CC BY NC

Zrecenzowany artykuł naukowy

DOI: 10.54215/BP.2026.10.20.Ostrowska

Bezpieczeństwo pracy w infrastrukturze krytycznej jako element systemu bezpieczeństwa państwa

dr Martyna Ostrowska[a] (ORCID: 0000-0003-4883-5608)



Fot. pvproductions/Magnific

W artykule przeanalizowano znaczenie bezpieczeństwa pracy w infrastrukturze krytycznej jako elementu systemu bezpieczeństwa państwa. Wskazano, że sprawność infrastruktury krytycznej zależy nie tylko od technologii, lecz także od przygotowania pracowników. Omówiono główne zagrożenia (takie jak awarie, cyberataki i katastrofy naturalne) i podkreślono ich kaskadowy charakter. Zwrócono uwagę na niedostateczną integrację bezpieczeństwa pracy z zarządzaniem kryzysowym. Na przykładzie pandemii COVID-19 pokazano, że ochrona personelu jest kluczowa dla utrzymania ciągłości działania. Wnioski podkreślają, że bezpieczeństwo pracy stanowi istotny filar odporności państwa i wymaga dalszego rozwoju.

Słowa kluczowe: infrastruktura krytyczna, bezpieczeństwo państwa

Occupational safety in critical infrastructure as an element of the national security system

The article analyses the importance of occupational safety in critical infrastructure as an element of the national security system. It indicates that the efficiency of critical infrastructure depends not only on technology, but also on the preparedness of employees. The paper discusses the main threats (such as failures, cyberattacks, and natural disasters) and emphasizes their cascading nature. Attention is drawn to the insufficient integration of occupational safety with crisis management. Using the COVID-19 pandemic as an example, it is shown that the protection of staff is crucial for maintaining operational continuity. The conclusions emphasise that occupational safety constitutes an important pillar of national resilience and requires further development.

Keywords: critical infrastructure, national security

[a] Uniwersytet Jana Kochanowskiego w Kielcach, kontakt: martyna.ostrowska@ujk.edu.pl.

Wstęp

Współczesne państwa funkcjonują w warunkach dynamicznie zmieniającego się środowiska bezpieczeństwa. Rosnące znaczenie mają zarówno zagrożenia naturalne, jak i te wynikające z działalności człowieka. Szczególną rolę w zapewnieniu stabilności państwa odgrywa infrastruktura krytyczna, która obejmuje systemy oraz obiekty niezbędne do prawidłowego funkcjonowania gospodarki i społeczeństwa. W konsekwencji zakłócenie lub zniszczenie tej infrastruktury rodzi nie tylko problemy techniczne, lecz także poważne konsekwencje społeczne i gospodarcze.

Jednym z kluczowych elementów funkcjonowania infrastruktury krytycznej jest człowiek, który jako pracownik odpowiada za obsługę, nadzór oraz utrzymanie jej sprawności. Oznacza to, że efektywność działania infrastruktury jest bezpośrednio uzależniona od poziomu bezpieczeństwa pracy i przygotowania personelu. W związku z tym bezpieczeństwo pracy rozumiane jako ogół działań mających na celu ochronę życia i zdrowia pracowników nabiera szczególnego znaczenia [1]. W sektorach infrastruktury krytycznej pracownicy są narażeni na specyficzne zagrożenia. Wynikają one zarówno z charakteru wykonywanych zadań, jak i z potencjalnych sytuacji kryzysowych.

Bezpieczeństwo pracy w infrastrukturze krytycznej stanowi istotny element systemu bezpieczeństwa państwa, ponieważ wpływa bezpośrednio na zdolność do zapewnienia stabilności operacyjnej kluczowych usług. Z tego względu bezpieczeństwo pracy należy traktować nie jako odrębny obszar, lecz jako integralny element systemu bezpieczeństwa państwa. W sytuacjach kryzysowych (takich jak katastrofy naturalne, awarie techniczne, cyberataki czy pandemie) odpowiednie przygotowanie pracowników i skuteczne procedury bezpieczeństwa mogą decydować o ograniczeniu strat oraz szybkim przywróceniu normalnego funkcjonowania państwa.

Celem artykułu jest analiza roli bezpieczeństwa pracy w infrastrukturze krytycznej w systemie bezpieczeństwa państwa, ze szczególnym uwzględnieniem wpływu czynnika ludzkiego na odporność państwa w sytuacjach kryzysowych. Tezą jest stwierdzenie, że bezpieczeństwo pracy w infrastrukturze krytycznej stanowi jeden z kluczowych

filarów systemu bezpieczeństwa państwa, a jego właściwe funkcjonowanie ma istotny wpływ na systemową odporność na sytuacje kryzysowe.

Infrastruktura krytyczna – charakterystyka i znaczenie

Zgodnie z art. 3 pkt 2 ustawy o zarządzaniu kryzysowym [2] przez infrastrukturę krytyczną należy rozumieć obiekty, urządzenia, instalacje, sieci, systemy lub usługi oraz powiązane z nimi funkcjonalnie elementy. Są one niezbędne do realizacji ważnych interesów państwa, funkcjonowania organów administracji publicznej i przedsiębiorstw, zaspokajania potrzeb obywateli oraz zapewnienia świadczenia kluczowych usług. Definicja ta wyraźnie wskazuje, że infrastruktura krytyczna obejmuje nie tylko elementy techniczne, lecz także usługi oraz wzajemne zależności pomiędzy nimi. Odpowiada to współczesnemu rozumieniu bezpieczeństwa państwa.

Nowe brzmienie definicji infrastruktury krytycznej akcentuje jej funkcjonalny charakter. Odejście od wyłącznie sektorowego podejścia pozwala uwzględnić wzajemne zależności pomiędzy poszczególnymi elementami infrastruktury oraz podkreśla ich znaczenie dla zapewnienia ciągłości działania państwa. W praktyce oznacza to, że zakłócenie funkcjonowania jednego systemu może wywołać efekt kaskadowy w innych sektorach, dlatego bezpieczeństwo infrastruktury powinno być analizowane w sposób kompleksowy, obejmujący aspekty techniczne, organizacyjne oraz związane z bezpieczeństwem pracy.

Infrastruktura krytyczna stanowi jeden z podstawowych filarów funkcjonowania współczesnego państwa. Determinuje zarówno poziom bezpieczeństwa obywateli, jak i stabilność systemu gospodarczego [3]. Należy jednak zauważyć, że jej znaczenie jest często analizowane głównie w wymiarze technicznym i organizacyjnym, podczas gdy czynnik ludzki (w tym bezpieczeństwo pracy) pozostaje niedostatecznie eksponowany. Znaczenie infrastruktury krytycznej wynika z faktu, że zapewnia ona ciągłość działania kluczowych usług i systemów, bez czego niemożliwe jest utrzymanie sprawności struktur państwowych oraz prawidłowe funkcjonowanie społeczeństwa [4]. Szczególna rola infrastruktury krytycznej ujawnia się w sytuacjach kryzysowych. W tym kontekście zasadne jest przyjęcie szerszej perspektywy i uwzględnienie nie tylko odporności systemów, lecz także zdolności personelu do ich bezpiecznej obsługi w warunkach presji i zagrożeń. Uszkodzenie lub zakłócenie działania infrastruktury krytycznej może prowadzić do poważnych konsekwencji, w tym zagrożenia życia i zdrowia ludności, strat materialnych oraz destabilizacji procesów społeczno-gospodarczych. W tym kontekście infrastruktura krytyczna powinna być postrzegana nie tylko jako zbiór obiektów i systemów technicznych, lecz jako złożony układ wzajemnie powiązanych elementów warunkujących sprawność i ciągłość funkcjonowania państwa. Istotnym aspektem jest również zdolność infrastruktury krytycznej do zachowania stabilności operacyjnej w warunkach zakłóceń. Oznacza to konieczność podejmowania działań zarówno w zakresie jej ochrony przed zagrożeniami, jak i w obszarze zwiększania odporności (umożliwiającej szybkie reagowanie na awarie, minimalizowanie ich skutków oraz sprawne odtwarzanie utraconych funkcji). Takie podejście pozwala ograniczyć negatywne konsekwencje dla obywateli i gospodarki. Nie bez znaczenia pozostaje także fakt, że znaczna część infrastruktury krytycznej znajduje się w rękach podmiotów prywatnych. Rodzi to istotne wyzwania w zakresie jednolitości standardów bezpieczeństwa pracy, gdyż podmioty te mogą się kierować różnymi priorytetami (od ekonomicznych po regulacyjne). Operatorzy infrastruktury krytycznej funkcjonują często w warunkach presji ekonomicznej, co może prowadzić do ograniczania kosztów związanych z bezpieczeństwem pracy, ze szkoleniami oraz z redundancją systemów. W rezultacie pojawia się konflikt pomiędzy efektywnością ekonomiczną a odpornością infrastruktury krytycznej. Z perspektywy bezpieczeństwa państwa oznacza to ryzyko podporządkowania strategicznych funkcji logice rynkowej. W związku z tym skuteczna ochrona tego obszaru wymaga ścisłej współpracy pomiędzy administracją publiczną a sektorem prywatnym. Brak spójnych mechanizmów nadzoru oraz standaryzacji procedur może skutkować powstawaniem luk w systemie bezpieczeństwa państwa. Koordynacja działań, wymiana informacji oraz wypracowanie wspólnych procedur stanowią kluczowe elementy efektywnego systemu zarządzania kryzysowego. Infrastruktura krytyczna pełni strategiczną funkcję w zapewnieniu bezpieczeństwa państwa oraz jego obywateli. Jej znaczenie wykracza poza wymiar techniczny – obejmuje również aspekty społeczne i ekonomiczne. To czyni jej ochronę jednym z priorytetowych zadań polityki bezpieczeństwa państwa [5].

Nowelizacja ustawy o zarządzaniu kryzysowym [2] wzmacnia podejście oparte na odporności infrastruktury krytycznej i kładzie większy nacisk na analizę zagrożeń, analizę ryzyka, zapewnienie ciągłości działania oraz integrację bezpieczeństwa fizycznego, technicznego, osobowego, teleinformatycznego i organizacyjnego. Jednocześnie rozszerza obowiązki operatorów infrastruktury krytycznej w zakresie identyfikacji zagrożeń oraz planowania działań zapewniających nieprzerwane funkcjonowanie kluczowych systemów. Bezpieczeństwo pracy powinno być zatem traktowane jako integralny element zarządzania infrastrukturą krytyczną już na etapie planowania, projektowania i eksploatacji obiektów. W konsekwencji przestaje ono być wyłącznie elementem ochrony pracowników i staje się jednym z podstawowych instrumentów budowania odporności infrastruktury krytycznej oraz całego systemu bezpieczeństwa państwa.

Zagrożenia dla infrastruktury krytycznej

Infrastruktura krytyczna jest narażona na różnorodne zagrożenia mogące zakłócić funkcjonowanie państwa i podstawowych usług publicznych. Źródłem tych zagrożeń są zarówno zjawiska naturalne, awarie technologiczne, jak i działania człowieka. Mogą one prowadzić do efektów kaskadowych między poszczególnymi sektorami. Dlatego identyfikacja oraz analiza tych zagrożeń są istotnymi elementami budowania odporności infrastruktury krytycznej i skutecznego zarządzania kryzysowego.

Do najważniejszych zagrożeń naturalnych (wynikających z działania sił przyrody), stanowiących istotny czynnik ryzyka dla bezpieczeństwa ludności i funkcjonowania infrastruktury krytycznej należą:

- powodzie – naturalne zjawiska o wysokim potencjale destrukcyjnym, obejmujące zazwyczaj rozległe obszary i powodujące uszkodzenia infrastruktury transportowej (dróg, mostów), energetycznej (stacji transformatorowych), wodno-kanalizacyjnej oraz obiektów użyteczności publicznej. Może to skutkować przerwami w dostawach energii, wody i ograniczeniem dostępu do usług publicznych;
- silne wiatry – zjawiska atmosferyczne o trudnym do przewidzenia zasięgu, które mogą prowadzić do uszkodzeń sieci elektroenergetycznych i telekomunikacyjnych (np. do zerwania linii przesyłowych), a także infrastruktury

transportowej. W konsekwencji dochodzi do zakłóceń w dostawie energii, problemów z łącznością oraz utrudnień logistycznych;
- długotrwałe susze – wpływające przede wszystkim na systemy zaopatrzenia w wodę i na sektor energetyczny (np. ograniczenie możliwości chłodzenia elektrowni), a także na bezpieczeństwo żywnościowe. Skutkiem mogą być niedobory zasobów oraz wzrost kosztów funkcjonowania gospodarki;
- oblodzenia i intensywne opady śniegu – powodujące zakłócenia w funkcjonowaniu systemów transportowych, energetycznych i telekomunikacyjnych. Obciążenie linii przesyłowych lodem i śniegiem prowadzi do ich uszkodzeń, a zaspy oraz oblodzenia utrudniają dostęp do kluczowych obiektów infrastruktury krytycznej. Może to opóźniać działania ratownicze i serwisowe. W rejonach górskich dodatkowym zagrożeniem są natomiast lawiny śnieżne, które mogą niszczyć elementy infrastruktury oraz izolować całe obszary [6].

Uwzględnienie wpływu zagrożeń naturalnych na infrastrukturę krytyczną podkreśla konieczność budowania jej odporności, w tym poprzez odpowiednie planowanie przestrzenne, redundancję systemów i rozwój procedur zarządzania kryzysowego [6].

Zagrożenia w obszarze technologicznym wynikają przede wszystkim z braku alternatywnych dróg transmisji, występowania błędów produkcyjnych lub konstrukcyjnych, a także z niskiej jakości oprogramowania i jego zabezpieczeń. Skutkiem tego może być przejęcie systemu w przypadku awarii lub usterki. Znaczenie mają również odporność technologii i transmisji na zakłócenia (w tym elektromagnetyczne), warunki środowiskowe i czas bezawaryjnej pracy urządzeń [7]. Dla infrastruktury krytycznej szczególnym zagrożeniem jest *blackout*, czyli długotrwała i rozległa awaria systemu elektroenergetycznego prowadząca do przerw w dostawach energii elektrycznej. Jego skutki mają charakter kaskadowy i obejmują zakłócenia funkcjonowania transportu, łączności, systemów teleinformatycznych, ochrony zdrowia i administracji publicznej [8]. W takich warunkach dużego znaczenia nabiera bezpieczeństwo pracy personelu odpowiedzialnego za utrzymanie infrastruktury krytycznej. Dlatego właśnie przygotowanie procedur awaryjnych, zapewnienie zasilania rezerwowego oraz odpowiednie szkolenie pracowników stanowią podstawowe elementy budowania odporności infrastruktury krytycznej i planowania ciągłości działania.

Kolejnym rodzajem są zagrożenia w obszarze danych i sieci, związane z wykorzystywanymi technikami transmisji oraz protokołami przesyłania danych, ze sposobem projektowania i skalowania systemów, standardami implementacyjnymi sprzętu różnych producentów, z brakiem synchronizacji sieci czy wysokim stopniem ich złożoności [7]. Współczesna infrastruktura krytyczna jest silnie uzależniona od systemów teleinformatycznych, w związku z czym rośnie znaczenia cyberbezpieczeństwa. Cyberataki wymierzone w systemy energetyczne, transportowe czy wodociągowe mogą prowadzić do zakłóceń o charakterze kaskadowym. Specyficznymi zagrożeniami są ataki *ransomware*, sabotaż cyfrowy oraz działania hybrydowe prowadzone przez państwa lub grupy przestępcze.

Z kolei zagrożenia wynikające z czynnika ludzkiego obejmują takie działania, jak kradzież, sabotaż czy terroryzm, ale także zachowania wynikające z niezadowolenia pracowników lub obywateli oraz nieświadome błędy użytkowników spowodowane brakiem wiedzy. Do tej grupy zalicza się również niedostateczne regulacje w zakresie bezpieczeństwa, luki prawne, brak wykwalifikowanej kadry zarządzającej oraz niewystarczające szkolenia i działania podnoszące świadomość w zakresie bezpieczeństwa [7].

Analiza zagrożeń wskazuje jednoznacznie, że bezpieczeństwo pracy stanowi element odporności infrastruktury krytycznej. Brak odpowiedniego przygotowania personelu może prowadzić do eskalacji skutków nawet niewielkich zakłóceń. Zagrożenia naturalne dodatkowo potęgują ryzyko destabilizacji systemów. Ich wpływ ujawnia konieczność łączenia podejścia technicznego z organizacyjnym i kadrowym.

Bezpieczeństwo pracy w infrastrukturze krytycznej

Praca w sektorach infrastruktury krytycznej charakteryzuje się wysokim poziomem odpowiedzialności i często podwyższonym ryzykiem zawodowym. Specyfika ta powoduje, że bezpieczeństwo pracy należy rozpatrywać w kontekście szerszym niż standardowe regulacje bhp. Dotyczy to zwłaszcza takich obszarów, jak energetyka, transport, ochrona zdrowia czy systemy teleinformatyczne. Do głównych cech pracy w tych sektorach należą: konieczność zapewnienia stabilności operacyjnej systemów, system zmianowy, narażenie na podwyższony stres oraz kontakt z niebezpiecznymi substancjami lub urządzeniami, odpowiedzialność za bezpieczeństwo dużej liczby osób. Wymagania dotyczące bezpieczeństwa pracy są tu więc znacznie wyższe niż w wielu innych branżach, ponieważ nie ograniczają się wyłącznie do klasycznego rozumienia przepisów bhp, lecz obejmują również przygotowanie pracowników do funkcjonowania w warunkach kryzysowych. W analizie bezpieczeństwa infrastruktury krytycznej często marginalizuje się psychologiczne obciążenie pracowników. Tymczasem długotrwały stres, zmęczenie oraz presja odpowiedzialności mogą się przyczyniać do wzrostu liczby błędów operacyjnych.

Bezpieczeństwo pracy w infrastrukturze krytycznej jest ściśle powiązane z systemem ochrony fizycznej obiektów, obejmującej środki techniczne oraz organizacyjne i fizyczne (w tym kontrolę dostępu, monitoring oraz obecność służb ochrony). Szczególną rolę odgrywają tu pracownicy – będacy zarówno podmiotami ochrony, jak i aktywnymi elementami systemu bezpieczeństwa. Skuteczność działań związanych z ochroną obiektów zależy od właściwego opracowania procedur i poziomu przygotowania personelu do reagowania na sytuacje kryzysowe. W tym kontekście bezpieczeństwo infrastruktury krytycznej należy rozpatrywać w ścisłym powiązaniu z bezpieczeństwem pracy, gdyż ochrona obiektów zapewnia jednocześnie ochronę życia i zdrowia osób w nich zatrudnionych [9].

W literaturze przedmiotu wskazuje się na szereg ograniczeń współczesnego systemu bezpieczeństwa infrastruktury krytycznej. Podkreśla się, że jego konstrukcja ma w dużej mierze charakter formalny. Oznacza to, że przyjęte rozwiązania nie zawsze przekładają się na realną zdolność do reagowania na zagrożenia. Zwraca się również uwagę na brak pełnej integracji pomiędzy poszczególnymi obszarami bezpieczeństwa (w tym z bezpieczeństwem pracy), co może prowadzić do niespójności działań. Problemem jest zwłaszcza niedostateczne uwzględnienie czynnika ludzkiego, mimo że to pracownicy odpowiadają za funkcjonowanie infrastruktury krytycznej i utrzymanie ciągłości jej działania [10].

Zapewnienie ochrony osobowej można rozumieć jako zespół skoordynowanych działań organizacyjnych i technicznych, których celem jest ograniczenie ryzyka zakłócenia funkcjonowania infrastruktury krytycznej, wynikającego z aktywności osób posiadających uprawniony dostęp do jej obiektów. Należy podkreślić, że każda osoba przebywająca w otoczeniu

infrastruktury krytycznej (niezależnie od pełnionej funkcji) może stanowić potencjalne źródło zagrożenia. Dotyczy to zarówno pracowników etatowych, jak i osób trzecich (np. podwykonawców lub gości). Struktura organizacyjna operatora infrastruktury krytycznej oraz zakres obowiązków poszczególnych pracowników określają poziom i zakres dostępu do określonych elementów systemu (w tym obiektów, instalacji, stref i informacji). W konsekwencji właściwe zarządzanie dostępem jest jednym z kluczowych elementów systemu bezpieczeństwa. W budowaniu bezpieczeństwa osobowego ważna jest identyfikacja wizualna personelu oraz pracowników podmiotów współpracujących, ponieważ umożliwia szybkie określenie ich przynależności organizacyjnej i zakresu uprawnień. Rozwiązanie to zwiększa przejrzystość systemu i ułatwia kontrolę dostępu do wrażliwych obszarów infrastruktury. Duże znaczenie ma również właściwe postępowanie w przypadku zakończenia współpracy z pracownikiem. W takiej sytuacji konieczne jest przeprowadzenie indywidualnej oceny ryzyka, obejmującej możliwość ujawnienia informacji lub wykorzystania posiadanej wiedzy. Równocześnie niezbędne jest niezwłoczne odebranie wszelkich uprawnień dostępowych, w tym dezaktywacja kart identyfikacyjnych, haseł i dostępów do systemów teleinformatycznych [10].

Analiza przypadku

Analizę przypadku, pokazującą rzeczywisty związek pomiędzy bezpieczeństwem pracy, zarządzaniem kryzysowym i odpornością państwa na sytuacje nadzwyczajne, przeprowadzono na przykładzie pandemii COVID-19. Wywołała ona kryzys, który ujawnił znaczenie bezpieczeństwa pracy dla funkcjonowania infrastruktury krytycznej. Sytuacja ta pokazała, że zapewnienie ciągłości działania kluczowych systemów państwa zależy nie tylko od rozwiązań technicznych, lecz także od odpowiedniego przygotowania i ochrony personelu.

Kluczowym warunkiem skutecznego reagowania na wywołany pandemią kryzys, który generował istotne zagrożenia dla szeroko rozumianego bezpieczeństwa i dobrostanu społecznego, było ograniczenie transmisji wirusa. W związku z tym za priorytet uznano zapewnienie ciągłości działania infrastruktury krytycznej.

Uwzględniając te uwarunkowania, 16 marca 2020 r. (w krótkim czasie od identyfikacji pierwszych przypadków zakażeń w Polsce) opracowano „Wytyczne dla operatorów infrastruktury krytycznej w zakresie działań prewencyjnych zapobiegających rozprzestrzenianiu się koronawirusa SARS-CoV-2". Dokument ten zawierał zestaw rekomendacji skierowanych do operatorów (właścicieli) obiektów infrastruktury krytycznej i określał metody zapewnienia bezpiecznych warunków pracy oraz ciągłości operacyjnej [11]. Wskazywał zwłaszcza na konieczność:

- realizacji działań informacyjno-edukacyjnych wśród personelu, obejmujących zagadnienia związane z mechanizmami transmisji wirusa, okresem inkubacji, symptomatologią oraz zasadami postępowania minimalizującymi ryzyko zakażenia (w tym ze stosowaniem indywidualnych środków profilaktycznych);
- wprowadzenia zmian organizacyjnych w środowisku pracy oraz wdrożenia dodatkowych środków bezpieczeństwa, takich jak: upowszechnienie pracy zdalnej, ograniczenie bezpośrednich kontaktów interpersonalnych między pracownikami, uregulowanie zasad spożywania posiłków oraz zredukowanie liczby interakcji w przestrzeniach wspólnych;
- kontroli i ograniczenia liczby punktów wejścia i wjazdu na teren obiektów infrastruktury krytycznej, w połączeniu z wdrożeniem obowiązkowych procedur dezynfekcji rąk i pomiaru temperatury ciała osób wchodzących;
- zwiększenia częstotliwości dezynfekcji i utrzymania wysokiego standardu czystości powierzchni użytkowych, ze szczególnym uwzględnieniem miejsc o zwiększonym natężeniu kontaktów;
- opracowania i wdrożenia szczegółowych procedur postępowania w przypadku identyfikacji u pracownika objawów wskazujących na potencjalne zakażenie wirusem (zarówno na terenie obiektu, jak i poza nim), w tym określenia zasad organizacji kwarantanny w miejscu pracy [12].

Sformułowane rekomendacje pozostawały zgodne z wytycznymi Głównego Inspektora Sanitarnego, jednak ze względu na strategiczne znaczenie infrastruktury krytycznej wymagały rozszerzenia o dodatkowe środki. Dokument stanowił wyraźny impuls do aktualizacji planów ochrony infrastruktury krytycznej (POIK) zatwierdzanych przez Rządowe Centrum Bezpieczeństwa (RCB) i podlegających okresowej weryfikacji. Pandemia COVID-19 ujawniła ograniczoną gotowość operatorów infrastruktury krytycznej do funkcjonowania w warunkach długotrwałego kryzysu epidemiologicznego. Szczególnie widoczne były problemy związane z ochroną personelu, niedoborami kadrowymi i koniecznością szybkiej reorganizacji pracy. Istotne stało się również zapewnienie ciągłości działania poprzez weryfikację scenariuszy operacyjnych i identyfikację ról o krytycznym znaczeniu. Rekomendacje RCB podkreślały konieczność bieżącego monitorowania adekwatności planów ciągłości działania w sytuacji ograniczonej dostępności pracowników oraz wdrażania działań korygujących w przypadku wystąpienia zakłóceń operacyjnych [12].

Ponadto operatorom infrastruktury krytycznej zalecono wcześniejsze przygotowanie się na tzw. scenariusz skrajny, zakładający konieczność całkowitego opuszczenia obiektu przez personel, oraz opracowanie adekwatnych procedur postępowania w takiej sytuacji. Alternatywnie rekomendowano wdrożenie modelu pracy zdalnej na szeroką skalę. Polegał on na pozostawieniu w obiekcie jedynie minimalnej, niezbędnej obsady operacyjnej (tzw. załogi szkieletowej), przy jednoczesnym skierowaniu pozostałych pracowników do wykonywania obowiązków w trybie zdalnym. W celu zapewnienia ciągłości świadczenia usług operatorom, którzy dysponowali odpowiednimi zasobami organizacyjnymi i technicznymi, sugerowano uruchomienie równoległego, zapasowego stanowiska kierowania. Jednocześnie wskazano na zasadność podziału służb dyspozytorskich na dwa odrębne zespoły operacyjne, funkcjonujące w reżimie ścisłej separacji (z wykluczeniem bezpośrednich kontaktów interpersonalnych między ich członkami) [12].

Omawiane wytyczne miały charakter niewiążących zaleceń i okazały się niewystarczające dla zapewnienia pełnej skuteczności działań, co implikowało konieczność wprowadzenia dodatkowych rozwiązań o charakterze normatywnym. Niezbędne było zwłaszcza ustanowienie podstaw prawnych umożliwiających realizację działań gwarantujących ciągłość funkcjonowania operatorów infrastruktury krytycznej w warunkach pandemii COVID-19. Początkowe regulacje prawne, wprowadzone w ramach tzw. Tarczy Antykryzysowej 1.0 [13], nie przewidywały instrumentów wspierających operatorów infrastruktury krytycznej w organizacji działań ochronnych. Dopiero nowelizacja tej ustawy [14] wprowadziła przepisy umożliwiające modyfikację systemu i rozkładu czasu pracy pracowników w warunkach stanu zagrożenia epidemicznego lub stanu epidemii. Celem tych regulacji

było zwiększenie odporności infrastruktury krytycznej poprzez ochronę kluczowego zasobu, jakim jest personel. Jednocześnie rozszerzono zakres oddziaływania przepisów ustawy na podmioty współpracujące (podwykonawców, dostawców), które formalnie nie należą do infrastruktury krytycznej, jednak odgrywają istotną rolę w zapewnieniu ciągłości jej funkcjonowania [12].

Na podstawie znowelizowanej Tarczy Antykryzysowej 1.0 [13, 14] pracownicy obiektów infrastruktury krytycznej oraz podmiotów powiązanych mogli zostać objęci tzw. skoszarowaniem, polegającym na czasowej izolacji w miejscu pracy. W takiej sytuacji na pracodawcy spoczywał obowiązek zapewnienia pracownikom odpowiednich warunków zakwaterowania oraz wyżywienia, niezbędnych do wykonywania obowiązków służbowych. Ponadto przepisy te przyznały pracodawcom dodatkowe uprawnienia organizacyjne, obejmujące możliwość [12]:

- zobowiązania pracowników do świadczenia pracy w godzinach nadliczbowych w zakresie koniecznym dla utrzymania ciągłości funkcjonowania przedsiębiorstwa lub instalacji;
- odmowy udzielenia urlopu wypoczynkowego (w tym na żądanie), urlopu bezpłatnego lub innej formy zwolnienia od pracy oraz zmiany terminów wcześniej zaplanowanych urlopów;
- odwołania pracownika z już rozpoczętego urlopu, jeśli taki wymóg wynikał z potrzeb operacyjnych związanych z zapewnieniem ciągłości działania.

Analiza regulacji prawnych i wytycznych dotyczących operatorów infrastruktury krytycznej byłaby niepełna bez uwzględnienia zaleceń opracowanych przez Ministerstwo Aktywów Państwowych oraz Ministerstwo Klimatu i RCB [15], bazujących na wytycznych Ministerstwa Rozwoju i Głównego Inspektoratu Sanitarnego. Dokument ten został przekazany 3 września 2020 r. przez Departament Bezpieczeństwa i Zarządzania Kryzysowego Ministerstwa Aktywów Państwowych do operatorów infrastruktury krytycznej sektora energetycznego, w tym operatorów systemów dystrybucyjnych, oraz do operatora systemu przesyłowego. Zawarte w nim zalecenia koncentrowały się na czterech zasadniczych obszarach [15]:

- wzmocnieniu bezpieczeństwa pracowników, podmiotów współpracujących oraz interesantów poprzez wdrożenie szczegółowych procedur organizacyjnych i sanitarnych;
- minimalizacji ryzyka transmisji zakażeń w środowisku pracy;
- ograniczeniu liczby kontaktów interpersonalnych w określonych przedziałach czasowych;
- wdrożeniu działań przeciwepidemicznych adekwatnych do aktualnej sytuacji epidemicznej.

Wybuch pandemii COVID-19 uwidocznił ograniczenia istniejących systemów bezpieczeństwa pracy, które w wielu przypadkach nie były przygotowane na długotrwałe zagrożenie o charakterze globalnym. Reakcje operatorów infrastruktury krytycznej często miały charakter reaktywny (a nie systemowy), co wskazuje na niedostateczny poziom wcześniejszego przygotowania. Można zatem stwierdzić, że pandemia była testem odporności – nie tylko infrastruktury technicznej, lecz przede wszystkim infrastruktury organizacyjnej oraz kadrowej. System ochrony infrastruktury krytycznej był w tamtym czasie przygotowany głównie na zagrożenia krótkoterminowe i lokalne, natomiast w ograniczonym stopniu uwzględniał możliwość wystąpienia długotrwałego kryzysu globalnego.

Podsumowanie

Bezpieczeństwo pracy w infrastrukturze krytycznej stanowi istotny, choć często niedoceniany element systemu bezpieczeństwa państwa.

Przeprowadzona analiza wskazuje, że mimo istnienia rozbudowanych regulacji prawnych i procedur organizacyjnych obszar ten nadal wymaga doskonalenia (zwłaszcza w zakresie integracji z zarządzaniem kryzysowym). Kluczowe znaczenie ma uwzględnienie zasobów ludzkich jako elementu strategicznego, a nie jedynie wykonawczego. Biorąc pod uwagę współczesne zagrożenia (cyberataki, pandemie, konflikty zbrojne itd.), to właśnie przygotowanie pracowników oraz ich bezpieczeństwo warunkują zdolność państwa do utrzymania ciągłości działania infrastruktury krytycznej. Można więc uznać, że ciągły rozwój systemów bezpieczeństwa pracy powinien być jednym z priorytetów polityki bezpieczeństwa państwa.

Problemem wciąż pozostaje niedostateczna integracja systemów bezpieczeństwa pracy z planowaniem kryzysowym oraz ograniczony poziom praktycznych szkoleń personelu. W konsekwencji wiele procedur ma charakter formalny i nie zawsze przekłada się na rzeczywistą odporność organizacyjną.

W perspektywie kolejnych lat znaczenie bezpieczeństwa pracy w infrastrukturze krytycznej będzie wzrastać wraz z postępującą cyfryzacją i automatyzacją procesów. Jednocześnie będzie się zwiększać podatność systemów na cyberzagrożenia i działania hybrydowe. Oznacza to konieczność odejścia od tradycyjnego postrzegania bezpieczeństwa pracy wyłącznie jako obszaru regulacji bhp i włączenia go do strategicznego systemu bezpieczeństwa państwa.

BIBLIOGRAFIA

[1] Wróbel A., *Bezpieczeństwo i higiena pracy – pojęcie i odpowiedzialność*, „Acta Universitatis Wratislaviensis. Przegląd Prawa i Administracji", 2014, 96: 93–100.

[2] Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (t.j. Dz.U. z 2026 r. poz. 574 z późn. zm.).

[3] Jakubiak E., *Ochrona infrastruktury krytycznej w Polsce*, „Zeszyty Naukowe SGSP", 2018, 66: 167–175.

[4] Żuber M., *Infrastruktura krytyczna państwa jako obszar potencjalnego oddziaływania terrorystycznego*, „Rocznik Bezpieczeństwa Międzynarodowego", 2014, 8(2): 178–197.

[5] *Systemy infrastruktury krytycznej*, Rządowe Centrum Bezpieczeństwa, 2024; https://www.gov.pl/web/rcb/systemy-infrastruktury-krytycznej.

[6] Milewski J., *Identyfikacja infrastruktury krytycznej i jej zagrożeń*, „Zeszyty Naukowe AON", 2016, 4 (105): 99–115.

[7] Ciekanowski Z., Żurawski S., Wyrębek H., *Zagrożenia infrastruktury krytycznej*, „Studia Administracji i Bezpieczeństwa", 2022, 13(13): 263–272.

[8] *Długotrwały brak prądu (blackout)*; https://www.gov.pl/web/poradnikbezpieczenstwa/dlugotrwaly-brak-pradu-blackout.

[9] Panasiuk A., Sierański S., *Ochrona obiektów infrastruktury krytycznej*, „Kontrola Państwowa", 2017, 62: 76–86.

[10] Banasik M., Bagińska J., *Krytyczne uwagi dotyczące bezpieczeństwa infrastruktury krytycznej*, „Rocznik Bezpieczeństwa Międzynarodowego", 2019, 13(2): 69–88.

[11] *Wytyczne dla operatorów infrastruktury krytycznej w zakresie działań prewencyjnych zapobiegających rozprzestrzenianiu się koronawirusa SARS-CoV-2*, Warszawa: Rządowe Centrum Bezpieczeństwa, 2020; https://www.gov.pl/web/aktywa-panstwowe/zalecenia-zwiazane-z-epidemia-sars-cov-2.

[12] Wróbel R., Wróbel I.K., *Critical Infrastructure in Poland during the COVID-19 Pandemic*, „Safety & Fire Technology", 2021, 57(1): 50–62.

[13] Ustawa z dnia 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych (Dz.U. poz. 374).

[14] Ustawa z dnia 31 marca 2020 r. o zmianie ustawy o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych oraz niektórych innych ustaw (Dz.U. poz. 568).

[15] Zalecenia Ministra Aktywów Państwowych, Ministra Klimatu oraz Dyrektora Rządowego Centrum Bezpieczeństwa dla urzędów i instytucji państwowych, jednostek podległych i nadzorowanych przez Ministra Aktywów Państwowych i Ministra Klimatu oraz operatorów infrastruktury krytycznej z systemu zaopatrzenia w energię, surowce energetyczne i paliwa, a także Operatorów Systemów Dystrybucyjnych i Operatora Systemu Przesyłowego; https://www.gov.pl/web/klimat/zalecenia-dla-urzedow-i-instytucji-panstwowych-w-trakcie-epidemii-sars-cov-2-w-polsce.