

FORT  KRAKÓW

GOTOWI NA KRYZYS

BEZPIECZNY
SAMORZĄD
W PRAKTYCE

 KRAKOWSKI
PARK
TECHNOLOGICZNY



Wydawca

Krakowski Park Technologiczny sp. z o. o.

Autorzy tekstów

Łukasz Gawron

Piotr Janik

Kamil Jenek

Redakcja

Kacper Miodoński

Projekt graficzny i skład

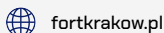
Agnieszka Zacharzewska

Współpraca



FORT Kraków to polski ośrodek innowacji obronnych i technologii podwójnego zastosowania (dual-use), tworzony wspólnie przez Krakowski Park Technologiczny oraz Akademię Górniczo-Hutniczą w Krakowie. Inicjatywa koncentruje się na technologiach deep tech i defence tech z obszaru emerging and disruptive technologies (EDT) wspierających bezpieczeństwo, obronność i odporność państwa.

FORT Kraków pełni funkcję pomostu między środowiskiem naukowym, firmami technologicznymi, Siłami Zbrojnymi RP, przemysłem obronnym i administracją publiczną. Ośrodek jest czynnym uczestnikiem międzynarodowych inicjatyw obronnych, realizując programy na poziomie NATO i Unii Europejskiej.



Spis treści

Rozdział 1

Zarządzanie w czasie kryzysu	4
Ramy prawne	5
Gdy to urząd pada ofiarą kryzysu	7
Pierwsze trzy dni – prosty schemat działania	7
Gotowość do działania – samoocena	10
Arkusz sytuacyjny – wspólne źródło informacji	11
Najczęstsze błędy	16
Najważniejsze wnioski	17

Rozdział 2

Łączność i komunikacja w czasie kryzysu	18
Ramy prawne	18
Łączność ≠ komunikacja	19
Wyspy informacyjne	20
Meldunki	21
Kontakt z mieszkańcami	22
Warstwy łączności	23
Wspólny obraz sytuacji	24
Systemy ogólnokrajowe	25
Arkusz samooceny	26
Najważniejsze wnioski	28

Rozdział 3

Obiekty Zbiorowej Ochrony (OZO)	30
Ramy prawne	30
Podstawowe pojęcia	31
Nowe i istniejące budynki	32
Kto za co odpowiada?	34
Dostosowanie obiektów gminnych – krótki przewodnik	34
Najważniejsze wnioski	38

Rozdział 4

Cyberzagrożenia dla samorządów	39
Ramy prawne	40
Najczęstsze metody ataku	41
Słabe punkty infrastruktury	42
Jak się chronić?	
Podstawowe reguły bezpieczeństwa	43
Cyberincydent – kogo powiadomić?	44
Suwerenność technologiczna a urząd	44
Lokalne Centra Cyberbezpieczeństwa	45
Najważniejsze wnioski	46

Rozdział 5

Mity obrony cywilnej	47
-----------------------------	-----------

Rozdział 6

Nowe technologie w służbie samorządu	53
---	-----------

Autorzy tekstów	60
------------------------	-----------

Bibliografia	62
---------------------	-----------

Innowacje i technologie dla bezpieczeństwa samorządów

Szanowni Państwo,

„bezpieczeństwo”, „odporność”, „kryzys”, „obrona” – te słowa na stałe zagościły w języku debaty publicznej. Wojny, napięcia geopolityczne i konflikty hybrydowe sprawiają, że kwestie, którym jeszcze niedawno poświęcaliśmy ograniczoną uwagę, dziś wymagają konkretnych działań. Dotyczy to administracji, przedsiębiorstw i społeczności lokalnych.

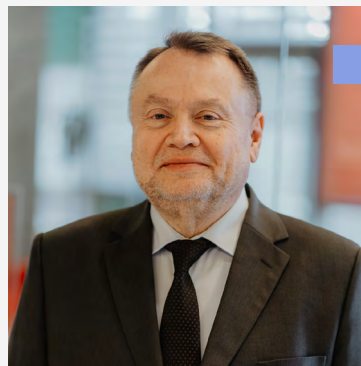
Szczególnie ważna rola przypada samorządom. Ustawa o ochronie ludności i obronie cywilnej wzmacnia ich miejsce w systemie bezpieczeństwa i stawia przed nimi zadania wymagające odpowiednich procedur, zasobów, przygotowanych kadr i sprawnej współpracy z innymi podmiotami. Samorządy muszą nie tylko reagować na kryzysy, ale również utrzymywać niezbędne zasoby, przygotowywać urzędy do działania w sytuacjach poważnego zagrożenia, współtworzyć system obiektów zbiorowej ochrony i budować odporność, również w sferze cyfrowej.

Dlatego Krakowski Park Technologiczny zacieśnia współpracę z samorządami i firmami tworzącymi rozwiązania dla bezpieczeństwa. Działając w konsorcjum z Akademią Górniczo-Hutniczą pod marką **FORT Kraków** – pierwszego polskiego akceleratora technologii obronnych i podwójnego zastosowania – łączymy doświadczenie we współpracy z administracją publiczną, Ministerstwem Obrony Narodowej oraz NATO z wiedzą

technologiczną i biznesową. Od maja do listopada 2026 roku 12 polskich firm uczestniczy w programie „**Nowe technologie dla bezpieczeństwa samorządów**”, mającym na celu wsparcie odporności lokalnej, zidentyfikowanie potrzeb jednostek samorządu terytorialnego i zaproponowanie skutecznych rozwiązań.

Niniejsza publikacja jest częścią tych działań. We współpracy ze Stowarzyszeniem Świadoma Obrona Cywilna oraz klastrem #CyberMadeInPoland przygotowaliśmy praktyczny poradnik dla samorządowców. Poruszamy w nim zagadnienia związane z organizacją zarządzania kryzysowego, łącznością i komunikacją, obiektami zbiorowej ochrony oraz cyberbezpieczeństwem. Wyjaśniamy też najczęstsze nieporozumienia dotyczące ochrony ludności i przedstawiamy rozwiązania rozwijane przez firmy uczestniczące w programie FORT-u Kraków.

Życzę owocnej lektury.



dr hab. **Andrzej Kulig**
prezes zarządu Krakowskiego Parku Technologicznego

Odporność budujemy od podstaw

Szanowni Państwo,

w ostatnim czasie wiele mówimy o bezpieczeństwie. Wyrażenie to na wskroś wypełniło publiczną debatę na różnych poziomach. Odczytujemy je jako ważną społecznie potrzebę, która zdaje się o sobie przypominać szczególnie w kontekście otaczających nas realiów i wyzwań, z jakimi przechodzi nam się mierzyć.

Nie ulega wątpliwości, że właśnie teraz potrzebujemy skutecznych form zabezpieczenia. Jedną z nich jest odporność społeczna. Dobrze wiemy, że jak każdą odporność, tak i tą musimy budować od podstaw. Taki bowiem model, ściśle zorientowany na poziom lokalnej społeczności, pozwala efektywnie zapobiegać zagrożeniom i właściwie na nie reagować – już na wczesnym etapie rozwoju sytuacji kryzysowej.

Szanowni Państwo! Drodzy samorządowcy i przedstawiciele wspólnot lokalnych! Mając na uwadze powierzoną Wam odpowiedzialną misję w tym zakresie, wdrażamy rządowy Program Ochrony Ludności i Obrony Cywilnej, który kompleksowo reguluje system ochrony obywateli w czasie pokoju oraz obrony cywilnej na wypadek wojny. Zależy nam na tym i robimy wszystko, aby nie był to teoretyczny dokument, ale praktyczne narzędzie wyznaczające priorytety i kierunki działań. To również realne wsparcie dla samorządów w misji budowania filarów bezpieczeństwa, chociażby w zakresie rozwoju i modernizacji obiektów zbiorowej ochrony, unowocześnianiu

systemów ostrzegania, alarmowania i powiadamiania, zabezpieczenia zasobów krytycznych, zacieśniania współpracy czy też podnoszenia świadomości społecznej, edukacji i szkoleń.

Życzę, aby ten poradnik przyniósł Państwu odpowiedzi na pytania dotyczące ochrony ludności i obrony cywilnej oraz zarządzania kryzysowego na poziomie lokalnym. Niech zawarte w tej publikacji praktyczne wskazówki pozwolą podejmować działania na rzecz budowania od podstaw odporności społecznej.



dr inż. **Krzysztof Jan Klęczar**
Wojewoda Małopolski

Rozdział 1

Zarządzanie w czasie kryzysu

Autor: Kamil Jenek

Gdy dochodzi do klęski żywiołowej, mieszkańcy nie zastanawiają się, który szczebel administracji odpowiada za podjęcie konkretnych decyzji. Oczekując pomocy, kierują się do urzędu gminy, dzwonią do burmistrza, sołtysa albo lokalnej jednostki OSP. Chcą wiedzieć, czy trzeba się ewakuować, gdzie otrzymają wodę, którędy mogą przejechać i kiedy wróci prąd.

Samorządowcy nie zastąpią straży pożarnej, policji ani systemu ochrony zdrowia, muszą jednak stworzyć warunki, w których służby mogą swobodnie i szybko działać, mieszkańcy otrzymują jasne informacje, zasoby lokalne są prawidłowo wykorzystywane, a podstawowe usługi publiczne nie przestają funkcjonować.

Warunkiem niezbędnym do opanowania kryzysu jest sprawna współpraca z przedstawicielami służb. Za kierowanie działaniami ratowniczymi odpowiada wyznaczony

funkcjonariusz¹. Samorządowi w uzyskaniu pełniejszego obrazu sytuacji może pomóc skierowanie do przedstawicieli służb następujących pytań:

- jakiego wsparcia oczekują służby?
- czy zabudowania i mieszkańcy są bezpośrednio zagrożeni?
- które drogi są nieprzejezdne lub powinny zostać wyłączone z ruchu przez właściwe organy?
- gdzie można zorganizować zaplecze?
- jakie informacje urząd może bezpiecznie przekazać mieszkańcom?

Dotyczą spraw podstawowych, ale mających kapitalne znaczenie w dobie klęski: o sukcesie w zarządzaniu kryzysem może przesądzić zadbanie właśnie o najbardziej elementarne kwestie.

¹ Rozporządzenie MSWiA z dnia 24 czerwca 2026 r. w sprawie szczegółowej organizacji krajowego systemu ratowniczo-gaśniczego [Dz.U. z 2026 r. poz. 872], § 22 ust. 1.

Ramy prawne

Ustawa o ochronie ludności i obronie cywilnej (OLiOC) nakłada na samorządy obowiązki związane między innymi z przygotowaniem zasobów, ostrzeganiem ludności, ewakuacją i organizacją pomocy. W zależności od skali administracji i lokalnych zagrożeń trzeba zapewnić dostęp między innymi do wody, żywności, środków medycznych i tymczasowych miejsc pobytu². Ustawa wymaga też, aby samorząd miał dostęp do zasobów potrzebnych do wykonywania wskazanych zadań ochrony ludności **przez co najmniej trzy dni zagrożenia**.

Ustawa o zarządzaniu kryzysowym stanowi, że na terenie gminy za zarządzanie kryzysowe odpowiada wójt, burmistrz albo prezydent miasta. To on kieruje przygotowaniami, reagowaniem na zagrożenia i usuwaniem ich skutków. Powołuje zespół zarządzania kryzysowego i określa sposób jego pracy. Gmina musi przy tym zapewnić sprawne alarmowanie właściwych osób oraz przyjmowanie i przekazywanie informacji, także poza godzinami pracy urzędu³.

W myśl ustawy o samorządzie gminnym samorząd odpowiedzialny jest między innymi za drogi i mosty, zaopatrzenie w wodę, kanalizację, gospodarkę odpadami, transport lokalny, pomoc społeczną, ochronę zdrowia, porządek publiczny oraz ochronę przeciwpożarową i przeciwpowodziową⁴. **Katastrofa nie zawiesza tych obowiązków**. Przeciwnie – sprawia, że wiele z nich trzeba realizować jednocześnie i pod presją czasu oraz opinii publicznej.

Ustawa o stanie klęski żywiołowej określa szczególne zasady działania po formalnym wprowadzeniu tego stanu⁵. Nie trzeba jednak czekać na ogłoszenie, aby ostrzegać mieszkańców, organizować pomoc, prowadzić ewakuację czy podejmować inne działania przewidziane w zwykłych przepisach dotyczących zarządzania kryzysowego i ochrony ludności.

² Ustawa OLiOC, art. 33 ust. 1, 3-4.

³ Ustawa o zarządzaniu kryzysowym, art. 19 ust. 1 i ust. 2 pkt 1, art. 20.

⁴ Ustawa z dnia 8 marca 1990 r. o samorządzie gminnym (Dz.U. z 2026 r. poz. 662), art. 7 ust. 1 pkt 2-6 i 14.

⁵ Ustawa z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej (Dz.U. z 2025 r. poz. 112), art. 1 oraz art. 7-11



Zakres odpowiedzialności samorządu najlepiej uwidacznia się podczas zdarzeń o dużej skali, takich jak pożary, w których działania służb ratowniczych są tylko jednym z elementów większej całości.

Pożar w Puszczy Solskiej w maju 2026 r. objął łącznie około 1157 ha lasu. W działania zaangażowanych było w szczytowym momencie ponad tysiąc osób, a akcję wspierało lotnictwo gaśnicze; podczas działań zginął pilot samolotu⁶.

Urząd może być potrzebny przy organizacji zaplecza, wyznaczaniu objazdów, informowaniu mieszkańców oraz przygotowaniu pomocy dla osób szczególnie narażonych na skutki zadymienia lub przerw w dostawie energii. W czasie pożaru z całą mocą ujawnia się znaczenie wiedzy na temat lokalnych uwarunkowań i rzeźby terenu. Leśnicy, druhowie OSP, sołtysi i mieszkańcy najlepiej znają drogi pożarowe, dojazdy do zbiorników wodnych i miejsca, w których ciężki sprzęt może ugrzęznąć.

⁶ Ministerstwo Klimatu i Środowiska, *Bilans pożaru w Puszczy Solskiej – trwa szacowanie strat i planowanie odnowy lasu*, 15 maja 2026 r.

Gdy to urząd pada ofiara kryzysu

Kiedy nie działają telefony, internet i sieć energetyczna, klasyczny model pracy urzędu przestaje się sprawdzać. Zalanie lub inne uszkodzenie budynku urzędu oznacza utratę dostępu do dokumentacji, komputerów i stanowisk pracy. Należy zakładać, że w czasie katastrofy jednostka administracyjna może utracić część swoich zdolności. Dlatego tak ważne jest zabezpieczenie alternatywnego obiegu informacji i zapasowej infrastruktury. W zależności od lokalnych zagrożeń warto przygotować:

- awaryjne miejsce pracy władz i zespołu kryzysowego
- alternatywne źródła zasilania
- zapasowe środki łączności, w tym radiowej lub satelitarnej
- papierowe formularze i listy kontaktowe
- lokalne punkty informacyjne w różnych częściach gminy
- fizyczny system przekazywania informacji przez sołtysów, OSP i kurierów terenowych.

Proste rozwiązania bywają w takich kryzysowych sytuacjach skuteczniejsze niż rozbudowane systemy informacyjne. Jako efektywne metody komunikacji mogą służyć:

- tablica ogłoszeń przy remizie
- samochód OSP z megafonem
- kartka z numerami telefonów wywieszona w powszechnie dostępnym, widocznym miejscu.

Powódź w Łądku-Zdroju miała miejsce we wrześniu 2024 r. i była częścią kataklizmu, który nawiedził dorzecze Odry. Po rozmyciu części ziemnej zapory suchego zbiornika przeciwpowodziowego w Stroniu Śląskim woda przełała się przez obiekt, pogłębiając zniszczenia w miejscowościach położonych poniżej zbiornika. Powódź spowodowała rozległe zniszczenia zabudowy i infrastruktury oraz poważnie ograniczyła dostęp do dróg, energii, wody i łączności. W krytycznym momencie, gdy nie działała łączność telefoniczna, informacje o sytuacji przekazywano do centrum zarządzania kryzysowego za pośrednictwem strażników miejskich⁷. Żywił **nie tylko zagroził mieszkańcom**, lecz także **uszkodził infrastrukturę niezbędną do kierowania kryzysem**.

Pierwsze trzy dni – prosty schemat działania

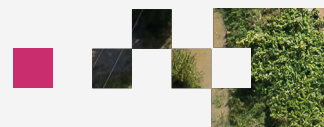
Ustawa wymaga, aby samorząd miał dostęp do zasobów potrzebnych do wykonywania wskazanych zadań przez co najmniej trzy dni zagrożenia, ale sama nie określa godzinowego harmonogramu reagowania.

Przykładowy, rozpisany na godziny plan działania może służyć jako model do samodzielnego rozwinięcia, z uwzględnieniem specyfiki gminy i posiadanych zasobów.

⁷ PGW Wody Polskie, *Awaria zbiornika Stronie Śląskie – oświadczenie Wód Polskich*, 24 września 2024 r., aktualizacja 4 lutego 2025 r.

0h - 2h	
Działanie	Zakres / sposób realizacji
Potwierdzenie skali zdarzenia	Zweryfikować informacje w co najmniej dwóch niezależnych źródłach, np. u służb, sołtysów, pracowników terenowych, operatorów infrastruktury lub na podstawie monitoringu.
Uruchomienie dyżuru	Zapewnić stałą obsadę punktu przyjmowania zgłoszeń i przekazywania informacji.
Zwołanie zespołu zarządzania kryzysowego	Wyznaczyć: • koordynatora pracy urzędu • osobę odpowiedzialną za komunikację z mieszkańcami • osobę prowadzącą dziennik działań i decyzji.
Przekazanie pierwszego komunikatu mieszkańcom	Komunikat powinien odpowiadać na pytania: • co się stało • gdzie występuje zagrożenie • czego mieszkańcy nie powinni robić • gdzie i kiedy pojawią się kolejne informacje.
Rozpoczęcie kontroli zużycia zasobów	Rejestrować zużycie paliwa, wody, sprzętu i innych kluczowych zasobów.
Prowadzenie dokumentacji	Prowadzić dziennik działań i decyzji oraz dokumentować wydatki, wykorzystany sprzęt, czas pracy i stwierdzone szkody. Materiały te mogą być później potrzebne przy rozliczaniu działań, dochodzeniu roszczeń lub ubieganiu się o pomoc.

2h - 12h	
Działanie	Zakres / sposób realizacji
Uruchomienie punktów pomocy	Wyznaczyć lokalizację, obsadę, zakres udzielanej pomocy i sposób zaopatrzenia punktów.
Zabezpieczenie transportu	Ustalić dostępność autobusów, pojazdów terenowych, ciężarówek i innych środków transportu.
Sprawdzenie sytuacji osób najbardziej narażonych	W pierwszej kolejności objąć rozpoznaniem: • osoby starsze i samotne • osoby z niepełnosprawnościami • pacjentów zależnych od urządzeń medycznych wymagających zasilania elektrycznego • mieszkańców domów pomocy społecznej • szkoły i przedszkola • placówki medyczne • osoby z terenów zagrożonych ewakuacją.
Regularne raportowanie	Każde sołectwo lub osiedle powinno przekazywać krótki raport obejmujący: • liczbę osób zagrożonych • stan dróg • dostęp do wody i energii • najpilniejsze potrzeby.



12h - 72h	
Działanie	Zakres / sposób realizacji
Wprowadzenie pracy zmianowej	Ustalić harmonogram zmian, zastępstwa i czas odpoczynku osób zaangażowanych w działania.
Bieżąca kontrola zużycia paliwa, wody i sprzętu	Aktualizować stan zapasów, przewidywać moment ich wyczerpania i planować uzupełnienia.
Przygotowanie planu na kolejne doby	Określić przewidywany rozwój sytuacji, potrzeby kadrowe, logistyczne i finansowe oraz konieczne wsparcie zewnętrzne.
Ewidencjonowanie pomocy humanitarnej	Rejestrować przyjmowane dary, ich ilość, miejsce składowania, sposób wydawania oraz aktualne potrzeby.



Gotowość do działania – samoocena

Odpowiadając na poniższe pytania, można wstępnie określić gotowość do działania w ekstremalnych warunkach klęski żywiołowej lub innego kryzysu.

- ☐ Czy osoba przyjmująca zgłoszenie wie, kogo powiadomić po godzinach pracy?
- ☐ Czy urząd może pracować bez prądu, internetu i telefonii komórkowej?
- ☐ Czy wyznaczono zapasowe miejsce kierowania działaniami?
- ☐ Czy sołtysi i OSP mają aktualne numery kontaktowe do zespołu kryzysowego?
- ☐ Czy gmina ma zgodną z prawem i regularnie aktualizowaną procedurę ustalania, kto może potrzebować dodatkowego wsparcia podczas ewakuacji?
- ☐ Czy miejsca ewakuacji mają wodę, sanitariaty, ogrzewanie i zasilanie?
- ☐ Czy awaria jednego mostu lub drogi nie odetnie wszystkich zasobów?
- ☐ Czy gmina ma zapewniony dostęp do potrzebnego sprzętu i wie, kto może go dostarczyć, uruchomić i obsługiwać także poza godzinami pracy?
- ☐ Czy podpisano wcześniej umowy lub porozumienia dotyczące użycia sprzętu?
- ☐ Czy przygotowano gotowe komunikaty na wypadek pożaru, powodzi i ewakuacji?
- ☐ Czy ktoś odpowiada za przyjmowanie i wydawanie pomocy humanitarnej?
- ☐ Czy wszystkie decyzje są zapisywane od pierwszych godzin zdarzenia?



Im więcej odpowiedzi twierdzących, tym wyższy poziom przygotowania.
Nawet zdobycie ich kompletu nie może jednak uśpić czujności.

Arkusz sytuacyjny – wspólne źródło informacji

Wszyscy odpowiedzialni za zwalczanie skutków kryzysu muszą mieć dostęp do kluczowych informacji. Ułatwia to koordynację całej akcji oraz zapobiega marnowaniu cennych zasobów, czasu i wysiłku zaangażowanych osób.

Arkusz sytuacyjny jest w pewnym przybliżeniu odpowiednikiem mapy sztabowej, oddaje bowiem sytuację w danym miejscu i czasie. Powinien zawierać przynajmniej:



godzinę
aktualizacji



obszar
zagrożenia



liczbę osób
ewakuowanych



stan dróg
i mostów



dostępność
wody, energii
i łączności



dostępne
zasoby



najpilniejsze
braki



zadania wraz
z nazwiskiem
osoby
odpowiedzialnej



termin
wykonania



potrzeby
przekazane do
powiatu lub
województwa



treść ostatniego
komunikatu dla
mieszkańców



Warto – jeśli to możliwe – sporządzić go w formie elektronicznej i udostępnić wyznaczonym osobom.

ARKUSZ SYTUACYJNY

Jednostka (gmina/powiat) np. Gmina Nowa Wieś	Obszar zagrożenia np. Dzielnica Stare Miasto, ul. Rzeczna 1-20 – zagrożenie powodziowe	
Osoba aktualizująca Jan Kowalski, GCZK	Liczba osób ewakuowanych np. 128 osób, w tym 34 dzieci; ewakuowano do szkoły przy ul. Szkolnej 5	
Data i godzina aktualizacji 08.08.2026, 14:30		
Kontakt tel. 500 000 000	Następna aktualizacja 16:00	Wersja arkusza 3

1 STAN INFRASTRUKTURY

Element	Drogi	Mosty	Woda	Energia	Łączność	Inne
Status	Ograniczone					
Opis sytuacji	Droga wojewódzka 705 przejezdna z ograniczeniami prędkości					
Lokalizacja/obszar	Odcinek Nowa Wieś – Podgórze					
Źródło informacji	Zarząd Dróg Wojewódzkich					
Godzina aktualizacji	13:45					
Osoba	Anna Nowak					
Uwagi						

2 DOSTĘPNE ZASOBY

Zasób	Agregat prądotwórczy
Ilość/dostępność	2 szt
Lokalizacja	Magazyn OSP Nowa Wieś
Dysponent	OSP Nowa Wieś
Gotowość	Gotowy
Możliwy czas działania	do 12 h ciągłej pracy
Sposób uruchomienia/kontakt	tel. 500 100 200 (naczelnik OSP)
Uwagi	

3 NAJPILNIEJSZE BRAKI

Brak/potrzeba	Brak łózek polowych i koców
Priorytet	Wysoki
Wpływ na działania	Ogranicza możliwość zakwaterowania ewakuowanych
Wymagane działanie	Zamówić transport z magazynu powiatowego
Zgłoszono do	Powiat
Godzina zgłoszenia	13:10
Status	Wysłane
Uwagi	

4 ZADANIA I ODPOWIEDZIALNOŚĆ

ID	1
Zadanie	Dostarczyć agregaty prądotwórcze do punktu ewakuacyjnego
Osoba odpowiedzialna	Jan Kowalski [OSP]
Termin wykonania	08.08.2026, 18:00
Status	W toku
Godzina ostatniej aktualizacji	14:00
Zależności/potrzebne zasoby	Transport z magazynu powiatowego
Uwagi	

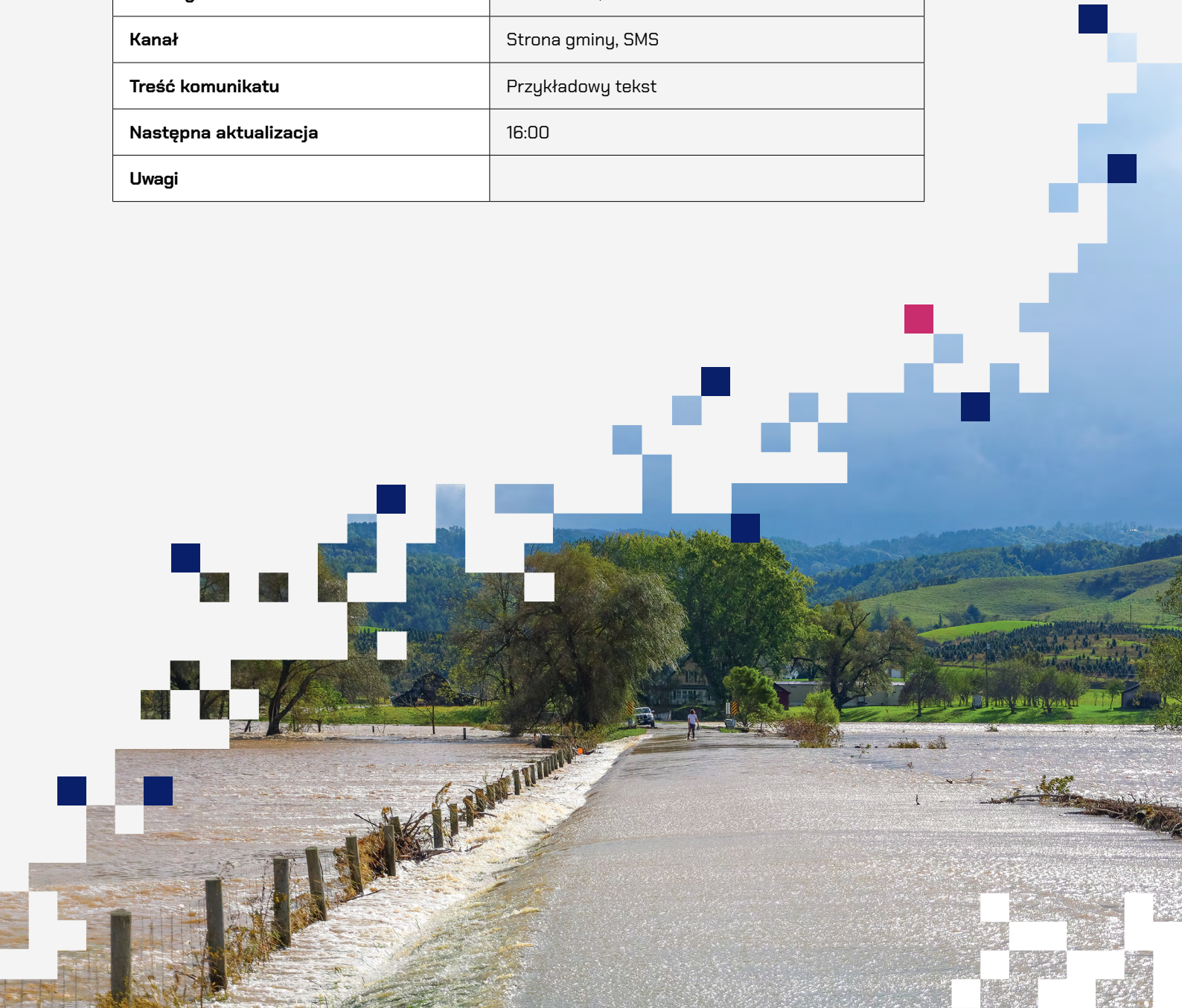
5 POTRZEBY PRZEKAZANE DO POWIATU LUB WOJEWODY

Potrzeba/wniosek	Wsparcie w postaci dodatkowych agregatów i pomocy medycznej
Adresat	Powiat
Data i godzina	08.08.2026, 13:00
Osoba zgłaszająca	Jan Kowalski
Status	W realizacji
Odpowiedź/decyzja	Przyjęto do realizacji
Termin realizacji	08.08.2026, 20:00
Uwagi	

6

OSTATNI KOMUNIKAT DLA MIESZKAŃCÓW

Data i godzina	08.08.2026, 14:15
Kanał	Strona gminy, SMS
Treść komunikatu	Przykładowy tekst
Następna aktualizacja	16:00
Uwagi	



Najczęstsze błędy

Całkowite ustrzeżenie się błędów jest niemożliwe, co nie znaczy, że nie warto próbować. Do tych najczęstszych i mających potencjalnie najbardziej negatywny wpływ na całość działań w czasie sytuacji kryzysowej należą:

Traktowanie planu jako dokumentu potrzebnego wyłącznie podczas kontroli: plan, którego pracownicy nie znają i nie rozumieją, nie jest przydatnym narzędziem.

Oparcie całej komunikacji na telefonach komórkowych: w razie powodzi, pożaru lub długotrwałej awarii zasilania sieć może przestać działać.

Zgromadzenie całego wyposażenia w jednym magazynie: zalana droga, uszkodzenie mostu lub podobne zdarzenie mogą odciąć dostęp do wszystkich zasobów.

Pomijanie lokalnych partnerów: sołtysi, OSP, organizacje społeczne, parafie, przedsiębiorcy i operatorzy ciężkiego sprzętu często docierają do mieszkańców szybciej niż administracja.

Brak jednej osoby odpowiedzialnej za komunikaty: gdy różni przedstawiciele urzędu przekazują sprzeczne informacje, zaufanie mieszkańców spada, a plotki zaczynają zastępować oficjalny przekaz.

Zakładanie, że wszystkie problemy rozwiążą służby: funkcjonariusze ratują życie, zdrowie i mienie, nie będą jednak prowadzić punktu pomocy społecznej, organizować odbioru odpadów, zarządzać darami czy odtwarzać pracy urzędu.

Najważniejsze wnioski

Samorząd nie zatrzyma gwałtownej powodzi i nie ugasi samodzielnie rozległego pożaru. Od jego postawy zależy jednak, czy mieszkańcy otrzymają pomoc w sposób uporządkowany i czy kryzys nie przerodzi się w chaos

Największą wartość mają rzeczy proste: aktualna lista telefonów, zapasowe miejsce pracy, sprawny agregat, radiotelefony, przygotowane komunikaty, mapa lokalnych zasobów. Wszyscy zaangażowani muszą znać zakres swoich obowiązków.

Katastrofa zawsze zaskakuje swoim przebiegiem. Każdorazowo należy być jednak gotowym na perspektywę działania bez prądu, internetu i pod ogromną presją społeczną.

O gotowości na sytuacje ekstremalne świadczy nie liczba dokumentów przechowywanych w segregatorach, a to, czy od pierwszych godzin kryzysu wiadomo, kto odpowiada za:

- podejmowanie kluczowych decyzji
- kontakt ze służbami
- informowanie mieszkańców
- zapewnienie dostępu do podstawowych zasobów i transportu
- zaplanowanie pracy urzędu w chwili, gdy jego główna siedziba przestanie funkcjonować.



Rozdział 2

Łączność i komunikacja w czasie kryzysu

Autor: Kamil Jenek

Łączność jest układem nerwowym zarządzania kryzysowego: bez niej nie ma ostrzegania, koordynacji ani wspólnego obrazu sytuacji. Potencjał ludzi i sprzętu pozostanie niewykorzystany, jeśli informacje nie dotrą we właściwym czasie do osób decyzyjnych. Skuteczny system musi łączyć gminę z administracją, służbami, operatorami infrastruktury, zespołami terenowymi i mieszkańcami. Dla każdej kluczowej relacji warto wskazać **podstawowy sposób kontaktu, rozwiązanie zapasowe i prostą procedurę na wypadek awarii**.



⁸ Ustawa OLiOC, art. 67 ust. 1-2 oraz art. 71 ust. 1-2 i 4.

⁹ Ustawa z dnia 29 maja 2026 r. o zmianie ustawy o zarządzaniu kryzysowym oraz niektórych innych ustaw [Dz.U. z 2026 r. poz. 815], art. 29 ust. 9; RCB, *Zatwierdzenie planów zarządzania kryzysowego – wyjaśniamy!*, 7 lipca 2026 r.

Ramy prawne

Ustawa o ochronie ludności i obronie cywilnej stanowi, że jeżeli urząd lub inny podmiot ochrony ludności jako pierwszy otrzyma informację o zagrożeniu, powinien niezwłocznie rozpocząć powiadamianie, ostrzeganie lub alarmowanie. Musi także poinformować właściwe organy, przekazując swoją ocenę sytuacji i wiadomość o planowanych działaniach.

Art. 71 tej ustawy przewiduje wykorzystanie różnych kanałów ostrzegania, między innymi:

- syren i urządzeń nagłaśniających
- krajowych, regionalnych i lokalnych systemów ostrzegania, w tym Regionalnego Systemu Ostrzegania
- Alertu Rządowego Centrum Bezpieczeństwa
- radia i telewizji
- oficjalnych serwisów internetowych
- innych rozwiązań cyfrowych służących szybkiemu przekazywaniu ostrzeżeń⁸.

Komunikat należy przekazać **bez zbędnej zwłoki, kanałami odpowiednimi do rodzaju i zasięgu zagrożenia**. Na poziomie gminy za organizację zadań ochrony ludności, w tym lokalnego ostrzegania i alarmowania mieszkańców, odpowiada wójt, burmistrz albo prezydent miasta.

Ważne:

Od 4 lipca 2026 roku obowiązują zmienione przepisy ustawy o zarządzaniu kryzysowym. Dotychczasowe plany zachowują moc do czasu przyjęcia nowych dokumentów i mogą być nadal aktualizowane. Przy każdej aktualizacji warto jednak sprawdzić, czy procedury są zgodne z obecnym stanem prawnym⁹.

Łączność ≠ komunikacja

Dysponując sprawnym radiotelefonem, sztab kryzysowy może nadać i odebrać sygnał, zachowując tym samym **łączność**. **Nie oznacza to automatycznie, że informacja dotarła, została zrozumiana i będzie skutkować podjęciem konkretnych działań** – aby mieć co do tego pewność, należy opanować zasady skutecznej **komunikacji**.

Każda informacja operacyjna powinna mieć wyraźnie oznaczonego **nadawcę, godzinę przekazania, odbiorcę i aktualny status**. Warto rozróżnić co najmniej:

- informację odebraną
- informację zweryfikowaną
- zadanie przyjęte do wykonania
- zadanie wykonane.

Bez określenia choćby tych podstawowych parametrów wymiana komunikatów będzie tworzyć ruch w sieci, ale nie pomoże w zarządzaniu kryzysem. Źródłem problemów są często pozornie drobne zaniedbania: **niejednolite nazewnictwo, brak potwierdzenia zadania, niejasny podział odpowiedzialności**. Jeśli tych błędów nie udaje się uniknąć, już na wczesnych etapach akcji w działania może wkraść się chaos.

Komunikacja pionowa

łączy gminę z powiatem, województwem i administracją centralną.

Komunikacja pozioma

obejmuje kontakt ze służbami, OSP, spółkami, szkołami, podmiotami medycznymi, operatorami, sołtysami i mieszkańcami.

Oba kierunki są niezbędne. Meldowanie do wojewody nie pomoże bez kontaktu z lokalną OSP, a dobra współpraca lokalna nie wystarczy, jeśli nie można uzyskać wsparcia z zewnątrz.



Wyspy informacyjne

Po gwałtownej ulewie kilka miejscowości wchodzących w skład gminy zostaje podtopionych. Zaczyna się akcja ratunkowa, podczas której:

- jednostka OSP pracuje na własnym kanale radiowym i wie o nieprzejezdnym przepuście, ale informacja nie trafia do przewoźnika odpowiedzialnego za ewakuację
- policja korzysta z własnej sieci i zamyka drogę, mapa zespołu kryzysowego nie zostaje jednak zaktualizowana
- spółka wodociągowa zgłasza przez komunikator podejrzenie skażenia ujęcia wody, lecz do osób odpowiedzialnych za tworzenie komunikatów dla mieszkańców ta wiadomość nie dociera
- zarządca drogi wysyła informacje pocztą elektroniczną
- sołtysi dzwonią do różnych pracowników urzędu
- władze powiatu oczekują meldunku w preferowanej przez siebie formie.

Poszczególne podmioty zaangażowane w działania mają informacje i środki łączności, ale nie potrafią połączyć ich w jeden, aktualny obraz sytuacji. Powstają odseparowane od siebie „wyspy informacyjne”. Skutek: nieefektywne wykorzystanie zasobów, chaos organizacyjny i potencjalne straty w ludziach i sprzęcie.

Opisana sytuacja jest fikcyjna, ale oddaje problemy zbliżone do tych, które Najwyższa Izba Kontroli stwierdziła w systemach łączności służb podległych Ministerstwu Spraw Wewnętrznych i Administracji. Kontrola wykazała między innymi ograniczoną współpracę części systemów radiowych, utrzymywanie starszych rozwiązań analogowych oraz korzystanie z telefonów komórkowych – w niektórych sytuacjach także prywatnych – jako kanału zastępczego¹⁰.

¹⁰ NIK, Funkcjonowanie systemu łączności w służbach podległych MSWiA, P/24/033, Warszawa 2025, s. 14, 46-49, 55-56.

Meldunki

Meldunek operacyjny to krótka, uporządkowana informacja o bieżącej sytuacji, podjętych działaniach i potrzebnej decyzji. Dobrze przygotowany powinien odpowiadać na dziewięć pytań:

1	kto melduje?	6	co już zrobiono?
2	kiedy melduje?	7	jak sytuacja może się rozwinąć?
3	co się wydarzyło?	8	czego brakuje?
4	gdzie?	9	jakiej decyzji oczekujemy?
5	kogo dotyczy zagrożenie?		

Poniższy fikcyjny meldunek można traktować jako modelowy – jest zwięzły i zawiera wszystkie istotne informacje. Fakty są oddzielane od prognoz i **zgłoszona zostaje konkretna potrzeba**.

Kto i kiedy melduje?	OSP Nieistniejewice, godz. 14:20.
Co i gdzie się wydarzyło?	Woda przerwała drogę gminną przy moście na ul. Leśnej. Przejazd niemożliwy w obu kierunkach.
Kogo dotyczy zagrożenie?	Odciętych jest około 40 gospodarstw, w jednym z nich przebywa osoba korzystająca z koncentratora tlenu.
Co już zrobiono?	Drogę zabezpieczono, wystawiono patrol.
Jak sytuacja może się rozwinąć?	Poziom wody rośnie, przewidujemy odcięcie kolejnych 10 gospodarstw w kierunku południowym.
Czego brakuje i jakiej decyzji oczekujemy?	Potrzebujemy autobusu od strony północnej, zespołu do ewakuacji osoby zależnej od zasilania i potwierdzenia miejsca przyjęcia mieszkańców.
Godzina kolejnej aktualizacji	Kolejny meldunek o 14:50.

Kontakt z mieszkańcami

Informowanie mieszkańców o sytuacji jest równie istotne jak sprawny kontakt pomiędzy służbami. Prawidłowo przygotowany komunikat nie tylko pozwala obywatelom używać obraz sytuacji. Spełnia też szereg innych zadań: **zmniejsza ryzyko wystąpienia paniki i podatność na dezinformację oraz sygnalizuje, że służby i władze działają. Gdy administracja milczy, szybko rodzą się plotki**, zwłaszcza w dobie mediów społecznościowych i szybkiej komunikacji międzyludzkiej.

Dobrze skonstruowany komunikat powinien wskazywać:

- | | |
|---|--|
| 1 co się wydarzyło | 4 czego robić nie powinni |
| 2 jakiego obszaru dotyczy zagrożenie | 5 gdzie mogą uzyskać pomoc |
| 3 co mieszkańcy powinni zrobić | 6 kiedy zostanie przekazana następna aktualizacja |

Uwaga: jeśli w momencie przygotowywania komunikatu urząd nie zna jeszcze wszystkich faktów, powinien wskazać wyraźnie, co sprawdza i kiedy uzupełni informacje.

Przykładowy komunikat dla mieszkańców może brzmieć następująco:

W tym wzorcowym komunikacie znalazła się informacja na temat jakości wody – zalecenia zdrowotne urząd może formułować jedynie w porozumieniu z przedsiębiorstwem wodociągowym i służbami sanitarnymi.

Co się wydarzyło i jakiego obszaru dotyczy zagrożenie?

Czego nie wolno robić?

Gdzie można uzyskać pomoc?

Godzina kolejnej aktualizacji

UWAGA. Z powodu uszkodzenia ujęcia wody od godz. 16.00 w Nieistniejewicach

nie wolno używać wody z sieci do picia, przygotowywania posiłków ani mycia zębów, także po przegotowaniu.

Wodę butelkowaną można odbierać przy remizach OSP od godz. 18.00. Osoby, które nie mogą dotrzeć do punktu, prosimy zgłaszać pod numerem dyżuru 000 000 000 lub sołtysowi.

Kolejny komunikat o godz. 20.00.

Należy operować konkretnymi. **Lakoniczna formuła „Prosimy zachować szczególną ostrożność” nie jest użyteczną instrukcją.**

Warstwy łączności

Każda gmina powinna dysponować łącznością wielowarstwową. Wykorzystanie kilku różnych sposobów komunikacji zwiększa odporność całego systemu. Na potrzeby planowania można ją podzielić na warstwy:

- **podstawową** – służbowa łączność instytucjonalna i operacyjna
- **komercyjną** – telefonia, transmisja danych, poczta i zatwierdzone aplikacje
- **awaryjną** – radio, łączność satelitarna, lokalna sieć lub mobilny punkt komunikacyjny
- **fizyczną** – patrole, kurierzy, sołtysi, remizy, tablice, megafony i stałe punkty informacyjne.

Procedury korzystania z poszczególnych systemów muszą zostać jasno opisane – sformułowanie „w razie awarii użyć radia” takiej roli z pewnością nie spełnia. Trzeba wskazać:

- kto korzysta z urządzeń
- na jakim kanale prowadzona jest łączność
- kiedy obowiązuje nasłuch
- jak ładować urządzenia i zapewnić zasilanie zapasowe
- jaki jest przewidywany zasięg
- jak przekazać informację podmiotom, które nie dysponują kompatybilnym sprzętem.

Jeżeli stosowane są kryptonimy, powinny być wcześniej uzgodnione i znane użytkownikom.





Wspólny obraz sytuacji

Utworzenie grupy na komunikatorze może usprawnić doraźny kontakt, ale szanse na wypracowanie spójnego obrazu sytuacji są niewielkie. W czasie intensywnych działań naprawdę ważne informacje gubią się w strumieniu wiadomości, a ich weryfikacja staje się stopniowo coraz trudniejsza.

Gmina potrzebuje jednej mapy lub tablicy pokazującej: zdarzenia, przejezdność dróg, osoby wymagające pomocy, rozmieszczenie zespołów, awarie infrastruktury, punkty pomocy, zadania, odpowiedzialnych za ich realizację i czas aktualizacji. Może to być system cyfrowy, arkusz, mapa papierowa albo ich połączenie. **Podstawowym warunkiem powodzenia jest, by użytkownicy korzystali z tej samej wersji.** Dane pozwalające

zidentyfikować konkretnych mieszkańców powinny być dostępne tylko dla osób, które naprawdę ich potrzebują.

Dostępne na rynku systemy mogą łączyć mapy, pozycje zespołów, zadania, zgłoszenia oraz komunikację z mieszkańcami. **Nie każde rozwiązanie będzie jednak odpowiednie dla każdej jednostki samorządu.** Przed zakupem warto sprawdzić, czy system działa bez stałego dostępu do internetu, współpracuje z innymi programami, pozwala wyeksportować dane i zapewnia odpowiedni poziom bezpieczeństwa. Trzeba również ocenić koszty utrzymania, zasady korzystania z danych oraz ryzyko uzależnienia od jednego dostawcy. Naturalnie zakup należy przeprowadzić zgodnie z zasadami gospodarowania środkami publicznymi i odpowiednimi przepisami.



Systemy ogólnokrajowe

System Powiadamiania Ratunkowego

Obejmuje 17 centrów, które obsługują zgłoszenia alarmowe i przekazują informacje do właściwych służb. Centra mogą się wzajemnie zastępować w razie awarii lub przeciążenia. System służy obsłudze zgłoszeń alarmowych, ale nie zastępuje gminnego obiegu informacji.

Alert RCB

Dociera w formie wiadomości SMS do osób znajdujących się na określonym obszarze i nie wymaga instalowania aplikacji. Jest wykorzystywany w sytuacjach poważnego zagrożenia życia lub zdrowia i nie zastępuje lokalnych kanałów ostrzegania.

Regionalny System Ostrzegania

Przekazuje ostrzeżenia i poradniki przez aplikację mobilną, strony internetowe i kanały naziemnej telewizji cyfrowej; za komunikaty regionalne odpowiadają wojewódzkie centra zarządzania kryzysowego.

System Bezpiecznej Łączności Państwowej

Jest przewidywany przez ustawę o ochronie ludności i obronie cywilnej jako rozwiązanie odporne, wielowarstwowe i interoperacyjne, obejmujące kanały stacjonarne, radiowe, komórkowe i satelitarne¹¹.

¹¹ MSWiA, *Centra Powiadamiania Ratunkowego* oraz *Regionalny System Ostrzegania*; RCB, „Alert RCB – najważniejsze pytania i odpowiedzi”; ustawa OLiOC, art. 74 ust. 1, 3-4.

Arkusz samooceny



Korzystając z poniższego arkusza, można samodzielnie ocenić, na ile urząd jest gotowy do prowadzenia sprawnej komunikacji i zidentyfikować najpoważniejsze braki.

Pytanie kontrolne	Ocena 0–2	Dowód / stan faktyczny	Zidentyfikowany brak lub ryzyko
Czy każda kluczowa relacja ma kanał podstawowy i zapasowy?			
Czy numery dyżurne są całodobowe i regularnie testowane?			
Czy wyznaczono zastępstwa osób funkcyjnych?			
Czy gmina i lokalni partnerzy uzgodnili minimalny zakres informacji, które powinien zawierać każdy meldunek?			
Czy wyznaczono osoby odpowiedzialne za tworzenie i aktualizowanie wspólnego obrazu sytuacji?			
Czy gmina może działać bez internetu i sieci komórkowej?			
Czy gmina ma możliwość zasilania kluczowych urządzeń łączności przez wymagany czas, z uwzględnieniem zapasowych baterii, ładowarek itp.?			
Czy istnieje zapasowe miejsce pracy zespołu kryzysowego?			
Czy OSP, sołtysi i spółki komunalne znają procedurę awaryjną?			
Czy przygotowano wzory komunikatów dla głównych zagrożeń?			
Czy można dotrzeć do mieszkańców bez kanałów elektronicznych?			
Czy system sprawdzono podczas ćwiczenia bez prądu, internetu i sieci GSM?			
WYNIK ŁĄCZNY			



Działanie do wykonania	Osoba odpowiedzialna	Termin

Uwaga: ocena ma charakter orientacyjny i wewnętrzny, nie jest równoważna audytowi i nie potwierdza zgodności z przepisami.

Skala ocen:

0 – nie, rozwiązanie nie istnieje lub nie jest stosowane

1 – częściowo, rozwiązanie istnieje, ale jest niepełne, nieaktualne albo niesprawdzone

2 – tak, rozwiązanie istnieje, jest aktualne i zostało sprawdzone podczas ćwiczenia albo rzeczywistego zdarzenia

Interpretacja wyniku:

0 – 8 punktów: system opiera się głównie na improwizacji

9 – 16 punktów: istnieją jego elementy, ale brakuje odporności

17 – 24 punkty: są podstawy operacyjne, które trzeba regularnie testować

Najważniejsze pytanie, jakie muszą sobie zawsze zadać osoby odpowiedzialne za planowanie i system łączności, powinno brzmieć: „Kiedy faktycznie zostały sprawdzone?”.

Najważniejsze wnioski

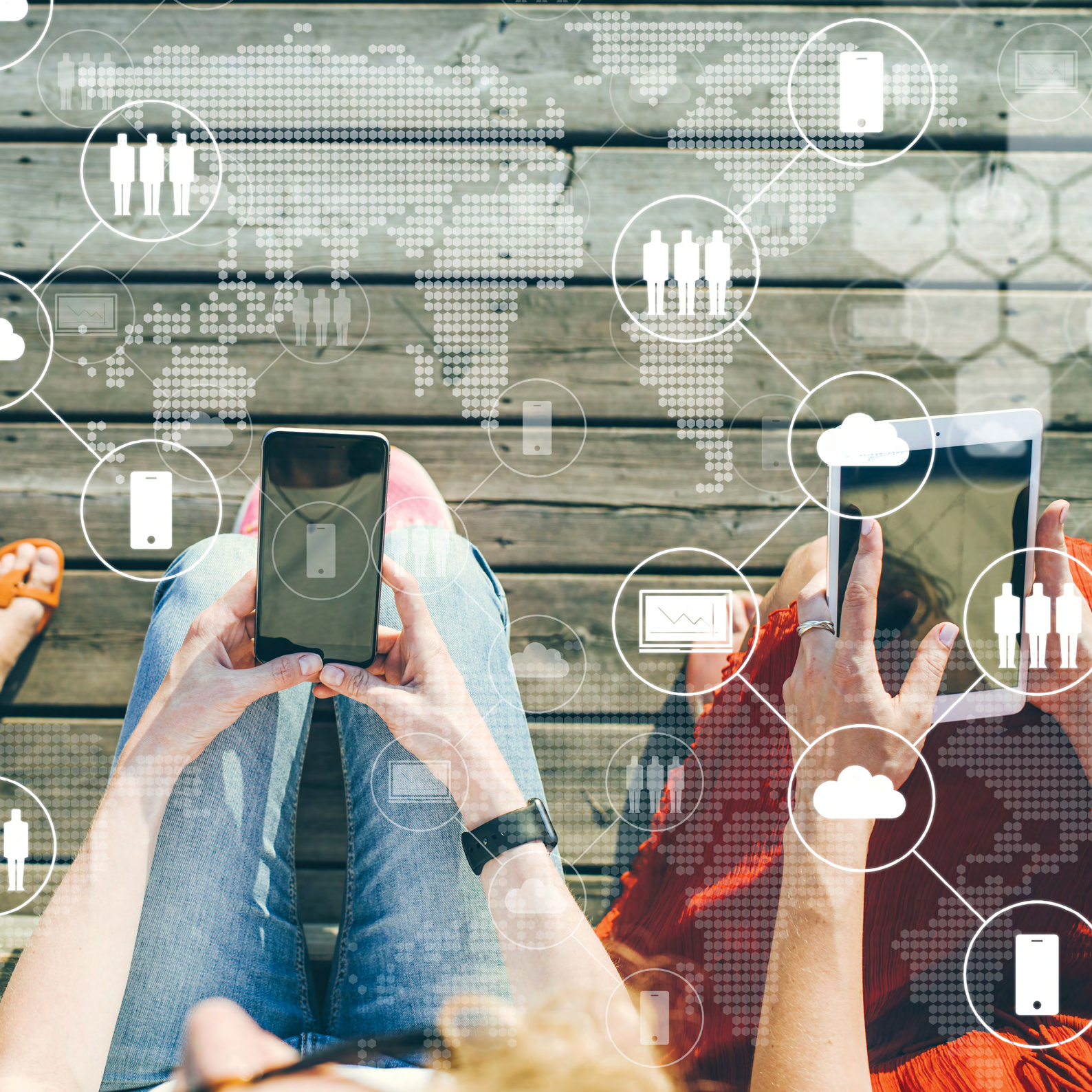
O jakości i użyteczności systemu łączności świadczy nie liczba funkcji, ale jego zdolność do funkcjonowania w warunkach braku energii elektrycznej, przeciążenia sieci i utraty dostępu do zasobów urzędu.

Należy go zaplanować tak, by umożliwiał współpracę osób korzystających z różnych technologii, a jednocześnie chronił informacje przed dostępem osób nieuprawnionych..

Komunikaty dla ludności muszą operować konkretnymi; dzięki temu nie tylko przekazują istotne informacje, ale również zmniejszają ryzyko wybuchu paniki.

Informacja ma wartość dopiero wtedy, gdy prowadzi do działania.





Rozdział 3

Obiekty Zbiorowej Ochrony (OZO)

Autor: Piotr Janik

Jakiś czas temu słowo „schron” kojarzyło się głównie z zakurzoną piwnicą z okresu PRL albo luksusowym bunkrem dla milionerów za oceanem. Ostatnie lata przynoszą jednak fundamentalną zmianę sposobu myślenia. Obiekty zbiorowej ochrony (OZO), zapewniając przetrwanie ludności cywilnej, słusznie uznawane są za jeden z kluczowych elementów budowania odporności państwa.

¹² Ustawa OLIOC (Dz.U. z 2024 r. poz. 1907, z późn. zm.).

¹³ Rozporządzenie MSWiA z dnia 4 listopada 2025 r. w sprawie warunków technicznych dla budowli ochronnych oraz warunków technicznych ich użytkowania i usytuowania (Dz.U. z 2025 r. poz. 1548).

¹⁴ Rozporządzenie MSWiA z dnia 21 lutego 2025 r. w sprawie kryteriów uznawania obiektów budowlanych albo ich części za budowle ochronne (Dz.U. z 2025 r. poz. 235).

¹⁵ Rozporządzenie MSWiA z dnia 9 lipca 2025 r. w sprawie warunków organizowania oraz wymagań, jakie powinny spełniać miejsca doraźnego schronienia (Dz.U. z 2025 r. poz. 932).

¹⁶ Rozporządzenie Rady Ministrów z dnia 31 lipca 2025 r. w sprawie szczegółowych warunków wyznaczania budynków użyteczności publicznej, w których zapewnia się budowle ochronne (Dz.U. z 2025 r. poz. 1070).

¹⁷ Rozporządzenie MSWiA z dnia 1 lipca 2025 r. w sprawie sposobu przygotowania obiektu zbiorowej ochrony do użycia, warunków eksploatacji budowli ochronnych i ich niezbędnego wyposażenia (Dz.U. z 2025 r. poz. 933).

¹⁸ Rozporządzenie MSWiA z dnia 7 lipca 2025 r. w sprawie Centralnej Ewidencji Obiektów Zbiorowej Ochrony (Dz.U. z 2025 r. poz. 922).

Ramy prawne

Ustawa o ochronie ludności i obronie cywilnej definiuje w rozdziale 9 [art. 82–116] obowiązki gmin, powiatów i województw w zakresie tworzenia obiektów zbiorowej ochrony¹². Szczegóły techniczne określają rozporządzenia:

- o warunkach technicznych dla budowli ochronnych¹³.
- o kryteriach uznawania obiektów budowlanych za budowle ochronne¹⁴.
- o warunkach organizowania miejsc doraźnego schronienia¹⁵.
- o wyznaczaniu budynków użyteczności publicznej, w których zapewnia się budowle ochronne¹⁶.
- o sposobie przygotowania obiektu zbiorowej ochrony do użycia oraz warunkach eksploatacji budowli ochronnych¹⁷.
- o Centralnej Ewidencji Obiektów Zbiorowej Ochrony¹⁸.

* Ogólnokrajowy, cyfrowy rejestr danych o schronach, ukryciach i miejscach doraźnego schronienia. Prowadzi go Komendant Główny Państwowej Straży Pożarnej. Informacje ogólne dostępne są pod adresem ceozo.pl.

Podstawowe pojęcia

Obiekty zbiorowej ochrony to szeroka kategoria obejmująca dwa główne typy: **budowle ochronne oraz miejsca doraźnego schronienia**.

Budowle ochronne dzielą się dodatkowo na:

- **schrony** – obiekty o konstrukcji hermetycznej, wyposażone w filtrowentylację, chronią przed bronią masowego rażenia, bezpośrednim ostrzałem i skażeniami. W zależności od zapewnianego poziomu ochrony, mogą należeć do kategorii S-1, S-2 lub S-3
- **ukrycia** – niehermetyczne; chronią przed falą nadciśnienia, odłamkami i zagruzowaniem, ale nie zapewniają pełnej izolacji od skażonego powietrza zewnętrznego. Podobnie jak w przypadku schronów, wyróżnia się trzy poziomy ochrony: U-1, U-2 lub U-3.

Miejsca doraźnego schronienia (MDS) to osobna podgrupa obiektów zbiorowej ochrony. Ich lokalizację planuje się i przygotowuje już w czasie pokoju, ale faktycznie organizuje dopiero po wprowadzeniu stanu nadzwyczajnego lub w czasie wojny, jeżeli liczba schronów i ukryć jest niewystarczająca¹⁹. W praktyce będą to głównie istniejące kondygnacje podziemne budynków wielorodzinnych oraz użyteczności publicznej.

Poza obiektami zbiorowej ochrony wyróżnia się dodatkowo punkty schronienia. To miejsca zapewniające podstawową, doraźną ochronę, np. przed odłamkami lub skutkami gwałtownych zjawisk pogodowych.



¹⁹ Ustawa OLiOC, art. 102 ust. 1-4.

Ustawa o ochronie ludności i obronie cywilnej wskazuje, jakiemu odsetkowi mieszkańców władze lokalne zobowiązane są zapewnić schronienie:

Obszar	Łączna pojemność OZO	w tym budowle ochronne
W granicach miast	min. 50% populacji	min. 25% populacji
Poza granicami miast	min. 25% populacji	min. 15% populacji

Obowiązków samorządu nie można sprowadzić wyłącznie do osiągnięcia wymaganego progu. By system mógł sprawnie działać i rzeczywiście podnosić poziom bezpieczeństwa, należy uwzględnić czynniki dodatkowe. Podczas planowania priorytet powinny mieć obszary o największej gęstości zaludnienia i deficycie miejsc, obiekty skupiające dużo osób w ciągu dnia oraz sąsiadujące z infrastrukturą

krytyczną. Trzeba też uwzględnić potrzeby dzieci, seniorów i osób z niepełnosprawnościami. Znaczenie ma również odległość. MDS planuje się co do zasady w odległości nie większej niż 500 m od miejsc stałego przebywania ludzi. W przypadku budowli ochronnych maksymalna odległość wynosi 500 m w miastach i 1000 m poza ich granicami.

Nowe i istniejące budynki

W budynkach użyteczności publicznej zasadą jest zapewnienie budowli ochronnej, choć przepisy przewidują wyjątki. Obecnie obowiązujący katalog obejmuje obiekty z co najmniej jedną kondygnacją podziemną, m.in. siedziby administracji i wymiaru sprawiedliwości, szpitale i placówki służb ratowniczych, obiekty dla ponad 50 osób (oświatowe, kulturalne, sportowe, biurowce) oraz pozostałe o powierzchni powyżej 2500 m² lub przeznaczone dla ponad 100 osób²⁰.

Zasada powszechności ochrony doraźnej obowiązuje od **1 stycznia 2026 r.** – nowe wymagania dotyczą co

do zasady inwestycji, dla których po **31 grudnia 2025 r.** złożono odpowiedni wniosek budowlany lub dokonano zgłoszenia.

Jeżeli w nowym budynku wielorodzinnym lub budynku użyteczności publicznej nie powstaje schron albo ukrycie, jego część podziemną trzeba co do zasady zaprojektować tak, aby w razie potrzeby można było urządzić w niej MDS²¹. Wymaganą pojemność ustala się na podstawie wskaźników powierzchni przypadającej na osobę – innych dla budynków użyteczności publicznej, budynków mieszkalnych i garaży. Obowiązek

²⁰ Ustawa OLiOC, art. 93.

²¹ Ustawa OLiOC, art. 94; art. 206.

nie dotyczy najmniejszych inwestycji – ustawa określa progi dotyczące liczby mieszkańców oraz powierzchni budynku i garażu.

Podobny obowiązek dotyczy **budowli ochronnej (czyli ukrycia lub schronu)**: przy nowych inwestycjach, które jej wymagają, inwestor zawiadamia wójta, burmistrza lub prezydenta miasta, a właściwy organ ma 45 dni na określenie wymaganej pojemności i kategorii odporności. Jeśli nie zrobi tego w ciągu trzech miesięcy, inwestor może sam przyjąć kategorię, przy zachowaniu pojemności co najmniej 30 osób. Jeżeli inwestorem jest sama gmina, powiat lub wojewoda, kategorię i pojemność można dobrać do własnych potrzeb.

Dlatego wymagania dotyczące miejsc doraźnego schronienia lub budowli ochronnych powinny być uwzględniane możliwie najwcześniej, już na etapie koncepcji inwestycji lub przygotowania programu funkcjonalno-użytkowego. Późniejsze zmiany mogą być trudne i kosztowne.

Podsumowując: nie wszystkie obiekty wykorzystywane w systemie ochrony muszą należeć do samorządu. Mogą to być również nieruchomości innych właścicieli, a ich obowiązki zależą od rodzaju obiektu i sytuacji, w której ma zostać wykorzystany.

Budowla ochronna formalnie uzyskuje status po spełnieniu jednego z trzech trybów przewidzianych ustawą – w każdym przypadku otrzymuje też kategorię odporności:

- obiekt gminny – zarządzenie wójta, burmistrza lub prezydenta miasta
- obiekt prywatny, za zgodą właściciela – porozumienie
- obiekt prywatny, bez porozumienia – decyzja administracyjna.

Źródło: Ustawa OLiOC, art. 83 ust. 1-2 oraz art. 86-88.



Kto za co odpowiada?

Najwięcej zadań na poziomie lokalnym wykonuje wójt, burmistrz lub prezydent miasta. Starosta zajmuje się obiektami ważnymi z punktu widzenia całego powiatu, a wojewoda – obiektami o znaczeniu ponadlokalnym. Dlatego nie za każdy obiekt na terenie gminy odpowiada ten sam organ.

Dostosowanie obiektów gminnych – krótki przewodnik

Poniżej znajduje się lista działań, jakie samorząd może podjąć, przygotowując się do adaptacji istniejących obiektów na budowle ochronne lub miejsca doraźnego schronienia. Punkty 1-3 dotyczą wstępnych aktywności, a warianty A i B opisują odpowiednio czynności dla budowli ochronnych (ukryć i schronów) oraz miejsc doraźnego schronienia. Proponowane ramy każdorazowo trzeba dostosować do konkretnych wyzwań stojących przed gminą.

1. Działania porządkujące

W urzędzie warto jednoznacznie wskazać osobę odpowiedzialną za koordynowanie działań dotyczących OZO i określić harmonogram prac. Wstępny etap może przebiegać następująco:

- sprawdzenie stanu wyjściowego
- porównanie tego stanu ze wskaźnikiem ustawowym – poznanie skali potrzeb
- inwentaryzacja obiektów, które potencjalnie można wykorzystać lub dostosować
- przygotowanie wstępnego harmonogramu i zabezpieczenie środków.

Należy rozważyć profesjonalny audyt uwzględniający lokalne uwarunkowania, potrzeby i zagrożenia, a nie tylko same wymogi ustawowe.

2. Rozpoznanie lokalnych potrzeb

Przydatne będą przede wszystkim informacje o:

- liczbie i rozmieszczeniu mieszkańców w podziale na osiedla/dzielnice (gęstość zaludnienia, obszary o zabudowie wysokiej lub jednorodzinnej]
- kondygnacjach podziemnych w budynkach wielorodzinnych i budynkach użyteczności publicznej (piwnice, garaże podziemne), wraz z orientacyjną wolną powierzchnią
- lokalizacji obiektów szczególnie wrażliwych (szkoły, przedszkola, szpitale itd.)
- położeniu terenów zagrożonych (np. obszary zalewowe)
- rozmieszczeniu infrastruktury krytycznej, zakładów przemysłowych, węzłów komunikacyjnych
- stanie istniejącej infrastruktury schronowej (często z okresu PRL – może nadawać się jeszcze do odtworzenia).

Ich zestawienie pozwala określić, **gdzie nowe obiekty są najbardziej potrzebne**.

Uwaga: powyższe kryteria dotyczą przede wszystkim przydatności obiektu jako schronu lub ukrycia. Miejsce doraźnego schronienia ma znacznie łagodniejsze wymagania – głównie odpowiednią pojemność i lokalizację – dlatego obiekt, który ich nie spełnia, może mimo to dobrze sprawdzić się jako MDS.

3. Wstępna selekcja obiektów

Przed zleceniem pełnej ekspertyzy urząd może własnymi siłami dokonać wstępnej selekcji, odpowiadając na pytania z krótkiej listy:

- czy obiekt ma kondygnację podziemną z wolną powierzchnią, która pozwala na schronienie co najmniej 15 osób?
- czy konstrukcja jest wystarczająco masywna, by bezpiecznie przystosować obiekt?
- czy liczba okien w ścianach zewnętrznych jest niewielka?
- czy można wygospodarować wyjście zapasowe poza strefę zagruzowania (czyli obszar wokół budynku, na który mogą spaść elementy jego konstrukcji – przyjmuje się, że odpowiada 1/3 wysokości konstrukcji)?

Im więcej odpowiedzi twierdzących, tym większa szansa, że adaptacja budynku znajdzie ekonomiczne i organizacyjne uzasadnienie.

Będzie ona jednak znacznie trudniejsza lub wręcz niemożliwa, jeśli:

- strop nie ma wystarczającej nośności, a jego wzmocnienie jest nieopłacalne
- występują nieusuwalne kolizje z instalacjami niebezpiecznymi (np. gazowymi)
- nie da się doprowadzić wentylacji lub zasilania awaryjnego
- przestrzeń ma zbyt wiele przegród.

Wstępna selekcja nie zastępuje naturalnie ekspertyzy technicznej, pozwala jednak ograniczyć dalszą analizę do obiektów, których dostosowanie ma największe szanse powodzenia.

W zależności od docelowego statusu obiektu, możliwe są dwie ścieżki:

wariant A:

dla schronów i ukryć (budowli ochronnych)

wariant B:

dla planowanych miejsc doraźnego schronienia (MDS)

**Wariant A:
budowle ochronne (schrony i ukrycia)**

Ocena techniczna i przygotowanie obiektu

Docelową kategorię odporności (od U-1 do S-3) dla wybranego obiektu nadaje się formalnie dopiero przy uznaniu go za budowlę ochronną. Podstawę stanowi **ekspertyza techniczna**, obejmująca aspekty konstrukcyjne, architektoniczne, instalacyjne, pożarowe i formalno-prawne – w tym ocenę możliwości przystosowania

obiektu do konkretnego typu i kategorii budowli ochronnej. Na jej podstawie przygotowujemy jest projekt adaptacji obiektu wraz ze wstępnym kosztorysem.

W dalszej kolejności wykonuje się wymagane prace oraz przeprowadza odbiór, oznakowanie i wyposażenie. Organ, który uznał obiekt za budowlę ochronną, wprowadza dane do **Centralnej Ewidencji Obiektów Zbiorowej Ochrony**.

Utrzymanie schronu lub ukrycia w gotowości

Za stan techniczny obiektu odpowiada właściciel lub zarządca. To on zabezpiecza go przed dewastacją, kradzieżą i dostępem osób postronnych do instalacji technicznych. Przeglądy (m.in. ocenę stanu konstrukcji, szczelności zamknięć, sprawności instalacji, apteczek) należy wykonywać nie rzadziej niż raz w roku. Wyznacza się kierownika, odpowiedzialnego za gotowość i obsługę budowli w razie użycia.

Wszystkie działania podejmowane w ramach opieki nad budowlą (przeglądy, usunięte usterki, szkolenia itd.) należy dokumentować – tak uzyskuje się i utrzymuje realną gotowość do użycia.

Po użyciu schronu lub ukrycia trzeba je ponownie przygotować do działania – uporządkować przestrzeń, uzupełnić zużyte zasoby, przywrócić sprawność urządzeń.



Wariant B: planowane miejsce doraźnego schronienia (MDS)

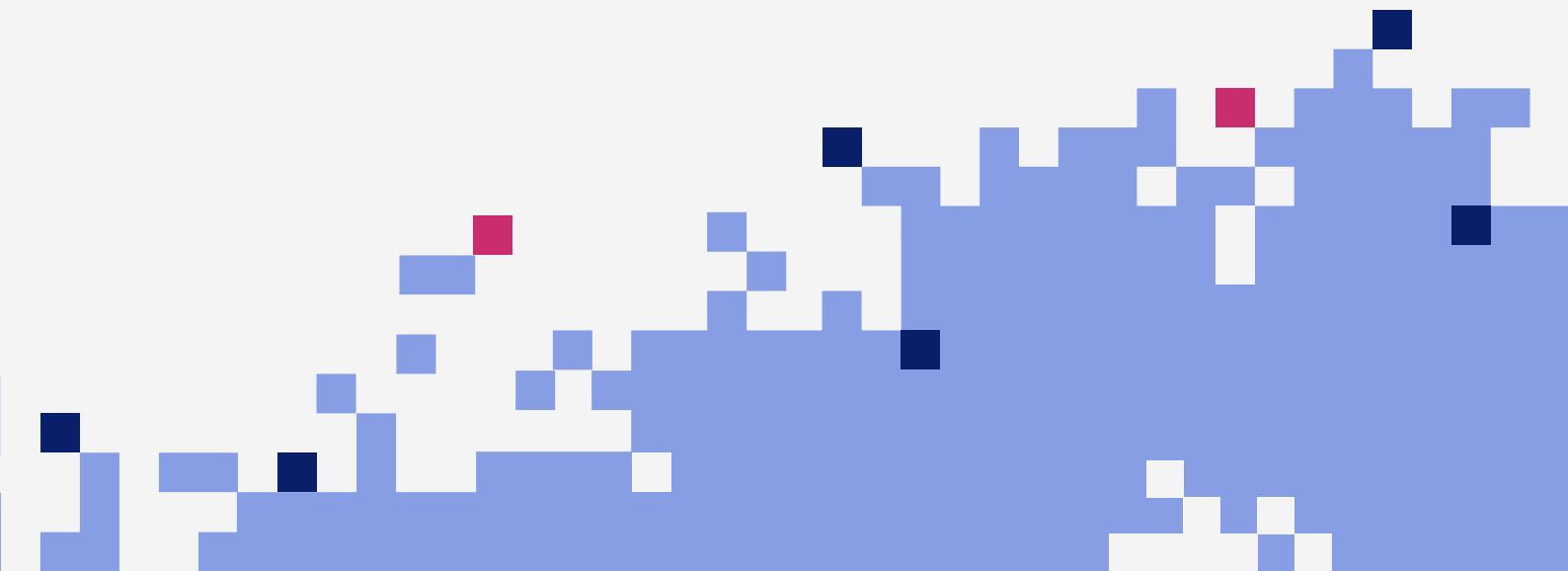
W czasie pokoju potencjalne MDS jest przede wszystkim planowane i przygotowywane. O jego faktycznym uruchomieniu postanawia organ ochrony ludności dopiero po wprowadzeniu stanu nadzwyczajnego lub w czasie wojny, gdy dostępnych schronów i ukryć jest za mało. W przypadku prywatnej nieruchomości obowiązek jej przystosowania może zostać nałożony decyzją administracyjną.

Za przygotowanie przestrzeni odpowiada właściciel lub zarządca obiektu. Miejsce dla ukrywających się oraz drogi ewakuacyjne trzeba opróżnić ze zbędnego wyposażenia, wykonać niezbędne naprawy, wdrożyć wcześniej zakładane rozwiązania (np. system podpór), odpowiednio oznakować obiekt. Mieszkańców informuje się przez lokalny system ostrzegania i lokalne plany ochrony ludności.

Im więcej czasu poświęcono na wcześniejsze przygotowania, tym szybciej obiekt można udostępnić mieszkańcom. Dlatego dokumentacja techniczna, procedura przygotowania obiektu oraz potrzebne materiały powinny być dostępne z wyprzedzeniem.

Planowane miejsca doraźnego schronienia również muszą trafić do **Centralnej Ewidencji Obiektów Zbiorowej Ochrony**.

Gmina sprawdza stan wyjściowy i porównuje go ze wskaźnikiem ustawowym, w ramach rozpoznania potrzeb ustala, że ma kilka garaży podziemnych i piwnic z wolną powierzchnią, po czym przeprowadza wstępną selekcję – odrzuca obiekty poniżej progu 15 osób lub z wyraźnymi przeciwwskazaniami, a dla 2-3 najbardziej obiecujących zleca wizję lokalną. Żaden z nich nie nadaje się jednak na schron ani ukrycie: gmina wybiera go jako planowane miejsce doraźnego schronienia i przechodzi do **wariantu B**.





Najważniejsze wnioski

Schron lub ukrycie to budowla ochronna przygotowywana już w czasie pokoju; planowane miejsce doraźnego schronienia (MDS) organizuje się dopiero w stanie nadzwyczajnym lub w czasie wojny.

Planowanie OZO powinno zaczynać się od rozpoznania istniejących zasobów i rzeczywistych potrzeb.

Znaczenie ma nie tylko liczba miejsc, lecz również ich rozmieszczenie, dostępność i czas potrzebny na przygotowanie obiektu do użycia.

Wstępną selekcję potencjalnych obiektów może przeprowadzić urząd, natomiast ich ocena techniczna wymaga udziału odpowiednich specjalistów.

W nowych inwestycjach wymagania dotyczące ochrony powinny być uwzględniane od początku procesu inwestycyjnego.

Schrony i ukrycia trzeba utrzymywać w gotowości, a dla planowanych MDS wcześniej przygotować dokumentację, procedury i potrzebne materiały.



Rozdział 4

Cyberzagrożenia dla samorządów

Autor: Łukasz Gawron

Samorządy i podległe im jednostki korzystają z systemów obsługujących ewidencję ludności, oświatę, pomoc społeczną, transport, gospodarkę komunalną i wiele innych usług. Wraz z postępującą cyfryzacją rośnie też skala zagrożeń. Jednostki administracji publicznej, w przeciwieństwie do dużych firm prywatnych, często dysponują ograniczonymi budżetami, a zadania informatyczne realizuje niewielki zespół, który jednocześnie utrzymuje systemy, wspiera pracowników i odpowiada za bezpieczeństwo. Stają się tym samym łatwym i bardzo atrakcyjnym celem.



Ramy prawne

Rozporządzenie w sprawie Krajowych Ram Interoperacyjności zobowiązuje podmioty publiczne m.in. do zarządzania bezpieczeństwem informacji, przeprowadzania wewnętrznego audytu przynajmniej raz w roku, aktualizowania oprogramowania i szkolenia pracowników – to fundament, na którym budowane są kolejne regulacje²².

Nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa (KSC) – od 3 kwietnia 2026 r. obowiązują przepisy wdrażające dyrektywę NIS2. Rozszerzają one katalog organizacji objętych KSC i wprowadzają podział na podmioty **kluczowe i ważne** oraz nowe obowiązki dotyczące m.in. zarządzania ryzykiem, zabezpieczenia systemów, zgłaszania incydentów i systemu zarządzania bezpieczeństwem informacji (SZBI). **Administracja publiczna, w tym samorządy i jednostki im podległe, może być objęta KSC jako podmiot kluczowy lub ważny.** Status konkretnej jednostki i zakres jej obowiązków zależą od kryteriów określonych w ustawie. Podmioty

publiczne objęte KSC są wpisywane do Wykazu z urzędu. Podmioty, które spełniały kryteria KSC już 3 kwietnia 2026 r., mają czas do **3 kwietnia 2027 r.** na wdrożenie obowiązków wynikających z nowych przepisów, w tym SZBI. Za realizację obowiązków z zakresu cyberbezpieczeństwa odpowiada kierownik podmiotu.

Uwaga: zawsze należy dokonać samodzielnej weryfikacji – **każda jednostka powinna sprawdzić, czy podlega KSC, jaki ma status i jakie obowiązki musi spełnić**²³.

CER (dyrektywa o odporności podmiotów krytycznych)²⁴ – uzupełnia NIS2 o wymiar fizyczny i organizacyjny: ochronę obiektów infrastruktury krytycznej (m.in. wodociągów, ciepłownictwa, energetyki) przed zakłóceniami takimi jak awarie, sabotaże czy klęski żywiołowe. Polskie przepisy wdrażające CER obowiązują od 4 lipca 2026 r. To naturalne uzupełnienie tematu – cyberbezpieczeństwo i bezpieczeństwo fizyczne infrastruktury komunalnej trzeba rozpatrywać łącznie.



²² Rozporządzenie w sprawie Krajowych Ram Interoperacyjności, § 19 ust. 1-2.

²³ Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (KSC), t.j. Dz.U. z 2026 r. poz. 20, z późn. zm., art. 5, 8, 11-12b; ustawa z dnia 23 stycznia 2026 r. o zmianie ustawy o KSC (Dz.U. z 2026 r. poz. 252), art. 33 ust. 1; Ministerstwo Cyfryzacji, „Nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa (KSC) – jak dokonać samoidentyfikacji?”, 27 kwietnia 2026 r.

²⁴ Ustawa z dnia 29 maja 2026 r. o zmianie ustawy o zarządzaniu kryzysowym (Dz.U. z 2026 r. poz. 815), art. 73 (data wejścia w życie); ustawa wdraża m.in. dyrektywę Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych.

Najczęstsze metody ataku

Wiedza o metodach i kierunkach ataku ma kluczowe znaczenie – znając je, można tak dostosować procedury i systemy, by zmniejszyć ryzyko. Najpowszechniejsze zagrożenia dla jednostek samorządowych obejmują:

Ransomware – oprogramowanie blokujące dostęp do systemów lub szyfrujące pliki; atakujący najczęściej domagają się okupu za zdjęcie blokady, niekiedy grożą też ujawnieniem wrażliwych informacji. **Odcięcie dostępu do baz danych, systemów dziedzicznych czy ewidencji może sparaliżować pracę urzędu na tygodnie** i skutkować utratą dostępu do danych mieszkańców (jak to miało miejsce np. w 2021 r. w przypadku Urzędu Marszałkowskiego Województwa Małopolskiego)²⁵. W pierwszej połowie 2026 r. ataki ransomware dotknęły m.in. urzędy w Obrazowie, Lewinie Kłodzkim i Nowej Rudzie; poważny incydent cyberbezpieczeństwa odnotował także Urząd Miasta Myszkowa.

Jeżeli kopie zapasowe nie są odpowiednio przechowywane oraz testowane, a samorząd nie dysponuje odpowiednimi procedurami ciągłości działania, konsekwencją może być trwała utrata części lub całości danych.

Phishing i oszustwa wykorzystujące pocztę elektroniczną (BEC – Business Email Compromise) – fałszywe wiadomości od nadawców podszywających się pod przełożonego, kontrahenta albo dostawcę. Mogą zawierać złośliwy załącznik lub link do zainfekowanej albo fałszywej strony www. Często ich celem jest nakłonienie pracownika do przelewu, zmiany numeru rachunku albo ujawnienia danych logowania. Oprócz właściwie przeszkolonego pracownika, który często stanowi najważniejszą linię obrony, równie istotne jest stosowanie **uwierzytelniania wieloskładnikowego (MFA)**.

Ataki DDoS (Distributed Denial of Service) – celowe przeciążanie stron i systemów urzędowych. Witryny i serwery otrzymują gigantyczną liczbę zapytań od zainfekowanych urządzeń, przez co działają znacznie wolniej lub stają się całkowicie niedostępne dla zwykłych użytkowników. Ataki tego rodzaju mogą nasilać się w okresach zwiększonego zainteresowania usługami publicznymi lub napięć politycznych.

Skala problemu rośnie: w 2025 r. zespół CERT Polska otrzymał 658 320 zgłoszeń; na ich podstawie zarejestrowano 260 783 incydenty bezpieczeństwa. W porównaniu z 2024 r. liczba zgłoszeń wzrosła o około 10%, a liczba zarejestrowanych incydentów – aż o 152%²⁶.

²⁵ Samorząd Województwa Małopolskiego, *Zaktualizowana informacja o naruszeniu ochrony danych osobowych*, 26 października 2021 r.; Urząd Gminy Obrazów, *Bardzo ważny komunikat. Zawiadomienie o naruszeniu ochrony danych osobowych*, 10 lutego 2026 r.; Gmina Lewin Kłodzki, *Komunikat w sprawie cyberataku na infrastrukturę Urzędu Gminy Lewin Kłodzki*, 5 maja 2026 r.; Gmina Miejska Nowa Ruda, *Komunikat dotyczący ataku cybernetycznego na infrastrukturę teleinformatyczną Urzędu Miejskiego w Nowej Rudzie*, 24 czerwca 2026 r.; Urząd Miasta Myszkowa, *Komunikat w sprawie cyberbezpieczeństwa*, 18 marca 2026 r.

²⁶ CERT Polska, *Raport roczny z działalności CERT Polska w 2025 roku*. Krajobraz bezpieczeństwa polskiego Internetu w 2025 roku, NASK – Państwowy Instytut Badawczy, Warszawa 2026, s. 117.



Słabe punkty infrastruktury

Każda infrastruktura ma swoje słabe punkty i ta cyfrowa nie jest wyjątkiem. Więcej uwagi warto poświęcić neralgicznym miejscom:

Podatności w powszechnie używanych systemach – część gmin korzysta z tych samych, często przestarzałych aplikacji od zewnętrznych dostawców. Jeśli luki nie zostaną w porę usunięte, zagrożone będą wszystkie jednostki korzystające z oprogramowania.

Poddostawcy – atak na dostawcę oprogramowania, firmę świadczącą usługi chmurowe lub obsługującą IT dla kilku gmin może uderzyć jednocześnie w wielu.

Organizacja pracy i czynnik ludzki – błędy użytkowników, braki kadrowe, rotacja pracowników, niewystarczające szkolenia, niejasne procedury, mała świadomość zagrożeń pozostają istotną luką w części jednostek administracji samorządowej.

Jak się chronić?

Podstawowe reguły bezpieczeństwa

System nie zawsze trzeba przebudowywać od podstaw. Do zauważalnego podniesienia poziomu bezpieczeństwa wystarczy niekiedy wdrożenie kilku sprawdzonych zasad i strategii:

Kopie zapasowe danych w modelu 3-2-1-1-0 (trzy kopie, dwa nośniki, jedna poza siedzibą urzędu, jedna odizolowana lub niemodyfikowalna, a całość cechuje zero błędów) – regularnie testowane pod kątem odtwarzalności, chronione przed zmianą lub usunięciem przez potencjalnego atakującego.

Wieloskładnikowe uwierzytelnianie (MFA) wszędzie tam, gdzie to możliwe, zwłaszcza dla poczty, systemów pracy zdalnej, kont administratorów – to pojedyncza zmiana o potencjalnie największym stosunku efektu do kosztu.

Monitorowanie systemów – wczesne wykrycie ataku zwiększa szanse na jego odparcie i zabezpieczenie plików.

Szkolenia pracowników – cykliczne, praktyczne, oparte na wiarygodnych scenariuszach phishingu, które nie ograniczają się do prezentacji.

Segmentacja sieci – oddzielenie sieci biurowej od systemów sterujących np. monitoringiem, oświetleniem czy infrastrukturą. Przy podziale na strefy atak na jeden z elementów nie oznacza automatycznie paraliżu drugiego.

Zarządzanie podatnościami i aktualizacjami – szczególnie w systemach dziedzicznych, które bywają zaniedbywane latami.

Plan ciągłości działania i reagowania na incydenty – spisany, przetestowany, ze wskazaniem kto, kiedy i gdzie zgłasza konkretne zdarzenie.

Audyty i testy bezpieczeństwa – regularne, najlepiej realizowane przez zewnętrznego, niezależnego podmiotu. Podmioty publiczne są ponadto zobligowane, na mocy Krajowych Ram Interoperacyjności, do przeprowadzania wewnętrznego sprawdzenia bezpieczeństwa informacji co najmniej raz w roku.

Należy pamiętać, że skuteczność opisanych wyżej metod zależy od ogólnego stanu systemów. **Zmiany każdorazowo należy wprowadzać w powiązaniu z wynikami analizy ryzyka.**

Cyberincydent – kogo powiadomić?

CSIRT NASK / CERT Polska

W przypadku cyberataku, złośliwego oprogramowania, phishingu, włamania lub innych incydentów teleinformatycznych. Dla urzędów obsługujących JST jest to właściwy krajowy zespół CSIRT.

Właściwy CSIRT sektorowy

Jeżeli urząd lub spółka jest podmiotem kluczowym albo ważnym objętym ustawą o KSC. Formalne zgłoszenia incydentów poważnych przekazywane są za pośrednictwem systemu S46.

Prezes UODO

Jeżeli doszło również do naruszenia ochrony danych osobowych i zachodzą przesłanki obowiązkowego zgłoszenia.

Policja lub prokuratura

Jeżeli incydent może stanowić przestępstwo, np. włamanie, oszustwo, kradzież danych lub wymuszenie okupu.

Jedno zdarzenie może wymagać kilku zgłoszeń. Powiadomienie CERT/CSIRT nie zastępuje zgłoszenia naruszenia danych do UODO ani zawiadomienia organów ścigania²⁷.

Suwerenność technologiczna a urząd

Decyzja o wyborze dostawców systemów, chmury czy oprogramowania ma dziś rangę strategiczną. Uzależnienie od pojedynczego podmiotu – niezależnie od kraju jego pochodzenia – może rodzić ryzyko utraty kontroli nad danymi mieszkańców i braku wpływu

na warunki umowy w sytuacji kryzysowej; nie ma też gwarancji, że dane przetwarzane są zgodnie z polskim i unijnym prawem. Może również zwiększać podatność na podwyżki cen, zwłaszcza ze strony największych graczy rynkowych.

²⁷ Ustawa o KSC, art. 11; CERT Polska, *Zgłoś incydent*; UODO, *Zgłaszanie naruszeń*.

Przy wyborze rozwiązań IT powinno się brać pod uwagę nie tylko cenę, lecz także:

- gdzie i na jakich zasadach są przetwarzane dane
- jakie podmioty i podwykonawcy mogą uzyskać do nich dostęp
- jakie prawo i jaka jurysdykcja mają zastosowanie
- czy dostawca zapewnia sprawne wsparcie serwisowe, również w sytuacji kryzysowej
- czy możliwe jest wyeksportowanie danych i przejście do innego rozwiązania

- co stanie się z danymi po zakończeniu umowy
- czy istnieje alternatywa na wypadek przerwania współpracy.

Wybór krajowych dostawców rozwiązań z zakresu cyberbezpieczeństwa może okazać się korzystny w budowaniu odporności technologicznej, gdyż oferują wsparcie w języku polskim, dobrze znają realia administracji publicznej i zapewniają serwis na terenie kraju.

Lokalne Centra Cyberbezpieczeństwa

Dla wielu mniejszych gmin samodzielne utrzymywanie całodobowego zespołu specjalistów i zaawansowanych narzędzi byłoby zbyt kosztowne. Kilka jednostek działających wspólnie ma większe szanse na zgromadzenie potrzebnych kompetencji, zapewnienie zastępstw i sprawne reagowanie na incydenty.

Od 31 lipca do 30 października 2026 roku trwa nabór na tworzenie **Lokalnych Centrów Cyberbezpieczeństwa**, prowadzony przez Centrum Projektów Polska Cyfrowa. Na dofinansowanie projektów przeznaczono niemal 269,7 mln zł, a wsparcie może objąć do 100% wydatków kwalifikowanych.

LCC mają świadczyć wspólne usługi z zakresu bezpieczeństwa, takie jak:

- monitorowanie systemów i obsługę incydentów
- zarządzanie podatnościami, aktualizacjami i uprawnieniami
- ochronę danych oraz tworzenie i testowanie kopii zapasowych
- wsparcie w przygotowaniu planów ciągłości działania
- szkolenia pracowników
- wdrażanie i rozwijanie systemu zarządzania bezpieczeństwem informacji.

O wsparcie mogą ubiegać się wyłącznie jednostki samorządu terytorialnego realizujące projekt w partnerstwie z co najmniej jedną inną jednostką. Maksymalna kwota wsparcia zależy od liczby uczestniczących samorządów i wynosi od **6 mln zł** dla dwóch jednostek do **15 mln zł** dla partnerstwa obejmującego co najmniej 20 jednostek²⁸. Szczegółowe informacje dostępne są na stronie internetowej [Centrum Projektów Polska Cyfrowa](#).

²⁸ CPPC, dokumentacja naboru FERC.04.01-IP01-003/26 „Lokalne Centra Cyberbezpieczeństwa”, stan na sierpień 2026 r.

Najważniejsze wnioski

Odporność samorządu na zagrożenia informatyczne decyduje o bezpieczeństwie mieszkańców w równym stopniu, co jego zdolność do reagowania na powodzie czy pożary lasów.

Zakup najbardziej wyrafinowanego oprogramowania nie zastąpi procedur, szkoleń, klarownego podziału odpowiedzialności i regularnych ćwiczeń.

Świadomy pracownik to pierwsza linia obrony przed cyberzagrożeniami.

Warto rozważyć podjęcie współpracy w ramach Lokalnych Centrów Cyberbezpieczeństwa: informacje dostępne są na stronie internetowej [Centrum Projektów Polska Cyfrowa](#).

Kopia zapasowa ma wartość tylko wtedy, gdy rzeczywiście można z niej odtworzyć dane.





Rozdział 5

Mity obrony cywilnej

Autor: Kamil Jenek

Przez lata obywatele przywykli, że bezpieczeństwo zapewnia „ktoś”. Państwo ma wojsko, samorząd dysponuje planami, a służby zjawia się chwilę po złożeniu zawiadomienia.

Ten model sprawnie funkcjonuje przy pojedynczym wypadku, ale zostaje wystawiony na ciężką próbę, gdy powódź obejmuje kilka gmin, blackout trwa parę dni albo tysiące osób jednocześnie potrzebują pomocy.

W kwietniu 2024 r. 62% badanych przez CBOS deklarowało, że w żaden sposób nie przygotowuje się na okoliczność zbrojnej napaści Rosji. Tylko 7% gromadziło wodę, żywność, leki i inne podstawowe zapasy²⁹. Trudno czynić z tego zarzut obywatelom, funkcjonującym w budowanym od lat systemie, i przekonywanym, że są przede wszystkim odbiorcami pomocy.

Nowa ustawa o ochronie ludności i obronie cywilnej porządkuje odpowiedzialność państwa i samorządów, wprowadza szkolenia, ćwiczenia, zasoby oraz korpus obrony cywilnej. Nie zmienia jednak podstawowego faktu: **podczas zdarzenia masowego profesjonalna pomoc zawsze będzie udzielana według priorytetów**. Dlatego odporność wspólnoty zależy jednocześnie od instytucji, służb i przygotowanych mieszkańców. Warto skonfrontować się z kilkoma mitami, jakie przez lata funkcjonowały wokół obrony cywilnej. Niektóre mają bardzo podstawowy charakter, hołdowanie innym może mieć potencjalnie katastrofalne skutki.

²⁹ CBOS, J. Scovil, *O wojnie w Ukrainie i ewentualnym rozszerzeniu konfliktu*, Komunikat z badań nr 48/2024, Warszawa 2024, s. 7-8.



Każdy trójkąt w pomarańczowym kole jest znakiem obrony cywilnej

Międzynarodowy znak obrony cywilnej to równoboczny niebieski trójkąt na pomarańczowym tle. Jeden z jego wierzchołków powinien być skierowany pionowo w górę, a żaden nie powinien dotykać krawędzi tła. **Znak służy do rozpoznawania organizacji, personelu, obiektów i środków obrony cywilnej oraz schronień dla ludności³⁰.** Nie jest zwykłym logo ani dowolnym symbolem „bezpieczeństwa”.

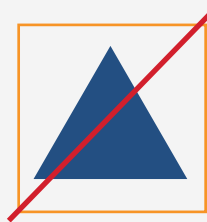
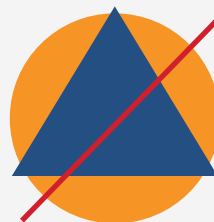
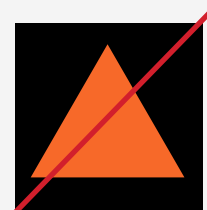
Podobne oznaczenie stosuje się na pojazdach Sił Zbrojnych RP: z przodu umieszczana jest żółta, a z tyłu czerwona okrągła tarcza z czarnym trójkątem.

Różnica koloru trójkąta i przeznaczenia znaku ma znaczenie. Stylizowanie symbolu obrony cywilnej zwiększa ryzyko pomyłki i osłabia jego funkcję rozpoznawczą.

Wniosek: przed umieszczeniem znaku na budynku, pojeździe, odzieży lub materiale promocyjnym trzeba sprawdzić nie tylko jego wygląd, lecz także podstawę i cel użycia.



PRAWIDŁOWY



NIEPRAWIDŁOWY

³⁰ Protokół dodatkowy I do Konwencji genewskich z 12 sierpnia 1949 r., art. 66 ust. 4; rozporządzenie MSWiA z dnia 4 listopada 2025 r. w sprawie warunków technicznych dla budowli ochronnych [Dz.U. z 2025 r. poz. 1548], załącznik nr 11.



Obrona cywilna oznacza, że ktoś będzie bronił cywilów

Obrona cywilna nie jest osobną służbą, która w czasie wojny roztoczy opiekę nad wszystkimi mieszkańcami.

System **ochrony ludności działa w czasie pokoju**. Po wprowadzeniu **stanu wojennego i w czasie wojny przekształca się w system obrony cywilnej**³¹. Jej zadania wykonują organy, podmioty, zasoby i formalnie wyznaczony personel. W skład personelu wchodzi między innymi osoby z przydziałem mobilizacyjnym, powołane w ramach naboru ochotniczego, funkcjonariusze PSP. Osobno ustawa przewiduje rezerwę obrony cywilnej³². Nie każdy obywatel automatycznie staje się więc personelem obrony cywilnej.

Każdy może jednak zwiększać albo zmniejszać obciążenie systemu. Człowiek rozumiejący alarmy, znający miejsce spotkania rodziny, umiejący udzielić pierwszej

pomocy i zdolny do funkcjonowania przez pewien czas bez zewnętrznego wsparcia, nie zastępuje służb. Daje im jednak dodatkowy czas na dotarcie do osób, które nie mogą poradzić sobie samodzielnie.

Ustawa przewiduje coroczne ćwiczenia organów ochrony ludności oraz edukację mieszkańców dotyczącą zagrożeń i zasad postępowania. W jej myśl społeczeństwo staje się aktywnym i przygotowanym do wspólnego działania uczestnikiem systemu.

Wniosek: edukacja mieszkańców nie może kończyć się na publikacji poradnika. Potrzebne są lokalne spotkania, ćwiczenia, instrukcje dla sołectw i konkretne role dla wolontariuszy.

³¹ Ustawa OLiOC, art. 117.

³² Ustawa OLiOC, art. 125 ust. 1-4.



Służby uratują wszystkich od razu

Zasoby służb nie są nieskończone. Podczas zdarzenia masowego pomoc kierowana jest najpierw tam, gdzie zagrożone są życie i zdrowie. Dowóz wody do każdego domu, ładowanie telefonów czy zabezpieczanie prywatnego mienia schodzą na dalszy plan.

Dlatego w ustawie wskazano bardzo konkretny próg: **wójt, starosta i wojewoda mają zapewnić zasoby niezbędne do wykonywania zadań ochrony ludności przez co najmniej trzy dni zagrożenia.** Należy przez to rozumieć zdolność systemu do podtrzymania podstawowych działań, a nie zaopatrzenia każdego gospodarstwa domowego.

Dlatego rządowy **Poradnik bezpieczeństwa** zaleca, by w każdym domu i mieszkaniu znalazły się zapasy na minimum trzy dni, w tym co najmniej trzy litry wody na osobę na dobę³³. Obie strony mają do wykonania własne zadania: **instytucje organizują system pomocy, a mieszkańcy ograniczają swoją zależność od natchmiastowego wsparcia.**

Wniosek: komunikat „przygotujcie zapasy” powinien wskazywać ilość, czas i sposób przygotowania, a także wyjaśniać, gdzie pomoc otrzymają ci, którzy z przyczyn zdrowotnych lub ekonomicznych nie mogą zatroszczyć się o zasoby samodzielnie.



Społeczeństwa nie da się zaangażować

Polacy wielokrotnie pokazali, że potrafią [współ]działać. Według GUS w pierwszym półroczu 2022 r. pomocy mieszkańcom Ukrainy udzieliło 70,2% gospodarstw domowych w Polsce. Tylko w pierwszych pięciu tygodniach pełnoskalowej wojny dodatkowe działania podjęło 28,8 tys. podmiotów gospodarki społecznej, przekazując wsparcie rzeczowe szacowane na 511 mln zł i finansowe w wysokości 140 mln zł³⁴.

Stałym przykładem zaangażowania lokalnego są OSP. W listopadzie 2025 r. w krajowym systemie ratowniczo-gaśniczym działało 5239 jednostek OSP³⁵. To tysiące lokalnych zespołów zakorzenionych w miejscowościach, znających teren i mieszkańców.

Często najważniejszym problemem jest nie brak gotowości do pomocy, lecz to, że obywatelska chęć udzielenia wsparcia jest zagospodarowywana dopiero po wystąpieniu katastrofy. **Spontaniczny wolontariusz bez zadania, wyposażenia i koordynatora może blokować dojazd, powielać pracę albo sam stać się poszkodowanym.**

Wniosek: jeszcze przed kryzysem warto prowadzić rejestr organizacji i lokalnych liderów, ustalić punkt zgłoszeń wolontariuszy oraz przygotować krótkie instrukcje: kto przyjmuje pomoc, gdzie kieruje ludzi i jak potwierdza wykonanie zadania.

³³ MSWiA, MON, RCB, *Poradnik bezpieczeństwa*, Warszawa 2025, s. 20-21.

³⁴ GUS, *Pomoc udzielona przez gospodarstwa domowe mieszkańcom Ukrainy w I półroczu 2022 r. w świetle wyników badania budżetów gospodarstw domowych*, 27 października 2022 r.; GUS, *Zaangażowanie podmiotów gospodarki społecznej w pomoc w związku z działaniami wojennymi na terytorium Ukrainy (24.02 – 31.03.2022 r.)*, 5 października 2022 r.



Najważniejsze są zasoby i infrastruktura

Sprzęt jest potrzebny, ale sam nie tworzy zdolności.

Agregat bez paliwa, przewodu, operatora i instrukcji uruchomienia pozostaje jedynie ciężkim przedmiotem. Radiotelefon bez przypisanego kanału, jasno określonej procedury użycia i naładowanej baterii nie zapewnia łączności.

W raporcie z marca 2024 roku NIK zaprezentowała wyniki kontroli przeprowadzonej wśród 32 gmin. **68% schronów i ponad połowa ukryć poddanych oględzinom nie spełniały wymaganych warunków technicznych.** Izba przywołała też dane Państwowej Straży Pożarnej, według których w takich obiektach mogłoby się zmieścić niespełna 4% mieszkańców Polski³⁶.

Raport powstał jeszcze przed wejściem w życie obecnej ustawy, ale dobrze pokazuje różnicę między wpisem w ewidencji a faktyczną gotowością.

Wniosek: każdy zasób trzeba opisać pięcioma pytaniami:

- gdzie jest
- kto nim dysponuje
- kto potrafi go użyć
- jak długo może działać
- czym zostanie zastąpiony po awarii.

³⁵ KG PSP, Włączenie jednostek OSP do krajowego systemu ratowniczo-gaśniczego z okazji Narodowego Święta Niepodległości, 2025.

³⁶ NIK, Zapewnienie obywatelom miejsc schronienia w budowach ochronnych na wypadek wystąpienia zagrożenia, nr kontroli P/23/D61, Warszawa 2024, s. 17, 52.





Poważny kryzys nas nie dotknie

To przekonanie jest zrozumiałe. Przez lata obywatele korzystali z pokoju, stabilnych instytucji, infrastruktury i międzynarodowych sojuszy. Z czasem bezpieczeństwo zaczęło przypominać usługę, która po prostu działa.

Ustawa przewiduje, że na ochronę ludności i obronę cywilną co roku przeznaczane będą środki w wysokości nie niższej niż 0,3% PKB³⁷, a nakazuje też cykliczne szkolenia i ćwiczenia. Sama skala finansowania wyraźnie wskazuje na wagę zagadnienia jako jednego z filarów odporności państwa.

Jednocześnie wiedza nie zawsze przeradza się w działanie. Z badania CBOS z marca 2026 roku wynika, że 41% osób, które zapoznały się z rządowym *Poradnikiem bezpieczeństwa*, nie podjęło po lekturze żadnych nowych przygotowań. Jednocześnie 25% przygotowało

wyposażenie awaryjne, 19% zgromadziło zapasy, a 11% wzięło udział w szkoleniu z pierwszej pomocy albo bezpieczeństwa³⁸. **Obok działań edukacyjnych kluczową rolę odgrywa przypisanie choćby prostych zadań, osadzenie ich w lokalnym kontekście i umożliwienie przećwiczenia.**

Obywatel ma prawo oczekiwać ostrzeżenia, profesjonalnej pomocy i sprawnego państwa. Nie powinien jednak zakładać, że podczas rozległego kryzysu pomoc dotrze do każdego natychmiast. Przygotowana rodzina nie zdejmuje odpowiedzialności z państwa. Daje mu jednak czas, aby najpierw ratować tych, którzy naprawdę nie są w stanie pomóc sobie sami. **Prawdziwa obrona cywilna zaczyna się więc od prostego pytania: „co mogę przygotować wcześniej i komu pomogę, zanim dotrze wsparcie?”.**

³⁷ Ustawa OLiOC, art. 155 ust. 1.

³⁸ CBOS, J. Scovil, *Polacy o „Poradniku bezpieczeństwa”*, CBOS Flash nr 13/2026, Warszawa 2026, s. 5-6.

Rozdział 6

Nowe technologie w służbie samorządu

Organizacja pracy, procedury, przyjmowanie dobrych praktyk czy poszerzanie wiedzy mają ogromne znaczenie dla podniesienia poziomu bezpieczeństwa. W dobie skokowego rozwoju technologii – w tym nowych metod ataku – musi im towarzyszyć również wdrażanie nowoczesnych rozwiązań. Swoje propozycje w kluczowych obszarach przedstawia 12 firm uczestniczących w programie „Nowe technologie dla bezpieczeństwa samorządów”. Od systemów ostrzegania ludności po schrony modułowe, polskie przedsiębiorstwa rozwijają innowacyjne pomysły i zapraszają do współpracy samorządy.



ARX Modular

ARX Modular projektuje i wykonuje prefabrykowane, modułowe systemy ochronne – schrony, miejsca doraźnego schronienia i konstrukcje polowe, które powstają w kilka dni zamiast miesięcy, za ułamek kosztu budownictwa tradycyjnego. System przeszedł badania w Wojskowym Instytucie Techniki Inżynierskiej (WITI) i zaliczył test odporności zgodny ze STANAG 2280 na poziomie C5, czyli bezpośrednie oddziaływanie amunicji artyleryjskiej 155 mm. Posiada już 10 certyfikatów STANAG. Rozwiązanie jest objęte międzynarodowym zgłoszeniem patentowym (PCT).

The logo for ARX Modular, featuring the letters 'ARX' in a stylized, bold font, followed by the word 'MODULAR' in a smaller, spaced-out font.

Kontakt:

Wojciech Milke, e-mail: w.milke@arxmodular.com, tel.: 576 151 131

BARWA SYSTEM

BARWA SYSTEM to polska firma specjalizująca się w projektowaniu i produkcji metalowych sufitów podwieszanych, fasad wentylowanych, okładzin architektonicznych oraz rozwiązań akustycznych i ochronnych. Firma łączy własne zaplecze inżynierskie, doświadczenie produkcyjne i elastyczne podejście do projektów niestandardowych. Jej rozwiązania są stosowane w obiektach komercyjnych, publicznych, przemysłowych i infrastrukturalnych, gdzie liczą się estetyka, trwałość, bezpieczeństwo oraz możliwość dostosowania produktu do indywidualnych wymagań inwestycji.

The logo for Barwa System, featuring a stylized blue square icon with a white geometric pattern inside, followed by the text 'Barwa System' with a registered trademark symbol.

Barwa System®

Kontakt:

Patrycjusz Szwarz, e-mail: biuro@barwasystem.pl, tel.: 89 522 09 10

Blue Dot Solutions

Blue Dot Solutions to polska firma technologiczna specjalizująca się w systemach GPS/GNSS oraz satelitarnych obserwacjach Ziemi. Jej technologia PLUTONIC zapewnia precyzyjny dostęp do czasu z dokładnością do 0,01 sekundy, niezależnie od źródeł internetowych czy sygnału satelitarnego GPS. Powstały w wyniku współpracy z Europejską Agencją Kosmiczną system jest odporny na zakłócenia i fałszowanie sygnału GNSS, dzięki czemu może zabezpieczać działanie urządzeń oraz infrastruktury krytycznej.



Kontakt:

Krzysztof Kanawka, e-mail: office@bluedotsolutions.eu

Civil Defence Services

Zapewnienie niezawodnej komunikacji między samorządem a mieszkańcami w obliczu zagrożeń geopolitycznych i zmian klimatu to główna misja Civil Defence Services. Realizowana jest poprzez Lokalny System Ostrzegania, które pozwala samorządom każdego szczebla punktowo ostrzegać mieszkańców konkretnej wsi lub dzielnicy wtedy, gdy zawodzić sieć komórkowa i internet. Przekazywane komunikaty są autoryzowane przez samorząd lub służby, co skutecznie wyklucza dezinformację, uzupełniając istniejące narzędzia dokładnie tam, gdzie one przestają działać.



Kontakt:

Michał Pokora, e-mail: kontakt@civildefenceservices.pl,
tel.: 517 322 270

CortexMine

CortexMine to prywatna platforma AI dla podmiotów, w których poufność danych jest warunkiem koniecznym. Model działa on-prem lub w prywatnej chmurze, więc dane mieszkańców i akta nie opuszczają infrastruktury urzędu, co wspiera zgodność z RODO, UKSC i AI Act. Platforma przejmuje powtarzalne zadania dokumentowe: odnajdywanie i porównywanie procedur oraz uchwał, projekty pism i uzasadnień, wsparcie obsługi mieszkańców i kontroli zarządczej. Odpowiedzi opierają się wyłącznie na dokumentach urzędu i wskazują źródło. Człowiek pozostaje w pętli: AI przygotowuje, urzędnik weryfikuje i podpisuje.

Kontakt:

Fryderyk Pryjma, e-mail: fryderyk.pryjma@cortexmine.com,
tel.: 500 069 552



DroneFort

DroneFort to platforma dowodzenia i kontroli (C2), która daje służbom publicznym i samorządom widok z powietrza dokładnie wtedy, gdy jest najbardziej potrzebny – bez szkoleń i skomplikowanej obsługi. System integruje dowolny sensor – radar, akustykę, RF, kamery, Remote ID – w jeden obraz sytuacyjny. Operator wskazuje miejsce na mapie, dron leci sam i przesyła obraz na żywo w mniej niż 3 minuty.

Kontakt:

Roman Savchuk, e-mail: roman@dronefort.tech, tel.: 505 281 347



Gekko Photonics

Gekko Photonics to wrocławska firma deep-tech z obszaru fotoniki przemysłowej. Buduje analizatory Spectrally™, które mierzą skład chemiczny bezpośrednio w procesie produkcyjnym, w czasie rzeczywistym i bez pobierania ani przygotowania próbek. Wynik jest gotowy w kilka sekund i od razu trafia do automatyki zakładu. System rozpoznaje do 93% substancji występujących w przemyśle chemicznym z dokładnością do pojedynczych ppm i działa jak niezależny dział kontroli jakości: nie tylko mierzy, ale też pomaga sterować procesem.



Kontakt:

Dariusz Gajewicz, e-mail: dariusz.gajewicz@gekkophotonics.com,
tel.: 602 808 995

Mobile Monitoring

Mobile Monitoring rozwija autonomiczne technologie do monitoringu, wykrywania zagrożeń i zwiększania świadomości sytuacyjnej na obszarach wodnych oraz infrastruktury krytycznej. Ich rozwiązania łączą drony nawodne i latające, inteligentne boje pomiarowe, kamery 360° oraz systemy analizy obrazu. Pozwalają automatycznie wykrywać anomalie i potencjalne zagrożenia, prowadzić ciągły monitoring oraz przekazywać operatorom alerty i dane w czasie rzeczywistym. Technologie Mobile Monitoring znajdują zastosowanie m.in. w portach, przemyśle, ochronie środowiska oraz sektorze bezpieczeństwa i obrony.



Kontakt:

Dawid Walczyzna, e-mail: kontakt@mobilemonitoring.pl,
tel.: 728 197 849

Muotech

Muotech to polska spółka DeepTech rozwijająca technologie nieinwazyjnego obrazowania obiektów i infrastruktury. Rozwiązania firmy umożliwiają wykrywanie i lokalizowanie ukrytych elementów oraz uzyskiwanie informacji o wewnętrznej strukturze obiektów bez ich otwierania, demontażu czy ingerencji w konstrukcję. Technologia odpowiada na potrzeby obronności i bezpieczeństwa, gdzie kluczowe znaczenie ma rozpoznanie obiektów niewidocznych z zewnątrz, w tym znajdujących się pod ziemią, wewnątrz konstrukcji lub za osłonami.



Kontakt:

Noemi Zabari, e-mail: noemi@muotech.io, tel.: 790 377 752

Resquant

Resquant to europejska spółka z obszaru cyberbezpieczeństwa, rozwijająca rozwiązania z zakresu kryptografii postkwantowej (Post-Quantum Cryptography, PQC). Firma projektuje technologie umożliwiające ochronę zarówno nowych, jak i istniejących systemów przed zagrożeniami związanymi z rozwojem komputerów kwantowych, oferując własne IP Cores dla układów scalonych oraz sprzętowe rozwiązania do zabezpieczania infrastruktury krytycznej.

Kontakt:

Justyna Pelc, e-mail: contact@resquant.com, tel.: 512 543 418

RIFFSEC

RIFFSEC to system wczesnego ostrzegania przed cyberzagrożeniami, z priorytetem dla rynku europejskiego. Monitoruje internet, deep web, darknet i komunikatory takie jak Telegram, wykrywając wycieki danych, phishing i podszywanie się pod markę, zanim przełożą się na realne straty. Dostarcza zespołom bezpieczeństwa gotowy kontekst, a także pełne feedy informacji, skracając czas reakcji. Wspiera wdrożenie NIS2. Zaufali im m.in. PZU oraz Bankowy Fundusz Gwarancyjny.



Kontakt:

Konrad Latkowski, e-mail: hello@riffsec.com

Sencity

Sencity to CMMS – system zarządzania rozproszonymi zasobami – budujący warstwę cyfrową dla świata fizycznego. Platforma tworzy cyfrowe bliźniaki urządzeń – od publicznych defibrylatorów, przez oświetlenie, po infrastrukturę miejską – i porządkuje cały cykl życia urządzenia: serwis, gwarancje i operacje posprzedażowe w jednym miejscu. Rozwiązanie jest niezależne od hardware'u – integruje urządzenia i czujniki różnych producentów, a operator floty widzi w czasie rzeczywistym stan tysięcy obiektów w terenie, zanim awaria stanie się problemem.

The logo for Sencity, consisting of the word 'SENCITY' in a white, sans-serif font, with a small registered trademark symbol (®) to the upper right. The text is set against a dark grey, rounded rectangular background.

SENCITY®

Kontakt:

Michał Zelek, e-mail: michal.zelek@sencity.ai, tel.: 570 819 931

Autorzy tekstów



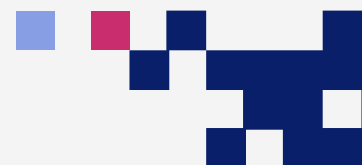
Łukasz Gawron

Prezes Zarządu Polskiego Klastra Cyberbezpieczeństwa #CyberMade-inPoland, związany z organizacją od wielu lat, wcześniej jako wiceprezes. Odpowiada za strategiczne kierunki rozwoju klastra, kluczowe projekty oraz obszar business development, a także reprezentuje interesy firm członkowskich w dialogu z administracją publiczną. Wcześniej koordynował projekt Digital Innovation Hub i zdobywał doświadczenie w organizacjach pozarządowych. Ekspert rynku cyberbezpieczeństwa, prelegent konferencji branżowych oraz autor raportów i opracowań poświęconych rozwojowi sektora. Posiada certyfikaty PRINCE2 Foundation i Agile Foundation oraz uprawnienia Pełnomocnika Zarządu ds. Zintegrowanego Systemu Zarządzania Bezpieczeństwem Informacji. Absolwent stosunków międzynarodowych na Uniwersytecie Jagiellońskim oraz Zarządzania Cyberbezpieczeństwem w Akademii Leona Koźmińskiego.



Piotr Janik

Architekt z wieloletnim doświadczeniem, czynny członek IARP. Specjalizuje się w projektowaniu obiektów laboratoryjnych o szerokim spektrum działania, obiektów zbiorowej ochrony oraz budynków użyteczności publicznej. Współwłaściciel i wiceprezes Archetus Sp. z o.o., dyrektor działu projektowego CCD Skills Sp. z o.o.





Kamil Jenek

Żołnierz, zawodnik mieszanych sztuk walki oraz kwalifikowany pracownik ochrony fizycznej. Absolwent zaawansowanego szkolenia SERE C, skoczek spadochronowy, instruktor strzelectwa bojowego i sportowego, strzelec wyborowy oraz instruktor MMA. Praktyk i szkoleniowiec specjalizujący się w bezpieczeństwie, przygotowaniu do działania w sytuacjach kryzysowych, ochronie ludności i obronie cywilnej oraz budowaniu odporności społecznej. Współzałożyciel CCD Skills oraz Stowarzyszenia Świadoma Obrona Cywilna. Współtwórca pierwszego w Polsce Cywilnego Centrum Działań – miejsca łączącego szkolenia, edukację, przygotowanie operacyjne i praktyczne kompetencje potrzebne do reagowania w sytuacjach zagrożenia.

Bibliografia

Akty prawne

- Protokół dodatkowy I do Konwencji genewskich z 12 sierpnia 1949 r., sporządzony w Genewie dnia 8 czerwca 1977 r.
- Ustawa z dnia 8 marca 1990 r. o samorządzie gminnym, tekst jednolity: Dz.U. z 2026 r. poz. 662.
- Ustawa z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej, tekst jednolity: Dz.U. z 2025 r. poz. 112.
- Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, tekst jednolity: Dz.U. z 2026 r. poz. 574, z późn. zm.
- Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, tekst jednolity: Dz.U. z 2026 r. poz. 20, z późn. zm.
- Rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, Dz.U. z 2024 r. poz. 773.
- Ustawa z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej, Dz.U. z 2024 r. poz. 1907, z późn. zm.
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 21 lutego 2025 r. w sprawie kryteriów uznawania obiektów budowlanych albo ich części za budowle ochronne, Dz.U. z 2025 r. poz. 235.
- Rozporządzenie MSWiA z dnia 1 lipca 2025 r. w sprawie sposobu przygotowania obiektu zbiorowej ochrony do użycia, warunków eksploatacji budowli ochronnych i ich niezbędnego wyposażenia [Dz.U. z 2025 r. poz. 933]
- Rozporządzenie MSWiA z dnia 7 lipca 2025 r. w sprawie Centralnej Ewidencji Obiektów Zbiorowej Ochrony [Dz.U. z 2025 r. poz. 922]
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 9 lipca 2025 r. w sprawie warunków organizowania oraz wymagań, jakie powinny spełniać miejsca doraźnego schronienia, Dz.U. z 2025 r. poz. 932.
- Rozporządzenie Rady Ministrów z dnia 31 lipca 2025 r. w sprawie szczegółowych warunków wyznaczania budynków użyteczności publicznej, w których zapewnia się budowle ochronne, Dz.U. z 2025 r. poz. 1070.
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 4 listopada 2025 r. w sprawie warunków technicznych dla budowli ochronnych oraz warunków technicznych ich użytkowania i usytuowania, Dz.U. z 2025 r. poz. 1548.
- Ustawa z dnia 23 stycznia 2026 r. o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw, Dz.U. z 2026 r. poz. 252.
- Ustawa z dnia 29 maja 2026 r. o zmianie ustawy o zarządzaniu kryzysowym oraz niektórych innych ustaw, Dz.U. z 2026 r. poz. 815.
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 24 czerwca 2026 r. w sprawie szczegółowej organizacji krajowego systemu ratowniczo-gaśniczego, Dz.U. z 2026 r. poz. 872.

Raporty, badania i poradniki

- CBOS, Jonathan Scovil, *O wojnie w Ukrainie i ewentualnym rozszerzeniu konfliktu*, Komunikat z badań nr 48/2024, Warszawa 2024.

- CBOS, *Polacy o Poradniku bezpieczeństwa*, CBOS Flash nr 13/2026, Warszawa 2026.
- CERT Polska, *Raport roczny z działalności CERT Polska w 2025 roku. Krajobraz bezpieczeństwa polskiego Internetu w 2025 roku*, NASK – Państwowy Instytut Badawczy, Warszawa 2026.
- Główny Urząd Statystyczny, *Pomoc udzielona przez gospodarstwa domowe mieszkańcom Ukrainy w I półroczu 2022 r. w świetle wyników badania budżetów gospodarstw domowych*, 27 października 2022 r.
- Główny Urząd Statystyczny, *Zaangażowanie podmiotów gospodarki społecznej w pomoc w związku z działaniami wojennymi na terytorium Ukrainy* [24.02 – 31.03.2022 r.], 5 października 2022 r.
- Ministerstwo Spraw Wewnętrznych i Administracji, Ministerstwo Obrony Narodowej, Rządowe Centrum Bezpieczeństwa, *Poradnik bezpieczeństwa*, Warszawa 2025.
- Najwyższa Izba Kontroli, *Funkcjonowanie systemu łączności w służbach podległych MSWiA*, P/24/033, Warszawa 2025.
- Najwyższa Izba Kontroli, *Zapewnienie obywatelom miejsc schronienia w budowlach ochronnych na wypadek wystąpienia zagrożenia*, P/23/061, Warszawa 2024.

Materiały urzędowe i aktualne programy

- Centrum Projektów Polska Cyfrowa, Dokumentacja naboru FERC.04.01-IP.01-003/26 „Lokalne Centra Cyberbezpieczeństwa”, 2026.
- Gmina Lewin Kłodzki, *Komunikat w sprawie cyberataku na infrastrukturę Urzędu Gminy Lewin Kłodzki*, 5 maja 2026 r.
- Gmina Miejska Nowa Ruda, *Komunikat dotyczący ataku cybernetycznego na infrastrukturę teleinformatyczną Urzędu Miejskiego w Nowej Rudzie*, 24 czerwca 2026 r.
- Komenda Główna Państwowej Straży Pożarnej, *Włączenie jednostek OSP do krajowego systemu ratowniczo-gaśniczego z okazji Narodowego Święta Niepodległości*, 11 listopada 2025 r.
- Ministerstwo Cyfryzacji, *Nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa (KSC) – jak dokonać samoidentyfikacji?*, 27 kwietnia 2026 r.
- Ministerstwo Klimatu i Środowiska, *Bilans pożaru w Puszczy Solskiej – trwa szacowanie strat i planowanie odnowy lasu*, 15 maja 2026 r.
- Ministerstwo Spraw Wewnętrznych i Administracji, *Centra Powiadamiania Ratunkowego*.
- Ministerstwo Spraw Wewnętrznych i Administracji, *Regionalny System Ostrzegania*.
- Państwowe Gospodarstwo Wodne Wody Polskie, *Awaria zbiornika Stronie Śląskie – oświadczenie Wód Polskich*, 24 września 2024 r., aktualizacja 4 lutego 2025 r.
- Rządowe Centrum Bezpieczeństwa, *Alert RCB – najważniejsze pytania i odpowiedzi*.
- Rządowe Centrum Bezpieczeństwa, *Zatwierdzanie planów zarządzania kryzysowego – wyjaśniamy!*, 7 lipca 2026 r.
- Samorząd Województwa Małopolskiego, *Zaktualizowana informacja o naruszeniu ochrony danych osobowych*, 26 października 2021 r.
- Urząd Gminy Obrazów, *Bardzo ważny komunikat. Zawiadomienie o naruszeniu ochrony danych osobowych*, 10 lutego 2026 r.
- Urząd Miasta Myszkowa, *Komunikat w sprawie cyberbezpieczeństwa*, 18 marca 2026 r.



Zastrzeżenie

Publikacja ma charakter informacyjny i edukacyjny. Nie stanowi porady prawnej, technicznej ani specjalistycznej i nie powinna być traktowana jako podstawa do podejmowania decyzji wymagających indywidualnej oceny prawnej, organizacyjnej lub technicznej. Nie zastępuje obowiązujących przepisów prawa, oficjalnych wytycznych, stanowisk właściwych organów ani dokumentacji właściwej dla konkretnego przypadku. Informacje zawarte w publikacji nie mogą być również traktowane jako podstawa do ustalenia stanu prawnego w konkretnej sprawie.

Dołożono wszelkich starań, aby informacje i materiały przedstawione w publikacji były rzetelne, aktualne i możliwie wyczerpujące. Krakowski Park Technologiczny sp. z o.o. oraz autorzy publikacji nie gwarantują jednak ich kompletności, aktualności ani bezbłędności i nie ponoszą odpowiedzialności za ewentualne błędy, braki, nieścisłości lub pomyłki zawarte w publikacji.

Krakowski Park Technologiczny sp. z o.o. oraz autorzy nie ponoszą również odpowiedzialności za skutki działań lub zaniechań podjętych wyłącznie na podstawie informacji zawartych w publikacji. W przypadku zamiaru praktycznego zastosowania informacji przedstawionych w publikacji rekomendowane jest każdorazowe zweryfikowanie ich adekwatności do konkretnego stanu faktycznego oraz skorzystanie z profesjonalnego doradztwa prawnego, technicznego lub innego doradztwa specjalistycznego.

Publikację opracowano według stanu prawnego oraz informacji dostępnych w sierpniu 2026 r. Ze względu na możliwość zmian przepisów, procedur, programów wsparcia, wytycznych, jak również innych danych, aktualność informacji zawartych w publikacji powinna być każdorazowo weryfikowana w oficjalnych źródłach.



Usługa zrealizowana w ramach Zadania: „FORT Kraków Polski Akcelerator DIANA” dofinansowanego w ramach Programu Ministra Finansów i Gospodarki na lata 2025–2029 pn. „Wsparcie kompetencji w obszarze innowacji dual-use” dot. wyłonienia operatora Programu akceleratorycznego DUET - Dual-Use Emerging Technologies. Umowa nr: II/446/P/15011/2830/25/DIP z dnia 05.12.2025.

➔ [KPT.KRAKOW.PL/BEZPIECZNY-SAMORZAD](https://kpt.krakow.pl/bezpieczny-samorzad)



→ FORTKRAKOW.PL

