zmieniły się dwa podstawowe akty prawne dla tej grupy.

Nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa, wdrażająca dyrektywę NIS2 (ustawa z 23 stycznia 2026 r., Dz.U. 2026 poz. 252), obowiązuje od 3 kwietnia 2026 roku. Dzieli podmioty na kluczowe i ważne, wymaga od nich samoidentyfikacji i rejestracji, zarządzania ryzykiem, szkoleń pracowników oraz wieloetapowego zgłaszania poważnych incydentów, a kierownictwo ponosi odpowiedzialność za wdrożenie środków bezpieczeństwa (ifirma.pl, Clifford Chance). Podmioty objęte ustawą miały sześć miesięcy, do 3 października 2026 roku, na złożenie wniosku o wpis do właściwego wykazu, a na dostosowanie systemów, procedur i struktur mają czas do 3 kwietnia 2027 roku. Podmioty kluczowe przeprowadzają pierwszy audyt bezpieczeństwa do 3 kwietnia 2028 roku, a kolejne co najmniej co trzy lata (ITwiz). Przed zastosowaniem w organizacji sprawdź terminy i obowiązki właściwe dla twojego podmiotu.

Nowelizacja ustawy o zarządzaniu kryzysowym, wdrażająca dyrektywę CER o odporności podmiotów krytycznych (ustawa z 29 maja 2026 r., Dz.U. 2026 poz. 815), obowiązuje od 4 lipca 2026 roku. Wprowadza pojęcie usług kluczowych i podmiotów krytycznych obok operatorów infrastruktury krytycznej, obowiązki w zakresie środków technicznych, bezpieczeństwa i organizacyjnych, zgłaszania zdarzeń zakłócających oraz niejawną dokumentację ochrony infrastruktury krytycznej w miejsce dotychczasowych planów ochrony. Operatorzy infrastruktury krytycznej składają coroczne raporty o stanie ochrony do 31 marca, a podmioty krytyczne przeprowadzają ocenę ryzyka co najmniej raz na dwa lata. Ustawa pozwala też na niszczenie, unieruchamianie lub przejmowanie kontroli nad dronami i innymi bezzałogowymi obiektami stanowiącymi zagrożenie (Prawo.pl).



Rys. 29. Najważniejsze terminy nowelizacji ustaw o krajowym systemie cyberbezpieczeństwa i o zarządzaniu kryzysowym · źródła: ITwiz, Prawo.pl

Dla pracownika wynikają z tego proste wnioski: dokumentacja dotycząca ochrony i odporności obiektu jest coraz częściej niejawna, a zgłaszanie incydentów jest obowiązkiem organizacji, który zaczyna się od tego, że pracownik zgłosi zdarzenie wewnątrz.

Praktyka cyfrowa. ABW opisuje incydenty z 2025 roku, w których atakujący uzyskali dostęp do systemów sterowania stacji uzdatniania wody w Jabłonnie Lackiej, Szczytnie, Małdytach, Tolkmicku i Sierakowie, wykorzystując niewłaściwą politykę haseł i niezabezpieczone panele zarządzania dostępne bezpośrednio z internetu. Agencja wskazuje też ataki na łańcuchy dostaw, w których celem są dokumentacja projektowa i dane logowania kontrahentów. Wnioski:

- żaden panel sterowania (HMI, SCADA, sterowniki, routery) nie powinien być dostępny bezpośrednio z internetu,
- hasła domyślne zmienia się przy instalacji, a dostęp zdalny wymaga MFA,
- dostęp serwisowy dostawców jest czasowy i rejestrowany,
- dokumentacji technicznej nie wysyła się prywatną pocztą ani nie przechowuje w prywatnych chmurach,
- pracownicy nie publikują zrzutów ekranu z systemów, nawet „dla pochwalenia się" nowym wdrożeniem.

Praktyka fizyczna. Przypadek stacji Starlink pokazał, że atak może polegać na pokonaniu ogrodzenia i podpaleniu szafy elektrycznej, poprzedzonym rozpoznaniem z zewnątrz. Pracownicy obiektów powinni wiedzieć, jakie zachowania odnotować i komu je zgłosić (rozdział 4.9): fotografowanie zabezpieczeń, spacery wzdłuż ogrodzenia, pytania o godziny zmian, pozostawione przedmioty, ślady przy ogrodzeniu, drony nad obiektem. Drona nad obiektem zgłasza się ochronie i policji. Pracownik nie próbuje go samodzielnie neutralizować, bo mogą to robić wyłącznie formacje i osoby uprawnione na podstawie ustawy i procedur obiektu.

15.10. Rodzina

Rodzina osoby pracującej w wojsku lub infrastrukturze krytycznej nie powinna znać szczegółów pracy, ale powinna znać kilka zasad:

- nie publikujemy informacji o wyjazdach, ćwiczeniach, dyżurach i nieobecnościach, ani w trakcie, ani z wyprzedzeniem,
- nie publikujemy zdjęć w mundurze z oznaczeniami jednostki, z terenu obiektów ani ze sprzętem,
- nie odpowiadamy na pytania obcych osób o pracę bliskiego, także osób podających się za jego kolegów lub przełożonych; mówimy „przekażę, niech oddzwoni",
- informujemy bliskiego o każdym nietypowym zainteresowaniu nim lub rodziną,
- dzieci wiedzą, że o pracy rodzica nie opowiada się w internecie ani obcym.

15.11. Po zakończeniu służby lub pracy

Obowiązek ochrony informacji niejawnych i tajemnicy służbowej nie kończy się z dniem odejścia. Byli żołnierze i byli pracownicy infrastruktury krytycznej są dla obcych służb atrakcyjni, bo mają wiedzę, kontakty i często mniejszy nadzór niż w czasie służby. Oferty pracy, konsultacji czy „wspomnieniowych" wywiadów dotyczących dawnej jednostki lub obiektu wymagają tej samej ostrożności co w czasie służby. W razie wątpliwości warto skonsultować się z byłym pełnomocnikiem ochrony informacji lub właściwą służbą.

15.12. Gdzie zgłaszać

Sprawa	Do kogo
Sygnały działania obcych służb wobec żołnierzy, pracowników resortu obrony, jednostek wojskowych i podmiotów pracujących dla wojska	Pełnomocnik ds. ochrony informacji niejawnych lub przełożony zgodnie z procedurą jednostki; Służba Kontrwywiadu Wojskowego; aktualny kanał zgłoszeń sprawdź na oficjalnej stronie skw.gov.pl przed zgłoszeniem.
Sygnały działania obcych służb wobec infrastruktury krytycznej i podmiotów cywilnych, próby werbunku, rozpoznanie obiektów	ABW: dyżurny 22 585 82 21, chatbot @ABW_STOPdywersji_bot, delegatury
Incydenty cyberbezpieczeństwa w podmiotach objętych ustawą o KSC	Właściwy CSIRT (CSIRT GOV, CSIRT MON lub CSIRT NASK) zgodnie z ustawą i procedurą organizacji
Zdarzenia zakłócające świadczenie usług kluczowych	Zgodnie z ustawą o zarządzaniu kryzysowym i procedurą operatora lub podmiotu krytycznego, przez wyznaczonego pełnomocnika
Zagrożenie bezpośrednie, przestępstwo w toku, dron nad obiektem, podejrzany przedmiot	112 i ochrona obiektu

15.13. Scenariusz 10: „badanie rynku” dla technika z wodociągów

Sytuacja. Damian jest technikiem automatyki w spółce wodociągowej średniego miasta. Na portalu zawodowym pisze do niego przedstawicielka zagranicznej „firmy badawczej”. Proponuje 500 euro za 45-minutową rozmowę o tym, jakie systemy sterowania stosuje spółka, kto jest dostawcą, jak wygląda zdalny serwis i jak spółka przygotowuje się do nowych przepisów o cyberbezpieczeństwie. Prosi o przejście na prywatny komunikator i podkreśla, że to „rutynowe badanie branżowe, wszystkie odpowiedzi są anonimowe”.

Sygnały ostrzegawcze: wysokie wynagrodzenie za informacje o systemach i dostępie zdalnym, przeniesienie rozmowy do prywatnego kanału, zapewnienia o anonimowości, zainteresowanie konkretnym podmiotem infrastruktury krytycznej.

Możliwe wyjaśnienia: istnieją legalne platformy eksperckich konsultacji, ale prawdziwe badania nie wymagają ujawniania konfiguracji i dostępu zdalnego konkretnego operatora; firma może też zbierać dane dla konkurencji; może chodzić o rozpoznanie przed atakiem.

Zalecane działania: odmówić udziału, nie przekazywać żadnych informacji o systemach, zachować korespondencję, poinformować przełożonego i osobę odpowiedzialną za cyberbezpieczeństwo w spółce, która rozważy zgłoszenie do ABW i właściwego CSIRT, sprawdzić, czy podobne wiadomości nie trafiły do innych pracowników.

Błędy do uniknięcia: rozmowa „tylko ogólnie”, bo ogólnie też ujawnia dostawcę i model serwisu; przyjęcie pieniędzy; usunięcie korespondencji; uznanie, że skoro informacje są „w przetargu”, to można je potwierdzić.

Wnioski. ABW opisuje ataki na stacje uzdatniania wody i na łańcuchy dostaw, których celem jest budowa wiedzy o architekturze obiektów. Pytania o dostawcę, wersje systemów i sposób dostępu zdalnego są dokładnie tym, czego potrzebuje ktoś przygotowujący taki atak.

15.14. Lista kontrolna OPSEC dla wojska, przemysłu obronnego i infrastruktury krytycznej

- ☐ Znam informacje krytyczne w moim zespole i wiem, które z nich nie mogą wyjść poza krąg uprawnionych.
- ☐ Stosuję zasady jednostki lub organizacji dotyczące urządzeń w strefach ochronnych.
- ☐ Moje profile w aplikacjach sportowych są prywatne, nie rejestruję treningów na terenie i wokół obiektów.
- ☐ Historia lokalizacji jest wyłączona, zdjęcia publikuję bez lokalizacji, po fakcie i po sprawdzeniu tła.
- ☐ Nie publikuję zdjęć z jednostki, obiektu, ćwiczeń, ze sprzętem, ekranami i tablicami w tle.
- ☐ Mój profil zawodowy nie wymienia obiektów, systemów i szczegółów projektów.
- ☐ Grupy w prywatnych komunikatorach służą tylko sprawom niewrażliwym.
- ☐ Nie rozmawiam o pracy w lokalach, sklepach i środkach transportu w pobliżu jednostek i obiektów.
- ☐ Oferty płatnych konsultacji i „badań rynku" dotyczących mojej pracy weryfikuję i zgłaszam.
- ☐ Nie robię „drobnych przysług" związanych z dostępem, przepustkami, zdjęciami i paczkami.
- ☐ Podróże do państw o podwyższonym ryzyku i nietypowe kontakty zgłaszam zgodnie z procedurą.
- ☐ Jeśli mam problemy finansowe lub inne, które mogą być wykorzystane do nacisku, szukam pomocy wcześnie.
- ☐ Rodzina zna zasady publikowania i odpowiadania na pytania obcych.
- ☐ W infrastrukturze krytycznej: żaden panel sterowania nie jest dostępny z internetu, hasła domyślne są zmienione, dostęp zdalny ma MFA.
- ☐ Dokumentacji technicznej nie przetwarzam poza systemami organizacji.
- ☐ Dostęp serwisowy dostawców jest czasowy i rejestrowany.
- ☐ Wiem, jakie zachowania przy ogrodzeniu i obiekcie odnotować i komu je zgłosić, w tym drony.
- ☐ Znam właściwe kanały zgłoszeń: pełnomocnik, SKW lub ABW, właściwy CSIRT, 112.
- ☐ Po zakończeniu służby lub pracy nadal chronię informacje, które poznałem.

15.15. Karta informacyjna do przekazania pracownikom i żołnierzom

Poniższą kartę można wydrukować na jednej stronie, rozdać na odprawie lub szkoleniu wstępnym albo wysłać nowym pracownikom i podwykonawcom. Jest napisana tak, żeby była zrozumiała bez lektury reszty przewodnika.

Dlaczego to dotyczy ciebie. Według ABW rosyjskie służby prowadzą w Polsce rozpoznanie obiektów wojskowych i infrastruktury krytycznej na masową skalę, a do prostych zadań werbują przypadkowe osoby przez komunikatory, płacąc w kryptowalutach. W 2025 roku ABW wszczęła 48 śledztw w sprawie szpiegostwa, najwięcej od początku lat dziewięćdziesiątych. Informacje mogą wyciekać także przez zdjęcia, aplikacje, rozmowy i publikacje członków rodziny.

Co robisz zawsze:

- stosujesz zasady swojej jednostki lub firmy dotyczące telefonów, zegarków i aparatów w strefach ochronnych,
- trzymasz profile w aplikacjach sportowych jako prywatne i nie rejestrujesz treningów na terenie obiektów i wokół nich,

- publikujesz zdjęcia dopiero po fakcie i po sprawdzeniu, bez lokalizacji, sprzętu, ekranów, tablic i oznaczeń w tle; publikacja po czasie nie jest zgodą na ujawnienie informacji,
- o sprawach służbowych wymagających ochrony rozmawiasz wyłącznie w dozwolonych miejscach i kanałach, nie w sklepie, barze, pociągu czy na przystanku,
- dokumentację i dane techniczne przetwarzasz wyłącznie w systemach organizacji,
- zmieniasz hasła domyślne, używasz MFA, nie zostawiasz paneli i dostępu zdalnego otwartych do internetu.

Czego nie robisz nigdy:

- nie wykonujesz „drobnych przysług" związanych z dostępem: przepustka, wpuszczenie kogoś, zdjęcie, wydruk, paczka,
- nie przyjmujesz płatnych „konsultacji", „badań rynku" ani zleceń od nieznanych podmiotów dotyczących twojej pracy,
- nie odpowiadasz na oferty łatwego zarobku za zdjęcia obiektów, przejazdy trasą czy dostarczanie paczek,
- nie konfrontujesz się z osobą, która fotografuje obiekt lub kręci się przy ogrodzeniu.

Na co zwracasz uwagę:

- ktoś fotografuje zabezpieczenia, kamery, bramy, szafy zasilające albo chodzi wzdłuż ogrodzenia bez celu,
- ktoś wypytuje ciebie lub rodzinę o harmonogramy, wyjazdy, liczbę osób, dostępy,
- nowa znajomość szybko kieruje rozmowę na twoją pracę,
- dostajesz wiadomość z ofertą pracy lub zlecenia, która przechodzi do prywatnego komunikatora,
- drony nad obiektem, ślady przy ogrodzeniu, pozostawione przedmioty.

Gdzie zgłaszasz:

Sytuacja	Kontakt
Zagrożenie bezpośrednie, przestępstwo w toku, dron nad obiektem, podejrzany przedmiot	112 i ochrona obiektu
Sprawy związane z wojskiem i resortem obrony	Pełnomocnik ds. ochrony informacji niejawnych, przełożony, Służba Kontrwywiadu Wojskowego
Próba werbunku, rozpoznanie infrastruktury, sygnały działania obcych służb	ABW: 22 585 82 21, Telegram @ABW_STOPdywersji_bot
Incydent w systemach IT lub automatyki	Dział IT lub bezpieczeństwa, właściwy CSIRT
Podejrzane SMS-y i strony	CERT Polska: SMS na 8080, incydent.cert.pl

> Pamiętaj. Zgłoszenie nie wymaga pewności i nikogo nie oskarża. Jeśli coś już zrobiłeś, na przykład wykonałeś zdjęcie na zlecenie nieznanej osoby, zgłoś to od razu: prawo w określonych przypadkach przewiduje niepodleganie karze, ale tylko po spełnieniu wszystkich ustawowych warunków, w tym dobrowolnego zaprzestania działalności i ujawnienia organom ścigania wszystkich istotnych okoliczności. Samo zgłoszenie nie daje gwarancji, dlatego od razu porozmawiaj z prawnikiem. Obowiązek ochrony informacji nie kończy się z dniem odejścia ze służby lub z pracy.

Aneksy

Aneksy zawierają materiał referencyjny: przepisy, na które powołuje się przewodnik, kontakty do instytucji, wzór notatki z incydentu, wykaz źródeł, program szkolenia i pytania kontrolne. Dokument zaktualizowano 24 października 2026 roku. Źródła poszczególnych informacji podano w tekście i w aneksie D, a poziom pewności zdarzeń w tabelach. Informacje zmienne w czasie, w tym przepisy, terminy i kontakty, sprawdź przed szkoleniem, podróżą lub zastosowaniem w organizacji.

Aneks A. Podstawy prawne

Zestawienie nie jest wykładnią prawa. W sprawach indywidualnych skonsultuj się z prawnikiem.

Akt i przepis	Czego dotyczy	Znaczenie dla czytelnika	Źródło
Kodeks karny, art. 130 (w brzmieniu nadanym nowelizacją z 17 sierpnia 2023 r.)	Szpiegostwo: udział w działalności obcego wywiadu lub działanie na jego rzecz, udzielanie wiadomości, zgłaszanie gotowości, gromadzenie informacji, dywersja, sabotaż i dezinformacja na rzecz obcego wywiadu	Kary od 6 miesięcy pozbawienia wolności do dożywocia, zależnie od typu czynu, np. udział w działalności obcego wywiadu przeciwko RP: co najmniej 5 lat; dywersja lub sabotaż na jego rzecz: co najmniej 10 lat albo dożywocie. Karalne jest także samo zgłoszenie gotowości działania na rzecz obcego wywiadu i gromadzenie dla niego informacji (od 6 miesięcy do 8 lat).	arslege.pl, rp.pl, e-prawnik.pl
Kodeks karny, art. 131	Niepodleganie karze w razie dobrowolnego ujawnienia	§ 2: przy m.in. zgłoszeniu gotowości działania na rzecz obcego wywiadu lub gromadzeniu dla niego informacji (art. 130 § 3) sprawca nie podlega karze, jeżeli dobrowolnie poniechał dalszej działalności, podjął istotne starania zmierzające do zapobieżenia popełnieniu zamierzonego czynu i ujawnił organowi ścigania wszystkie istotne okoliczności. § 1: przy usiłowaniu cięższych postaci (m.in. art. 130 § 1, 2, 5, 7 i 9) wymagane jest dobrowolne poniechanie dalszej działalności i ujawnienie wszystkich istotnych okoliczności. Zgłoszenie nie jest automatyczną gwarancją; sprawa wymaga indywidualnej oceny prawnej (Dz.U. 2023 poz. 1834).	Tekst ujednolicony Kodeksu karnego

Akt i przepis	Czego dotyczy	Znaczenie dla czytelnika	Źródło
Kodeks karny, art. 190a	Uporczywe nękanie	Podstawa zgłoszenia na policję, gdy ta sama osoba uporczywie pojawia się w twoim życiu wbrew twojej woli.	Tekst ujednolicony Kodeksu karnego
Kodeks karny, art. 25	Obrona konieczna	Prawo do odparcia bezpośredniego, bezprawnego zamachu. W przewodniku traktowane jako ostateczność.	Tekst ujednolicony Kodeksu karnego
Kodeks postępowania karnego, art. 243	Ujęcie osoby na gorącym uczynku przestępstwa lub w pościgu podjętym bezpośrednio po nim	Uprawnienie przysługujące każdemu, gdy zachodzi obawa ukrycia się tej osoby albo nie można ustalić jej tożsamości; osobę ujętą trzeba niezwłocznie oddać Policji. Ze względu na ryzyko fizyczne i prawne nie rekomendowane w praktyce bezpieczeństwa osobistego.	Tekst ujednolicony k.p.k.
Ustawa o obronie Ojczyzny, art. 616a i 683a (po zmianie ustawą z 25 czerwca 2025 r., od 12 sierpnia 2025 r.)	Zakaz fotografowania, filmowania i przesyłania obrazu obiektów	Zakaz określony w art. 616a ustawy o obronie Ojczyzny dotyczy oznaczonych obiektów zajmowanych przez jednostki wojskowe lub służby specjalne oraz wskazanych w przepisie ruchomości i wizerunków osób, z ustawowymi wyjątkami. Naruszenie może stanowić wykroczenie zagrożone karą grzywny, a w określonych przypadkach możliwy jest przepadek sprzętu. Wyjątki obejmują m.in. obraz będący szczegółem krajobrazu, zgromadzenie lub nagranie z przejeżdżającego samochodu.	prawo.pl
Ustawa z 10 czerwca 2016 r. o działaniach antyterrorystycznych, art. 15–16	Stopnie alarmowe ALFA, BRAVO, CHARLIE, DELTA i ich odpowiedniki CRP	Wprowadzane zarządzeniem Prezesa Rady Ministrów, a w sprawach niecierpiących zwłoki przez ministra spraw wewnętrznych. Warunki wprowadzenia poszczególnych stopni określa art. 15. Aktualne stopnie, ich zakres terytorialny i okres obowiązywania sprawdzasz w zarządzeniach Prezesa Rady Ministrów i komunikatach RCB. Stan opisany w części głównej dokumentu dotyczy 24 października 2026 r.	gov.pl, Forsal
Ustawa z 5 sierpnia 2010 r. o ochronie informacji niejawnych	Ochrona informacji niejawnych	Informacje niejawne nie mogą być przedmiotem rozmów w lokalach publicznych. Postępowanie przy utracie lub ujawnieniu wyłącznie według procedury pełnomocnika ochrony.	Tekst ujednolicony ustawy

Akt i przepis	Czego dotyczy	Znaczenie dla czytelnika	Źródło
RODO, art. 32 i 33	Bezpieczeństwo przetwarzania danych osobowych; zgłaszanie naruszeń	Obowiązek stosowania odpowiednich środków ochrony. Administrator zgłasza naruszenie Prezesowi UODO bez zbędnej zwłoki, w miarę możliwości w ciągu 72 godzin od jego stwierdzenia, chyba że ryzyko dla praw lub wolności osób jest mało prawdopodobne. Pracownik zgłasza zdarzenie wewnętrznie od razu.	Rozporządzenie (UE) 2016/679
Ustawa o prawie autorskim i prawach pokrewnych, art. 81	Ochrona wizerunku	Rozpowszechnianie wizerunku osoby co do zasady wymaga jej zezwolenia. Nie publikuj zdjęć osób, które wydały ci się podejrzane.	Tekst ujednolicony ustawy
Przepisy o zastrzeganiu numeru PESEL (od 17 listopada 2023 r.; obowiązek weryfikacji przez instytucje od 1 czerwca 2024 r.)	Zastrzeżenie numeru PESEL	Bezpłatne zastrzeżenie i cofnięcie w mObywatelu lub urzędzie gminy; ochrona przed zaciągnięciem zobowiązań na twoje dane.	informacja za Ministerstwem Cyfryzacji
Ustawa z 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej (w mocy od 25 września 2023 r.)	Smishing, podszywanie się pod numery i nadawców, lista ostrzeżeń przed niebezpiecznymi domenami	Operatorzy blokują SMS-y wyłudzające dane oraz blokują połączenia z podrobionym numerem albo ukrywają taki numer. Za nadużycia w komunikacji elektronicznej grozi kara pozbawienia wolności. Podejrzane SMS-y przekazujesz na numer 8080.	e-prawnik.pl

Przepisy szczególnie istotne dla rozdziału 15:

Akt i przepis	Czego dotyczy	Znaczenie dla czytelnika	Źródło
Decyzja nr 77/MON Ministra Obrony Narodowej z 9 czerwca 2020 r.	Zasady używania urządzeń do przetwarzania obrazu i dźwięku w resorcie obrony	Możliwość wnoszenia i używania urządzeń prywatnych i służbowych zależy od klasy strefy ochronnej; szczegóły w rozkazach jednostki.	Defence24
Ustawa o krajowym systemie cyberbezpieczeństwa (po nowelizacji ustawą z 23 stycznia 2026 r., Dz.U. 2026 poz. 252, wdrażającej NIS2, obowiązującej od 3 kwietnia 2026 r.)	Podmioty kluczowe i ważne, zarządzanie ryzykiem, zgłaszanie incydentów, łańcuch dostaw	Obowiązki organizacji i odpowiedzialność kierownictwa; wymagania przenoszone na podwykonawców. Przed zastosowaniem sprawdź terminy i obowiązki właściwe dla konkretnego podmiotu.	ifirma.pl, Clifford Chance
Ustawa o zarządzaniu kryzysowym (po nowelizacji ustawą z 29 maja 2026 r., Dz.U. 2026 poz. 815, wdrażającej dyrektywę CER, obowiązującej od 4 lipca 2026 r.)	Operatorzy infrastruktury krytycznej, podmioty krytyczne, usługi kluczowe	Środki odporności, zgłaszanie zdarzeń zakłócających, niejawna dokumentacja ochrony IK zamiast planów ochrony.	Prawo.pl

Akt i przepis	Czego dotyczy	Znaczenie dla czytelnika	Źródło
Ustawa o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego	Właściwość SKW	SKW odpowiada za ochronę kontrwywiadowczą Sił Zbrojnych i resortu obrony; sprawy związane z wojskiem zgłasza się tam lub przez pełnomocnika ochrony.	Tekst ujednolicony ustawy

Aneks B. Kontakty i formy pomocy

Instytucja	Kiedy	Kontakt
Numer alarmowy	Bezpośrednie zagrożenie życia, zdrowia, mienia; pożar; wypadek; przestępstwo w toku	112
Agencja Bezpieczeństwa Wewnętrznego, dyżurny oficer operacyjny	Próby werbunku, sygnały działania obcych służb, rozpoznanie infrastruktury krytycznej, dywersja	tel. 22 585 82 21; ul. Rakowiecka 2A, 00-993 Warszawa; poczta@abw.gov.pl (BIP ABW, dane teleadresowe)
ABW, chatbot w Telegramie	Anonimowe zgłoszenie próby werbunku lub dywersji, w językach polskim, angielskim, ukraińskim i rosyjskim	@ABW_STOPdywersji_bot
Delegatury ABW	Zgłoszenia regionalne	Lista i numery dyżurnych na stronie abw.gov.pl, np. Katowice tel. 32 200 51 21, Białystok tel. 85 654 48 06, Gdańsk tel. 58 301 34 30, Bydgoszcz tel. 52 375 61 09
Policja (komisariat)	Uporczywe nękanie, kradzież, zgubienie urządzenia, zgłoszenia niewymagające natychmiastowej interwencji	Najbliższa jednostka Policji lub jej numer kontaktowy z oficjalnej strony. Przy nagłym zagrożeniu albo zdarzeniu wymagającym pilnej interwencji dzwonisz pod 112.
CERT Polska (CSIRT NASK)	Podejrzane SMS-y, e-maile, strony, incydenty bezpieczeństwa komputerowego	SMS: przekaż na 8080; formularz: incydent.cert.pl; e-mail: cert@cert.pl (Telepolis)
mObywatel	Zastrzeżenie numeru PESEL, zgłoszenie utraty dowodu osobistego	Aplikacja mObywatel, serwis mobywatel.gov.pl lub dowolny urząd gminy
Rządowe Centrum Bezpieczeństwa	Aktualne stopnie alarmowe, ostrzeżenia, alerty	gov.pl/rcb
Ministerstwo Spraw Zagranicznych	Ostrzeżenia dla podróżnych, rejestracja podróży w systemie Odyseusz	Strona „Informacje dla podróżujących” na gov.pl/web/dyplomacja; system Odyseusz (odyseusz.gov.pl, od 2026 roku także w aplikacji mObywatel)
Prezes Urzędu Ochrony Danych Osobowych	Zgłaszanie naruszeń ochrony danych przez administratora	uodo.gov.pl

Instytucja	Kiedy	Kontakt
Dział bezpieczeństwa organizacji, pełnomocnik ds. ochrony informacji niejawnych, inspektor ochrony danych	Wszystkie sprawy związane z pracą	Zgodnie z procedurą organizacji (wpisz tutaj): _____
Zaufana osoba	Plan podróży, godziny kontrolne, umówiony sygnał	Imię i telefon (wpisz tutaj): _____

Kontakty dla spraw związanych z Ukrainą (rozdział 14):

Instytucja	Kiedy	Kontakt
Służba Bezpieczeństwa Ukrainy (SBU)	Próby werbunku, nacisku lub szantażu dotyczące działań w Ukrainie, także wobec pracowników i ich rodzin	Bezpłatna infolinia 1516; chatbot w Telegramie t.me/spaly_fsb_bot (Interfax-Ukraina)
MSZ, system Odyseusz	Rejestracja podróży do Ukrainy, aktualne ostrzeżenia i kontakty do placówek RP	odyseusz.gov.pl
Ambasada RP w Kijowie i konsulaty RP w Ukrainie	Pomoc konsularna	Numery dyżurne sprawdź przed wyjazdem w serwisie Odyseusz i na oficjalnych stronach placówek.

Aneks C. Wzór notatki z incydentu

Notatkę sporządza się możliwie szybko po odzyskaniu bezpieczeństwa, najlepiej tego samego dnia. Fakty zapisuj w lewej części, oceny i przypuszczenia oddzielnie, z poziomem pewności. Nie uzupełniaj luk domysłami: napisz „nie pamiętam" lub „nie widziałem".

Pole	Treść
Data i godzina sporządzenia notatki	
Data, godzina i czas trwania zdarzenia	
Miejsce (adres, lokal, piętro, punkty charakterystyczne)	
Co robiłem i z kim byłem	
Co zauważyłem (opisowo, w kolejności)	
Opis osoby lub osób: cechy trwałe (wzrost, budowa, twarz, sposób poruszania się, znaki szczególne)	
Opis osoby lub osób: ubiór i przedmioty	
Pojazd (rodzaj, kolor, marka, numer, jeśli widoczny)	
Słowa wypowiedziane przez osobę (możliwie dosłownie)	
Czy to pierwsza obserwacja, czy powtórzenie (daty i miejsca wcześniejszych)	
Świadkowie (kto, kontakt, jeśli znany)	

Pole	Treść
Co zrobiłem w reakcji i o której	
Kogo poinformowałem (osoba, instytucja, numer sprawy)	
Załączniki (zrzuty ekranu, zdjęcia, potwierdzenia)	
Moja ocena i jej poziom pewności (ustalone / prawdopodobne / możliwe)	
Zwyczajne wyjaśnienia, które rozważyłem	
Co proponuję zmienić	

Notatkę przechowuj w zatwierdzonym repozytorium z dostępem ograniczonym do uprawnionych osób, nie w ogólnodostępnych folderach ani prywatnych chmurach, i przekaż ją tylko osobom lub instytucjom, którym zgłaszasz sprawę.

Karta dla osoby przyjmującej zgłoszenie

Przełożony, dyżurny lub pracownik działu bezpieczeństwa, który przyjmuje zgłoszenie, postępuje w tej kolejności:

1. Ustal, czy ktoś potrzebuje natychmiastowej pomocy; jeśli tak, najpierw 112.
2. Zapisz fakty, czas zgłoszenia i dane zgłaszającego.
3. Nie przesądzaj winy ani motywacji, ani wobec zgłaszającego, ani wobec osób, których zgłoszenie dotyczy.
4. Zabezpiecz materiały (zrzuty ekranu, wiadomości, notatki) zgodnie z procedurą organizacji i niczego nie usuwaj.
5. Przekaż sprawę właściwej osobie lub instytucji (rozdział 4.6).
6. Powiedz zgłaszającemu, co ma zrobić dalej i do kogo się zwracać.
7. Nie obiecuj całkowitej poufności ani określonego wyniku postępowania.

Aneks D. Źródła

Źródła otwierano i sprawdzano podczas przygotowania dokumentu, ostatnio 24 października 2026 roku. Sprawdzenie źródła oznacza, że przytoczona informacja się w nim znajduje, a nie że sprawa jest rozstrzygnięta. Informacje dotyczące śledztw w toku mogą się zmieniać wraz z kolejnymi ustaleniami.

Raporty i analizy:

- Agencja Bezpieczeństwa Wewnętrznego, Agencja Bezpieczeństwa Wewnętrznego 2024–2025. Wybrane aktywności, Warszawa 2026 (publikacja maj 2026).
- J. Lanchès, K. Rękawek, More of the Same. Russia's Crime-Terror Nexus: Criminality as a Tool of Hybrid Warfare Revisited, ICCT, 23 lutego 2026.
- Radio Prague International o pierwszym raporcie GLOBSEC i ICCT (110 incydentów od 2022 roku).
- P. Buchalik, Rosyjscy jednorazowi agenci – wyzwanie w świetle raportu ABW, Instytut Nowej Europy, 29 lipca 2026 (w tym dane z białej księgi PISM z 29 maja 2026).

Incydenty:

- AP o sabotażu na linii Warszawa–Lublin, 18 listopada 2025.

- Ukraińska Prawda o naruszeniu przestrzeni powietrznej 9–10 września 2025.
- Notes from Poland o ustaleniach w sprawie pożaru Marywilska 44, 12 maja 2025.
- Notes from Poland o zatrzymaniu obywatela Rosji przygotowującego zabójstwo w Warszawie, 13 sierpnia 2026.
- LIGA.net za Die Zeit o dronie z ładunkiem na lotnisku Lipsk/Halle, sierpień 2026.
- TVP Info o zatrzymaniach w sprawie podpalenia stacji Starlink, październik 2026.
- TVP Info o zatrzymaniu w Niemczech kobiety, trzeciej podejrzanej, październik 2026.
- Kyiv Post o ocenie duńskiej służby PET.

Werbunek i zgłaszanie:

- Notes from Poland o uruchomieniu chatbota ABW, 18 grudnia 2025.
- Spider's Web o SMS-ach z ofertą pracy zdalnej, wrzesień 2026.
- ABW, kontakt i delegatury.
- Telepolis o numerze 8080 CERT Polska.

Prawo i stopnie alarmowe:

- Prawo.pl o nowych zasadach zakazu fotografowania, 12 sierpnia 2025.
- Rzeczpospolita o nowelizacji przepisów o szpiegostwie.
- e-prawnik.pl o zmianach w Kodeksie karnym.
- Tekst art. 130 Kodeksu karnego (arslege.pl).
- Gov.pl o przedłużeniu stopni alarmowych do 31 maja 2026.
- Forsal o przedłużeniu stopni alarmowych do 31 sierpnia 2026.
- Informacja o zastrzeganiu numeru PESEL.

Biznes z Ukrainą i w Ukrainie (rozdział 14):

- Kyiv Post za Reuters o atakach sabotażowych na duńskie firmy zbrojeniowe (ocena PET), 8 października 2026.
- MSZ, serwis Odyseusz, informacje o Ukrainie (poziom 4).
- SUD.UA o przedłużeniu stanu wojennego do 31 października 2026, 24 lipca 2026.
- Interfax-Ukraina o 75 wyrokach za publikowanie materiałów o obronie przeciwlotniczej.
- Interfax-Ukraina o kampanii SBU przeciw werbunkowi i liczbie incydentów w 2026.
- Euromaidan Press o werbunku z podszywaniem się pod SBU.
- The Hacker News, przegląd komunikatów CERT-UA.
- SOC Prime o kampanii APT28 wykorzystującej lukę w Office (za CERT-UA).

OPSEC w wojsku i infrastrukturze krytycznej (rozdział 15):

- Defence24 o decyzji nr 77/MON w sprawie używania smartfonów.
- Sejm, interpelacja nr 8712 o udostępnianiu danych lokalizacyjnych przez żołnierzy, 17 marca 2025.
- TVP Info o danych z aplikacji Strava z baz USA na Bliskim Wschodzie.
- Eska o zatrzymaniu przez ABW trzech obywateli Polski w maju 2026.
- Rzeczpospolita o skutkach NIS2 dla łańcucha dostaw.
- ifirma.pl o obowiązkach z nowelizacji KSC.
- Clifford Chance o nowelizacji ustawy o KSC, marzec 2026.

- Prawo.pl o nowelizacji ustawy o zarządzaniu kryzysowym.

Weryfikacja faktów (23 października 2026):

- RCB na samorzad.gov.pl o stopniach alarmowych od 1 września do 30 listopada 2026.
- Ustawa z 17 sierpnia 2023 r. o zmianie ustawy Kodeks karny, Dz.U. 2023 poz. 1834 (art. 130 i 131).
- Reuters przez MarketScreener o liście zakładów opublikowanej przez rosyjskie MO 15 kwietnia 2026.
- Meduza o liście rosyjskiego MO i wypowiedzi Miedwiediewa.
- Interia Motoryzacja o zasadach kontroli przez nieumundurowanych policjantów.
- Interia Motoryzacja o żółtych naklejkach PLK.
- Informacja urzędowa o zastrzeganiu PESEL z urzędu przy unieważnieniu dowodu.
- UkraNews o przedłużeniu stanu wojennego w Ukrainie do 31 października 2026.

Sprawdzenie uzupełniające po recenzji (23 października 2026):

- standardyprawa.pl, art. 131 Kodeksu karnego i prawnik.cc, art. 131 k.k.: przesłanki niepodlegania karze w § 1 i § 2.
- RCB, przedłużenie stopni alarmowych do 30 listopada 2026 r., komunikat z 26 sierpnia 2026 r. (zarządzenia nr 47–50).
- CERT Polska o publicznych sieciach Wi-Fi, 13 grudnia 2025 r.
- ICCT, More of the Same… Revisited, 23 lutego 2026 r.: 151 incydentów, 172 sprawców, Polska 31, zastrzeżenie o niepełności danych.
- UODO, Sztuczna inteligencja.
- Metryka ustawy z 23 stycznia 2026 r. o zmianie ustawy o krajowym systemie cyberbezpieczeństwa, Dz.U. 2026 poz. 252.
- Metryka ustawy z 29 maja 2026 r. o zmianie ustawy o zarządzaniu kryzysowym, Dz.U. 2026 poz. 815.
- InfoSecurity24 o ochronie infrastruktury krytycznej przed dronami, 28 lipca 2026 r., i Świat Dronów o nowelizacji, 26 czerwca 2026 r.

Akty prawne w Internetowym Systemie Aktów Prawnych (dostęp: 24 października 2026 r.):

- Ustawa z 6 czerwca 1997 r. Kodeks karny, art. 178b.
- Ustawa z 11 marca 2022 r. o obronie Ojczyzny, art. 616a.
- Ustawa z 10 czerwca 2016 r. o działaniach antyterrorystycznych, tekst pierwotny, art. 15–16.

Weryfikacja w wersji z 24 października 2026 r.:

- BIP ABW, dane teleadresowe: numer dyżurnego oficera operacyjnego, adres i e-mail centrali.
- InfoSecurity24 o ustaleniach ABW w sprawie stacji Starlink, RMF24 o zatrzymaniu trzeciej osoby i OKO.press o rozpoznaniu przed atakiem, październik 2026.
- Eska o zarzutach dla trzeciej osoby w sprawie sabotażu na kolei, listopad 2025.
- Reuters o polsko-rumuńskiej operacji przeciw paczkom z ładunkami, 21 października 2025.
- Espreso o zamknięciu konsulatu w Poznaniu, Polskie Radio o opuszczeniu konsulatu w Krakowie i Prawo.pl o zamknięciu konsulatu w Gdańsku.
- Super Express o liczbie sklepów w centrum Marywilska 44.
- ITwiz o terminach wdrożenia nowelizacji ustawy o KSC.
- e-prawnik.pl o ustawie o zwalczaniu nadużyć w komunikacji elektronicznej i Rzeczpospolita o obowiązku blokowania SMS-ów.

- CNN o oszustwie z użyciem deepfake w firmie Arup, 16 maja 2024.
- Lege Artis o systemie Odyseusz w aplikacji mObywatel, lipiec 2026.
- Dla Pilota o mapie DroneMap PAŻP.
- Warta o czterech poziomach ostrzeżeń MSZ i CUK o ostrzeżeniu MSZ dla Ukrainy, aktualizacja z maja 2026; MSZ, Informacje dla podróżujących.
- Spider's Web o żółtych naklejkach PLK, wrzesień 2026.
- The Defense Post o analizie Sky News dotyczącej aplikacji Strava, 18 sierpnia 2026.
- Instytut Nowej Europy o białej księdze PISM: tytuł i zakres białej księgi.
- prawnik.cc, art. 131 k.k. i arslege.pl, art. 130 k.k.: paragrafy i wysokość kar.

Aneks E. Program trzygodzinnego szkolenia

Program jest propozycją dla prowadzącego szkolenie stacjonarne dla grupy do 20 osób. Czasy można skracać, ale nie pomijaj ćwiczenia na scenariuszach, bo dopiero ono pokazuje, czy uczestnicy stosują procedurę z rozdziału 6.

Czas	Moduł	Materiał	Cel
0:00–0:20	Kontekst zagrożeń	Rozdział o kontekście, wykresy i oś czasu zdarzeń	Uczestnicy znają skalę zjawiska i odróżniają fakty od ocen.
0:20–0:45	Świadomość sytuacyjna i ocena ryzyka	Rozdział 1, siatka ryzyka	Uczestnicy przypisują spotkanie do poziomu ryzyka.
0:45–1:10	Miejsce spotkania i ochrona rozmowy	Rozdziały 2, 3 i 7, szkic sali, trzy warunki bezpiecznej rozmowy	Uczestnicy wybierają lokal i stolik oraz ograniczają szczegóły.
1:10–1:20	Przerwa		
1:20–1:45	Niepożądana uwaga i procedura w siedmiu krokach	Rozdziały 4 i 6, siła sygnału, schemat procedury	Uczestnicy oceniają sygnał i wybierają adresata zgłoszenia.
1:45–2:05	Bezpieczeństwo cyfrowe i podszywanie się	Rozdział 8, w tym podrozdział 8.15	Uczestnicy ustawiają powiadomienia i MFA oraz weryfikują prośby innym kanałem.
2:05–2:45	Ćwiczenie stołowe	Scenariusze 3, 7 i 8 z rozdziału 12 albo scenariusz 9 lub 10; podrozdział 6.9	Zespoły przechodzą procedurę i sporządzają notatkę.
2:45–3:00	Zamknięcie i pytania kontrolne	Aneks F, karta kieszonkowa z podrozdziału 13.8	Uczestnicy znają kanały zgłoszeń i wiedzą, gdzie szukać list kontrolnych.

Dla grup z wojska, przemysłu obronnego i infrastruktury krytycznej moduł o bezpieczeństwie cyfrowym można zastąpić rozdziałem 15 i kartą informacyjną z podrozdziału 15.15, a dla firm pracujących z Ukrainą rozdziałem 14.

Aneks F. Pytania kontrolne z odpowiedziami

Pytania służą do sprawdzenia, czy uczestnicy zapamiętali najważniejsze zasady. W nawiasie podano podrozdział, w którym jest uzasadnienie odpowiedzi.

Nr	Pytanie	Odpowiedź
1	Co robisz najpierw, gdy coś cię niepokoi?	Oceniasz, czy zagrożenie jest bezpośrednie. Jeśli tak, oddalasz się w stronę ludzi i dzwonisz pod 112, a wyjaśnienia rozważasz później (6.2).
2	Czy jedno spotkanie tej samej osoby w dwóch miejscach dowodzi obserwacji?	Nie. Pojedyncze zdarzenie zwykle nie pozwala ustalić intencji; wagę sygnału podnosi powtarzalność w niezwiązanych miejscach (4.2, 4.3).
3	Czy usunięcie nazwisk i dat wystarcza, żeby omawiać sprawę poufną w kawiarni?	Nie. Samo „co" i „dlaczego" może zdradzić produkt albo słabość zabezpieczeń; w lokalu omawiasz tylko informacje dopuszczone do ujawnienia (7.1).
4	Gdzie siadasz z laptopem w lokalu?	Plecami do ściany, z ekranem zwróconym do ściany, z dala od przejść, okien i kamer. Filtr prywatności nie chroni przed osobą za plecami (2.4, 7.5).
5	Dostajesz ofertę 200 zł za zdjęcia dworca z lokalizacją, płatne w kryptowalucie. Co robisz?	Nie wykonujesz zadania, nie kasujesz korespondencji, robisz zrzuty ekranu i zgłaszasz sprawę do ABW (22 585 82 21, @ABW_STOPdywersji_bot) lub na policję (4.9).
6	Czy zgłoszenie się po wykonaniu zadania gwarantuje niepodleganie karze?	Nie. Art. 131 k.k. wymaga spełnienia wszystkich ustawowych warunków; od razu skonsultuj się z adwokatem lub radcą prawnym (4.9).
7	Ktoś fotografuje szafy zasilające i kamery przy terminalu, a na widok ochrony odchodzi. Co robisz?	Nie podchodzisz. Zapamiętujesz czas, miejsce i opis, informujesz ochronę, a gdy zdarzenie trwa, dzwonisz pod 112; przy powtórzeniach zgłoszenie trafia też do ABW (4.9, 12.8).
8	Telefon zginął w pociągu. Jakie są pierwsze dwa kroki?	Zdalna blokada z zaufanego urządzenia i powiadomienie IT, a bez zbędnej zwłoki zakończenie sesji i zmiana haseł (8.9).
9	Dzwoni „bank", na ekranie widać jego prawdziwy numer, a rozmówca prosi o kod. Co robisz?	Nie podajesz kodu, rozłączasz się i oddzwaniasz na numer z karty lub z oficjalnej strony; numer na ekranie można podrobić (8.15).
10	Partner z Ukrainy prosi o pilny przelew na nowy rachunek. Jak to sprawdzasz?	Wstrzymujesz płatność, oddzwaniasz na numer znany wcześniej, potwierdzasz u drugiej osoby po stronie partnera, a decyzję zatwierdzają dwie osoby (14.4).
11	Co powinna zawierać notatka z incydentu?	Fakty oddzielone od ocen, cechy trwałe przed ubiorem, czas, miejsce, świadków, twoją reakcję i poziom pewności (4.4, aneks C).
12	Czy wolno ująć osobę podejrzaną o rozpoznanie obiektu?	Kodeks postępowania karnego pozwala na ujęcie w ściśle określonych warunkach, ale przewodnik tego nie rekomenduje: oddalasz się i zgłaszasz (4.7).
13	Gdzie zgłaszasz sygnały działania obcych służb wobec żołnierza lub firmy pracującej dla wojska?	Do pełnomocnika ds. ochrony informacji niejawnych lub przełożonego zgodnie z procedurą jednostki oraz do Służby Kontrwywiadu Wojskowego (15.12).
14	Alarm lotniczy w Ukrainie, a w pobliżu nie ma schronu. Gdzie się kryjesz?	W pomieszczeniu bez okien, oddzielonym od zewnątrz co najmniej dwiema ścianami, np. w korytarzu lub łazience (14.6).

MATTHEW
HALABA.

halaba.online
matthew@halaba.online