Zeszyty Naukowe SGSP 2022, Nr 83, s. 141–161
ISSN: 0239-5223; e-ISSN: 2720-0779

DOI: 10.5604/01.3001.0016.0229

dr Robert Wódkiewicz
e-mail: robertwww@wp.pl
ORCID: 0000-0001-6074-5969

PODSTAWOWE ZAGROŻENIA FUNKCJONOWANIA OBIEKTÓW INFRASTRUKTURY KRYTYCZNEJ

Abstrakt

W artykule przedstawiono etymologię pojęcia infrastruktury krytycznej oraz rolę obiektów infrastruktury krytycznej w funkcjonowaniu gospodarki narodowej. W dalszej części artykułu omówiono pojęcie zagrożenia oraz podstawowe zagrożenia, na jakie narażony jest obiekt infrastruktury krytycznej, w tym zagrożenia naturalne i spowodowane działalnością człowieka.
Celem artykułu jest przybliżenie najistotniejszych zagrożeń funkcjonowania obiektów infrastruktury krytycznej z położeniem akcentu na jedno z najważniejszych zagrożeń dla obiektu przemysłu rafineryjnego, to jest pożaru.

Słowa kluczowe: infrastruktura krytyczna, gospodarka narodowa, zagrożenia, system

BASIC THREATS TO THE FUNCTIONING OF THE CRITICAL INFRASTRUCTURE FACILITIES

Abstract

The article presents the etymology of the concept of critical infrastructure and the role of critical infrastructure facilities in the functioning of the national economy. The article goes on to discuss the concept of threat and the primary threats to which a critical infrastructure facility is exposed, including natural and man-made hazards.
The aim of the article is to present the most important threats to the operation of critical infrastructure facilities, with the emphasis on one of the most important threats to the refinery industry facility, i.e. fire.

Keywords: critical infrastructure, national economy, threats, system

Wstęp

Pojęcie infrastruktury krytycznej jest terminem stosunkowo nowym, którego znaczenie w ciągu ostatnich lat nabrało dużego znaczenia. Przyczynę tego zjawiska stanowi wzrastające napięcie związane z możliwością wystąpienia ataków terrorystycznych, które mogą być ukierunkowane nie tylko na ludność cywilną danego państwa, ale przede wszystkim na pozbawienie zdolności funkcjonalnych infrastruktury krytycznej. Częściowe bądź całkowite zniszczenie infrastruktury krytycznej państwa powoduje jego paraliż i prowadzi do pozbawienia społeczeństwa dostępu między innymi do energii, zaopatrzenia w wodę i żywność oraz np. do utraty łączności w przypadku zniszczenia przekaźników sieci komórkowych.

Termin „infrastruktura" pojawił się w NATO na przełomie lat pięćdziesiątych i sześćdziesiątych ubiegłego wieku do oznaczenia obiektów trwałego użytku (koszar, lotnisk itp.). Szybko rozpowszechnił się także poza środowiskiem wojskowym, wchodząc na stałe do literatury ekonomicznej [26, s. 28]. Militarne rozumienie pojęcia infrastruktury podaje również *Encyklopedia Webstera*, w której oznacza ona między innymi „system baz, usług, szkoleń niezbędny dla wykorzystania przez wojsko w działaniach operacyjnych lub podstawowy zakres każdej organizacji" [2, s. 10]. Kolejną definicję infrastruktury, która wiąże się z obronnością, można znaleźć w *Leksykonie wiedzy wojskowej*. Określa on infrastrukturę obronną jako urządzenia i instytucje warunkujące skuteczne działanie systemu obronnego państwa [13, s. 145]. W *Słowniku terminów z zakresu bezpieczeństwa narodowego* infrastruktura obronna to część infrastruktury państwa, obejmująca obiekty i urządzenia stałe oraz instytucje niezbędne do funkcjonowania systemu obronnego państwa. Tworzona jest głównie w czasie pokoju, ale rozwijana również w okresie zagrożenia i wojny [28, s. 48].

Inną, odmienną definicję pojęcia „infrastruktury krytycznej" przedstawił W. Wójtowicz, który stwierdził, że „pewna infrastruktura narodowa jest tak życiowo istotna, że jej niesprawność lub zniszczenie osłabiłoby bezpieczeństwo obronne i ekonomiczne państwa, i w tym sensie czyniło ją «krytyczną»" [35, s. 12]. Prawo Unii Europejskiej określa infrastrukturę krytyczną jako składnik, system lub część infrastruktury zlokalizowanej na terytorium państw członkowskich, które mają podstawowe znaczenie dla utrzymania niezbędnych funkcji społecznych, zdrowia, bezpieczeństwa, ochrony, dobrobytu materialnego lub społecznego ludności oraz których zakłócenie lub zniszczenie miałoby istotny wpływ na dane państwo członkowskie w wyniku utracenia tych funkcji [40]. W Polsce termin „infrastruktura krytyczna" pojawił się w 2002 r. w związku z pracami prowadzonymi w ramach NATO [26, s. 51]. Jedną z pierwszych definicji zaproponował W. Wojciechowicz, który określał ją jako zespół podstawowych urządzeń i instytucji usługowych niezbędnych do należytego funkcjonowania produkcyjnych działów gospodarki [32]. Definicja infrastruktury krytycznej została zawarta w ustawie z 26 kwietnia 2007 r. o zarządza-

niu kryzysowym (ustawa o zarządzaniu kryzysowym). Za infrastrukturę krytyczną uznaje ona systemy i wchodzące w ich skład obiekty, kluczowe dla bezpieczeństwa państwa i jego obywateli, w tym zapewniające ciągłość działania organów administracji publicznej, instytucji i przedsiębiorców. Ponadto obejmuje ona następujące systemy: zaopatrzenia w energię, surowce energetyczne i paliwa, łączności, sieci teleinformatycznych, finansowe, zaopatrzenia w żywność, zaopatrzenia w wodę, ochrony zdrowia, transportowe, ratownicze, zapewniające ciągłość działania administracji publicznej oraz produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych.

Infrastruktura krytyczna jest nierozerwalnie związana z zarządzaniem kryzysowym, ponieważ w przypadku jej awarii, ataków na nią lub też innych zdarzeń powodujących zakłócenie jej działania uruchamiane są odpowiednie procedury w ramach przedsięwzięć reagowania kryzysowego.

Wagę zagadnienia ochrony infrastruktury krytycznej podkreśla fakt umieszczenia informacji na jej temat w Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej.

1. Rola obiektów infrastruktury krytycznej w funkcjonowaniu gospodarki narodowej

Państwo ma wspierać operatorów infrastruktury krytycznej oraz tworzyć warunki do jej ochrony. Współczesne państwo, realizując swoje podstawowe funkcje, koncentruje się na tych kwestiach. Z sześciu obszarów wewnętrznej aktywności państwa połowa funkcji odwołuje się bezpośrednio do problematyki bezpieczeństwa i jest ściśle powiązana z infrastrukturą. Elementami tymi są: zapewnienie porządku i bezpieczeństwa publicznego, ochrona mienia i zdrowia obywateli, działania na rzecz zapewnienia zewnętrznego bezpieczeństwa państwa. Realizacja pozostałych, to jest zabezpieczenie występującego w państwie systemu własności, utrzymywanie i rozwijanie stosunków z innymi państwami czy działania sprzyjające przepływowi informacji oraz kontaktom międzyludzkim, jest pośrednio zależna od infrastruktury technicznej oraz stworzonego i gwarantowanego przez państwo systemu prawnego. Można więc wskazać, że funkcjonowanie społeczeństwa i państwa jest zależne od infrastruktury, a stopień jej rozwoju wpływa na skuteczność i efektywność realizowanych przez to państwo zadań. W konsekwencji – rozwój technologiczny tworzy system współzależności i wzajemnego oddziaływania pomiędzy państwem a infrastrukturą [25, s. 14].

Zgodnie z art. 5b ust. 1 ustawy o zarządzaniu kryzysowym Rada Ministrów uchwałą z 26 marca 2013 r. przyjęła pierwszy Narodowy Program Ochrony Infrastruktury Krytycznej (NPOIK), określając w nim ministrów odpowiedzialnych za poszczególne systemy infrastruktury krytycznej. Kolejne wersje NPOIK przyjęto

uchwałą Rady Ministrów Nr 210/2015 z 2 listopada 2015 r. – NPOIK 2015, uchwałą Rady Ministrów Nr 121/2018 z 7 września 2018 r. – NPOIK 2018 oraz uchwałą Nr 116/2020 Rady Ministrów z 13 sierpnia 2020 r. – NPOIK 2020. Aktualizacja NPOK wynikała z konieczności dostosowania jego treści do zmian w strukturze działów administracji rządowej. Celem NPOIK jest stworzenie warunków do poprawy bezpieczeństwa infrastruktury krytycznej. Wraz z innymi dokumentami programowymi składa się na cel nadrzędny, który stanowi podniesienie bezpieczeństwa Rzeczypospolitej Polskiej.

Infrastruktura krytyczna służy do zaspokojenia potrzeb wszystkich obywateli. Nadrzędnym jej celem jest utrzymanie ciągłości świadczenia usług kluczowych dla państwa. Główny wysiłek realizacji NPOIK spoczywa na Rządowym Centrum Bezpieczeństwa (RCB), ministrach odpowiedzialnych za systemy infrastruktury krytycznej oraz operatorach infrastruktury krytycznej (właściciel oraz posiadacz samoistny i zależny obiektów, instalacji, urządzeń i usług infrastruktury krytycznej) [43] wyszczególnionych w wykazie infrastruktury krytycznej. Najlepszą wiedzę i warunki do ograniczenia zagrożeń dla infrastruktury krytycznej oraz zmniejszenia jej podatności na te zagrożenia mają operatorzy infrastruktury krytycznej. Zobowiązani są oni między innymi do przygotowania i wdrożenia, stosownie do przewidywanych zagrożeń, planów ochrony infrastruktury krytycznej oraz utrzymywania własnych systemów rezerwowych zapewniających bezpieczeństwo i podtrzymujących funkcjonowanie tej infrastruktury do czasu jej pełnego odtworzenia, a także do niezwłocznego przekazywania Szefowi Agencji Bezpieczeństwa Wewnętrznego informacji dotyczących zagrożeń o charakterze terrorystycznym dla infrastruktury krytycznej.

Systemy infrastruktury krytycznej różnią się między sobą charakterystyką funkcjonowania, uwarunkowaniami prawnymi oraz użytkownikami tych systemów, dlatego NPOIK wskazuje ministrów odpowiedzialnych za poszczególne systemy. Odpowiedzialność ta polega w szczególności na wsparciu RCB w budowie systemu ochrony infrastruktury krytycznej, inicjowaniu zmian aktów prawnych w celu ułatwienia i wsparcia wykonywania zadań z zakresu ochrony infrastruktury krytycznej, współpracy z organami, w kompetencji których znajdują się sprawy dotyczące części składowych systemu infrastruktury krytycznej, niebędących bezpośrednio we właściwości koordynatora oraz współpracy z operatorami infrastruktury krytycznej w zakresie jej ochrony, animowanie tej współpracy i jej podtrzymywanie [43].

Istotną rolę w realizacji zadań na rzecz ochrony infrastruktury krytycznej odgrywa Prezydent Rzeczypospolitej Polskiej. Ze względu na posiadane kompetencje w obszarze bezpieczeństwa państwa jest gwarantem zaangażowania władz państwa w proces poprawy poziomu bezpieczeństwa infrastruktury krytycznej, a co za tym idzie – również całego państwa. Prezydent uczestniczy w NPOIK w zakresie swoich konstytucyjnych kompetencji, obejmujących bezpieczeństwo narodowe i obronność. Wspiera również administrację rządową i samorządową w działaniach na rzecz ochrony infrastruktury krytycznej.

Rola Rady Ministrów jest równie znacząca. Przyjmuje ona w drodze uchwały NPOIK, a poprzez podległe jej organy i podmioty oraz Rządowy Zespół Zarządzania Kryzysowego czuwa nad przestrzeganiem zasad i wypełnieniem postanowień NPOIK, wspiera i promuje działania na rzecz osiągnięcia celów NPOIK oraz umożliwia uzyskanie środków finansowych na ochronę infrastruktury krytycznej, uwzględniając te zadania w budżecie państwa.

Istotną rolę w systemie ochrony infrastruktury krytycznej pełnią służby specjalne – Agencja Bezpieczeństwa Wewnętrznego (ABW), Agencja Wywiadu (AW), a także wojskowe służby specjalne: Służba Kontrwywiadu Wojskowego (SKW) oraz Służba Wywiadu Wojskowego (SWW). Dysponują bowiem potencjałem ludzkim i technicznym, wystarczającym do zidentyfikowania potencjalnych zagrożeń infrastruktury krytycznej. Wymiana informacji o tych zagrożeniach z operatorami infrastruktury krytycznej i innymi podmiotami właściwymi w sprawach ochrony infrastruktury krytycznej (z zachowaniem przepisów o ochronie informacji niejawnych) jest priorytetem w procesie planowania ochrony infrastruktury krytycznej [17, s. 24]. Szczególną rolę odgrywa ABW. Jej szefowi organy administracji publicznej, właściciele i posiadacze obiektów, urządzeń infrastruktury krytycznej przekazują informacje dotyczące zagrożeń o charakterze terrorystycznym dla infrastruktury krytycznej. W przypadku powzięcia informacji o możliwości wystąpienia zdarzenia o charakterze terrorystycznym zagrażającego infrastrukturze krytycznej Szef ABW może wydawać polecenia organom administracji publicznej, właścicielom i posiadaczom obiektów, urządzeń infrastruktury krytycznej. Mają one na celu przeciwdziałanie zagrożeniom, ich usunięcie albo minimalizację oraz przekazywanie im niezbędnych do tego celu informacji [17, s. 24].

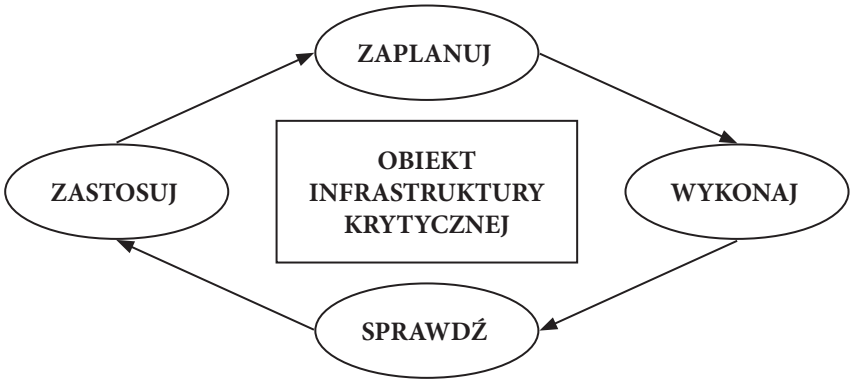
Infrastruktura krytyczna zlokalizowana jest na terenie gmin, miast i powiatów. Z tego względu starostowie, wójtowie, burmistrzowie i prezydenci miast odgrywają ważną rolę w zakresie ochrony ludności narażonej na potencjalne skutki zakłócenia funkcjonowania infrastruktury krytycznej oraz w zakresie ochrony infrastruktury krytycznej, umożliwiając jak najszybsze wsparcie jej operatorów. Ich zadania obejmują między innymi ujęcie w planach zarządzania kryzysowego zadań z zakresu ochrony infrastruktury krytycznej zlokalizowanej w obszarze ich właściwości, określenie procedur reagowania na wypadek zniszczenia lub zakłócenia funkcjonowania infrastruktury krytycznej w obszarze właściwości oraz ochronę ludności przed skutkami zakłócenia funkcjonowania infrastruktury krytycznej z wykorzystaniem zasobów własnych oraz operatora infrastruktury krytycznej.

Ochrona infrastruktury krytycznej to długofalowy, skomplikowany proces zapewnienia jej bezpieczeństwa. Składa się on między innymi ze wskazania zakresu celów, które należy osiągnąć w ramach ochrony infrastruktury krytycznej oraz adresatów tych działań, oceny ryzyka i identyfikacji krytycznych zasobów, funkcji oraz określenia sieci powiązań z innymi systemami infrastruktury krytycznej, w tym podmiotami i organami, a także z rozwoju i wdrożenia systemu ochrony in-

frastruktury krytycznej, w tym opracowania i akceptacji planów ochrony i odtwarzania infrastruktury krytycznej. W jego skład wchodzi również testowanie (przez ćwiczenia) i przegląd (przez audyt i samoocenę) systemu ochrony infrastruktury krytycznej oraz pomiaru postępów na drodze do osiągnięcia celu [17, s. 27].

Konieczność nieustannego doskonalenia procesu ochrony infrastruktury krytycznej pozwala na jego ujęcie w cykl Deminga. Wersja popularna tego cyklu składa się z działań następujących po sobie w porządku logicznym: zaplanuj (wskaż zakres, cele do osiągnięcia w ramach ochrony infrastruktury krytycznej oraz adresatów), wykonaj (zidentyfikuj krytyczne zasoby, funkcje oraz zależności, dokonaj oceny ryzyka, wskaż priorytety działania, opracuj i wdróż system ochrony infrastruktury krytycznej), sprawdź (testuj i przeglądaj system ochrony infrastruktury krytycznej), zastosuj (doskonal, wprowadzając modyfikacje i korekty). Według encyklopedii zarządzania cykl Deminga to koncepcja z zakresu zarządzania jakością, zwana także kołem Deminga, cyklem poprawy lub cyklem PDCA. PDCA jest skrótem pochodzącym od pierwszych liter angielskich słów: Plan, Do, Check, Action, które oznaczają kolejno: planowanie, wykonanie, sprawdzenie (kontrolę) i działanie [44].

Pętla Deminga zakłada cykliczną realizację wyżej wymienionych etapów, a kolejne powtórzenia cyklu przybliżają do osiągnięcia coraz to większego poziomu ochrony infrastruktury krytycznej. Staje się ona mniej podatna na wszelkiego rodzaju zagrożenia.



Rys. 1. Proces ochrony IK w cyklu Deminga

Źródło: [17, s. 28]

W załączniku niejawnym do NPOIK zawarty jest wykaz obiektów wchodzących w skład infrastruktury krytycznej w podziale na województwa oraz systemy [17, s. 48].

W literaturze przedmiotu można znaleźć wiele podziałów sektorów infrastruktury krytycznej. Jeden z nich zaproponował M. Żmigrodzki.

Tab. 1. Wykaz sektorów infrastruktury krytycznej

Sektor	Składniki sektorów
Energia	gaz, ropa naftowa, paliwa płynne; urządzenia do wydobywania, przetwarzania i przechowywania gazu, paliw płynnych i ropy naftowej; elektrownie; energetyczne sieci transmisyjne i dystrybucyjne dostarczające różnego rodzaju energię
Woda	zasoby wodne, zbiorniki wodne, rezerwuary wodne; systemy transportujące i dostarczające wodę do użytkowania w różnym celu; urządzenia do filtrowania, uzdatniania wody i systemy kontroli jakości wód; oczyszczalnie ścieków
Transport	transport drogowy wraz ze wszystkimi rodzajami dróg, samochody osobowe i ciężarówki; transport kolejowy wraz z sieciami kolejowymi, stacjami i taborem kolejowym; linie lotnicze, lotniska i samoloty; transport morski i oceaniczny oraz śródlądowy wraz z flotą i portami; system dystrybucji towarów krytycznych
Systemy i technologia teleinformatyczna	sieci teleinformatyczne, oprogramowania, procesy i zasoby ludzkie dbające o działanie i bezpieczeństwo tego systemu; stacjonarne i mobilne sieci telekomunikacyjne; łączność i nawigacja radiowa oraz satelitarna; systemy powiadamiania; internet
Zdrowie	szpitale, laboratoria, stacje przechowywania krwi i składników krwiopochodnych; zdrowie publiczne; przemysł farmaceutyczny
Żywość	produkcja, magazynowanie i dystrybucja żywności
Finanse	banki, ubezpieczenia, giełdy, systemy rezerw finansowych
Administracja państwowa	Ministerstwo Obrony Narodowej i inne ministerstwa, służba ochrony państwa, parlament, służby ratunkowe; elektrownie jądrowe; usługi doręczycielskie i poczta; centra zarządzania kryzysowego
Ochrona zabytków	budynki, muzea, pomniki, obiekty sportowe nacechowane patriotyczną wartością
Gospodarka	przemysł zbrojeniowy i ciężki; produkcja i magazynowanie produktów niebezpiecznych; składowanie odpadów niebezpiecznych
Wymiar sprawiedliwości	sądownictwo, sądy i kadra sądownicza
Przestrzeń kosmiczna	ochrona prowadzenia prac badawczych w przestrzeni kosmicznej i wprowadzanie nowych technologii
Zasoby	centra handlowe, budynki szkolne i biurowe, obiekty sportowe, parki rozrywki

Źródło: [39, s. 166-168]

Kryteria pozwalające wyodrębnić obiekty, instalacje, urządzenia i usługi wchodzące w skład infrastruktury krytycznej zostały podzielone na:

- kryteria sektorowe (systemowe): system zaopatrzenia w energię i paliwa, system łączności i sieci teleinformatyczne, system finansowy, system zaopatrzenia w żywność i wodę, system ochrony zdrowia, system komunikacji i transportu, system ratowniczy, system zapewnienia ciągłości działania administracji publicznej, system produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych;
- kryteria przekrojowe: ofiary w ludziach, skutki finansowe, utrata usługi, konieczność ewakuacji, czas odbudowy, efekt międzynarodowy, unikatowość [17, s. 13].

IK wtedy jest krytyczna, kiedy spełnione są co najmniej 2 z 7 kryteriów przekrojowych dla n-tego elementu, który się rozpatruje w procesie identyfikacji.

2. Zagrożenia dla obiektów infrastruktury krytycznej

Podczas rozważań o bezpieczeństwie obiektu infrastruktury krytycznej nie sposób pominąć terminu „zagrożenie". To z jednej strony stan psychiczny lub świadomościowy wywołany postrzeganiem zjawisk, które subiektywnie ocenia się jako niekorzystne lub niebezpieczne, a z drugiej jako czynnik obiektywny, powodujący stany niepewności i obaw [30, s. 17]. Można go również zdefiniować jako sytuację, w której pojawia się zwiększone prawdopodobieństwo powstania stanu niebezpiecznego dla otoczenia [28, s. 162]. Logicznym jest zatem wywód, że bezpieczeństwo określa pewien stan, natomiast zagrożenie kojarzy się bardziej ze zjawiskiem naruszającym ten stan [24, s. 23–32]. Inna definicja prezentuje zagrożenie jako „ogół czynników, najczęściej zewnętrznych, powodujących pojawienie się różnych barier, przeszkód i przeciwności, utrudniających realizację przyjętej strategii rozwoju i bezpieczeństwa" [6, s. 19]. Reasumując, można stwierdzić, że zagrożenie jest czynnikiem zakłócającym prawidłowe funkcjonowanie podmiotu i naruszającym stan jego bezpieczeństwa.

Można wyróżnić dwie zasadnicze strategie postępowania podmiotów, które ukierunkowane są na uzyskiwanie i utrzymywanie pożądanych stanów bezpieczeństwa [21, s. 26]. Pierwsza oparta jest na negatywnym (wąskim) rozumieniu bezpieczeństwa i koncentruje się na przedsięwzięciach ukierunkowanych na maksymalizację poziomu skutecznej ochrony przed zidentyfikowanymi zagrożeniami. Druga natomiast opiera się na pozytywnym (szerokim) pojmowaniu bezpieczeństwa i skupia się na korzystnym dla zainteresowanego podmiotu kształtowaniu otoczenia, tak aby oddalać i minimalizować możliwość powstania i materializowania się zagrożeń [21, s. 26]. Oba te podejścia pokazują, że zagrożenie jako ka-

tegoria ma podstawowe znaczenie dla bezpieczeństwa [4, s. 5]. Jest to jeden z tych czynników, które w różnych konfiguracjach oddziałują na bezpieczeństwo w taki sposób, że musimy postrzegać go nie jako kategorię statystyczną, ale jako dynamiczny, zmienny w czasie proces [21, s. 26]. Według J. Sztumskiego: „nie ma zagrożeń jako takich. Jesteśmy zawsze narażeni na konkretne zagrożenia, które występują lub mogą pojawić się w najbliższej przyszłości, czyli pojawiają się lub mogą pojawić się tu i teraz" [29, s. 30]. Zagrożenia najczęściej są konkretyzowane przez wartości, jakie mogą być utracone przez przedmiot destrukcyjnych oddziaływań lub cechy źródeł tychże zagrożeń [27, s. 57]. Według J. Sztumskiego można wyróżnić trzy różne postawy podejścia do zagrożenia. Jest to postawa fatalistyczna, która charakteryzuje się uznawaniem nieuchronności zaistniałych zagrożeń oraz przeświadczeniem o istnieniu ponadnaturalnych sił, które bezdyskusyjnie ustalają obowiązujący porządek rzeczy; hołdujący tej postawie nie widzą możliwości jakiegokolwiek przeciwstawienia się zagrożeniom, kolejną jest postawa fideistyczna, która charakteryzuje się tym, że także wiąże się z wiarą w istnienie nadprzyrodzonych mocy sprawujących władzę nad światem, zawiera jednak w sobie elementy pewnej aktywności w postaci różnych form apelowania do tych sił o przychylność i niesprowadzanie lub oddalenie zagrożeń, ostatnia to postawa naukowa, która sprowadza się do wniosku, że tylko taka postawa, oparta na racjonalnym oglądzie i systematycznych dociekaniach badawczych, oraz stosowanie w praktyce życia społecznego nabytej tą drogą wiedzy w zakresie identyfikowania, zapobiegania oraz zwalczania zagrożeń jest wyborem, który umożliwia skuteczne działanie na rzecz bezpieczeństwa [29, s. 31].

B. Balcerowicz twierdzi, że pojęcia „bezpieczeństwa" i „zagrożenia" są ze sobą w tak ścisłej zależności dialektycznej, że ich odrębne rozpatrywanie nie ma sensu. Bezpieczeństwo semantycznie oznacza tyle, co „niezagrożenie", stan pokoju, pewności, co świadczy o etymologicznej pierwotności znaczenia słowa „zagrożenie". Bezpieczny to ten, który „nie potrzebuje pieczy", czyli opieki, gdyż nie jest zagrożony. W łacinie oraz językach pochodnych obserwujemy analogiczne zjawisko – *sine cura, securitas*, to jest „bez pieczy" [1, s. 50]. Określenie zagrożeń dla obiektu infrastruktury krytycznej jest bardzo ważne przede wszystkim z uwagi na społeczny wymiar skutków tych zagrożeń, ale również dlatego, że od ich rodzaju, skali i prawdopodobieństwa wystąpienia zależą podejmowane środki służące ich przeciwdziałaniu [26, s. 75]. Uwzględniając źródła powstawania zagrożeń, możemy je podzielić na zagrożenia naturalne – zdarzenia wynikające z przyczyn naturalnych, często zwane też „dziełem Boga", nagłe, jednorazowe, społecznie destrukcyjne, określone co do miejsca i czasu oraz wywołane działalnością człowieka – zdarzenia nagłe, wynikające ze złożonych procesów technologicznych, organizacyjnych i społecznych; mogą być wywołane błędem ludzkim; ich wpływ może być nieograniczony geograficznie, a konsekwencje zauważone z opóźnieniem; duże katastrofy przemysłowe występują rzadko, a mniejsze zdarzenia społeczno-techniczne mają

ograniczony wpływ bezpośredni na społeczność lokalną; obejmują również zdarzenia wynikające z działalności wojennej [21, s. 30].

2.1. Zagrożenia naturalne

Według A. Lisowskiego „zagrożenie naturalne jest zjawiskiem lub procesem przyrodniczym, które może wpłynąć na pogorszenie sytuacji życiowej człowieka wskutek zakłócenia zaspokajania jego potrzeb, od najbardziej elementarnych po potrzeby wyższego rzędu, niezależnie od woli poszkodowanej osoby lub grupy społecznej" [15, s. 30].

Obszar Polski narażony jest na występowanie zagrożeń naturalnych. Mimo iż warunki geograficzne naszego kraju wskazują generalnie na umiarkowane cechy klimatu, a budowa geologiczna na łagodne w większości obszaru ukształtowanie terenu oraz asejsmiczność, występujące współcześnie na terenie Polski ekstremalne zjawiska naturalne są dowodem, iż zagrożenie rzeczywiście istnieje [16, s. 142]. Wśród zagrożeń naturalnych wyróżnić możemy: zagrożenie powodziowe, silny wiatr, upał/suszę, mróz i gołoledź oraz intensywne opady śniegu.

Zagrożenie powodziowe

Powódź to wezbranie wód, w wyniku którego np. zasoby wodne rzeki po przekroczeniu stanu brzegowego lub przerwaniu wałów zalewają otoczenie, zagrażając ludziom, powodując straty społeczne, ekonomiczne i przyrodnicze [7, s. 17]. Ustawa z 18 lipca 2001 r. Prawo wodne definiuje powódź jako „wezbranie wody w ciekach naturalnych, zbiornikach wodnych, kanałach lub na morzu, podczas którego woda po przekroczeniu stanu brzegowego zalewa doliny rzeczne albo tereny depresyjne i powoduje zagrożenia dla ludności lub mienia" [42].

Podstawowe rodzaje powodzi to:

- powodzie roztopowe – dominujące w okresie zimowym i wczesnowiosennym,
- powodzie sztormowe – dominujące od późnej jesieni do wiosny oraz sporadycznie w pozostałych porach roku,
- powodzie zatorowe – dominujące w okresie zimowym i wczesnowiosennym,
- powodzie opadowe – występujące od wczesnej wiosny do późnej jesieni [22, s. 25–26].

Przykładem zagrożenia powodziowego dla obiektu infrastruktury krytycznej może być powódź w Płocku w 1982 r., podczas której największe zagrożenie stanowiła możliwość zmiany koryta Wisły oraz zalania ujęcia wody dla Petrochemii (ówczesne Mazowieckie Zakłady Rafineryjne i Petrochemiczne, obecnie PKN Orlen) i w konsekwencji konieczność zatrzymania kombinatu, co spowodowałoby

m.in. wyłączenie ogrzewania dla mieszkańców Płocka oraz pozbawienia ich wody pitnej. Ponadto istniało niebezpieczeństwo zerwania rurociągu „Przyjaźń", tłoczącego ropę z ZSRR do Mazowieckich Zakładów Rafineryjnych i Petrochemicznych, a następnie do kombinatu Schwedt w NRD, przechodzącego nad Wisłą [47].

Silny wiatr

Wiatrem nazywamy poziomą składową ruchu powietrza względem powierzchni ziemi. Tworzy się on w wyniku oddziaływania sił powstających w niejednorodnym polu ciśnienia w obrębie atmosfery. Do oceny jego prędkości stosuje się, oprócz regularnych pomiarów anemometrycznych, opisową skalę opracowaną przez Francisa Beauforta, stworzoną w latach 1806–1808. Skala ta pozwala oszacować prędkości wiatru na podstawie opisu skutków jego działania na lądzie oraz w wodzie [10, s. 133–135]. Wichury, zjawiska typowe dla naszej szerokości geograficznej, pojawiają się na terenie całego kraju, w okresie od listopada do marca [34, s. 56]. Wichury i huragany, oprócz zagrożeń dla życia i zdrowia ludzi, mogą być przyczyną powstania dużych zniszczeń i strat materialnych w sieciach energetycznych i telekomunikacyjnych, budownictwie przemysłowym oraz w transporcie. Wiatry towarzyszące innym ekstremom pogodowym mogą potęgować ich skutki [22, s. 27]. Skutkami silnych wiatrów mogą być:

- zagrożenia dla życia i zdrowia pracowników,
- zerwania linii wysokiego napięcia i powstanie przerw w dostawach energii elektrycznej,
- przerwy w kursowaniu pociągów transportujących produkty z obiektu infrastruktury krytycznej,
- awarie związane z uszkodzeniami urządzeń powodowanymi przez wiatr,
- uszkodzenia budynków, szczególnie poszycia dachowego w obiektach infrastruktury krytycznej.

Przykładem może być przejście huraganu Harvey 27 sierpnia 2017 r. w okolicach Houston. Znajdująca się w okolicy rafineria będąca filią Valero Energy Partners poinformowała o wycieku związanym z przejściem huraganu Harvey. Wyjaśniła, że w wyniku wycieku doszło do emisji benzenu i innych szkodliwych komponentów. Huragan spowodował przerwanie pracy w rafineriach w Teksasie, a ich moc przerobowa spadła o 25 procent. Zakłady te po kilkudniowej przerwie wznowiły normalną pracę [46].

Upał/susza

Polska zaliczana jest do krajów o ubogich zasobach wodnych. Deficyt ten wynika jednak nie tylko z warunków klimatycznych, ale także z nierównomiernego rozmieszczenia terytorialnego oraz ze złej jakości wód. Dla zagospodarowania zasobów istotne są zbiorniki retencyjne, czyli budowle pozwalające na regulację

odpływu rzecznego. Na obszarze Polski znajduje się około 100 takich zbiorników. Posiadają one łączną pojemność około 4 mld m^3. Niestety zatrzymują jedynie 6% odpływu rocznego, co nie zapewnia dostatecznej ochrony przed okresowymi deficytami lub nadmiarami wody [3, s. 158]. Susza to długotrwały brak wody w przyrodzie. Poprzedza ją okres niewielkich opadów lub ich brak (susza atmosferyczna), a w wyniku przedłużania się niedoboru opadów następuje przesychanie coraz głębszych warstw gleby (susza glebowa). Ostatnią fazą jest susza hydrologiczna – obniżeniu ulega poziom wód podziemnych, zmniejsza się przepływ w rzekach, wysychają źródła, a nawet mniejsze cieki wodne. Bezpośrednim skutkiem suszy jest zakłócenie naturalnego bilansu wodnego danego obszaru [11, s. 238]. Występowanie susz może prowadzić do:

- wzrostu zagrożeń pożarowych,
- obniżenia poziomu wód gruntowych skutkującego zaburzeniami pracy ujęć wody.

Upały mogą spowodować uszkodzenia nawierzchni dróg dojazdowych do obiektu infrastruktury krytycznej i prowadzącego do niego szlaku kolejowego. W konsekwencji może to doprowadzić do katastrof komunikacyjnych. Wysokie temperatury oraz susza zwiększają groźbę pożaru na terenie obiektu infrastruktury krytycznej.

Przykładem jest sytuacja z sierpnia 2015 r., gdy wskutek utrzymujących się w Polsce wysokich temperatur i niekorzystnej sytuacji hydrologicznej nastąpiło pogorszenie warunków pracy sieci energetycznych związane ze znacznymi ubytkami mocy wytwórczych oraz dużym wzrostem krajowego zapotrzebowania na moc. Polskie Sieci Elektroenergetyczne S.A., po wykorzystaniu wszystkich dostępnych środków zaradczych dla pokrycia zapotrzebowania na moc, 10 sierpnia 2015 r. wprowadziły na obszarze Rzeczypospolitej Polskiej ograniczenia w dostarczaniu i poborze energii elektrycznej w trybie normalnym na polecenie Operatora Systemu Przesyłowego. W godzinach 10:00–17:00 ogłoszony został 20 stopień zasilania, zaś w godzinach 17:00–22:00 – 19 stopień zasilania.

W związku z utrzymującym się zagrożeniem bezpieczeństwa dostaw energii elektrycznej, 11 sierpnia 2015 r. Rada Ministrów wydała rozporządzenie, na mocy którego ograniczenia w dostarczaniu i poborze energii elektrycznej zostały wprowadzone od 11 sierpnia 2015 r. od godziny 24:00 do 31 sierpnia 2015 r. do godziny 24:00 na terytorium Rzeczypospolitej Polskiej dla odbiorców energii elektrycznej o mocy umownej powyżej 300 kW [46].

Mróz i gołoledź

Mróz to temperatura powietrza poniżej 0°C mogąca spowodować odmrożenia, a nawet zamarznięcia ludzi, trudności w komunikacji i gospodarce. Zimy charakteryzują się w postaci:

- bardzo niskich temperatur powietrza i powierzchni ziemi poniżej -10°C,
- niskich temperatur powietrza i powierzchni ziemi, niewiele poniżej 0°C, wywołując zamarzanie wody ze stopionego śniegu lub przechłodzonych kropel mżawki i deszczu, powodując gołoledź,
- zamieci śnieżnej polegającej na przenoszeniu śniegu przez mniej lub bardziej silny wiatr, powodując tworzenie się np. zasp śnieżnych,
- zawiei śnieżnej, w czasie której występuje opad śniegu porywany przez silny wiatr,
- szadzi powstającej w wyniku osadzania się przechłodzonych kropelek mgły w czasie mrozów [33, s. 292].

Gołoledź jest jednym ze zjawisk meteorologicznych, niosących ze sobą zagrożenia w wielu sektorach gospodarki oraz powodujących utrudnienia w działalności ludzkiej. Niekiedy może również stwarzać niebezpieczeństwo dla życia ludzkiego. Podstawowe zagrożenia i zniszczenia powodowane przez gołoledź to:

- oblodzenie dróg oraz chodników powodujące utrudnienia komunikacyjne; może być przyczyną zagrożenia życia ludzkiego,
- uszkodzenie drzewostanu, polegające na licznych złamaniach i łukowatych wygięciach pni ku dołowi spowodowane osadzaniem się na gałęziach i koronach drzew warstwy lodu, może być spotęgowane przez uprzednio występujące zjawisko szadzi lub opady śniegu, które osadzając się na drzewach, zwiększają ich powierzchnię i powodują dodatkowe osadzanie marznącego opadu,
- uszkodzenia linii napowietrznych; polegają na licznych złamaniach słupów podtrzymujących linie napięcia (linie energetyczne pod ciężarem lodu wyginają się i odkształcają lub ulegają zerwaniu); zniszczenia mogą być spotęgowane przez uprzednio występujące zjawisko szadzi lub opady śniegu, które osadzając się na liniach napowietrznych i słupach, zwiększają ich powierzchnię i powodują dodatkowe osadzanie marznącego opadu,
- oblodzenie statków powietrznych w locie oraz na powierzchni ziemi; powoduje trudności komunikacyjne, opóźnienia lotów i niebezpieczeństwo wypadku (zwłaszcza dla mniejszych samolotów bez zaawansowanych instalacji odlodzeniowych) [45].

Szczególne zagrożenia związane z pojawieniem się gołoledzi mogą powstać na drogach dojazdowych do obiektu infrastruktury krytycznej. Mogą także wystąpić oblodzenia linii trakcyjnych na szlaku kolejowym prowadzącym do tego obiektu. Niskie temperatury mogą powodować na terenie obiektu infrastruktury krytycznej:

- awarie: magistrali ciepłowniczych, wodociągów, sieci kanalizacyjnej i linii przesyłowych wysokiego napięcia,
- przerwy w dostawach: wody, energii elektrycznej i ciepła,
- zlodowacenie nawierzchni dróg oraz oblodzenie trakcji kolejowych,
- powstanie zjawisk lodowych na rzekach mogące skutkować powodzią zatorową w rejonie obiektu infrastruktury krytycznej.

Intensywne opady śniegu

O intensywnych opadach śniegu mówimy, gdy obfite opady występują na rozległych obszarach i trwają przez kilka dni [23, s. 100]. Intensywne opady śniegu stwarzają zagrożenie, kiedy nagle tworzy się co najmniej trzycentymetrowa warstwa śniegu. Mogą one powodować:

- utrudnienia komunikacyjne na drogach dojazdowych do obiektu infrastruktury krytycznej oraz na prowadzącym do niego szlaku kolejowym,
- wypadki na drogach dojazdowych do obiektu infrastruktury krytycznej,
- zawalenie się obiektów budowlanych pod wpływem ciężaru śniegu i lodu,
- zerwanie linii wysokiego napięcia pod ciężarem śniegu i powstanie przerw w zaopatrzeniu w energię elektryczną obiektu infrastruktury krytycznej.

2.2. Zagrożenia wywołane działalnością człowieka

Terroryzm

Departament Obrony Stanów Zjednoczonych wykorzystuje definicję, która wskazuje że „(…) terroryzm to bezprawne użycie – bądź groźba użycia – siły czy przemocy wobec osoby lub mienia, by wymuszać lub zastraszać rządy czy społeczeństwa, często dla osiągnięcia celów politycznych, religijnych czy ideologicznych" [9, s. 188]. W innym ujęciu „terroryzm to stosowanie gwałtu do osiągnięcia celów politycznych lub ekonomicznych w stosunkach międzynarodowych. Forma interwencji dokonywanej przemocą przez specjalne jednostki wojska lub Policji, albo przez organizacje terrorystyczne" [19, s. 3509]. W ostatnich latach zagrożenie to nabrało szczególnego znaczenia i w coraz większym stopniu stanowi realną groźbę jego wystąpienia. Najbardziej prawdopodobny rodzaj ataków terrorystycznych, jakie mogą być przeprowadzone w odniesieniu do obiektu infrastruktury krytycznej, stanowi atak z użyciem materiałów wybuchowych.

Zakłócenia porządku publicznego

Termin bezpieczeństwo publiczne pojawił się w literaturze w XIX stuleciu. W Polsce jednym z prekursorów zajmujących się tym zagadnieniem był W. Kawka, który określał je jako „stan, w którym całość społeczeństwa oraz państwo ze swoimi priorytetami mają zapewnioną ochronę od jakichkolwiek zagrożeń" [38, s. 85]. Zdaniem E. Ochendowskiego jest „ono zapewnieniem nienaruszalności: życia, zdrowia, godności, wolności, majątku, porządku prawnego oraz instytucji państwa" [18, s. 21]. Głównymi zdarzeniami zakłócającymi bezpieczeństwo i porządek publiczny na terenie obiektu infrastruktury krytycznej mogą być strajki spowodowane redukcją zatrudnienia lub zmiany w strukturze organizacyjnej. Zakłócenia bezpieczeństwa i porządku publicznego mogą spowodować zagrożenia dla życia

i zdrowia osób protestujących, niszczenie mienia, duże straty materialne, zakłócenia w normalnym funkcjonowaniu obiektu infrastruktury krytycznej.

Techniczne

Wśród zagrożeń zakładu wywołanych awariami technicznymi wyróżnia się między innymi:

- awarie systemu energetycznego,
- awarie zasilania w wodę,
- awarie sieci gazowej.

Awaria sieci energetycznej zaopatrującej obiekt infrastruktury krytycznej w energię elektryczną może być spowodowana samoistnymi uszkodzeniami elementów sieci, działaniem osób trzecich lub oddziaływaniem czynników pogodowych (huraganowe wiatry, intensywne opady śniegu, osadzająca się na drutach szadź lub powódź). Przerwanie dostaw energii może w sposób poważny zakłócić funkcjonowanie obiektu infrastruktury krytycznej i doprowadzić do zatrzymania przebiegu procesów produkcyjnych. Rozległa awaria systemowa sieci energetycznej może być także następstwem oddziaływania bardzo niskich temperatur lub wystąpienia stanu głębokiego deficytu mocy w krajowym systemie elektroenergetycznym. Awaria sieci energetycznej może powstać w wyniku zaburzenia lub uszkodzenia systemów: informatycznych, telekomunikacyjnych, monitorowania i sterowania lub ataku terrorystycznego.

Awaria zasilania w wodę może powstać w wyniku zakłócenia funkcjonowania zakładowego ujęcia wody lub magistrali i rurociągów.

Przyczynami powstawania awarii mogą być:

- błąd człowieka,
- niekorzystne warunki meteorologiczne (np. silne mrozy),
- awarie urządzeń technicznych w zakładowym ujęciu wody,
- przerwy w dostawach energii elektrycznej,
- skażenie wody w zbiornikach, z których pobierana jest woda przez stacje wodociągów,
- atak terrorystyczny.

Awaria sieci gazowej może powstać w wyniku rozszczelnienia się gazociągu lub uszkodzenia urządzeń w stacji gazowej doprowadzającej gaz do obiektu infrastruktury krytycznej. Awarii może towarzyszyć nieplanowy wyciek gazu i stwarzanie niebezpieczeństwa wybuchu oraz pożaru. Przyczynami wystąpienia awarii sieci gazowej mogą być:

- uszkodzenia podczas nieostrożnego prowadzenia prac ziemnych,
- zły stan techniczny sieci gazowej,
- wady materiałów, z których wykonana jest sieć gazowa,
- skrajnie niekorzystne warunki atmosferyczne,

- terroryzm, sabotaż,
- kradzież elementów sieci,
- kradzież gazu z gazociągu,
- korozja gazociągu,
- błędy ludzi obsługujących sieć gazową.

2.3. Pożar

Słowo „pożar" pochodzi od wyrazu „pożega" oznaczającego wielki ogień pożerający wszystko, co nie może mu się oprzeć z uwagi na swoją naturę, pożerający i niszczący [14, s. 439]. Z czasem wyraz „pożega" został wyparty przez wyraz „pożoga". Stan taki zauważalny był już w XV wieku, aczkolwiek nadal poprawne było używanie wyrazu „pożega" [31, s. 129]. J. Makarewicz definiuje pożar jako ogień szerzący się siłą żywiołową, przy czym pożaru nie utożsamia z każdym rodzajem ognia [31, s. 130]. Według B. Hołysta pożar to „samorzutne i niekontrolowane rozprzestrzenianie się ognia, powodujące straty materialne" [8, s. 7]. Pożar jest gwałtownie przebiegającym, z wydzielaniem płomieni oraz stałych, ciekłych i lotnych produktów spalania, procesem utleniania się materiałów palnych, czyli łączenia materiałów palnych z tlenem (lub innym utleniaczem, jednak z uwagi na to, że prawie 100% pożarów utlenianych jest tlenem, a prawie 90% z nich tlenem atmosferycznym, będziemy mówić tylko o tlenie jako czynniku podtrzymującym palenie) [49].

Bezpieczeństwo pożarowe za J. Zboiną to stan, sytuacja będąca rezultatem skuteczności (funkcjonowania) systemu ochrony przeciwpożarowej w odniesieniu do pożarów [46]. Bezpieczeństwo pożarowe można również zdefiniować jako stan, sytuację będącą rezultatem skuteczności (funkcjonowania) systemu ochrony przeciwpożarowej w odniesieniu do pożarów. Takie sformułowanie, choć ogólne, uwzględnia wszystkie działania na rzecz bezpieczeństwa pożarowego w ramach systemu ochrony przeciwpożarowej, tj. ratownicze, prewencyjne, a także profilaktykę i edukację społeczną [36, s. 15].

Pożar jest największym zagrożeniem dla obiektu infrastruktury krytycznej, którego główną działalnością jest przetwórstwo ropy naftowej. Pożary zbiorników z ropą naftową lub produktami naftowymi, a szczególnie ich najbardziej niekorzystny wariant, gdy pali się ciecz na całej powierzchni zbiornika, z całą odpowiedzialnością można określić jako kataklizm w skali lokalnej [12, s. 160]. Przybliżając skalę zagrożenia, W. Lasota przedstawił podsumowanie 479 pożarów zbiorników magazynowych produktów naftowych na świecie od 1951 do 2003 r. Informacje na temat pożarów pochodzą z USA, Europy i kilku innych krajów anglojęzycznych. Ponadto brano tu pod uwagę pożar w parku zbiorników, niezależnie od tego, czy palił się jeden czy kilka zbiorników. W skrajnych przypadkach pożarem objętych było od 30 do 40 zbiorników.

Tab. 2. Liczba odnotowanych pożarów zbiorników na dekadę od roku 1950

Dekada	1951–1960	1961–1970	1971–1980	1981–1990	1991–2000	2001–2010	2011–2020
Liczba pożarów	13	28	80	135	161	62	Brak danych

Źródło: [12]

Ze statystyk wynika, że spośród 479 zidentyfikowanych pożarów w około 150 przypadkach przyczyną zapalenia było wyładowanie atmosferyczne, dla około 190 przypadków niedostępne są dane dotyczące przyczyn powstania pożaru, pozostałe przypadki dotyczyły powstania pożaru podczas np. prac remontowych, spawalniczych oraz w wyniku działań wojennych oraz terrorystycznych [12, s. 163]. Ogromne znaczenie dla powodzenia akcji gaśniczej ma właściwe zaplanowanie taktyki i logistyki przed rozpoczęciem natarcia pianowego na palący się zbiornik. W każdym z powyższych przypadków pożarów konieczne było użycie pomp i działek pianowych o dużej wydajności oraz wysokiej jakości środka pianotwórczego. Zmniejszenie intensywności palenia zbiornika osiągano zazwyczaj po upłynięciu około od 10 do 30 minut, ale czas do całkowitego ugaszenia jest trudny do określenia [12, s. 165]. Pożar w Norco Refinery Orion Luizjana z 7 czerwca 2001 r. zbiornika o średnicy 82,4 m jest największym dotychczas skutecznie ugaszonym pożarem zbiornika. W zbiorniku znajdowało się 47 700 m^3 89,7 oktanowej benzyny. Czas ugaszenia wyniósł 65 minut [12, s. 165–166]. Według W. Lasoty zasadnym byłoby przeprowadzanie testów pożarowych na zbiornikach o dużej średnicy (100 m i więcej). Testy te wymagają jednak dużych nakładów środków finansowych, powodują również zanieczyszczenie środowiska, ale dają potwierdzoną informację, że zastosowane rozwiązania przeciwpożarowe są skuteczne [12, s. 166].

W Polsce największym pożarem, który miał miejsce w zakładzie przemysłu rafineryjnego, był pożar w rafinerii Czechowice-Dziedzice 26 czerwca 1971 r. W następstwie wybuchu zbiorników zginęły 33 osoby (25 strażaków, siedmiu żołnierzy oraz jeden pracownik rafinerii). W wyniku odniesionych ran i oparzeń zmarło jeszcze w ciągu kolejnych 2 miesięcy czterech ratowników.

Wnioski

Infrastruktura krytyczna ma niewątpliwie bardzo duże znaczenie dla prawidłowego funkcjonowania państwa, a wchodzące w jej skład obiekty i systemy są kluczowymi z punktu widzenia bezpieczeństwa. W wyniku zakłócenia jej funkcjonowania państwo i jego instytucje narażone są na utratę zdolności do wykonywania podstawowych funkcji administracyjnych i usługowych, a co więcej, może również utracić zdolność do sprawowania rzeczywistej kontroli nad całym swoim terytorium.

Wejście w życie ustawy o zarządzaniu kryzysowym stworzyło podstawowe mechanizmy jej zorganizowanej ochrony, ale ochrona ważnych dla państwa elementów nie rozpoczęła się wraz z jej uchwaleniem. Prowadzona była już wcześniej w oparciu o przepisy z dziedziny obronności oraz ochrony osób i mienia. W 1997 r. została przyjęta ustawa o ochronie osób i mienia, w której wskazano między innymi obszary, obiekty i urządzenia, które mają znaczenie dla obronności, gospodarki, bezpieczeństwa publicznego i innych ważnych interesów państwa. Miały być one obowiązkowo chronione przez specjalne, uzbrojone formacje lub odpowiednie zabezpieczenia techniczne. W ramach ochrony obowiązkowej kierownik jednostki, który bezpośrednio zarządza tymi obszarami, obiektami i urządzeniami, został zobowiązany do opracowania oraz uzgodnienia z właściwym terytorialnie komendantem wojewódzkim policji planu ochrony tych obszarów, obiektów i urządzeń.

W literaturze przedmiotu spotkać można różne kryteria podziałów zagrożeń dla funkcjonowania infrastruktury krytycznej. Podział zaproponowany przez autora na zagrożenia naturalne (powódź, silny wiatr, upał/susza, mróz i gołoledź oraz intensywne opady śniegu), zagrożenia wywołane działalnością człowieka (terroryzm, zakłócenia porządku publicznego oraz techniczne) odzwierciedla realne zagrożenia dla funkcjonowania obiektu infrastruktury krytycznej. Zagrożenie pożarem wyodrębniono i opisano jako najważniejsze zagrożenie dla obiektu infrastruktury krytycznej, którego działalność opiera się na przerobie ropy naftowej. Mimo bardzo wysokiego poziomu środków bezpieczeństwa w rafineriach, wskaźnika zagrożenia pożarowego nie można zredukować do zera. Pożar zbiornika czy też innego obiektu rafineryjnego wiąże się nie tylko z utratą paliwa, ale niesie za sobą również ryzyko eksplozji, stanowiącej zagrożenie dla całego kompleksu rafinerii oraz ludzi i obiektów usytuowanych poza jego granicami. Przykładem może być, oprócz pożaru opisanego powyżej, który miał miejsce w rafinerii w Czechowicach-Dziedzicach, pożar zbiornika w rafinerii w Gdańsku. Pożar miał miejsce 3 maja 2003 r. Wybuch i pożar zbiornika spowodował straty w ludziach oraz mieniu. Najdotkliwszą stratę stanowi śmierć trzech pracowników firmy BALTIC MARINE SURVEYORS. Poza tym rafineria w Gdańsku poniosła ogromne straty finansowe związane z nakładami inwestycyjnymi w związku z koniecznością budowy zbiornika (10 746 448 zł), stratami w benzynie (2 515 990 zł), kosztami akcji ratowniczej, zabezpieczenia terenu, usuwania skutków pożaru (2 150 000 zł), kosztami wydobycia i rozbiórki elementów zbiornika (245 000 zł) oraz przyszłymi, szacunkowymi nakładami przewidzianymi na dokonanie odbudowy zbiornika, w tym wykonanie dokumentacji (4 894 000 zł), co daje razem sumę 20 551 438 zł [20, s. 8].

Powyższy przykład pokazuje wagę Narodowego Programu Ochrony Infrastruktury Krytycznej i tworzenia odpowiednich warunków do budowania odpowiedzi na realne zagrożenia jej funkcjonowania. Odpowiedzialność i główny

wysiłek spoczywa przede wszystkim na operatorze infrastruktury krytycznej, ale obowiązek dbałości o jej bezpieczeństwo – na wszystkich pracownikach danego obiektu.

Bibliografia/References

1. Balcerowicz B., *Wybrane problemy obronności państwa*, AON, Warszawa 1999.
2. Brzozowska K., *Finansowanie inwestycji infrastrukturalnych przez kapitał prywatny na zasadzie project finance*, CeDeWu, Warszawa 2009.
3. Drab-Kurowska A., *Zagrożenia środowiska, powodowane przez działalność człowieka* [w:] K. Małachowski (red.), *Gospodarka a środowisko i ekologia*, Warszawa 2007.
4. Fehler W., *Bezpieczeństwo wewnętrzne współczesnej Polski. Aspekty teoretyczne i praktyczne*, Arte, Warszawa 2012.
5. Fehler W., *Zagrożenie – kluczowa kategoria teorii bezpieczeństwa* [w:] K. Jałoszyński, B. Wiśniewski, T. Wojtuszek (red.), *Współczesne postrzeganie bezpieczeństwa*, Wyższa Szkoła Administracji, Bielsko-Biała 2007.
6. Ficoń K., *Inżynieria zarządzania kryzysowego. Podejście systemowe*, BEL Studio, Warszawa 2007.
7. Grocki R., *Vademecum zagrożeń*, Dom wydawniczy Bellona, Warszawa 2003.
8. Hołyst B., *Kryminalistyczna problematyka pożarów*, Wydawnictwo Zakładu Kryminalistyki Komendy Głównej MO, Warszawa 1962.
9. Jałoszyński K., *Terroryzm a wojsko*, „Zeszyty Naukowe AON" 2000, nr 2(39).
10. Kożuchowski K. (red.), *Meteorologia i klimatologia*, PWN, Warszawa 2005.
11. Kudlicki Ł., *Długofalowe konsekwencje zmian klimatycznych*, „Bezpieczeństwo Narodowe" II-2006/2, Warszawa 2006.
12. Lasota W., *Pożary w przemyśle naftowym – przebieg zdarzeń, przyczyny powstawania*, „Bezpieczeństwo i Technika Pożarnicza" 2018, nr 4, CNBOP, Józefów 2018.
13. *Leksykon wiedzy wojskowej*, MON, Warszawa 1979.
14. Linde M.S., *Słownik języka polskiego*, MCMLI, t. IV, Lwów 1958.
15. Lisowski A., *Skutki występowania zagrożeń naturalnych i ich percepcje w Polsce*, Uniwersytet Warszawski, Warszawa 1993.
16. Marek H., *Występowanie współczesnych zagrożeń naturalnych na terenie Polski,* „Przegląd Naukowo-Metodyczny. Edukacja dla Bezpieczeństwa" 2009, nr 3.
17. Narodowy Program Ochrony Infrastruktury Krytycznej 2020.
18. Ochendowski E., *Podmioty administracji publicznej i prawne formy ich działania*, Toruń 2005.
19. Omańczyk J.E., *Encyklopedia spraw międzynarodowych i ONZ*, Warszawa 1974.
20. Państwowa Inspekcja Pracy, *Raport z badania okoliczności i przyczyn wybuchu i pożaru zbiornika benzyny w Rafinerii Gdańskiej S.A. oraz wypadku zbiorowego śmiertelnego trzech pracowników firmy BALTIC MARINE SURVEYORS Sp. z o.o. podczas pobierania prób benzyny ze zbiornika*, Gdańsk 2003.
21. Pietrek G., *System zarządzania kryzysowego*, Difin, Warszawa 2018.
22. Pietrek G., *Zarządzanie w sytuacjach kryzysowych*, Akademia Pomorska w Słupsku, Słupsk 2014.

23. Pokojski W., Korzeniecki P., Kowalewski M., *Klimatyczne zagrożenia naturalne w Polsce – wybór wskaźników*, „Prace i Studia Geograficzne" 2014, t. 55.
24. Prońko J., *System kierowania reagowaniem kryzysowym w sytuacjach nadzwyczajnych zagrożeń dla ludzi i środowiska*, AON, Warszawa 2001.
25. Pyznar M., Abgarowicz G., *Rola infrastruktury krytycznej w funkcjonowaniu państwa* [w:] J. Świątkowska, Z. Fałek (red.), *Bezpieczeństwo infrastruktury krytycznej wymiar teleinformatyczny*, Instytut Kościuszki, Kraków 2014.
26. Radziejewski R., *Ochrona infrastruktury krytycznej. Teoria a praktyka*, PWN, Warszawa 2014.
27. Sienkiewicz P., *Modelowanie bezpieczeństwa systemów*, „Zeszyty Naukowe AON" 1991, nr 3/4.
28. *Słownik terminów z zakresu bezpieczeństwa narodowego*, Akademia Obrony Narodowej, Warszawa 2008.
29. Sztumski J., *Brak bezpieczeństwa jako problem społeczny* [w:] W. Fehler (red.), *Bezpieczeństwo publiczne w przestrzeni miejskiej*, Arte, Warszawa 2010.
30. Szubrycht T. (red.), *Leksykon bezpieczeństwa morskiego,* AMW, Gdynia 2008.
31. Witczak D., *Pojęcie pożaru w świetle obowiązujących przepisów prawnych, nauki prawa i orzecznictwa*, „Zeszyty Naukowe SGSP" 2015, nr 53(1).
32. Wojciechowicz W., *Ochrona infrastruktury krytycznej państwa*, „Myśl Wojskowa" 2004, nr 1.
33. Wolanin J., *Zarys teorii bezpieczeństwa obywateli. Ochrona ludności na czas pokoju,* Danmar, Warszawa 2005.
34. Woś A., *Klimat Polski*, PWN, Warszawa 1999.
35. Wójtowicz W., *Bezpieczeństwo infrastruktury krytycznej*, MON, Warszawa 2006.
36. Zboina J., Iwańska M., *Bezpieczeństwa pożarowe* [w:] J. Zboina, P. Gancarczyk (red.), *Certyfikacja usług w ochronie przeciwpożarowej w ujęciu praktycznym i teoretycznym*, CNBOP-PIB, Józefów 2016.
37. Lasota W., *Pożary w przemyśle naftowym – przebieg zdarzeń, przyczyny powstawania*, „Bezpieczeństwo i Technika Pożarnicza" 2018, nr 4.
38. Zieliński A., *Bezpieczeństwo publiczne jako podstawowy obowiązek państwa ze szczególnym uwzględnieniem roli policji w tym obszarze działań*, „Security, Economy & Law" 2017, nr 3/2017 (XVI).
39. Żmigrodzki M. (red.), *Zarządzanie kryzysowe w państwie*, Towarzystwo Naukowe Powszechne S.A., Warszawa 2012.
40. Dyrektywa Rady 2008/114/WE z 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony (Dz.U. UE L.08.345.75).
41. Ustawa z 10 czerwca 2016 r. o działaniach antyterrorystycznych (t.j. Dz.U. z 2021 r. poz. 2234).
42. Ustawa z 20 lipca 2017 r. Prawo wodne (Dz.U. z 2021 r. poz. 624 t.j.).
43. Rozporządzenie Rady Ministrów z 30 kwietnia 2010 r. w sprawie Narodowego Planu Ochrony Infrastruktury Krytycznej (Dz.U. z 2010 r. Nr 83, poz. 541).
44. *Encyklopedia zarządzania*, https://mfiles.pl/pl/index.php/Cykl_Deminga (dostęp: 2.07.2022).

45. https://imgw.isok.gov.pl/mapy-zagrozen-i-ryzyka/zagrozenia-meteorologiczne/gololedz/zagrozenia-zwiazane-z-wystepowaniem.html (dostęp: 2.07.2022).
46. https://smart-grids.pl/index.php/aktualnosci/biznes/1820-raport-pse-nt-przyczyn-20-stopnia-zasilania-w-2015-r.html (dostęp: 2.07.2022).
47. https://dzieje.pl/rozmaitosci-historyczne/powodz-w-plocku-sprzed-40-lat-grozba-zmiany-koryta-wisly-zalania-ujecia (dostęp: 2.07.2022).
48. https://tvn24.pl/tvnmeteo/najnowsze/media-wladze-sprawdzaja-czy-nad-houston-unosi-sie-toksyczna-chmura-4906215 (dostęp: 2.07.2022).
49. https://asystentbhp.pl/pozar/ (dostęp: 2.07.2022).