Tom 17/2025, ss. 143-157
ISSN 0860-5637
e-ISSN 2657-7704
DOI: 10.19251/rtnp/2025.17(7)
www.rtnp.mazowiecka.edu.pl

Izabela Markiewicz
Uniwersytet Warszawski
i.markiewic2@student.uw.edu.pl
https://orcid.org/0009-0006-4697-2296

Infrastruktura krytyczna w Płocku na przykładzie systemu paliwowo-energetycznego: identyfikacja, znaczenie i potencjalne zagrożenia

Critical Infrastructure in Płock Based on the Fuel and Energy System: Identification, Significance and Potential Threats

Streszczenie
Celem artykułu jest identyfikacja i charakterystyka infrastruktury krytycznej w Płocku, ze szczególnym uwzględnieniem systemu paliwowo-energetycznego oraz ocena zagrożeń mogących naruszyć jej ciągłość działania. Opracowanie akcentuje nie tylko znaczenie infrastruktury krytycznej dla bezpieczeństwa narodowego, lecz także jej rolę w rozwoju społeczno-gospodarczym miasta i regionu. W pracy wykorzystano analizę ram prawnych i dokumentów programowych (ustawa o zarządzaniu kryzysowym, NPO-IK) oraz studium przypadku kompleksu rafineryjno-petrochemicznego

ORLEN i infrastruktury przesyłowej PERN. Analiza wskazuje, że Płock jest newralgicznym węzłem krajowego systemu bezpieczeństwa energetycznego i łańcuchów dostaw paliw, a zarazem przestrzenią kumulacji ryzyk: awarii przemysłowych, zakłóceń logistycznych, sabotażu, cyberataków oraz działań dezinformacyjnych. Szczególne znaczenie ma wzajemne przenikanie się zagrożeń cyfrowych i fizycznych, a także rozbieżności proceduralne pojawiające się na styku obowiązków operatorów, administracji publicznej i służb reagowania. Wnioski prowadzą do rekomendacji dotyczących zintegrowanego modelu ochrony, opartego na ciągłej ocenie ryzyka, współpracy międzyinstytucjonalnej, modernizacji zabezpieczeń technicznych oraz budowaniu odporności społecznej.

Słowa kluczowe: infrastruktura krytyczna, bezpieczeństwo energetyczne, Płock, zagrożenia hybrydowe, cyberbezpieczeństwo, zarządzanie kryzysowe, sektor paliwowo-energetyczny

Abstract

The article identifies and characterizes the critical infrastructure in Płock, with particular emphasis on the fuel and energy system, and assesses the threats that may disrupt its continuity of operation. The study highlights not only the role of critical infrastructure as a foundation of national security, but also its importance for the socio-economic development of the city and the region. The analysis combines the applicable legal framework and strategic documents (the Crisis Management Act and the National Programme for Critical Infrastructure Protection) with a case study of the ORLEN refinery and petrochemical complex and PERN transmission infrastructure. The findings indicate that Płock constitutes a critical node in the national energy security system and in fuel supply chains, while at the same time concentrating multiple risks: industrial failures, logistical disruptions, acts of sabotage, cyberattacks and disinformation activities. Particular importance is attached to the overlap of digital and physical threats, as well as to procedural discrepancies appearing at the interface between infrastructure operators, public administration and emergency services. The article recommends an integrated protection model based on continuous risk assessment, inter-institutional cooperation, the modernization of technical safeguards, and the strengthening of societal resilience.

Keywords: critical infrastructure, energy security, Płock, hybrid threats, cybersecurity, crisis management, fuel and energy sector

1. Wprowadzenie

Infrastruktura krytyczna (IK) stanowi fundament bezpieczeństwa narodowego, gdyż obejmuje systemy i obiekty warunkujące ciągłość funkcjonowania państwa, gospodarki oraz życia społecznego (Rządowe Centrum Bezpieczeństwa, 2025a). W warunkach narastającej niestabilności geopolitycznej, szczególnie po rosyjskiej agresji na Ukrainę, ochrona IK przestała być wyłącznie zagadnieniem technicznym lub administracyjnym. Stała się elementem strategicznego myślenia o odporności państwa, zdolności reagowania kryzysowego oraz bezpieczeństwie obywateli.

Znaczenie IK ujawnia się jednak nie tylko w sferze bezpieczeństwa. Infrastruktura ta stanowi również podstawę rozwoju społeczno-gospodarczego regionu: zwiększa atrakcyjność inwestycyjną, sprzyja lokowaniu nowoczesnej produkcji, wpływa na pozyskiwanie wykwalifikowanych kadr i podtrzymuje ciągłość łańcuchów dostaw. Jednocześnie niewłaściwe lokowanie obiektów, zaniedbania inwestycyjne lub niewystarczające zabezpieczenia mogą generować skumulowane ryzyka, zwłaszcza tam, gdzie mamy do czynienia z magazynowaniem, przesyłem i przetwarzaniem surowców energetycznych oraz substancji niebezpiecznych. Z tego względu analiza IK wymaga spojrzenia łączącego perspektywę techniczną, prawną, gospodarczą i społeczną.

Płock zajmuje w tym układzie miejsce szczególne. Miasto jest jednym z najważniejszych ośrodków przemysłowych w Polsce, a zarazem węzłem systemu paliwowo-energetycznego o znaczeniu wykraczającym poza wymiar lokalny. Kompleks rafineryjno-petrochemiczny ORLEN oraz infrastruktura przesyłowa PERN współtworzą system kluczowy dla bezpieczeństwa energetycznego państwa i stabilności rynku paliw. W konsekwencji potencjalne zakłócenia w funkcjonowaniu płockiej IK mogą oddziaływać jednocześnie na poziomie miejskim, regionalnym i ogólnokrajowym.

Celem artykułu jest identyfikacja i charakterystyka infrastruktury krytycznej Płocka w sektorze paliwowo-energetycznym oraz ocena zagrożeń mogących naruszyć jej ciągłość działania. W opracowaniu zwrócono uwagę nie tylko na obowiązujące ramy

prawne, lecz także na praktyczne uwarunkowania ochrony IK, w tym na proceduralne rozbieżności pojawiające się na styku operatorów infrastruktury, administracji publicznej i służb odpowiedzialnych za reagowanie kryzysowe.

W związku z tak określonym celem postawiono następujące pytania badawcze:

1. Które obiekty i systemy sektora paliwowo-energetycznego w Płocku spełniają kryteria infrastruktury krytycznej w świetle obowiązujących regulacji?
2. W jaki sposób usytuowanie Płocka w krajowym systemie dostaw paliw i surowców wzmacnia zarówno jego znaczenie strategiczne, jak i skalę potencjalnego ryzyka?
3. Jakie zagrożenia – cybernetyczne, hybrydowe, sabotażowe, terrorystyczne i informacyjne – należy uznać za najistotniejsze dla płockiej infrastruktury krytycznej?
4. Jakie rozwiązania organizacyjne, proceduralne i technologiczne mogą realnie podnieść odporność płockiej infrastruktury krytycznej?

Artykuł łączy analizę aktów prawnych i dokumentów programowych (m.in. ustawy o zarządzaniu kryzysowym oraz NPO-IK) ze studium przypadku kluczowych elementów płockiego systemu paliwowo-energetycznego. Takie podejście pozwala połączyć ujęcie definicyjne z wymiarem praktycznym i wskazać konkretne kierunki wzmacniania bezpieczeństwa miasta.

2. Definicja i zakres infrastruktury krytycznej

Pojęcie infrastruktury krytycznej zostało wprowadzone do polskiego porządku prawnego ustawą o zarządzaniu kryzysowym z 2007 roku. Zgodnie z definicją ustawową infrastrukturę krytyczną stanowią systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, urządzenia, instalacje i usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców (Ustawa z dnia 26

kwietnia 2007 r. o zarządzaniu kryzysowym). W praktyce są to te elementy infrastruktury, bez których niemożliwe byłoby utrzymanie minimalnego poziomu funkcjonowania państwa i lokalnych wspólnot.

Narodowy Program Ochrony Infrastruktury Krytycznej porządkuje katalog systemów podlegających szczególnej ochronie. Obejmuje on między innymi systemy zaopatrzenia w energię, surowce energetyczne i paliwa, sieci teleinformatyczne i łączność, systemy finansowe, zaopatrzenie w żywność i wodę, ochronę zdrowia, transport, ratownictwo, ciągłość działania administracji publicznej, a także systemy związane z produkcją, magazynowaniem i stosowaniem niebezpiecznych substancji chemicznych i promieniotwórczych (Ministerstwo Spraw Wewnętrznych i Administracji, 2023).

Tak szeroko ujmowany zakres IK pokazuje, że ma ona charakter sieciowy i współzależny. Obejmuje zarówno infrastrukturę materialną, jak i warstwę cyfrową, bez której współczesne systemy przemysłowe, logistyczne czy administracyjne nie są w stanie działać w sposób efektywny. Rosnące znaczenie systemów sterowania, komunikacji i wymiany danych sprawia, że ochrona IK nie może ograniczać się do ochrony fizycznej obiektów, lecz musi obejmować również cyberbezpieczeństwo oraz zdolność do utrzymania ciągłości działania w sytuacji zakłóceń.

Warto przy tym podkreślić, że nie każdy obiekt o dużym znaczeniu gospodarczym automatycznie staje się elementem IK. O zaliczeniu do tej kategorii decydują określone kryteria, w tym możliwa skala skutków awarii lub ataku. Ma to praktyczne znaczenie dla poziomu ochrony, zakresu planowania awaryjnego i obowiązków operatora. Zarazem pewna część informacji dotyczących klasyfikacji i szczegółowych zabezpieczeń ma charakter niejawny, co ogranicza ich publiczną dostępność (Rządowe Centrum Bezpieczeństwa, 2025a).

W praktyce problemem nie jest wyłącznie sama identyfikacja obiektu jako elementu IK, lecz także koordynacja procedur ochronnych. Część obowiązków spoczywa na operatorach, część na administracji rządowej i samorządowej, a część na służbach

ratowniczych oraz formacjach odpowiedzialnych za bezpieczeństwo. Do tego dochodzą procedury wynikające z ochrony środowiska, bezpieczeństwa przemysłowego, ochrony przeciwpożarowej, cyberbezpieczeństwa i zarządzania kryzysowego. Rozproszenie kompetencji może prowadzić do rozbieżności proceduralnych, zwłaszcza w sytuacjach wymagających szybkiej wymiany informacji i jednoczesnego działania wielu podmiotów.

Ochrona IK powinna więc obejmować nie tylko środki materialne, lecz także planowanie ciągłości działania, scenariusze awaryjne, wspólne ćwiczenia oraz ciągłą, kroczącą ocenę ryzyka. W realiach współczesnych zagrożeń decydujące znaczenie ma bowiem zdolność do szybkiego dostosowania procedur do zmieniającej się sytuacji bezpieczeństwa (Rządowe Centrum Bezpieczeństwa, 2025a).

3. Infrastruktura krytyczna Płocka – sektor paliwowo-energetyczny

Najważniejszym elementem infrastruktury krytycznej Płocka jest kompleks rafineryjno-petrochemiczny ORLEN. Skala przerobu ropy naftowej, produkcji paliw i petrochemikaliów, magazynowania surowców oraz utrzymywania rezerw powodują, że obiekt ten należy traktować jako jeden z kluczowych pojedynczych komponentów krajowej infrastruktury krytycznej (Wiśniewski, 2019). Zakład pełni funkcje produkcyjne, logistyczne i energetyczne, oddziałując nie tylko na gospodarkę miasta, lecz także na bezpieczeństwo paliwowe państwa.

Istotnym elementem tego systemu jest również własna infrastruktura energetyczna zakładu, w tym zdolność do wytwarzania energii elektrycznej i cieplnej na potrzeby procesów technologicznych oraz częściowo otoczenia zewnętrznego. Skala instalacji przemysłowych, obecność rozbudowanych zbiorników magazynowych i operowanie substancjami niebezpiecznymi sprawiają zarazem, że kompleks ten należy analizować nie tylko jako

zasób strategiczny, ale również jako potencjalne źródło poważnych skutków w przypadku awarii, sabotażu lub zakłóceń systemów sterowania.

Drugim filarem płockiej IK w tym obszarze jest infrastruktura przesyłowa PERN. Rurociągi łączą rafinerię z Naftoportem w Gdańsku oraz z magistralą „Przyjaźń", co nadaje Płockowi znaczenie węzła o charakterze ponadlokalnym. Po 2022 roku znaczenie dostaw alternatywnych wobec kierunku rosyjskiego dodatkowo wzrosło, a gdański Naftoport stał się jednym z kluczowych elementów dywersyfikacji dostaw ropy do polskich rafinerii (Ruszel i Ogarek, 2022). W konsekwencji zakłócenia na tym odcinku mogą oddziaływać nie tylko na Płock, lecz również na bezpieczeństwo energetyczne państwa i stabilność dostaw w szerszej skali regionalnej.

Znaczenie płockiej IK nie sprowadza się jednak wyłącznie do produkcji i przesyłu paliw. Skupienie wyspecjalizowanych instalacji przemysłowych oddziałuje na lokalny rynek pracy, strukturę usług, infrastrukturę techniczną miasta oraz poziom jego atrakcyjności gospodarczej. Płock pełni zarazem funkcję węzła łączącego procesy produkcyjne, logistyczne i dystrybucyjne. Z tej perspektywy każda poważna awaria, zaniedbanie modernizacyjne lub zakłócenie dostaw może uruchomić efekt domina – od strat środowiskowych i zagrożenia dla mieszkańców po perturbacje na rynku paliw i w łańcuchach dostaw w skali krajowej.

Świadomość tych zagrożeń przekłada się na rozbudowany system zabezpieczeń. Na terenie zakładu funkcjonują wyspecjalizowane służby ochrony i ochrony przeciwpożarowej, prowadzone są ćwiczenia praktyczne, a operator współpracuje z Państwową Strażą Pożarną i podmiotami administracji lokalnej w ramach miejskiego i powiatowego systemu reagowania kryzysowego (Wiśniewski, 2019; Lejman, 2022; Urząd Miasta Płocka, 2022). Działania te mają na celu zarówno ograniczanie prawdopodobieństwa incydentów, jak i skracanie czasu reakcji w razie ich wystąpienia.

Incydenty związane z rozszczelnieniem rurociągów w Polsce pokazały, że nawet jeśli źródłem zakłóceń nie jest sabotaż, sama podatność infrastruktury przesyłowej staje się problemem

bezpieczeństwa (Kublik, 2022). W dyskusji eksperckiej zasadnie podnosi się więc potrzebę rozwijania rozwiązań redundantnych, modernizacji infrastruktury i zwiększania możliwości szybkiego przełączenia dostaw w razie uszkodzeń (Ruszel i Ogarek, 2022).

W konsekwencji płocki system paliwowo-energetyczny należy postrzegać jako układ, w którym potencjał rozwojowy i potencjał ryzyka współistnieją oraz wzajemnie się warunkują. To właśnie ta ambiwalencja czyni go jednym z najbardziej wymagających obszarów polityki bezpieczeństwa na poziomie lokalnym i krajowym.

4. Aktualne wyzwania bezpieczeństwa infrastruktury krytycznej

Współczesne środowisko bezpieczeństwa cechuje wysoka dynamika, wielowarstwowość i trudna do przewidzenia eskalacja zagrożeń. Infrastruktura krytyczna znajduje się w centrum zainteresowania zarówno podmiotów odpowiedzialnych za ochronę państwa, jak i aktorów wrogich – od grup przestępczych po podmioty sponsorowane przez państwa. Szczególnie istotne stają się dziś zagrożenia cybernetyczne, sabotażowe, terrorystyczne oraz informacyjne, które coraz częściej przenikają się i wzajemnie wzmacniają. Ocenę ryzyka należy więc traktować jako proces ciągły i aktualizowany wraz ze zmianą sytuacji geopolitycznej.

4.1. Zagrożenia cybernetyczne

Infrastruktura krytyczna coraz częściej staje się celem zaawansowanych cyberataków wymierzonych w systemy informatyczne, sieci przemysłowe i rozwiązania sterowania procesami. W Polsce odnotowuje się rosnącą liczbę incydentów w sektorach uznawanych za krytyczne, w tym w energetyce i transporcie (Sawczuk, 2025). Z tej perspektywy Płock, jako ośrodek o dużej koncentracji infrastruktury petrochemicznej i energetycznej, należy

traktować jako obszar szczególnie narażony na działania rozpoznawcze i zakłócające prowadzone w cyberprzestrzeni.

Specyfika cyberzagrożeń polega na ich ukrytym charakterze. Próby uzyskania dostępu do systemów mogą pozostawać niewidoczne przez długi czas, a skutki udanego ataku mogą być porównywalne z fizycznym sabotażem. Zakłócenie pracy systemów sterowania w rafinerii mogłoby wymusić zatrzymanie produkcji, a skuteczny atak na elementy infrastruktury energetycznej mógłby doprowadzić do przerw w dostawach energii i uruchomienia efektu domina obejmującego także łączność, wodociągi czy transport (a&s Polska, 2024).

Dodatkowym wyzwaniem jest zacieranie się granicy między środowiskami IT i OT. Jeszcze kilkanaście lat temu systemy sterujące instalacjami przemysłowymi częściej pozostawały odseparowane od sieci biurowych. Dziś, wraz z rozwojem zdalnego nadzoru, analityki danych i automatyzacji, wzrasta liczba punktów styku, które mogą stać się wektorami ataku. Eksperci zwracają uwagę również na scenariusze łączące wtargnięcie fizyczne z ingerencją cyfrową, na przykład przez podmianę urządzeń lub wprowadzenie złośliwego oprogramowania do środowiska sterowania (a&s Polska, 2024).

Dla Płocka oznacza to konieczność stałego inwestowania w kompetencje personelu, segmentację sieci, monitoring zdarzeń, kopie zapasowe, testy odporności oraz procedury odtwarzania działalności. Cyberbezpieczeństwo nie może być traktowane jako odrębna domena techniczna, lecz jako integralny składnik ochrony infrastruktury krytycznej.

4.2. Zagrożenia hybrydowe, sabotaż fizyczny i szpiegostwo

Zagrożenia hybrydowe polegają na skoordynowanym wykorzystywaniu instrumentów politycznych, informacyjnych, dywersyjnych, ekonomicznych i siłowych w celu osłabienia przeciwnika poprzez uderzenie w jego słabe punkty (NATO Review, 2021). Infrastruktura krytyczna staje się w tym modelu naturalnym celem, ponieważ jej uszkodzenie albo nawet czasowe

wyłączenie może wywołać jednocześnie skutki gospodarcze, społeczne i psychologiczne.

Doświadczenia ostatnich lat pokazały, że zagrożenie sabotażowe na terytorium Polski ma charakter realny. Ujawnienie siatki działającej na rzecz rosyjskiego wywiadu i przygotowującej akty dywersyjne przeciwko infrastrukturze transportowej unaoczniło, że działania rozpoznawcze i sabotażowe mogą poprzedzać próbę uderzenia w newralgiczne elementy systemu państwa (Sonne, Miller i Belton, 2023). W takim układzie Płock, mimo położenia poza strefą przygraniczną, pozostaje potencjalnym celem z uwagi na strategiczną rolę rafinerii i infrastruktury przesyłowej.

Możliwe scenariusze zagrożeń obejmują zarówno bezpośredni sabotaż instalacji, podpalenia, próby uszkodzenia rurociągów i węzłów logistycznych, jak i działania rozpoznawcze prowadzone z wykorzystaniem dronów lub pozornie legalnej aktywności gospodarczej. Wysokie znaczenie mają w tym kontekście środki kontrwywiadowcze, współpraca operatorów ze służbami oraz rozwijanie zdolności do wykrywania nietypowej aktywności wokół obiektów i ciągów przesyłowych.

Szczególną uwagę należy poświęcić tak zwanym miękkim punktom systemu, czyli tym elementom, które pozostają poza główną strefą ochrony, lecz są niezbędne dla funkcjonowania całości. Mogą to być węzły zasilania, połączenia teleinformatyczne, infrastruktura logistyczna lub personel obsługujący kluczowe procesy. W praktyce to właśnie uderzenie w takie elementy bywa najbardziej efektywne z punktu widzenia sprawcy.

4.3. Zagrożenie terrorystyczne

Choć Polska nie była dotychczas celem ataków terrorystycznych na skalę porównywalną z niektórymi państwami Europy Zachodniej, poziom ryzyka wzrósł wraz z wojną w Ukrainie, wsparciem udzielanym przez Polskę oraz pogorszeniem środowiska bezpieczeństwa w regionie. Utrzymywanie podwyższonych stopni alarmowych i stopni alarmowych CRP pokazuje, że państwo traktuje ochronę kluczowych obiektów jako obszar

wymagający zwiększonej czujności (Rządowe Centrum Bezpieczeństwa, 2025b).

W warunkach lokalnych oznacza to konieczność wzmacniania kontroli dostępu, przeglądów pirotechnicznych, doskonalenia procedur alarmowych i prowadzenia ćwiczeń z udziałem operatorów, służb ratowniczych oraz administracji. Istotne znaczenie mają tu również zagrożenia związane z wykorzystaniem bezzałogowych statków powietrznych. Testowanie systemów antydronowych na obiektach ORLEN wskazuje, że także ten wektor zagrożenia jest już uwzględniany w praktyce ochronnej (TVP Warszawa, 2022).

Potencjalny atak terrorystyczny na płocką IK mógłby przybrać formę użycia ładunku wybuchowego, próby podpalenia, ataku na transport substancji niebezpiecznych albo działania wymierzonego w systemy wsparcia. Znaczenie ma zatem nie tylko ochrona samego obiektu, lecz także przygotowanie planów reagowania, ewakuacji, dekontaminacji i komunikacji z ludnością. W tym kontekście duże znaczenie mają ćwiczenia praktyczne, które pozwalają przetestować zdolność współdziałania różnych służb i podmiotów (Lejman, 2022).

4.4. Dezinformacja i odporność społeczna

Współczesne zagrożenia dla infrastruktury krytycznej nie ograniczają się do fizycznego uszkadzania obiektów. Równie istotne może być wywołanie chaosu informacyjnego, paniki zakupowej albo spadku zaufania do instytucji publicznych. Pokazał to początek marca 2022 roku, gdy w mediach społecznościowych rozpowszechniano informacje o rzekomych brakach paliwa, co doprowadziło do kolejek na stacjach i lokalnych napięć na rynku (Money.pl, 2022).

Z punktu widzenia bezpieczeństwa Płocka oznacza to, że lokalne władze, operatorzy infrastruktury oraz media powinni traktować komunikację kryzysową jako jeden z filarów ochrony IK. Szybkie dementowanie nieprawdziwych informacji, przekazywanie jednoznacznych komunikatów i budowanie zaufania

społecznego ogranicza możliwość wywołania efektów destabilizacyjnych bez użycia przemocy fizycznej.

Odporność społeczna staje się zatem uzupełnieniem ochrony technicznej. Społeczeństwo, które dysponuje rzetelną informacją, zna podstawowe procedury reagowania i ufa oficjalnym kanałom komunikacji, jest mniej podatne na operacje psychologiczne. W przypadku miasta o tak wysokiej koncentracji infrastruktury strategicznej jak Płock jest to czynnik o znaczeniu porównywalnym z wybranymi środkami ochrony fizycznej i cyfrowej.

Analiza zagrożeń pokazuje, że bezpieczeństwo infrastruktury krytycznej Płocka ma charakter systemowy. Cyberataki, sabotaż fizyczny, terroryzm i dezinformacja nie funkcjonują dziś w izolacji, lecz tworzą układ zależności, w którym jedno zdarzenie może uruchamiać kolejne. Z tego względu ochrona IK wymaga nieprzerwanego monitorowania otoczenia, aktualizacji scenariuszy ryzyka oraz gotowości do reagowania na incydenty o nieprzewidywalnym przebiegu.

5. Wnioski i rekomendacje

Przeprowadzona analiza potwierdza, że Płock jest jednym z najważniejszych węzłów infrastruktury krytycznej w Polsce. Znaczenie lokalnego systemu paliwowo-energetycznego wykracza daleko poza poziom miejski, gdyż oddziałuje na bezpieczeństwo energetyczne państwa, stabilność łańcuchów dostaw oraz funkcjonowanie wielu gałęzi gospodarki. Jednocześnie właśnie ta koncentracja zasobów, instalacji przemysłowych i ciągów przesyłowych powoduje nagromadzenie ryzyk o charakterze technicznym, środowiskowym, logistycznym i politycznym.

W artykule wykazano również, że ochrona IK nie może być rozumiana wyłącznie jako ochrona pojedynczego obiektu. Musi ona obejmować cały system zależności: powiązania między produkcją, przesyłem, zasilaniem, łącznością, procedurami administracyjnymi, działaniami służb oraz odpornością społeczną. Właśnie na styku tych sfer najczęściej pojawiają się rozbieżności

proceduralne, które w sytuacji kryzysowej mogą obniżać skuteczność reakcji.

W praktyce oznacza to potrzebę wdrażania zintegrowanego modelu ochrony, obejmującego zarówno działania techniczne, jak i organizacyjne oraz komunikacyjne.

Tabela 1. Priorytetowe kierunki wzmacniania odporności infrastruktury krytycznej Płocka

Obszar	Priorytetowe działania
Cyberbezpieczeństwo	segmentacja środowisk IT/OT, monitoring systemów sterowania, kopie zapasowe, testy odporności i procedury odtwarzania działalności
Ochrona fizyczna i techniczna	modernizacja monitoringu, kontrola dostępu, zabezpieczenie rurociągów i instalacji magazynowych, rozwój systemów antydronowych i rozwiązań redundantnych
Koordynacja proceduralna	ujednolicanie planów operatorów, miasta i służb; wspólne ćwiczenia; szybka wymiana informacji; regularna aktualizacja scenariuszy reagowania
Odporność społeczna i komunikacja	sprawna komunikacja kryzysowa, współpraca z lokalnymi mediami, przeciwdziałanie dezinformacji i edukacja mieszkańców w zakresie zachowań kryzysowych

Źródło: opracowanie własne na podstawie analizy literatury i dokumentów.

Bezpieczeństwo płockiej infrastruktury krytycznej wymaga zatem równoczesnego wzmacniania ochrony fizycznej, cyfrowej i organizacyjnej. Niezbędne jest także utrzymywanie wysokiego poziomu współpracy między operatorami infrastruktury, administracją samorządową i rządową, służbami ratowniczymi oraz podmiotami odpowiedzialnymi za bezpieczeństwo państwa.

W perspektywie strategicznej przyszłość bezpieczeństwa IK Płocka będzie zależeć od zdolności do antycypowania nowych form zagrożeń i elastycznego dostosowywania procedur ochronnych do zmieniających się warunków. Tylko takie podejście pozwoli skutecznie zabezpieczyć kluczowe funkcje miasta i regionu wobec coraz bardziej złożonych i trudnych do przewidzenia wyzwań współczesnego środowiska bezpieczeństwa.

Bibliografia

a&s Polska (2024), *Cyberzagrożenia wobec infrastruktury krytycznej*, https://aspolska.pl/cyberzagrozenia-wobec-infrastruktury-krytycznej/ [dostęp: 14.06.2025].

Kublik, A. (2022), *„Rurociąg Przyjaźń. Awaria i wyciek ropy. Co się wydarzyło?"*, OKO.press, https://oko.press/rurociag-przyjazn-awaria-wyciek [dostęp: 14.06.2025].

Lejman, A. (2022), *Ćwiczenia praktyczne na terenie zakładu ORLEN PALIWA Sp. z o.o. – Rozlewnia Gazu Płynnego w Płocku, ul. Długa 1, Komenda Miejska Państwowej Straży Pożarnej w Płocku*, https://www.gov.pl/web/kmpsp-plock/cwiczenia-praktyczne-na-terenie-zakladu-orlen-paliwa-sp-z-oo--rozlewnia-gazu-plynnego-w-plocku-ul-dluga-1 [dostęp: 14.06.2025].

Ministerstwo Spraw Wewnętrznych i Administracji (2023), Narodowy Program Ochrony Infrastruktury Krytycznej 2023 – tekst jednolity, Warszawa.

Money.pl (2022), *Manipulacja cenami paliw. Ostra reakcja Orlenu*, https://www.money.pl/gospodarka/manipulacja-cenami-paliw-ostra-reakcja-orlenu-6741122558913024a.html [dostęp: 14.06.2025].

NATO Review (2021), *Wojna hybrydowa – nowe zagrożenia, złożoność i „zaufanie" jako antidotum*, https://www.nato.int/docu/review/pl/articles/2021/11/30/wojna-hybrydowa-nowe-zagrozenia-zlozonosc-i-zaufanie-jako-antidotum/index.html [dostęp: 02.06.2025].

Rządowe Centrum Bezpieczeństwa (2025a), Infrastruktura krytyczna, https://www.gov.pl/web/rcb/infrastruktura-krytyczna [dostęp: 14.06.2025].

Rządowe Centrum Bezpieczeństwa (2025b), Przedłużenie obowiązywania stopni alarmowych do 31 sierpnia 2025 r., https://www.gov.pl/web/rcb/przedluzenie-obowiazywania-stopni-alarmowych-do-31-sierpnia-2025-r [dostęp: 14.06.2025].

Ruszel, M., Ogarek, P. (2022), *Polska infrastruktura krytyczna w dobie wstrzymania rosyjskich dostaw ropy naftowej i paliw – czy jesteśmy gotowi na embargo?*, Nowa Energia, https://nowa-energia.com.pl/2022/08/10/polska-infrastruktura-krytyczna-w-dobie-wstrzymania-rosyjskich-dostaw-ropy-naftowej-i-paliw-czy-jestesmy-gotowi-na-embargo/ (dostęp: 14.06.2025).

Sawczuk, M. (2025), *„Infrastruktura krytyczna coraz częściej celem cyberataków"*, eGospodarka.pl, https://www.egospodarka.pl/192131,In-

frastruktura-krytyczna-coraz-czesciej-celem-cyberatakow,1,12,1.html [dostęp: 02.06.2025].

Sonne, P., Miller, G., Belton, C. (2023), *Russia's GRU sabotaged Ukraine weapons in Poland*, The Washington Post, https://www.washingtonpost.com/world/2023/08/18/ukraine-weapons-sabotage-gru-poland/ [dostęp: 02.06.2025].

TVP Warszawa (2022), „PKN Orlen testuje nowoczesny system antydronowy", https://warszawa.tvp.pl/63744543/pkn-orlen-testuje-nowoczesny-system-antydronowy [dostęp: 14.06.2025].

Urząd Miasta Płocka (2022), Komunikat dotyczący bezpieczeństwa funkcjonowania kompleksu przemysłowego PKN ORLEN, https://nowybip.plock.eu/dokumenty/nowybip/komunikat/2022/9730/fda4f1ee33aee4a829ec65f98b1a36f5.pdf [dostęp: 14.06.2025].

Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, Dz.U. 2007 Nr 89, poz. 590.

Wiśniewski, M. (2019), *Zarządzanie sytuacyjne bezpieczeństwem infrastruktury krytycznej państwa*, Warsaw University of Technology, Warszawa, https://repo.pw.edu.pl/info/book/WUT89ce511881f64f86a37ef2ba3beb76b0/ [dostęp: 10.06.2025].