Wydział Zarządzania
POLITECHNIKA WARSZAWSKA

Michał Wiśniewski

Zarządzanie sytuacyjne bezpieczeństwem infrastruktury krytycznej państwa

MANAGEMENT SCIENCES SERIES Vol. IX

Michał WIŚNIEWSKI

Zarządzanie sytuacyjne bezpieczeństwem infrastruktury krytycznej państwa

Wydział Zarządzania
POLITECHNIKA WARSZAWSKA

Warszawa 2019

Michał Wiśniewski

Zarządzanie sytuacyjne bezpieczeństwem infrastruktury krytycznej państwa

W monografii wykorzystano treść doktoratu, który został obroniony z wyróżnieniem w 2018 r. na Wydziale Zarządzania Politechniki Warszawskiej.

Promotor: **prof. dr hab. inż. Tadeusz KRUPA, Politechnika Warszawska**

Recenzenci: **prof. dr hab. inż. Jacek SZOŁTYSEK, Uniwersytet Ekonomiczny w Katowicach, prof. dr hab. Jerzy WOLANIN, Szkoła Główna Służby Pożarniczej**

www.wz.pw.edu.pl

ISBN 978-83-63370-32-9
ISBN 978-83-63370-33-6

Projekt okładki: Marcin Król
Opracowanie wydawnicze: Anna Skrok, Marta Pobereszko, Joanna Iwanowska

Wydawnictwo Naukowe Instytutu Technologii Eksploatacji – Państwowego Instytutu Badawczego
Radom, ul. K. Pułaskiego 6/10, tel. centr. 48 36 442 41, fax 48 36 447 65
e-mail: instytut@itee.radom.pl, http://www.itee.radom.pl

Spis treści

Wprowadzenie **5**

Rozdział 1. Uwarunkowania zarządzania bezpieczeństwem IK w Polsce **11**
1.1. Infrastruktura krytyczna Polski i Unii Europejskiej 11
1.2. Stosowane metodyki zarządzania bezpieczeństwem IK 20
1.3. Uwarunkowania formalnoprawne zarządzania bezpieczeństwem IK 25
1.4. Ujęcia teoretyczne i praktyczne 27
1.5. Technologie wykorzystywane w procesie zarządzania bezpieczeństwem IK 44
1.6. Wnioski z rozdziału 46

Rozdział 2. Integralny model bezpieczeństwa IK **47**
2.1. Struktura integralnego modelu bezpieczeństwa IK 47
2.2. Model sytuacji IK 49
2.3. Metoda szacowania ryzyka 57
2.4. Metoda generowania scenariuszy przebiegu zdarzenia niekorzystnego 62
2.5. Metoda formułowania problemu decyzyjnego 70
2.6. Wnioski z rozdziału 80

Rozdział 3. Metodyka zarządzania sytuacyjnego bezpieczeństwem IK **83**
3.1. Charakterystyka etapów metodyki ZS-BIK 83
3.2. Zastosowanie metodyki ZS-BIK dla płaskiego problemu decyzyjnego 90
3.3. Zastosowanie metodyki ZS-BIK dla hierarchicznego problemu decyzyjnego 93
3.4. Wnioski z rozdziału 97

Rozdział 4. Studium wykonalności metodyki ZS-BIK **99**
4.1. Opis założeń studium wykonalności 99
4.2. Przykład płaskiego problemu decyzyjnego 100
4.3. Przykład hierarchicznego problemu decyzyjnego 119
4.4. Wnioski z rozdziału 127

Podsumowanie **131**

Bibliografia **133**
Pozycje literaturowe 133
Akty prawne/plany 138
Źródła internetowe 140
Tezaurus pojęć **141**
Skróty i oznaczenia stosowane w tekście **155**
Spis rysunków **159**
Spis tabel **161**
Załączniki **165**
Załącznik A – Implementacja modelu sytuacji IK w narzędziu symulacyjnym 166
Załącznik B – Implementacja procedury budowy problemu decyzyjnego w narzędziu informatycznym 172
Załącznik C – Przykłady obliczeniowe zastosowania elementów IM-BIK 176
Załącznik D – Wykaz scenariuszy zdarzeń niekorzystnych dla rafinerii PKN ORLEN S.A. 190
Załącznik E – Wybrane akty normatywne i planistyczne dotyczące zarządzania bezpieczeństwem IK 201
Załącznik F – Charakterystyka metodyk oceny ryzyka na potrzeby zarządzania kryzysowego 205
Załącznik G – Wykaz zależności i współzależności systemów IK 221

Wprowadzenie

Niniejsza monografia stanowi podsumowanie badań przeprowadzonych przez autora, które dotyczyły zagadnienia bezpieczeństwa infrastruktury krytycznej[1]. Ich efektem jest integralny model bezpieczeństwa infrastruktury krytycznej[2] (IM-BIK) oraz bazująca na nim metodyka zarządzania sytuacyjnego bezpieczeństwem IK[3] (ZS-BIK).

Genezą zaobserwowanego problemu badawczego dotyczącego bezpieczeństwa IK jest ciągły rozwój cywilizacyjny, który prowadzi do uzależniania się społeczeństwa od szeroko rozumianej infrastruktury, co sprawia, że ludzie przestają być samowystarczalni. Część infrastruktur, od których zależne jest społeczeństwo to tzw. infrastruktura krytyczna[4] (IK). IK państwa podzielona jest na systemy IK[5], których prawidłowe funkcjonowanie jest warunkiem koniecznym stabilności bezpieczeństwa narodowego w obszarze:

- rozwoju gospodarczego,
- suwerenności państwa,
- wzrostu standardu życia ludności.

Ograniczenie funkcjonalności[6] systemów IK skutkuje [Wiśniewski, Ostrowska, 2016, s. 121; Manas, 2017, ss. 239; Hatton, Brown, Kipp, et al. 2018, ss. 59–61]:

---

[1] Bezpieczeństwo IK – stan powstały w wyniku zastosowania zabezpieczeń przed zagrożeniami, w którym ryzyko utraty funkcjonalności jest niższe niż wynika to z akceptowanej wartości ryzyka jej utraty.

[2] Integralny model bezpieczeństwa IK – zbiór pojęć umożliwiający modelowe odwzorowanie sytuacji IK należącej do dowolnego systemu IK, rozpoznanie przebiegu zdarzeń niekorzystnych, oszacowanie ryzyka wynikającego z zagrożeń, na które podatna jest IK oraz określenie problemu decyzyjnego dotyczącego zabezpieczeń IK przed rozpoznanymi zagrożeniami.

[3] Metodyka zarządzania sytuacyjnego bezpieczeństwem IK – zbiór etapów, pozwalających na: określnie sytuacji IK, oszacowanie wartości ryzyka wynikającego z sytuacji IK oraz sformułowanie problemu decyzyjnego mającego na celu wskazać zabezpieczenia utrzymujące dostępność funkcjonalności powyżej progu bezpieczeństwa, gdzie wyniki uzyskane z wykonania etapu poprzedzającego stanowią dane wejściowe dla kolejnego etapu.

[4] Infrastruktura krytyczna – to systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców [Dz.U. 2017 poz. 209, art. 3, pkt 2], podzielone na 11 systemów IK.

[5] System IK – układ wzajemnie powiązanych elementów IK, stanowiących logicznie uporządkowaną całość, realizujący zbiór funkcjonalności: system zaopatrzenia w energię, surowce energetyczne i paliwa, system łączności, system sieci teleinformatycznych, system finansowy, system zaopatrzenia w żywność, system zaopatrzenia w wodę, system ochrony zdrowia, system transportowy, system ratowniczy, system zapewniający ciągłość działania administracji publicznej, system produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych

[6] Funkcjonalność – zbiór funkcji urządzenia, oprogramowania lub systemu określających zdolność do zaspokajania potrzeb użytkownika w określonych warunkach.

- poważnymi stratami ekonomicznymi,
- skażeniem środowiska naturalnego,
- realnym zagrożeniem dla zdrowia i życia ludności.

Ze względu na swoją rolę obiekty należące do IK powinny podlegać ochronie zmierzającej do ograniczania ryzyka utraty funkcjonalności, w większości bez względu na ekonomiczną opłacalność działań zabezpieczających.

Obowiązek zapewnienia bezpieczeństwa IK spoczywa na jej operatorze. W Polsce są to przede wszystkim przedsiębiorcy prywatni [Biała księga, 2013, s. 100; Radziejewski, 2014, s. 52]. Konieczność utrzymywania systemów rezerwowych podtrzymujących dostępność funkcjonalności IK do czasu jej pełnego odtworzenia [NPOIK, 2015, s. 16] wprowadza rozbieżność między celami biznesowymi operatorów IK[7] a oczekiwaniem społeczeństwa dotyczącym funkcjonalności IK[8].

Operatorzy IK [Dz.U. 2013 r. poz. 1166, art. 6, pkt 1] są zobowiązani ustawowo do realizacji zadań z zakresu zarządzania:

- gromadzenia i przetwarzania informacji dotyczących zagrożeń,
- opracowywania i wdrażania procedur na wypadek ich wystąpienia,
- współpracy z administracją publiczną i innymi operatorami IK.

Realizacja obowiązków operatorów IK jest utrudniona przez rosnącą liczbę systemów uznawanych za IK, które nieustannie wzajemnie oddziałują, tworząc sieć zależności [Korzeniowska, ss. 19–20; Szewczyk, Pyznar, 2010, ss. 54–55; Alcaraz, Zeadally, 2015, s. 54; Macaulty, 2016, s. 27–32; Stergiopoulos, Kotzanikolaou, Theocharidou, et al. 2016; Chen, Milanovic, 2017, s. 600; Bloomfield, Popov, Salako, 2017, ss. 198–217], w ramach której realizują się scenariusze zdarzeń niekorzystnych[9] (SZN). Scenariusze te należy uwzględnić, rozważając zabezpieczenia dla IK [Zielona Księga, 2005, s. 3, pkt 2; Wiśniewski, 2015, ss. 8511–8521; Edi, Rosato, 2016, s. 44; Pescaroli, Kelman, 2017, ss. 56–67]. Obecnie akty normatywne nie wskazują metod generowania SZN oraz nie definiują tego pojęcia, pozostawiając jego interpretację operatorom IK.

---

[7] Operator IK jest zainteresowany wypełnieniem obowiązku narzuconego przepisami, ponosząc możliwie niskie koszty, natomiast społeczeństwo oczekuje nieprzerwanej dostępności funkcjonalności IK, np. produkcji paliw.

[8] Dowodem na istnienie rozbieżności celów i jednocześnie sposobem częściowo rozwiązującym problem są założenia NPOIK dotyczące finansowania ochrony IK w ramach partnerstwa publiczno-prywatnego [NPOIK, 2015, s. 44]. Przykładem takiego działania jest budowa Terminalu LNG w Świnoujściu przez firmę Gaz-System S.A. (właściciela Polskie LNG S.A.). Powstanie Terminalu LNG miało ograniczyć negatywne skutki wahających się dostaw gazu z Federacji Rosyjskiej dla odbiorców prywatnych i przemysłowych i wzmocnić pozycję negocjacyjną Polski przy ustalaniu przyszłych cen dostarczanego gazu. Koszt inwestycji to 3,04 mld PLN. Część nakładów inwestycyjnych została sfinansowana z dotacji Unii Europejskiej z Programu Operacyjnego Infrastruktura i Środowisko 2007–2013 oraz z European Energy Programme for Recovery (EEPR). Łącznie budowę Terminalu LNG w Świnoujściu dofinansowano w kwocie 1,42 mld PLN, co stanowi około 46,7% kosztów inwestycji [www.gaz-system.pl/terminal-lng/finansowanie, data odczytu 27.06.2017].

[9] Scenariusz zdarzenia niekorzystnego – opis zdarzeń mogących wywołać sytuację kryzysową, pozwalający na określenie sposobu reagowania w przypadku zmaterializowania się zagrożeń [Kosieradzka, Zawiła-Niedźwiecki, 2016, s. 368].

Wymianę informacji warunkującą skuteczną ochronę IK między podmiotami odpowiedzialnymi za bezpieczeństwo IK komplikuje fakt, że przepisy (Polskie oraz Unii Europejskiej) definiują zadania jednostek administracji publicznej oraz operatów IK w sposób ogólny, pozostawiając im dowolność w zakresie raportowania danych oraz metod, jakimi dane te są gromadzone [Tyburska, 2009, s. 96; Krupa, Wiśniewski, 2015, s. 94; Lidwa, 2015, ss. 165–176].

Brak jednolitego systemu pojęciowego[10] oraz metodyki zarządzania bezpieczeństwem IK jest przyczyną trudności w koordynacji ochrony IK, utrudnia wzajemną wymianę doświadczeń i pociąga za sobą ryzyko pozostawienia obszaru, w którym brak koordynacji działań podmiotów odpowiedzialnych za bezpieczeństwo IK może doprowadzić do eskalacji zagrożenia i skutków jego wystąpienia. Stąd problemem badawczym jest opracowanie wspólnego systemu pojęć oraz jednolitej metodyki zarządzania bezpieczeństwem IK możliwych do stosowania przez wszystkie podmioty odpowiedzialne za bezpieczeństwo IK.

Znaczenie IK dla bezpieczeństwa narodowego, rosnący stopień wzajemnej zależności systemów IK, konieczność wymiany informacji przez podmioty odpowiedzialne za bezpieczeństwo IK, nieprecyzyjne przepisy prawne oraz rozbieżność między celami biznesowymi operatorów IK i oczekiwaniem społeczeństwa prowadzą do narastania luki dotyczącej prac nad wspólnym systemem pojęciowym oraz jednolitą metodyką zarządzania bezpieczeństwem IK.

Doświadczenia zebrane podczas realizacji prac badawczych[11] pozwoliły na sprecyzowanie problemu badawczego do zagadnienia modelowego odwzorowania istoty funkcjonalności IK i określenia problemu decyzyjnego umożliwiającego efektywny dobór zabezpieczeń chroniących przed jej utratą.

Stąd przedmiotem niniejszego opracowania jest integralny model bezpieczeństwa infrastruktury krytycznej (IM-BIK) oraz bazująca na nim metodyka zarządzania sytuacyjnego bezpieczeństwem infrastruktury krytycznej (ZS-BIK), których opracowanie warunkuje efektywną wymianę informacji między podmiotami odpowiedzialnymi za bezpieczeństwo IK.

---

[10] Wynikający z częstych zmian definicji IK – w 1996 r. Zarządzenie prezydenta USA 13010, 1998 r. Prezydencka Dyrektywa nr 63(PDD-63) USA, 2003 r. Prezydencka Dyrektywa nr 7 (HSPD-7) USA, 2005 r. Zielona księga w sprawie Europejskiego programu ochrony Infrastruktury Krytycznej, 2007 r. Decyzja Rady Unii Europejskiej z dnia 12 lutego 2007 r. ustanawiająca na lata 2007–2013 jako część ogólnego programu w sprawie bezpieczeństwa i ochrony wolności, szczegółowy program „Zapobiegania, gotowości i zarządzanie skutkami terroryzmu i innymi rodzajami ryzyka dla bezpieczeństwa", Polska Ustawa o zarządzaniu kryzysowym z dnia 26 kwietnia 2007 r., 2008 r. Dyrektywa Rady 2008/114/WE z dnia 8 grudnia 2008 r. w sprawie rozpoznania i wyznaczenia europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie jej poprawy, 2013 r. Narodowy program ochrony infrastruktury krytycznej (Polska), 2013 r. Decyzja Parlamentu Europejskiego i Rady Nr 1313/2013/EU z dnia 17 grudnia 2013 r. w sprawie Unijnego Mechanizmu Ochrony Ludności Dz.U. UE z dnia 20 grudnia 2013 r.

[11] W ramach projektu finansowanego ze środków NCBiR pt. „Metodyka oceny ryzyka na potrzeby systemu zarządzania kryzysowego RP" oraz „Wysokospecjalistyczna platforma wspomagająca planowanie cywilne i ratownictwo w administracji publicznej RP oraz w jednostkach organizacyjnych Krajowego Systemu Ratowniczo Gaśniczego".

Przedmiot opracowania wskazuje na dwa pytania badawcze:

- Jakie elementy musi zawierać IM-BIK, aby móc stanowić zaplecze narzędziowe dla metodyki ZS-BIK?
- Jakie etapy postępowania powinna zawierać metodyka ZS-BIK, aby umożliwić zarządzanie bezpieczeństwem IK, uwzględniając wszystkie podmioty odpowiedzialne za bezpieczeństwo IK?

Podstawione pytania badawcze wskazują na dwie grupy zagadnień:

- integralny model bezpieczeństwa infrastruktury krytycznej (rozdz. 2), obejmujący:
  - koncepcję IM-BIK (rozdz. 2.1),
  - modelowe odwzorowanie zabezpieczeń i zagrożeń funkcjonalności zasobów IK (rozdz. 2.2), w tym model formalny SZN (rozdz. 2.4),
  - mierniki IM-BIK (rozdz. 2.3),
  - podejmowanie decyzji dotyczących reakcji na zagrożenia (rozdz. 2.5),
- metodykę zarządzania sytuacyjnego bezpieczeństwem infrastruktury krytycznej (rozdz. 3), obejmująca:
  - organizacyjne aspekty ZS-BIK (rozdz. 3.1), w tym:
    - powołanie zespołu ZS-BIK,
    - określenie progów bezpieczeństwa,
    - określenie charakterystyk IK,
    - formalny opis SZN,
    - sformułowanie problemu decyzyjnego,
    - analizę i szacowanie ryzyka,
    - podjęcie decyzji w sprawie wdrożenia zabezpieczeń,
  - procedury wykonania metodyki ZS-BIK dla płaskiego (rozdz. 3.2) i hierarchicznego (rozdz. 3.3) problemu decyzyjnego,
  - opis eksperymentów obliczeniowych (rozdz. 4.1),
  - procedury zastosowania metodyki ZS-BIK dla płaskiego (rozdz. 4.2) i hierarchicznego (rozdz. 4.3) problemu decyzyjnego,
  - ocenę metodyki ZS-BIK (rozdz. 4.4).

Prace nad IM-BIK oraz ZS-BIK pozwoliły na uporządkowanie i zintegrowanie procedur postępowania przez podmioty odpowiedzialne za bezpieczeństwo IK. Wspólna metodyka ZS-BIK jest warunkiem przyspieszenia procesu uzgadniania planów ochrony infrastruktury krytycznej (POIK) oraz skutecznego podejmowania działań prewencyjnych i naprawczych. Za pomocą metodyki ZS-BIK rozwiązywane są dwa odmienne rodzaje problemów decyzyjnych:

- płaskie problemy decyzyjne[12],
- hierarchiczne problemy decyzyjne[13].

[12] Płaski problem decyzyjny – zbiór obszarów decyzyjnych wyznaczonych przez zagrożenia, na które podatna jest IK, których ryzyko nie pozwala na osiągnięcie założonego progu bezpieczeństwa i w stosunku do których rozstrzygnięcia zapadają na jednym poziomie decyzyjnym. Zagrożenia są wyznaczane na podstawie sytuacji rozpatrywanej IK lub SZN.

[13] Hierarchiczny problem decyzyjny – zbiór obszarów decyzyjnych wyznaczonych przez zagrożenia, na które podatna jest IK, których ryzyko nie pozwala na osiągnięcie założonego progu bezpieczeństwa, dla których rozstrzygnięcia o zabezpieczeniach nie zapadają na jednym poziomie decyzyjnym. Zagrożenia są wyznaczane na podstawie sytuacji rozpatrywanej IK lub SZN.

Metodykę ZS-BIK zweryfikowano na podstawie eksperymentów obliczeniowych, które zostały przeprowadzone na danych pozyskanych z Planów Zarządzania Kryzysowego[14] (PZK). Eksperymenty wykonano w celu potwierdzenia użyteczności metodyki ZS-BIK dla podmiotów odpowiedzialnych za bezpieczeństwo IK. Wykonano dwa eksperymenty, po jednym dla przypadku płaskiego i hierarchicznego problemu decyzyjnego.

Nierozłączną częścią opracowania jest tezaurus, w którym zawarto system pojęć stosowanych w opracowaniu oraz załączniki uzupełniające rozważania teoretyczne przedstawione w rozdziałach zasadniczych o pełne przykłady obliczeniowe ilustrujące sposób wykonania IM-BIK.

Opracowanie przeznaczone jest dla teoretyków i praktyków związanych z procesem planowania cywilnego, zarządzania kryzysowego oraz zajmujących się planowaniem ochrony infrastruktury krytycznej. Monografia może stanowić również podręcznik akademicki dla studentów kierunków: bezpieczeństwo publiczne, bezpieczeństwo narodowe, zarządzanie bezpieczeństwem, zarządzanie bezpieczeństwem infrastruktury krytycznej, którzy zrealizowali kurs podstawowy z zakresu zarządzania ryzykiem.

[14] Pozyskano dane z dokumentacji PZK Powiatu Płockiego z 2015 r.

Rozdział 1. Uwarunkowania zarządzania bezpieczeństwem IK w Polsce

Zarządzanie bezpieczeństwem infrastruktury krytycznej mieści się obecnie w jednym z najbardziej dynamicznie rozwijających się obszarów badań, jakim jest szeroko rozumiane bezpieczeństwo. O ile dobrze rozpoznane są podwaliny teoretyczne i praktyczne analizy ryzyka będącego miarą bezpieczeństwa, o tyle cały obszar zarządzania ryzykiem (bezpieczeństwem), w szczególności w Polsce, wymaga jeszcze dużo wysiłku w sferze nauki i praktyki. Problem ten jest szczególnie widoczny w obszarze zarządzania bezpieczeństwem IK, który w Polsce został uregulowany dopiero w 2007 r. ustawą o zarządzaniu kryzysowym. Uregulowanie prawne nie oznacza jednak wyeliminowania wszystkich niejasności a tym bardziej wprowadzenia metodycznego podejścia do omawianego zagadnienia. Dlatego w niniejszym rozdziale wykonano:

- uporządkowanie pojęć z zakresu zarządzania bezpieczeństwem IK (rozdz. 1.1),
- analizę metodyk oceny ryzyka na potrzeby zarządzania kryzysowego stosowane w USA, Australii, wybranych krajach UE oraz polskie procedury stosowane w tym zakresie w celu określenia bazowych etapów metodyki ZS-BIK oraz składowych IM-BIK (rozdz. 1.2),
- identyfikację uwarunkowań formalnoprawnych dotyczących ochrony IK, zarządzania kryzysowego i planowania cywilnego, które pozwoliły na wskazanie kanonu charakterystyki IK (rozdz. 1.3).

Ponadto określono koncepcję rozwiązania zaobserwowanych problemów w przestrzeni zarządzania bezpieczeństwem IK poprzez dobór metod z obszaru odwzorowania charakterystyki obiektu, formułowania scenariuszy zdarzeń, szacowania ryzyka i rozwiązywania problemów decyzyjnych możliwych do zastosowania w IM-BIK (rozdz. 1.4) oraz identyfikacji narzędzi informatycznych wspomagających proces zarządzania bezpieczeństwem IK, które stanowią źródła danych dla metodyki ZS-BIK (rozdz. 1.5).

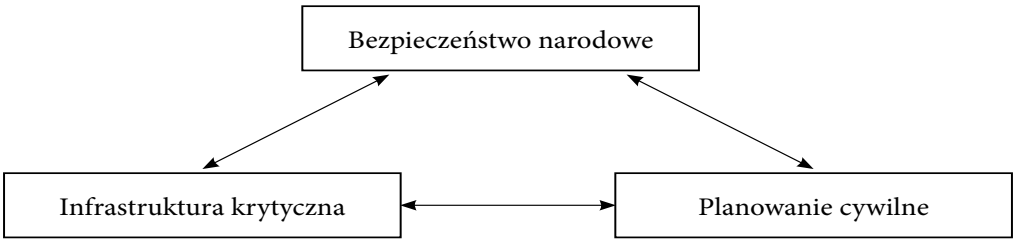
1.1. Infrastruktura krytyczna Polski i Unii Europejskiej

Bezpieczeństwo narodowe w obszarze rozwoju gospodarczego, suwerenności państwa oraz wzrostu standardu życia ludności jest uzależnione od funkcjonalności IK podatnych na zagrożenia[15] [Lidwa, Krzeszowski, Więcek, Kmiński, 2012, ss. 10–14; Rehak, Markuci, Hormada, et al. 2016, ss. 3–4; Pursiainen, 2018, ss. 635–637]. Nośnikiem funkcjonalności są obiekty zabezpieczane w ramach procesu planowania cywilnego[16],

[15] Zagrożenie – spodziewane oddziaływanie na zasoby lub między zasobami, w wyniku którego mogą ulec degradacji ich cechy funkcjonalno-strukturalne.

[16] Planowanie cywilne – działania mające na celu przygotowanie administracji publicznej do zarządzania

którego uzupełnieniem jest zarządzanie kryzysowe[17] [Kulińska, Dornnfeld, 2009, ss. 53–60; Kaczmarek, 2010, ss. 129–131; Krupa, Wiśniewski, 2016, ss. 301–302]. Wymienione zależności wskazują na związek pojęć: bezpieczeństwo narodowe, planowanie cywilne i IK (rys. 1.1a).



Rysunek 1.1a. Zależność pojęć bezpieczeństwo narodowe – planowanie cywilne – infrastruktura krytyczna
Źródło: opracowanie własne.

Ochrona IK to złożony proces wykraczający poza granice państwa, na terenie którego IK jest zlokalizowana. Przykład tego procesu stanowi Europejska Infrastruktura Krytyczna[18] (EIK) chroniona w ramach Europejskiego Programu Ochrony Infrastruktury Krytycznej (EPOIK). Podejmowane inicjatywy w celu ochrony EIK są regulowane przez międzynarodowe przepisy[19], które mają zapewnić ciągłość funkcjonowania IK, przede wszystkim dzięki wzajemnemu informowaniu i ostrzeganiu [Tyburska, Nalepski, 2008, s. 22; Radziejewski, 2014, s. 44; Caldwell, 2015, ss. 5096–5097; Hofreiter, Zvakova, 2016, ss. 139–140; Kosieradzka, Zawiła-Nedźwiecki, 2016, s. 20, Skomra, 2017, ss. 245––246; Häyhtiö, Zaerens, 2017, ss. 45–47]. Proces wzajemnej wymiany informacji jest utrudniony ze względu na brak jednolitej definicji IK w różnych systemach prawnych. Przykładem rozbieżności definicji IK w powiązanych systemach prawnych są terminy stosowane w UE oraz Polsce:

kryzysowego, planowania w zakresie wspierania Sił Zbrojnych Rzeczpospolitej Polskiej w razie ich użycia oraz planowanie wykorzystania Sił Zbrojnych Rzeczpospolitej Polskiej do realizacji zadań z zakresu zarządzania kryzysowego [Dz.U. 2017 poz. 209, art. 3, pkt 4].

[17] Zarządzanie kryzysowe – działalność organów administracji publicznej będąca elementem kierowania bezpieczeństwem narodowym, która polega na zapobieganiu sytuacjom kryzysowym, przygotowaniu do przejmowania nad nimi kontroli w drodze zaplanowanych działań, reagowaniu w przypadku wystąpienia sytuacji kryzysowych, usuwaniu ich skutków oraz odtwarzaniu zasobów i infrastruktury krytycznej [Dz.U. 2017 poz. 209, art. 2].

[18] Europejska IK – systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia i instalacje kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców, wyznaczone w systemach infrastruktury krytycznej w zakresie energii elektrycznej, ropy naftowej i gazu ziemnego oraz transportu drogowego, kolejowego, lotniczego, wodnego śródlądowego, żeglugi oceanicznej, żeglugi morskiej bliskiego zasięgu i portów, zlokalizowane na terytorium państw członkowskich Unii Europejskiej, których zakłócenie lub zniszczenie miałoby istotny wpływ na co najmniej dwa państwa członkowskie [Dz.U. 2017 poz. 209, art. 3].

[19] W szczególności: Dyrektywa Rady 2008/114/WE z 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania EIK oraz oceny potrzeb w zakresie poprawy jej ochrony.

- definicja IK stosowana w UE: infrastruktura krytyczna – składnik, system lub część infrastruktury, zlokalizowane na terytorium państw członkowskich, które mają podstawowe znaczenie dla utrzymania niezbędnych funkcji społecznych, zdrowia, bezpieczeństwa, ochrony dorobku materialnego lub społecznego ludności oraz których zakłócenie lub zniszczenie miałoby istotny wpływ na dane państwo członkowskie w wyniku utracenia tych funkcji [Dz.U.UE 2008 nr 345 poz. 75, art. 2b],
- definicja IK stosowana w Polsce: infrastruktura krytyczna – systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi, kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców [Dz.U. 2017 poz. 209, art. 3, pkt 2].

Definicja IK stosowana przez UE podkreśla znaczenie funkcjonalności IK, co sugeruje, że w procesie zarządzania bezpieczeństwem IK należy kłaść nacisk przede wszystkim na ochronę funkcjonalności IK oraz jej odtworzenie w przypadku uszkodzenia lub zniszczenia IK[20]. W przypadku polskiej definicji IK akcentowane są obiekty dostarczające świadczeń, od których zależne jest społeczeństwo, gospodarka oraz administracja publiczna.

Różnice w pojmowaniu IK przez systemy prawne skutkują odmienną definicją ochrony IK:

- definicja ochrony IK stosowana w UE: ochrona IK – wszelkie działania zmierzające do zapewnienia funkcjonalności, ciągłości działania i integralności IK w celu zapobiegania zagrożeniom, ryzykom lub słabym punktom oraz ograniczania i neutralizacji ich skutków [Dz.U.UE 2008 nr 345 poz. 75, art. 2e],
- definicja ochrony IK stosowana w Polsce: ochrona IK – wszelkie działania zmierzające do zapewnienia funkcjonalności, ciągłości działań i integralności infrastruktury krytycznej w celu zapobiegania zagrożeniom, ryzykom lub słabym punktom oraz ograniczenia i neutralizacji ich skutków oraz szybkiego odtworzenia tej infrastruktury na wypadek awarii, ataków oraz innych zdarzeń zakłócających jej prawidłowe funkcjonowanie [Dz.U. 2017 poz. 209, art. 3, pkt 3].

Analizując treść obu definicji, widać rozbieżność. W polskiej definicji dodano fragment wskazujący na konieczność odtworzenia IK. Natomiast definicja UE koncentruje się na przywróceniu funkcjonalności IK. Może to prowadzić do innego ukierunkowania zadań przewidzianych w Planie Ochrony Infrastruktury Krytycznej (POIK), które skupią się na odbudowie IK w celu przywrócenia funkcjonalności, zamiast na odtworzeniu funkcjonalności IK np. na innych dostępnych zasobach.

Różnice wynikające z odmiennych definicji IK są również widoczne na liście systemów IK UE i Polski (tab. 1.1a).

[20] Obserwacja jest zbieżna z dokumentem Access to Essential Services. Nowe podejście do identyfikacji obiektów krytycznych zostało przedstawione w dyrektywie NIST z dnia 21 kwietnia 2016 r. w sprawie bezpieczeństwa sieci i systemów teleinformatycznych. Państwa członkowskie są zobowiązane do włączenia zapisów tej dyrektywy do prawa krajowego w ciągu 21 miesięcy od czasu jej przyjęcia.

Tabela 1.1a. Zestawienie systemów IK w UE i Polsce

Europejskie systemy IK	Polskie systemy IK
• energia • przemysł jądrowy • technologie informacyjno-komunikacyjne • woda • żywność • zdrowie • sektor finansowy • transport • przemysł chemiczny • przemysł kosmiczny • infrastruktura badawcza	• system zaopatrzenia w energię, surowce energetyczne i paliwa • system łączności • system sieci teleinformatycznych • system finansowy • system zaopatrzenia w żywność • system zaopatrzenia w wodę • system ochrony zdrowia • system transportowy • system ratowniczy • system zapewniający ciągłość działania administracji publicznej • system produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych

Źródło: Dz.U.UE 2008 nr 345 poz. 75, art. 2b i Dz.U. 2017 poz. 209, art. 3, pkt 2.

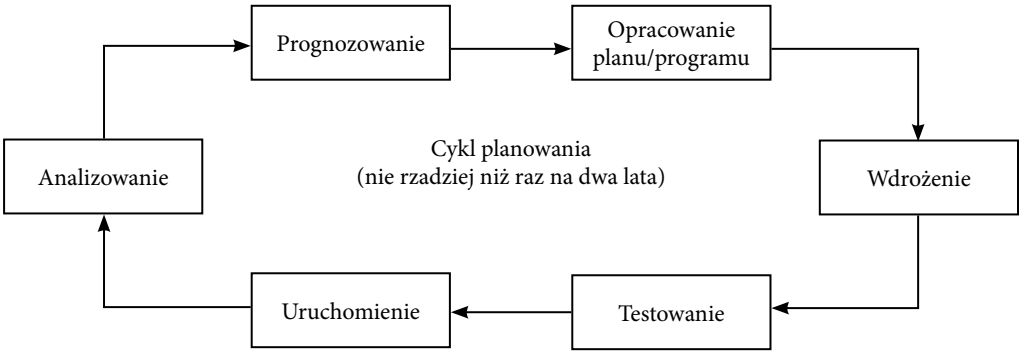
Brak wspólnego systemu pojęciowego oraz rozproszenie przepisów dotyczących ochrony IK [Stec, 2011, ss. 181–197] utrudnia opracowanie scenariuszy zdarzeń niekorzystnych[21] (SZN) [Ouyang, 2014, ss. 43–44; Pescaroli, Alexander, 2016, ss. 175–177], których umieszczenie w POIK jest usankcjonowane prawnie w UE oraz w Polsce[22]. Obowiązujące przepisy nie definiują, jakimi metodami SZN mają być opracowane ani co mają zawierać [Wiśniewski, Kunikowski, Kisilowski, 2016, ss. 97–110]. Sytuację komplikuje fakt, że podmioty odpowiedzialne za bezpieczeństwo IK[23] posługują się różnymi wykazami zagrożeń[24]. Obecnie ze względu na brak dedykowanych metod i narzędzi zarządzania bezpieczeństwem IK w Polsce ochrona IK jest zapewniana w ramach procesu planowania cywilnego realizowanego w tzw. cyklu planowania, który został zobrazowany na rys. 1.1b.

[21] Zdarzenie niekorzystne – zdarzenie będące efektem spełnienia się zagrożenia, mające negatywne skutki dla organizacji, środowiska naturalnego lub ludności.

[22] Dyrektywa Parlamentu Europejskiego I Rady (UE) 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii Dz.U.UE 2016 nr 194 poz. 1, s. 7; Dyrektywa Rady 2008/114/WE z dnia 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie jej ochrony Dz.U.UE 2008 nr 345 poz. 75, zał II, art. 2; Procedura opracowywania raportu cząstkowego do RZBN, ss. 10–18.

[23] Podmioty odpowiedzialne za bezpieczeństwo IK – jednostki operacyjne realizujące zadania dotyczące bezpieczeństwa IK na określonych poziomach decyzyjnych określone w Ustawie z dnia 26 kwietnia 2017 r. o zarządzaniu kryzysowym (Dz.U. 2007 nr 89 poz. 590).

[24] Przykład rozbieżności dotyczących klasyfikacji zagrożeń, sposobu opisu skutków materializacji zagrożeń oraz obszarów działań podejmowanych w celu zabezpieczenia się przed rozpoznanymi zagrożeniami można znaleźć np. w Wojewódzkich PZK Województwa Mazowieckiego i Województwa Podlaskiego z 2015 r.



Rysunek 1.1b. Cykl planowania cywilnego
Źródło: Dz.U. 2017 poz. 209, 2007.

Proces planowania cywilnego[25] jest realizowany przez wszystkie poziomy administracji publicznej i jest nadzorowany przez Rządowe Centrum Bezpieczeństwa (RCB). RCB opracowuje Krajowy Plan Zarządzania Kryzysowego (KPZK), a następnie na jego podstawie powstają wojewódzkie, powiatowe i gminne Plany Zarządzania Kryzysowego (PZK). Opracowanie KPZK jest poprzedzone zebraniem danych dotyczących zagrożeń dla bezpieczeństwa narodowego w postaci Raportów o Zagrożeniach Bezpieczeństwa Narodowego (RZBN).

Obowiązek sporządzenia RZBN mają ministerstwa, urzędy centralne oraz wojewodowie. Na poziomie powiatu i gminy nie ma ustawowego obowiązku opracowania RZBN, dlatego decyzja o ich opracowaniu jest podejmowana przez lokalne władze. Koordynatorem procesu opracowywania RZBN jest RCB, które na podstawie zabranych raportów cząstkowych sporządza zbiorczy RZBN. W odpowiedzi na zbiorczy RZBN powstaje KPZK.

Do zadań procesu planowania cywilnego należy [Dz.U. 2017 poz. 209, 2007, art. 4, ust. 1]:

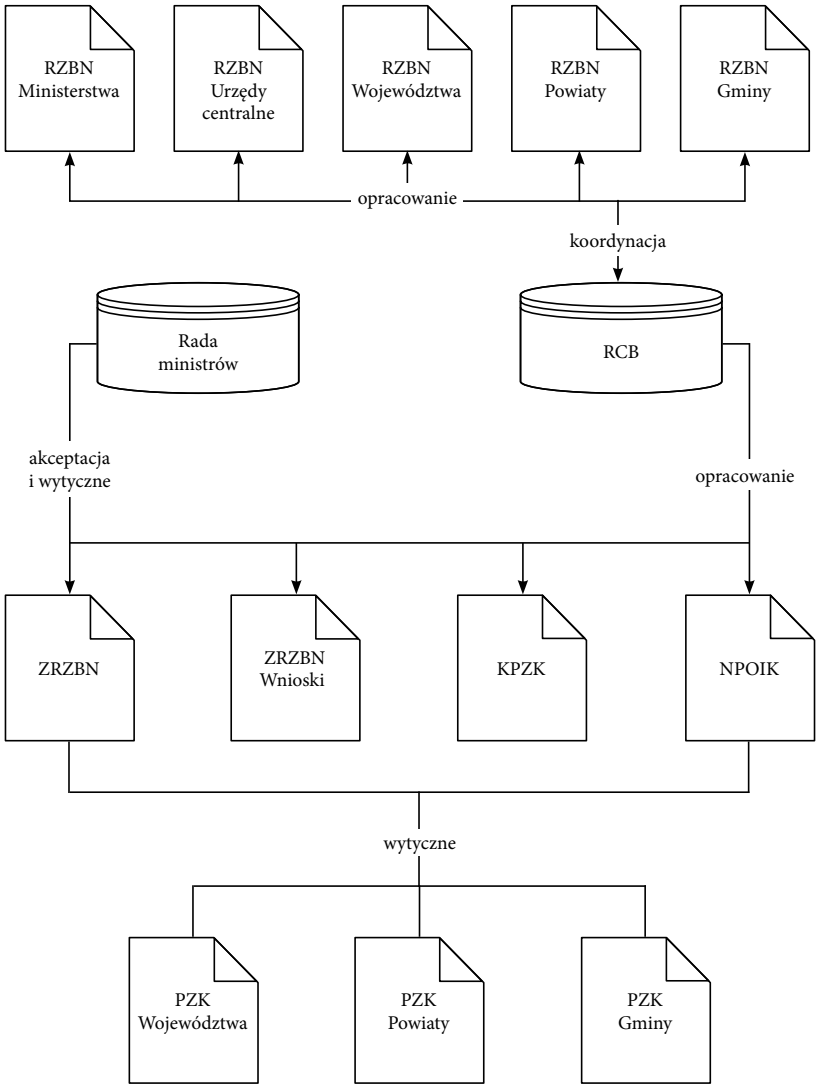
- przygotowanie planów zarządzania kryzysowego,
- przygotowanie struktur uruchamianych w sytuacjach kryzysowych,
- przygotowanie i utrzymanie zasobów niezbędnych do wykonania zadań ujętych w planie zarządzania kryzysowego,
- utrzymywanie baz danych niezbędnych w procesie zarządzania kryzysowego,
- przygotowanie rozwiązań na wypadek zniszczenia lub zakłócenia funkcjonowania infrastruktury krytycznej,
- zapewnienie spójności między planami zarządzania kryzysowego a innymi planami sporządzonymi w tym zakresie przez właściwe organy administracji publicznej, których obowiązek wynika z odrębnych przepisów (np. plan ochrony przeciwpożarowej).

W ramach obowiązującej procedury planowania cywilnego powstaje również NPOIK określający zadania dla operatorów IK dotyczące ochrony IK [Dz.U. 2017 poz. 209]. Zadania dla uczestników NPOIK dotyczą [NPOIK, 2015, s. 16]:

[25] Cele zdefiniowane w ramach ustawy o zarządzaniu kryzysowym [Dz.U. 2017 poz. 209, art. 4].

- przygotowania POIK,
- utrzymywania niezbędnych systemów zapasowych,
- uzgadniania POIK z innymi operatorami, a także jednostkami administracji publicznej.

Całość procesu planowania cywilnego przedstawiono na rys. 1.1c.

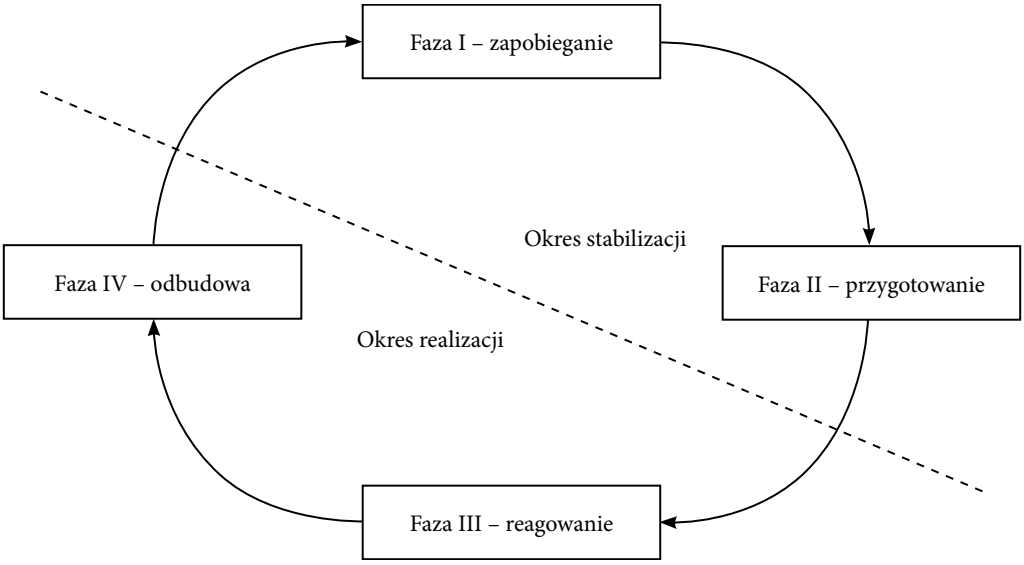


(NPOIK – Narodowy Program Ochrony IK, KPZK – Krajowy Plan Zarządzania Kryzysowego, PZK – Plan Zarządzania Kryzysowego, RCB – Rządowe Centrum Bezpieczeństwa, RZBN – Raport Zagrożeń Bezpieczeństwa Narodowego, ZRZBN – Zbiorczy Raport Zagrożeń Bezpieczeństwa Narodowego)

Rysunek 1.1c. Schemat procesu planowania cywilnego

Źródło: Krupa, Wiśniewski, 2015, s. 95.

Uzupełnieniem procesu planowania cywilnego jest proces zarządzania kryzysowego zobrazowany na rys. 1.1d, którego fazy są realizowane w przypadku wystąpienia sytuacji kryzysowej.



Rysunek 1.1d. Proces zarządzania kryzysowego

Źródło: opracowanie na podstawie Dz.U. 2017 poz. 209.

Proces zarządzania kryzysowego składa się z dwóch okresów i czterech faz:

- okres stabilizacji – do tego okresu zalicza się fazę I – zapobiegania i II – przygotowania. Okres stabilizacji odnosi się do całokształtu działań organizacyjnych podejmowanych na wszystkich szczeblach administracji publicznej, obejmujących przygotowanie i wdrożenie działań zapobiegających potencjalnym zagrożeniom, a także opracowanie i wdrożenie procedur operacyjnych;
- okres realizacji – do tego okresu zalicza się fazę III – reagowania i IV – odbudowy. Okres realizacji obejmuje całokształtu działań podejmowanych w wyniku materializacji zagrożenia, które doprowadziło do powstania sytuacji kryzysowej oraz działania zmierzające do przywrócenia stanu sprzed materializacji zagrożenia.

Faza I – zapobieganie koncentruje się na eliminowaniu lub ograniczaniu ryzyka poprzez wdrażanie zabezpieczeń przed rozpoznanymi zagrożeniami.

Faza II – przygotowanie obejmuje działania mające zapewnić zabezpieczenia przed rozpoznanymi zagrożeniami, których nie da się uniknąć. W fazie przygotowania określa się przede wszystkim procedury postępowania z rozpoznanymi zagrożeniami. Faza druga jest zbiorem przedsięwzięć, których zadaniem jest przeciwdziałanie zagrożeniom lub ograniczanie negatywnych skutków ich wystąpienia.

Faza III – reagowanie obejmuje przedsięwzięcia podejmowane w momencie zaistnienia sytuacji kryzysowej. Polega na podejmowaniu działań w celu ograniczania

zniszczeń oraz na jak najszybszym przejęciu kontroli nad sytuacją kryzysową, w drodze działań określonych w planach, co ma przywrócić funkcjonalności obiektu dotkniętego sytuacją kryzysową.

Faza IV – odbudowy jest ostatnią fazą w procesie zarządzania kryzysowego. Jej celem jest powrót do normalnego stanu. Zakłada ona prowadzenie działań normujących warunki życia w zakresie powrotu do pożądanego stanu funkcjonowania rozpatrywanego obiektu. Działania te podzielone są na doraźne i długofalowe. Wiąże się to z zapewnieniem warunków przetrwania, a następnie odbudowy w taki sposób, aby uodpornić środowisko na zdarzenia, jakie występowały w przeszłości i potencjalne, a także w znacznym stopniu ograniczyć wrażliwość społeczeństwa na skutki tych zagrożeń.

Procesy planowania cywilnego i zarządzania kryzysowego są źródłem dokumentów planistycznych mających na celu wyeliminowanie zagrożeń lub ograniczenie skutków ich wystąpienia[26]:

- Planów Zarządzania Kryzysowego (PZK),
- Planów Ochrony Infrastruktury Krytycznej (POIK).

Zarówno proces planowania cywilnego, jak i proces zarządzania kryzysowego zawierają: wykaz celów, terminy ich cyklicznej realizacji oraz wskazują podmioty odpowiedzialne za realizację wyznaczonych zadań. W przepisach prawnych definiujących oba procesy brakuje podejścia metodycznego dedykowanego do osiągnięcia założonych celów. Sprawia to, że podmioty odpowiedzialne za przygotowanie PZK oraz POIK same definiują zakres danych umieszczanych w PZK i POIK oraz metody ich pozyskania, co powoduje rozbieżności w obszarze szczegółowości poszczególnych planów. Utrudnia to wymianę i analizę danych dotyczących zagrożeń.

Obecnie najpopularniejszą metodą stosowaną przez podmioty odpowiedzialne za zarządzanie bezpieczeństwem IK w celu określenia poziomu ryzyka związanego z zagrożeniami oddziałującymi na IK jest matryca ryzyka [Skomra, 2005, s. 203]. Użycie tego narzędzia pozwala oszacować prawdopodobieństwo wystąpienia zagrożenia oraz jego skutek, co umożliwia uszeregowanie zagrożeń i wskazanie strategii postępowania z ryzykiem. Innymi popularnymi narzędziami z obszaru zarządzania kryzysowego są mapy zagrożeń oraz siatki bezpieczeństwa.

Jednostki administracji publicznej opracowujące PZK oraz operatorzy IK sporządzający POIK (rys. 1.1e) stanowią grupę podmiotów odpowiedzialnych za bezpieczeństwo IK, realizującą zadania dotyczące zarządzania bezpieczeństwa IK. Stąd jednostki te należy uznać za podmioty badawcze, które można podzielić na trzy poziomy:

- poziom operatorów IK – operatorzy IK,
- poziom administracyjny – Centra Zarządzania Kryzysowego i Zespoły Zarządzania Kryzysowego,
- poziom centralny – Rada Ministrów i RCB.

[26] Wymagania dotyczące zawartości tych dokumentów omówiono w rozdz. 1.2.

<table>
<tr><td rowspan="8">Poziom administracyjny</td><td rowspan="2">Kraj</td><td colspan="2">Rada Ministrów</td><td rowspan="8">Rządowe Centrum Bezpieczeństwa (Poziom centralny)</td></tr>
<tr><td colspan="2">Rządowy Zespół Zarządzania Kryzysowego (RZZK)</td></tr>
<tr><td rowspan="2">Województwo (16 województw)</td><td colspan="2">Wojewoda</td></tr>
<tr><td>Wojewódzki Zespół Zarządzania Kryzysowego (WZZK)</td><td>Wojewódzkie Centrum Zarządzania Kryzysowego</td></tr>
<tr><td rowspan="2">Powiat (314 powiatów) + (66 miast na prawach powiatu)</td><td colspan="2">Starosta</td></tr>
<tr><td>Powiatowy Zespół Zarządzania Kryzysowego (PZZK)</td><td>Powiatowe Centrum Zarządzania Kryzysowego</td></tr>
<tr><td rowspan="2">Gmina (2478 gmin)</td><td colspan="2">Wójt/Burmistrz/Prezydent Miasta</td></tr>
<tr><td>Gminny Zespół Zarządzania Kryzysowego (GZZK)</td><td>Gminne Centrum Zarządzania Kryzysowego</td></tr>
<tr><td>Poziom operatora IK</td><td>Systemy IK (11 systemów IK)</td><td colspan="2">Elementy IK</td></tr>
</table>

Rysunek 1.1e. Podmioty odpowiedzialne za bezpieczeństwo IK
Źródło: opracowanie własne.

Podsumowując rozdział, można wskazać potrzeby podmiotów odpowiedzialnych za bezpieczeństwo IK. Dotyczą one:

- stosowania integralnego modelu zarządzania bezpieczeństwem infrastruktury krytycznej, co jest określone:
  - koniecznością uzgadniania POIK na wielu poziomach decyzyjnych,
  - faktem, że skuteczna ochrona IK wymaga komunikacji, koordynacji i współpracy na poziomie krajowym i UE pomiędzy wszystkimi zainteresowanymi stronami,
  - istnieniem rozbieżności terminologicznych w obszarze ochrony IK, które powodują niedostateczne zdefiniowanie metod realizacji zadań ochrony IK,
  - sugestią uwzględnienia w POIK scenariuszy zdarzeń niekorzystnych,
- stosowania wspólnej metodyki zarządzania bezpieczeństwem IK, zapewniającej możliwość odwzorowania sytuacji, w jakiej znajduje się rozpatrywana IK oraz podejmowania skoordynowanych inicjatyw na rzecz podnoszenia bezpieczeństwa IK,
- uwzględnienia w procesie zarządzania bezpieczeństwem IK funkcjonalności IK.

Opracowanie IM-BIK oraz bazującej na nim metodyki ZS-BIK umożliwi podmiotom odpowiedzialnym za bezpieczeństwo IK zarządzanie sytuacyjne bezpieczeństwem IK polegające na podejmowaniu zespołu działań realizowanych w obszarze funkcji zarządzania, uzależnionych od sytuacji IK, w celu osiągnięcia wymaganego progu bezpieczeństwa[27].

[27] Próg bezpieczeństwa – poziom funkcjonalności uznany przez operatora IK za wystarczający do realizacji zadań IK wynikających z zobowiązań wobec społeczeństwa.
Zagadnienie progu bezpieczeństwa porusza również publikacja [Garschagen, Sandholz, 2018, s. 1233].

1.2. Stosowane metodyki zarządzania bezpieczeństwem IK

Zadania wykonywane w procesie zarządzania bezpieczeństwem IK są scharakteryzowane w metodykach oceny ryzyka na potrzeby zarządzania kryzysowego, których procedury realizacji przedstawiono w zał. F. Metodyki dostarczają wiedzy na temat etapów procesu zarządzania bezpieczeństwem IK oraz stanowią źródło możliwych do zastosowania metod pracy podmiotów odpowiedzialnych za bezpieczeństwo IK. Pod tym kątem przeanalizowano metodykę oceny ryzyka na potrzeby zarządzania kryzysowego stosowaną w Polsce oraz metodyki krajów, które są uznane za wiodące w tym obszarze[28] (tab. 1.2a), tj.:

- metodyka Australii,
- metodyka Szwecji,
- metodyka Niemiec,
- metodyka Irlandii,
- metodyka Kanady,
- metodyka Holandii,
- metodyka USA.

Wzorcem dla wymienionych metodyk jest norma PN-EN ISO 31000:2012 zarządzanie ryzykiem – zasady i wytyczne, która zakłada realizację procesu oceny ryzyka w trzech etapach:

1) ustalenie kontekstu,
2) ocena ryzyka (identyfikacja, analiza i ewaluacja),
3) decyzja o postępowaniu z ryzykiem.

Z tab. 1.2a wynika, że niemal wszystkie metodyki rozpoczynają się od etapu ustalenia kontekstu, w którym rozpoznawane są zasoby podatne na zagrożenia, dla których ma być wykonana ocena ryzyka. Wyjątkiem od tej reguły jest metodyka holenderska, której pierwszym etapem jest opracowanie scenariuszy zdarzeń kryzysowych oraz szwedzka, która jest rozpoczynana od określenia obszarów odpowiedzialności i przyjęcia metody analizy ryzyka. Podobne rozwiązanie stosowane jest w polskiej zaawansowanej metodyce oceny ryzyka w publicznym zarządzaniu kryzysowym, gdzie pierwszy moduł zakłada organizację pracy zespołu oceny ryzyka. Metodyka szwedzka przewiduje również dodatkowy etap, niewystępujący w normie PN-EN ISO 31000:2012, zakładający dokonanie oceny podatności zasobów na zagrożenia. Wszystkie metodyki przewidują realizację składowych procesu oceny ryzyka rekomendowanego przez normę PN-EN ISO 31000:2012, tzn. analizę i szacowanie ryzyka.

Etap kończący analizowane metodyki oceny ryzyka na potrzeby zarzadzania kryzysowego stanowi podjęcie decyzji dotyczącej postępowania z ryzykiem. Decyzja jest podejmowana, na podstawie uzyskanych wyników etapu oceny ryzyka i dotyczy doboru adekwatnych zabezpieczeń eliminujących lub ograniczających ryzyko.

[28] Wybrane na podstawie publikacji: [Wójtowicz, 2006, s. 51], [Abgarowicz, 2015, s. 117], [Skomra, 2015, s. 21], [Wróblewski, 2015, s. 152], [Kosieradzka, Zawiła-Niedźwiecki, 2016, s. 247], opisane w zał. F.

Tabela 1.2a. Wykaz etapów działań rozpatrywanych metodyk oceny ryzyka na potrzeby zarządzania kryzysowego

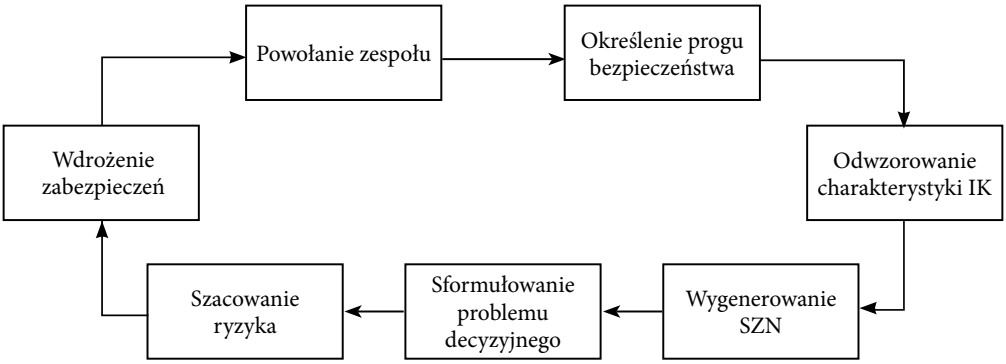
Lp.	Metodyka	Etapy metodyki oceny ryzyka na potrzeby zarządzania kryzysowego		Dobre praktyki
1	polska	• ustalenie kontekstu • identyfikacja zagrożeń • analiza ryzyka • szacowanie ryzyka • ocena ryzyka	• moduł 1 – organizacja pracy zespołu oceny ryzyka • moduł 2 – charakterystyka podmiotu chronionego • moduł 3 – wyznaczenie podsystemów i grup zasobów IK państwa • moduł 4 – obliczenie zmiennych ryzyka • moduł 5 – identyfikacja zagrożeń oraz analiza i oszacowanie ryzyka • moduł 6 – kryteria akceptowalności ryzyka • moduł 7 – uwzględnienie zależności w ocenie ryzyka oraz prognozowanie rozprzestrzeniania się zagrożeń • moduł 8 – ustalenie kryteriów przejścia zagrożenia w sytuację kryzysową • moduł 9 – sprawozdawczość i międzyszczeblowe przekazywanie oceny ryzyka	• wykaz zagrożeń inicjujących i wtórnych • uwzględnienie analizy kompetencji zespołu oceny ryzyka • identyfikacja zależności zagrożeń • prognozowanie rozprzestrzeniania się ryzyka
3	australijska	• ustanowienie kontekstu • identyfikacja ryzyka • analiza ryzyka • ewaluacja ryzyka • postępowanie z ryzykiem		• usystematyzowane podejście do identyfikacji mechanizmów kontroli i możliwość zastosowania adekwatnych rozwiązań • powiązanie przyczyn zagrożenia i jego skutków • ustandaryzowane matryce tolerancji ryzyka
4	szwedzka	• punkt startowy • rola i obszar odpowiedzialności • określenie metody i perspektywy analizy ryzyka • ocena ryzyka • identyfikacja ryzyka • analiza ryzyka • ewaluacja ryzyka • ocena podatności • ocena zdolności • analiza podatności • postępowanie z ryzykiem • rezultaty i wnioski • ciągła praca, siły i środki, plany reakcji		• określenie wpływu na społeczeństwo i badaną organizację • analizy wielokryterialne • wykorzystanie metod scenariuszowych

Lp.	Metodyka	Etapy metodyki oceny ryzyka na potrzeby zarządzania kryzysowego	Dobre praktyki
5	niemiecka	• opis zdefiniowanego obszaru • selekcja zagrożeń i opis scenariuszy • szacowanie prawdopodobieństwa • szacowanie wpływu • identyfikacja i wizualizacja ryzyka	• odniesienie analizy ryzyka do zdefiniowanego obszaru (obiektu, miejsca) • agregacja wyników analizy ryzyka oparta o arytmetykę (w tym ocena ważona)
6	irlandzka	• ustanowienie kontekstu • identyfikacja zagrożeń • oceny ryzyka • prezentacja zagrożeń na matrycy ryzyka	• wizualizacja wyników analizy ryzyka w postaci rozbudowanej matrycy ryzyka uwzględniającej obszary: zapobiegania i redukcji ryzyka, zwiększenia sił reagowania
7	kanadyjska	• ustanowienie kontekstu • identyfikacja ryzyka • analiza ryzyka • ewaluacja ryzyka • postępowanie z ryzykiem	• wskazanie zestawu metod i technik wspierających poszczególne etapy metodyki • analizy średnio- i długoterminowe (5–25 lat)
8	holenderska	• opracowanie scenariuszy • ocena ryzyka • ocena zdolności reakcji na zagrożenie • opracowanie raportu podsumowującego oraz rekomendacji	• budowa i podział opracowanych scenariuszy zagrożeń na grupę scenariuszy realnych (do materializacji tu i teraz) i rozwojowych (możliwych do zrealizowania w przyszłości) • modyfikacja wzoru na ryzyko poprzez podział parametru odpowiedzialnego za prawdopodobieństwo i skutek zagrożenia na podkategorie
9	amerykańska	• identyfikacja zasobów • szacowanie ryzyka • identyfikacja zagrożeń • opis zagrożeń • klasyfikacja zagrożeń • szacowanie strat • wskazanie możliwych działań • opracowanie planów łagodzenia ryzyka • implementacja planów łagodzenia ryzyka	• modułowa budowa metodyki • wykorzystanie systemów GIS

Źródło: opracowanie syntetycznego wykazu etapów metodyk oceny ryzyka na potrzeby zarządzania kryzysowego na podstawie materiałów zawartych w zał. F.

Analiza metodyk oceny ryzyka na potrzeby zarządzania kryzysowego pozwoliła na rozpoznanie podejmowanych działań oraz dobrych praktyk związanych z zarządzaniem bezpieczeństwem IK, co umożliwiło ustalenie koniecznych etapów metodyki ZS-BIK (rys. 1.2a). Są to:

- powołanie zespołu – etap, w ramach którego wskazywani są członkowie zespołu analitycznego dobierani na podstawie analizy charakterystyki rozpatrywanej IK ustalonej w poprzednim cyklu metodyki ZS-BIK,
- określenie progów bezpieczeństwa – etap, w ramach którego określany jest próg bezpieczeństwa dla funkcjonalności charakteryzujących rozpatrywaną IK oraz akceptowalną wartość ryzyka,
- odwzorowanie charakterystyk IK – etap, w ramach którego określana jest aktualna charakterystyka rozpatrywanej IK (zgodnie z przyjętym wzorcem),
- wygenerowanie SZN – etap, w ramach którego generowane są SZN dla rozpoznanych zagrożeń (na które podatna jest IK) w celu uzupełnienia wiedzy zespołu analitycznego o potencjalnych skutkach materializacji zagrożeń,
- sformułowanie problemu decyzyjnego – etap, w ramach którego zespół analityczny formułuje problem decyzyjny dotyczący zagrożeń (na które podatna jest IK) oraz zabezpieczeń, jakie można zastosować w celu uzyskania odporności na zagrożenia lub minimalizacji ich skutków,
- szacowanie ryzyka – etap, w ramach którego zespół analityczny weryfikuje, czy zabezpieczenia pozwolą na osiągnięcie założonego progu bezpieczeństwa IK,
- wdrożenie zabezpieczeń – etap, w ramach którego zespół analityczny podejmuje decyzję o wdrożeniu zabezpieczeń, aktualizuje charakterystykę IK i kończy cykl metodyki ZS-BIK.

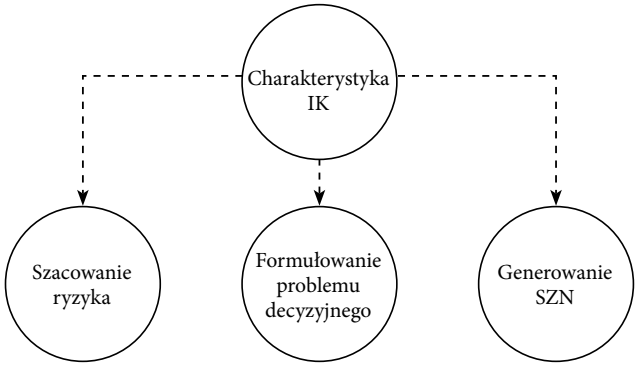


Rysunek 1.2a. Cykl metodyki ZS-BIK

Etapy metodyki ZS-BIK wskazują na potrzebę integracji działań podmiotów odpowiedzialnych za bezpieczeństwo IK od momentu rozpoznania zagrożeń do syntezy zabezpieczeń w jeden łańcuch działań. Obejmuje on:

- odwzorowanie charakterystyki IK,
- szacowanie ryzyka,
- budowę sieci zależności IK, które pozwolą na wygenerowanie SZN,
- formułowanie problemu decyzyjnego dotyczącego rozpatrywanej IK,

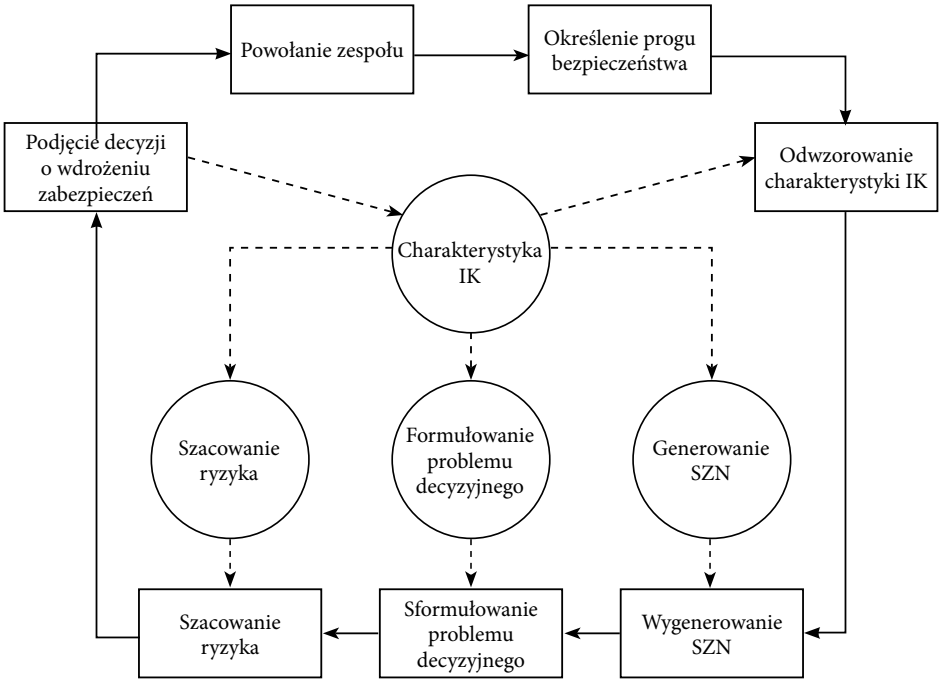
Integralność podejmowanych działań osiąga się poprzez uzależnienie obszaru generowania SZN, formułowania problemu decyzyjnego oraz szacowania ryzyka od danych charakteryzujących rozpatrywaną IK. Zostało to zilustrowane na rys. 1.2b.



Rysunek 1.2b. Elementy IM-BIK

Źródło: opracowanie własne.

Elementy widoczne na rys. 1.2b stanowią podstawę IM-BIK. Zależność etapów metodyki ZS-BIK od elementów IM-BIK ilustruje rys. 1.2c. Linie ciągłe symbolizują sekwencję etapów metodyki ZS-BIK. Linie przerywane wskazują na wykorzystanie elementów IM-BIK przez metodykę ZS-BK.



Rysunek 1.2c. Zależność etapów metodyki ZS-BIK od elementów modelu IM-BIK

Źródło: opracowanie własne.

Opracowanie metodyki ZS-BIK jest warunkiem poprawy efektywności podejmowanych przez podmioty odpowiedzialne za bezpieczeństwo IK skoordynowanych inicjatyw na rzecz podnoszenia bezpieczeństwa IK. Jednocześnie uwzględnienie w metodyce ZS-BIK etapu związanego z generowaniem SZN spełnia zalecenia komisji europejskiej oraz NPOIK dotyczące umieszczenia w POIK analizy rozprzestrzeniania się zagrożeń.

1.3. Uwarunkowania formalnoprawne zarządzania bezpieczeństwem IK

Zarządzanie bezpieczeństwem IK, zgodnie z przyjętą definicją, wymaga zebrania danych charakteryzujących rozpatrywaną IK i na ich podstawie zaproponowanie działań zmierzających do zapewnienia bezpieczeństwa IK w postaci POIK lub PZK.

Analiza zbioru danych obligatoryjnych[29] i opcjonalnych[30] dla POIK i PZK pozwoliła na rozpoznanie wspólnych kategorii danych występujących w opisie IK. W celu ustalenia tych danych przeanalizowano zapisy aktów normatywnych i planistycznych obowiązujących w UE i Polsce (zał. E), z czego najistotniejsze są:

- dyrektywa rady 2008/114/WE z 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania EIK oraz oceny potrzeb w zakresie poprawy jej ochrony, która wskazuje na konieczność uwzględnienia w procesie zarządzania bezpieczeństwem IK [Dz.U.UE 2008 nr 345 poz. 75]:
  - wykazu składników IK,
  - istniejących rozwiązań służących ochronie IK,
  - analiz ryzyka,
  - scenariuszy rozwoju sytuacji kryzysowych[31],
  - analizy podatności IK na zagrożenia,
  - hierarchii ważności środków przeciwdziałania i procedur postępowania;
- ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, która wskazuje na konieczność uwzględnienia w procesie zarządzania bezpieczeństwem IK [Dz.U. 2017 poz. 209]:
  - zestawienia potencjalnych zagrożeń wraz z ich charakterystyką,
  - wykazu wariantów zasięgu zagrożeń,
  - wykazu podmiotów odpowiedzialnych za usuwanie zagrożeń,
  - obszaru geograficznego objętego zasięgiem zagrożenia,
  - wykazu skutków wystąpienia zagrożenia,
  - wykazu struktur uruchamianych w sytuacjach kryzysowych,
  - wykazu sił i środków niezbędnych do wykonania zadań ujętych w PZK,
  - oceny ryzyka wystąpienia zagrożeń,
  - wykazu zadań i obowiązków uczestników zarządzania kryzysowego,
  - wykazu zadań dotyczących monitorowania zagrożeń,

[29] Dane obligatoryjne – wymagane obowiązującymi przepisami prawnymi, które należy zgromadzić lub do których należy się odnieść, proponując działania ochronne dla IK w postaci PZK lub POIK.

[30] Dane opcjonalne – wynikające z dokumentów planistycznych, tj. strategii, programów itp., które wskazują kierunki rozszerzenia zbioru danych obligatoryjnych.

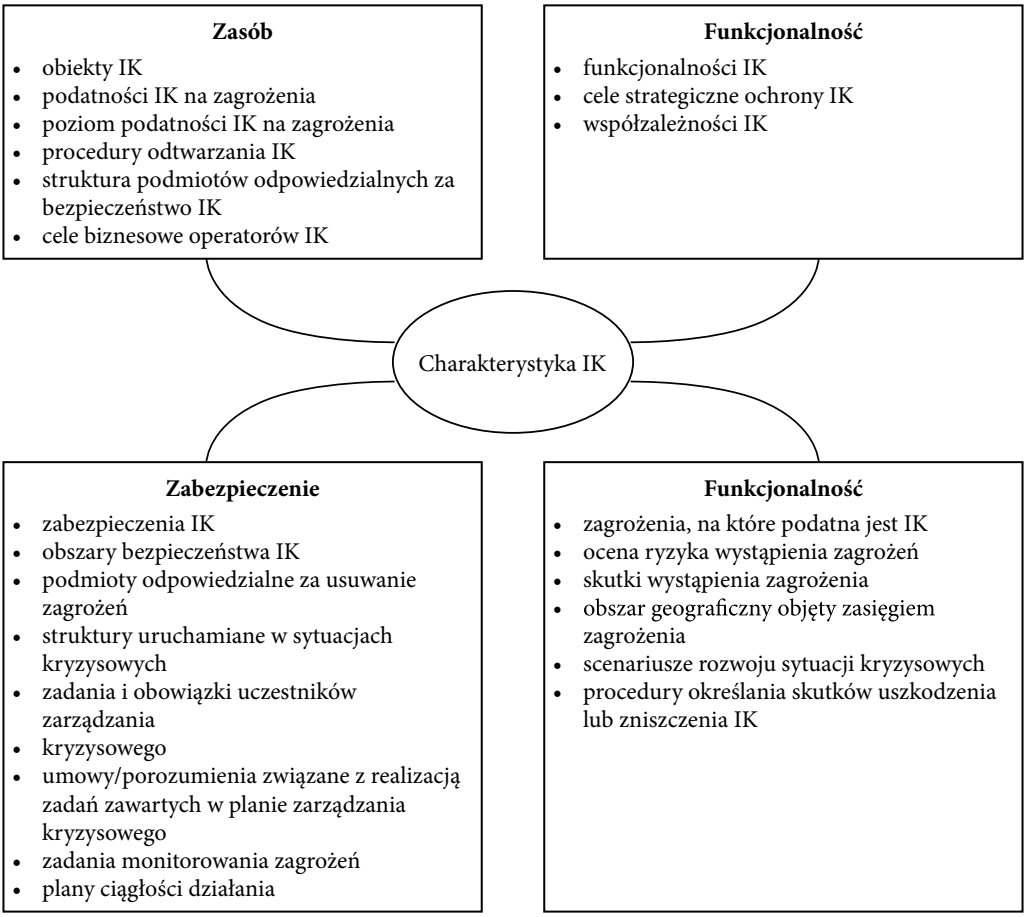
[31] Sytuacja kryzysowa – należy przez to rozumieć sytuację wpływającą negatywnie na poziom bezpieczeństwa ludzi, mienia w znacznych rozmiarach lub środowiska, wywołującą znaczne ograniczenia w działaniu właściwych organów administracji publicznej ze względu na nieadekwatność posiadanych sił i środków [Dz.U. 2013 poz. 1166, art. 3, pkt 1].

- wykazu zawartych umów związanych z realizacją zadań zawartych w PZK,
- wykazu obiektów, instalacji oraz usług istotnych dla bezpieczeństwa państwa.

Rozpoznane kategorie danych (rys. 1.3a) wskazują, na kanon charakteryzujący IK:

- zasób – fragment rzeczywistości materialnej (fizycznej) lub wirtualnej (np. pojęciowej, informacyjnej, metajęzykowej) o niepustym zbiorze funkcjonalności,
- funkcjonalność – zdolność zasobu do zaspokojenia potrzeb użytkownika w określonych warunkach,
- zagrożenie – spodziewane oddziaływanie na zasoby lub między zasobami, w wyniku realizacji którego mogą ulec degradacji ich cechy funkcjonalno-strukturalne,
- zabezpieczenie – działania, systemy lub zasoby stosowane w reakcji na rozpoznane zagrożenie w celu wyeliminowania lub ograniczenia ryzyka z nim związanego.

Analiza zapisów NPOIK pozwoliła na wskazanie obszarów bezpieczeństwa (fizycznego, technicznego, osobowego, teleinformatycznego, prawnego oraz ciągłość działania) w jakich należy podejmować działania chroniące IK [NPOIK, 2015, zał. 1, s. 5].



Rysunek 1.3a. Klasyfikacja danych stosowanych w POIK i PZK do charakterystyki IK

Źródło: Wiśniewksi, Ostrowska, 2016, s. 118–119.

Rzeczywistym przykładem charakterystyki IK odnoszącym się do klasyfikacji danych przedstawionej na rys. 1.3a jest sytuacja rafinerii PKN ORLEN S.A., na terenie której znajdują się dwie spółki wpływające na jej bezpieczeństwo:

- Basell Orlen Polyolefins sp. z o.o.,
- Zakład Produkcyjny ORLEN OIL sp. z o.o. w Płocku.

Do głównych działalności rafinerii PKN ORLEN S.A. (jej podstawowe funkcjonalności) należy [Plan Zarządzania Kryzysowego powiat płocki, 2015, s. 20]:

- przerób ropy naftowej oraz wytwarzanie produktów i półproduktów ropopochodnych (rafineryjnych i petrochemicznych),
- magazynowanie, składowanie i przechowywanie ropy naftowej i paliw płynnych oraz tworzenie i utrzymywanie zapasów paliw,
- wytwarzanie, przesyłanie i obrót energią cieplną i elektryczną.

Z uwagi na prowadzone procesy technologiczne na terenie rafinerii PKN ORLEN S.A. oraz zagrożenia spowodowane siłami natury istnieje możliwość powstania [Plan Zarządzania Kryzysowego powiat płocki, 2015, s. 21]:

- pożaru,
- wybuchu,
- skażenia środowiska.

Operator rafinerii PKN ORLEN S.A. w odpowiedzi na rozpoznane zagrożenia stosuje zabezpieczenia [Plan Zarządzania Kryzysowego powiat płocki, 2015, s. 21] takie jak:

- zakładowa straż pożarna,
- służba ochrony zakładu (ORLEN ochrona Sp. z o.o.),
- zakładowa służba medyczna (ORLEN Medica Sp. z o.o.),
- monitorowanie stanu środowiska.

Przyjętym celem biznesowym rafinerii PKN ORLEN S.A. jest utrzymanie wykorzystania mocy produkcyjnych dla głównych funkcjonalności na poziomie 90%[32]. Pełną charakterystykę sytuacji rafinerii PKN ORLEN S.A. oraz działania z niej wynikające przedstawiono w rozdz. 3.4 i rozdz. 3.6.

1.4. Ujęcia teoretyczne i praktyczne

Analiza metodyk oceny ryzyka na potrzeby zarządzania kryzysowego (rozdz. 1.2) pozwoliła na określenie jakie bazowe etapy powinna zawierać metodyka ZS-BIK. Etapy te wyznaczyły elementy IM-BIK, które będą wykorzystywane w poszczególnych etapach metodyki ZS-BIK.

Metodyki oceny ryzyka na potrzeby zarządzania kryzysowego, oprócz etapów działań podejmowanych na rzecz bezpieczeństwa IK, zawierają wykazy metod, które są wykorzystywane do ich realizacji. Metody te podzielono wg kryterium elementów IM-BIK (tab. 1.4a), a następnie oceniono pod kątem ich użyteczności dla IM-BIK (tab. 1.4b––1.4g). Do oceny użyto kryteriów uwzględniających potrzebę gromadzenia i przetwarzania danych[33] dotyczących procesu zarządzania bezpieczeństwem IK oraz zapewniających integralność elementów IM-BIK.

[32] Wynik ustalony na podstawie raportu Grupy Orlen z 2016 r. [Orlen, 2016, s. 295].

[33] Znak + oznacza, że rozpatrywana metoda ma wymaganą cechę.

Tabela 1.4a. Metody wykorzystywane w ocenie ryzyka na potrzeby zarządzania kryzysowego

Elementy IM-BIK	Metody możliwe do wykorzystania
określenie charakterystyk IK	matryce ryzyka, bow-tie, analiza drzewa zdarzeń (ETA), drzewa zdarzeń i nadzoru nad ryzykiem (HAZOP), wielowymiarowa analiza aktywności (MVA), analiza zagrożeń i wrażliwości (ROSA), mapy GIS, analiza sytuacji obiektu, wiedza ekspercka, wywiady ustrukturalizowane, lista kontrolna, klasyfikacja zagrożeń, analiza SWOT, metoda PHA
wygenerowanie SZN	bow-tie, analiza drzewa zdarzeń (ETA), drzewa zdarzeń i nadzoru nad ryzykiem (HAZOP), analiza zależności (RIB), wielowymiarowa analiza aktywności (MVA), analiza zagrożeń i wrażliwości (ROSA), metoda IBERO, analiza Bayesa, mapy GIS, wiedza ekspercka, burza mózgów, modele przyczynowo -skutkowe, analiza zagrożeń i krytycznych punktów kontroli, wykres Ishikawy, metody scenariuszowe
sformułowanie problemu decyzyjnego	wiedza ekspercka, metoda delficka, algorytmy genetyczne
szacowanie ryzyka	bow-tie, analiza drzewa zdarzeń (ETA), drzewa zdarzeń i nadzoru nad ryzykiem (HAZOP), wiedza ekspercka, metoda FMEA

Źródło: opracowanie na podstawie opisów metodyk oceny ryzyka na potrzeby zarządzania kryzysowego zawartych w zał. F.

Dane zebrane w tab. 1.4a wskazują szeroki zbiór metod możliwych do wykorzystania w celu odwzorowania charakterystyki IK oraz ustalenia SZN. W przypadku pozostałych obszarów IM-BIK, tj. możliwości formułowania problemu decyzyjnego oraz szacowania ryzyka, przeanalizowane metodyki zarządzania ryzykiem na potrzeby zarządzania kryzysowego wskazują głównie na metody eksperckie. Z tego powodu zbiór metod dla tych obszarów został uzupełniony o narzędzia wyznaczone na podstawie przeglądu metod wykorzystywanych w naukach o zarządzaniu i rekomendowanych przez normę PN-ISO 31010:2010 zarządzanie ryzykiem – metody szacowania ryzyka, tj.: sieci neuronowe, zbiory rozmyte, algorytmy genetyczne, tablice decyzyjne oraz metody: AIDA, drzewa zdarzeń, metoda delficka [Bogdanienko, 2002, ss. 33–157; Kulinska, Dorntfeld, 2009, ss. 41–42; Ouyang, 2014; Skomra, 2015, ss. 48–82; Kulińska, Rut, 2016, ss. 32–48; Hurley, 2017; Kosieradzka, Zawiła-Niedźwiecki, 2016, ss. 107–133; Cai, Xie, Liu, et al. 2017; Tien, Kiureghain, 2017; Johansen, Tien, 2018].

Celem analizy istniejących metod i technik z obszaru nauk o zarządzaniu jest wskazanie tych rozwiązań, które pozwolą na opracowanie elementów IM-BIK stanowiących propozycję rozwiązań w obszarze:

- modelowego odwzorowania charakterystyki IK – w tym obszarze można zastosować m.in.: macierze ryzyka, analizę SWOT, podejście sytuacyjne, metodę BIA,
- uzupełnienia charakterystyki IK o możliwe SZN z jej udziałem – w tym obszarze można zastosować m.in.: metodę bow-tie, scenariusze symulacyjne, analizę Bayesa, modele przyczynowo-skutkowe,
- wskazania zabezpieczeń dla zagrożeń, na które podatna jest IK – w tym obszarze można zastosować m.in.: zbiory rozmyte, algorytmy genetyczne, sieci neuronowe, metodę AIDA,

- określenia ryzyka przed i po wprowadzeniu nowych zabezpieczeń dla IK – w tym obszarze można zastosować m.in.: metodę PHA, metodę ETA, metodę matematyczną, podstawowy wzór na ryzyko.

Macierz ryzyka

Metoda macierzy ryzyka jest popularną metodą stosowaną przy opracowywaniu PZK na wszystkich poziomach administracyjnych. Pozwala ona na jednoczesne zobrazowanie zbioru ryzyk zdefiniowanego dla rozpatrywanego przedsięwzięcia lub obiektu. Konstrukcja macierzy ryzyka polega na przypisaniu każdemu zidentyfikowanemu zagrożeniu prawdopodobieństwa jego wystąpienia oraz skutku, jaki ze sobą niesie. Dzięki temu można określić stopień ryzyka, który w zestawieniu z posiadanymi mechanizmami zapobiegania zagrożeniom pozwoli na określenie istotności danej kategorii zagrożenia. Macierze ryzyka pokazują zależność dwóch zmiennych: prawdopodobieństwa wystąpienia zagrożenia i wpływu tego zagrożenia na rozpatrywany obiekt np. IK.

Macierze ryzyka są prostą metodą pozwalającą w syntetyczny sposób przedstawić dane dotyczące rozpatrywanego obiektu. Wadą tej metody jest możliwość charakteryzacji obiektu trzema parametrami, tj. prawdopodobieństwem wystąpienia zagrożenia, skutkiem wystąpienia zagrożenia oraz ryzykiem związanym z zagrożeniem.

Analiza SWOT

SWOT jest metodą analizy strategicznej organizacji, która pozwala na zbadanie wnętrza organizacji oraz jej otoczenia. Polega na identyfikacji kluczowych atutów oraz słabości przedsiębiorstwa i zestawieniu ich z szansami i zagrożeniami pochodzącymi z otoczenia. Metoda SWOT może być również zastosowana jako narzędzie formułowania strategii firmy [Gierszewska, Romanowska, 2014, s. 178].

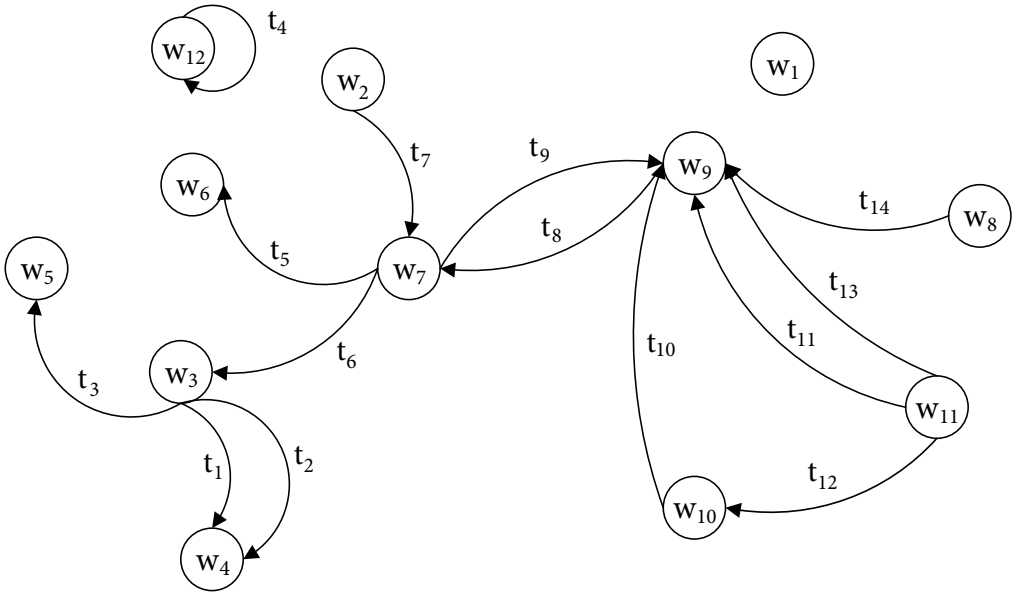
Metoda SWOT, w ramach IM-BIK może zostać wykorzystana jako narzędzie integrujące dane o zagrożeniach IK, jej podatnościach oraz stosowanych zabezpieczeniach. W metodzie SWOT brakuje narzędzi pozwalających na uwzględnienie wzajemnej zależności zagrożeń oraz IK. Jej opisowy charakter utrudnia zbudowanie modelu sytuacji IK oraz określenie hierarchiczności składowych rozpatrywanej IK.

Podejście sytuacyjne

Podstawowym założeniem ujęcia sytuacyjnego jest stwierdzenie, że rzeczywistość biznesowa jest zbyt złożona, aby stosować do niej uniwersalne zasady i aby stosowanie jednego sposobu postępowania mogło stanowić wskazówkę dla praktyków zarządzania [Bogdanienko, 2002, s. 33]. Pogląd ten potwierdza A. Hamrol, dodając, że organizacje są systemami złożonymi, probabilistycznymi, spójnymi, o nieograniczonych zbiorach sprzężeń wewnętrznych i zewnętrznych. Nie ma zatem sytuacji identycznych i powtarzalnych, w których można wprost zastosować znane rozwiązania. Dopiero analiza konkretnej sytuacji daje możliwość doboru adekwatnych modeli, metod czy rozwiązań oraz pozwala na określenie ich skuteczności w określonych warunkach [Hamrol, 1998, s. 68]. Zamiast uniwersalnych metod postępowania w nurcie sytuacyjnym przyjmuje się, że [Maracz, 1983, s. 276; Kaczmarek, 1999, ss. 24–25]:

- twierdzenia i zalecenia szkoły sytuacyjnej mają służyć jako sugestie sprawdzonych rozwiązań w różnych sytuacjach,
- każda organizacja jest jedyna w swoim rodzaju i wymaga, aby zachowania kierownicze warunkowane były zmiennymi właściwymi dla danej sytuacji,
- celowym jest opracowanie zbiorów modelowych rozwiązań dotyczących różnych poziomów i aspektów zarządzania w organizacji,
- rozwiązania modelowe stanowią zbiór możliwości, z których należy wybrać najlepsze w danej sytuacji.

Szczególnie użyteczne podejście do zażądania sytuacyjnego, w kontekście zarządzania bezpieczeństwem IK, przedstawia J. Kłykow. Definiuje on sytuację jako zbiór W węzłów $w_1, w_2, \ldots, w_n$ związanych ze sobą skierowanymi połączeniami [Kłykow, Jurek, 1988, ss. 71–72]. Węzły oznaczają elementy odwzorowywanej rzeczywistości. Przykład systuacji systemu obrazuje rys. 1.4a.



Rysunek 1.4a. Struktura sytuacji
Źródło: Kłykow, Jurek, 1988, s. 71.

Każdy węzeł może być skojarzony z dowolną sytuacją, która w takim przypadku stanowi jego rozszerzoną zawartość. Dzięki temu założeniu można budować struktury hierarchiczne. Sytuację skojarzoną z węzłem v nazywa się kontekstem v. Istotne jest, że różne konteksty mogą zawierać te same węzły związane w różny sposób w tych kontekstach.

Zastosowanie podejścia sytuacyjnego w IM-BIK pozwoli na uwzględnienie wszystkich elementów charakterystyki IK, tj. elementów IK, zagrożeń, na które podatna jest IK, stosowanych zabezpieczeń, powiązań IK. Ponadto podejście sytuacyjne zapewnia mechanizmy pozwalające na odwzorowanie wzajemnego zawierania się elementów IK.

Metoda Business Impact Analysis (BIA)

BIA jest rozbudowaną metodą stosowaną do opisu kluczowych procesów realizowanych w przedsiębiorstwie. Celem metody jest oszacowanie skutków niedostępności usług lub produktów, które są rezultatem procesów kluczowych dla przedsiębiorstwa. Wynikiem metody jest lista kluczowych procesów, dla których [Kosieradzka, Zawiła-Niedźwiecki, 2016, s. 66]:

- określony zostaje czas ich odtworzenia,
- identyfikowane są powiązania z między procesami,
- wskazywane są zasoby niezbędne do realizacji procesów na określonym poziomie.

W ramach analizy przedsiębiorstwa metodą BIA określane są również kluczowe wskaźniki dotyczące:

- docelowego czasu odtworzenia procesu i zasobów Recovery Time Objective (RTO),
- minimalnego poziom odtworzenia dostępności usługi lub produktu,
- poziomu akceptowalnej utraty danych Recovery Point Objective (RPO).

Metoda BIA może zostać wykorzystana do opisu rozpatrywanej IK jej funkcjonalnościmi, zagrożeniami, stosowanymi zabezpieczeniami oraz innymi parametrami. Jednak opisowy charakter metody utrudnia jej zastosowanie w sytuacji konieczności gromadzenia syntetycznych danych na temat rozpatrywanej IK, które na podstawie jednolitych reguł pozwolą na zbudowanie jej modelu przez różne podmioty odpowiedzialne za bezpieczeństwo IK.

W tab. 1.4b przedstawiono syntetyczną ocenę użyteczności omówionych metod z obszaru odwzorowania charakterystyki obiektu dla projektowanego IM-BIK.

Tabela 1.4b. Ocena metod możliwych do zastosowania w obszarze odwzorowania charakterystyki IK

Wyszczególnienie / **Kryterium oceny**	**Macierz ryzyka**	**Analiza SWOT**	**Podejście sytuacyjne**	**Metoda BIA**
możliwość oznaczenia zasobów IK	+	+	+	+
możliwość oznaczenia funkcjonalności IK			+	+
możliwość oznaczenia zagrożeń, na które podatna jest IK	+	+	+	+
możliwość oznaczenia stosowanych zabezpieczeń		+	+	+
możliwość oznaczenia zależności między IK			+	+
możliwość elastycznej modyfikacji zbioru parametrów określających charakterystykę IK			+	+
możliwość zbudowania modelu IK na podstawie zebranych danych			+	
możliwość odwzorowania hierarchiczności IK			+	
Podsumowanie	2	3	8	6

Źródło: opracowanie własne.

Metoda bow-tie

Metoda bow-tie jest graficzną metodą pozwalającą na połączenie przyczyn zdarzenia z jego skutkami. Metoda jest kombinacją metody analizy drzewa zdarzeń i analizy drzewa błędów. W ramach metody bow-tie oprócz identyfikacji skutków oraz ich przyczyn możliwe jest oznaczenie barier pomiędzy ryzykiem a jego przyczynami oraz ryzykiem i jego konsekwencjami. Bariery w przypadku generowania SZN mogą symbolizować odporność IK na zagrożenia, której wartość jest określona przez stosowane zabezpieczenia. Źródłem danych dla metody bow-tie są m.in. [Kosieradzka, Zawiła-Niedźwiecki, 2016, s. 77]:

- metoda FTA,
- metoda burzy mózgów,
- metoda BIA.

Metoda bow-tie pozwala na identyfikację SZN na podstawie wielu czynników powodujących różne skutki. Dzięki tej właściwości możliwe jest przewidywanie wpływu wielu zagrożeń na rozpatrywaną IK, jednak nie można za jej pomocą odwzorować wzajemnego zawierania się elementów IK. Metoda bow-tie jest przeznaczona do odwzorowania zależności elementów wpływających na wartość ryzyka, bez przypisywania im parametrów opisujących. Sprawia to, że wymaga ona modyfikacji w celu uwzględniania wartości parametrów oznaczających prawdopodobieństwo wystąpienia zagrożenia i podatność IK na zagrożenie.

Scenariusze symulacyjne

Scenariusze symulacyjne wywodzą się z obszaru prognozowania scenariuszowego, które jest elementem podejścia prognostycznego. Przedmiotem tego podejścia są prognozy przyszłych zdarzeń, procesów i tendencji niezależnych od decydenta, jednak wpływających na jego decyzje. Ze względu na często występującą lukę informacyjną użyteczność prognoz dla rzeczywistego procesu zarządzania przedsiębiorstwem jest ograniczona. Skuteczniejszym narzędziem są tzw. prognozy scenariuszowe, których zadaniem jest wskazanie możliwości i ukierunkowanie myślenia menadżerów [Bogdanienko, 2002, ss. 139–151]. Jedną z metod stosowanych w prognozowaniu scenariuszowym są scenariusze symulacyjne, które służą dokonywaniu wyprzedzającej oceny wartości poszczególnych wyborów strategicznych zależnie od oddziaływania otoczenia. Proces budowy scenariuszy symulacyjnych składa się z siedmiu etapów [Gierszewska, Romanowska, 2014, ss. 57–58]:

- etap I – definiuje się problemy i opracowuje listę istotnych czynników w otoczeniu, mających wpływ na funkcjonowanie organizacji. Poszczególnym czynnikom przypisuje się jednostki miary, zakres czasowy i obszar występowania;
- etap II – określenie deskryptorów służących opisowi problemu głównego;
- etap III – ustalenie prawdopodobieństwa wystąpienia deskryptorów;
- etap IV – opracowanie macierzy zależności deskryptorów;
- etap V – opracowanie scenariuszy wraz z ich częścią opisową na podstawie modelu z poprzedniego etapu;
- etap VI – przeprowadza się analizę podatności, która polega na wprowadzeniu do zbioru danych o procesach zachodzących w otoczeniu informacji o wydarzeniach mało prawdopodobnych niosących ze sobą poważne skutki dla organizacji;

- etap VII – formułuje się strategię działania organizacji. Określa się skutki danych wyborów, ocenia zdolność organizacji do podjęcia wyzwań pochodzących z otoczenia, które wynikają z poszczególnych scenariuszy.

Opracowane scenariusze powinny spełniać następujące założenia [Bogdanienko, 2008, s.113]:

- scenariusze mają być prawdopodobne,
- scenariusze muszą być strukturalnie zróżnicowane,
- scenariusze powinny być wewnętrznie zgodne.

Metoda modeli symulacyjnych pozwala na opracowanie modelu systemu złożonego z kilku IK. W ramach metody możliwe jest określenie parametrów, tj. prawdopodobieństwa wystąpienia zagrożenia oraz podatności IK na zagrożenie. Wadą metody jest konieczność opracowania macierzy zależności parametrów opisujących model.

Analiza Bayesa

Metoda analizy Bayesa zakłada, że możliwe jest zapisanie dowodnej informacji w postaci ciągu zdarzeń, który pozwoli na ustalenie prawdopodobieństwa wystąpienia rozpatrywanego zdarzenia. Twierdzenie Bayesa można wyrazić wzorem [Bolstad, 2004]:

$$P(A|B) = \{P(A) * P(B|A)\} / \sum P(B|E_i) * P(E_i) \quad (1.4a)$$

gdzie:
P(A) – prawdopodobieństwo zajścia zjawiska A,
P(A|B) – prawdopodobieństwo zajścia zdarzenia A pod warunkiem zdarzenia B,
E_i – rozpatrywane zdarzenie.

Narzędziem realizacji metody analizy Bayesa jest graficzny model składający się z węzłów, które reprezentują zmienną losową, np. prawdopodobieństwo wystąpienia zagrożenia lub podatność IK na zagrożenie, tzw. sieć Bayesowska[34]. W modelu występują przepływy łączące węzły, co może być interpretowane jako odwzorowanie wzajemnej zależności zagrożeń lub IK.

Model zależności opracowany na podstawie twierdzenia Bayesa może być wykorzystywany do badania związków przyczynowo-skutkowych, ułatwiając zrozumienie mechanizmu powstania określonych skutków, które obserwuje podmiot odpowiedzialny za bezpieczeństwo IK. Na podstawie modelu zależności można również szacować wpływ wprowadzenia zmian na funkcjonalności IK np. zwiększenia odporności IK na zagrożenie poprzez wprowadzenie dodatkowych zabezpieczeń.

Modele przyczynowo-skutkowe

Modele przyczynowo-skutkowe są metodą, w ramach której budowany jest model zjawiska w postaci zbioru równań. W równaniach występują zmienne objaśniające,

[34] Sieć Bayesowska to acykliczny graf skierowany. Każdy wierzchołek reprezentuje zmienną losową, a krawędzie reprezentują relacje przyczynowo-skutkowe pomiędzy tymi zmiennymi losowymi. Dla każdego wierzchołka X jest zdefiniowana tablica prawdopodobieństw warunkowych, gdzie P_1, P_2, … są bezpośrednimi rodzicami X. Dla wierzchołków bez rodziców (tzw. przyczyn pierwotnych) prawdopodobieństwa warunkowe sprowadzają się do prostych prawdopodobieństw.

odzwierciedlające przyczyny zmian zmiennej prognozowanej. Etapy budowy struktury, przedstawiają się następująco [Bogdanienko, 2002, s. 144]:

- sprecyzowanie zakresu badań i budowa modelu odpowiadającego potrzebom, tzn. układu równań zawierającego odpowiedni zestaw zmiennych wyrażających wpływ różnych czynników na badane zjawisko,
- zebranie danych statystycznych i szacowanie parametrów struktury modelu, czyli określenie siły dotychczasowego wpływu zmiennych objaśniających na zmienną objaśnianą oraz wpływu zmiennych losowych, czyli zjawisk przypadkowych,
- weryfikacja i ewentualna modyfikacja modelu poprzez wzbogacenie lub zredukowanie zestawu zmiennych objaśniających,
- oszacowanie poziomu zmiennych objaśniających, który prawdopodobnie wystąpi w przyszłości, aby określić ich wpływ na badane zjawisko w okresie przyszłym,
- wyznaczenie prognozy.

W przypadku IM-BIK zmienną objaśnianą może być prawdopodobieństwo negatywnego wpływu zagrożenia na rozpatrywaną IK, a zmiennymi objaśniającymi prawdopodobieństwo wystąpienia zagrożenia oraz podatność IK na to zagrożenie. Wadą metody jest konieczność zobrazowania zależności zmiennej objaśnianej i zmiennych objaśnianych w postaci wzorów matematycznych. W przypadku zarządzania bezpieczeństwem IK istnieje potrzeba uwzględniania wpływu wielu zagrożeń, które mogą negatywnie oddziaływać na IK. Stąd układ równań charakteryzujący rozpatrywany system będzie bardzo rozbudowany.

W tab. 1.4c przedstawiono syntetyczną ocenę użyteczności omówionych metod z obszaru generowania SZN dla projektowanego IM-BIK.

Tabela 1.4c. Ocena metod możliwych do zastosowania w obszarze generowania SZN

Wyszczególnienie / **Kryterium oceny**	**Metoda bow-tie**	**Metoda scenariuszy symulacyjnych**	**Metoda Bayesa**	**Modele przyczynowo-skutkowe**
możliwość oznaczenia wzajemnego zawierania się składników IK		+	+	
możliwość oznaczenia zasobów IK	+	+	+	
możliwość uwzględnienia prawdopodobieństwa wystąpienia zagrożenia		+	+	+
możliwość uwzględnienia podatności IK na zagrożenie		+	+	+
możliwość generowania wielu SZN	+	+	+	+
możliwość generowania ciągu zdarzeń występujących w SZN	+	+	+	+
możliwość intuicyjności budowy modelu zależności IK	+		+	
możliwość obliczenia prawdopodobieństwa wystąpienia zagrożenia od warunkiem wystąpienia innego zagrożenia			+	+
Podsumowanie	4	6	8	5

Źródło: opracowanie własne.

Zbiory rozmyte

Zbiory rozmyte są jedną z metod wspomagających proces podejmowania decyzji. Służą one do obrazowania informacji nieprecyzyjnych i pozwalają na opisywanie zjawisk o charakterze wieloznacznym. Z tego powodu zbiory rozmyte mogą być wykorzystane do opisu wpływu zabezpieczeń na podatność rozpatrywanej IK na zagrożenia[35].

Zbiorem rozmytym A w pewnej przestrzeni X nazywany jest zbiór par [Zadeh, 1965, ss. 339–340]:

$$A = \{(x, \mu_A(x)), x \in X\} \tag{1.4b}$$

gdzie
$\mu_A: X \rightarrow < 0,1 >$

jest funkcją przynależności zbioru rozmytego A. Funkcja przypisuje elementom zbioru $x \in X$ stopień przynależności do zbioru A:

$\mu_A(x) = 1$ oznacza pełną przynależność do zbioru A,
$\mu_A(x) = 0$ oznacza brak przynależności do zbioru A,
$0 < \mu_A(x) < 1$ oznacza częściową przynależność do zbioru A.

W kontekście zastosowania zbiorów rozmytych do definiowania i rozwiązywania problemów decyzyjnych w IM-BIK należy założyć, że pojedynczy zbiór A przestrzeni X stanowi odwzorowanie zagrożenia, na które podatna jest IK. Elementy zbioru A powinny być interpretowane jako możliwe zabezpieczenia, dla których przypisywana jest wartość wpływu zabezpieczenia na odporność IK na zagrożenia. To samo zabezpieczenie może być wskazywane dla różnych zagrożeń, z różnym wskaźnikiem przynależności[36]. W tym kontekście funkcja celu powinna dotyczyć znalezienia takiej kombinacji zabezpieczeń dla rozpoznanych zagrożeń, która pozwoli na maksymalizację wskaźnika odporności IK.

Wadą zastosowania zbiorów rozmytych w IM-BIK jest problem z odwzorowaniem hierarchiczności obszarów decyzyjnych oraz brak możliwości nadawania wag podzbiorom A przestrzeni X. Zbiory rozmyte uniemożliwiają również oznaczenie par zabezpieczeń, które nie mogą razem występować w jednym rozwiązaniu problemu decyzyjnego.

Algorytmy genetyczne

Algorytmy genetyczne są techniką przeszukiwania i optymalizacji wykorzystującą zasady przejęte z teorii ewolucji. Ich intuicyjność oraz prostota działania sprawiły, że są często wykorzystywane w naukach o zarządzaniu, w szczególności do rozwiązywania problemów optymalizacji kombinatorycznej. Podstawowym elementem algorytmu genetycznego jest chromosom, czyli zestaw cech charakteryzujący rozpatrywany

[35] Efektywność zabezpieczenia może być różna w zależności od innych zabezpieczeń stosowanych w ramach rozpatrywanej IK.

[36] Rozpatrywane zabezpieczenie może różnie wpływać na poziom odporności IK, w zależności od zagrożenia, przeciwko któremu jest stosowane.

obiekt[37]. Schemat działania algorytmu genetycznego można zobrazować za pomocą sześciu kroków [Rutkowska, Pilińska, Rutkowski, 1999]:

- inicjacja – utworzenie populacji początkowej poprzez losowy wybór ustalonej liczby chromosomów,
- ocena przystosowania – obliczenie wartości funkcji przystosowania dla każdego chromosomu[38],
- selekcja chromosomów – wybór chromosomów, które biorą udział w tworzeniu nowej populacji na podstawie uzyskanych ocen przystosowania,
- zastosowanie operatorów genetycznych – na grupie chromosomów wybranej drogą selekcji działają operatory genetyczne (krzyżowania[39] i mutacji[40]).
- utworzenie nowej populacji – chromosomy otrzymane jako rezultat działania operatorów genetycznych wchodzą w skład nowej populacji,
- wyprowadzenie chromosomu – najlepszym rozwiązaniem jest chromosom o największej wartości funkcji przystosowania.

Nową populację tworzą chromosomy powstałe w wyniku selekcji i działania operatorów genetycznych. Nowa populacja zastępuje w całości starą i staje się bieżącą w kolejnej iteracji algorytmu genetycznego. Iteracje są powtarzane do momentu uzyskania pożądanego wyniku.

Wadą algorytmów genetycznych w kontekście rozwiazywania problemów decyzyjnych w ramach IM-BIK jest brak możliwości wygenerowania pełnej listy potencjalnych rozwiązań problemu decyzyjnego oraz utrudniona możliwość oznaczania par zabezpieczeń, które nie mogą razem występować w jednym rozwiązaniu. Ponadto w przypadku algorytmów genetycznych nie występują mechanizmy umożliwiające odwzorowanie hierarchiczności obszarów decyzyjnych.

Sieci neuronowe

Sieci neuronowe to zbiór jednostek obliczeniowych przetwarzających dane, komunikujących się ze sobą i pracujących równolegle. Cechą wspólną sieci neuronowych jest to, że są zbudowane z tzw. neuronów połączonych synapsami. Z synapsami związane są wartości liczbowe, których interpretacja zależy od rozpatrywanego problemu decyzyjnego i które mogą ulegać zmianom w trakcie procesu uczenia. Dowolna sieć neuronowa może zostać zbudowana poprzez określenie [Siderska, 2013, s. 90]:

- modelu neuronu,
- topologii sieci,
- reguły uczenia sieci.

[37] W przypadku IM-BIK chromosom może odpowiadać zagrożeniu oraz zabezpieczeniom, które pozwolą ograniczyć jego skutki.

[38] Funkcja przystosowania w przypadku IM-BIK może dotyczyć poziomu odporności, jaki należy uzyskać dla rozpatrywanej IK podatnej na rozpoznane zagrożenia.

[39] W wyniku krzyżowania na podstawie dwóch rozwiązań (rodzice) tworzone są dwa nowe osobniki (dzieci). W przypadku IM-BIK krzyżowanie może oznaczać sprawdzanie różnych kombinacji zabezpieczeń pod kątem ich wpływu na całkowitą odporność IK na rozpatrywany zbiór zabezpieczeń.

[40] W przypadku mutacji modyfikowany jest jeden osobnik, a następnie sprawdzane jest, w jaki sposób wpłynie to na wynik funkcji przystosowania.

Elementami składowymi neuronu są [Stefanowski, 2006]:

- n wejść neuronowych wraz z wagami w_i (wektor wag w i sygnałów wejściowych x),
- jeden sygnał wyjściowy y,
- pobudzenie jako suma ważona sygnałów wejściowych pomniejszona o próg błędu,
- funkcja aktywacji (przejścia).

W przypadku sieci neuronowych wyróżnia się dwa typy architektury [Stefanowski, 2006]:

- sieci jednokierunkowe – sieci o jednym kierunku przepływu sygnałów, szczególnym przypadkiem sieci jednokierunkowej jest sieć warstwowa[41],
- inne typy – np. sieci rekurencyjne – sieci ze sprzężeniami zwrotnymi (sieć Hopfielda), sieci uczenia się przez współzawodnictwo (sieć Kohonena).

W ramach sieci neurony łączone są na zasadzie każdy z każdym, dzięki czemu powstaje sieć zależności. Poprawne działanie sieci wymaga przeprowadzenia procesu uczenia, który pozwoli ustawić właściwe wagi dla wejść neuronów.

W przypadku IM-BIK neuron może być interpretowany jako zagrożenie, na które podatna jest IK. Wejścia neuronu symulują zabezpieczenia, które można zastosować, aby przeciwdziałać zagrożeniu. Wagi poszczególnych wejść określają wpływ zastosowania zabezpieczenia na podatność IK na zagrożenie. Przy takiej interpretacji składowych neuronu możliwe jest generowanie przez sieć rozwiązań, które doprowadzą do uzyskania pożądanego poziomu odporności IK na rozpoznane zagrożenia. Problemem utrudniającym zastosowanie sieci neuronowych jest przede wszystkim fakt braku możliwości prześledzenia procesu uzyskiwania wyniku oraz utrudnienia z oznaczeniem zabezpieczeń, które nie mogą razem występować w jednym rozwiązaniu problemu decyzyjnego.

Metoda Analysis of Interconnected Decision Areas (AIDA)

Metoda AIDA może być wykorzystywana w dwóch odmiennych celach: do generowania dopuszczalnych elementów przestrzeni decyzyjnej D oraz do generowania trajektorii dyskretnych stanów systemu w przestrzeni D. Istota metody AIDA sprowadza się do [Krupa, Ostrowska, 2012, s. 28]:

- zbudowania modelu problemu decyzyjnego:
  - wydzielenia obszarów decyzyjnych i ich elementarnych decyzji,
  - zaznaczenia par elementarnych decyzji znajdujących się w relacji pełnej sprzeczności,
  - wyznaczenia wag względnej[42] istotności V_i obszarów decyzyjnych D_i na skali procentowej oraz wag względnej istotności v_{ji} (kosztów do sumy 1 w każdym obszarze decyzyjnym D_i) elementarnych decyzji d_{ji} na skali $<0, 1>$,
- wygenerowania zbioru dopuszczalnych decyzji niezawierających par elementarnych decyzji znajdujących się w relacji pełnej sprzeczności,
- dokonania wyboru i podjęcia decyzji:

[41] W przypadku IM-BIK sieć warstwowa może odzwierciedlać hierarchiczne problemu decyzyjne.

[42] Względna istotność obszaru decyzyjnego oznacza stopień jego istotności względem pozostałych rozpoznanych obszarów decyzyjnych.

- przeprowadzenia oceny kosztowej wszystkich poprawnie utworzonych decyzji (bez relacji sprzeczności) i uporządkowanie ich w malejącej kolejności kosztów,
- analizy uzyskanych rozwiązań, wytypowanie grupy najbardziej pożądanych wariantów decyzji, dokonanie wyboru jednej z nich i wykonanie decyzji,
- analizy skutków podjętej (wykonanej) decyzji.

Względna waga istotności pojedynczej decyzji Q jest liczona jako suma iloczynów wag istotności obszarów decyzyjnych i wag istotności elementarnych decyzji z odpowiadających im obszarów decyzyjnych wg wzoru:

$$Q = \Sigma V_i * v_{ji} \tag{1.4c}$$

gdzie:
V_i – relatywna waga istotności obszaru decyzyjnego D_i na skali otwartej <0%, 100%>,
v_{ji} – relatywna waga istotności elementarnej decyzji d_{ji} na skali otwartej <0, 1>.

W tab. 1.4d przedstawiono syntetyczną ocenę użyteczności omówionych metod z obszaru formułowania problemu decyzyjnego dla projektowanego IM-BIK.

Tabela 1.4d. Ocena metod możliwych do zastosowania w obszarze formułowania problemu decyzyjnego

Wyszczególnienie / **Kryterium oceny**	**Zbiory rozmyte**	**Algorytmy genetyczne**	**Sieci neuronowe**	**AIDA**
możliwość określenia funkcji celu	+	+	+	+
możliwość wyznaczenia zbioru obszarów decyzyjnych	+	+	+	+
możliwość określenia istotności obszarów decyzyjnych			+	+
możliwość wyznaczenia zbioru decyzji elementarnych dla obszaru decyzyjnego	+	+	+	+
możliwość określenia istotności decyzji elementarnych w obszarze decyzyjnym	+	+	+	+
możliwość redukcji zbioru rozwiązań problemu decyzyjnego poprzez oznaczenie decyzji elementarnych, które nie mogą razem występować				+
możliwość wygenerowania kompletnej listy rozwiązań	+			+
możliwość obliczenia wartości poszczególnych rozwiązań problemu decyzyjnego	+	+	+	+
możliwość intuicyjnego formułowania problemu decyzyjnego	+	+	+	+
możliwość formułowania płaskich problemów decyzyjnych	+	+	+	+
możliwość formułowania hierarchicznych problemów decyzyjnych			+	+
Podsumowanie	8	7	9	11

Źródło: opracowanie własne.

Metoda Preliminary Hazard Analysis (PHA)

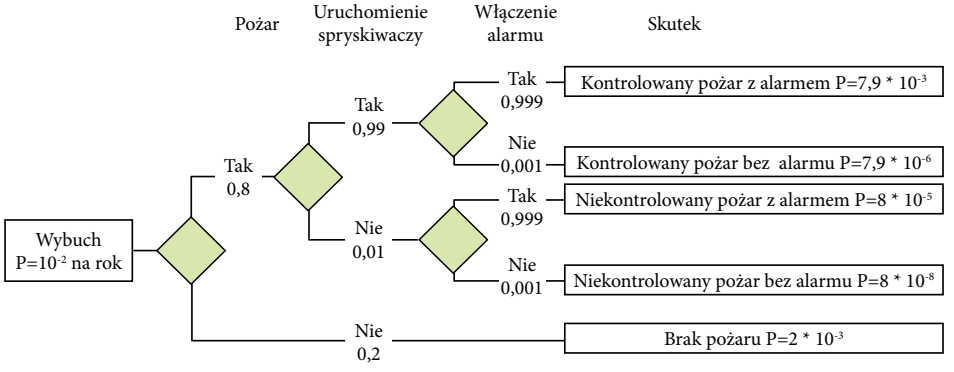
Metoda wstępnej analizy zagrożeń umożliwia identyfikację zarówno pojedynczych zagrożeń, jak i SZN dla rozpatrywanego obiektu np. IK. Metoda PHA jest głównie wykorzystywana w sytuacjach, gdy zestaw danych dotyczący procesów realizowanych w przedsiębiorstwie jest niekompletny lub dane nie są szczegółowe. Co sprawia, że wyniki metody stanowią wstępny etap dla właściwego oszacowania wartości ryzyka [Kosieradzka, Zawiła-Niedźwiecki, 2016, s. 74]. Metoda PHA umożliwia szeregowanie rozpoznanych zagrożeń wg istotności oraz identyfikację czynników ryzyka:

- przyczyny wystąpienia rozpatrywanego skutku,
- środki kontroli,
- prawdopodobieństwo wystąpienia zagrożenia,
- wpływ zdarzenia na rozpatrywany obiekt.

Metoda PHA nie uwzględnia podatności obiektu na zagrożenie. W celu zastosowania jej w ramach IM-BIK konieczne jest dodatnie tego parametru. Istotną wadą metody PHA jest dopuszczenie opisowych wartości dla wartości ryzyka, np. małe, średnie, duże. Może to powodować trudności w określeniu poziomu istotności zagrożeń przez podmiot odpowiedzialny za bezpieczeństwo IK. W celu zastosowania metody PHA w IM-BIK konieczne jest przyjęcie wzoru, który pozwoli na ilościowe obliczenie wartości ryzyka przy uwzględnieniu zebranych danych dotyczących rozpatrywanego zdarzenia.

Metoda analizy drzewa zdarzeń (ETA)

ETA jest graficzną metodą reprezentacji zależności przyczynowo skutkowych rys. 1.4b występujących w rozpatrywanym problemie np. wzajemne powiązanie zagrożeń, na które podatna jest rozpatrywana IK. Zasadą metody jest założenie, że analizowany skutek jest uwarunkowany ciągiem zdarzeń. Stąd drzewo zdarzeń rozpoczyna się od zdarzenia inicjującego (korzenia), a jego gałęzie reprezentują możliwe kombinacje zdarzeń prowadzące do obserwowanego skutku. Prawdopodobieństwo analizowanego skutku jest otrzymywane na podstawie przemnożenia prawdopodobieństw wystąpienia zdarzeń prowadzących od zdarzenia inicjującego do rozpatrywanego skutku, występujących w ramach jednej ścieżki [Kosieradzka, Zawiła-Niedźwiecki, 2016, s. 76].



Rysunek 1.4b. Przykład diagramu szacowania zagrożeń metodą ETA

Źródło: Norma ISO/IEC 31010.

Metoda ETA może być wykorzystywana do określenia wartości ryzyka wystąpienia pojedynczego zagrożenia jak i SZN. Wadą metody jest uwzględnianie jedynie prawdopodobieństwa wystąpienia zdarzenia. W celu jej zastosowania w ramach IM-BIK należy wprowadzić modyfikacje, które pozwolą na uwzględnienie: skutku wystąpienia zagrożenia dla funkcjonalności IK, podatność IK na zagrożenie oraz wpływu stosowanych zabezpieczeń na podatność IK.

Metoda matematyczna

Metoda matematyczna polega na szacowaniu ryzyka z wykorzystaniem reguł matematycznych. Stosuje się ją według następującego schematu [Kulińska, Dornfeld, 2009, s. 41–42]:

- identyfikacja wszystkich możliwych zadań[43],
- określenie wag dla kryteriów oceny ryzyka, przy czym suma wag musi wynosić jeden,
- określenie priorytetów kierownictwa, dla każdego priorytetu ustalane są wagi,
- uwzględnienie czynnika ryzyka, jakim jest czas, który upłynął od ostatniego badania i przypisanie mu wagi,
- przypisanie punktów kryterium oceny ryzyka,
- ocena ryzyka na podstawie kryteriów według wzoru:

$$[WK_1 * P_1 + WK_2 * P_2 + \ldots + WK_n * P_n] / m * 100\% \quad (1.4d)$$

gdzie:
$WK_{1...n}$ – wagi przypisane kryteriom,
$P_{1...n}$ – punkty przypisane kryteriom,
m – wartość maksymalna, jaką można przyznać dla danego kryterium,

- ocena ryzyka po uwzględnieniu daty ostatniej kontroli – ocena ryzyka według kryteriów oraz waga czynnika data ostatniego audytu,
- ocena ryzyka po uwzględnieniu priorytetu kierownictwa – ocena ryzyka według: daty ostatniego audytu oraz wagi czynnika priorytet kierownictwa,
- sprowadzenie uzyskanych wyników procentowych do wspólnego mianownika przez podzielenie wartości uzyskanej dla danego zadania przez maksymalną wartość, którą może uzyskać zadanie w analizie ryzyka,
- przyporządkowanie poszczególnym zadaniom odpowiedniej liczby dni roboczych na podstawie wyników końcowych.

W celu przeprowadzenia oszacowania ryzyka metodą matematyczną uwzględnia się kryteria: istotność, jakość zarządzania, kontrola wewnętrzna, czynniki zewnętrzne,

[43] W przypadku zastosowania tej metody w IM-BIK zbiór zadań należy zastąpić zbiorem zagrożeń dla rozpatrywanej IK.

czynniki operacyjne [Kuzinkiewicz, 2007, s. 82]. W przypadku zastosowania tej metody w IM-BIK kryteria te powinny zostać zmodyfikowane, tak aby odpowiadały danym, które są wymagane w procesie zarządzania bezpieczeństwem IK: prawdopodobieństwo wystąpienia zagrożenia, skutek dla funkcjonalności IK, podatność IK na zagrożenie, wpływ zabezpieczeń na podatność IK.

Podstawowy wzór na ryzyko

Z zagadnieniem zarządzania ryzykiem wiążą się dwa podstawowe pojęcia: niepewność i ryzyko[44]. Niepewność charakteryzuje każde podejmowanie działanie, a obserwator, w danym miejscu i czasie, nie może być pewien dalszego przebiegu tego działania. Stopień niepewności jest związany z mechanizmem zjawiska, które zawsze jest przypadkowe, a z perspektywy człowieka lub systemu, będącego wytworem ludzkim, jest związany z niedoskonałością percepcji czynników zjawiska, właściwą specyfice subiektywnego postrzegania przez człowieka [Zawiła-Niedźwiecki, 2013, s. 33]. Natomiast pojęcie ryzyka jest definiowane jako iloczyn wartości prawdopodobieństwa wystąpienia zagrożenia oraz wielkości skutków będących jego efektem [Monkiewicz, 2004, s. 26]. Wartość ryzyka można więc wyrazić wzorem:

$$R = P * S \tag{1.4e}$$

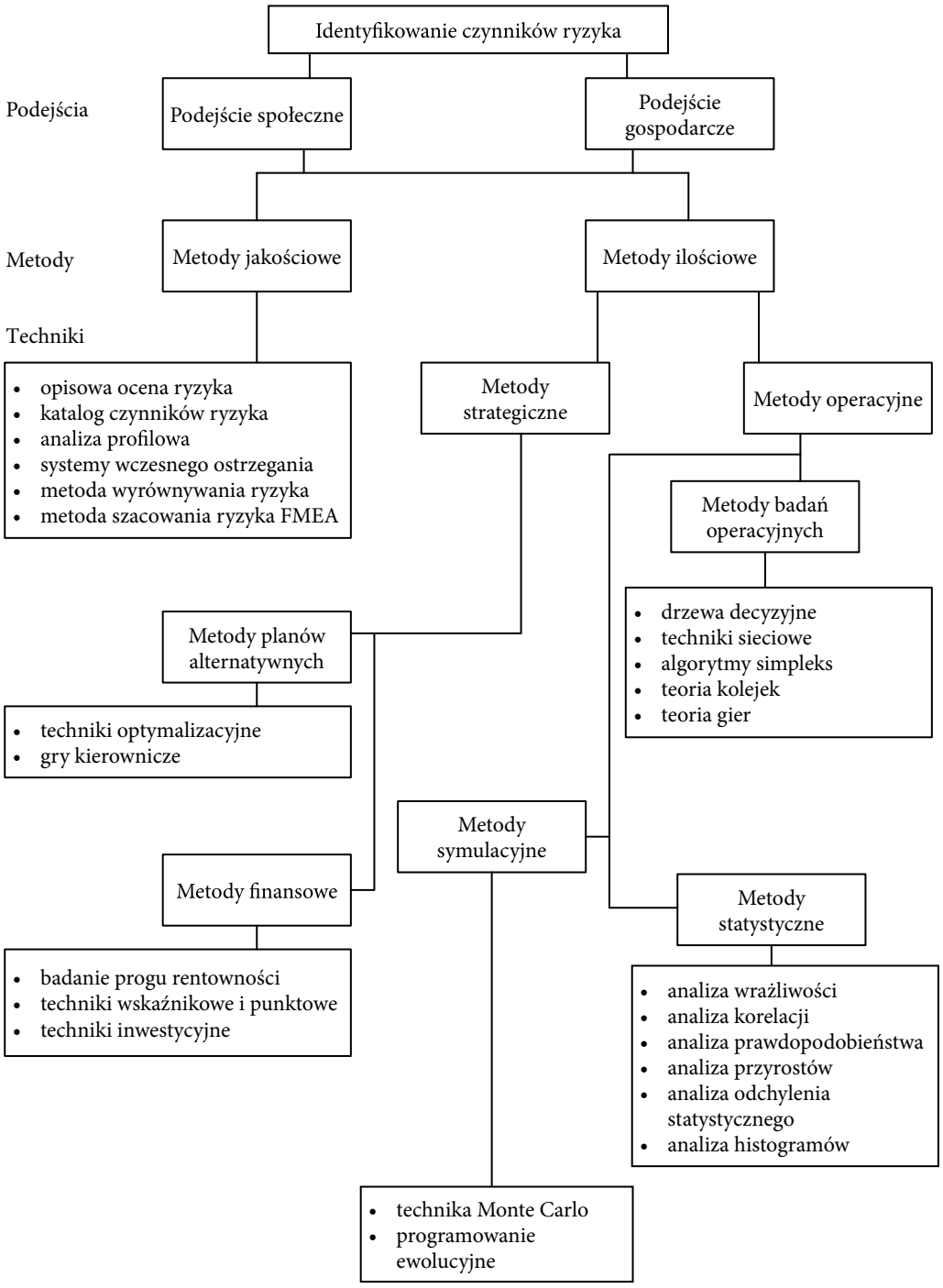
gdzie:
R – oznacza ryzyko,
P – prawdopodobieństwo wystąpienia zagrożenia,
S – skutek wystąpienia zagrożenia.

Do ustalenia wartości parametru oznaczającego prawdopodobieństwo wystąpienia zagrożenia oraz skutek wystąpienia zagrożenia używany jest szeroki wybór metod i technik rys. 1.4c. Jednak wszystkie techniki ostatecznie prowadzą do określenia wartości ryzyka na podstawie przytoczonego wzoru (1.4e).

Dodatkową cechą wzoru 1.4e jest możliwość jego modyfikacji w taki sposób, aby odzwierciedlał szerszy zakres zmiennych wpływających na wartość ryzyka. Przykład takiej modyfikacji można znaleźć w publikacji [Kosieradzka, Zawiła-Niedźwiecki, 2016, s. 247–258].

W tab. 1.4e przedstawiono syntetyczną ocenę użyteczności omówionych metod z obszaru szacowania ryzyka dla projektowanego IM-BIK.

[44] Szczegółowo przedstawionych w publikacjach m.in.: [Winiarski, 2007]; [Klimczak, 2008]; [Kaczmarek, Ćwiek, 2009]; [Zawiła-Niedźwiecki, 2013].



Rysunek 1.4c. Pomiar ryzyka – podejścia, metody, techniki
Źródło: Bizon-Górecka, 1998.

Tabela 1.4e. Ocena metod możliwych do zastosowania w obszarze szacowania ryzyka

Wyszczególnienie / Kryterium oceny	Metoda PHA	Metoda ETA	Metoda matematyczna	Podstawowy wzór na ryzyko
możliwość uwzględnienia wartości prawdopodobieństwa wystąpienia zagrożenia	+	+	+	+
możliwość uwzględnienia wartości skutku zagrożenia dla funkcjonalności IK	+		+	+
możliwość uwzględnienia wartości podatności IK na zagrożenie			+	+
możliwość uwzględnienia wpływu zabezpieczeń na podatność IK na zagrożenia	+		+	+
możliwość intuicyjnego zastosowania przez podmioty odpowiedzialne za bezpieczeństwo IK	+	+		+
Podsumowanie	4	2	4	5

Źródło: opracowanie własne.

Wyniki oceny (tab. 14b–1.4e) metod możliwych do zastosowania w celu opracowania elementów IM-BIK wskazują, że:

- w celu odwzorowania charakterystyki IK w IM-BIK należy zastosować podejście sytuacyjne (tab. 1.4b), które pozwala na:
  - uwzględnienie kanonu IK,
  - elastyczne rozszerzanie listy kategorii danych dla modelu sytuacji IK, w zależności od wymogów definiowanych w aktach normatywnych dotyczących IK,
  - odwzorowanie hierarchii elementów IK,
  - odwzorowanie zależności między IK;
- w celu generowania SZN należy zastosować metodę Bayesa (tab. 1.4c), która umożliwia:
  - odwzorowanie hierarchicznych zależności występujących między IK,
  - uwzględnienie parametru określającego prawdopodobieństwo wystąpienia zagrożenia oraz parametru określającego podatność zasobu na zagrożenie,
  - wygenerowanie ciągu zdarzeń występujących w SZN,
  - obliczenie prawdopodobieństwa wystąpienia zagrożenia pod warunkiem materializacji innego zagrożenia,
  - intuicyjne konstruowanie struktury, w której realizowane są SZN w postaci schematu graficznego;
- w celu formułowania problemu decyzyjnego należy zastosować metodę AIDA (tab. 1.4d), która pozwala na:
  - odwzorowanie hierarchii poziomów decyzyjnych,
  - nadanie składowym metody interpretacji odpowiadającej potrzebom IM-BIK, tzw. obszary decyzyjne odpowiadają zagrożeniem, na które podatna jest IK, decyzje elementarne odpowiadają zabezpieczeniom podnoszącym odporność IK na zagrożenia,
  - intuicyjne sformułowanie problemu decyzyjnego na podstawie danych dotyczących charakterystyki IK (w postaci schematu graficznego);

- w celu szacowania ryzyka należy zastosować klasyczny wzór na ryzyko (tab. 1.4e), który umożliwia wprowadzenie modyfikacji, dzięki czemu zostaną uwzględnione parametry odpowiedzialne za:
  - prawdopodobieństwo wystąpienia zagrożenia,
  - wpływ zagrożenia na funkcjonalność,
  - podatność IK na zagrożenie,
  - wpływ zabezpieczeń na poziom podatności.

1.5. Technologie wykorzystywane w procesie zarządzania bezpieczeństwem IK

Efektywne wykorzystanie elementów IM-BIK jest warunkowane wsparciem ze strony narzędzi informatycznych umożliwiających gromadzenie i przetwarzanie danych dotyczących incydentów występujących w systemach IK. Wyniki badania[45] przeprowadzonego w 2014 r. w ramach prac nad polską metodyką oceny ryzyka na potrzeby zarządzania kryzysowego wykazały, że aplikacja wspierająca zarządzanie kryzysowe (a więc i zarządzanie bezpieczeństwem IK) powinna zawierać bazę danych o zagrożeniach, moduł zobrazowania graficznego występowania i oddziaływania zagrożeń oraz moduł prognozowania przebiegu zagrożeń [Kędzierska, Banulska, Sobór, 2014, s. 138]. Narzędzia te są elementami dedykowanych systemów informatycznych wspierających zarządzanie kryzysowe, do których m.in. można zaliczyć [Galicki, Świszcz, 2013, ss. 310–319], [Szwarc, 2014, ss.129–132], [Wojtyto, Kulma, 2017]:

- System Numeru Alarmowego 112 – transmisja danych na potrzeby centrów powiadamiania ratunkowego, obsługa jednostek ratownictwa medycznego, Państwowej Straży Pożarnej, policji oraz integracja komponentów informatycznych system powiadamiania ratunkowego;
- System Szybkiego Ostrzegania (ARGUS) – opracowany na potrzeby alarmowania o zagrożeniach dla IK w ramach UE, który jest platformą integrującą systemy wczesnego ostrzegania;
- System ELIKSIR – wspieranie planowania działań w czasie kryzysu na poziomie gminy, umożliwia on tworzenie kolejnych elementów PZK zgodnie z zakresem określonym w ustawie o zarządzaniu kryzysowym;
- SARNA – monitorowanie zagrożeń epidemiologicznych;
- System Jaśmin-TELDAT – wsparcie dowodzenia umożliwiające dystrybucję informacji o zagrożeniach oraz zautomatyzowany system informowania o bieżącym położeniu sił własnych;
- Centralna Aplikacja Raportująca (CAR) – opracowana ze względu na potrzeby koordynacyjne, decyzyjne i planistyczne urzędów centralnych. CAR gromadzi dane w sześciu kategoriach: kategoria zdarzenia, przebieg (opis) zdarzenie/zagrożenia, przyczyny zdarzenia, podjęte działania, przewidywany rozwój wydarzeń, wnioski i rekomendacje (uwagi);
- *Situation Awareness of Critical Infrastructure and Networks* (SACIN) – platforma zapewniająca wspólny obraz operacyjny IK, wykorzystująca model łączenia

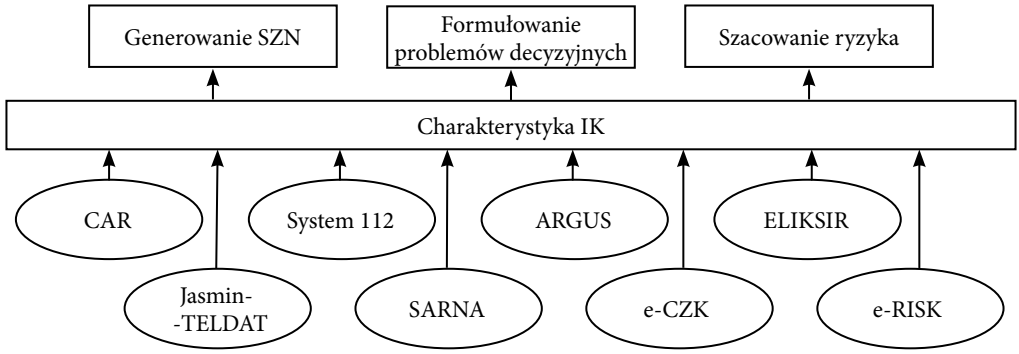
[45] Badanie objęło podmioty odpowiedzialne za przygotowanie Planów Zarządzania Kryzysowego na poziomie gminy, powiatu, województwa.

danych *Joint Director of Laboratories* (JDL) w celu integracji różnych systemów IK. Platforma umożliwia gromadzenie danych dotyczących charakterystyki IK i na tej podstawie przewidywanie wpływu rozpatrywanej IK na obiekty powiązane [Puuska, Rummkainen, Timonen, 2018];

- e-Risk – oprogramowanie ułatwiające przeprowadzenie procesu zarządzania ryzykiem na etapie określenia celów i zadań danej organizacji, identyfikacji zagrożeń, analizy ryzyka, oceny ryzyka, reakcji na ryzyko oraz monitorowania i komunikacji, zgodnie z normą PN-ISO 31000:2012;
- e-CZK – aplikacja przeznaczona do rejestracji zdarzeń zaistniałych na danym terenie administracyjnym (program obsługuje zagrożenia z województwa śląskiego).

Wymienione systemy wspomagają proces planowania cywilnego i zarządzania kryzysowego na różnych poziomach (UE, krajowym, samorządowym, sektorowym). Każdy z wymienionych systemów gromadzi i przetwarza dane, które mogą stanowić źródło danych dla IM-BIK zasilającego metodykę ZS-BIK (rys. 1.5a).

Różnorodność dostępnych systemów informatycznych może wynikać z zaobserwowanego braku wspólnego systemu pojęciowego i metodyki zarządzania bezpieczeństwem IK. Utrudnia to integrację powstających narzędzi informatycznych, ponieważ nie istnieje standard opisu charakterystyki rozpatrywanej IK. Potwierdzają to projekty badawcze[46], w ramach których powstają narzędzia informatyczne mające wspierać zarządzanie kryzysowe i ochronę IK.



Rysunek 1.5a. Schemat wykorzystania danych zebranych w istniejących systemach informatycznych wspierających proces planowania cywilnego i zarządzania kryzysowego przez elementy IM-BIK

Źródło: opracowanie własne.

[46] Projekt nr DOBR/0015/R/ID1/2012/03 pt. „Zaawansowane technologie teleinformatyczne wspomagające projektowanie systemu ratowniczego na poziomach: gmina, powiat, województwo"; Projekt nr DOBR/0016/R/ID2/2012/03 pt. „Zintegrowany system budowy planów zarządzania kryzysowego w oparciu o nowoczesne technologie informatyczne"; Projekt nr DOBR/0077/R/ID3/2013/03 pt. „Metodyka oceny ryzyka na potrzeby systemu zarządzania kryzysowego RP"; Projekt nr DOB-BIO7/11/02/2015 pt. „Wysokospecjalistyczna platforma wspomagająca planowanie cywilne i ratownictwo w administracji publicznej RP oraz w jednostkach organizacyjnych Krajowego Systemu Ratowniczo Gaśniczego".

1.6. Wnioski z rozdziału

Analiza literatury z zakresu zarządzania bezpieczeństwem IK, planowania cywilnego i zarządzania kryzysowego (rozdz. 1.1) pozwoliła na identyfikację podmiotów odpowiedzialnych za bezpieczeństwo IK (tab. 1.1e) oraz rozpoznanie barier utrudniających ich współdziałanie w obszarze ochrony IK. Są to:

- rozbieżności definicji IK i ochrony IK,
- brak standardu charakterystyki IK,
- brak metodyki zarządzania bezpieczeństwem IK.

W celu ustalenia wzorcowych etapów metodyki zarządzania bezpieczeństwem IK przeanalizowano metodyki oceny ryzyka na rzecz zarządzania kryzysowego stosowane w Polsce, USA, Kanadzie, Australii i w wybranych państwach UE (rozdz. 1.2). Ustalono, że wszystkie analizowane metodyki wykorzystują proces oceny ryzyka rekomendowany przez normę PN-EN ISO 31000:2012 zarządzanie ryzykiem – zasady i wytyczne, którego etapy stanowią podstawę dla metodyki ZS-BIK. Uwzględniając dodatkowe działania występujące w metodyce polskiej, holenderskiej i szwedzkiej uzyskano wymagane etapy metodyki ZS-BIK, tj. powołanie zespołu analitycznego, określenie progów bezpieczeństwa, odwzorowanie charakterystyk IK, wygenerowanie SZN, sformułowanie problemu decyzyjnego, szacowanie ryzyka, wdrożenie zabezpieczeń (rys. 1.2a). Etapy metodyki ZS-BIK wskazują na bazowe elementy IM-BIK, tj. możliwość odwzorowania charakterystyki IK, generowania SZN, formułowania problemu decyzyjnego, szacowania ryzyka (rys. 1.2b).

W celu rozpoznania wymaganych obszarów charakterystyki IK przeanalizowano uwarunkowania formalnoprawne procesu planowania cywilnego i zarządzania kryzysowego. Uwzględniając dane obligatoryjne (wymienione w decyzjach UE, ustawach i rozporządzeniach) oraz opcjonalne (wymienione w strategiach, programach, raportach), zidentyfikowano kanon IK (rys. 1.3a).

W rezultacie ustalenia składowych IM-BIK przeanalizowano istniejące metody wykorzystywane do określania charakterystyki rozpatrywanego obiektu, formułowania scenariuszy zdarzeń, szacowania ryzyka i rozwiązywania problemów decyzyjnych (rozdz. 1.4). Celem analizy było wskazanie zbioru metod umożliwiających przejście od zaobserwowanej charakterystyki IK do wskazania zbioru zabezpieczeń zapewniających próg bezpieczeństwa IK. Wyboru dokonano na podstawie kryteriów związanych z danymi charakteryzującymi IK oraz zapewniających współdziałanie elementów IM-BIK (tab. 1.4b–1.4e). Na podstawie dokonanej oceny ustalono, że:

- model charakterystyki IK będzie wykorzystywał podejście sytuacyjne w postaci modelu sytuacji Kłykowa,
- metoda szacowania ryzyka będzie bazować na klasycznym wzorze na ryzyko,
- metoda generowania SZN będzie wykorzystywała twierdzenie Bayesa,
- metoda formułowania problemu decyzyjnego będzie bazować na metodzie AIDA.

Uwzględniając etapy procesu planowania cywilnego oraz zarządzania kryzysowego dokonano identyfikacji stosowanych systemów informatycznych, wspierających wymienione procesy (rozdz. 1.5). Zidentyfikowane narzędzia informatyczne gromadzą dane, które będą stanowić źródło danych dla IM-BIK.

Rozdział 2. Integralny model bezpieczeństwa IK

W rozdziale zaprezentowano strukturę IM-BIK (rozdz. 2.1) oraz szczegółowo omówiono przyjęte rozwiązania w obszarze:

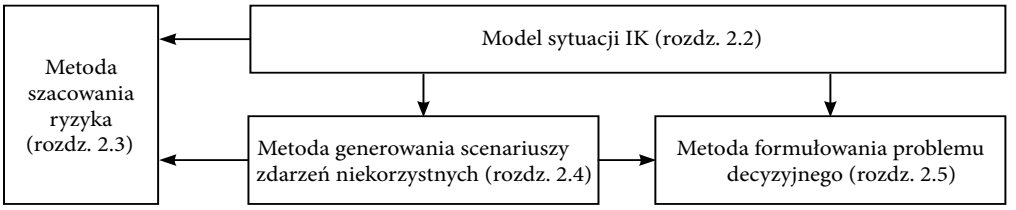
- odwzorowania charakterystyki IK, do czego wykorzystano podejście sytuacyjne umożliwiające uwzględnienie kanonu charakterystyki IK, określenie hierarchii rozpatrywanych IK oraz odwzorowanie zależności występujących między IK (rozdz. 2.2),
- szacowania ryzyka za pomocą wzoru na ryzyko dostosowanego do kanonu IK (rozdz. 2.3),
- formalnego modelu generowania SZN wykorzystującego twierdzenie Bayesa, dzięki czemu IM-BIK pozwala wygenerować ciąg zdarzeń wywołanych materializacją rozpatrywanego zagrożenia oraz określić prawdopodobieństwo wystąpienia zagrożenia pod warunkiem materializacji innego zagrożenia (rozdz. 2.4),
- formułowania problemu decyzyjnego za pomocą metody AIDA, dzięki czemu podmioty odpowiedzialne za bezpieczeństwo IK mogą wskazać kombinacje zabezpieczeń pozwalające na osiągnięcie przyjętego progu bezpieczeństwa (rozdz. 2.5).

Funkcjonowanie IM-BIK zilustrowano przykładami obliczeniowymi obrazującymi sposób wykonania modelu sytuacji IK oraz powiązanych z nim metod.

Uzupełnieniem rozdziału są załączniki: A – implementacja modelu sytuacji IK, w którym omówiono uwarunkowania pozwalające na zastosowanie modelu sytuacji IK oraz metody generowania SZN w narzędziu informatycznym IBM Websphere Business Modeler, służącym do modelowania oraz symulacji przebiegu procesów biznesowych w przestrzeni przyjętych warunków decyzyjnych; B – narzędzie implementujące procedurę budowy problemu decyzyjnego, prezentujący funkcjonalności autorskiego narzędzia informatycznego pozwalającego na opisanie danymi ilościowymi zaobserwowanego problemu decyzyjnego, oznaczenie par decyzji elementarnych pozostających w sprzeczności, wyznaczenie możliwych wariantów decyzyjnych stanowiących rozwiązanie problemu decyzyjnego oraz wyznaczenie oceny kosztowej decyzji dopuszczalnych; C – przykłady obliczeniowe zastosowania elementów IM-BIK, w którym przedstawiono sposób wykonania modelu sytuacji IK.

2.1. Struktura integralnego modelu bezpieczeństwa IK

Na podstawie analizy metodyk oceny ryzyka na potrzeby zarządzania kryzysowego ustalono, że niezbędnymi elementami IM-BIK są rozwiązania w obszarze odwzorowania charakterystyki IK, szacowania ryzyka, generowania SZN oraz formułowania problemu decyzyjnego. Zależności elementów IM-BIK ilustruje rys. 2.1a.



Rysunek 2.1a. Koncepcja IM-BIK
Źródło: opracowanie własne.

Analiza uwarunkowań formalnoprawnych zarządzania bezpieczeństwem IK wykazała, że istnieją cztery kluczowe obszary danych, które charakteryzują IK i pozwalają na opracowanie POIK[47]. Stąd model sytuacji IK[48], odpowiedzialny za odwzorowanie charakterystyki IK, integruje funkcjonalności IK z zasobami podatnymi[49] na zagrożenia, których materializacja może doprowadzić do uszkodzenia lub zniszczenia zasobu[50] i negatywnie wpłynąć na funkcjonalności IK[51]. Z kolei zagrożenia wskazują na konieczność stosowania zabezpieczeń warunkujących prawidłowe działanie zasobów i dostęp do funkcjonalności. Model sytuacji IK, wykorzystujący podejście sytuacyjne[52], wprowadza system pojęć umożliwiający odwzorowanie charakterystyki IK w taki sam sposób (niezależny od systemu IK, z którego pochodzi rozpatrywana IK). Dane zgromadzone w modelu sytuacji IK stanowią pakiet wejściowy dla wszystkich metod IM-BIK.

Określenie charakterystyki IK za pomocą modelu sytuacji IK umożliwia szacowanie wartości ryzyka związanego z zagrożeniami, na które podatna jest IK. Metoda szacowania ryzyka (rozdz. 2.3) stosowana w IM-BIK wykorzystuje zmodyfikowany wzór na ryzyko, którego składowe dostosowano do modelu sytuacji IK. Na podstawie uzyskanej

[47] POIK – Plan Ochrony Infrastruktury Krytycznej.

[48] Model sytuacji IK – obejmuje elementy kanonu IK rozszerzone o zbiór wzbudzanych zagrożeń oraz zależności z innymi obiektami.

[49] Podatność IK – prawdopodobieństwo zmiany dostępności funkcjonalności IK w wyniku wystąpienia rozpatrywanego zagrożenia, wynikające z cech konstrukcyjnych IK.

[50] Uszkodzenie lub zniszczenie zasobu w wyniku materializacji zagrożenia jest warunkowane podatnością zasobu na zagrożenie. Oznacza to, że zasób może nie ulec uszkodzeniu lub zniszczeniu w wyniku wystąpienia zagrożenia. Przykładem ilustrującym jest rafineria naftowa spółki PKN Orlen S.A. zlokalizowana w centralnej części Polski na obrzeżach miasta Płocka. Miasto Płock, a więc i rafineria ze względu na przepływającą przez nie rzekę Wisłę jest zagrożone powodzią. Jednak lokalizacja rafinerii w odległości około 3,5 km od rzeki i około 40 m nad doliną rzeki obniża podatność rafinerii na zagrożenie powodzi.

[51] Przykładem ilustrującym zjawisko utraty funkcjonalności w wyniku uszkodzenia zasobu może być szpital prowadzący cztery oddziały i wyposażony w lądowisko dla helikopterów. Każdy oddział szpitala jest traktowany jako jedna funkcjonalność, której dostępność jest określana liczbą łóżek szpitalnych i personelu medycznego. Funkcjonalność szpitala stanowi również lądowisko dla śmigłowców Lotniczego Pogotowia Ratunkowego (LPR). Rozważane jest hipotetyczne zdarzenie, w którym na terenie lądowiska wybuchł pożar. Pożar uszkadza płytę lotniska, wyłączając je z użytku na tydzień. W tym przypadku IK, jaką jest szpital, traci jedną ze swoich funkcjonalności na czas wykonania niezbędnych napraw.

[52] Podejście sytuacyjne jak i inne metody wykorzystywane w IM-BIK (twierdzenie Bayesa, metoda AIDA, wzór na ryzyko) zostały omówione i ocenione pod kątem użyteczności dla IM-BIK w rozdz. 1.4.

wartości ryzyka prognozowana jest dostępność funkcjonalności IK w sytuacji wystąpienia określonego zagrożenia. W przypadku gdy prognozowana wartość funkcjonalności IK nie osiąga progu bezpieczeństwa, formułowany jest problem decyzyjny uwzględniający zagrożenia, z których wynika rozpatrywane ryzyko.

W celu określenia możliwych konsekwencji materializacji zagrożenia dla IK opracowano metodę generowania SZN (rozdz. 2.4). Dane pochodzące z modelu sytuacji IK pozwalają na opracowanie sieci zależności[53] dla zbioru IK. Określenie tej sieci umożliwia rozpoznanie SZN, które pozwalają na zweryfikowanie czy model sytuacji IK uwzględnia wszystkie zagrożenia dla IK. Wyznaczanie SZN odbywa się na podstawie prawdopodobieństwa wystąpienia zagrożenia oraz podatności IK na to zagrożenie. Dla każdego SZN możliwe jest określenie wartości ryzyka związanego z zagrożeniami ujętymi w scenariuszu. Jeśli ryzyko związane SZN nie pozwala na osiągnięcie progu bezpieczeństwa, formułowany jest problem decyzyjny dla zagrożeń występujących w scenariuszu. Ustalenie prawdopodobieństwa wystąpienia zagrożenia pod warunkiem materializacji innego zagrożenia w metodzie generowania SZN jest realizowane z wykorzystaniem twierdzenia Bayesa.

Model sytuacji IK i SZN dostarcza podmiotom odpowiedzialnym za bezpieczeństwo IK informacji na temat zagrożeń, przed którymi należy chronić IK. Informacje te umożliwiają, za pomocą metody formułowania problemu decyzyjnego (rozdz. 2.5), jego formalny zapis i rozwiązanie. Rozwiązaniem problemu decyzyjnego w IM-BIK jest zestaw zabezpieczeń dla każdego rozpoznanego zagrożenia, pozwalający na osiągnięcie bezpieczeństwa IK. Metoda formułowania problemu decyzyjnego stanowi modyfikację metody analizy połączonych obszarów decyzyjnych (AIDA[54]). Zbiór zabezpieczeń wynikający z rozwiązania problemu decyzyjnego stanowi dla operatora IK rekomendację działań w odpowiedzi na ryzyko wynikające z zagrożeń, na które podatna jest IK. Jeśli zbiór ten zostanie zastosowany przez operatora IK, to zmieni on charakterystykę IK i ustanowi nową sytuację rozpatrywanej IK.

2.2. Model sytuacji IK

Przyjęte pojmowanie charakterystyki IK jako obiektu złożonego z zasobów, realizującego funkcjonalności, podatnego na zagrożenia i stosującego zabezpieczenia redukujące wartość ryzyka związanego z zagrożeniami pozwala na zastosowanie podejścia sytuacyjnego dla celów procesu zarządzania bezpieczeństwem IK. Użyteczny w kontekście procesu zarządzania bezpieczeństwem IK model sytuacji zaproponował J. Kłykow. Według Kłykowa sytuacja to [Kłykow, Jurek, 1988, ss. 71–72]:

- zbiór węzłów związanych ze sobą skierowanymi połączeniami[55], które odwzorowują zależności między węzłami, tworząc strukturę sytuacji,
- węzły reprezentujące elementy modelowanej rzeczywistości,
- poszczególne węzły mogą reprezentować inne struktury sytuacji, co umożliwia budowę struktur hierarchicznych.

[53] Sieć zależności – zbiór powiązań występujący między infrastrukturami krytycznymi i zagrożeniami wyrażany za pomocą wirtualnych kanałów.

[54] AIDA – ang. *Analysis Interconnected Decision Areas*.

[55] Skierowane połączenie – odwzorowanie zależności dwóch obiektów, kierunek połączenia symbolizuje sekwencję oddziaływania.

Zgodnie z definicją Kłykowa sytuację określa się jako zbiór [Kłykow, Jurek, 1988, s. 72]:

$$<W, G, T, S> \quad (2.2a)$$

gdzie:

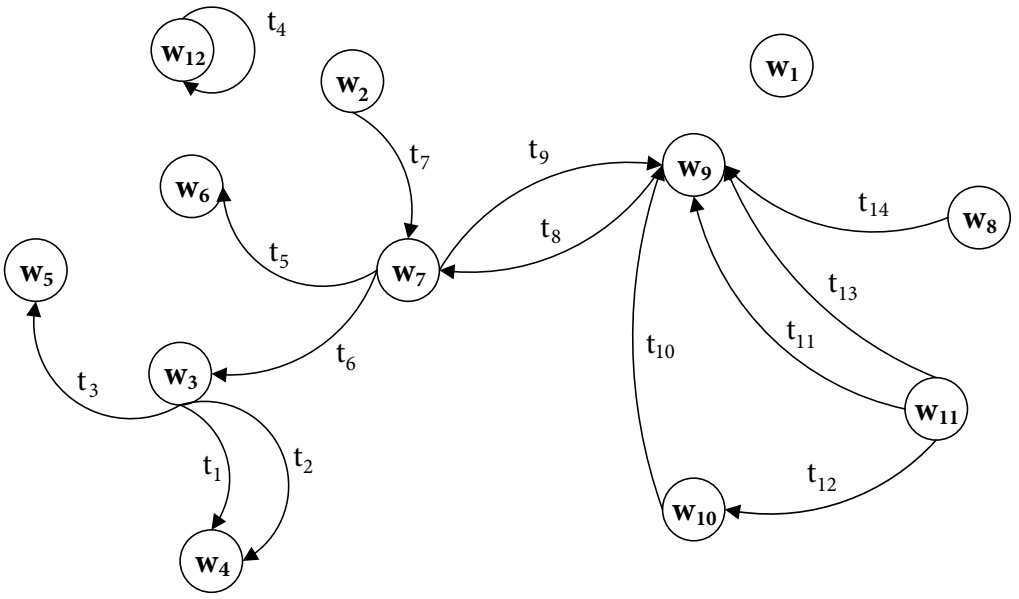
W – zbór węzłów, np. zbiór dwunastu obiektów $W\{w_1 .. w_{12}\}$, widoczny na rys. 2.2a, obiektem mogą być dowolne zasoby, m.in.: maszyny, urządzenia, zbiory danych, IK;

G – odwzorowanie przypisane każdemu węzłowi $w \in W$ – jeżeli $G_{(w)}$ jest zbiorem pustym, to oznacza to, że nie ma połączeń wychodzących z w, np. $G(_{w1})$ {} z rys. 2.2a. W szczególności $G_{(w)}$ może niejeden raz włączyć w, opisując w ten sposób pętle z w do w. Przykładem jest jednoelementowy zbiór $G_{(w12)}$ $\{t_4\}$ wskazujący, że z węzła w_{12} wychodzi jedno odwzorowanie t_4 (rys. 2.2a);

T – odwzorowanie W, zbiór wektorów zadających zawartość węzłów, przykładem jest zbiór $T\{t_1..t_{14}\}$, symbolizujący wzajemne odziaływanie węzłów ze zbioru W (rys. 2.2a);

S – odwzorowanie zbioru połączeń to suma wartości par postaci (w, t), gdzie $w \in W$, t – dowolne wejście węzła do $G_{(w).}$ Przykładem odwzorowania zbioru połączeń $S_{(w7)}$ są pary $[(w_7, t_7), (w_7, t_8)]$ (rys. 2.2a) informujące, że do węzła w_7 przyłączone są odwzorowania t_7 i t_8.

W kontekście IM-BIK zbiór węzłów W z modelu sytuacji Kłykowa jest interpretowany jako charakterystyka IK, czyli suma zbiorów V (zasobów składających się na IK), Φ (funkcjonalności realizowanych za pomocą zasobów IK), Z (zagrożeń, na które podatna jest IK) oraz M (zabezpieczeń).



Rysunek 2.2a. Przykład sytuacji wg modelu Kłykowa

Źródło: Kłykow, Jurek, 1988, s. 71.

Zagrożenia, na które podatna jest IK, mogą w wyniku materializacji wzbudzać[56] inne zagrożenia, np. awaria techniczna może ograniczyć funkcjonalność IK i jednocześnie wywołać pożar powodujący dalsze zniszczenia. Stąd charakterystykę IK należy uzupełnić o zbiór H – dostarczający wiedzy o zależności zagrożeń[57], którego postać ilustruje tab. 2.2c.

Między samymi IK również występują zależności (zbiór G, którego postać ilustruje tab. 2.2f). Dostępność funkcjonalności jednej IK warunkuje możliwość realizacji funkcjonalności przez inną IK[58]. Utrata lub ograniczenie funkcjonalności tworzy warunki sprzyjające zagrożeniom, na które podatne są inne IK[59].

Na podstawie powyższego rozumowania sformułowano model sytuacji IK[60] (2.2b).

$$<V, \Phi, Z, H, M, G> \quad (2.2b)$$

gdzie:

V – rozpatrywana IK,
Φ – zbiór funkcjonalności IK,
Z – zbiór zagrożeń, na które podatna jest IK,
H – zbiór zależności między zagrożeniami,
M – zbiór modeli zabezpieczeń IK,
G – zbiór zależności rozpatrywanej IK z innymi IK.

Przykład graficznego odwzorowania przyjętej definicji sytuacji IK obrazuje rys. 2.2b, na którym przedstawiono trzy elementy zbioru V (V_1 – szpital, V_2 – rafineria naftowa oraz V_3 – otoczenie rozpatrywanych IK). Schemat uzupełnia zbiór zależności G występujących między IK (G_1 – susza oddziałująca na V_1, G_2 – susza oddziałująca na V_2, G_3 – pożar oddziałujący na V_1, G_4 – ograniczony personel oddziałujący na V_1, G_5 – skażenie środowiska oddziałujące na V_1, G_6 – pożar oddziałujący na V_2, G_7 – awaria techniczna oddziałująca na V_2 oraz G_8 – skażenie środowiska oddziałujące na V_3).

Dodatkowo na rys. 2.2b dla IK V_1 oznaczono realizowane przez nią funkcjonalności ($\Phi_{1,1}$ – oddział leczenia oparzeń, $\Phi_{1,2}$ – lądowisko dla Lotniczego Pogotowia Ratunkowego (LPR), $\Phi_{1,3}$ – dostępność personelu medycznego), stosowane zabezpieczenia ($M_{1,1,1}$ – środki gaśnicze, $M_{1,2,1}$ – własne ujęcie wody pitnej, $M_{1,3,1}$ – system filtrów powietrza, $M_{1,4,1}$ – mobilizacja personelu niebędącego na dyżurze) oraz zagrożenia, na które podatna jest rozpatrywana IK ($Z_{1,1}$ – pożar, $Z_{1,2}$ – susza, $Z_{1,3}$ – skażenie środowiska, $Z_{1,4}$ – ograniczony personel).

Model sytuacji IK widoczny na rys. 2.2b zawiera odwzorowanie zależności zagrożeń (H_3 – zależność między zagrożeniem $Z_{1,3}$ i $Z_{1,4}$), jakie występuje w modelu sytuacji IK V_1.

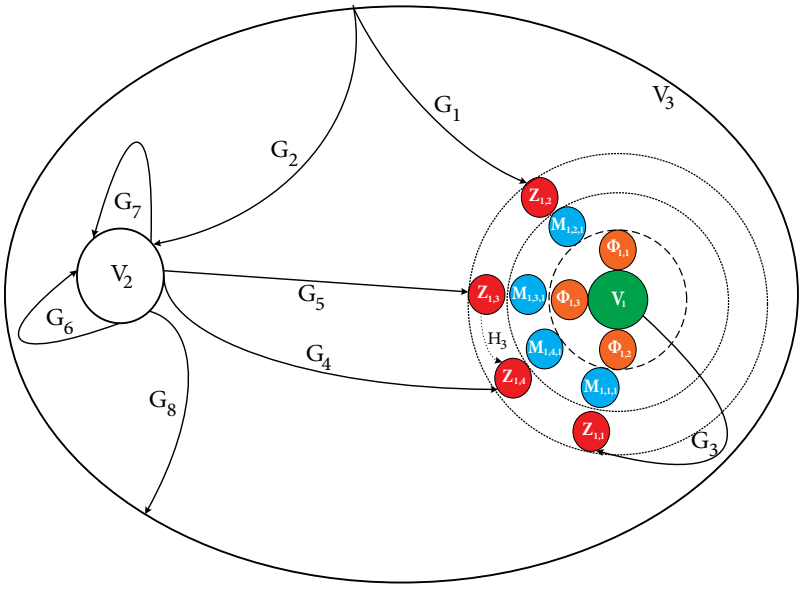
[56] Wzbudzenie zagrożenia – zaistnienie sprzyjających warunków do materializacji zagrożenia.

[57] Wystąpienie jednego zagrożenia może stworzyć warunki sprzyjające materializacji innego zagrożenia, np. wystąpienie suszy tworzy warunki sprzyjające pożarom.

[58] Przepompownia ścieków, żeby móc odbierać nieczystości, potrzebuje dostaw prądu do zasilania pomp. Zerwanie sieci trakcyjnej wywołane oblodzeniem powoduje brak zasilania pomp i utratę funkcjonalności przepompowni.

[59] Pożar w zakładzie produkcyjnym powoduje ograniczenie dostępności pracowników, którzy zostali poszkodowani. Powoduje to wystąpienie zagrożenia dla szpitala (konieczność przyjęcia dużej liczby poszkodowanych), ograniczającego jego funkcjonalność (dostępność miejsc na oddziale ratunkowym).

[60] Sytuacja IK – aktualnie obowiązująca charakterystyka IK określana w obszarze zasobów, funkcjonalności, zagrożeń oraz zabezpieczeń, uwzględniająca zależności rozpatrywanej IK z innymi IK.



Rysunek 2.2b. Przykład graficznej ilustracji zależności IK

Źródło: opracowanie własne.

Odwzorowanie charakterystyki IK w postaci modelu sytuacji IK wymaga określenia:

- zbioru V rozpatrywanych IK (w przypadku pojedynczej IK określa się zbiór zasobów, od których zależne są funkcjonalności IK),
- zbioru Φ funkcjonalności dla każdego elementu zbioru V,
- zbioru Z zagrożeń, na które podatne są elementy zbioru V,
- zbioru H zależności występujących między elementami zbioru Z,
- zbioru M stosowanych zabezpieczeń dla każdego elementu zbioru Z,
- zbioru G zależności występujących między elementami zbioru V.

Poszczególne elementy modelu sytuacji IK są określane przez podmiot odpowiedzialny za bezpieczeństwo IK na podstawie dostępnych danych lub wiedzy eksperckiej:

- Operatorzy IK – wykorzystują do tego celu wewnętrze dokumenty przedsiębiorstwa oraz posiadane POIK,
- Gminne Zespoły Zarządzania Kryzysowego – wykorzystują do tego celu gminne PZK,
- Powiatowe Zespoły Zarządzania Kryzysowego – wykorzystują do tego celu powiatowe PZK,
- Wojewódzkie Zespoły Zarządzania Kryzysowego – wykorzystują do tego celu wojewódzkie PZK oraz RZBN,
- Rządowe Centrum Bezpieczeństwa – wykorzystuje do tego celu krajowy PZK oraz RZBN.

Opracowany model sytuacji IK stanowi źródło danych dla:

- metody szacowania ryzyka – model sytuacji IK dostarcza danych o zagrożeniach, na które podatna jest IK, ich przewidywanym wpływie na funkcjonalności IK oraz stosowanych zabezpieczeniach,
- metody generowania SZN – model sytuacji IK dostarcza danych o zależnościach między rozpatrywanymi IK oraz zależnościach zagrożeń,

- metody formułowania problemu decyzyjnego – model sytuacji IK dostarcza danych o zagrożeniach będących obszarami decyzyjnymi rozpatrywanego problemu decyzyjnego.

Podstawowe składowe charakteryzujące kanon IK oraz zależności zagrożeń i IK zostały przedstawione odpowiednio w tab. 2.2a–2.2f. Zgromadzenie tych danych jest warunkiem umożliwiającym wykonanie metod: generowania SZN, szacowania ryzyka i formułowania problemu decyzyjnego. We wszystkich przypadkach zbiór atrybutów może być dowolnie rozszerzany w zależności od potrzeb określanych obowiązującymi aktami normatywnymi.

W tab. 2.2a przedstawiono podstawowe atrybuty charakteryzujące zasób. Zasoby dla ułatwienia prowadzenia analiz można grupować w klastry zasobów określonego typu[61]. Przyjęcie tego założenia pozwala na budowanie klastrów zasobów o jednakowym zbiorze zagrożeń, a w konsekwencji jednakowych modelach zabezpieczeń, co w przypadku złożonych struktur modeli sytuacji IK przyspieszy proces analizy ryzyka[62].

Tabela 2.2a. Podstawowe atrybuty zasobu

Atrybuty	Symbol	Skala
Nazwa zasobu V o indeksie α	V_{α}	–
Zagrożenie Z o indeksie β dla zasobu o indeksie α	$Z_{\alpha,\beta}$	–
Funkcjonalność Φ o indeksie γ zasobu o indeksie α	$\Phi_{\alpha,\gamma}$	–
Poziom podatności U zasobu o indeksie α na zagrożenie o indeksie β	$U_{\alpha,\beta}$	<0, 1>
Zależność G o indeksie n	G_{n}	-

Źródło: Wiśniewski, 2016b, s. 302.

Zagrożenia można również poddać klasyfikacji na poszczególne typy[63]. Podstawowe atrybuty składające się na opis zagrożenia przedstawia tab. 2.2b.

Tabela 2.2b. Podstawowe atrybuty zagrożenia

Atrybuty	Symbol	Skala
Nazwa zagrożenia Z o indeksie β oddziałującego na zasób o indeksie α	$Z_{\alpha,\beta}$	–
Rodzaj zagrożenia	IN lub OUT	–
Skutek ΔΦ wystąpienia zagrożenia wpływający na funkcjonalność Φ o indeksie γ zasobu o indeksie α	$\Delta\Phi_{\alpha,\gamma}$	<0%, 100%>
Prawdopodobieństwo P wystąpienia zagrożenia o indeksie β oddziałującego na zasób o indeksie α	$P_{\alpha,\beta}$	<0, 1>
Zabezpieczenie M o indeksie λ przed zagrożeniem o indeksie β dla zasobu α	$M_{\alpha,\beta,\lambda}$	–
Zależność zagrożeń	H_{n}	–

Źródło: Wiśniewski, 2016a, s. 436.

Dla zbioru zagrożeń, na które podatna jest IK, należy określić wykaz zagrożeń, które są wzbudzane w wyniku ich wystąpienia. Podstawowe atrybuty składające się na opis zależności zagrożeń zawarto w tab. 2.2c.

[61] Typ zasobu – zbiór zasobów o jednakowym zestawie cech.

[62] Analiza ryzyka – metoda badania procesów polegająca na rozpatrywaniu związków zachodzących między poszczególnymi elementami tych procesów, potencjalnych skutków oraz prawdopodobieństwa ich wystąpienia.

[63] Typ zagrożenia – zbiór zagrożeń o jednakowym zestawie skutków.

Tabela 2.2c. Podstawowe atrybuty zależności zagrożeń

Atrybuty	Symbol
Zależność zagrożeń	H_n
Nazwa zagrożenia wzbudzającego	$Z_{\alpha,\beta}$
Nazwa zagrożenia wzbudzanego	$Z_{\alpha,\beta}$

Źródło: opracowanie własne.

Dostępność funkcjonalności jest ustalana na podstawie:
- szacunków eksperta,
- wydajności linii/instalacji produkcyjnej, np. dzienna produkcja etanolu,
- liczby zasobów niezbędnych do jej uzyskania, np. liczba łóżek na oddziale szpitalnym.

Podstawowe atrybuty składające się na opis funkcjonalności przedstawia tab. 2.2d.

Tabela 2.2d. Podstawowe atrybuty funkcjonalności

Atrybuty	Symbol	Skala
Funkcjonalność Φ o indeksie γ zasobu o indeksie α	$\Phi_{\alpha,\gamma}$	–
Wartość ϕ funkcjonalność Φ o indeksie γ zasobu o indeksie α w rozpatrywanym okresie	$\phi_{\alpha,\gamma}$	<0%, 100%>
Wartość progu bezpieczeństwa ϕ^{PB} funkcjonalność Φ o indeksie γ zasobu o indeksie α w rozpatrywanym okresie	$\phi^{PB}_{\alpha,\gamma}$	<0%, 100%>

Źródło: opracowanie własne.

Model zabezpieczeń oznacza, uporządkowany zgodnie z celami zarządzania kryzysowego[64], zbiór zasobów i/lub procedur obniżających podatność IK na zagrożenie w ramach wymaganych przepisami prawa obszarów ochrony IK[65]. W celu opracowania pełnego modelu zabezpieczenia rozpatrywanej IK należy wskazać zabezpieczenia we wszystkich obszarach ochrony IK spełniających wszystkie cele zarządzania kryzysowego. Podstawowe atrybuty składające się na opis zabezpieczenia przedstawia tab. 2.2e.

Tabela 2.2e. Podstawowe atrybuty modelu zabezpieczeń

Atrybuty	Symbol	Skala
Zabezpieczenie M o indeksie λ przed zagrożeniem o indeksie β dla zasobu α	$M_{\alpha,\beta,\lambda}$	–
Wartość podniesienia odporności rozpatrywanej IK o indeksie α na zagrożenie o indeksie β w wyniku zastosowania zabezpieczenia o indeksie λ,	$m_{\alpha,\beta,\lambda}$	<0, 1>
Cel A zarządzania kryzysowego realizowany przez zabezpieczenie	A	–
Obszar O ochrony IK zabezpieczany przez rozpatrywany środek ochronny	O	–

Źródło: opracowanie własne.

[64] Cele zarządzania kryzysowego – zapobieganie sytuacjom kryzysowym, przygotowanie do przejmowania nad nimi kontroli w drodze zaplanowanych działań, reagowanie w przypadku wystąpienia sytuacji kryzysowych, usuwanie ich skutków oraz odtwarzanie zasobów i infrastruktury krytycznej [Dz.U. 2017 poz. 209, art. 2].

[65] Obszary ochrony IK – bezpieczeństwo fizyczne, bezpieczeństwo techniczne, bezpieczeństwo osobowe, bezpieczeństwo teleinformatyczne, bezpieczeństwo prawne, ciągłość działania [NPOIK, 2015, zał. 1, s. 5].

Ostatnim elementem modelu sytuacji IK jest zbiór zależności rozpatrywanej IK z innymi IK. Nośnikiem zależności są zagrożenia, których wystąpienie obniża dostępność funkcjonalności rozpatrywanej IK. Ograniczona funkcjonalność lub jej brak może wywołać kolejne zagrożenia, na które podatna jest zarówno rozpatrywana IK, jak i inne IK[66]. Podstawowe atrybuty składające się na opis zależności IK przedstawia tab. 2.2f.

Tabela 2.2f. Podstawowe atrybuty odwzorowujące zależność IK

Atrybuty	Symbol
Zależność G o indeksie n	G_n
Nazwa zasobu wpływającego V	V_α
Nazwa zasobu zależnego V'	V'_α
Nazwa zagrożenia Z wpływającego na zasób V'	$Z_{\alpha,\beta}$

Źródło: opracowanie własne.

Syntetyczny zapis sytuacji rozpatrywanej IK V_1 (szpitala realizującego trzy funkcjonalności, podatnego na cztery zagrożenia, chronionego czterema zabezpieczeniami, na który oddziałuje środowisko naturalne) ilustrują tab. 2.2g[67] oraz 2.2h. Pełen zapis sytuacji IK przedstawionej na rys. 2.2b umieszczono w zał. C – część A.

Tabela 2.2g. Zapis zależności zagrożeń dla elementów IK: V_1 – szpital, V_3 – środowisko naturalne

Symbol zasobu:	**V_3**	
Symbol zależności	**Zasób zależny**	**Zagrożenie wpływające**
G_1	V_1	Susza
Symbol zasobu:	**V_1**	
G_3	V_1	Pożar

Źródło: opracowanie własne.

[66] Przykładem zależności jest zdarzenie pożaru w sterowni sygnalizacji świetlnej na terenie miasta. Wystąpienie pożaru wywołało zniszczenie zasobów odpowiedzialnych za funkcjonowanie sygnalizacji świetlnej, co spowodowało utratę tej funkcjonalności. Brak sygnalizacji świetlnej wywołał zwiększoną liczbę wypadków drogowych, co wpłynęło na obniżenie dostępności funkcjonalności szpitalnego oddziału ratunkowego w wyniku konieczności przyjęcia zwiększonej liczby poszkodowanych.

[67] Z danych zawartych w tabeli 2.2g wynika, że otoczenie szpitala V_3 wpływa na szpital V_1 poprzez zagrożenie suszy, o czym informuje zależność G_1. Ponadto szpital jest podatny na pożar, dla którego sam tworzy warunki sprzyjające, o czym informuje zależność G_3.

Tabela 2.2h. Przykład syntetycznego zapisu sytuacji IK (V_1 – szpital)

IK	Funkcjonalności		Zagrożenia									Podatność na zagrożenie
								Zabezpieczenie				
	Symbol	Wartość funkcjonalności	Symbol	Rodzaj	Wzbudzane zagrożenie	Prawdopodobieństwo	Ograniczenie funkcjonalności IK	Symbol	Stopień obniżenia podatności	Cel zarządzania kryzysowego	Obszar ochrony IK	
V_1	$\Phi_{1,1}$	70%	$Z_{1,1}$	IN	–	0,3	-30%($\Phi_{1,1}$) -20%($\Phi_{1,3}$)	$M_{1,1,1}$	0,05	Przejmowanie kontroli	Bezpieczeństwo techniczne	0,5
			$Z_{1,2}$	OUT	awaria techniczna	0,4	-10%($\Phi_{1,3}$)	$M_{1,2,1}$	0,9	Zapobieganie	Ciągłość działania	0,8
	$\Phi_{1,2}$	100%	$Z_{1,3}$	OUT	awaria techniczna, zwiększona liczba poszkodowanych	0,05	-100%($\Phi_{1,2}$) -15%($\Phi_{1,3}$)	$M_{1,3,1}$	0,3	Zapobieganie	Bezpieczeństwo techniczne	0,7
	$\Phi_{1,3}$	85%	$Z_{1,4}$	OUT	–	0,65	-50%($\Phi_{1,1}$) -5%($\Phi_{1,3}$) -10%($\Phi_{1,2}$)	$M_{1,4,1}$	0,04	Przejmowanie kontroli	Ciągłość działania	0,65

Źródło: opracowanie własne.

2.3. Metoda szacowania ryzyka

Szacowanie ryzyka polega na ustaleniu umownej wartości ryzyka na podstawie prawdopodobieństwa wystąpienia zagrożenia oraz jego skutków w celu porównania wyniku z przyjętym kryterium określającym czy ryzyko jest akceptowalne [Kosieradzka, Zawiła-Niedźwiecki, 2016, s. 369]. Podmioty odpowiedzialne za bezpieczeństwo IK często mają do czynienia z danymi niepełnymi[68] i nieprecyzyjnymi[69] określanymi na podstawie danych historycznych lub wiedzy eksperckiej. Niemniej na ich podstawie konieczne jest zaproponowanie działań, które wyeliminują lub ograniczą skutki zdarzeń niekorzystnych. W tym celu opracowano metodę szacowania ryzyka dla IM-BIK, która przewiduje cztery etapy omówione w niniejszym rozdziale:

- określenie wartości parametrów ryzyka na podstawie modelu sytuacji IK,
- obliczanie wartości ryzyka utraty rozpatrywanej funkcjonalności IK,
- prognozę rozpatrywanej funkcjonalności w kolejnym okresie,
- podjęcie decyzji o postępowaniu z zagrożeniami.

Podstawowym miernikiem dla IM-BIK jest ryzyko utraty funkcjonalności. Często ryzyko jest definiowane jako iloczyn wartości prawdopodobieństwa wystąpienia zagrożenia oraz skutków będących jego efektem [Monkiewicz, 2004, s. 26], co wyraża wzór 2.3a

$$R = P * S \tag{2.3a}$$

gdzie:
R – oznacza ryzyko,
P – prawdopodobieństwo wystąpienia zagrożenia,
S – skutek wystąpienia zagrożenia.

Wyrażenie ryzyka za pomocą wartości liczbowej jest ułatwieniem w procesie zarządzania bezpieczeństwem IK, które pozwala decydentowi przyjąć strategię postępowania z ryzykiem[70].

W przypadku IM-BIK konieczna jest modyfikacja wzoru 2.3a, tak aby równanie wykorzystywało dane zgromadzone w modelu sytuacji IK, który odzwierciedla jej charakterystykę w rozpatrywanym momencie.

Modyfikacja wzoru na ryzyko wynika z przyjętej w rozprawie definicji ryzyka. Ryzyko jest rozumiane jako wartość liczbowa wyrażająca procentowo przewidywany stopień utraty funkcjonalności IK, jaki może powstać w wyniku materializacji zagrożenia. Stąd zmienna S – określająca skutek materializacji zagrożenia (2.3a) jest zastąpiona zmienną $\Delta\Phi$, która symbolizuje zmianę funkcjonalności w wyniku materializacji zagrożenia.

---

[68] Podmiot odpowiedzialny za bezpieczeństwo IK nie zna pełnej listy zagrożeń.

[69] Podmioty odpowiedzialne za bezpieczeństwo IK obecnie szacują prawdopodobieństwo wystąpienia zagrożeń na pięciostopniowej skali jakościowej. Również skutki materializacji zagrożeń są szacowane przez ekspertów, na pięciostopniowej skali jakościowej [Procedura, 2010, s. 14].

[70] Przykład możliwych strategii postępowania z ryzykiem: redukcja zagrożeń, ograniczenie skutków, transfer ryzyka, podjęcie ryzyka [Zawiła-Niedźwiecki, 2013, ss. 81–84].

Wzór na ryzyko wykorzystywany w IM-BIK uwzględnia U – podatność[71] IK na zagrożenie. Podatność jest rozumiana jako prawdopodobieństwo wystąpienia utraty rozpatrywanej funkcjonalności IK w wyniku wystąpienia zagrożenia, które wynika z cech konstrukcyjnych IK[72]. Podatność IK na zagrożenie zwiększa ryzyko związane z zagrożeniem. Stąd we wzorze na ryzyko należy rozróżnić zmienną odpowiedzialną za prawdopodobieństwo występowania zagrożenia od zmiennej obrazującej prawdopodobieństwo wystąpienia niepożądanych skutków.

W wyniku wprowadzenia zmiennej określającej podatność IK na zagrożenie, logicznym następstwem jest powiązanie jej ze zmienną M – określającą wpływ stosowanych zabezpieczeń na odporność rozpatrywanej IK[73].

W efekcie podstawiając w miejsce zmiennej S (2.3a) zmienną $\Delta\Phi$ symbolizującą zmianę funkcjonalności wywołaną materializacją zagrożenia oraz uwzględniając podatność U rozpatrywanej IK na zagrożenie i stosowane zabezpieczenia M, zaproponowano wzór na ryzyko pasujący do kanonu IK (2.3b).

$$R_{\alpha,\beta} = P_{\alpha,\beta} * \left|\Delta\Phi_{\alpha,\gamma}\right| * (U_{\alpha,\beta} - M_{\alpha,\beta}) \tag{2.3b}$$

$$U_{\alpha,\beta} - M_{\alpha,\beta} = 0 \quad \text{dla} \quad M_{\alpha,\beta} \geq U_{\alpha,\beta}$$

gdzie:

α – indeks IK,
β – indeks zagrożenia,
γ – indeks funkcjonalności rozpatrywanej IK,
$R_{\alpha,\beta}$ – wartość ryzyka <0%, 100%>,
$P_{\alpha,\beta}$ – prawdopodobieństwo wystąpienia zagrożenia β na skali <0, 1>,
$U_{\alpha,\beta}$ – podatność IK na zagrożenie β na skali <0, 1>,
$\Delta\Phi_{\alpha,\gamma}$ – skutek materializacji zagrożenia β <0%, 100%>,
$M_{\alpha,\beta}$ – suma wpływu zabezpieczeń na podatność IK na zagrożenie β na skali <0, 1>.

Zastosowanie wzoru 2.3b ilustruje ryzyko wynikające z podatności IK V_1 – szpitala na zagrożenie $Z_{1,1}$ – pożar, które może ograniczyć dostępność dwóch funkcjonalności szpitala $\Phi_{1,1}$ – liczbę miejsc na oddziale leczenia oparzeń oraz $\Phi_{1,3}$ – dostępność personelu medycznego[74]. Ryzyko związane z utratą funkcjonalności $\Phi_{1,1}$ wynosi 4,05%, a ryzyko związane z utratą funkcjonalności $\Phi_{1,3}$ wynosi 2,7%.

---

[71] Zagadnienie podatności IK na zagrożenie jest poruszane m.in. w publikacji [Krupa, Ostrowska, 2017; Pursiainen, Rod, Backer, 2017].

[72] Serwer danych jest podatny na zagrożenie braku prądu, ponieważ potrzebuje zasilania, natomiast nie jest podatny na zagrożenie niskich temperatur.

[73] Odporność – zdolność obiektu do realizacji funkcjonalności przy oddziaływaniu zakłóceń. Stosowanie zabezpieczeń podnosi odporność IK na zagrożenia (inaczej obniża podatność IK na zagrożenia). Stąd różnica między podatnością i wpływem stosowanych zabezpieczeń (U - M) wyraża zależność między podatności IK na zagrożenia i stosowanymi zabezpieczeniami.

[74] Dane ilościowe określające prawdopodobieństwo i skutek wystąpienia zagrożenia $Z_{1,1}$, a także podatność IK V_1 na zagrożenie oraz wpływ stosowanych zabezpieczeń na podatność IK przedstawia tab. 2.2h.

$$R_{1,1} = P_{1,1} * |\Delta\Phi_{1,1}| * (U_{1,1} - M_{1,1}) = 0{,}3 * |-30\%| * (0{,}5 - 0{,}05) = 4{,}05\%$$

$$R_{1,1} = P_{1,1} * |\Delta\Phi_{1,3}| * (U_{1,1} - M_{1,1}) = 0{,}3 * |-20\%| * (0{,}5 - 0{,}05) = 2{,}7\%$$

Zmodyfikowany wzór na ryzyko[75] (2.3b) uzależnia wielkość ryzyka od kluczowych elementów modelu sytuacji IK:

- zasobów – podatności zasobu na zagrożenie (U),
- zagrożeń – prawdopodobieństwa wystąpienia zagrożenia (P),
- funkcjonalności – spadku dostępności funkcjonalności w wyniku materializacji zagrożenia (ΔΦ),
- zabezpieczeń – wpływu zabezpieczeń na podatność IK na zagrożenie (M).

IK są z reguły narażone na wiele zagrożeń. Dlatego, w celu określenia wartości ryzyka dla IK, należy zsumować wartości ryzyk, związanych z zagrożeniami, na które podatna jest IK. Utrata części danej funkcjonalności jest dyskretną zmienną losową z określonymi wagami dla każdego zagrożenia, na które podatna jest rozpatrywana IK. Wagi te są równe prawdopodobieństwu zmaterializowania się zagrożenia $P_{\alpha,\beta}$ podzielonemu przez sumę prawdopodobieństw wystąpienia zagrożeń oddziałujących na IK. Stąd wzór na sumę ryzyk IK przyjmuje postać:

$$R_{\Phi\alpha,\gamma} = \Sigma_{\alpha=1}^{n} \Sigma_{\beta=1}^{j} \frac{P_{\alpha,\beta}}{\Sigma_{\alpha=1}^{n} \Sigma_{\beta=1}^{j} P_{\alpha,\beta}} * |\Delta\Phi_{\alpha,\gamma}| * (U_{\alpha,\beta} - M_{\alpha,\beta}) \tag{2.3c}$$

gdzie

$R_{\Phi\alpha,\gamma}$ – ryzyko dla rozpatrywanej funkcjonalności IK,
j – liczba zagrożeń, na które podatna jest IK o indeksie α,
n – liczba rozpatrywanych IK,
$R_{\alpha,\beta}$ – wartość ryzyka <0%, 100%>,
$P_{\alpha,\beta}$ – prawdopodobieństwo wystąpienia zagrożenia β na skali <0, 1>,
$U_{\alpha,\beta}$ – podatność IK na zagrożenie β na skali <0, 1>,
$\Delta\Phi_{\alpha,\gamma}$ – skutek materializacji zagrożenia β <0%, 100%>,
$M_{\alpha,\beta}$ – suma wpływu zabezpieczeń na podatność IK na zagrożenie β na skali <0, 1>.

Do sumy ryzyk związanych z zagrożeniami oddziałującymi na funkcjonalności IK nie wlicza się ryzyk wynikających z zagrożeń oddziałujących na rozpatrywany zasób, ale niemających wpływu na rozpatrywaną funkcjonalność. Uwzględnienie takich zagrożeń w sumie ryzyk związanych z konkretną funkcjonalnością spowoduje błędne oszacowanie wag ryryk rzeczywiście ograniczających dostępność funkcjonalności rozpatrywanej IK.

Przykład obliczeniowy ilustrujący szacowanie ryzyka na podstawie dostosowanego do kanonu IK wzoru na ryzyko (2.3c) wykorzystuje dane charakteryzujące szpital (V_1)

[75] Główna zmiana we wzorze na ryzyko dotyczy wprowadzenia zmiennej odpowiedzialnej za określenie stopnia podatności IK na zagrożenie. Uwzględnienie tej zmiennej wynika bezpośrednio z wniosków rozdz. 1.3 oraz analizy literatury przedmiotu [Zawiła-Niedźwiecki, 2013, ss. 61–62; Krupa, Ostrowska, 2017, s. 59–60, Pursiainen, 2018]. Potrzeba uwzględnienia podatności zasobu na zagrożenie została również uwidoczniona w wyniku cyberataku na strony KNF [Maciąg, Tarnowski, 2017, s. 4], natomiast o potrzebie wzmacniania odporności m.in. IK dyskutowano na spotkaniu ekspertów zorganizowanym przez RCB [Zasadzińska-Baraniewska, 2017, s. 4].

z tab. 2.2h. W przykładzie analizowane jest ryzyko związane z podatnością szpitala na cały zbiór rozpoznanych zagrożeń, które mogą mieć negatywny wpływ na funkcjonalność $\Phi_{1,2}$ – lądowisko dla LPR. Szpital jest podatny na cztery zagrożenia:

- $Z_{1,1}$ – pożar (o prawdopodobieństwie wystąpienia $P_{1,1} = 0,3$),
- $Z_{1,2}$ – susza (o prawdopodobieństwie wystąpienia $P_{1,2} = 0,4$),
- $Z_{1,3}$ – skażenie środowiska (o prawdopodobieństwie wystąpienia $P_{1,3} = 0,05$),
- $Z_{1,4}$ – ograniczony personel (o prawdopodobieństwie wystąpienia $P_{1,4} = 0,65$).

Operator szpitala w modelu sytuacji IK nie wskazał negatywnych skutków wystąpienia zagrożeń $Z_{1,1}$ i $Z_{1,2}$ dla rozpatrywanej funkcjonalności $\Phi_{1,2}$. Natomiast wystąpienie zagrożenia $Z_{1,3}$ powoduje całkowitą utratę funkcjonalności $\Phi_{1,2}$ ($\Delta\Phi_{1,2}$ =100%), a wystąpienie zagrożenia $Z_{1,4}$ obniża dostępność funkcjonalności $\Phi_{1,2}$ o $\Delta\Phi_{1,2}$ – 10%. Z modelu sytuacji szpitala (tab. 2.2h) wynika, że podatność IK V_1 na:

- pożar wynosi $U_{1,1} = 0,5$,
- suszę wynosi $U_{1,2} = 0,8$,
- skażenie środowiska wynosi $U_{1,3} = 0,7$,
- ograniczony personel wynosi $U_{1,4} = 0,65$.

Operator IK w reakcji na zagrożenie ujęte w modelu sytuacji szpitala stosuje cztery zabezpieczenia:

- $M_{1,1,1}$ – system środków gaśniczych (obniża podatność szpitala na zagrożenie $Z_{1,1}$ o $m_{1,1,1} = 0,05$),
- $M_{1,2,1}$ – własne ujęcie wody pitnej (obniża podatność szpitala na zagrożenie $Z_{1,2}$ o $m_{1,2,1} = 0,9$),
- $M_{1,3,1}$ – system filtrów powietrza (obniża podatność szpitala na zagrożenie $Z_{1,3}$ o $m_{1,3,1} = 0,3$),
- $M_{1,4,1}$ – mobilizacja personelu niebędącego na dyżurze (obniża podatność szpitala na zagrożenie $Z_{1,4}$ o $m_{1,4,1} = 0,04$).

Opisana sytuacja szpitala jest syntetycznie przedstawiona w postaci poniższego zbioru równań.

$$R_{\Phi 1,2} \approx 8,52\%$$

$$R_{1,3} = \frac{P_{1,3}}{\sum_{\alpha=1}^{1}\sum_{\beta=1}^{4} P_{\alpha,\beta}} * \left|\Delta\Phi_{1,2}\right| * (U_{1,3} - M_{1,3,1}) = \frac{0,05}{1,4} * 100\% * (0,7 - 0,3) \approx 2,86\%$$

$$R_{1,4} = \frac{P_{1,4}}{\sum_{\alpha=1}^{1}\sum_{\beta=1}^{4} P_{\alpha,\beta}} * \left|\Delta\Phi_{1,2}\right| * (U_{1,4} - M_{1,4,1}) = \frac{0,65}{1,4} * 10\% * (0,65 - 0,04) \approx 5,66\%$$

W przykładzie obliczeniowym sumaryczne ryzyko utraty funkcjonalności $\Phi_{1,2}$ wyniosło w przybliżeniu $R_{\Phi 1,2} = 8,52\%$. Uzyskany wynik oznacza, że uwzględniając prawdopodobieństwo wystąpienia zagrożeń ($P_{1,3}$, $P_{1,4}$), wpływ zagrożeń na funkcjonalność ($\Delta\Phi_{1,2}$), podatność szpitala na zagrożenia ($U_{1,3}$, $U_{1,4}$) oraz stosowane zabezpieczenia ($M_{1,3,1}$, $M_{1,4,1}$) operator IK ponosi ponad 8% ryzyko utraty dostępności lądowiska dla LPR.

W zależności od bazowego poziomu funkcjonalności $\Phi_{1,2}$ oraz założonego progu bezpieczeństwa[76] operator może podjąć decyzję o postępowaniu z ryzykiem, np. przewidywana utrata funkcjonalności poniżej progu bezpieczeństwa sugeruje wdrożenie dodatkowych zabezpieczeń obniżających wartość ryzyka.

W rozpatrywanym przykładzie obliczeniowym pominięto zagrożenia $Z_{1,1}$ i $Z_{1,2}$ ponieważ nie mają one wpływu na rozpatrywaną funkcjonalność $\Delta\Phi_{1,2} = 0$, co powoduje, że wartość ryzyka związana z tymi zagrożeniami wynosi zero. Dodatkowo w przypadku zagrożenia $Z_{1,2}$ oddziaływanie zabezpieczeń $M_{1,2}$ jest większe niż podatność IK $U_{1,2}$ na rozpatrywane zagrożenie, co również sprowadza wartość ryzyka związanego z tym zagrożeniem do zera.

Znajomość wartości ryzyka utraty funkcjonalności w połączeniu z danymi pochodzącymi z modelu sytuacji rozpatrywanej IK daje możliwość określenia, jaka będzie dostępność funkcjonalności w momencie materializacji zagrożenia i czy nie spadnie poniżej założonego progu bezpieczeństwa. Zależność ta jest zobrazowana wzorem 2.3d.

$$\Phi_{\alpha,\gamma}(t_{n+1}) = \Phi_{\alpha,\gamma}(t_n) - R_{\Phi\alpha,\gamma}(t_n) \tag{2.3d}$$

gdzie:
$\Phi_{\alpha,\gamma}(t_{n+1})$ – prognozowy poziom funkcjonalności w momencie t_{n+1},
$\Phi_{\alpha,\gamma}(t_n)$ – zmierzony/oszacowany poziom funkcjonalności w momencie t_n, wynikający z modelu sytuacji rozpatrywanej IK,
$R_{\Phi\alpha,\gamma}(t_n)$ – wartość ryzyka utraty funkcjonalności w momencie t_n.

Posługując się wzorem 2.3d, można oszacować przewidywany poziom funkcjonalności $\Phi_{1,2}$ – lądowisko dla LPR, w wyniku materializacji zagrożeń $Z_{1,3}$ – skażenie środowiska i $Z_{1,4}$ – ograniczony personel. Ryzyko dla utraty funkcjonalności $\Phi_{1,2}$ wynosi 8,52%. Dostępność tej funkcjonalności w rozpatrywanym okresie początkowym (t_n) wynosi 100% (tab. 2.2h). Stąd przewidywana dostępność funkcjonalności $\Phi_{1,2}$ w okresie t_1 wyniesie 91,48%.

$$\Phi_{\alpha,\gamma}(t_1) = 100\% - 8{,}52\% \approx 91{,}48\%$$

Możliwość oszacowania dostępności funkcjonalności w wyniku materializacji konkretnego zagrożenia lub SZN pozwala określić strategię postępowania wobec zagrożeń. Przyjmując czterostopniową skalę dostępności funkcjonalności[77] (tab. 2.3a), można podjąć decyzję dotyczącą postępowania z ryzykiem[78].

---

[76] Próg bezpieczeństwa – poziom funkcjonalności uznany przez podmiot odpowiedzialny za bezpieczeństwo IK za wystarczający do realizacji zadań IK.

[77] Zarówno liczba przedziałów, jak i ich granice muszą być dostosowywane do specyfiki rozpatrywanej IK.

[78] Możliwość podejmowania decyzji dotyczących postępowania z ryzykiem współgra ze sposobem reakcji na wartość ryzyka związanego z zagrożeniami, zalecanym przez RCB w procedurze przygotowania raportów cząstkowych do raportu o zagrożeniach bezpieczeństwa narodowego [Procedura, 2010, ss. 17–18].

Tabela 2.3a. Przykład przedziałów określających postępowanie z ryzykiem

Nazwa przedziału	Rozpiętość przedziału	Działanie
stan akceptowalny	(75%, 100%>	nie są wymagane żadne dodatkowe zabezpieczenia
stan ostrzegawczy	(50%, 75%>	należy dokonać oceny, czy wprowadzenie dodatkowych zabezpieczeń przyczyni się do poprawy bezpieczeństwa IK
stan awaryjny	(25%, 50%>	należy wprowadzić dodatkowe zabezpieczenia np. w ciągu 6 miesięcy
stan kryzysowy	<0%, 25%>	należy podjąć natychmiastowe działania w celu zwiększenia bezpieczeństwa IK

Źródło: opracowanie własne na podstawie Procedura, 2010, ss. 17–18.

Z tab. 2.3a wynika, że prognozowana dostępność funkcjonalności powyżej 75% nie wymaga żadnej reakcji ze strony operatora IK. Stąd, dla rozpatrywanego przypadku, próg bezpieczeństwa wynosi 75%.

Wykorzystując wzór na prognozowany poziom dostępności funkcjonalności, można sformułować relację pomiędzy poziomem ryzyka utraty funkcjonalności a progiem bezpieczeństwa. IK można uznać za bezpieczną, gdy próg bezpieczeństwa Φ^{PB} jest mniejszy lub równy pozimowi funkcjonalności w momencie zakładającym wystąpienie zagrożenia $\Phi_{\alpha,\gamma}(t_{n+1})$ (2.3e).

$$\Phi^{PB} \leq \Phi_{\alpha,\gamma}(t_{n+1}) \tag{2.3e}$$

$$\Phi^{PB} \leq \Phi_{\alpha,\gamma}(t_n) - R_{\Phi_{\alpha,\gamma}}(t_n)$$

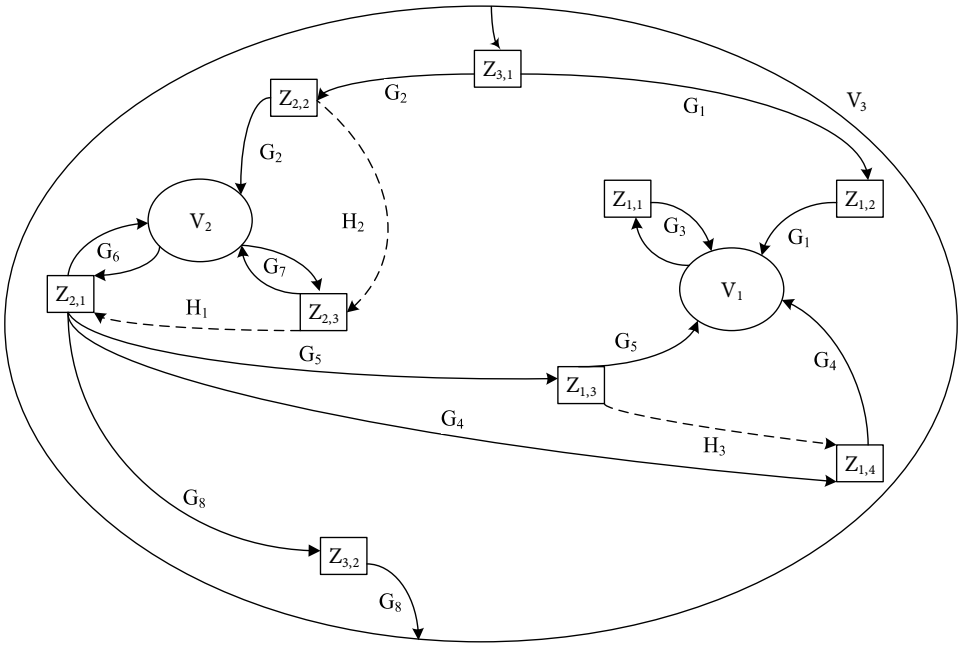
W przypadku gdy warunek 2.3d nie jest spełniony, operator IK ma obowiązek sformułować i rozwiązać problem decyzyjny, którego rozwiązanie pozwoli na wskazanie zabezpieczeń ograniczających wartość ryzyka.

2.4. Metoda generowania scenariuszy przebiegu zdarzenia niekorzystnego

System powiązanych IK (SPIK) powstaje na podstawie danych zawartych w rozpatrywanych modelach sytuacji IK, które są jego składowymi. Przykładem SPIK jest zbiór IK V_1 – szpital, który funkcjonuje w obrębie jednego miasta (V_3) obok IK V_2 – rafinerii naftowej (rys. 2.4a).

IK V_1 jest podatna na cztery zagrożenia $Z_{1,1}$ – pożar, $Z_{1,2}$ – susza, $Z_{1,3}$ – skażenie środowiska i $Z_{1,4}$ – ograniczony personel, natomiast IK V_2 jest podatna na trzy zagrożenia $Z_{2,1}$ – pożar, $Z_{2,2}$ – susza i $Z_{2,3}$ awaria techniczna. Między zagrożeniami IK V_1 występuje zależność H_3 informująca, że materializacja zagrożenia $Z_{1,3}$ wzbudza zagrożenie $Z_{1,4}$. Podobne zależności występują między zagrożeniami IK V_2: zależność H_1 informuje o wzbudzeniu zagrożenia $Z_{2,1}$ w wyniku materializacji zagrożenia $Z_{2,3}$, a zależność H_2 informuje o wzbudzeniu zagrożenia $Z_{2,3}$ w wyniku materializacji zagrożenia $Z_{2,2}$. Rozpatrywane IK oddziałują na siebie wzajemnie, co ilustruje zbiór zależności G, np. zależność G_4 – wskazuje na wpływ IK V_2 na IK V_1 wynikający z materializacji zagrożenia $Z_{2,1}$ – pożaru, w wyniku którego nastąpiła utrata funkcjonalności $\Phi_{2,3}$ – dostępności personelu,

co powoduje materializację zagrożenia $Z_{1,4}$ – ograniczenia personelu szpitalnego, który zajmuje się poszkodowanymi w pożarze. Wystąpienie zagrożenia $Z_{1,4}$ w wyniku materializacji zagrożenia $Z_{2,1}$ negatywnie wpływa na funkcjonalność $\Phi_{1,3}$ szpitala obniżając dostępność personelu medycznego w IK V_1.



Elipsy oznaczają IK (V_α), prostokąty – zagrożenia ($Z_{\alpha,\beta}$), strzałki ciągłe – zależności rozpatrywanych IK (G_n), strzałki przerywane – wzbudzanie zagrożeń (H_n)

Rysunek 2.4a. Przykład identyfikacji zależności IK w rozpatrywanym SPIK[79]

Źródło: opracowanie własne.

SPIK jest przestrzenią, w której realizują się SZN[80]. Wiedza dotycząca przebiegu SZN jest uzupełnieniem informacji o zagrożeniach, na które podatna jest rozpatrywana IK. Dzięki analizie przebiegu SZN można zweryfikować czy nie pominięto zagrożeń dla rozpatrywanej IK oraz czy odpowiednio oceniono konsekwencje wystąpienia zdarzenia niekorzystnego (wzbudzenie innych zagrożeń).

Uwzględnienie SZN w procesie analizy ryzyka jest odpowiedzią na potrzebę podmiotów odpowiedzialnych za bezpieczeństwo IK, która dotyczy przygotowania planów reakcji na zagrożenia i zaangażowania odpowiednich zasobów we właściwym czasie i miejscu oraz racjonalnego gospodarowania nimi.

[79] Rysunek 2.4a przedstawia przykład SPIK opracowany na podstawie modeli sytuacji IK zawartych w zał. C – część A.

[80] Zdarzenie niekorzystne – zdarzenie będące efektem spełnienia się zagrożenia, mające negatywne skutki dla organizacji, środowiska naturalnego lub ludności.

Zdarzenie niekorzystne rozprzestrzenia się dzięki zależnościom, które występują między IK (charakteryzowanych przez zbiór G modelu sytuacji IK) oraz zagrożeniami (charakteryzowanych przez zbiór H modelu sytuacji IK). Zależności mogą być określane na podstawie:

- wiedzy eksperckiej – w tym przypadku ekspert wykorzystując własne doświadczenia, wskazuje, jaki wpływ na rozpatrywaną IK, a także inne IK, będzie miało wystąpienie zdarzenia niekorzystnego. Przykład zależności określonych w ten sposób występujących między systemami IK został przedstawiony w zał. G;
- danych statystycznych – zależności są identyfikowane na podstawie zdarzeń zapisanych w bazach danych gromadzących dane o zdarzeniach niekorzystnych. Analizując zdarzenia, możliwe jest określenie, jakie skutki zostały wzbudzone przez rozpatrywane zdarzenie niekorzystne[81],
- analizy procesów – podstawą wskazywania możliwych następstw zdarzenia niekorzystnego są powiązania procesowe występujące między IK[82] dotyczące realizacji produktów lub usług;
- analizy modeli sytuacji IK – do określenia zależności między IK wykorzystuje się dane zawarte w modelach sytuacji IK będących składowymi SPIK.

Do wykonania SPIK przedstawionego na rys. 2.4a wykorzystano metodę generowania scenariuszy zdarzeń niekorzystnych, która zakłada dwa etapy:

- opracowanie SPIK na podstawie danych zawartych w modelach sytuacji IK,
- przygotowanie wykazu SZN.

Utworzenie SPIK polega na opracowaniu graficznego modelu składającego się z:

- węzłów, które reprezentują zmienne losowe:
  - prawdopodobieństwo wystąpienia zagrożenia (prostokąty na rys. 2.4a, np. zagrożenie $Z_{1,1}$),
  - podatność IK na zagrożenia (elipsy na rys. 2.4a[83], np. IK V_1);
- strzałek łączących węzły, co jest interpretowane jako odwzorowanie zależności zagrożeń (strzałki przerywane na rys. 2.4a, np. zależność H_3) i IK (strzałki ciągłe na rys. 2.4a, np. zależność G_4).

Zależności w przypadku IM-BIK są wyrażane przez wirtualne kanały[84] określające:

- zależności IK – komunikacja podatności $U_{\alpha,\beta}$ IK V_α i prawdopodobieństwa wystąpienia zagrożenia $P_{\alpha,\beta}$ wyrażona na skali <0, 1>, określająca prawdopodobieństwo utraty funkcjonalności po uwzględnieniu podatności IK na rozpatrywane zagrożenie, co można zapisać $P(P_{\alpha,\beta}|U_{\alpha,\beta})$, gdzie: α – indeks IK; β – indeks zagrożenia;

[81] Przykładem baz danych gromadzących dane o zdarzeniach niekorzystnych są m.in.: Centralna Aplikacja Raportująca i System Wspomagania Decyzji Państwowej Straży Pożarnej.

[82] Przykładem może być sytuacja awarii warszawskiego systemu wypożyczania rowerów, która miała miejsce w 2013 r. Z powodu dużych opadów w Niemczech swoją funkcjonalność utraciły serwery zlokalizowane w miejscowości Jena obsługujące system Nextbike na całym świecie. Skutkiem tego był brak łączności i utrudnienia w korzystaniu z rowerów miejskich w Warszawie [Veturilo nie działa, <nasze miasto.pl> data odczytu: 07.08.2017 r.].

[83] W SPIK symbol elipsy przechowuje informację o podatności IK na wszystkie zagrożenia.

[84] Wirtualny kanał – zależność między zasobem i zagrożeniem lub między zagrożeniem i zagrożeniem.

- zależności zagrożeń – komunikacja prawdopodobieństwa zagrożenia $P_{\alpha,\beta}$ pod warunkiem wystąpienia innego zagrożenia $P'_{\alpha,\beta}$ wyrażona na skali <0, 1>, określająca prawdopodobieństwo materializacji rozpatrywanej pary zagrożeń, co można zapisać $P(P_{\alpha,\beta}|P'_{\alpha,\beta})$ gdzie: α – indeks IK; β – indeks zagrożenia.

Wirtualne kanały dotyczące zależności IK i zależności zagrożeń mogą być dodawane lub usuwane z SPIK:

- zależność IK jest dodawana do SPIK w wyniku identyfikacji podatności rozpatrywanej IK na zagrożenie, przykładem jest zależność G_7 symbolizująca podatność IK V_2 na zagrożenie $Z_{2,3}$ (rys. 2.4a);
- zależność IK jest usuwana z SPIK w wyniku uzyskania przez IK odporności na rozpatrywane zagrożenie tylko w sytuacji, gdy rozpatrywane zagrożenie nie wzbudza innych zagrożeń, na które podatna jest rozpatrywana IK – oznacza to, że zależność G_3 może zostać usunięta ze SPIK (rys. 2.4a), jeśli IK V_1 przestanie być podatna na zagrożenie $Z_{1,1}$, natomiast uzyskanie odporności IK V_1 na zagrożenie $Z_{1,3}$ nie może spowodować usunięcia zależności G_5 z SPIK, ponieważ zagrożenie $Z_{1,3}$ oprócz oddziaływania na IK V_1 wzbudza również zagrożenie $Z_{1,4}$, na które IK V_1 jest podatna;
- zależność zagrożeń jest dodawana do SPIK w wyniku identyfikacji możliwości wzbudzenia przez rozpatrywane zagrożenie innego zagrożenia zawartego w SPIK, na które podana jest przynajmniej jedna IK, przykładem jest zależność H_3 (rys. 2.4a) symbolizująca możliwość wzbudzenia zagrożenia $Z_{1,4}$ w wyniku materializacji zagrożenia $Z_{1,3}$;
- zależność zagrożeń, jeśli raz została rozpoznana, nie jest usuwana ze SPIK nawet w sytuacji uzyskania przez IK odporności na zagrożenie wzbudzające inne zagrożenia.

Kanały funkcjonują w strukturze obiektów SPIK. Wykorzystując zapis określający zawieranie się zbiorów, można odwzorować położenie IK względem siebie (2.4a). Na rys. 2.4a obiekt V_3 jest nadrzędny w stosunku do obiektów V_1 i V_2, co można zapisać w postaci:

$$V_3 \ni \{V_1, V_2\} \tag{2.4a}$$

Formuła 2.4a oznacza, że IK V_3 zawiera w sobie dwa elementy: IK V_1 i IK V_2. Oznacza to, że na terenie IK V_3 znajduje się IK V_1 i IK V_2.

W celu wygenerowania SZN oraz ustalenia wartości ryzyka, jakie jest z nimi związane, należy syntetycznie przedstawić dane pochodzące z rozpatrywanych modeli sytuacji IK ujętych w SPIK, które dotyczą podatności IK na zagrożenia i zależności zagrożeń.

Tabela 2.4a przedstawia ideowy zapis odwzorowujący podatności składowych SPIK na zagrożenia. W kolumnie 1 wyszczególnione są wszystkie zagrożenia, jakie zostały zidentyfikowane dla rozpatrywanego SPIK ($Z_{\alpha,\beta}$). W kolumnie 2 i kolejnych znajdują się zasoby (V_α), które stanowią składowe SPIK. W polach kolumny 2 i kolejnych wpisywane są:

a) prawdopodobieństwo $P_{\alpha,\beta}$ wystąpienia zagrożenia $Z_{\alpha,\beta}$,
b) podatność $U_{\alpha,\beta}$ zasobu V_α na zagrożenie $Z_{\alpha,\beta}$,
c) wpływ zabezpieczenia $M_{\alpha,\beta,\lambda}$, zmniejszający podatności zasobu V_α na zagrożenie $Z_{\alpha,\beta}$.

Tabela 2.4a. Ideowy zapis odwzorowujący podatności składowych SPIK na zagrożenia

Wyszczególnienie	**Zasób (V_α)**	
Kolumna 1	**Kolumna 2**	
Zagrożenia ($Z_{\alpha,\beta}$)	$P_{\alpha,\beta}$	$U_{\alpha,\beta}$
		$M_{\alpha,\beta,\lambda}$

Źródło: Wiśniewski, 2016a, s. 437.

Tabela 2.4b przedstawia ideowy zapis odwzorowujący zależności zagrożeń występujących w SPIK. W wierszach i kolumnach są wyszczególnione wszystkie zagrożenia, na jakie podatne są składowe rozpatrywanego SPIK. W przypadku gdy zagrożenie oznaczone w wierszu ($Z_{\alpha,\beta}$) wzbudza zagrożenie oznaczone w kolumnie ($Z'_{\alpha,\beta}$), na ich przecięciu wpisywane są prawdopodobieństwa wystąpienia tych zagrożeń.

Tabela 2.4b. Ideowy zapis odwzorowujący zależności zagrożeń w SPIK

Wyszczególnienie	Zagrożenia ($Z'_{\alpha,\beta}$)	
Zagrożenia ($Z_{\alpha,\beta}$)	$P'_{\alpha,\beta}$	$p'_{\alpha,\beta}$
	$P_{\alpha,\beta}$	$p_{\alpha,\beta}$

Źródło: opracowanie własne.

Zebrane dane pozwalają na zastosowanie wybranej techniki generowania SZN. W celu przyspieszenia procesu generowania SZN proponuje się zastosowanie symulacji komputerowej, której założenia przedstawiono w zał. A.

Zastosowane narzędzie symulacyjne wykorzystuje twierdzenie Bayesa, które zakłada, że możliwe jest zapisanie dowolnej informacji w postaci ciągu zdarzeń, który pozwoli na ustalenie prawdopodobieństwa wystąpienia rozpatrywanego zdarzenia. Twierdzenie Bayesa wyraża się wzorem 2.4b [Bolstad, 2004]:

$$P(A|B) = \{P(A) * P(B|A)\}/ \sum P(B|E_i) * P(E_i) \quad (2.4b)$$

gdzie:
$P(A)$ – prawdopodobieństwo zdarzenia A,
$P(A|B)$ – prawdopodobieństwo zdarzenia A pod warunkiem nastąpienia zdarzenia B,
E_i – rozpatrywane zdarzenie.

Przykładem zastosowania twierdzenia Bayesa dla rozpatrywanego SPIK (rys. 2.4a) jest obliczenie prawdopodobieństwa wystąpienia zagrożenia $Z_{1,4}$ – ograniczenie dostępności personelu medycznego pod warunkiem materializacji zagrożenia $Z_{1,3}$ – skażenia środowiska. Prawdopodobieństwa wystąpienia zagrożeń kształtują się następująco: zagrożenie $Z_{1,3}$ – $P_{1,3} = 0{,}05$, a $Z_{1,4}$ – $P_{1,4} = 0{,}65$. Podstawiając prawdopodobieństwo wystąpienia rozpatrywanych zagrożeń do wzoru 2.4b, uzyskuje się prawdopodobieństwo wystąpienia zagrożenia $Z_{1,4}$ w wyniku materializacji zagrożenia $Z_{1,3}$, $P(Z_{1,4}| Z_{1,3}) = 0{,}93$.

$$P(Z_{1,4} | Z_{1,3}) = \frac{(P_{1,4} * 0{,}5)}{(P_{1,4} * 0{,}5) + (P_{1,3} * 0{,}5)}$$

$$P(Z_{1,4} | Z_{1,3}) = \frac{(0{,}65 * 0{,}5)}{(0{,}65 * 0{,}5) + (0{,}55 * 0{,}5)} = 0{,}93$$

Rysunki 2.4b i 2.4c ilustrują SPIK przedstawiony na rys. 2.4a, zaimplementowany w narzędziu informatycznym służącym do symulacji procesów biznesowych[85]. Na rysunkach widać:

- sterownik – element służący do sterowania wzbudzaniem zagrożeń,
- obiekty niebieskie – symbolizujące zagrożenia, w ramach których zapisano prawdopodobieństwo ich wystąpienia,
- obiekty pomarańczowe – symbolizujące zasoby, w ramach których określono podatności zasobów na zagrożenia uszczegółowione na rys. 2.4c,
- obiekty żółte – symbolizujące podatność zasobu V_{α} na zagrożenie $Z_{\alpha,\beta}$,
- obiekty szare – odwzorowujące zawieranie się elementów zbioru V.

Na podstawie symulacji przeprowadzonej na próbie 1000 wzbudzeń zagrożenia $Z_{3,1}$ – susza, uzyskano 18 SZN, z których 11 zakończyło się negatywnymi skutkami dla rozpatrywanych IK lub ich otoczenia. Przykład opisu SZN ilustruje tab. 2.4c, natomiast pełne wyniki symulacji przedstawiono w zał. C – część B.

Tabela 2.4c. Przykład opisu SZN dla zagrożenia $Z_{3,1}$ – susza

Wyszczególnienie	Sekwencja zdarzeń			Liczba przypadków	Rozkład
	Wzbudzenie	Materializacja	Skutek		
Scenariusz 5	$Z_{2,1}$-D	$Z_{2,1}$-P		1	0,10%
	$Z_{2,2}$-D	$Z_{2,2}$-P			
	$Z_{2,3}$-D	$Z_{2,3}$-P			
	$Z_{1,2}$-D	$Z_{1,2}$-P			
	$Z_{1,3}$-D				
	$Z_{1,4}$-D	$Z_{1,4}$-P	$Z_{1,4}$-R		
	$Z_{3,1}$-D	$Z_{3,1}$-P			
	$Z_{3,2}$-D				

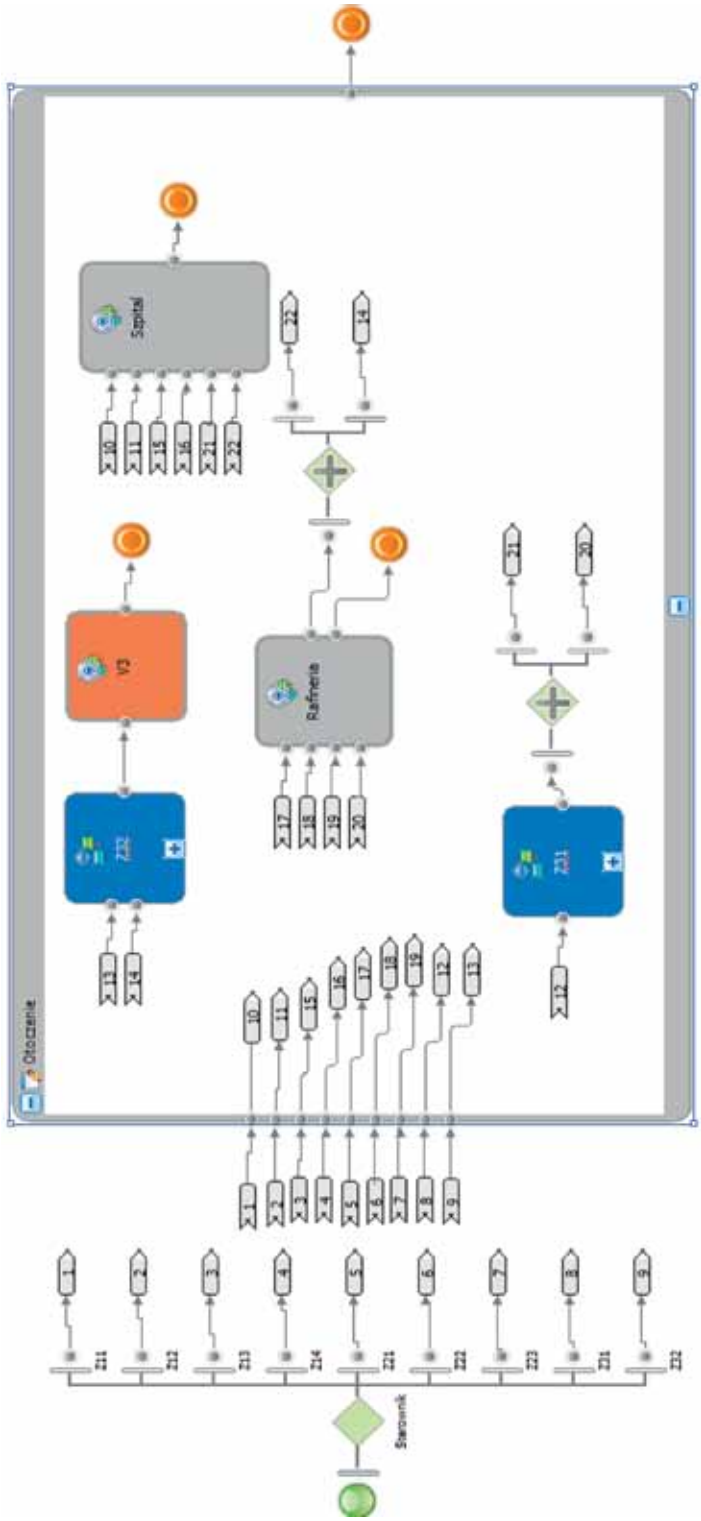
Źródło: opracowanie własne.

Dane zawarte w tab. 2.4c informują podmiot odpowiedzialny za bezpieczeństwo IK, że w ramach SZN nr 5 zostało wzbudnych osiem zagrożeń ($Z_{1,2}$; $Z_{1,3}$; $Z_{1,4}$; $Z_{2,1}$; $Z_{2,2}$; $Z_{2,3}$; $Z_{3,1}$ i $Z_{3,2}$). W wyniku zaistnienia sprzyjających warunków sześć zagrożeń zmaterializowało się[86] ($Z_{1,4}$; $Z_{2,1}$; $Z_{2,1}$; $Z_{2,2}$; $Z_{2,3}$ i $Z_{3,1}$). Materializacja zagrożenia $Z_{1,4}$ [87] wywołała negatywne skutki dla funkcjonalności IK V_1 określone w tab. 2.2a.

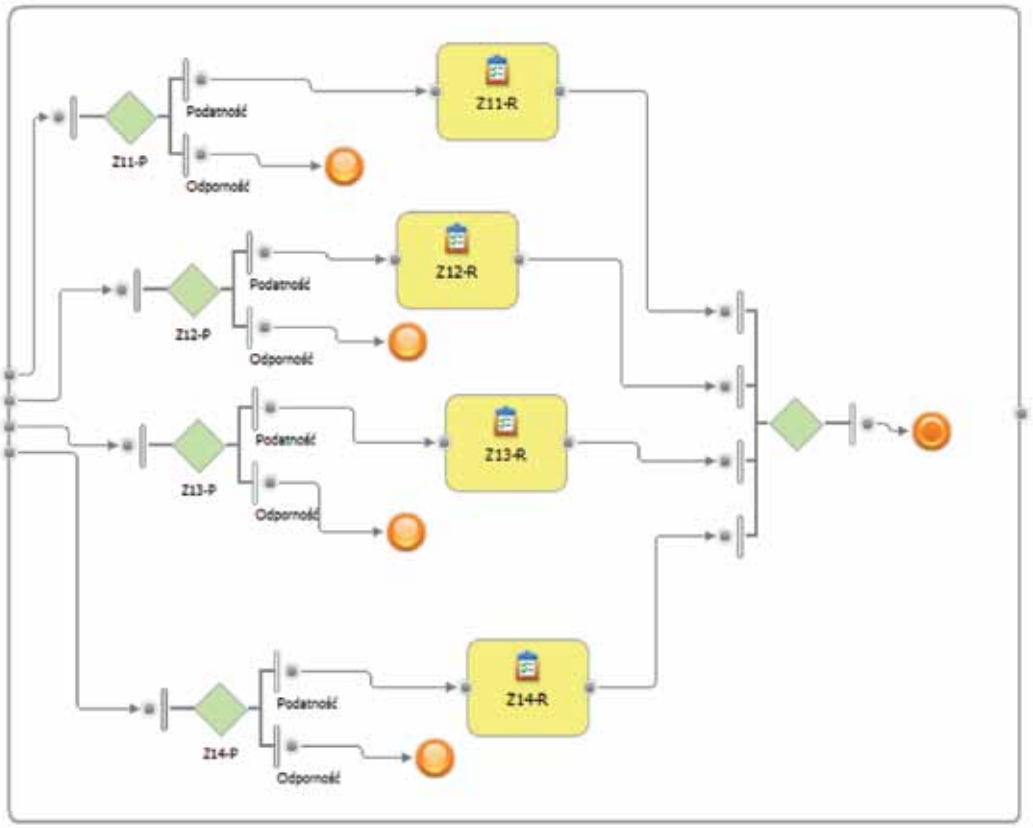
[85] Narzędziem zastosowanym do przeprowadzenia symulacji SZN jest IBM Websphere Business Modeler 7.0.

[86] O tym, czy zagrożenie zmaterializowało się, decyduje prawdopodobieństwo wystąpienia zagrożenia $Z_{\alpha,\beta}$.

[87] O tym, czy zagrożenie wywoła negatywne skutki dla zasobu, decyduje podatność zasobu V_{α} na zagrożenie $Z_{\alpha,\beta}$.



Rysunek 2.4b. Przykład implementacji SPIK przedstawionego na rys. 2.4a w narzędziu informatycznym umożliwiającym symulację SZN
Źródło: opracowanie własne.



Rysunek 2.4c. Przykład ilustrujący podatności zasobu V_1 na zagrożenia
Źródło: opracowanie własne.

Analizując SPIK (rys. 2.4a), można odtworzyć przebieg rozpatrywanego SZN nr 5. Wzbudzenie zagrożenia: $Z_{3,1}$ – susza doprowadziło do jego materializacji, co wzbudziło zagrożenia $Z_{1,2}$ – susza na terenie zajmowanym przez IK V_1 – szpital i $Z_{2,2}$ – susza na terenie zajmowanym przez IK V_2 – rafinerię naftową. Oba zagrożenia zmaterializowały się. Materializacja zagrożenia $Z_{1,2}$ nie doprowadziła do negatywnych skutków dla IK V_1 (utraty funkcjonalność), co oznacza, że zabezpieczenia zastosowane przez operatora IK V_1 okazały się skuteczne. Materializacja zagrożenia $Z_{2,2}$ nie doprowadziła do utrat funkcjonalności przez IK V_2, jednak wzbudziła zagrożenie $Z_{2,3}$ – awarię techniczną, która nie wywołała negatywnych skutków dla IK V_2, ale wzbudziła zagrożenie $Z_{2,1}$ – pożar. Materializacja zagrożenia $Z_{2,1}$ nie przyniosła negatywnych skutków dla IK V_2, jednak wzbudziła zagrożenia $Z_{3,2}$ – skażenie środowiska na terenie całego miasta, $Z_{1,3}$ – skażenie środowiska na terenie zajmowanym przez IK V_1 oraz $Z_{1,4}$ – ograniczenie personelu. Mimo zaistnienia sprzyjających warunków zagrożenia $Z_{3,2}$ i $Z_{1,3}$ nie zmaterializowały się. Zagrożenie $Z_{1,4}$ zmaterializowało się (ze względu na pożar w IK V_2 część personelu szpitala oddelegowano do obsługi potencjalnych poszkodowanych) i negatywnie wpłynęło na IK V_1 – czyli ograniczyło jej funkcjonalności:

- $\Phi_{1,1}$ – liczba miejsc na oddziale oparzeń została ograniczona o 50%,
- $\Phi_{1,2}$ – czas dostępności lądowiska dla LPR został ograniczony o 10%,
- $\Phi_{1,3}$ – o 5% ograniczona została dostępność personelu.

Przyjmując przedstawiony przebieg materializacji zagrożenia $Z_{1,4}$ oraz wykorzystując twierdzenie Bayesa, można wyznaczyć prawdopodobieństwo negatywnego wpływu tego zagrożenia na IK V_1. Według SZN nr 5 materializację zagrożenia $Z_{1,4}$ poprzedza wystąpienie czterech zagrożeń $Z_{3,1}$; $Z_{2,2}$; $Z_{2,3}$; $Z_{2,1}$. Podstawiając wartości prawdopodobieństw wystąpienia tych zagrożeń do wzoru 2.4b, uzyskuje się prawdopodobieństwo materializacji zagrożenia $Z_{1,4}$ pod warunkiem wystąpienia zagrożeń $Z_{3,1}$; $Z_{2,2}$; $Z_{2,3}$; $Z_{2,1}$[88].

$$P(Z_{1,4} | Z_{3,1}; Z_{2,2}; Z_{2,3}; Z_{2,1}) = \frac{P_{1,4} * 0{,}2}{0{,}2 * [(P_{1,4}) + (P_{3,1}) + (P_{2,2}) + (P_{2,3}) + (P_{2,1})]} = 0{,}31$$

Na podstawie SZN możliwe jest również obliczenie wartości ryzyka związanego z rozpoznanymi zagrożeniami, które ograniczają funkcjonalności rozpatrywanych IK. Przykład obliczania ryzyka dla SZN umieszczono w zał. C – część C.

2.5. Metoda formułowania problemu decyzyjnego

Podejmowanie decyzji stanowi proceduralno-technologiczną cechę procesu zarządzania [Targalski, 1986, s. 194], która wymaga sformułowania problemu decyzyjnego rozumianego jako zbiór obszarów decyzyjnych, w których należy wskazać poszukiwane rozstrzygnięcia w celu jego rozwiązania. Metoda formułowania problemu decyzyjnego opracowana dla IM-BIK jest modyfikacją metody analizy powiązanych obszarów decyzyjnych (rozdz. 1.4), której etapami są [Krupa, Ostrowska, 2012, s. 28]:

- zbudowanie modelu problemu decyzyjnego:
  - wydzielenie obszarów decyzyjnych i ich elementarnych decyzji,
  - zaznaczenie par elementarnych decyzji znajdujących się w relacji pełnej sprzeczności,
  - wyznaczenie wag względnej istotności V_i obszarów decyzyjnych D_i na skali procentowej oraz wag względnej istotności v_{ji} (kosztów do sumy równej 1 w każdym obszarze decyzyjnym D_i) elementarnych decyzji d_{ji} na skali <0, 1>;
- wygenerowanie zbioru dopuszczalnych decyzji niezawierających par elementarnych decyzji znajdujących się w relacji pełnej sprzeczności;
- dokonanie wyboru i podjęcie decyzji poprzez:
  - przeprowadzenie oceny kosztowej wszystkich poprawnie utworzonych decyzji (bez relacji sprzeczności) i uporządkowanie ich w malejącej kolejności oceny kosztowej,
  - analizę uzyskanych rozwiązań, wytypowanie grupy najbardziej pożądanych wariantów decyzji, dokonanie wyboru jednej z nich i wykonanie decyzji;
- analiza skutków podjętej (wykonanej) decyzji.

[88] Metodę sieci Bayesa można również wykorzystać do określenia odporności IK na zagrożenia [Cai, Xie, Liu, et al. 2017].

W IM-BIK problem decyzyjny jest interpretowany jako zbiór obszarów decyzyjnych wynikających z zagrożeń, na które podatna jest rozpatrywana IK, wskazanych w modelu sytuacji rozpatrywanej IK. Dlatego oznaczenia stosowane w metodzie AIDA należy dostosować do używanych w IM-BIK. Stąd:

- obszary decyzyjne są oznaczane symbolem $Z_{\alpha,\beta}$, a ich względna istotność dla problemu decyzyjnego symbolem $D_{\alpha,\beta}$,
- decyzje elementarne są oznaczane symbolem $M_{\alpha,\beta,\lambda}$, a ich względna istotność dla obszaru decyzyjnego symbolem $d_{\alpha,\beta,\lambda}$.

Przykładem problemu decyzyjnego jest sytuacja IK V_2 – rafinerii naftowej. Rafineria jest podatna na trzy zagrożenia $Z_{2,1}$ – pożar ($P_{2,1} = 0,5$; $U_{2,1} = 0,7$), $Z_{2,2}$ – suszę ($P_{2,2} = 0,4$; $U_{2,2} = 0,8$) i $Z_{2,3}$ – awarię techniczną ($P_{2,3} = 0,35$; $U_{2,3} = 0,65$). Materializacja tych zagrożeń ma negatywny wpływ na funkcjonalność $\Phi_{2,3}$ – dostępność personelu ($Z_{2,1} - \Delta\Phi_{2,3} = -30\%$; $Z_{2,2} - \Delta\Phi_{2,3} = -10\%$; $Z_{2,3} - \Delta\Phi_{2,3} = -15\%$). Obecny poziom funkcjonalności $\Phi_{2,3}$ jest równy 90%. Na potrzeby przykładu przyjmuje się, że operator IK nie stosuje żadnych zabezpieczeń dla rozpoznanych zagrożeń, a jego celem jest utrzymanie funkcjonalności $\Phi_{2,3}$ w przedziale <80%, 90%>.

Ryzyko utraty funkcjonalności (wyliczone na podstawie wzoru 2.3c) w wyniku materializacji zagrożeń $Z_{2,1}$; $Z_{2,2}$ i $Z_{2,3}$ wynosi w przybliżeniu 13,69%.

$$\sum_{\beta=1}^{3} R_{\alpha,\beta} \approx 13,69\%$$

$$R_{2,1} = \frac{0,5}{1,25} * |30\%| * 0,7 \approx 8,4\%$$

$$R_{2,2} = \frac{0,4}{1,25} * |10\%| * 0,8 \approx 2,56\%$$

$$R_{2,3} = \frac{0,35}{1,25} * |15\%| * 0,65 \approx 2,73\%$$

Wartość ryzyka związana z trzema rozpatrywanymi zagrożeniami sugeruje potencjalną dostępność funkcjonalności w wyniku materializacji zagrożeń na poziomie 76,31% (wg wzoru 2.3d). W związku z tym wszystkie trzy zagrożenia zostają zaliczone do zbioru obszarów decyzyjnych w rozpatrywanym problemie decyzyjnym.

Rozwiązanie problemu decyzyjnego polega na wskazaniu kombinacji zabezpieczeń, po jednym dla każdego obszaru decyzyjnego, realizującej przyjęty cel w jednym z trzech wariantów:

- maksymalna wartość oceny kosztowej,
- minimalna wartość oceny kosztowej,
- wartość oceny kosztowej zawiera się w przyjętym przedziale.

Cel dla problemu decyzyjnego jest określany przez operatora IK. Ze względu na kryteria przekrojowe identyfikacji IK można wskazać następujące przykłady celów podmiotów odpowiedzialnych za bezpieczeństwo IK (tab. 2.5a).

Tabela 2.5a. Wykaz możliwych celów problemów decyzyjnych w kontekście kryteriów przekrojowych

Cel	Kryterium przekrojowe	Przykład parametru opisującego decyzję elementarną
minimalizacja ofiar w ludziach	ofiary w ludziach	• wpływ zabezpieczenia na zmniejszenie liczby poszkodowanych • wpływ zabezpieczenia na zmniejszenie liczby zabitych
minimalizacja skutków finansowych	skutki finansowe	• wpływ zabezpieczenia na zmniejszenie utraconych przychodów • wpływ zabezpieczenia na zmniejszenie odszkodowań z tytułu niedostarczonych produktów/usług
minimalizacja czasu potrzebnego na ewakuację ludności	konieczność ewakuacji	• wpływ zabezpieczenia na zmniejszenie czasu potrzebnego na ewakuację ludności
utrzymanie funkcjonalności w założonym przedziale	utrata usługi	• wpływ zabezpieczenia na zwiększenie odporności IK na zagrożenie
minimalizacja czasu potrzebnego na odzyskanie funkcjonalności na założonym poziomie	czas odbudowy	• wpływ zabezpieczenia na skrócenie czasu potrzebnego na przywrócenie funkcjonalności do założonego poziomu
minimalizacja wpływu na powiązane zagraniczne IK	efekt międzynarodowy	• wpływ zabezpieczenia na zmniejszenie wpływu na powiązane zagraniczne IK
minimalizacja czasu potrzebnego na odbudowę IK	unikatowość	• wpływ zabezpieczenia na zmniejszenie czasu potrzebnego na odbudowę IK

Źródło: opracowanie własne na podstawie: NPOIK, 2015, s. 13.

Przyjęcie celu przez podmiot odpowiedzialny za bezpieczeństwo IK warunkuje parametr ilościowy, jakim będą opisywane decyzje elementarne w ramach obszarów decyzyjnych.

Ze względu na fakt, że to utrata funkcjonalności warunkuje negatywne skutki dla życia i zdrowia ludności, środowiska naturalnego oraz konsekwencje ekonomiczne dla operatora IK, przyjmuje się, że cel w obszarze bezpieczeństwa IK dotyczył utrzymania rozpatrywanej funkcjonalności powyżej założonego progu bezpieczeństwa.

Niezależnie od przyjętego celu wartości parametrów opisujących decyzje elementarne są określane na podstawie:

- wiedzy eksperckiej lub
- analizy danych statystycznych dotyczących zdarzeń z przeszłości.

W rozpatrywanym problemie decyzyjnym związanym z sytuacją IK V_2 – rafinerii naftowej, operator IK może zastosować następujące zabezpieczenia[89] dla:

- zagrożenia $Z_{2,1}$ – pożarem:
  - $M_{2,1,1}$ zakładowa straż pożarna ($m_{2,1,1} = 0{,}4$),
  - $M_{2,1,2}$ system środków gaśniczych ($m_{2,1,2} = 0{,}1$),
  - $M_{2,1,3}$ kombinezony ochronne ($m_{2,1,3} = 0{,}05$),

[89] $m_{\alpha,\beta\lambda}$ oznacza wartość podniesienia odporności rozpatrywanej IK o indeksie α na zagrożenie o indeksie β w wyniku zastosowania zabezpieczenia o indeksie λ.

- zagrożenia $Z_{2,2}$ – suszą:
  - $M_{2,2,1}$ zapas wody pitnej ($m_{2,2,1} = 0,1$),
  - $M_{2,2,2}$ dostawy wody pitnej ($m_{2,2,2} = 0,3$),
- zagrożenia $Z_{2,3}$ – awarią techniczną:
  - $M_{2,3,1}$ dział utrzymania ruchu ($m_{2,3,1} = 0,35$),
  - $M_{2,3,2}$ produkcja na innym urządzeniu ($m_{2,3,2} = 0,2$).

Istotność obszaru decyzyjnego ($D_{\alpha,\beta}$) wynika z udziału ryzyka związanego z rozpatrywanym zagrożeniem w sumie wartości ryzyk zawartych w modelu sytuacji IK[90] (2.5a):

$$D_{\alpha,\beta} = \frac{R_{\alpha,\beta}}{\sum_{\beta=1}^{j} R_{\alpha,\beta}} * 100\% \tag{2.5a}$$

gdzie:

α – indeks rozpatrywanej IK,

β – indeks zagrożenia, na które podatna jest IK,

$D_{\alpha,\beta}$ – względna istotność obszaru decyzyjnego związanego z zagrożeniem o indeksie β,

$R_{\alpha,\beta}$ – wartość ryzyka związanego z zagrożeniem o indeksie β, na które podatna jest IK, wyliczona ze wzoru 2.3b,

j – zagrożeń, na które podatna jest IK określona w modelu sytuacji rozpatrywanej IK.

Znając wartość ryzyka związanego z rozpatrywanymi zagrożeniami $Z_{2,1}$; $Z_{2,2}$ i $Z_{2,3}$ ($R_{2,1}$ – 10,5%; $R_{2,2}$ – 3,2%; $R_{2,3}$ – 3,4%), ustalono (stosując wzór 2.5a) istotność obszarów decyzyjnych względem siebie.

$$D_{2,1} = \frac{R_{2,1}}{\sum_{\beta=1}^{3} R_{\alpha,\beta}} * 100\% \approx 61$$

$$D_{2,2} = \frac{R_{2,2}}{\sum_{\beta=1}^{3} R_{\alpha,\beta}} * 100\% \approx 19$$

$$D_{2,3} = \frac{R_{2,3}}{\sum_{\beta=1}^{3} R_{\alpha,\beta}} * 100\% \approx 20$$

Decyzje elementarne $M_{\alpha,\beta,\lambda}$ dla obszarów decyzyjnych symbolizują zabezpieczenia i środki reakcji na dane zagrożenie. Parametr opisujący decyzję elementarną w IM-BIK odnosi się do zwiększenia odporności na rozpatrywane zagrożenie. Dlatego względną istotność decyzji elementarnej definiuje się jako udział wpływu rozpatrywanego zabezpieczenia w sumarycznym wpływie zabezpieczeń wskazanych dla rozpatrywanego obszaru decyzyjnego $Z_{\alpha,\beta}$, (2.5b):

[90] IM-BIK służy realizacji etapów procesu planowania cywilnego (rozpoznaniu aktualnej charakterystyki IK, przewidzeniu możliwych scenariuszy rozwoju zdarzeń niekorzystnych, podjęciu decyzji o postępowaniu z ryzykiem i zaplanowaniu działań eliminujących lub ograniczających przyszłe skutki materializacji zagrożeń), a jego zastosowanie do zarządzania dynamicznymi sytuacjami kryzysowymi ogranicza się do faz: zapobiegania i przygotowania, które są realizowane w okresie stabilizacji procesu zarzadzania kryzysowego. Zbiór zagrożeń w ramach jednego cyklu zastosowania IM-BIK nie ulega zmianie.

$$d_{\alpha,\beta,\lambda} = \frac{m_{\alpha,\beta,\lambda}}{\sum_{\lambda=1}^{1} m_{\alpha,\beta,\lambda}} \tag{2.5b}$$

gdzie:

λ – indeks zabezpieczenia,
$d_{\alpha,\beta,\lambda}$ – względna istotność decyzji elementarnej λ związanej z zagrożeniem o indeksie β, na które podatna jest IK o indeksie α,
$m_{\alpha,\beta,\lambda}$ – wartość podniesienia odporności rozpatrywanej IK o indeksie α na zagrożenie o indeksie β w wyniku zastosowania zabezpieczenia o indeksie λ,
i – liczba wszystkich dostępnych dla podmiotu odpowiedzialnego za bezpieczeństwo IK zabezpieczeń, które można zastosować w reakcji na zagrożenie o indeksie β.

Względna istotność decyzji elementarnych została obliczona (wg wzoru 2.5b) i po zaokrągleniu do dwóch miejsc po przecinku wyniosła:

$$d_{2,1,1} = \frac{m_{2,1,1}}{\sum_{\lambda=1}^{3} m_{\alpha,\beta,\lambda}} \approx 0{,}73$$

$$d_{2,1,2} = \frac{m_{2,1,2}}{\sum_{\lambda=1}^{3} m_{\alpha,\beta,\lambda}} \approx 0{,}18$$

$$d_{2,1,3} = \frac{m_{2,1,3}}{\sum_{\lambda=1}^{3} m_{\alpha,\beta,\lambda}} \approx 0{,}09$$

$$d_{2,2,1} = \frac{m_{2,2,1}}{\sum_{\lambda=1}^{2} m_{\alpha,\beta,\lambda}} \approx 0{,}25$$

$$d_{2,2,2} = \frac{m_{2,2,2}}{\sum_{\lambda=1}^{2} m_{\alpha,\beta,\lambda}} \approx 0{,}75$$

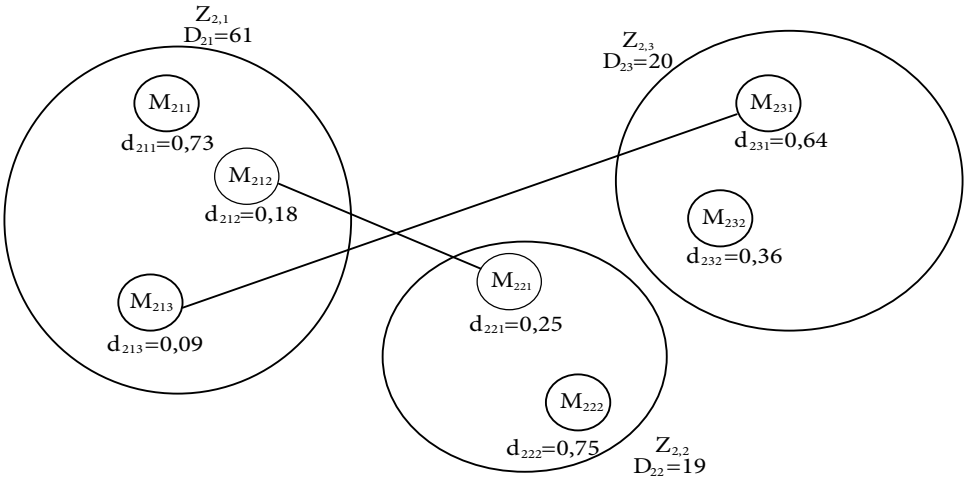
$$d_{2,3,1} = \frac{m_{2,3,1}}{\sum_{\lambda=1}^{3} m_{\alpha,\beta,\lambda}} \approx 0{,}64$$

$$d_{2,3,2} = \frac{m_{2,3,2}}{\sum_{\lambda=1}^{2} m_{\alpha,\beta,\lambda}} \approx 0{,}36$$

Sprzeczność zabezpieczeń (decyzji elementarnych) może wynikać m.in. z:
- przeszkód technicznych,
- przeszkód prawnych,
- przeszkód organizacyjnych,
- przeszkód finansowych.

Stosując założenia metody AIDA, sprzeczność decyzji elementarnych oznacza się linią ciągłą łączącą dwa elementy problemu decyzyjnego (rys. 2.5a). W rozpatrywanym problemie decyzyjnym występują sprzeczności[91]:

- $M_{2,1,2} - M_{2,2,1}$,
- $M_{2,1,3} - M_{2,3,1}$.



Rysunek 2.5a. Przykład problemu decyzyjnego sformułowanego dla sytuacji IK – rafineria
Źródło: opracowanie własne.

Rozwiązanie problemu decyzyjnego wymaga dokonania obliczeń. W tym celu problem decyzyjny można przedstawić w postaci równania macierzowego, którego rozwiązanie pozwoli wskazać zestaw zabezpieczeń realizujący przyjęty cel. Obszary decyzyjne należy zapisać w formule zbiorów. Problem decyzyjny przyjmie wówczas postać (2.5c):

$$\begin{array}{llllll} Z_{\alpha,\beta} & \{M_{\alpha,\beta,1}, & M_{\alpha,\beta,\lambda+1}, & \ldots, & M_{\alpha,\beta,i} & \} \\ Z_{\alpha,\beta+1} & \{M_{\alpha,\beta+1,1}, & M_{\alpha,\beta+1,\lambda+1}, & \ldots, & M_{\alpha,\beta+1,i} & \} \\ \ldots & \{\ldots, & \ldots, & \ldots, & \ldots & \} \\ Z_{\alpha,j} & \{M_{\alpha,j,1}, & M_{\alpha,j,\lambda+1}, & \ldots, & M_{\alpha,j,i} & \} \end{array} \quad (2.5c)$$

gdzie:

α – indeks rozpatrywanej IK,
β – indeks zagrożenia, na które podatna jest IK,
i – liczba możliwych zabezpieczeń dla rozpatrywanego zagrożenia,
j – liczba zagrożeń, na jakie podatna jest IK.

[91] Zabezpieczenie $M_{2,1,2}$ – system środków gaśniczych nie może występować razem z zabezpieczeniem $M_{2,2,1}$ – zapasem wody pitnej ze względu na możliwość skażenia wody oraz zabezpieczenie $M_{2,1,3}$ – kombinezon ochronny nie może być zastosowany razem z zabezpieczeniem $M_{2,3,1}$ – działem utrzymania ruchu, ponieważ utrudnia to wykonywanie obowiązków pracownikom tego działu.

Posiadając zapis obszarów decyzyjnych, w notacji zbiorów należy wskazać wszystkie krotki[92], jakie mogą być rozwiązaniami danego problemu decyzyjnego. Następnie ze zbioru powstałych krotek usuwa się te, które zawierają pary elementów sprzecznych. W ten sposób uzyskuje się wykaz dopuszczalnych decyzji rozwiązujących rozpatrywany problem decyzyjny.

Uzyskany zbiór krotek można zapisać w postaci macierzowej, gdzie kolumny oznaczają kolejne obszary decyzje, a wiersze dopuszczalne decyzje – kombinacje zabezpieczeń (tab. 2.5b).

Tabela 2.5b. Macierz możliwych rozwiązań problemu decyzyjnego

	$\mathbf{M}_{2,1,\lambda}$	$\mathbf{M}_{2,2,\lambda}$	$\mathbf{M}_{2,3,\lambda}$
Decyzja 1	$M_{2,1,1}$	$M_{2,2,1}$	$M_{2,3,1}$
Decyzja 2	$M_{2,1,1}$	$M_{2,2,1}$	$M_{2,3,2}$
Decyzja 3	$M_{2,1,1}$	$M_{2,2,2}$	$M_{2,3,1}$
Decyzja 4	$M_{2,1,1}$	$M_{2,2,2}$	$M_{2,3,2}$
Decyzja 5	$M_{2,1,2}$	$M_{2,2,2}$	$M_{2,3,1}$
Decyzja 6	$M_{2,1,2}$	$M_{2,2,2}$	$M_{2,3,2}$
Decyzja 7	$M_{2,1,3}$	$M_{2,2,1}$	$M_{2,3,2}$
Decyzja 8	$M_{2,1,3}$	$M_{2,2,2}$	$M_{2,3,2}$

Źródło: opracowanie własne.

Podstawiając wartości względnej istotności decyzji elementarnych $d_{\alpha,\beta,\lambda}$, w miejsce symboli zabezpieczeń $M_{\alpha,\beta,\lambda}$ tworzy się macierz wartości zabezpieczeń rozwiązujących problem decyzyjny. Mnożąc tę macierz przez macierz względnej istotności poszczególnych obszarów decyzyjnych $D_{\alpha,\beta}$, uzyskuje się ocenę kosztową poszczególnych rozwiązań problemu decyzyjnego (tab. 2.5c).

Wykorzystując ocenę kosztową rozwiązań problemu decyzyjnego, możliwe jest bezpośrednie wskazanie rozwiązania najlepszego dla celu zakładającego maksymalizację lub minimalizację przyjętego efektu. Rozwiązaniem jest decyzja o najwyższej lub najniższej ocenie kosztowej.

Ocena kosztowa rozwiązań problemu decyzyjnego nie pozwala na bezpośrednie wskazanie decyzji realizujących cel zakładający utrzymanie funkcjonalności w założonym przedziale. W tym przypadku należy uzyskane rozwiązania podstawić kolejno do wzoru na ryzyko (2.3c) i wyliczyć jego wartość, następnie oszacować dostępność funkcjonalności po materializacji rozpatrywanych zagrożeń (2.3d), co ilustruje tab. 2.5d.

[92] Krotka – rozwiązanie problemu decyzyjnego zawierające liczbę decyzji elementarnych $M_{\alpha,\beta,\lambda}$ równą liczbie obszarów decyzyjnych $Z_{\alpha,\beta}$ (po jednej decyzji elementarnej z każdego obszaru decyzyjnego). Krotki są wyznaczane na podstawie iloczynu kartezjańskiego wszystkich obszarów decyzyjnych $Z_{\alpha,\beta}$.

Tabela 2.5c. Przykład obliczenia wartości oceny kosztowej rozwiązań problemu decyzyjnego przedstawionego na rys. 2.5a

	$d_{2,1,\lambda}$	$d_{2,2,\lambda}$	$d_{2,3,\lambda}$		$D_{2,\beta}$		Ocena kosztowa
Decyzja 1	0,73	0,25	0,64		61		62,37
Decyzja 2	0,73	0,25	0,36		19		56,77
Decyzja 3	0,73	0,75	0,64		20		71,81
Decyzja 4	0,73	0,75	0,36	*		=	66,27
Decyzja 5	0,18	0,75	0,64				38,10
Decyzja 6	0,18	0,75	0,36				32,50
Decyzja 7	0,09	0,25	0,36				17,48
Decyzja 8	0,09	0,75	0,36				26,98

Źródło: opracowanie własne.

Tabela 2.5d. Zestawienie wartości ryzyka utraty funkcjonalności i wartości funkcjonalności dla rozwiązań problemu decyzyjnego przedstawionego na rys. 2.5a

Decyzja	Ocena kosztowa	Wartość ryzyka	Wartość funkcjonalności
1	62,37	7,1%	82,9%
2	56,77	7,73%	82,27%
3	**71,81**	**6,46%**	**83,54%**
4	66,27	7,09%	82,91%
5	38,1	10,06%	79,94%
6	32,5	10,69%	79,31%
7	17,48	11,93%	78,07%
8	26,98	11,29%	78,71%

Źródło: opracowanie własne.

Analizując tab. 2.5d, widać, że decyzje 1, 2, 3 oraz 4 spełniają przyjęty cel operatora IK i utrzymują dostępność funkcjonalności $\Phi_{2,3}$ w założonym przedziale <80%, 90%> dostępności personelu.

Najskuteczniejszą kombinacją zabezpieczeń dla rozpatrywanego zbioru zagrożeń jest decyzja nr 3, zakładająca użycie zakładowej straży pożarnej, dostaw wody pitnej oraz utworzenie działu utrzymania ruchu w celu przeciwdziałania rozpoznanym zagrożeniom. Wdrożenie decyzji nr 3 pozwala na osiągnięcie wartości ryzyka utraty funkcjonalności $\Delta\Phi_{2,3}$ na poziomie 6,46%, co potencjalnie ogranicza rozpatrywaną funkcjonalność do poziomu 83,54%.

$$\sum_{\beta=1}^{3} R_{\alpha,\beta} \approx 6{,}46\%$$

$$R_{2,1} = \frac{0{,}5}{1{,}25} * |30\%| * (0{,}7 - 0{,}4) \approx 3{,}6\%$$

$$R_{2,2} = \frac{0{,}4}{1{,}25} * |10\%| * (0{,}8 - 0{,}3) \approx 1{,}6\%$$

$$R_{2,3} = \frac{0{,}35}{1{,}25} * |15\%| * (0{,}65 - 0{,}35) \approx 1{,}26\%$$

Metoda formułowania problemu decyzyjnego[93] została zaimplementowana w autorskim narzędziu informatycznym umożliwiającym zapisanie problemu decyzyjnego i realizującym proces obliczeniowy (zał. B).

Problem decyzyjny może być sformułowany dla SZN. Wówczas dotyczy on zagrożeń, które negatywnie wpłynęły na IK w wyniku realizacji rozpatrywanego scenariusza. W przypadku SZN problem decyzyjny może integrować wiele IK. Przykładem jest SZN nr 7 (tab. 2.5e).

Tabela 2.5e. Opisu SZN nr 7 dla zagrożenia $Z_{3,1}$ – susza

Wyszczególnienie	Sekwencja zdarzeń			Liczba przypadków	Rozkład
	Wzbudzenie	Materializacja	Skutek		
Scenariusz 7	$Z_{2,1}$-D	$Z_{2,1}$-P		1	0,10%
	$Z_{2,2}$-D	$Z_{2,2}$-P			
	$Z_{2,3}$-D	$Z_{2,3}$-P	$Z_{2,3}$-R		
	$Z_{1,2}$-D				
	$Z_{1,3}$-D				
	$Z_{1,4}$-D	$Z_{1,4}$-P	$Z_{1,4}$-R		
	$Z_{3,1}$-D	$Z_{3,1}$-P			
	$Z_{3,2}$-D				

Źródło: opracowanie własne.

Problem decyzyjny dla SZN nr 7 dotyczy dwóch zagrożeń:

- zagrożenia $Z_{1,4}$ – ograniczenie personelu ($P_{1,4}$ = 0,65; $U_{1,4}$ = 0,65), które negatywnie wpływa na IK V_1 – szpital, ograniczając jego funkcjonalności: $\Phi_{1,1}$ – oddział leczenia oparzeń ($\Delta\Phi_{1,1}$ = - 50%); $\Phi_{1,2}$ – lądowisko dla LPR ($\Delta\Phi_{1,2}$ = - 10%); $\Phi_{1,3}$ – dostępność personelu ($\Delta\Phi_{1,3}$ = - 5%),
- zagrożenia $Z_{2,3}$ – awaria techniczna ($P_{2,3}$ = 0,35; $U_{2,3}$ = 0,65), które negatywnie wpływa na IK V_2 – rafinerię, ograniczając jej funkcjonalności: $\Phi_{2,1}$ – instalacja produkcji olefin ($\Delta\Phi_{2,1}$ = - 40%); $\Phi_{2,2}$ – oczyszczanie spalin ($\Delta\Phi_{2,2}$ = - 35%); $\Phi_{2,3}$ – dostępność personelu ($\Delta\Phi_{2,3}$ = - 15%).

Formułując problem decyzyjny dla SZN, należy wziąć pod uwagę, że wspólna funkcjonalność dla rozpatrywanych IK może nie istnieć. Brak wspólnej funkcjonalności powoduje problem z wyznaczeniem wag względnej istotności dla obszarów decyzyjnych. Przykładem ilustrującym tę sytuację jest próba wyznaczenia poziomu istotności obszaru decyzyjnego $Z_{1,4}$ dla problemu decyzyjnego zakładającego utrzymanie funkcjonalności $\Phi_{2,1}$ na poziomie 85% mocy wytwórczych przy założeniu, że obecnie poziom ten wynosi 90%. Ryzyko uraty tej funkcjonalności dla SZN nr 7, wyznaczone za pomocą wzoru. 2.3c wynosi 9,1%.

[93] Procedura formułowania problemów decyzyjnych stosowana w IM-BIK wpisuje się w plany RCB reorganizacji struktury Krajowego Planu Zarządzania Kryzysowego [rcb.gov.pl/koncepcja-zmiany-krajowego-planu-zarzadzania-kryzysowego, data odczytu 27.06.2017].

$$\sum_{\beta=1}^{2} R_{\alpha,\beta} \approx 9{,}1\%$$

$$R_{1,4} = \frac{0{,}65}{1} * |0\%| * 0{,}65 \approx 0\%$$

$$R_{2,3} = \frac{0{,}35}{1} * |40\%| * 0{,}65 \approx 9{,}1\%$$

Ryzyko $R_{1,4}$ związane z zagrożeniem $Z_{1,4}$ jest zerowe, ponieważ zagrożenie to nie oddziałuje na funkcjonalność, której dotyczy cel problemu decyzyjnego. Z tego powodu poziom istotności obszaru decyzyjnego $Z_{1,4}$ wyliczony na podstawie wzoru 2.5a również będzie wynosił zero, co jest sprzeczne z sytuacją wyznaczoną przez SZN nr 7, w którym zagrożenie $Z_{1,4}$ powoduje negatywne skutki dla funkcjonalności IK V_1.

$$D_{1,4} = \frac{R_{1,4}}{\sum_{\beta=1}^{2} R_{\alpha,\beta}} = \frac{0}{14} = 0$$

Z powodu trudności z wyznaczeniem wag istotności obszarów decyzyjnych problem decyzyjny formułowany na podstawie SZN należy zdefiniować inaczej i rozumieć go jako minimalizowanie podatności SPIK na zagrożenia wykazane w SZN. Takie zdefiniowanie problemu decyzyjnego wskazuje, że istotność obszaru decyzyjnego wynika z udziału podatności IK na zagrożenie ($U'_{\alpha,\beta}$), w sumie podatności rozpatrywanych IK na zagrożenia wynikające ze SZN (2.5d):

$$D_{\alpha,\beta} = \frac{U'_{\alpha,\beta}}{\sum_{\beta=1}^{j} U'_{\alpha,\beta}} * 100\% \qquad (2.5d)$$

gdzie:

$D_{\alpha,\beta}$ – względna istotność obszaru decyzyjnego związanego z zagrożeniem o indeksie β,
$U'_{\alpha,\beta}$ – podatność IK o indeksie α na zagrożenie o indeksie β po uwzględnieniu stosowanych zabezpieczeń (podatność IK na zagrożenie Uα,β minus suma wpływu stosowanych zabezpieczeń),
α – indeks rozpatrywanej IK,
β – indeks zagrożenia, na które podatna jest rozpatrywana IK o indeksie α,
j – indeks porządkujący – liczba wszystkich zagrożeń, na które podatne są IK.

Stosując wzór 2.5d oraz przyjmując założenia dotyczące podatności IK V_1 i V_2 na zagrożenia $Z_{1,4}$ i $Z_{2,3}$, wyznaczono wagi względnej istotności obszarów decyzyjnych dla problemu decyzyjnego wynikającego ze SZN nr 7.

$$D_{1,4} = \frac{U'_{1,4}}{U'_{1,4} + U'_{2,3}} * 100 = \frac{0{,}65}{0{,}65 + 0{,}65} * 100 = 50$$

$$D_{2,3} = \frac{U'_{2,3}}{U'_{1,4} + U'_{2,3}} * 100 = \frac{0{,}65}{0{,}65 + 0{,}65} * 100 = 50$$

Pozostałe etapy realizacji metody formułowania problemu decyzyjnego na podstawie SZN nie różnią się od tych realizowanych w przypadku formułowania problemu decyzyjnego na podstawie modelu sytuacji IK.

Przykład obliczeniowy ilustrujący realizację metody formułowania problemu decyzyjnego na podstawie SZN został przedstawiony w zał. C – część D.

2.6. Wnioski z rozdziału

Analiza aktów normatywnych i planistycznych wykonana w celu zapewnienia jednolitego sposobu określania charakterystyki IK ujawniła kanon charakterystyki IK. Wykorzystując wyniki analizy oraz model sytuacji Kłykowa (2.2a), zaprojektowano model sytuacji IK (2.2b) integrujący dane dotyczące kanonu IK oraz występujących zależności między zagrożeniami i IK. Dla modelu sytuacji IK zaproponowano procedurę realizacji dla rozpatrywanej IK oraz syntetyczny opis jego podstawowych składowych (tab. 2.2a–2.2f) warunkujących możliwość wykonania metod IM-BIK: szacowania ryzyka, generowania SZN oraz formułowania problemu decyzyjnego.

W celu umożliwienia podmiotom odpowiedzialnym za bezpieczeństwo IK wnioskowania na podstawie danych zawartych w modelu sytuacji IK opracowano metodę szacowania ryzyka (rozdz. 2.3), która jest realizowana w trzech etapach pozwalających na:

- określenie wartości ryzyka utraty funkcjonalności związanej z sytuacją IK,
- wykonanie prognozy dostępności funkcjonalności w kolejnym momencie (uwzględniając ryzyko związane z zagrożeniami ujętymi w modelu sytuacji IK),
- podjęcie decyzji o postępowaniu z ryzykiem.

Metoda szacowania ryzyka dla IM-BIK wykorzystuje wzór na ryzyko, który uzależnia wartość ryzyka od:

- prawdopodobieństwa wystąpienia zagrożenia,
- podatności IK na zagrożenie,
- stosowanych zabezpieczeń,
- skutków materializacji zagrożenia dla rozpatrywanej funkcjonalności IK.

Wykorzystując model sytuacji IK, opracowano metodę generowania SZN (rozdz. 2.4), której celem jest przewidzenie możliwych następstw materializacji zagrożenia oraz weryfikacja czy model sytuacji IK uwzględnia wszystkie zagrożenia oddziałujące na IK. Metoda jest realizowana w dwóch etapach:

- opracowanie graficznego modelu SPIK,
- przygotowanie wykazu SZN.

Pierwszy etap metody wykorzystuje dane zebrane w modelach sytuacji rozpatrywanych IK do graficznego zobrazowania zmiennych losowych (prawdopodobieństwa wystąpienia zagrożenia i podatności IK na zagrożenia) oraz zależności, jakie występują między IK i zagrożeniami. W drugim etapie SPIK jest implementowany w narzędziu symulacyjnym, które wykorzystując twierdzenie Bayesa pozwala na określenie, z jakim prawdopodobieństwem zagrożenia, na które podatne są elementy SPIK, doprowadzą do ograniczenia lub utraty funkcjonaliści IK przy uwzględnieniu zależności IK i zagrożeń.

Wykorzystując metodę analizy powiązanych obszarów decyzyjnych oraz model sytuacji IK, opracowano metodę formułowania problemów decyzyjnych (rozdz. 2.5) realizowaną w czterech etapach:

- zbudowanie modelu problemu decyzyjnego,
- wygenerowanie zbioru dopuszczalnych decyzji,
- dokonanie wyboru,
- podjęcie decyzji oraz analiza skutków podjętej decyzji.

Zastosowanie metody formułowania problemu decyzyjnego pozwala podmiotom odpowiedzialnym za bezpieczeństwo IK na wskazanie obszarów decyzyjnych (zagrożeń, na które podatna jest IK), określenie decyzji elementarnych dla każdego obszaru decyzyjnego (wskazanie dostępnych zabezpieczeń lub środków reakcji na zagrożenie) oraz wyznaczenie kombinacji zabezpieczeń, które realizują przyjęty cel (utrzymują przewidywaną dostępność funkcjonalności powyżej progu bezpieczeństwa).

Rozdział 3. Metodyka zarządzania sytuacyjnego bezpieczeństwem IK

W rozdziale omówiono siedem etapów metodyki ZS-BIK określających sposób powoływania zespołu analitycznego, ustalania progów bezpieczeństwa dla funkcjonalności IK, określania sytuacji IK, generowania SZN, szacowania ryzyka, formułowania i rozwiązywania problemów decyzyjnych oraz wdrażania zabezpieczeń (rozdz. 3.1). Uzupełnieniem metodyki ZS-BIK są dwie procedury jej realizacji opracowane dla płaskich (rozdz. 3.2) i hierarchicznych (rozdz. 3.3) problemów decyzyjnych.

3.1. Charakterystyka etapów metodyki ZS-BIK

W wyniku przeprowadzonej analizy stosowanych metodyk oceny ryzyka na potrzeby zarządzania kryzysowego (rozdz. 1.2) wskazano siedem etapów metodyki ZS-BIK:

- powołanie zespołu – etap, w ramach którego wskazywani są członkowie zespołu analitycznego, którzy dobierani są na podstawie charakterystyki rozpatrywanej IK oraz obowiązujących zapisów aktów normatywnych z obszaru ochrony IK,
- określenie progów bezpieczeństwa – etap, w ramach którego określany jest próg bezpieczeństwa dla funkcjonalności charakteryzujących rozpatrywaną IK,
- odwzorowanie charakterystyk IK – etap, w ramach którego określana jest aktualna charakterystyka rozpatrywanej IK zgodnie z modelem sytuacji IK,
- wygenerowanie SZN – etap, w ramach którego generowane są SZN dla rozpoznanych zagrożeń, na które podatna jest IK, w celu uzupełnienia wiedzy zespołu analitycznego o skutkach materializacji zagrożeń,
- sformułowanie problemu decyzyjnego – etap, w ramach którego zespół analityczny formułuje problem decyzyjny dotyczący zagrożeń, na które podatna jest IK oraz zabezpieczeń, jakie można zastosować w celu osiągnięcia założonego progu bezpieczeństwa,
- szacowanie ryzyka – etap, w ramach którego zespół dokonuje oszacowania ryzyka utraty funkcjonalności związanego z aktualną sytuacją IK, pozwala to na wskazanie problemów decyzyjnych[94], jakie należy rozwiązać oraz weryfikuje, czy dodatkowe zabezpieczenia pozwolą na osiągnięcie założonego progu bezpieczeństwa IK,
- wdrożenie zabezpieczeń – etap, w ramach którego zespół analityczny przekazuje rekomendację zabezpieczeń operatorowi IK i aktualizuje charakterystykę IK.

Celem metodyki ZS-BIK jest dostarczenie podmiotom odpowiedzialnym za bezpieczeństwo IK standardu postępowania, pozwalającego na osiągnięcie założonego progu bezpieczeństwa poprzez dobór kombinacji zabezpieczeń dla zagrożeń wynikających z sytuacji IK.

[94] Każda funkcjonalność, której prognoza według wzoru 2.3d jest poniżej wyznaczonego progu bezpieczeństwa, stanowi problem decyzyjny dla zespołu analitycznego.

Etapem rozpoczynającym działania podmiotów odpowiedzialnych za bezpieczeństwo IK w ramach metodyki ZS-BIK jest powołanie zespołu analitycznego, który zrealizuje kolejne etapy metodyki ZS-BIK. Etap ten jest wykonywany w dwóch krokach:

- analiza interesariuszy rozpatrywanej IK i dobór członków zespołu,
- weryfikacja matrycy kompetencji zespołu analitycznego.

Ustawa o zarządzaniu kryzysowym wskazuje, że operatorzy IK muszą posiadać, stosowny do przewidywanych zagrożeń, plan ochrony infrastruktury krytycznej (POIK) [Dz.U. 2017 poz. 209, art. 6, pkt 5]. Opracowanie POIK wymaga powołania zespołu, który będzie miał możliwe szeroką wiedzę na tematy:

- funkcjonalności realizowanych przez IK,
- zasobów niezbędnych do realizacji funkcjonalności IK,
- zagrożeń, na które podatne są zasoby IK,
- możliwych do zastosowania zabezpieczeń eliminujących lub ograniczających skutki zagrożeń dla IK,
- wpływu IK na jednostki uzależnione od funkcjonalności rozpatrywanej IK.

Bezpośrednim beneficjentem metodyki ZS-BIK są operatorzy IK i to ich przedstawiciele stanowią głównych interesariuszy, którzy tworzą zespół analityczny (interesariusze wewnętrzni). Wykaz interesariuszy wewnętrznych w metodyce ZS-BIK wynika z charakterystyki IK i jest związany z:

- funkcjonalnościami IK,
- zasobami realizującymi funkcjonalności IK.

Uzależnienie wykazu interesariuszy wewnętrznych od wykazu funkcjonalności IK pozwala na określenie zasobów niezbędnych do ich realizacji. Wiedza o zasobach pozwala na wskazanie osób znających specyfikę ich funkcjonowania, potrafiących określić, na jakie zagrożenia są podatne[95] oraz wskazać możliwe zabezpieczenia eliminujące lub ograniczające skutki zagrożeń.

IK funkcjonują w ramach społeczności reprezentowanych przez organy administracji publicznej oraz służby powołane do niesienia pomocy. Zarówno przedstawiciele organów administracji publicznej, jak i służb powołanych do niesienia pomocy powinni stanowić część składu zespołu analitycznego (interesariusze zewnętrzni). Ich udział pozwoli na szersze spojrzenie zespołu zarówno na zagrożenia, jakie mogą mieć wpływ na rozpatrywaną IK, jak i na skutki materializacji zagrożeń dla społeczności, w ramach której funkcjonuje IK.

Wykaz organów administracji publicznej i służb powołanych do niesienia pomocy, których przedstawiciele powinni być zaangażowani w opracowanie POIK, określa Rozporządzenie Rady Ministrów w sprawie w planów ochrony infrastruktury krytycznej [Dz.U. 2010 nr 83 poz. 542, § 4], są to:

- w zakresie właściwym terytorialnie:
  - wojewoda,
  - komendant wojewódzki Państwowej Straży Pożarnej,
  - komendant wojewódzki policji,
  - dyrektor regionalnego zarządu gospodarki wodnej,

[95] Określenie podatności na zagrożenia odbywa się na podstawie doświadczeń własnych interesariuszy lub danych historycznych dotyczących incydentów z przeszłości.

  - wojewódzki inspektorat nadzoru budowlanego,
  - wojewódzki lekarz weterynarii,
  - państwowy wojewódzki inspektorat sanitarny,
  - dyrektor urzędu morskiego,
- minister lub kierownik urzędu centralnego, we właściwości którego znajduje się system, do którego została zaliczona rozpatrywana IK.

Podmiotem administracji publicznej uzupełniającym wykaz interesariuszy zewnętrznych, który wskazuje ustawa o szczególnych uprawnieniach ministra właściwego do spraw Skarbu Państwa, jest pełnomocnik do spraw ochrony infrastruktury krytycznej, do którego zadań należy m.in. [Dz.U. 2010 Nr 65 poz. 404, art. 5, pkt 2]:

- monitorowanie działalności spółki w zakresie ochrony IK,
- przekazywanie informacji o IK dyrektorowi RCB,
- odbieranie informacji o zagrożeniach dla IK we współpracy z dyrektorem RCB.

Udział pełnomocnika do spraw ochrony IK w zespole analitycznym zapewni wymianę informacji o zagrożeniach, na które podatne są IK między operatorami IK. Pełnomocnik przekazując RCB informacje o ustalonych w ramach prac zespołu analitycznego zagrożeniach i zależnościach IK, poszerza bazę wiedzy, którą mogą wykorzystać zespoły pracujące w ramach innych IK. Mechanizm ten zapewnia wymianę doświadczeń dotyczących wpływu IK na jednostki zależne.

Rolą zespołu analitycznego jest określenie aktualnej charakterystyki IK, zgodnie z modelem sytuacji IK, przyjęcie wartości progów bezpieczeństwa dla realizowanych funkcjonalności IK, oszacowanie ryzyka utraty funkcjonalności wynikającego z sytuacji IK oraz, jeśli to konieczne, podjęcie decyzji zmierzających do wyznaczenia dodatkowych zabezpieczeń IK, pozwalających na osiągnięcie założonego progu bezpieczeństwa. Realizacja tego zadania wymaga, aby zespół analityczny posiadał właściwe kompetencje[96]. Ich kompletność pozwala zweryfikować matryca kompetencji (tab. 3.1a).

Tabela 3.1a. Matryca kompetencji zespołu analitycznego

Wyszczególnienie		**Interesariusze zewnętrzni**				**Interesariusze wewnętrzni**		
						V_α		
Zagrożenia	Obszary ochrony IK	Przedstawiciel wojewody	Przedstawiciel komendanta wojewódzkiego PSP	Przedstawiciel komendanta wojewódzkiego policji	…	Osoba 1	…	Osoba n
$Z_{\alpha,\beta}$	bezpieczeństwo fizyczne			+		+	…	
	bezpieczeństwo techniczne		+				…	+
	bezpieczeństwo osobowe	+				+	…	+
	bezpieczeństwo teleinformatyczne			+			…	
	bezpieczeństwo prawne	+					…	
	ciągłość działania					+	…	+

Źródło: opracowanie własne.

[96] Kompetencje to ogół wiedzy, umiejętności, doświadczeń, postaw i gotowości pracownika do działania w danych warunkach [Glinkowska, 2012, s. 127].

W wierszach matrycy (tab. 3.1a) przedstawione są wymagane kompetencje zespołu analitycznego wyznaczone na podstawie zagrożeń, na które podatna jest rozpatrywana IK[97]. Weryfikowane są kompetencje członków zespołu dotyczące znajomości środków eliminujących lub ograniczających skutki zagrożeń, na które podatna jest IK w obszarach ochrony IK wskazanych w NPOIK [NPOIK, 2015, zał. 1, s. 5]. Natomiast kolumny zawierają wykaz przedstawicieli interesariuszy zewnętrznych i wewnętrznych.

Każdy z przedstawicieli interesariuszy ma wiedzę w zakresie jednego lub kilku obszarów ochrony IK związanych z określonymi zagrożeniami i jest w stanie wskazać dla nich zabezpieczenia. Ważnym jest, aby przed przystąpieniem zespołu do pracy sprawdzić czy każde zagrożenie ma wskazaną osobę o potwierdzonych kompetencjach w rozpatrywanym obszarze ochrony IK. W przypadku stwierdzenia braku kompetencji zespołu konieczne jest poszerzenie składu zespołu o osoby z wymaganymi kompetencjami. Syntetycznie etap powołania zespołu podsumowuje tab. 3.1b.

Tabela 3.1b. Charakterystyka etapu metodyki ZS-BIK – powołanie zespołu

Nazwa etapu	Powołanie zespołu		
Cel etapu	**Stosowane narzędzia**	**Dane wejściowe**	**Dane wyjściowe**
Wskazanie składu osobowego zespołu analitycznego odpowiedzialnego za bezpieczeństwo IK	Model sytuacji IK Matryca kompetencji	Charakterystyka IK Wykaz interesariuszy IK	Skład personalny zespołu analitycznego
Postępowanie	• analiza interesariuszy rozpatrywanej IK i dobór członków zespołu • weryfikacja matrycy kompetencji zespołu analitycznego		

Źródło: opracowanie własne.

W metodyce ZS-BIK próg bezpieczeństwa jest definiowany jako poziom funkcjonalności uznany przez operatora IK za wystarczający do realizacji zadań IK wynikających z zobowiązań wobec społeczeństwa. Ustalenie progu bezpieczeństwa przez operatora IK dla funkcjonalności IK odbywa się w sposób deklaratywny, na podstawie posiadanej wiedzy dotyczącej jego zobowiązań[98]. Etap ten jest realizowany w trzech krokach:

- przyjęcie wykazu funkcjonalności IK wynikającego z modelu sytuacji IK,
- określenie progu bezpieczeństwa dla każdej funkcjonalności IK,
- zapisanie przyjętego progu bezpieczeństwa w modelu sytuacji IK.

Syntetycznie etap określenia progów bezpieczeństwa podsumowuje tab. 3.1c.

[97] W przypadku, gdy zespół analityczny w trakcie prac uzupełnia charakterystykę IK o nowe zagrożenie, jest zobowiązany również uzupełnić matrycę kompetencji i zweryfikować, czy zespół ma kompetencje w tym obszarze.

[98] Wykorzystując dane dotyczące zobowiązań właściciela IK w stosunku do odbiorców usług, możliwe jest opracowanie metody służącej wyznaczaniu progu bezpieczeństwa. Zagadnienie to wykracza jednak poza ramy niniejszego opracowania.

Tabela 3.1c. Charakterystyka etapu metodyki ZS-BIK – określenie progu bezpieczeństwa

Nazwa etapu	Określenie progu bezpieczeństwa		
Cel etapu	**Stosowane narzędzia**	**Dane wejściowe**	**Dane wyjściowe**
Deklaratywne przyjęcie poziomów funkcjonalności gwarantujących realizację zadań rozpatrywanej IK	Model sytuacji IK	Wykaz funkcjonalności rozpatrywanej IK	Wykaz funkcjonalności rozpatrywanej IK z określonymi progami bezpieczeństwa
Postępowanie	• przyjęcie wykazu funkcjonalności IK wynikającego z modelu sytuacji IK • określenie progu bezpieczeństwa dla każdej funkcjonalności IK • zapisanie przyjętego progu bezpieczeństwa w modelu sytuacji IK		

Źródło: opracowanie własne.

Kolejnym etapem metodyki ZS-BIK jest określenie charakterystyki IK. Celem etapu jest odwzorowanie aktualnej charakterystyki IK, wykorzystując do tego model sytuacji IK. Zastosowanie modelu sytuacji IK do określenia charakterystyki IK pozwala na syntetyczne zebranie danych (zasobów, funkcjonalności, zagrożeń, zabezpieczeń) wpływających na bezpieczeństwo IK, które mogą być wymieniane między podmiotami odpowiedzialnymi za bezpieczeństwo IK. Określenie sytuacji rozpatrywanej IK w dalszych etapach metodyki ZS-BIK pozwala na:

- oszacowanie ryzyka utraty funkcjonalności, które jest zależne od sytuacji IK,
- wygenerowanie SZN,
- sformułowanie problemu decyzyjnego i wyznaczenie zbioru zabezpieczeń pozwalających na osiągnięcie przyjętego progu bezpieczeństwa.

Określenie charakterystyki IK jest realizowane w sześciu krokach szczegółowo przedstawionych w rozdz. 2.2:

- określenia zbioru V rozpatrywanych IK,
- określenia zbioru Φ funkcjonalności dla każdego elementu zbioru V,
- określenia zbioru Z zagrożeń, na które podatne są elementy zbioru V,
- określenia zbioru H zależności występujących między elementami zbioru Z,
- określenia zbioru M stosowanych zabezpieczeń dla każdego elementu zbioru Z,
- określenia zbioru G zależności występujących między elementami zbioru V.

Poszczególne elementy modelu sytuacji IK są określane przez interesariuszy na podstawie dostępnych danych lub wiedzy eksperckiej.

Syntetycznie etap odwzorowania charakterystyki IK podsumowuje tab. 3.1d.

Celem etapu szacowania ryzyka jest określenie ryzyka utraty funkcjonalności przy uwzględnieniu zmiennych określających: prawdopodobieństwo występowania zagrożeń, skutków materializacji zagrożeń dla funkcjonalności IK, podatności IK na zagrożenia oraz wpływu stosowanych zabezpieczeń na odporność IK. Określenie ryzyka utraty funkcjonalności pozwala na wskazanie problemów decyzyjnych[99], które są rozwiązywane

[99] Każda funkcjonalność, której prognozowana wartość według wzoru 2.3d jest poniżej wyznaczonego progu bezpieczeństwa, stanowi problem decyzyjny dla zespołu analitycznego.

na etapie sformułowania problemu decyzyjnego. Procedura szacowania ryzyka jest realizowana w czterech krokach szczegółowo przedstawionych w rozdz. 2.3:

- określenia wartości parametrów ryzyka na podstawie modelu sytuacji IK,
- obliczania wartości ryzyka utraty rozpatrywanej funkcjonalności IK,
- prognozy rozpatrywanej funkcjonalności w kolejnym okresie,
- podjęcia decyzji o postępowaniu z zagrożeniami.

Syntetycznie etap szacowania ryzyka podsumowuje tab. 3.1e.

Tabela 3.1d. Charakterystyka etapu metodyki ZS-BIK – odwzorowanie charakterystyki IK

Nazwa etapu	Odwzorowanie charakterystyki IK		
Cel etapu	**Stosowane narzędzia**	**Dane wejściowe**	**Dane wyjściowe**
Odwzorowanie charakterystyki rozpatrywanej IK	Model sytuacji IK	Dane dotyczące: funkcjonalności IK zasobów niezbędnych do realizacji funkcjonalności podatności zasobów na zagrożenia stosowanych zabezpieczeń	Charakterystyka sytuacji rozpatrywanej IK
Postępowanie	• określenie zbioru V rozpatrywanych IK • określenie zbioru Φ funkcjonalności dla każdego elementu zbioru V • określenie zbioru Z zagrożeń, na które podatne są elementy zbioru V • określenie zbioru H zależności występujących między elementami zbioru Z • określenie zbioru M stosowanych zabezpieczeń dla każdego elementu zbioru Z • określenie zbioru G zależności występujących między elementami zbioru V		

Źródło: opracowanie własne.

Tabela 3.1e. Charakterystyka etapu metodyki ZS-BIK – szacowanie ryzyka

Nazwa etapu	Szacowanie ryzyka		
Cel etapu	**Stosowane narzędzia**	**Dane wejściowe**	**Dane wyjściowe**
Oszacowanie ryzyka utraty funkcjonalności IK	Metoda szacowania ryzyka	Model sytuacji IK Zbiór zabezpieczeń wynikający z rozwiązania problemu decyzyjnego	Wartość ryzyka utraty funkcjonalności uwzględniający zabezpieczenia
Postępowanie	• określenie wartości parametrów ryzyka na podstawie modelu sytuacji IK • obliczanie wartości ryzyka utraty rozpatrywanej funkcjonalności IK • prognoza rozpatrywanej funkcjonalności w kolejnym okresie • podjęcie decyzji o postępowaniu z zagrożeniami		

Źródło: opracowanie własne.

Etap generowania SZN jest odpowiedzią na potrzeby podmiotów odpowiedzialnych za bezpieczeństwo IK wskazaną w aktach normatywnych UE i Polski[100]. Celem tego

[100] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii Dz.U.UE. 2016 nr 194 poz. 1, s.7; Dyrektywa Rady 2008/114/WE z dnia 8 grudnia 2008 r. w sprawie rozpoznawania

etapu jest rozpoznanie możliwych scenariuszy zdarzeń niekorzystnych. Wiedza ta pozwala na weryfikację czy przyjęte założenia dotyczące skutków materializacji zagrożeń są prawidłowo oszacowane. Dodatkowo analiza uzyskanych SZN umożliwia sprawdzenie, czy w trakcie prac zespołu nie pominięto zagrożeń, ograniczając tym samym możliwość zabezpieczenia się przed nimi. Etap ten nie jest wymagany do zachowania ciągłości wnioskowania w ramach metodyki ZS-BIK, co obrazuje procedura realizacji metodyki dla płaskich problemów decyzyjnych (rozdz. 3.2).

Etap generowania SZN jest realizowany w dwóch krokach szczegółowo przedstawionych w rozdz. 2.4:

- opracowania SPIK na podstawie danych zawartych w modelach sytuacji IK,
- przygotowania wykazu SZN.

Syntetycznie etap generowania SZN podsumowuje tab. 3.1f.

Tabela 3.1f. Charakterystyka etapu metodyki ZS-BIK – wygenerowanie SZN

Nazwa etapu	Wygenerowanie SZN		
Cel etapu	**Stosowane narzędzia**	**Dane wejściowe**	**Dane wyjściowe**
Rozpoznanie możliwych scenariuszy zdarzeń niekorzystnych	Metoda generowania SZN	Modele sytuacji rozpatrywanych IK	Charakterystyka SPIK Wykaz SZN
Postępowanie	• opracowanie SPIK, na bazie danych zawartych w modelach sytuacji IK • przygotowanie wykazu SZN		

Źródło: opracowanie własne.

Dane wejściowe dla etapu formułowania problemu decyzyjnego pochodzą z modelu sytuacji IK lub SZN. Celem tego etapu jest sformułowanie problemu decyzyjnego wynikającego z sytuacji rozpatrywanej IK i wskazanie dopuszczalnych decyzji rozwiązujących ten problem. Obszary decyzyjne w ramach problemu decyzyjnego są wyznaczane przez zagrożenia, na które podatna jest IK lub w przypadku SZN przez zagrożenia, które negatywnie wpływają na rozpatrywaną IK. Decyzje elementarne w ramach obszarów decyzyjnych ilustrują możliwości zabezpieczenia się przed zagrożeniami. Oznacza to, że rozwiązanie problemu decyzyjnego dostarcza zespołowi analitycznemu wiedzy na temat zabezpieczeń, które należy zastosować w IK, aby osiągnąć wyznaczony próg bezpieczeństwa.

Procedura formułowania problemu decyzyjnego jest realizowana w czterech krokach przedstawionych w rozdz. 2.5:

- zbudowanie modelu problemu decyzyjnego,
- wygenerowanie zbioru dopuszczalnych decyzji niezawierających par elementarnych decyzji znajdujących się w relacji sprzeczności,
- dokonanie wyboru i podjęcie decyzji,
- analiza skutków podjętej decyzji.

Syntetycznie etap sformułowania problemu decyzyjnego podsumowuje tab. 3.1g.

i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie jej ochrony Dz.U.UE. 2008 nr 345 poz. 75, zał II, art. 2; Procedura opracowywania raportu cząstkowego do RZBN, ss. 10–18.

Tabela 3.1g. Charakterystyka etapu metodyki ZS-BIK – sformułowanie problemu decyzyjnego

Nazwa etapu	Sformułowanie problemu decyzyjnego		
Cel etapu	**Stosowane narzędzia**	**Dane wejściowe**	**Dane wyjściowe**
Opracowanie wykazu dopuszczalnych decyzji gwarantujących osiągnięcie wymaganego progu bezpieczeństwa dla rozpatrywanych funkcjonalności IK	Metoda formułowania problemu decyzyjnego	Modele sytuacji rozpatrywanych IK Wykaz rozpatrywanych SZN	Wykaz dopuszczalnych decyzji możliwych do zastosowania w reakcji na rozpoznane zagrożenia
Postępowanie	• zbudowanie modelu problemu decyzyjnego • wygenerowanie zbioru dopuszczalnych decyzji niezawierających par elementarnych decyzji znajdujących się w relacji sprzeczności • dokonanie wyboru i podjęcie decyzji • analiza skutków podjętej decyzji		

Źródło: opracowanie własne.

Ostatnim etapem metodyki ZS-BIK jest wdrożenie zabezpieczeń. Fizyczne wdrożenie zabezpieczeń w struktury rozpatrywanej IK jest realizowane przez operatora IK według odrębnych metod postępowania, np. za pomocą zasad zarządzania projektami. Z punktu widzenia metodyki ZS-BIK istotne jest, aby zespół analityczny uzupełnił model sytuacji rozpatrywanej IK o zabezpieczenia rekomendowane operatorowi IK, wynikające z rozwiązania problemu decyzyjnego. Pozwoli to na określenie nowej charakterystyki IK stanowiącej punkt wyjścia dla realizacji kolejnego cyklu metodyki ZS-BIK.

Syntetycznie etap wdrożenia zabezpieczeń podsumowuje tab. 3.1h.

Tabela 3.1h. Charakterystyka etapu metodyki ZS-BIK – wdrożenie zabezpieczeń

Nazwa etapu	Wdrożenie zabezpieczeń		
Cel etapu	**Stosowane narzędzia**	**Dane wejściowe**	**Dane wyjściowe**
Rekomendacja zabezpieczeń	Model sytuacji IK	Model sytuacji rozpatrywanej IK nieuwzględniający nowych zabezpieczeń	Model sytuacji rozpatrywanej IK uwzględniający nowe zabezpieczenia
Postępowanie	• rekomendacja zabezpieczeń operatorowi IK • uzupełnienie charakterystyki rozpatrywanej IK o dane dotyczące wdrożonych zabezpieczeń		

Źródło: opracowanie własne.

3.2. Zastosowanie metodyki ZS-BIK dla płaskiego problemu decyzyjnego

Płaski problem decyzyjny w metodyce ZS-BIK definiowany jest jako zbiór obszarów decyzyjnych wyznaczonych przez zagrożenia, na które podatna jest IK, których ryzyko nie pozwala na osiągnięcie założonego progu bezpieczeństwa i w stosunku do których rozstrzygnięcia zapadają na jednym poziomie decyzyjnym.

Procedurę realizacji metodyki ZS-BIK dla płaskich problemów decyzyjnych ilustruje rys. 3.2a. Natomiast tab. 3.2a zawiera opis symboli użytych na rys. 3.2a.

Tabela 3.2a. Opis elementów charakteryzujących procedurę zastosowania metodyki ZS-BIK

Symbol	Opis
	Elementy oznaczające etapy metodyki ZS-BIK, które są realizowane zgodnie z procedurą rozpatrywanego etapu przedstawioną w rozdz. 3.1.
	Czynności dodatkowe niezbędne do właściwego wykonania kolejnych etapów metodyki ZB-BIK.
	Elementy sterujące postępowaniem użytkownika w zależności od wartości weryfikowanego warunku.
	Elementy sterujące oznaczające, że jednocześnie może zostać wykonany jeden lub wiele przepływów wychodzących z elementu.
	Przepływ – element łączący czynności wykonywane w ramach procedury zastosowania metodyki ZS-BIK wskazujący sekwencję ich wykonania.
	Oznaczenie końca realizacji metodyki ZS-BIK.

Źródło: opracowanie własne.

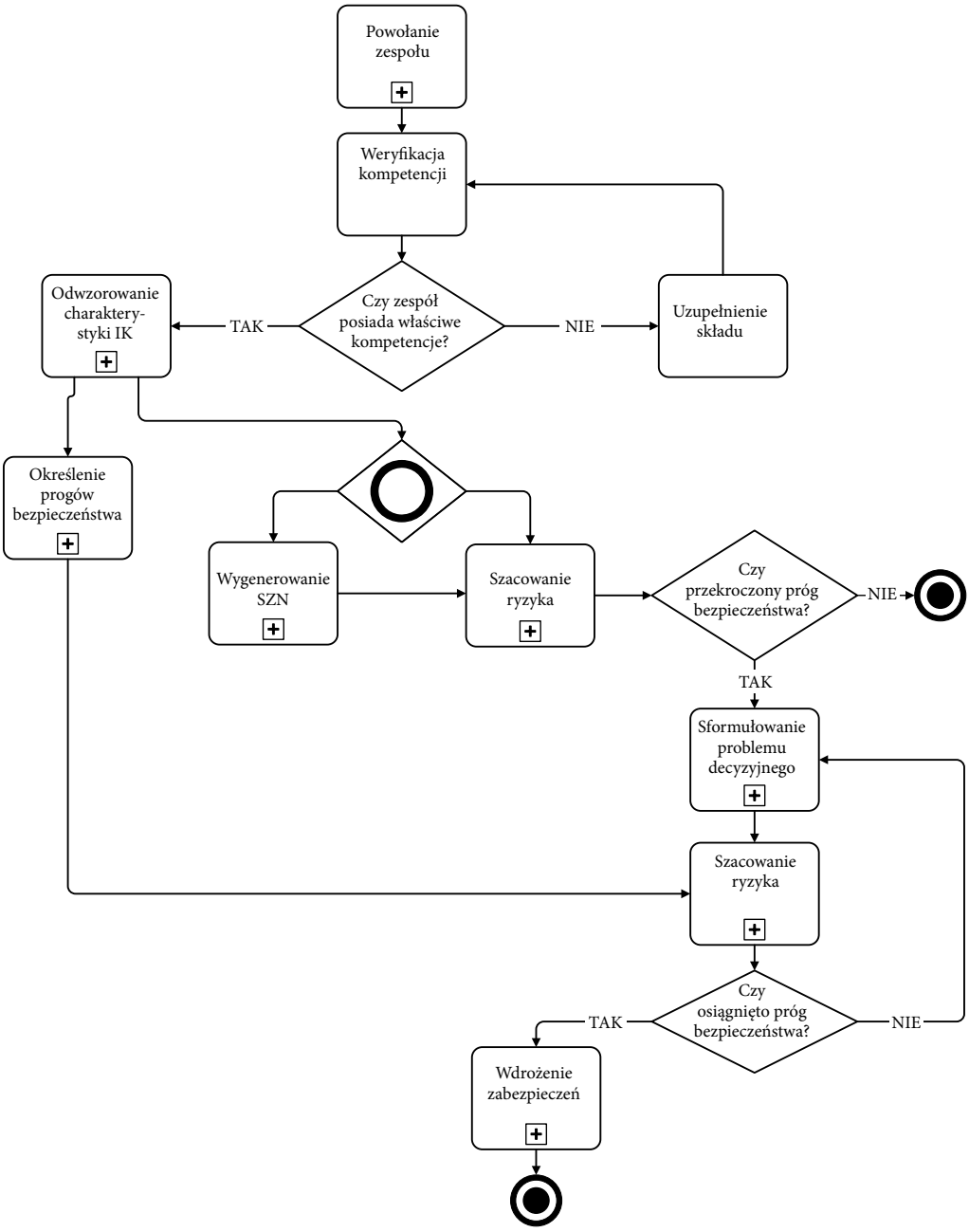
Etapem inicjującym wykonanie metodyki ZS-BIK dla płaskiego problemu decyzyjnego jest powołanie zespołu analitycznego. W wyniku realizacji tego etapu zostaje utworzona grupa ludzi o określonych kompetencjach, której zadaniem jest wykonanie charakterystyki IK, oszacowanie ryzyka utraty funkcjonalności IK i jeśli to konieczne, podjęcie działań zmierzających do wskazania zabezpieczeń pozwalających na osiągnięcie założonego progu bezpieczeństwa.

Procedura realizacji etapu powołania zespołu analitycznego umożliwia zweryfikowanie czy kompetencje zespołu są adekwatne do zagrożeń wynikających z charakterystyki IK. Weryfikacja dokonywana jest za pomocą matrycy kompetencji (tab. 3.1a). W przypadku stwierdzenia niewystarczających kompetencji zespołu analitycznego jego skład jest uzupełniany do momentu, gdy dla każdego zagrożenia, na które podatna jest IK, zostanie wskazana przynajmniej jedna osoba z wiedzą o zabezpieczeniach, które mogą zostać zastosowane przez operatora IK.

W przypadku stwierdzenia wystarczających kompetencji zespołu analitycznego realizowany jest etap odwzorowania charakterystyki IK według modelu sytuacji IK. Gdy metodyka ZS-BIK jest realizowana kolejny raz w ramach rozpatrywanej IK, następuje weryfikacja, czy dane zawarte w modelu sytuacji IK odpowiadają rzeczywistości.

Określenie charakterystyki rozpatrywanej IK umożliwia realizację dalszych etapów metodyki ZS-BIK. W szczególności określana jest wartość progu bezpieczeństwa dla funkcjonalności IK wskazanych w modelu sytuacji IK.

Po określeniu progu bezpieczeństwa dla funkcjonalności IK dokonuje się oszacowania ryzyka ich utraty związanego z zagrożeniami, na jakie podatna jest IK. W przypadku, gdy ryzyko utraty funkcjonalności IK związane z rozpatrywanymi zagrożeniami nie powoduje przekroczenia progu bezpieczeństwa, zespół analityczny może podjąć decyzję o zakończeniu prac. W przypadku przeciwnym zespół wykonuje kolejny etap metodyki ZS-BIK, tzn. formułuje problem decyzyjny.



Rysunek 3.2a. Procedura realizacji metodyki ZS-BIK dla płaskiego problemu decyzyjnego

Źródło: opracowanie własne.

Etap szacowania ryzyka może być wykonany jednocześnie z etapem opcjonalnym – wygenerowanie SZN. Jego celem jest określenie możliwych przebiegów zdarzeń niekorzystnych, które obrazują następstwa materializacji zagrożeń, na które podatna jest IK. Dla wygenerowanych SZN również szacuje się wartość ryzyka utraty funkcjonalności.

Zespół analityczny formułuje płaski problem decyzyjny w sytuacji, gdy operator IK może samodzielnie[101] podjąć decyzję o zabezpieczeniach, jakie zostaną wdrożone w reakcji na rozpatrywane zagrożenia. W rozpatrywanym problemie decyzyjnym, w postaci obszarów decyzyjnych, ujęte są wszystkie zagrożenia, których wystąpienie może doprowadzić do spadku funkcjonalności poniżej progu bezpieczeństwa. Zabezpieczenia, jakie mogą zostać zastosowane w reakcji na zagrożenia, są interpretowane jako decyzje elementarne dla obszaru decyzyjnego. Rozwiązania problemu decyzyjnego (decyzje dopuszczalne) wskazują zabezpieczenia, których zastosowanie pozwoli ograniczyć ryzyko utraty funkcjonalności.

Rozwiązanie problemu decyzyjnego skutkuje ponownym oszacowaniem ryzyka utraty funkcjonalności z uwzględnieniem dodatkowych zabezpieczeń wynikających z podjętej decyzji. W przypadku gdy rozwiązania bieżącego problemu decyzyjnego nie pozwalają na osiągnięcie progu bezpieczeństwa, zespół analityczny formułuje nowy problem decyzyjny uwzględniający wybrane rozwiązanie bieżącego problemu decyzyjnego.

W przeciwnym przypadku zespół analityczny aktualizuje model sytuacji IK o spodziewany wpływ dodatkowych zabezpieczeń na funkcjonalności IK i rekomenduje operatorowi IK wdrożenie odpowiednich zabezpieczeń.

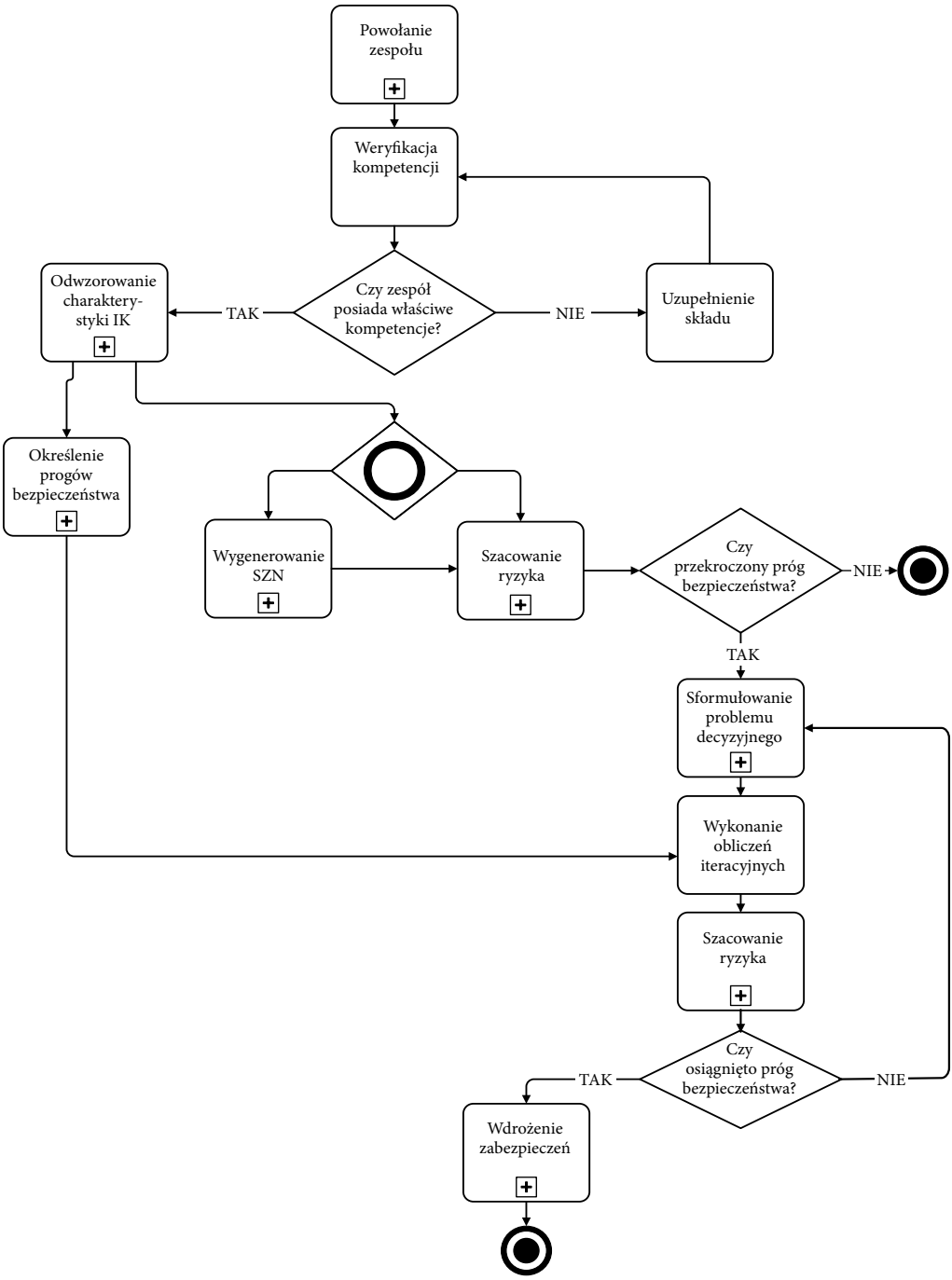
3.3. Zastosowanie metodyki ZS-BIK dla hierarchicznego problemu decyzyjnego

Hierarchiczny problem decyzyjny w metodyce ZS-BIK jest definiowany jako zbiór obszarów decyzyjnych wyznaczonych przez zagrożenia oddziałujące na IK, gdzie ryzyko nie pozwala na osiągnięcie założonego progu bezpieczeństwa, dla których rozstrzygnięcie o zastosowaniu zabezpieczeń nie zapada na jednym poziomie decyzyjnym.

Procedurę realizacji metodyki ZS-BIK dla hierarchicznych problemów decyzyjnych ilustruje rys. 3.3a. Notacja użyta do ilustracji procedury realizacji metodyki ZS-BIK dla hierarchicznego problemu decyzyjnego jest tożsama z notacją użytą w przypadku płaskiego problemu decyzyjnego (tab. 3.2a).

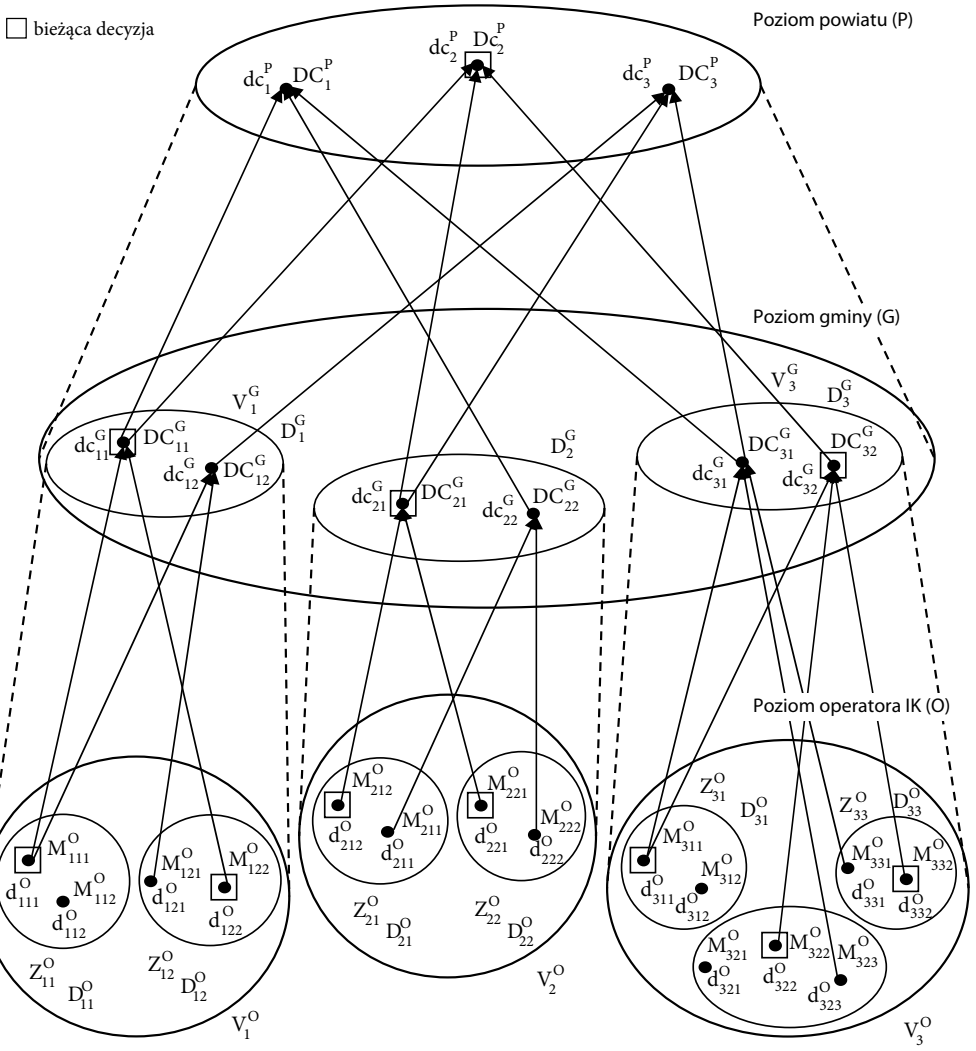
Elementem różniącym procedury realizacji metodyki ZS-BIK jest konieczność wykonania iteracyjnych obliczeń w przypadkach hierarchicznych problemów decyzyjnych.

[101] Bez konieczności dostosowywania zabezpieczeń do planów administracji publicznej lub innych operatorów IK.



Rysunek 3.3a. Procedura realizacji metodyki ZS-BIK dla hierarchicznego problemu decyzyjnego
Źródło: opracowanie własne.

Przykład hierarchicznego problemu decyzyjnego przedstawia rys. 3.3b.



Rysunek 3.3b. Przykład hierarchicznego problemu decyzyjnego

Źródło: Ostrowska, Krupa, Wiśniewski, 2015, s. 156.

Problem decyzyjny przedstawiony na rys. 3.3b dotyczy trzech poziomów decyzyjnych: powiatu (elementy z indeksem P), gminy (elementy z indeksem G) oraz operatora IK (elementy z indeksem O). Na poziomie operatora IK znajdują się trzy niezależnie funkcjonujące IK (V_α), usytułowane w obrębie jednej gminy. Każda IK jest podatna na dwa do trzech zagrożeń ($Z_{\alpha,\beta}$). W ramach każdego zidentyfikowanego zagrożenia operatorzy IK mogą zastosować od dwóch do trzech zabezpieczeń ($M_{\alpha,\beta,\lambda}$).

Rozwiązanie problemu decyzyjnego na rozpatrywanym poziomie decyzyjnym za pomocą metody formułowania problemu decyzyjnego (rozdz. 2.5) pozwala na uzyskanie pełnej listy dopuszczalnych decyzji dla tego poziomu. Uzyskane dopuszczalne decyzje stanowią zbiór decyzji elementarnych na wyższym poziomie decyzyjnym (elementy oznaczone symbolem $DC_{\alpha,n}$[102]).

W przypadku rozpatrywanego problemu decyzyjnego na poziomie gminy zostały wskazane po dwie dopuszczalne decyzje ($DC^G_{\alpha,n}$) dla każdej IK V_α, których wartości ($dc^G_{\alpha,n}$) zależą od oceny kosztowej decyzji elementarnych podjętych na poziomie operatora IK.

Na poziomie powiatu dostępne są trzy dopuszczalne decyzje (DC^P_n) dotyczące kombinacji zabezpieczeń dla wszystkich trzech IK funkcjonujących na poziomie gminy. Wartość tych decyzji (dc^P_n) zależy od oceny kosztowej decyzji elementarnych podjętych na poziomie gminy.

Złożoność obliczeniowa płaskich problemów decyzyjnych zależy od liczby obszarów decyzyjnych oraz decyzji elementarnych i jest wyrażona iloczynem tych dwóch wartości. W przypadku hierarchicznych problemów decyzyjnych poziom złożoności obliczeniowej rośnie w wyniku konieczności stosowania iteracyjnych obliczeń, spowodowanych wpływem podjętych decyzji elementarnych z poziomów niższych na rozwiązania na poziomach wyższych i odwrotnie.

Liczba oraz wartości decyzji elementarnych na poziomach decyzyjnych zależą od sumy ocen kosztowych decyzji elementarnych podjętych na niższym poziomie decyzyjnym[103]. Przykładem ilustrującym tę zależność są równania 3.3a wyznaczające wartości decyzji elementarnych dc^P_1, dc^P_2, dc^P_3 na poziomie powiatu. Składowymi decyzji DC^P_1, DC^P_2, DC^P_3 są decyzje elementarne podjęte na poziomie gminy, których wartości są określone na podstawie iloczynu wartości decyzji elementarnej ($dc^G_{\alpha,n}$) z poziomu gminy i istotności obszaru decyzyjnego (D^G_α) określonego przez władze gminy.

$$dc^P_1 = (D^G_1 \star dc^G_{11}) + (D^G_2 \star dc^G_{22}) + (D^G_3 \star dc^G_{31}) \tag{3.3a}$$

$$dc^P_2 = (D^G_1 \star dc^G_{11}) + (D^G_2 \star dc^G_{21}) + (D^G_3 \star dc^G_{32})$$

$$dc^P_3 = (D^G_1 \star dc^G_{12}) + (D^G_2 \star dc^G_{21}) + (D^G_3 \star dc^G_{31})$$

Przedstawione równania (3.3a) można zapisać w postaci macierzowej, której zastosowanie ułatwi iteracyjne obliczenia wymagane w przypadkach hierarchicznych problemów decyzyjnych (tab. 3.3a).

Tabela 3.3a. Zapis macierzowy zależności wartości decyzji elementarnych poziomu powiatu od wartości decyzji elementarnych poziomu gmin

dc^G_{11}	dc^G_{22}	dc^G_{31}		D^G_1		dc^P_1
dc^G_{11}	dc^G_{21}	dc^G_{32}	$\star$	D^G_2	=	dc^P_2
dc^G_{12}	dc^G_{21}	dc^G_{31}		D^G_3		dc^P_3

Źródło: opracowanie własne.

[102] α – indeks IK, z którą związana jest decyzja, n – indeks porządkowy (numer decyzji).

[103] Składowe poszczególnych decyzji elementarnych poziomu powiatu oraz gminy oznaczono na rys. 3.3b ciągłymi strzałkami.

Całość hierarchicznego problemu decyzyjnego przedstawionego na rys. 3.3b zapisanego w postaci równań macierzowych obrazuje tab. 3.3b. Zaczynając rozwiązywanie tego układu równań od równań odwzorowujących poziom najniższy, uzyskuje się wartości decyzji elementarnych na poziomie najwyższym, a tym samym ustala się wartość oceny kosztowej dopuszczalnych decyzji na wszystkich poziomach hierarchicznego problemu decyzyjnego.

Tabela 3.5b. Przykład zapisu macierzowego hierarchicznego problemu decyzyjnego

Zależności poziom powiatu – poziom gmin

dc^G_{11}	dc^G_{22}	dc^G_{31}	*	D^G_1	=	dc^P_1
dc^G_{11}	dc^G_{21}	dc^G_{32}		D^G_2		dc^P_2
dc^G_{12}	dc^G_{21}	dc^G_{31}		D^G_3		dc^P_3

Zależności poziom gmin – poziom operatorów IK

Problem decyzyjny V^G_1

d^O_{111}	d^O_{122}	*	D^O_{11}	=	dc^G_{11}
d^O_{111}	d^O_{121}		D^O_{12}		dc^G_{12}

Problem decyzyjny V^G_2

d^O_{212}	d^O_{221}	*	D^O_{21}	=	dc^G_{21}
d^O_{211}	d^O_{222}		D^O_{22}		dc^G_{22}

Problem decyzyjny V^G_3

d^O_{311}	d^O_{323}	d^O_{331}	*	D^O_{31}	=	dc^G_{31}
d^O_{311}	d^O_{322}	d^O_{332}		D^O_{32}		dc^G_{32}
				D^O_{33}		

Źródło: opracowanie własne.

3.4. Wnioski z rozdziału

W odpowiedzi na potrzeby podmiotów odpowiedzialnych za bezpieczeństwo IK, uwzględniając wnioski z analizy metodyk oceny ryzyka na potrzeby zarządzania kryzysowego stosowane w Polsce, USA, Kanadzie, Australii i wybranych krajach UE sformułowano siedem etapów metodyki ZS-BIK (rozdz. 3.1):

- powołanie zespołu,
- określenie progów bezpieczeństwa,
- odwzorowanie charakterystyk IK,
- wygenerowanie SZN,
- sformułowanie problemu decyzyjnego,
- szacowanie ryzyka,
- wdrożenie zabezpieczeń.

Etapy metodyki ZS-BIK są realizowane przy wykorzystaniu zaplecza narzędziowego zapewnianego przez IM-BIK. Ponadto metodykę ZS-BIK uzupełniają procedury jej realizacji dla przypadków płaskiego (rozdz. 3.2) i hierarchicznego (rozdz. 3.3) problemu decyzyjnego.

Rozdział 4. Studium wykonalności metodyki ZS-BIK

W rozdziale przedstawiono opis założeń studium wykonalności metodyki ZS-BIK (rozdz. 4.1), na podstawie których zilustrowano sposób wykonywania etapów metodyki ZS-BIK. Przykłady obliczeniowe (rozdz. 4.2 i 4.3) bazują na danych charakteryzujących rafinerię PKN ORLEN S.A. Dane pozyskano z Planu Zarządzania Kryzysowego powiatu płockiego. Wyniki przeprowadzonych obliczeń podsumowano w rozdz. 4.4.

4.1. Opis założeń studium wykonalności

Metodyka ZS-BIK wykorzystująca IM-BIK umożliwia powołanie zespołu analitycznego, którego członkowie mają niezbędne kompetencje pozwalające na:

- wyznaczenie progów bezpieczeństwa dla funkcjonalności IK,
- odwzorowanie charakterystyki rozpatrywanej IK zgodnie z modelem sytuacji IK,
- oszacowanie ryzyka utraty funkcjonalności IK,
- wygenerowanie SZN,
- sformułowanie problemu decyzyjnego i wskazanie środków reakcji na rozpoznane zagrożenia.

Weryfikowaną wartością dodaną metodyki ZS-BIK jest ciąg czynności możliwy do zastosowania przez podmiot odpowiedzialny za bezpieczeństwo IK, rozwiązujący dwa odmienne rodzaje problemów:

- płaskie problemy decyzyjne – zbiór obszarów decyzyjnych wyznaczonych przez zagrożenia, na które podatna jest IK, których ryzyko nie pozwala na osiągnięcie założonego progu bezpieczeństwa i w stosunku do których rozstrzygnięcia zapadają na jednym poziomie decyzyjnym,
- hierarchiczne problemy decyzyjne – zbiór obszarów decyzyjnych wyznaczonych przez zagrożenia, na które podatna jest IK, których ryzyko nie pozwala na osiągnięcie założonego progu bezpieczeństwa, dla których rozstrzygnięcia o zabezpieczeniach nie zapadają na jednym poziomie decyzyjnym.

Warunki zastosowania metodyki ZS-BIK zdefiniowano w procedurach jej realizacji dla przypadku płaskiego (rozdz. 3.2) i hierarchicznego (rozdz. 3.3) problemu decyzyjnego, według których przeprowadzono proces obliczeniowy.

Możliwości wykorzystania metodyki ZS-BIK dla przypadku płaskiego problemu decyzyjnego przedstawia rozdz. 4.2, w którym zaprezentowano przykład zastosowania metodyki ZS-BIK dla operatora IK odpowiedzialnego za funkcjonowanie rafinerii PKN ORLEN S.A. Możliwości wykorzystania metodyki ZS-BIK dla przypadku hierarchicznego problemu decyzyjnego przedstawiono w rozdz. 4.3, gdzie na podstawie SZN, w ramach którego występują zagrożenia oddziałujące na rafinerię PKN ORLEN S.A. oraz powiązane z nią przedsiębiorstwa, sformułowano i rozwiązano problem decyzyjny.

Dane niezbędne do realizacji etapów metodyki ZS-BIK pozyskano z planu zarządzania kryzysowego powiatu płockiego z 2015 r. Wykorzystanie rzeczywistych danych ma na celu weryfikację metodyki ZS-BIK w warunkach zbliżonych do rzeczywistych. Uzyskanie pozytywnych wyników zastosowania metodyki ZS-BIK w warunkach wyznaczonych przez PZK pozwoli na weryfikację opracowanego rozwiązania w warunkach laboratoryjnych na danych zbliżonych do rzeczywistych.

Ze względu na ograniczony dostęp do danych charakteryzujących IK, w ramach studium wykonalności zobrazowano realizację następujących etapów metodyki ZS-BIK:

- określenia charakterystyki rozpatrywanej IK,
- generowania SZN,
- formułowania problemu decyzyjnego,
- szacowania ryzyka utraty funkcjonalności,
- wdrożenia zabezpieczeń.

W ilustracji wykonania etapu generowania SZN wykorzystano środowisko symulacyjne programu IBM WebSphere Business Modeler 7.0, które pozwoliło na implementację modelu sytuacji rozpatrywanych IK oraz wygenerowanie SZN. Ponadto w ramach etapu formułowania problemu decyzyjnego wykorzystano autorskie narzędzie wspomagające proces obliczeniowy związany z metodą formułowania problemu decyzyjnego.

4.2. Przykład płaskiego problemu decyzyjnego

Przykład obliczeniowy obrazujący zastosowanie metodyki ZS-BIK dla przypadku płaskiego problemu decyzyjnego polega na odwzorowaniu sytuacji IK znajdującej się na terenie powiatu płockiego. Eksperyment przygotowano, wykorzystując dane zawarte w PZK powiatu płockiego z 2015 r. Obiektem rozpatrywanym w ramach eksperymentu, uznanym za IK[104], jest rafineria PKN ORLEN S.A.

Celem przykładu obliczeniowego jest przedstawienie sposobu wykonania etapów metodyki ZS-BIK na podstawie danych zbliżonych do rzeczywistych poprzez określenie sytuacji IK i wyznaczenie modelu zabezpieczeń na pojedynczym poziomie decyzyjnym (operatora IK). W ramach przykładu obliczeniowego zobrazowano następujące etapy metodyki ZS-BIK:

- odwzorowanie charakterystyki rozpatrywanej IK zgodnie z modelem sytuacji IK,
- wygenerowanie SZN,
- sformułowanie problemu decyzyjnego i osiągnięcie założonego progu bezpieczeństwa,
- oszacowanie wartości ryzyka utraty funkcjonalności po zastosowaniu nowych zabezpieczeń.

[104] Wystąpienie zdarzenia niekorzystnego na terenie rafinerii, np. pożaru, który nie zostanie opanowany, może skutkować znacznymi stratami finansowymi wynikającymi z uszkodzenia lub zniszczenia instalacji rafineryjnych oraz z niezrealizowania zamówień. Ponadto uwolnione w wyniku pożaru substancje chemiczne, tj. amoniak, chlor, ropa naftowa itp. mogą doprowadzić do skażenia środowiska i ewakuacji miejscowości znajdujących się w bezpośrednim sąsiedztwie rafinerii (w przypadku samego miasta Płocka jest to około 120 tys. mieszkańców). Wystąpienie pożaru na terenie rafinerii może przynieść negatywne skutki również w innych obszarach zaliczanych do kryteriów przekrojowych służących identyfikacji IK takich jak: ofiary w ludziach, utrata usługi (rafineria w Płocku o mocach przerobowych 16,3 mln t/rok jest jednym z największych zakładów przetwarzających surowce petrochemiczne na terenie Europy Środkowo-Wschodniej), czas odbudowy [Plan Zarzadzania Kryzysowego powiat płocki, 2015].

Charakterystyka IK

Rafineria PKN ORLEN S.A. położona jest na południowo-wschodnim skraju Pojezierza Dobrzyńskiego. Zajmuje obszar 1369 ha (w tym 793 ha powszechni instalacji produkcyjnych i 576 ha strefy ochronnej). Administracyjnie rafineria PKN ORLEN S.A. położona jest w granicach miasta Płocka i mieści się w jego północno – zachodniej części, w odległości ok. 5 km od centrum miasta i 1,5 km od zwartej zabudowy osiedli mieszkalnych oraz szpitala wojewódzkiego [Plan Zarządzania Kryzysowego powiat płocki, 2015, s. 20].

Na terenie rafinerii PKN ORLEN S.A. zlokalizowane są:

- Basell Orlen Polyolefins sp. z o.o.,
- Zakład Produkcyjny ORLEN OIL sp. z o.o. w Płocku.

Zakłady te należą do grupy przedsiębiorstw, których wzajemna lokalizacja sprzyja pogłębieniu się skutków zdarzeń niekorzystnych.

Ze względu na wzajemne umiejscowienie rafinerii PKN ORLEN S.A., przedsiębiorstwa Basell Orlen Polyolefins sp. z o.o. oraz Zakładu Produkcyjnego ORLEN OIL sp. z o.o. w Płocku należy przyjąć, że rozpatrywana IK jest złożona z trzech elementów oznaczonych:

- V_1 – rafineria PKN ORLEN S.A.,
- V_2 – Basell Orlen Polyolefins sp. z o.o.,
- V_3 – Zakład Produkcyjny ORLEN OIL sp. z o.o. w Płocku.

Do głównych obszarów działalności rafineria PKN ORLEN S.A. (jej podstawowych funkcjonalności) należą [Plan Zarządzania Kryzysowego powiat płocki, 2015, s. 20]:

- $\Phi_{1,1}$ – przerób ropy naftowej oraz wytwarzanie produktów i półproduktów ropopochodnych (rafineryjnych i petrochemicznych),
- $\Phi_{1,2}$ – magazynowanie, składowanie i przechowywanie ropy naftowej i paliw płynnych oraz tworzenie i utrzymywanie zapasów paliw,
- $\Phi_{1,3}$ – wytwarzanie, przesyłanie i obrót energią cieplną i elektryczną.

Z uwagi na prowadzone procesy technologiczne na terenie rafinerii PKN ORLEN S.A. istnieje możliwość powstania [Plan Zarządzania Kryzysowego powiat płocki, 2015, s. 21]:

- $Z_{1,1}$ – pożaru,
- $Z_{1,2}$ – wybuchu,
- $Z_{1,3}$ – skażenia środowiska.

Operator rafinerii PKN ORLEN S.A. w odpowiedzi na rozpoznane zagrożenia wprowadził następujące zabezpieczenia [Plan Zarządzania Kryzysowego powiat płocki, 2015, s. 21]:

- $M_{1,1,1}$ – zakładowa straż pożarna,
- $M_{1,1,2}$ – służba ochrony zakładu (ORLEN ochrona Sp. z o.o.),
- $M_{1,2,1}$ – zakładowa służba medyczna (ORLEN Medica Sp. z o.o.),
- $M_{1,3,1}$ – monitorowanie stanu środowiska.

Główną działalnością Basell Orlen Polyolefins sp. z o.o. (jego podstawową funkcjonalnością) jest [Plan Zarządzania Kryzysowego powiat płocki, 2015, s. 21]:

- $\Phi_{2,1}$ – produkcja tworzyw sztucznych typu polietylen i polipropylen.

Z uwagi na prowadzone procesy technologiczne na terenie Basell Orlen Polyolefins sp. z o.o. istnieje możliwość powstania [Plan Zarządzania Kryzysowego powiat płocki, 2015, s. 22]:

- $Z_{2,1}$ – pożaru,
- $Z_{2,2}$ – wybuchu,
- $Z_{2,3}$ – skażenia środowiska.

Operator Basell Orlen Polyolefins sp. z o.o. w odpowiedzi na rozpoznane zagrożenia wprowadził następujące zabezpieczenia [Plan Zarządzania Kryzysowego powiat płocki, 2015, s. 22]:

- $M_{2,1,1}$ – zakładowa straż pożarna,
- $M_{2,1,2}$ – służba ochrony zakładu (ORLEN ochrona Sp. z o.o.),
- $M_{2,2,1}$ – zakładowa służba medyczna (ORLEN Medica Sp. z o.o.),
- $M_{2,3,1}$ – monitorowanie stanu środowiska.

Do głównych obszarów działalności Zakładu Produkcyjnego ORLEN OIL Sp. z o.o. w Płocku (jego podstawowych funkcjonalności) należą [Plan Zarządzania Kryzysowego powiat płocki, 2015, s. 22]:

- $\Phi_{3,1}$ – produkcja olejów bazowych,
- $\Phi_{3,2}$ – produkcja gaczy parafinowych,
- $\Phi_{3,3}$ – produkcja ekstraktu furfurolowego.

Z uwagi na prowadzone procesy technologiczne na terenie Zakładu Produkcyjnego ORLEN OIL Sp. z o.o. w Płocku istnieje możliwość powstania [Plan Zarządzania Kryzysowego powiat płocki, 2015, s. 22]:

- $Z_{3,1}$ – pożaru,
- $Z_{3,2}$ – wybuchu,
- $Z_{3,3}$ – skażenia środowiska.

Operator Zakładu Produkcyjnego ORLEN OIL Sp. z o.o. w Płocku w odpowiedzi na rozpoznane zagrożenia wprowadził następujące zabezpieczenia [Plan Zarządzania Kryzysowego powiat płocki, 2015, s. 22]:

- $M_{3,1,1}$ – zakładowa straż pożarna,
- $M_{3,1,2}$ – służba ochrony zakładu (ORLEN ochrona Sp. z o.o),
- $M_{3,2,1}$ – zakładowa służba medyczna (ORLEN Medica Sp. z o.o.),
- $M_{3,3,1}$ – monitorowanie stanu środowiska.

W tab. 4.2a zdefiniowano zależności rozpatrywanych IK, które zilustrowano na rys. 4.2a.

Ze względu na wykorzystanie w PZK powiatu płockiego danych jakościowych określających wartość ryzyka związanego ze wskazanymi zagrożeniami oraz brak kryteriów wyznaczania oceny ryzyka, wartości ilościowe dotyczące prawdopodobieństwa wystąpienia zagrożeń, skutków ich wystąpienia oraz podatności rozpatrywanych IK zostały ustalone losowo[105] na przedziale zamkniętym od 0 do 100%. Natomiast poziom wykorzystania potencjału produkcyjnego (funkcjonalności) rozpatrywanych IK wynosi 93%[106].

Sytuacja rozpatrywanej IK została przedstawiona syntetycznie w tab. 4.2b.

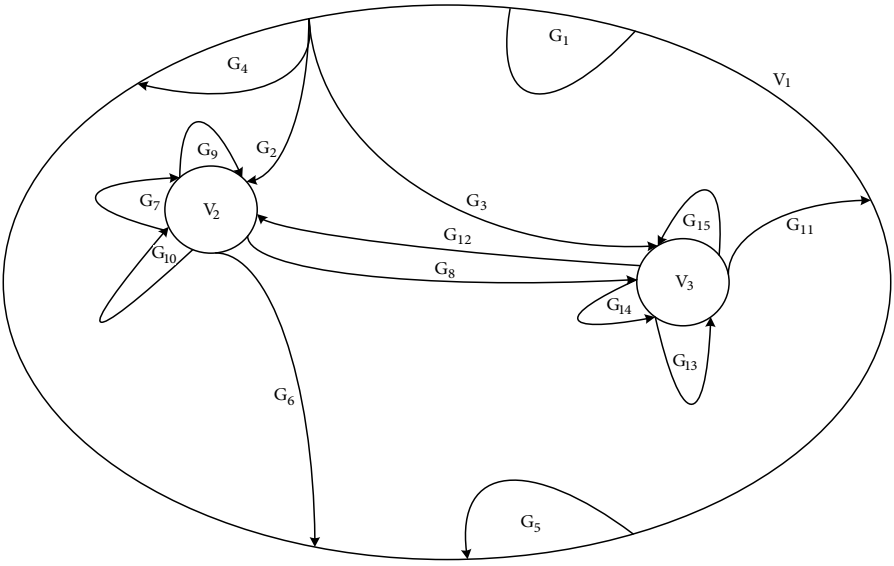
[105] Wykorzystanie losowych danych ilościowych nie wpływa na sposób realizacji metodyki ZS-BIK.

[106] Wynik ustalony na podstawie raportu Grupy Orlen z 2016 r. [Orlen, 2016, s. 295].

Tabela 4.2a. Syntetyczny zapis zależności pomiędzy rafinerią PKN ORLEN S.A., Basell Orlen Polyolefins sp. z o.o. oraz Zakładem Produkcyjnym ORLEN OIL sp. z o.o. w Płocku

Symbol zasobu:	**V_1**	
Symbol zależności	**Zasób zależny**	**Zagrożenie wpływające**
G_1	V_1	Pożar
G_2	V_2	
G_3	V_3	
G_4	V_1	Wybuch
G_5	V_1	Skażenie środowiska
Symbol zasobu:	**V_2**	
Symbol zależności	**Zasób zależny**	**Zagrożenie wpływające**
G_6	V_1	Pożar
G_7	V_2	
G_8	V_3	
G_9	V_2	Wybuch
G_{10}	V_2	Skażenie środowiska
Symbol zasobu:	**V_3**	
Symbol zależności	**Zasób zależny**	**Zagrożenie wpływające**
G_{11}	V_1	Pożar
G_{12}	V_2	
G_{13}	V_3	
G_{14}	V_3	Wybuch
G_{15}	V_3	Skażenie środowiska

Źródło: opracowanie własne.



Rysunek 4.2a. Graficzna ilustracja zależności rafinerii PKN ORLEN S.A., Basell Orlen Polyolefins sp. z o.o. oraz Zakładu Produkcyjnego ORLEN OIL sp. z o.o. w Płocku

Źródło: opracowanie własne.

Tabela 4.2b. Syntetyczny zapis sytuacji rafinerii PKN ORLEN S.A., Basell Orlen Polyolefins sp. z o.o. oraz Zakładu Produkcyjnego ORLEN OIL sp. z o.o. w Płocku

IK	Funkcjonalności		Zagrożenia									Podatność na zagrożenie
	Symbol	Wartość	Symbol	Rodzaj	Wzbudzane zagrożenie	Prawdopodobieństwo	Ograniczenie funkcjonalności IK	Zabezpieczenie				
								Symbol	Stopień obniżenia podatności	Cel zarządzania kryzysowego	Obszar ochrony IK	
V_1	$\Phi_{1,1}$	93%	$Z_{1,1}$	IN	skażenia środowiska, wybuch	0,7	-47% ($\Phi_{1,1}$) -37% ($\Phi_{1,2}$) -13% ($\Phi_{1,3}$)	$M_{1,1,1}$	0,46	Przejmowanie kontroli	Bezpieczeństwo techniczne	0,88
								$M_{1,1,2}$	0,31	Przejmowanie kontroli	Bezpieczeństwo techniczne	
	$\Phi_{1,2}$	93%	$Z_{1,2}$	IN	pożar	0,56	-42% ($\Phi_{1,1}$) -39% ($\Phi_{1,2}$) -46% ($\Phi_{1,3}$)	$M_{1,2,1}$	0,16	Przejmowanie kontroli	Bezpieczeństwo techniczne	0,81
	$\Phi_{1,3}$	93%	$Z_{1,3}$	IN	-	0,81	-9% ($\Phi_{1,1}$) -9% ($\Phi_{1,3}$)	$M_{1,3,1}$	0,16	Zapobieganie	Bezpieczeństwo techniczne	0,31
V_2	$\Phi_{2,1}$	93%	$Z_{2,1}$	IN	skażenia środowiska, wybuch	0,42	-94% ($\Phi_{2,1}$)	$M_{2,1,1}$	0,27	Przejmowanie kontroli	Bezpieczeństwo techniczne	0,56
								$M_{2,1,2}$	0,18	Przejmowanie kontroli	Bezpieczeństwo techniczne	
			$Z_{2,2}$	IN	pożar	0,35	-48% ($\Phi_{2,1}$)	$M_{2,2,1}$	0,17	Przejmowanie kontroli	Bezpieczeństwo techniczne	0,91
			$Z_{2,3}$	IN	-	0,61	-5% ($\Phi_{2,1}$)	$M_{2,3,1}$	0,52	Zapobieganie	Bezpieczeństwo techniczne	0,82
V_3	$\Phi_{3,1}$	93%	$Z_{3,1}$	IN	skażenia środowiska, wybuch	0,58	-55% ($\Phi_{3,1}$) -34% ($\Phi_{3,2}$) -65% ($\Phi_{3,3}$)	$M_{3,1,1}$	0,05	Przejmowanie kontroli	Bezpieczeństwo techniczne	0,92
								$M_{3,1,2}$	0,75	Przejmowanie kontroli	Bezpieczeństwo techniczne	
	$\Phi_{3,2}$	93%	$Z_{3,2}$	IN	pożar	0,52	-41% ($\Phi_{3,1}$) -27% ($\Phi_{3,2}$) -38% ($\Phi_{3,3}$)	$M_{3,2,1}$	0,14	Przejmowanie kontroli	Bezpieczeństwo techniczne	0,83
	$\Phi_{3,3}$	93%	$Z_{3,3}$	IN	-	0,49	-18% ($\Phi_{3,1}$) -19% ($\Phi_{3,2}$) -15% ($\Phi_{3,3}$)	$M_{3,3,1}$	0,26	Zapobieganie	Bezpieczeństwo techniczne	0,36

Źródło: opracowanie własne.

Oszacowanie ryzyka utraty funkcjonalności IK

W tab. 4.2c przedstawiono syntetyczne zestawienie ryzyka utraty funkcjonalności rozpatrywanych IK w wyniku materializacji zagrożeń, na które są one podatne. Wartości ryzyka inherentnego i rezydualnego obliczono na podstawie wzoru 2.3b. Natomiast sumę ryzyka dla funkcjonalności realizowanych przez rozpatrywane IK obliczono, wykorzystując wzór 2.3c.

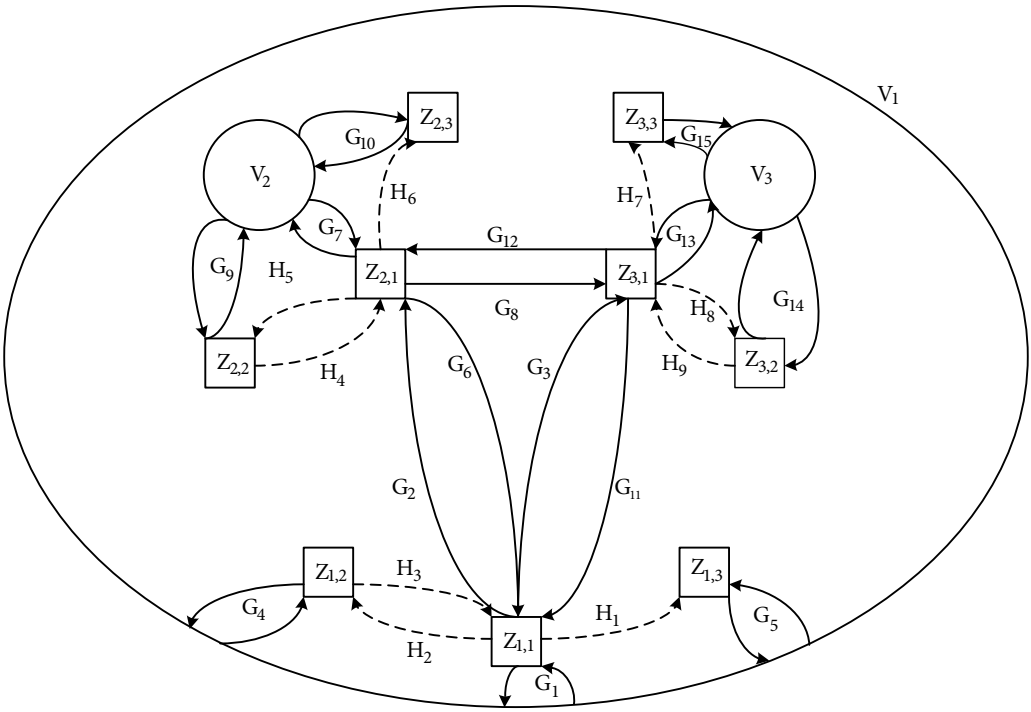
Tabela 4.2c. Syntetyczny zapis ryzyka utraty funkcjonalności dla rozpatrywanych IK

IK	Zagrożenie	Prawdopodobieństwo	Skutek		Podatność	Zabezpieczenie	Ryzyko inherentne	Ryzyko rezydualne
V_α	$Z_{\alpha,\beta}$	P	$\Phi_{\alpha,\gamma}$	$\Delta\Phi_{\alpha,\gamma}$	$U_{\alpha,\beta}$	$M_{\alpha,\beta}$	R^i	R^r
V_1	$Z_{1,1}$	0,7	Φ1,1	47%	0,88	0,77	28,95%	3,62%
			Φ1,2	37%			22,79%	2,85%
			Φ1,3	13%			8,01%	1,00%
	$Z_{1,2}$	0,56	Φ1,1	42%	0,81	0,16	19,05%	15,29%
			Φ1,2	39%			17,69%	14,20%
			Φ1,3	46%			20,87%	16,74%
	$Z_{1,3}$	0,81	Φ1,1	9%	0,31	0,16	2,26%	1,09%
			Φ1,3	9%			2,26%	1,09%
Suma ryzyka dla						Φ1,1	24,28%	9,66%
						Φ1,2	32,12%	13,53%
						Φ1,3	15,04%	9,1%
V_2	$Z_{2,1}$	0,42	Φ2,1	94%	0,56	0,45	22,11%	4,34%
	$Z_{2,2}$	0,35	Φ2,1	48%	0,91	0,17	15,29%	12,43%
	$Z_{2,3}$	0,61	Φ2,1	5%	0,82	0,52	2,50%	0,92%
Suma ryzyka dla						Φ2,2	28,91%	12,81%
V_3	$Z_{3,1}$	0,58	Φ3,1	55%	0,92	0,8	29,35%	3,83%
			Φ3,2	34%			18,14%	2,37%
			Φ3,3	65%			34,68%	4,52%
	$Z_{3,2}$	0,52	Φ3,1	41%	0,83	0,14	17,70%	14,71%
			Φ3,2	27%			11,65%	9,69%
			Φ3,3	38%			16,40%	13,63%
	$Z_{3,3}$	0,49	Φ3,1	18%	0,36	0,26	3,18%	0,88%
			Φ3,2	19%			3,35%	0,93%
			Φ3,3	15%			2,65%	0,74%
Suma ryzyka dla						Φ3,1	31,58%	12,21%
						Φ3,2	20,85%	8,16%
						Φ3,3	33,79%	11,88%

Źródło: opracowanie własne.

Wygenerowanie SZN

Na podstawie sytuacji rozpatrywanych IK (tab. 4.2a i 4.2b) opracowano schemat SPIK uwzgledniający wpływ zagrożeń na IK (rys. 4.2b).



Linie ciągłe oznaczają zależności IK, linie przerywane oznaczają zależności zagrożeń

Rysunek 4.2b. Graficzna ilustracja SPIK rafinerii PKN ORLEN S.A., Basell Orlen Polyolefins sp. z o.o. oraz Zakładu Produkcyjnego ORLEN OIL sp. z o.o. w Płocku

Źródło: opracowanie własne.

W tab. 4.2d przedstawiono syntetyczny zapis podatności składowych SPIK (rys. 4.2b) na zagrożenia, przygotowany na podstawie tab. 4.2b.

W tab. 4.2e przedstawiono syntetyczny zapis zależności zagrożeń występujących w SPIK (rys. 4.2b) przygotowany na podstawie tab. 4.2b.

Zebrane w tab. 4.2d i 4.2e dane pozwoliły na opracowanie modelu SPIK, który zaimplementowano w narzędziu informatycznym, umożliwiającym wykonanie symulacji przebiegu zdarzeń niekorzystnych (rys. 4.2c), która doprowadziła do uzyskania listy SZN (tab. D.1). Symulacja została przeprowadzona na próbie 1000 przypadków. Zagrożenia dla rafinerii PKN ORLEN S.A., Basell Orlen Polyolefins sp. z o.o. oraz Zakładu Produkcyjnego ORLEN OIL sp. z o.o. w Płocku były inicjowane losowo.

Tabela 4.2d. Opis oddziaływania zagrożeń na SPIK rafinerii PKN ORLEN S.A., Basell Orlen Polyolefins sp. z o.o. oraz Zakładu Produkcyjnego ORLEN OIL sp. z o.o. w Płocku

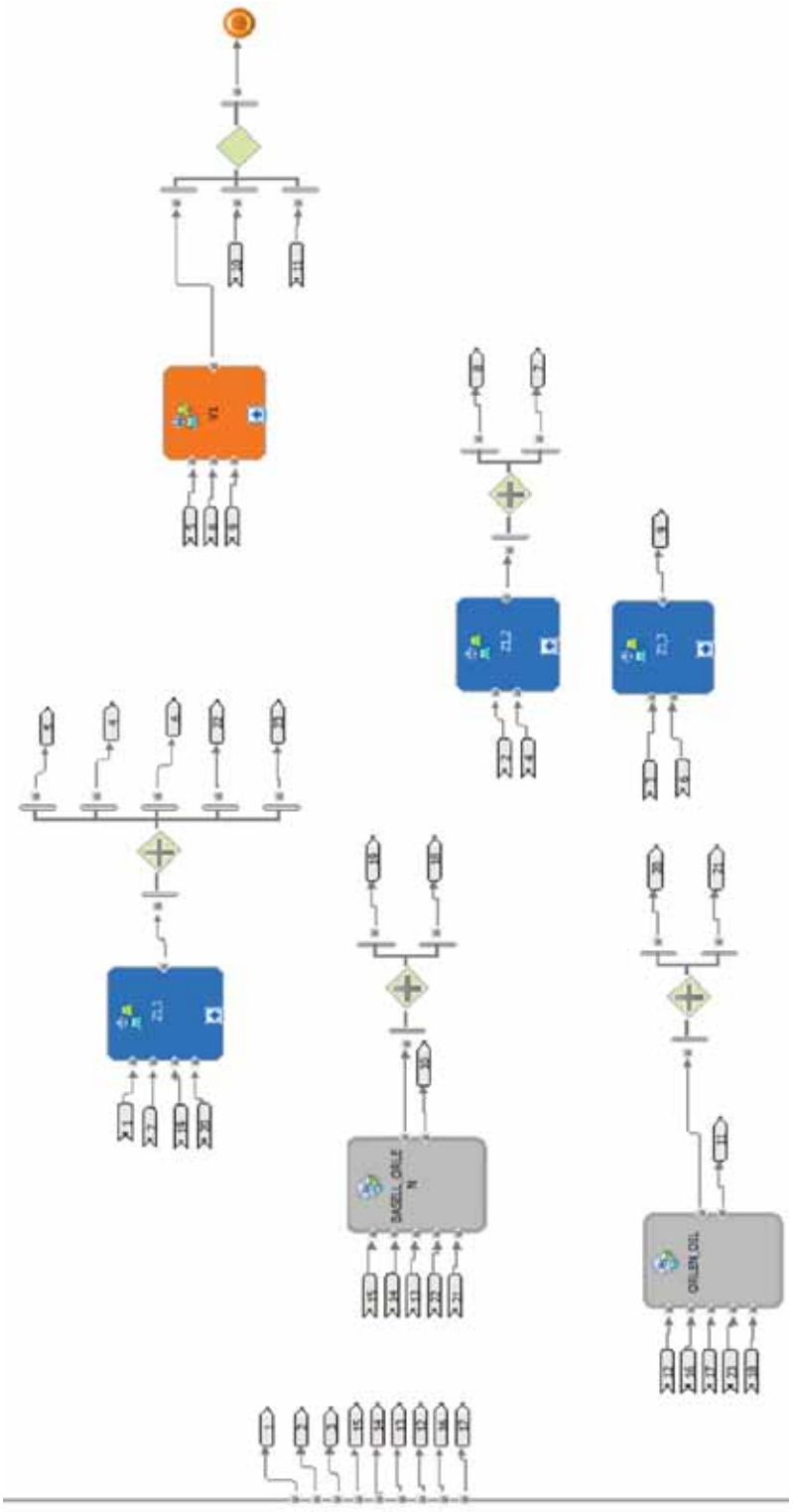
Wyszczególnienie	V_1		V_2		V_3	
	P	U	P	U	P	U
		M		M		M
$Z_{1,1}$	0,7	0,88				
		0,46+0,31				
$Z_{1,2}$	0,56	0,81				
		0,16				
$Z_{1,3}$	0,31	0,31				
		0,16				
$Z_{2,1}$			0,42	0,56		
				0,27+0,18		
$Z_{2,2}$			0,35	0,91		
				0,17		
$Z_{2,3}$			0,61	0,82		
				0,52		
$Z_{3,1}$					0,58	0,92
						0,05+0,75
$Z_{3,2}$					0,52	0,83
						0,14
$Z_{3,3}$					0,49	0,36
						0,26

Źródło: opracowanie własne.

Tabela 4.2e. Opis wzajemnego oddziaływania zagrożeń dla SPIK rafinerii PKN ORLEN S.A., Basell Orlen Polyolefins sp. z o.o. oraz Zakładu Produkcyjnego ORLEN OIL sp. z o.o. w Płocku

Zagrożenia	$Z'_{1,1}$		$Z'_{1,2}$		$Z'_{1,3}$		$Z'_{2,1}$		$Z'_{2,2}$		$Z'_{2,3}$		$Z'_{3,1}$		$Z'_{3,2}$		$Z'_{3,3}$	
$Z_{1,1}$			$P'_{1,2}$	0,56	$P'_{1,3}$	0,81	$P'_{2,1}$	0,42					$P_{3,1}$	0,58				
			$P_{1,1}$	0,7	$P_{1,1}$	0,7	$P_{1,1}$	0,7					$P_{1,1}$	0,7				
$Z_{1,2}$	$P'_{1,1}$	0,7																
	$P_{1,2}$	0,56																
$Z_{2,1}$	$P'_{1,1}$	0,7							$P'_{2,2}$	0,35	$P'_{2,3}$	0,61	$P'_{3,1}$	0,58				
	$P_{2,1}$	0,42							$P_{2,1}$	0,42	$P_{2,1}$	0,42	$P_{2,1}$	0,42				
$Z_{2,2}$							$P'_{2,1}$	0,42										
							$P_{2,2}$	0,35										
$Z_{3,1}$	$P'_{1,1}$	0,7					$P'_{2,1}$	0,42							$P'_{3,2}$	0,52	$P'_{3,3}$	0,49
	$P_{3,1}$	0,58					$P_{3,1}$	0,58							$P_{3,1}$	0,58	$P_{3,1}$	0,58
$Z_{3,2}$													$P'_{3,1}$	0,58				
													$P_{3,2}$	0,52				

Źródło: opracowanie własne.



Rysunek 4.2c. Fragment SPIK rafinerii PKN ORLEN S.A., Basell Orlen Polyolefins sp. z o.o. oraz Zakładu Produkcyjnego ORLEN OIL sp. z o.o. w Płocku zaimplementowany w IBM WebSphere Business Modeler 7.0

Źródło: opracowanie własne.

W ramach przeprowadzonego eksperymentu wygenerowano 94 SZN[107]. Łącznie SZN o negatywnym wpływie na IK doprowadziły do ograniczenia przynajmniej jednej funkcjonalności rozpatrywanej IK 316 razy, co stanowi 31,6% wszystkich badanych przypadków. Oznacza to, że w dwóch trzecich przypadków stosowane zabezpieczenia chronią IK przed zagrożeniami, na które są one podatne.

Stosując metodę Pareto, wskazano 21 SZN, które odpowiadają za przebieg 80% badanych przypadków negatywnie wpływających na IK (tab. 4.2f).

Tabela 4.2f. Wykaz SZN dla SPIK rafinerii PKN ORLEN S.A., Basell Orlen Polyolefins sp. z o.o. oraz Zakładu Produkcyjnego ORLEN OIL sp. z o.o. w Płocku agregujących 80% przypadków negatywnie wpływających na IK

Scenariusz	Liczba wystąpień	Skumulowany udział procentowy scenariusza w całkowitej liczbie badanych przypadków negatywnie wpływających na IK
Scenariusz 9	74	23%
Scenariusz 5	21	30%
Scenariusz 10	18	36%
Scenariusz 2	16	41%
Scenariusz 11	15	46%
Scenariusz 35	15	50%
Scenariusz 1	14	55%
Scenariusz 12	11	58%
Scenariusz 18	11	62%
Scenariusz 15	8	64%
Scenariusz 13	7	66%
Scenariusz 6	6	68%
Scenariusz 14	6	70%
Scenariusz 32	6	72%
Scenariusz 16	5	74%
Scenariusz 3	4	75%
Scenariusz 7	4	76%
Scenariusz 17	4	78%
Scenariusz 25	4	79%
Scenariusz 38	4	80%
Scenariusz 47	4	81%

Źródło: opracowanie własne.

Scenariusz 9 wyróżnia się pod względem liczby wystąpień. W jego ramach wzbudzonych zostało 9 zagrożeń ($Z_{1,1}$, $Z_{1,2}$, $Z_{1,3}$, $Z_{2,1}$, $Z_{2,2}$, $Z_{2,3}$, $Z_{3,1}$, $Z_{3,2}$, $Z_{3,3}$), z czego zmaterializowało się 5 zagrożeń ($Z_{1,1}$, $Z_{1,2}$, $Z_{1,3}$, $Z_{2,1}$, $Z_{3,1}$), a negatywnie na IK V_1 wpłynęło jedno zagrożenie ($Z_{1,2}$). Scenariusz ten wystąpił 74 razy.

[107] W ramach eksperymentu uzyskano 61 SZN o negatywnym wpływie na IK (tab. D.1) i 32 SZN, w których nie wystąpił negatywny wpływ na IK dla rafinerii PKN ORLEN S.A., Basell Orlen Polyolefins sp. z o.o. oraz Zakładu Produkcyjnego ORLEN OIL sp. z o.o. w Płocku. Ze względu na objętość tab. D.1 z SZN została umieszczona w zał. D.

Najwięcej zagrożeń negatywnie wpływających na badane IK wystąpiło w scenariuszu 28. W tym przypadku wzbudzonych zostało 9 zagrożeń ($Z_{1,1}$, $Z_{1,2}$, $Z_{1,3}$, $Z_{2,1}$, $Z_{2,2}$, $Z_{2,3}$, $Z_{3,1}$, $Z_{3,2}$, $Z_{3,3}$), z czego zmaterializowało się 6 zagrożeń ($Z_{1,1}$, $Z_{1,2}$, $Z_{1,3}$, $Z_{2,1}$, $Z_{3,1}$, $Z_{3,2}$), a negatywnie na IK V_1 i V_3 wpłynęły 3 zagrożenia ($Z_{1,1}$, $Z_{1,3}$, $Z_{3,2}$). Scenariusz ten wystąpił 2 razy.

Formułowanie problemu decyzyjnego

Przykładem problemu decyzyjnego, który wynika z sytuacji rozpatrywanych IK, jest niemal 10% ryzyko utraty funkcjonalności $\Phi_{1,1}$ – przerobu ropy naftowej oraz wytworzenia produktów i półproduktów ropopochodnych (tab. 4.2c). Na ryzyko utraty funkcjonalności $\Phi_{1,1}$ składają się ryzyka związane z zagrożeniami: $Z_{1,1}$ – pożarem ($R_{\Phi 1,1} = 1{,}75\%$), $Z_{1,2}$ – wybuchem ($R_{\Phi 1,1} = 7{,}39\%$) i $Z_{1,3}$ – skażeniem środowiska ($R_{\Phi 1,1} = 0{,}53\%$).

Na potrzeby przykładu obliczeniowego przyjmuje się, że celem operatora IK V_1 – rafinerii PKN ORLEN S.A, jest utrzymanie funkcjonalności $\Phi_{1,1}$ powyżej progu bezpieczeństwa wynoszącego 90%. Obecnie, przyjmując 9,66% ryzyko utraty funkcjonalności $\Phi_{1,1}$, jej dostępność w wyniku materializacji zagrożeń $Z_{1,1}$, $Z_{1,2}$ i $Z_{1,3}$ jest prognozowana (wg wzoru 2.3d) na 83,34%.

$$\Phi_{1,1}(t_1) = \Phi_{1,1}(t_0) - R_{\Phi_{1,1}}(t_0)$$

$$\Phi_{1,1}(t_1) = 93\% - 9{,}66\% = 83{,}34\%$$

Przyjęty próg bezpieczeństwa oraz wartość ryzyka związana z zagrożeniami, na które podatna jest IK V_1 wskazuje, że rozpatrywany problem decyzyjny ma trzy obszary decyzyjne[108] wyznaczone przez zagrożenia $Z_{1,1}$, $Z_{1,2}$ i $Z_{1,3}$. Wykorzystując wzór 2.5a, wyznaczono względne istotności obszarów decyzyjnych.

$$D_{1,1} = \frac{R_{1,1}}{\sum_{\beta=1}^{3} R_{1,\beta}} * 100\% = \frac{3{,}6\%}{20\%} * 100\% \approx 18$$

$$D_{1,2} = \frac{R_{1,2}}{\sum_{\beta=1}^{3} R_{1,\beta}} * 100\% = \frac{15{,}29\%}{20\%} * 100\% \approx 76$$

$$D_{1,3} = \frac{R_{1,3}}{\sum_{\beta=1}^{3} R_{1,\beta}} * 100\% = \frac{1{,}09\%}{20\%} * 100\% \approx 6$$

W celu ograniczenia ryzyka utraty funkcjonalności operator IK V_1 może zastosować dodatkowe zabezpieczenia wykorzystywane w rafinerii LOTOS S.A.[109]:

[108] Wyeliminowanie ryzyka związanego z pojedynczym zagrożeniem, np. $Z_{1,2}$ nie pozwala na osiągnięcie wymaganego progu bezpieczeństwa. Tylko ograniczenie ryzyka związanego ze wszystkimi zagrożeniami pozwoli na osiągnięcie wymaganego progu bezpieczeństwa.

[109] Zabezpieczenia zostały dobrane na podstawie rozwiązań stosowanych w rafinerii LOTOS S.A., o których informacje umieszczono w dokumencie pt. „Informacja o występujących zagrożeniach, przewidywanych skutkach tych zagrożeń, zastosowanych środkach zapobiegawczych i działaniach, które będą podjęte w przypadku wystąpienia awarii" [Lotos – Informacja o występujących zagrożeniach, data odczytu 04.04.2018].

- dla zagrożenia $Z_{1,1}$ – pożaru:
  - $M_{1,1,3}$ – okładziny ognioodporne[110] np. systemem FENDOLITE MII[111],
  - $M_{1,1,4}$ – zakup nowoczesnego sprzętu gaśniczego dla straży zakładowej, np. UEEX [UEEX, data odczytu 04.04.2018],
  - $M_{1,1,5}$ – instalacje pianowe[112];
- dla zagrożenia $Z_{1,2}$ – wybuchu:
  - $M_{1,2,2}$ – system odprowadzający opary i gazy na pochodnię gazową[113],
  - $M_{1,2,3}$ – zawory bezpieczeństwa[114] włączone w system odprowadzający opary i gazy na pochodnię gazową,
  - $M_{1,2,4}$ – urządzenia kontrolno-pomiarowe włączone w system blokad instalacji technologicznych[115],
- dla zagrożenia $Z_{1,3}$ – skażenia środowiska:
  - $M_{1,3,2}$ – monitoring parametrów technologicznych[116],
  - $M_{1,3,3}$ – monitoring stanu napełnienia zbiorników magazynowych[117],
  - $M_{1,3,4}$ – obwałowanie zbiorników[118].

---

[110] Okładziny ognioodporne – materiały stosowane w urządzeniach, instalacjach przeznaczonych do pracy w wysokiej temperaturze lub w obecności ognia.

[111] Zaprawa ogniochronna w postaci suchej mieszanki wermikulitu, cementu portlandzkiego oraz dodatków modyfikujących. Wchodzi w skład technologii stosowanej do wykonywania zabezpieczeń przeciwpożarowych przed pożarami węglowodorowymi i stanowi skuteczną ochronę stali przed szybkim przyrostem temperatury. Zastosowanie: Zabezpieczenia ogniochronne konstrukcji stalowych przed utratą nośności w pożarach węglowodorowych [Fendolite MII, data odczytu 04.04.2018].

[112] Instalacja pianowa – instalacja technologiczna rozpylająca pianę gaśniczą, która odcina dopływ powietrza do ogniska pożaru powodując jego wygasanie.

[113] Pochodnia gazowa – instalacja umożliwiająca spalenie nadmiaru gazu. Spalanie gazu w pochodniach stosuje się w dwóch przypadkach: zabezpieczenia otoczenia (lokalnego) przed skutkami niekontrolowanej migracji gazu (np. przed wybuchem, zatruciami, odorem), globalnej ochrony środowiska (przez zastąpienie emisji bardziej szkodliwych gazów palnych emisją mniej szkodliwych spalin).

[114] Zawór bezpieczeństwa – samoczynnie upuszcza czynnik w przypadku wzrostu ciśnienia powyżej ciśnienia nastawy, chroniąc zbiornik ciśnieniowy lub instalację przed rozerwaniem. Po ustabilizowaniu się ciśnienia poniżej wartości zadanej, następuje zamknięcie zaworu i zanik wypływu czynnika – zgodnie z dyrektywą ciśnieniową PED 2014/68/UE tego rodzaju zawory zalicza się do osprzętu zabezpieczającego.

[115] Instalacja technologiczna – zestaw urządzeń służących do przesyłania mediów takich jak prąd elektryczny, woda, gaz ziemny, paliwo, ścieki czy inne substancje. Na instalację składają się zwykle elementy liniowe odpowiednie do transportu danego medium takie jak rury czy przewody elektryczne oraz dodatkowe elementy służące do monitorowania i sterowania przepływem medium, tj. pompy, zawory, liczniki, bezpieczniki i inne.

[116] Monitoring parametrów technologicznych – obserwacja stanu parametrów związanych technologią wytwarzania produktów ropopochodnych w poszukiwaniu wartości zagrażających monitorowanej instalacji.

[117] Monitoring stanu napełnienia zbiorników – system czujników chroniący przed nadmiernym wypełnieniem zbiornika przechowującego produkty petrochemiczne, które może doprowadzić do jego uszkodzenia.

[118] Obwałowanie zbiornika – sposób zabezpieczenia wałami ziemnymi zbiorników przechowujących produkty petrochemiczne przed niekontrolowanym rozprzestrzenianiem powstałych wycieków.

Wśród wskazanych dodatkowych zabezpieczeń dostępnych dla operatora IK V_1 nie wskazano par sprzecznych. Oznacza to, że wymienione zabezpieczenia mogą być stosowane w dowolnej konfiguracji.

Ze względu na brak danych dotyczących skuteczności stosowanych zabezpieczeń ich wpływ na podatność IK V_1 został oszacowany losowo na skali od 0 do 1, gdzie 0 oznacza całkowity brak skuteczności zabezpieczenia, a 1 zapewnienie całkowitej odporności na zagrożenie. Wyniki szacowania umieszczono w tab. 4.2g.

Tabela 4.2g. Szacunkowy wpływ dodatkowych zabezpieczeń dostępnych dla operatora IK V_1 na podatność rozpatrywanej IK

Nazwa zabezpieczenia	**Symbol zabezpieczenia ($M_{\alpha,\beta,\lambda}$)**	**Wpływ zabezpieczenia na podatność IK na zagrożenia ($m_{\alpha,\beta,\lambda}$)**
okładziny ognioodporne	$M_{1,1,3}$	$m_{1,1,3} = 0{,}71$
nowoczesny sprzęt gaśniczy dla straży zakładowej	$M_{1,1,4}$	$m_{1,1,4} = 0{,}48$
instalacje pianowe	$M_{1,1,5}$	$m_{1,1,5} = 0{,}36$
system odprowadzający opary i gazy na pochodnię gazową	$M_{1,2,2}$	$m_{1,2,2} = 0{,}56$
zawory bezpieczeństwa	$M_{1,2,3}$	$m_{1,2,3} = 0{,}51$
urządzenia kontrolno-pomiarowe włączone w system blokad instalacji technologicznych	$M_{1,2,4}$	$m_{1,2,4} = 0{,}43$
monitoring parametrów technologicznych	$M_{1,3,2}$	$m_{1,3,2} = 0{,}13$
monitoring stanu napełnienia zbiorników magazynowych	$M_{1,3,3}$	$m_{1,3,3} = 0{,}07$
obwałowanie zbiorników	$M_{1,3,4}$	$m_{1,3,4} = 0{,}12$

Źródło: opracowanie własne.

Przyjmując wartości wpływu dodatkowych zabezpieczeń dostępnych dla operatora IK V_1, za pomocą wzoru 2.5b wyznaczono względne istotności decyzji elementarnych.

$$d_{1,1,3} = \frac{m_{1,1,3}}{\sum_{\beta=3}^{5} m_{1,\beta}} = \frac{0{,}71}{1{,}55} \approx 0{,}46$$

$$d_{1,1,4} = \frac{m_{1,1,4}}{\sum_{\beta=3}^{5} m_{1,\beta}} = \frac{0{,}48}{1{,}55} \approx 0{,}31$$

$$d_{1,1,5} = \frac{m_{1,1,5}}{\sum_{\beta=3}^{5} m_{1,\beta}} = \frac{0{,}36}{1{,}55} \approx 0{,}23$$

$$d_{1,2,2} = \frac{m_{1,2,2}}{\sum_{\beta=2}^{4} m_{1,\beta}} = \frac{0,56}{1,5} \approx 0,37$$

$$d_{1,2,3} = \frac{m_{1,2,3}}{\sum_{\beta=2}^{4} m_{1,\beta}} = \frac{0,51}{1,5} \approx 0,34$$

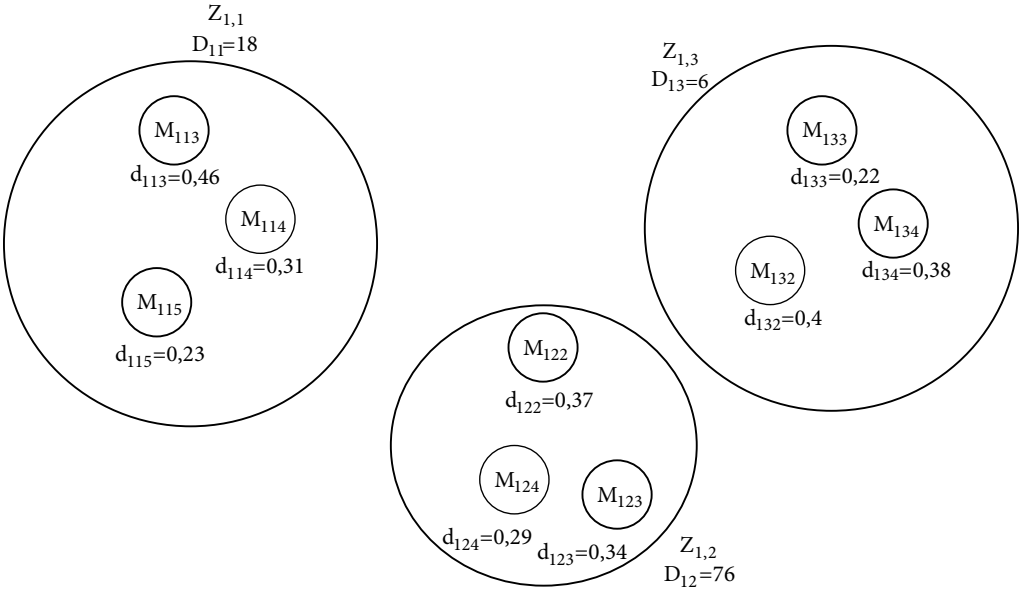
$$d_{1,2,4} = \frac{m_{1,2,4}}{\sum_{\beta=2}^{4} m_{1,\beta}} = \frac{0,43}{1,5} \approx 0,29$$

$$d_{1,3,2} = \frac{m_{1,3,2}}{\sum_{\beta=2}^{4} m_{1,\beta}} = \frac{0,13}{0,32} \approx 0,40$$

$$d_{1,3,3} = \frac{m_{1,3,3}}{\sum_{\beta=2}^{4} m_{1,\beta}} = \frac{0,07}{0,32} \approx 0,22$$

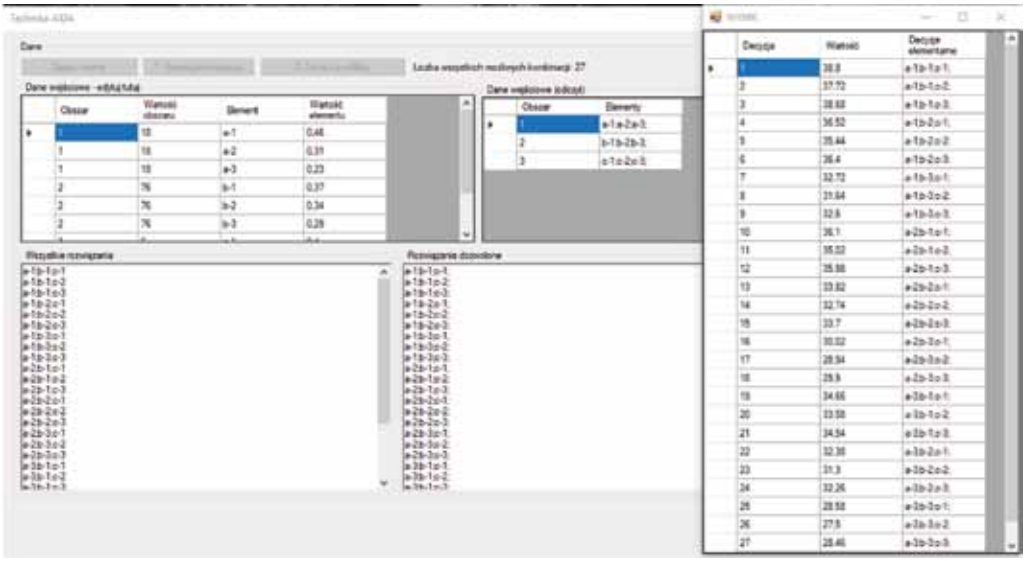
$$d_{1,3,4} = \frac{m_{1,3,4}}{\sum_{\beta=2}^{4} m_{1,\beta}} = \frac{0,12}{0,32} \approx 0,38$$

Na rys. 4.2d zilustrowano graficznie rozpatrywany problem decyzyjny operatora IK V_1.



Rysunek 4.2d. Ilustracja rozpatrywanego problemu decyzyjnego dotyczącego IK V_1
Źródło: opracowanie własne.

Problem decyzyjny przedstawiony na rys. 4.2d. zapisano w narzędziu służącym do rozwiązywania problemów decyzyjnych za pomocą metody AIDA (rys. 4.2e).



Rysunek 4.2e. Ilustracja zapisu rozpatrywanego problemu decyzyjnego operatora IK V_1 w narzędziu informatycznym

Źródło: opracowanie własne.

W tab. 4.2h przedstawiono macierz dopuszczalnych decyzji rozwiązujących rozpatrywany problem decyzyjny operatora IK V_1.

Zamieniając symbole zabezpieczeń ($M_{\alpha,\beta,\lambda}$) na wartości istotności decyzji elementarnych ($d_{\alpha,\beta,\lambda}$) i przemnażając uzyskaną macierz przez macierz istotności obszarów decyzyjnych ($D_{\alpha,\beta}$), uzyskano wyniki oceny kosztowej dopuszczalnych decyzji (tab. 4.2i).

Podstawienie wartości wpływu zabezpieczeń na podatności IK na zagrożenia do wzoru na ryzyko (2.3c) umożliwiło wskazanie zbioru decyzji pozwalających na osiągnięcie wyznaczonego celu – prognozowanej dostępności $\Phi_{1,1}$ – przerobu ropy naftowej oraz wytworzenia produktów i półproduktów ropopochodnych na poziomie 90% (tab. 4.2j).

Analiza wyników ryzyka utraty funkcjonalności $\Phi_{1,1}$ oraz jej prognozowanej wartości (tab. 4.2j) wskazuje, że przy przyjętym celu utrzymania dostępności funkcjonalności na poziomie 90% operator IK V_1 może zastosować dowolną kombinację rozpatrywanych zabezpieczeń. Każda z możliwych decyzji pozwala na utrzymanie dostępności funkcjonalności $\Phi_{1,1}$ w przedziale od 90,21% (decyzja 8, 17 i 26) do 91,91% (decyzja 1, 10 i 19).

Tabela 4.2h. Macierz dopuszczalnych decyzji rozwiązujących rozpatrywany problem decyzyjny operatora IK V1

Decyzja 1	M_{113}	M_{122}	M_{132}
Decyzja 2	M_{113}	M_{122}	M_{133}
Decyzja 3	M_{113}	M_{122}	M_{134}
Decyzja 4	M_{113}	M_{123}	M_{132}
Decyzja 5	M_{113}	M_{123}	M_{133}
Decyzja 6	M_{113}	M_{123}	M_{134}
Decyzja 7	M_{113}	M_{124}	M_{132}
Decyzja 8	M_{113}	M_{124}	M_{133}
Decyzja 9	M_{113}	M_{124}	M_{134}
Decyzja 10	M_{114}	M_{122}	M_{132}
Decyzja 11	M_{114}	M_{122}	M_{133}
Decyzja 12	M_{114}	M_{122}	M_{134}
Decyzja 13	M_{114}	M_{123}	M_{132}
Decyzja 14	M_{114}	M_{123}	M_{133}
Decyzja 15	M_{114}	M_{123}	M_{134}
Decyzja 16	M_{114}	M_{124}	M_{132}
Decyzja 17	M_{114}	M_{124}	M_{133}
Decyzja 18	M_{114}	M_{124}	M_{134}
Decyzja 19	M_{115}	M_{122}	M_{132}
Decyzja 20	M_{115}	M_{122}	M_{133}
Decyzja 21	M_{115}	M_{122}	M_{134}
Decyzja 22	M_{115}	M_{123}	M_{132}
Decyzja 23	M_{115}	M_{123}	M_{133}
Decyzja 24	M_{115}	M_{123}	M_{134}
Decyzja 25	M_{115}	M_{124}	M_{132}
Decyzja 26	M_{115}	M_{124}	M_{133}
Decyzja 27	M_{115}	M_{124}	M_{134}

Źródło: opracowanie własne.

Tabela 4.2i. Ocena kosztowa dopuszczalnych decyzji dla problemu decyzyjnego operatora IK V_1

	$d_{1,1,\lambda}$	$d_{1,2,\lambda}$	$d_{1,3,\lambda}$		$D_{\alpha,\beta}$		Ocena kosztowa
Decyzja 1	0,46	0,37	0,4		18		38,8
Decyzja 2	0,46	0,37	0,22		76		37,72
Decyzja 3	0,46	0,37	0,38		6		38,68
Decyzja 4	0,46	0,34	0,4				36,52
Decyzja 5	0,46	0,34	0,22				35,44
Decyzja 6	0,46	0,34	0,38				36,4
Decyzja 7	0,46	0,29	0,4				32,72
Decyzja 8	0,46	0,29	0,22				31,64
Decyzja 9	0,46	0,29	0,38				32,6
Decyzja 10	0,31	0,37	0,4				36,1
Decyzja 11	0,31	0,37	0,22				35,02
Decyzja 12	0,31	0,37	0,38				35,98
Decyzja 13	0,31	0,34	0,4	*		=	33,82
Decyzja 14	0,31	0,34	0,22				32,74
Decyzja 15	0,31	0,34	0,38				33,7
Decyzja 16	0,31	0,29	0,4				30,02
Decyzja 17	0,31	0,29	0,22				28,94
Decyzja 18	0,31	0,29	0,38				29,9
Decyzja 19	0,23	0,37	0,4				34,66
Decyzja 20	0,23	0,37	0,22				33,58
Decyzja 21	0,23	0,37	0,38				34,54
Decyzja 22	0,23	0,34	0,4				32,38
Decyzja 23	0,23	0,34	0,22				31,3
Decyzja 24	0,23	0,34	0,38				32,26
Decyzja 25	0,23	0,29	0,4				28,58
Decyzja 26	0,23	0,29	0,22				27,5
Decyzja 27	0,23	0,29	0,38				28,46

Źródło: opracowanie własne.

Tabela 4.2j. Wykaz decyzji realizujących cel operatora IK V_1

Decyzja	Ocena kosztowa	Wartość ryzyka utraty funkcjonalności $\Phi_{1,1}$	Prognozowana wartość funkcjonalności $\Phi_{1,1}$
Decyzja 1	38,8	1,09%	91,91%
Decyzja 2	37,72	1,3%	91,67%
Decyzja 3	38,68	1,13%	91,87%
Decyzja 4	36,52	1,66%	91,34%
Decyzja 5	35,44	1,87%	91,13%
Decyzja 6	36,4	1,7%	91,3%
Decyzja 7	32,72	2,57%	90,43%
Decyzja 8	31,64	2,78%	90,21%
Decyzja 9	32,6	2,61%	90,39%
Decyzja 10	36,1	1,09%	91,91%
Decyzja 11	35,02	1,3%	91,67%
Decyzja 12	35,98	1,13%	91,87%
Decyzja 13	33,82	1,66%	91,34%
Decyzja 14	32,74	1,87%	91,13%
Decyzja 15	33,7	1,7%	91,3%
Decyzja 16	30,02	2,57%	90,43%
Decyzja 17	28,94	2,78%	90,21%
Decyzja 18	29,9	2,61%	90,39%
Decyzja 19	34,66	1,09%	91,91%
Decyzja 20	33,58	1,3%	91,67%
Decyzja 21	34,54	1,13%	91,87%
Decyzja 22	32,38	1,66%	91,34%
Decyzja 23	31,3	1,87%	91,13%
Decyzja 24	32,26	1,7%	91,3%
Decyzja 25	28,58	2,57%	90,43%
Decyzja 26	27,5	2,78%	90,21%
Decyzja 27	28,46	2,61%	90,39%

Źródło: opracowanie własne.

Wdrożenie zabezpieczeń

Z tab. 4.2j. wynika, że decyzje 1, 10 i 19 pozwalają na osiągnięcie prognozowanej wartości funkcjonalności $\Phi_{1,1}$ na poziomie 91,91%. Z tego powodu rozwiązania wynikające z tych decyzji są rekomendowane do wdrożenia. Ze względu na identyczny wynik prognozowanej wartości funkcjonalności $\Phi_{1,1}$ operator IK może zastosować dodatkowe kryterium oceny i wdrożyć rozwiązanie np. o najniższym koszcie eksploatacji.

Ocena kosztowa wskazuje, że najlepszym rozwiązaniem dla operatora IK V_1 jest decyzja 1 (tab. 4.2.j), która zakłada zastosowanie dodatkowych zabezpieczeń: dla zagrożenia $Z_{1,1}$ – pożaru ($M_{1,1,3}$ – okładziny ognioodporne), dla zagrożenia $Z_{1,2}$ – wybuchu ($M_{1,2,2}$ – system odprowadzający opary i gazy na pochodnię gazową), dla zagrożenia $Z_{1,3}$ – skażenia środowiska ($M_{1,3,2}$ – monitoring parametrów technologicznych).

Wprowadzenie nowych zabezpieczeń ustala nową sytuację rozpatrywanej IK V_1 – rafinerii PKN ORLEN S.A. (tab. 4.2k).

Tabela 4.2k. Syntetyczny zapis sytuacji rafinerii PKN ORLEN S.A. po wdrożeniu nowych zabezpieczeń

IK	Funkcjonalności		Zagrożenia					Zabezpieczenie				Podatność na zagrożenie
	Symbol	Wartość funkcjonalności	Symbol	Rodzaj	Wzbudzane zagrożenie	Prawdopodobieństwo	Ograniczenie funkcjonalności IK	Symbol	Stopień obniżenia podatności	Cel zarządzania kryzysowego	Obszar ochrony IK	
V_1	$\Phi_{1,1}$	93%	$Z_{1,1}$	IN	skażenia środowiska, wybuch	0,7	-47% ($\Phi_{1,1}$) -37% ($\Phi_{1,2}$) -13% ($\Phi_{1,3}$)	$M_{1,1,1}$	0,46	Przejmowanie kontroli	Bezpieczeństwo techniczne	0,88
								$M_{1,1,2}$	0,31	Przejmowanie kontroli	Bezpieczeństwo techniczne	
								$M_{1,1,3}$	0,71	Zapobieganie	Bezpieczeństwo techniczne	
	$\Phi_{1,2}$	93%	$Z_{1,2}$	IN	pożar	0,56	-42% ($\Phi_{1,1}$) -39% ($\Phi_{1,2}$) -46% ($\Phi_{1,3}$)	$M_{1,2,1}$	0,16	Przejmowanie kontroli	Bezpieczeństwo techniczne	0,81
								$M_{1,2,2}$	0,56	Zapobieganie	Bezpieczeństwo techniczne	
	$\Phi_{1,3}$	93%	$Z_{1,3}$	IN	-	0,81	-9% ($\Phi_{1,1}$) -9% ($\Phi_{1,3}$)	$M_{1,3,1}$	0,16	Zapobieganie	Bezpieczeństwo techniczne	0,31
								$M_{1,3,2}$	0,13	Zapobieganie	Bezpieczeństwo techniczne	

Źródło: opracowanie własne.

Zastosowane dodatkowe zabezpieczenia mają wpływ na wszystkie funkcjonalności rozpatrywanej IK, co ilustruje wartość R^r_2 w tab. 4.2l.

Tabela 4.2l. Syntetyczny zapis ryzyka utraty funkcjonalności dla IK V_1 po wdrożeniu nowych zabezpieczeń

IK	Zagrożenie	Prawdopodobieństwo	Skutek		Podatność	Zabezpieczenie	Ryzyko inherentne	Ryzyko rezydualne
Vα	Zα,β	P	Φα,γ	ΔΦα,γ	Uα,β	ΣMα,β,λ	Ri	Rr_2
V_1	$Z_{1,1}$	0,7	Φ1,1	47%	0,88	0,88	28,95%	0,00%
			Φ1,2	37%			22,79%	0,00%
			Φ1,3	13%			8,01%	0,00%
	$Z_{1,2}$	0,56	Φ1,1	42%	0,81	0,72	19,05%	2,12%
			Φ1,2	39%			17,69%	1,97%
			Φ1,3	46%			20,87%	2,32%
	$Z_{1,3}$	0,81	Φ1,1	9%	0,31	0,29	2,26%	0,15%
			Φ1,3	9%			2,26%	0,15%
Suma ryzyka dla						Φ1,1	24,28%	1,09%
						Φ1,2	32,12%	1,56%
						Φ1,3	15,04%	1,19%

Źródło: opracowanie własne.

Wdrożenie dodatkowych zabezpieczeń powoduje redukcję ryzyka utraty funkcjonalności:

- $\Phi_{1,1}$ z poziomu 9,66% (tab. 4.2c) do 1,09% (tab. 4.2l),
- $\Phi_{1,2}$ z poziomu 13,53% (tab. 4.2c) do 1,56% (tab. 4.2l),
- $\Phi_{1,3}$ z poziomu 9,1% (tab. 4.2c) do 1,19% (tab. 4.2l).

4.3. Przykład hierarchicznego problemu decyzyjnego

W przykładzie obliczeniowym obrazującym zastosowanie metodyki ZS-BIK dla przypadku hierarchicznego problemu decyzyjnego wykorzystano jeden ze SZN uzyskany na podstawie symulacji przebiegu zdarzeń niekorzystnych wykonanej dla rafinerii PKN ORLEN S.A. W rozdziale zaprezentowano elementy procedury wykonania metodyki ZS-BIK dla przypadku hierarchicznego problemu decyzyjnego dotyczące:

- sformułowania hierarchicznego problemu decyzyjnego,
- wyznaczenia zbioru zabezpieczeń realizującego założony cel.

Rozpatrywany SZN

Problem decyzyjny dotyczy SZN nr 28 (tab. D.1). Scenariusz ten został wybrany ze względu na największą liczbę zagrożeń negatywnie wpływających na różne elementy rafinerii PKN ORLEN S.A. Zakłada on negatywny wpływ trzech zagrożeń na dwa elementy rozpatrywanej IK (tab. 4.3a):

- na rafinerię PKN ORLEN S.A. (V_1), negatywnie wpływają:
  - $Z_{1,1}$ – pożar,
  - $Z_{1,3}$ – skażenie środowiska,
- na Zakład Produkcyjny ORLEN OIL sp. z o.o. w Płocku (V_3), negatywnie wpływa:
  - $Z_{3,2}$ – wybuch.

Tabela 4.3a. Charakterystyka SZN negatywnie wpływającego na rafinerię PKN ORLEN S.A. oraz Zakład Produkcyjny ORLEN OIL sp. z o.o. w Płocku

Wyszczególnienie	Wzbudzenie	Materializacja	Skutek
Scenariusz 28	Z2,1-D		
	Z2,2-D		
	Z2,3-D		
	Z3,1-D	Z3,1-P	
	Z3,2-D	Z3,2-P	Z3,2-R
	Z3,3-D		
	Z1,1-D	Z1,1-P	Z1,1-R
	Z1,2-D	Z1,2-P	
	Z1,3-D	Z1,3-P	Z1,3-R

Źródło: opracowanie własne.

Ze względu na bezpieczeństwo społeczności władze miasta Płocka, na terenie którego znajduje się rozpatrywana IK, chcą dofinansować wdrożenie zabezpieczeń, które maksymalnie ograniczą podatność rafinerii PKN ORLEN S.A. oraz zakładu ORLEN OIL sp. z o.o. na zagrożenia wynikające ze SZN nr 28. Przyjęcie tego założenia powoduje stan, w którym decyzja o zabezpieczeniach dla IK zapada na szczeblu władz miejskich. Jednocześnie zbiór dopuszczalnych decyzji dla władz miejskich zależy od możliwości, jakie mają operatorzy IK.

Na podstawie modelu sytuacji IK (tab. 4.2b) ustalono, że operatorzy IK przed zagrożeniami wynikającymi ze SZN nr 28 obecnie stosują następujące zabezpieczenia:

- operator IK V_1 wykorzystuje dla zagrożenia:
  - $Z_{1,1}$ – zabezpieczenie $M_{1,1,1}$ (zakładową straż pożarną) i $M_{1,1,2}$ (służbę ochrony zakładu),
  - $Z_{1,3}$ – zabezpieczenie $M_{1,3,1}$ (monitorowanie stanu środowiska),
- operator IK V_3 wykorzystuje:
  - $Z_{3,2}$ – zabezpieczenie $M_{3,2,1}$ (zakładową służbę medyczną).

Stosowane zabezpieczenia pozwalają na ograniczenie podatności rozpatrywanych elementów IK do poziom $U'_{\alpha,\beta}$ (tab. 4.3b).

Tabela 4.3b. Syntetyczny zapis podatności V_1 i V_3 na zagrożenia ze SZN nr 28

IK	Zagrożenie	Podatność IK	Zabezpieczenie	Podatność IK uwzględniająca zabezpieczenia
$\mathbf{V_\alpha}$	$\mathbf{Z_{\alpha,\beta}}$	$\mathbf{U_{\alpha,\beta}}$	$\mathbf{M_{\alpha,\beta}}$	$\mathbf{U'_{\alpha,\beta}}$
V_1	$Z_{1,1}$	0,88	0,77	0,11
	$Z_{1,3}$	0,31	0,16	0,15
V_3	$Z_{3,2}$	0,83	0,14	0,69

Źródło: opracowanie własne.

Wykorzystując wzór 2.5d, wyznaczono względne istotności obszarów decyzyjnych dla IK V_1.

$$D_{1,1} = \frac{U'_{1,1}}{U'_{1,1} + U'_{1,3}} * 100 = \frac{0,11}{0,11 + 0,15} * 100 \approx 42$$

$$D_{1,3} = \frac{U'_{1,3}}{U'_{1,1} + U'_{1,3}} * 100 = \frac{0,15}{0,11 + 0,15} * 100 \approx 58$$

W przypadku zagrożenia $Z_{3,2}$ jego istotność dla operatora IK V_3 wynosi 100%, ponieważ jest to jedyny obszar decyzyjny w rozpatrywanym przez niego problemie decyzyjnym.

W celu ograniczenia ryzyka utraty funkcjonalności operatorzy IK V_1 i V_3 mogą zastosować następujące dodatkowe zabezpieczenia[119]:

- dla zagrożenia $Z_{1,1}$ – pożaru:
  - $M_{1,1,3}$ – okładziny ognioodporne,
  - $M_{1,1,4}$ – zakup nowoczesnego sprzętu gaśniczego dla straży zakładowej,
  - $M_{1,1,5}$ – instalacje pianowe,
- dla zagrożenia $Z_{1,3}$ – skażenia środowiska:
  - $M_{1,3,2}$ – monitoring parametrów technologicznych,
  - $M_{1,3,3}$ – monitoring stanu napełnienia zbiorników magazynowych,
  - $M_{1,3,4}$ – obwałowanie zbiorników,
- dla zagrożenia $Z_{3,2}$ – wybuchu:
  - $M_{3,2,2}$ – system odprowadzający opary i gazy na pochodnię gazową,
  - $M_{3,2,3}$ – zawory bezpieczeństwa włączone w system odprowadzający opary i gazy na pochodnię gazową,
  - $M_{3,2,4}$ – urządzenia kontrolno-pomiarowe włączone w system blokad instalacji technologicznych.

Wśród dodatkowych zabezpieczeń dostępnych dla operatorów IK nie wskazano par sprzecznych. Oznacza to, że wymienione zabezpieczenia mogą być stosowane w dowolnej konfiguracji.

Ze względu na brak danych dotyczących skuteczności stosowanych zabezpieczeń, ich wpływ na podatność IK na zagrożenia został oszacowany losowo na skali od 0 do 1, gdzie 0 oznacza całkowity brak skuteczności zabezpieczenia, a 1 zapewnienie całkowitej odporności na zagrożenie. Wyniki szacowania umieszczono w tab. 4.3c.

[119] Zabezpieczenia zostały dobrane na podstawie rozwiązań stosowanych w rafinerii LOTOS S.A. [Lotos – Informacja o występujących zagrożeniach, data odczytu 04.04.2018].

Tabela 4.3c. Szacunkowy wpływ dodatkowych zabezpieczeń na podatność rozpatrywanej IK V_1 i V_3 na zagrożenia

Nazwa zabezpieczenia	Symbol zabezpieczenia ($M_{\alpha,\beta,\lambda}$)	Wpływ zabezpieczenia na podatność IK na zagrożenia ($m_{\alpha,\beta,\lambda}$)
okładziny ognioodporne	$M_{1,1,3}$	$m_{1,1,3} = 0,71$
nowoczesny sprzęt gaśniczy dla straży zakładowej	$M_{1,1,4}$	$m_{1,1,4} = 0,48$
instalacje pianowe	$M_{1,1,5}$	$m_{1,1,5} = 0,36$
monitoring parametrów technologicznych	$M_{1,3,2}$	$m_{1,3,2} = 0,13$
monitoring stanu napełnienia zbiorników magazynowych	$M_{1,3,3}$	$m_{1,3,3} = 0,07$
obwałowanie zbiorników	$M_{1,3,4}$	$m_{1,3,4} = 0,12$
system odprowadzający opary i gazy na pochodnię gazową	$M_{3,2,2}$	$m_{3,2,2} = 0,36$
zawory bezpieczeństwa	$M_{3,2,3}$	$m_{3,2,3} = 0,5$
urządzenia kontrolno-pomiarowe włączone w system blokad instalacji technologicznych	$M_{3,2,4}$	$m_{3,2,4} = 0,23$

Źródło: opracowanie własne.

Przyjmując wartości wpływu dodatkowych zabezpieczeń dostępnych dla operatora IK V_1 oraz V_3 za pomocą wzoru 2.5b wyznaczono względne istotności decyzji elementarnych.

$$d_{1,1,3} = \frac{m_{1,1,3}}{\sum_{\beta=3}^{5} m_{1,\beta}} = \frac{0,71}{1,55} \approx 0,46$$

$$d_{1,1,4} = \frac{m_{1,1,4}}{\sum_{\beta=3}^{5} m_{1,\beta}} = \frac{0,48}{1,55} \approx 0,31$$

$$d_{1,1,5} = \frac{m_{1,1,5}}{\sum_{\beta=3}^{5} m_{1,\beta}} = \frac{0,36}{1,55} \approx 0,23$$

$$d_{1,3,2} = \frac{m_{1,3,2}}{\sum_{\beta=2}^{4} m_{1,\beta}} = \frac{0,13}{0,32} \approx 0,40$$

$$d_{1,3,3} = \frac{m_{1,3,3}}{\sum_{\beta=2}^{4} m_{1,\beta}} = \frac{0,07}{0,32} \approx 0,22$$

$$d_{1,3,4} = \frac{m_{1,3,4}}{\sum_{\beta=2}^{4} m_{1,\beta}} = \frac{0,12}{0,32} \approx 0,38$$

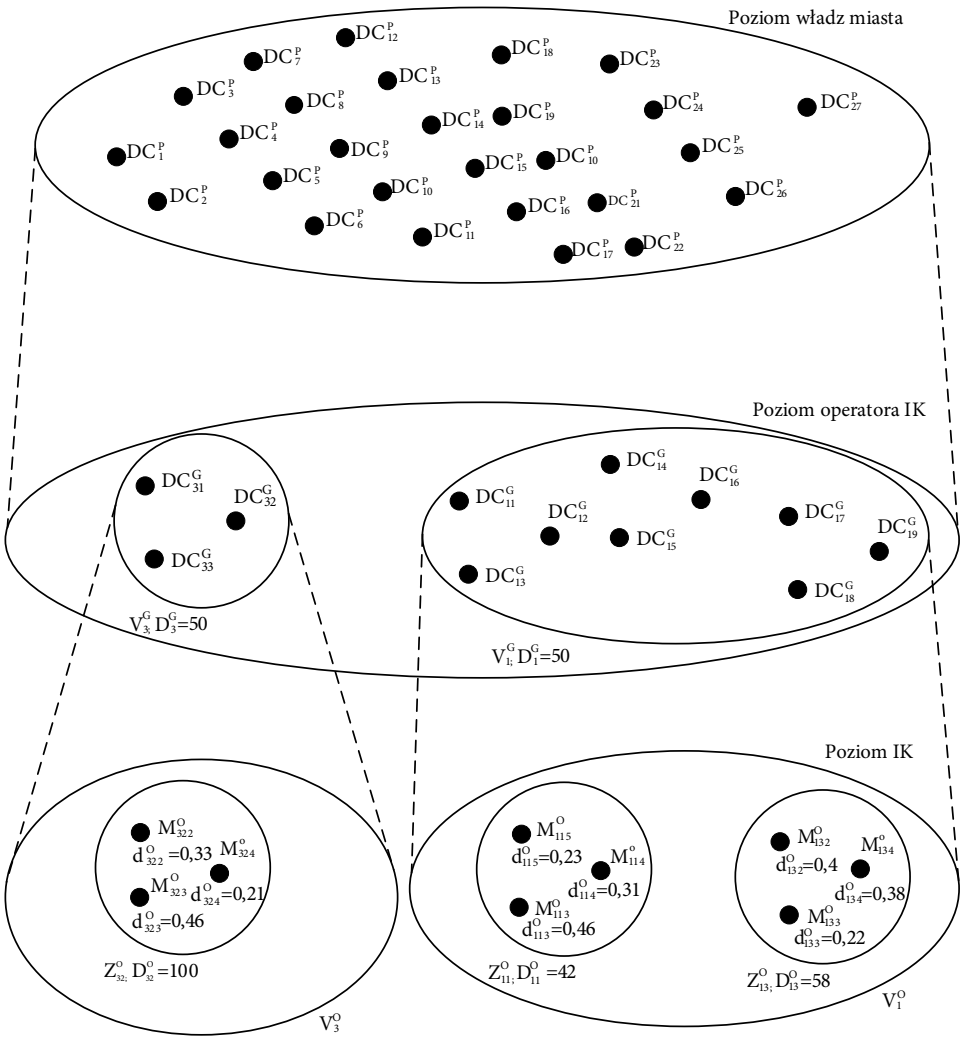
$$d_{3,2,2} = \frac{m_{3,2,2}}{\sum_{\beta=2}^{4} m_{3,\beta}} = \frac{0,36}{1,09} \approx 0,33$$

$$d_{3,2,3} = \frac{m_{3,2,3}}{\sum_{\beta=2}^{4} m_{3,\beta}} = \frac{0,5}{1,09} \approx 0,46$$

$$d_{3,2,4} = \frac{m_{3,2,4}}{\sum_{\beta=2}^{4} m_{3,\beta}} = \frac{0,23}{1,09} \approx 0,21$$

Brak par sprzecznych wskazuje, że operator IK V_1 ma do wyboru dziewięć możliwych kombinacji zabezpieczeń przed zagrożeniami $Z_{1,1}$ i $Z_{1,3}$. Operator IK V_3 ma trzy możliwe zabezpieczenia do wyboru w reakcji na zagrożenie $Z_{3,2}$. Sytuacja ta powoduje, że władze miejskie będą dokonywały wyboru spośród dwudziestu siedmiu dopuszczalnych decyzji.

Na rys. 4.3a przedstawiono ilustrację rozpatrywanego hierarchicznego problemu decyzyjnego. Względną istotność obszarów decyzyjnych dla IK V_1 wyznaczono za pomocą wzoru 2.5d. Natomiast względne istotności decyzji elementarnych dla obszarów decyzyjnych Z^O_{11}; Z^O_{13} oraz Z^O_{32} wyznaczono za pomocą wzoru 2.5b. Względna istotność obszarów decyzyjnych na poziomie operatora IK V^G_1 i V^G_3 została ustalona przez władze miasta na tym samym poziomie. Oznacza to, że rozpatrywane IK uznano za równie istotne.

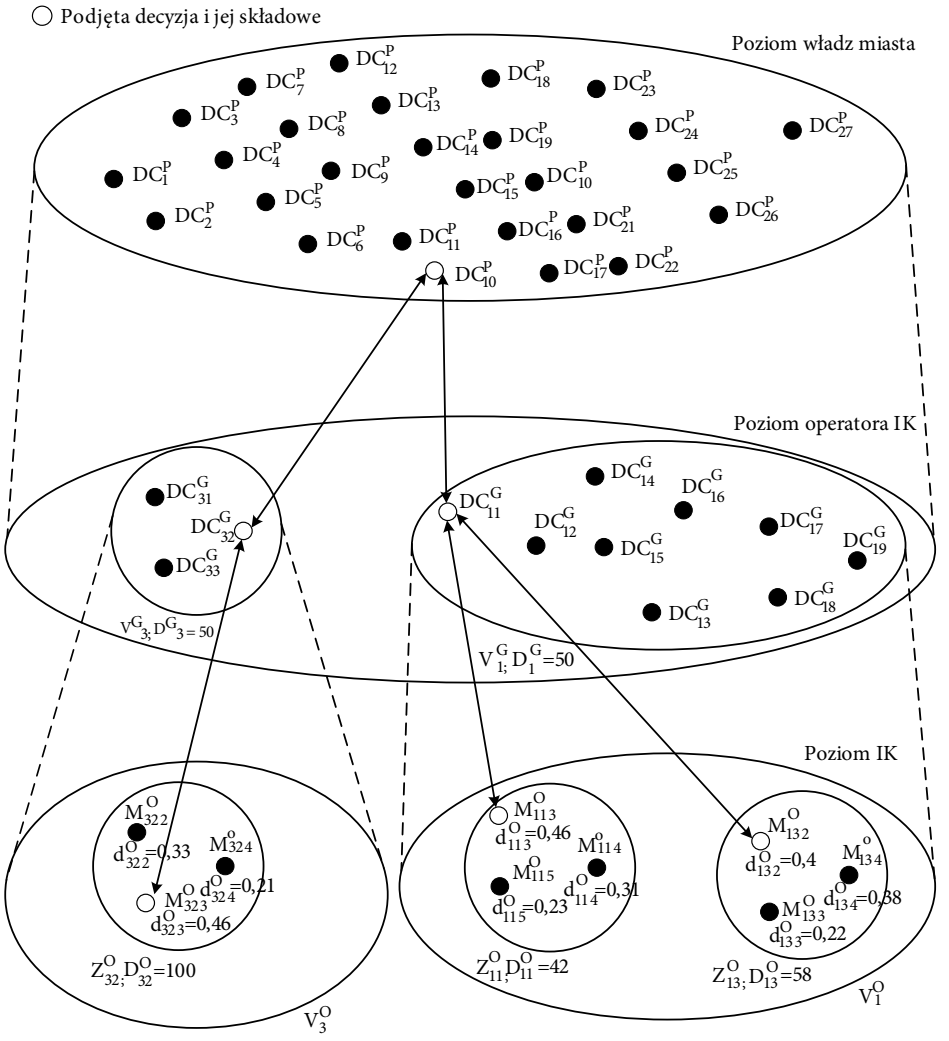


Rysunek 4.3a. Ilustracja rozpatrywanego problemu decyzyjnego dotyczącego SZN nr 28
Źródło: opracowanie własne.

Rozwiązanie hierarchicznego problemu decyzyjnego

Całość hierarchicznego problemu decyzyjnego przedstawionego na rys. 4.3a wraz z wartościami ocen kosztowych dopuszczalnych decyzji na poszczególnych poziomach decyzyjnych zapisano w postaci równań macierzowych (tab. 4.3d).

Najwyższą ocenę kosztową uzyskała decyzja DC^{P}_{10} (tab. 4.3d). Oznacza to, że zabezpieczenia składające się na t decyzję w największym stopniu podniosą odporność IK V_1 i V_3 na rozpatrywane zagrożenia $Z_{1,1}$; $Z_{1,3}$ i $Z_{3,2}$. Na rys. 4.3b zilustrowano składowe decyzje elementarne wynikające z decyzji DC^{P}_{10}, na wszystkich poziomach decyzyjnych.



Rysunek 4.3b. Ilustracja rozwiązania rozpatrywanego problemu decyzyjnego dotyczącego SZN nr 28

Źródło: opracowanie własne.

Tabela 4.3d. Zapis macierzowy rozpatrywanego hierarchicznego problemu decyzyjnego dotyczącego SZN nr 28

Zależności poziom operator IK – poziom władze miasta

$d_{31}^{G} = 33$	$d_{11}^{G} = 42{,}52$	$D_{1}^{G} = 50$		$dc_{1}^{P} = 3776$
$d_{31}^{G} = 33$	$d_{12}^{G} = 32{,}08$	$D_{3}^{G} = 50$		$dc_{2}^{P} = 3254$
$d_{31}^{G} = 33$	$d_{13}^{G} = 41{,}36$			$dc_{3}^{P} = 3718$
$d_{31}^{G} = 33$	$d_{14}^{G} = 36{,}22$			$dc_{4}^{P} = 3461$
$d_{31}^{G} = 33$	$d_{15}^{G} = 25{,}78$			$dc_{5}^{P} = 2939$
$d_{31}^{G} = 33$	$d_{16}^{G} = 35{,}06$			$dc_{6}^{P} = 3403$
$d_{31}^{G} = 33$	$d_{17}^{G} = 32{,}86$			$dc_{7}^{P} = 3293$
$d_{31}^{G} = 33$	$d_{18}^{G} = 22{,}42$			$dc_{8}^{P} = 2771$
$d_{31}^{G} = 33$	$d_{19}^{G} = 31{,}70$			$dc_{9}^{P} = 3235$
$d_{32}^{G} = 46$	$d_{11}^{G} = 42{,}52$			$dc_{10}^{P} = 4426$
$d_{32}^{G} = 46$	$d_{12}^{G} = 32{,}08$			$dc_{11}^{P} = 3904$
$d_{32}^{G} = 46$	$d_{13}^{G} = 41{,}36$			$dc_{12}^{P} = 4368$
$d_{32}^{G} = 46$	$d_{14}^{G} = 36{,}22$			$dc_{13}^{P} = 4111$
$d_{32}^{G} = 46$	$d_{15}^{G} = 25{,}78$	*	=	$dc_{14}^{P} = 3589$
$d_{32}^{G} = 46$	$d_{16}^{G} = 35{,}06$			$dc_{15}^{P} = 4053$
$d_{32}^{G} = 46$	$d_{17}^{G} = 32{,}86$			$dc_{16}^{P} = 3943$
$d_{32}^{G} = 46$	$d_{18}^{G} = 22{,}42$			$dc_{17}^{P} = 3421$
$d_{32}^{G} = 46$	$d_{19}^{G} = 31{,}70$			$dc_{18}^{P} = 3885$
$d_{33}^{G} = 21$	$d_{11}^{G} = 42{,}52$			$dc_{19}^{P} = 3176$
$d_{33}^{G} = 21$	$d_{12}^{G} = 32{,}08$			$dc_{20}^{P} = 2654$
$d_{33}^{G} = 21$	$d_{13}^{G} = 41{,}36$			$dc_{21}^{P} = 3118$
$d_{33}^{G} = 21$	$d_{14}^{G} = 36{,}22$			$dc_{22}^{P} = 2861$
$d_{33}^{G} = 21$	$d_{15}^{G} = 25{,}78$			$dc_{23}^{P} = 2339$
$d_{33}^{G} = 21$	$d_{16}^{G} = 35{,}06$			$dc_{24}^{P} = 2803$
$d_{33}^{G} = 21$	$d_{17}^{G} = 32{,}86$			$dc_{25}^{P} = 2693$
$d_{33}^{G} = 21$	$d_{18}^{G} = 22{,}42$			$dc_{26}^{P} = 2171$
$d_{33}^{G} = 21$	$d_{19}^{G} = 31{,}70$			$dc_{27}^{P} = 2635$

Zależności poziom IK – poziom operator IK

Problem decyzyjny V^{O}_{1}

$d_{113}^{O} = 0{,}46$	$d_{132}^{O} = 0{,}4$	$D_{11}^{O} = 42$		$d_{11}^{G} = 42{,}52$
$d_{113}^{O} = 0{,}46$	$d_{133}^{O} = 0{,}22$	$D_{13}^{O} = 58$		$d_{12}^{G} = 32{,}08$
$d_{113}^{O} = 0{,}46$	$d_{134}^{O} = 0{,}38$			$d_{13}^{G} = 41{,}36$
$d_{114}^{O} = 0{,}31$	$d_{132}^{O} = 0{,}4$			$d_{14}^{G} = 36{,}22$
$d_{114}^{O} = 0{,}31$	$d_{133}^{O} = 0{,}22$	*	=	$d_{15}^{G} = 25{,}78$
$d_{114}^{O} = 0{,}31$	$d_{134}^{O} = 0{,}38$			$d_{16}^{G} = 35{,}06$
$d_{115}^{O} = 0{,}23$	$d_{132}^{O} = 0{,}4$			$d_{17}^{G} = 32{,}86$
$d_{115}^{O} = 0{,}23$	$d_{133}^{O} = 0{,}22$			$d_{18}^{G} = 22{,}42$
$d_{115}^{O} = 0{,}23$	$d_{134}^{O} = 0{,}38$			$d_{19}^{G} = 31{,}70$

Problem decyzyjny V^{O}_{3}

$d_{322}^{O} = 0{,}33$		$D_{32}^{O} = 100$		$dc_{31}^{G} = 33$
$d_{323}^{O} = 0{,}46$		*	=	$dc_{32}^{G} = 46$
$d_{324}^{O} = 0{,}21$				$dc_{33}^{G} = 21$

Źródło: opracowanie własne.

Podjęcie przez władze miasta decyzji DC^{P}_{10} skutkuje wdrożeniem konkretnych zabezpieczeń przez operatorów rozpatrywanych IK:

- dla zagrożenia $Z_{1,1}$ – pożaru:
  - $M_{1,1,3}$ – okładziny ognioodporne,
- dla zagrożenia $Z_{1,3}$ – skażenia środowiska:
  - $M_{1,3,2}$ – monitoring parametrów technologicznych,
- dla zagrożenia $Z_{3,2}$ – wybuchu:
  - $M_{3,2,3}$ – zawory bezpieczeństwa włączone w system odprowadzający opary i gazy na pochodnię gazową.

W tab. 4.3e przedstawiono wpływ dodatkowych zabezpieczeń na podatność IK V_1 i V_3 na rozpatrywane zagrożenia $Z_{1,1}$; $Z_{1,3}$ i $Z_{3,2}$ (zmienna $M'_{\alpha,\beta}$). Podatność IK V_1 i V_3 na rozpatrywane zagrożenia po wdrożeniu dodatkowych zabezpieczeń reprezentuje zmienna $U''_{\alpha,\beta}$.

Tabela 4.3e. Syntetyczny zapis podatności V_1 i V_3 na zagrożenia ze SZN nr 28 po zastosowaniu dodatkowych zabezpieczeń

IK	Zagrożenie	Podatność	Zabezpieczenie	Podatność uwzględniająca zabezpieczenia	Wpływ dodatkowych zabezpieczeń	Podatność finalna
V_α	$Z_{\alpha,\beta}$	$U_{\alpha,\beta}$	$M_{\alpha,\beta}$	$U'_{\alpha,\beta}$	$M'_{\alpha,\beta}$	$U''_{\alpha,\beta}$
V_1	$Z_{1,1}$	0,88	0,77	0,11	0,71	0
	$Z_{1,3}$	0,31	0,16	0,15	0,48	0
V_3	$Z_{3,2}$	0,83	0,14	0,69	0,5	0,19

Źródło: opracowanie własne.

Dane przedstawione w tab. 4.3e wskazują, że po zastosowaniu dodatkowych zabezpieczeń podatność IK V_1 na zagrożenia $Z_{1,1}$ i $Z_{1,3}$ będzie wynosiła 0[120]. Oznacza to, że wskazana kombinacja zabezpieczeń powinna uczynić IK odporną na rozpatrywane zagrożenia. W przypadku IK V_3 (ostatni wiersz w tab. 4.3e) zastosowanie dodatkowych zabezpieczeń redukuje podatność rozpatrywanej IK na zagrożenia $Z_{3,2}$ do poziomu $U''_{3,2} = 0{,}19$.

Zabezpieczenia zastosowane w przypadku IK V_1 są nadmiarowe[121] w stosunku do potrzeb operatora IK. Daje to władzom miejskim możliwość zastosowania dodatkowego kryterium oceny dopuszczalnych decyzji np. kryterium ceny zakupu zabezpieczeń, które pozwoli wybrać tańszy zbiór zabezpieczeń, pozwalający na zredukowanie podatności IK na podobnym poziomie jak decyzja DC^{P}_{10}. Wskazanie takiego zbioru wymaga sformułowania nowego problemu decyzyjnego.

[120] Suma wpływu zastosowanych zabezpieczeń $M_{\alpha,\beta}$ jest większa lub równa podatności IK $U_{\alpha,\beta}$ na zagrożenia.

[121] Suma wpływu zastosowanych zabezpieczeń $M_{\alpha,\beta}$ jest większa od podatności IK $U_{\alpha,\beta}$ na zagrożenia.

4.4. Wnioski z rozdziału

Przedstawione przykłady obliczeniowe (rozdz. 4.2 i 4.3) wykorzystujące dane pochodzące z Planu Zarządzania Kryzysowego powiatu płockiego z 2015 r. (rozpatrywane IK, ich funkcjonalności, zagrożenia, na które podatne są IK i stosowane zabezpieczenia) oraz Raportu Zintegrowanego Grupy Orlen z 2016 r. (poziom funkcjonalności elementów IK) pozwoliły zweryfikować użyteczność metodyki ZS-BIK dla podmiotów odpowiedzialnych za bezpieczeństwo IK w warunkach płaskich i hierarchicznych problemów decyzyjnych. Metodyka ZS-BIK była weryfikowana w obszarze:

- możliwości określenia charakterystyki rozpatrywanej IK,
- możliwości wygenerowania SZN na podstawie modeli rozpatrywanych IK,
- możliwości sformułowania problemu decyzyjnego i wskazania zbioru zabezpieczeń,
- możliwości oszacowania wartości ryzyka utraty funkcjonalności przed i po zastosowaniu dodatkowych zabezpieczeń.

Ze względu na brak danych nie zweryfikowano etapu powoływania zespołu analitycznego oraz etapu wyznaczania progu bezpieczeństwa.

Używając liczb losowych, wyznaczono wartości liczbowe dotyczące:

- prawdopodobieństwa występowania zagrożeń,
- podatności elementów IK na zagrożenia,
- wpływu zabezpieczeń na odporność IK na zagrożenia.

Użycie losowych wartości parametrów dotyczących prawdopodobieństwa występowania zagrożeń, podatności IK na zagrożenia oraz wpływu zabezpieczeń na odporność IK nie wpływa na procedurę stosowania metodyki ZS-BIK. Należy jednak zaznaczyć, że uzyskane na ich podstawie rozwiązania nie mogą stanowić rzeczywistych rekomendacji dla operatorów IK.

Przykład obliczeniowy dla przypadku płaskiego problemu decyzyjnego polegał na określeniu sytuacji rafinerii PKN ORLEN S.A. i wyznaczeniu modelu zabezpieczeń dla wybranego przypadku przekroczenia progu bezpieczeństwa. W ramach eksperymentu ustalono, że na sytuację rafinerii PKN ORLEN S.A. mają wpływ przedsiębiorstwa Basell Orlen Polyolefins sp. z o.o. oraz Zakład Produkcyjny ORLEN OIL sp. z o.o. w Płocku. Wzajemne usytuowanie przedsiębiorstw powoduje zwiększenie prawdopodobieństwa występowania zagrożeń: pożaru, wybuchu i skażenia środowiska, co eskaluje ryzyko utraty funkcjonalności rozpatrywanych przedsiębiorstw. Z tego powodu uznano, że rozpatrywana IK jest złożona z trzech zależnych od siebie elementów. Charakterystykę oraz zależności elementów rozpatrywanej IK zilustrowano syntetycznie w tab. 4.2a i 4.2b.

Na podstawie sytuacji rafinerii PKN ORLEN S.A. oszacowano ryzyko utraty funkcjonalności jej składowych przy uwzględnieniu: zagrożeń, na jakie podatne są elementy rozpatrywanej IK, prawdopodobieństwa ich wystąpienia, podatności IK na te zagrożenia oraz stosowanych zabezpieczeń (tab. 4.2c).

W kolejnym etapie eksperymentu obliczeniowego sformułowano model SPIK, którego składowymi są rafineria PKN ORLEN S.A., przedsiębiorstwo Basell Orlen Polyolefins sp. z o.o. i Zakład Produkcyjny ORLEN OIL sp. z o.o. w Płocku (rys. 4.2a). Opracowany model SPIK oraz dane z modelu sytuacji rafinerii PKN ORLEN S.A. zaimplementowano

w narzędziu IBM WebSphere Business Modeler 7.0, co pozwoliło na wygenerowanie 93 SZN, jakie mogą zaistnieć w rozpatrywanych warunkach. Symulacja została przeprowadzona na próbie 1000 przypadków. Zagrożenia dla rafinerii PKN ORLEN S.A., przedsiębiorstwa Basell Orlen Polyolefins sp. z o.o. oraz Zakładu Produkcyjnego ORLEN OIL sp. z o.o. w Płocku były inicjowane losowo. Z uzyskanych 93 SZN, 61 SZN miało negatywny wpływ na przynajmniej jeden element rozpatrywanej IK. W 32 SZN negatywne skutki materializacji zagrożeń zostały wyeliminowane dzięki stosowanym przez operatorów IK zabezpieczeniom.

Etapem kończącym przykład obliczeniowy dla płaskiego problemu decyzyjnego było sformułowanie i rozwiązanie problemu decyzyjnego, który dotyczył 9,66% ryzyka utraty funkcjonalności $\Phi_{1,1}$ – przerobu ropy naftowej oraz wytwarzania produktów i półproduktów ropopochodnych (tab. 4.2c). Wykorzystując dane dotyczące możliwych zabezpieczeń stosowanych w rafinerii LOTOS S.A., wyznaczono zbiór decyzji elementarnych dla obszarów decyzyjnych zdefiniowanych przez zagrożenia, na które podatna jest rafineria PKN ORLEN S.A. Dodatkowe zabezpieczenia miały doprowadzić do osiągnięcia założonego na poziomie 90% progu bezpieczeństwa. Wykorzystując wzory 2.5a i 2.5b wyznaczono względne istotności obszarów decyzyjnych oraz decyzji elementarnych, co pozwoliło na zapis graficzny rozpatrywanego problemu decyzyjnego (rys. 4.2c). Stosując autorskie narzędzie wspomagające obliczenie oceny kosztowej dopuszczalnych decyzji, wyznaczono zbiór decyzji pozwalających na osiągnięcie założonego progu bezpieczeństwa (tab. 4.2j).

Ustalenie zbioru zabezpieczeń pozwalających na osiągnięcie założonego progu bezpieczeństwa pozwoliło na oszacowanie nowej wartości ryzyka (tab. 4.2l) i ustalenie nowej sytuacji rafinerii PKN ORLEN S.A. (tab. 4.2k).

Przykład obliczeniowy dla przypadku hierarchicznego problemu decyzyjnego sformułowano, wykorzystując dane ze SZN, który może mieć miejsce w rafinerii PKN ORLEN S.A. W ramach przykładu ustalono, że rozpatrywany SZN zakłada wystąpienie trzech zagrożeń niekorzystnie wpływających na rafinerię PKN ORLEN S.A. oraz Zakład Produkcyjny ORLEN OIL sp. z o.o. w Płocku. Dodatkowo wprowadzono założenie, że władze miasta Połock, na terenie którego znajdują się zagrożone przedsiębiorstwa, dofinansują wdrożenie nowych zabezpieczeń, które spowodują maksymalne ograniczenie możliwości wystąpienia zagrożeń przewidzianych w rozpatrywanym SZN. Przyjęcie tego założenia spowodowało stan, w którym decyzja o zabezpieczeniach dla IK zapada na szczeblu władz miejskich. Jednocześnie zbiór dopuszczalnych decyzji dla władz miejskich zależy od możliwości operatorów IK.

Wykorzystując rozwiązania stosowane w rafinerii LOTOS S.A. jako źródło danych o możliwych zabezpieczeniach dla rozpatrywanych zagrożeń, sformułowano hierarchiczny problem decyzyjny (rys. 4.3a). Stosując zapis macierzowy, opracowano układ równań opisujący sformułowany problem decyzyjny (tab. 4.3d), którego rozwiązanie pozwoliło na wskazanie kombinacji zabezpieczeń redukujących podatności rafinerii

PKN ORLEN S.A. oraz Zakładu Produkcyjnego ORLEN OIL sp. z o.o. w Płocku na rozpatrywane zagrożenia.

Przedstawione przykłady obliczeniowe pozwalają stwierdzić, że użyteczność metodyki ZS-BIK dla podmiotów odpowiedzialnych za bezpieczeństwo IK została pozytywnie zweryfikowana w obszarze:

- określenia charakterystyki rozpatrywanej IK,
- generowania SZN na podstawie modeli rozpatrywanych IK,
- formułowania problemu decyzyjnego i wskazania zbioru zabezpieczeń,
- szacowania wartości ryzyka utraty funkcjonalności przed i po zastosowaniu dodatkowych zabezpieczeń,
- wdrożenia zabezpieczeń.

Zweryfikowane etapy metodyki ZS-BIK wpisują się w proces planowania cywilnego (tab. 4.4a).

Tabela 4.4a. Powiązanie etapów metodyki ZS-BIK z etapami procesu planowania cywilnego

Etap metodyki ZS-BIK	Etap procesu planowania cywilnego	Uzasadnienie
Odwzorowanie charakterystyki IK	Analiza	Możliwość opisu rozpatrywanej IK według standardu zgodnego z obowiązującymi aktami normatywnymi z obszaru planowania cywilnego.
Wygenerowanie SZN	Prognozowanie	Możliwość pozyskania informacji o SZN dla rozpatrywanej IK.
Sformułowanie problemu decyzyjnego	Opracowanie planu	Możliwość pozyskania informacji, jakie zabezpieczenia zastosować w kontekście rozpoznanych zagrożeń, na które podatna jest IK.
Wygenerowanie SZN	Testowanie	Możliwość sprawdzenia, czy wartość ryzyka związany z zagrożeniem został właściwie oszacowany.
Szacowanie ryzyka	Wdrożenie	Możliwość pozyskania informacji o spodziewanym ryzyku i poziomie funkcjonalności IK po zastosowaniu nowych zabezpieczeń, dzięki czemu zespół analityczny może podjąć decyzję o wdrożeniu zabezpieczeń lub powtórzeniu etapów metodyki ZS-BIK.
Wdrożenie zabezpieczeń	Uruchomienie	Możliwość pozyskania informacji, jaki zestaw zabezpieczeń należy rekomendować operatorowi IK ze względu na rozpoznane zagrożenia i przyjęty próg bezpieczeństwa.

Źródło: opracowanie własne.

Etapy metodyki ZS-BIK mogą zostać wykorzystane jako procedury opracowania elementów POIK (tab. 4.4b) oraz PZK (tab. 4.4c).

Tabela 4.4b. Zestawienie elementów POIK z realizującymi je etapami ZS-BIK

Elementy POIK	Etap metodyki ZS-BIK
Dane ogólne: • obejmujące nazwę i lokalizację IK • pozwalające zidentyfikować operatora IK: nazwa, adres i siedziba numery REGON, NIP i KRS • pozwalające zidentyfikować zarządzającego przedsiębiorstwem w imieniu operatora IK: nazwa, adres, numery REGON, NIP i KRS • dane służbowe osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami właściwymi w zakresie ochrony IK • obejmujące imię i nazwisko osoby sporządzającej plan	Odwzorowanie charakterystyki IK
Dane IK: • charakterystyka i podstawowe parametry techniczne • plan z naniesieniem lokalizacji obiektów, instalacji lub systemu • połączenia z innymi obiektami, instalacjami, urządzeniami lub usługami	Odwzorowanie charakterystyki IK
Charakterystyka: • zagrożeń dla IK oraz oceny ryzyka ich wystąpienia wraz z przewidywanymi scenariuszami rozwoju zdarzeń • zależności IK od pozostałych systemów IK oraz możliwości zakłócenia jej funkcjonowania w wyniku zakłóceń powstałych w pozostałych systemach IK • zasobów własnych możliwych do wykorzystania w celu ochrony IK • zasobów właściwych terytorialnie organów możliwych do wykorzystania w celu ochrony IK	Odwzorowanie charakterystyki IK
Zasadnicze warianty: • działania w sytuacji zagrożenia lub zakłócenia funkcjonowania IK • zapewnienia ciągłości funkcjonowania IK • odtwarzania IK	Szacowanie ryzyka Generowanie SZN Formułowanie problemu decyzyjnego

Źródło: opracowanie własne na podstawie: Dz.U. 2010 nr 83 poz. 542, § 2, ust. 3.

Tabela 4.4c. Zestawienie elementów PZK z realizującymi je etapami ZS-BIK

Elementy PZK	Etapy metodyki ZS-BIK
Plan główny zawierający: • charakterystykę zagrożeń oraz ocenę ryzyka ich wystąpienia, w tym dotyczących IK oraz mapy ryzyka i mapy zagrożeń • zestawienie sił i środków do wykorzystania w sytuacjach kryzysowych	Odwzorowanie charakterystyki IK Szacowanie ryzyka
Zespół przedsięwzięć na wypadek sytuacji kryzysowych, w tym: • zadania w zakresie monitorowania zagrożeń	Generowanie SZN Formułowanie problemu decyzyjnego
Załączniki funkcjonalne planu głównego określające: • procedury realizacji zadań z zakresu zarządzania kryzysowego, w tym związane z ochroną IK • organizację systemu monitorowania zagrożeń, ostrzegania i alarmowania • organizację ochrony przed zagrożeniami charakterystycznymi dla danego obszaru	Formułowanie problemu decyzyjnego

Źródło: opracowanie własne na podstawie: Dz.U. 2017 poz. 209, art. 5, pkt 2.

Podsumowanie

Celem niniejszego opracowania było przedstawienie wyników badań, które doprowadziły do opracowania integralnego modelu bezpieczeństwa infrastruktury krytycznej (IM-BIK) oraz bazującej na nim metodyki zarządzania sytuacyjnego bezpieczeństwem infrastruktury krytycznej (ZS-BIK), warunkujących efektywną wymianę informacji między podmiotami odpowiedzialnymi za bezpieczeństwo IK na dowolnym poziomie decyzyjnym.

Cel opracowania wskazuje na dwie grupy problemowe:

- integralny model bezpieczeństwa IK (rozdz. 2),
- metodykę zarządzania sytuacyjnego bezpieczeństwem IK (rozdz. 3).

Wyniki uzyskane w pierwszej grupie problemowej IM-BIK są podstawą następujących wniosków:

1. Na kanon charakterystyki IK składają się zasoby, funkcjonalności, zagrożenia i zabezpieczenia – na co wskazują wyniki analizy uwarunkowań formalnoprawnych procesu planowania cywilnego i zarządzania kryzysowego (rozdz. 1.3).
2. Adaptacja modelu sytuacji Kłykowa do kanonu IK pozwoliła na sformułowanie modelu sytuacji IK (rozdz. 2.2), który warunkuje możliwość wykonania metod IM-BIK: szacowania ryzyka, generowania SZN oraz formułowania problemu decyzyjnego.
3. Opracowanie metody szacowania ryzyka (rozdz. 2.3), wykorzystującej autorski wzór na ryzyko, umożliwia podmiotom odpowiedzialnym za bezpieczeństwo IK wnioskowanie na podstawie danych zawartych w modelu sytuacji IK, tj. wskazanie zagrożeń, dla których należy sformułować i rozwiązać problem decyzyjny.
4. Metoda generowania SZN (rozdz. 2.4) pozwala na utworzenie modelu sieci zależności występujących między IK, dzięki czemu możliwe jest wskazanie następstw materializacji zagrożeń oraz weryfikacja, czy model sytuacji IK nie pomija zagrożeń, które mogą oddziaływać na IK.
5. Adaptacja metody powiązanych obszarów decyzyjnych do kanonu IK doprowadziła do opracowania metody formułowania problemów decyzyjnych (rozdz. 2.5), która pozwala podmiotom odpowiedzialnym za bezpieczeństwo IK na wskazanie obszarów decyzyjnych (zagrożeń, na które podatna jest IK), określenie decyzji elementarnych dla każdego obszaru decyzyjnego (wskazanie dostępnych zabezpieczeń lub środków reakcji na zagrożenie) oraz wyznaczenie kombinacji zabezpieczeń, które realizują przyjęty cel (utrzymują przewidywaną dostępność funkcjonalności powyżej progu bezpieczeństwa).

Wyniki uzyskane w drugiej grupie problemowej metodyka ZS-BIK pozwoliły na sformułowanie wniosków praktycznych:

1. W odpowiedzi na potrzeby podmiotów odpowiedzialnych za bezpieczeństwo IK, uwzględniając wnioski z analizy metodyk oceny ryzyka na potrzeby zarządzania kryzysowego stosowane w Polsce, USA, Kanadzie, Australii i wybranych krajach UE, opracowano metodykę ZS-BIK (rozdz. 3.1).
2. Dla metodyki ZS-BIK zaproponowano procedury realizacji dla przypadku płaskiego (rozdz. 3.2) i hierarchicznego (rozdz. 3.3) problemu decyzyjnego – wskazane procedury czynią metodykę ZS-BIK uniwersalną dla podmiotów odpowiedzialnych za bezpieczeństwo IK.
3. Użyteczności metodyki ZS-BIK dla podmiotów odpowiedzialnych za bezpieczeństwo IK wykazano na podstawie przykładu obliczeniowego imitującego płaski problem decyzyjny (rozdz. 4.2), którego wyniki pozwalają pozytywnie ocenić metodykę ZS-BIK w obszarze: określenia charakterystyki rozpatrywanej IK, generowania SZN, formułowania płaskiego problemu decyzyjnego i wskazania zbioru zabezpieczeń, szacowania wartości ryzyka utraty funkcjonalności przed i po zastosowaniu dodatkowych zabezpieczeń.
4. Użyteczność metodyki ZS-BIK dla przypadku hierarchicznego problemu decyzyjnego (rozdz. 4.3) wykazano w eksperymencie obliczeniowym imitujący przypadek, w którym władze powiatu mają zdecydować o wsparciu działań zabezpieczających w dwóch IK funkcjonujących na terenie im podległym, uzyskane wyniki pozwalają pozytywnie ocenić metodykę ZS-BIK w obszarze formułowania problemu decyzyjnego, wskazania zbioru zabezpieczeń oraz szacowania wartości ryzyka utraty funkcjonalności przed i po zastosowaniu dodatkowych zabezpieczeń.

Wskazanie kanonu charakterystyki IK oraz opracowanie składowych IM-BIK stanowi odpowiedź autora na pierwsze pytanie badawcze: Jakie elementy musi zawierać IM-BIK, aby móc stanowić zaplecze narzędziowe dla metodyki ZS-BIK?

Opracowanie metodyki ZS-BIK oraz procedur jej realizacji dla przypadku płaskiego i hierarchicznego problemu decyzyjnego odpowiada na drugie pytanie badawcze: Jakie etapy postępowania powinna zawierać metodyka ZS-BIK, aby umożliwić zarządzanie bezpieczeństwem IK, uwzględniając wszystkie podmioty odpowiedzialne za bezpieczeństwo IK?

Uzyskane wyniki w obu grupach problemowych wskazują, że IM-BIK oraz bazująca na nim metodyka ZS-BIK umożliwia podmiotom odpowiedzialnym za bezpieczeństwo IK zarządzanie sytuacyjne bezpieczeństwem IK.

Bibliografia

Pozycje literaturowe

[1] Abgarowicz, G., 2015. *Pamięć przyszłości. Analiza ryzyka dla zarządzania kryzysowego*. Józefów: Wydawnictwo CNBOP-PIB.

[2] Alcaraz, C., Zeadally, S., 2015. Critical Infrastructure Protection: Requirements and Challenges for the 21st Century. *International Jurnal of Critical Infrastructure Protection.* 8 (2015), ss. 53–66.

[3] AON, 2008. *Słownik terminów z zakresu bezpieczeństwa narodowego – wydanie szóste,* Warszawa: Akademia Obrony Narodowej.

[4] Bizon-Górecka, J., 1998. *Monitoring czynników ryzyka w przedsiębiorstwie.* Bydgoszcz: TNIOK.

[5] Bitkowska, A., 2009. *Zarządzanie procesami biznesowymi w przedsiębiorstwie.* Warszawa: Vizja Press & IT.

[6] Bloomfield, r., Popov, P., Salako, K., et al., 2017. Preliminary Interdependency Analysis: An Approach to Support Critical Infrastructure Risk Assessment. *Reliability Engineering & System Safety*, vol. 167, ss. 198–217.

[7] Bogdanienko, J., 2008. *W pogoni za nowoczesnością. Wybrane aspekty tworzenia i wprowadzania zmian*. Toruń: Towarzystwo Naukowe Organizacji i Kierownictwa.

[8] Bogdanienko, J., 2002. *Zarys koncepcji, metod i problemów zarządzania*. Toruń.

[9] Brzozowska, K., 2009. *Finansowanie inwestycji infrastrukturalnych przez kapitał prywatny na zasadzie Project finance.* Warszawa.

[10] Bolstad, W.M., 2004. *Introduction to Bayesian statistics*. Wiley-Interscience.

[11] Cai, B., Xie, M., Liu, Y., et al. 2017. A Novel Critical Infrastructure Resilience Assessment Approach using Dynamic Bayesian Networks. *Book Series: AIP Conference Proceedings*. Vol. 1890.

[12] Caldwell, B., 2015. Framing, information alignment, and resilience in distributed human coordination of critical infrastructure event response. *6th International Conference on Applied Human Factors and Ergonomics. Book Series: Procedia Manufacturing*. vol. 3, ss. 5095–5101.

[13] Chen, Y., Milanovic, J., 2017. Critical Appraisal of Tools and Methodologies for Studies of Cascading Failures in Coupled Critical Infrastructure Systems. *7th Ieee International Conference on Smart Technologies – Ieee Eurocon 2017 Conference Proceedings*. ss. 599–604.

[14] Galicki, K., Świszcz, G., 2013. Usprawnienie procesu obiegu informacji w systemie zarządzania kryzysowego. *Przegląd Bezpieczeństwa Wewnętrznego,* nr 9(5). ss. 310–319.

[15] Garschagen, M., Sandholz, S., The Role of Minimum Supply and Social Vulnerability Assessment for Govering Critical Infrastructure Failure: Current Gaps and Future Agenda. *Natural Hazards and Earth System Sciences,* vol. 18, ss. 1233–1246.
[16] Edi, M., Rosato, V., 2016. Critical Infrastructure Disruption Scenarios Analyses via Simulation. *Managing The Complexity Of Critical Infrastructures: A Modelling And Simulation Approach*. Book Series: Studies in Systems Decision and Control. vol. 90, ss. 43–61.
[17] Fayol, H., 1916. *General principles of management*. Classics of organization theory.
[18] Fayol, H., 1930. *Administration Industrielle et Generale (Industrial and General Administration)*, London: Sir I. Pitman & Sons, ltd.
[19] Gajda, J., 2017. *Prognozowanie i symulacje w ekonomii i zarządzaniu.* Warszawa: C.H. Beck.
[20] Gierszewska, G., Romanowska, M., 2014. *Analiza strategiczna przedsiębiorstwa.* Warszawa: PWE.
[21] Glinkowska, B., 2012. Kompetencje pracownika a efektywność organizacji, *Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu*, nr 262, ss. 126–133.
[22] Hamrol, A., 1998. *Zarządzanie jakością. Teoria i praktyka*. Warszawa: PWN.
[23] Hatton, T., Brown, C., Kipp, r., et al., 2018. Developing a Model and Instrument to Measure the Resilience of Critical Infrastructure Sector Organisations. *International Journal Of Critical Infrastructures.* vol. 14, issue: 1, ss. 59–79.
[24] Haykin, S., 1994. *Neural networks. A comprehensive foundation*. New York: Macmillan College Publishing Company.
[25] Häyhtiö, M., Zaerens, K., 2017. A Comprehensive Assessment Model for Critical Infrastructure Protection. *Management and Production Engineering.* Vol. 8, nr 4, ss. 42–53.
[26] Hofreiter, L., Zvakova, Z., 2016. Theoretical Aspects of Critical Infrastructure Protection. *Durability of Critical Infrastructure, Monitoring and Testing, ICDCF 2016.* Book Series: Lecture Notes in Mechanical Engineering. ss. 39–147.
[27] Hurley, J., 2017. Quantifying Decision Making in the Critical Infrastructure via the Analytic Hierarchy Process (AHP). *International Journal of Cyber Warfare and Terrorism*. vol. 7, issue: 4, ss. 23–34.
[28] Iwaszkiewicz, A., 2005. *Zarządzanie jakością w przykładach i zadaniach.* Tychy: Śląskie Wydawnictwo Naukowe.
[29] Johansen, C., Tien, I., 2018. Probabilistic multi-scale modeling of interdependencies between critical infrastructure systems for resilience. *Sustainable and Resilient Infrastructure*. vol: 3, issue: 1, ss. 1–15.
[30] Kaczmarek, B, Sikorski, C., 1999. *Podstawy zarządzania – zachowania organizacyjne.* Łódź.
[31] Kaczmarek, T., 2010. *Zarządzanie ryzykiem. Ujęcie interdyscyplinarne.* Warszawa: Difin.
[32] Kaczmarek, T., Ćwiek G., 2009. *Ryzyko kryzysu a ciągłość działania.* Warszawa: Difin.

[33] Kędzierska, M., Banulska, A., Sobór, E., 2014. Zarządzanie kryzysowe w gminach i powiatach – stan faktyczny i oczekiwania w świetle badań ankietowych. *Bezpieczeństwo i Technika Pożarnicza*, vol. 33, issue 1, ss. 129–143.

[34] Kisilowski, J., Pomierny, W., Wojtkiewicz, T., 2014. *Ekspertyza nr 1 dla Wydziału Zarządzania Politechniki Warszawskiej z zakresu identyfikacji i analizy dotyczących Infrastruktury Krytycznej RP*. Warszawa.

[35] Kisilowski, M., Zawiła-Niedźwiecki, J., 2015. Zarządzanie kryzysowe – zagadnienie na styku nauk o bezpieczeństwie oraz nauk o zarządzaniu. *Organizacja i kierowanie*, nr 1, ss. 51–62.

[36] Klimczak, K., 2008. *Pochodzenie ryzyka* W: Stec, I., Zawiła-Niedźwiecki, J., Zarządzanie ryzykiem operacyjnym. Warszawa: C.H. Beck. ss. 11–12.

[37] Kłykow, J., Jurek, J., 1988. *Dialogowo semiotyczne systemy podejmowania decyzji*. Warszawa: PWN.

[38] Kosieradzka, A., Zawiła-Niedźwiecki, J. red., 2016. *Zaawansowana metodyka oceny ryzyka w publicznym zarządzaniu kryzysowym.* Kraków-Legionowo: *edu-Libri*.

[39] Krupa, T., 2006. *Elementy organizacji- zasoby i zadani.* Warszawa: WNT.

[40] Krupa, T., Ostrowska, T., 2012. Decision – Making in Flat and Hierarchical Decision Problems. *Foundations of Management*, vol. 4, no. 2, ss. 23–36.

[41] Krupa, T., Ostrowska, T., 2017. Prakseologiczne aspekty teorii zdarzeń – symetria zagrożeń i podatności. Kieżuń, W., Wołejszo. J. (red.). *Prakseologia w zarządzaniu i dowodzeniu, vol. 3 Ekonomiczność w zarządzaniu*. Kalisz: Państwowa Wyższa Szkoła Zawodowa im. Prezydenta S. Wojciechowskiego.

[42] Krupa, T., Wiśniewski, M., 2015. Situational Management of Critical Infrastructure Resources United Threat. *Foundations of Management*, vol. 7, annual 2015, ss. 93–104.

[43] Kulińska, E., Rut, J., 2016, *Procesy decyzyjne w logistyce i pokrewnych obszarach badawczych*. Opole: Politechnika Opolska.

[44] Kulińska, E., Dornfeld, A., 2009. *Zarządzanie ryzykiem procesów identyfikacja – modelowanie – zastosowanie*. Opole: Politechnika Opolska.

[45] Lidwa, W., 2015. *Zarządzanie kryzysowe.* Warszawa: AON.

[46] Lidwa, W., Krzeszowski, W., Więcek, W., Kamiński, P., 2012. *Ochrona infrastruktury krytycznej.* Warszawa: AON.

[47] Maciąg, A., Tarnowski, I., 2017. Atak teleinformatyczny na polski sektor finansowy. *Biuletyn RCB*, nr 18, ss. 3–8.

[48] Macaulty, T., 2016. *Critical Infrastructure – Understanding its Component Parts, Vulnerabilities, Operating Risk and Interdependencies.* London – New York: CRC Press.

[49] Manas, P., 2017. The Protection of Critical Infrastructure Objects – Technical Principles. *Durability of Critical Infrastructure, Monitoring and Testing, ICDCF 2016*. Book Series: Lecture Notes in Mechanical Engineering. ss. 239–248.

[50] Maracz, T., 1983. *Ujęcie sytuacyjne.* W A. Koźmiński, red., 1983. *Współczesne teorie organizacji*. Warszawa: PWN, ss. 274–310.

[51] Maslow, A., 2016. *Motywacja i osobowość.* Warszawa: Wydawnictwo Naukowe PWN.

[52] Monkiewicz, J., red., 2004. *Podstawy ubezpieczeń.* Warszawa: Poltext.

[53] Obiedzińska, A., Kochanek, K., Kiślowski, M., 2014. *Ekspertyza nr 3 dla Wydziału Zarządzania Politechniki Warszawskiej z zakresu identyfikacji i analizy zagrożeń dotyczących Infrastruktury Krytycznej RP*. Warszawa.
[54] Orlen, 2016. *Raport zintegrowany grupy Orlen 2016.* Płock: Rolen.
[55] Ostrowska, T., Krupa, T., Wiśniewski, M, 2015. Dynamic Hazards in Critical Infrastructure of State. *Foundations of Management*, vol. 7, annual 2015, ss. 143–158.
[56] Ouyang, M., 2014, Review on Modeling and Simulation of Interdependent Critical Infrastructure Systems. *Reliability Engineering* & *System Safety*, vol. 121, ss. 43–60.
[57] Pescaroli, G., Kelman, I., 2017. How Critical Infrastructure Orients International Relief in Cascading Disasters, *Journal Of Contingencies And Crisis Management*. vol. 25, issue: 2, ss. 56–67.
[58] Pescaroli, G., Alexander, D., 2016. Critical infrastructure, panarchies and the vulnerability paths of cascading disasters. *Natural Hazards.* Vol. 82, issue: 1, ss. 175–192.
[59] Pijanowski, S., Marczewski, M., Staniszewski, M., 2014. *Ekspertyza nr 2 dla Wydziału Zarządzania Politechniki Warszawskiej z zakresu identyfikacji i analizy zagrożeń dotyczących Infrastruktury Krytycznej RP wykonana przez zespół ekspertów Resilia Sp. z o.o.* Warszawa.
[60] Pilich, A., 1989. *Encyklopedia Gospodarki Materiałowej*. Warszawa: Państwowe Wydawnictwo Ekonomiczne.
[61] Pursiainen, C., 2018. Critical infrastructure resilience: A Nordic model in the making? *International Journal Of Disaster Risk Reduction*. vol. 27, ss. 632–641.
[62] Pursiainen, C., Road, B., Baker, G., et al. 2017. Critical Infrastructure Resilience Index. *Risk, Reliability And Safety: Innovating Theory And Practice*. ss. 2183–2190.
[63] Puuska, S., Rummukainen, L., Timonen, J., 2018. Nationwide critical infrastructure monitoring using a common operating picture framework. *International Journal of Critical Infrastructure Protection*. vol. 20, ss. 28–47.
[64] Radziejewski, r., 2014. *Ochrona infrastruktury krytycznej – teoria a praktyka.* Warszawa: Wydawnictwo Naukowe PWN.
[65] Rehak, D., Markuci, J., Hromada, M., et al. 2016, Quantitative Evaluation of the Synergistic Effects of Failures in a Critical Infrastructure System. *International Journal of Critical Infrastructure Protection*. vol. 14, ss. 3–17.
[66] Rutkowska, D., Piliński, M., Rutkowski, L., 1999. *Sieci neuronowe, algorytmy genetyczne i systemy rozmyte.* Warszawa: Wydawnictwo Naukowe PWN.
[67] Ruktowski, C., 1995. *Bezpieczeństwo i obronność: strategie – koncepcje – doktryny*. Warszawa.
[68] Skomra, W., 2017. Risk Management as Part of Crisis Management Tasks. *Foundations of Management*, vol. 9, annual 2017, ss. 245–256.
[69] Skomra, W., 2015. *Metodyka oceny ryzyka na potrzeby systemu zarządzania kryzysowego RP.* Warszawa.
[70] Siderska, J., 2013. Analiza możliwości zastosowania sieci neuronowych do modelowania wartości kapitału społecznego w firmach IT. *Economics and Management*. nr 1, ss. 84–97.

[71] Sobolewski, G., 2010. *Zarządzanie kryzysowe wobec współczesnych wyzwań i zagrożeń.* W: E. Sobczak (red.), 2010. *Nowe wyzwania i wykorzystanie współczesnej nauki w zarządzaniu kryzysowym*. Warszawa: WAiNS PW. ss. 45–58.

[72] Stabryła, A. Trzcieniecki, J., (red.), 1986. *Organizacja i zarządzanie. Zarys problematyki.* Kraków: Akademia Ekonomiczna w Krakowie.

[73] Staniec, I., Zawiła-Niedźwiecki, J. red., 2008. *Zarządzanie ryzykiem operacyjnym.* Warszawa: C.H. Beck.

[74] Stec, K., 2011. *Wybrane prawne narzędzia ochrony infrastruktury krytycznej w Polsce.* Bezpieczeństwo Narodowe, nr 19, ss. 181–197.

[75] Stergiopoulos, G., Kotzanikolaou, P., Theocharidou, M., et al. 2016. Time-based critical infrastructure dependency analysis for large-scale and cross-sectoral failures. *International Journal Of Critical Infrastructure Protection*. vol. 12, ss. 46–60.

[76] Szewczyk, T., Pyznar, M., 2010. Ochrona infrastruktury krytycznej a zagrożenia symetryczne. *Przegląd Bezpieczeństwa Wewnetrznego,* nr 2 (2) 2010, ss. 53–59.

[77] Szwarc, K., 2014. *Technologia teleinformatyczna w zarządzaniu kryzysowym.* W: W. Chmielarz, J. Kisielnicki, T. Paarys, 2014. *Informatyka 2 przyszłości*. Warszawa: Wydawnictwo Naukowe Wydziału Zarządzania UW. ss. 123–136.

[78] Targalski, J., 1986. Podejmowanie decyzji. Stabryła, A., Trzcieniecki, J. (red.). *Organizacja i zarządzanie.* Warszawa.

[79] Tien, I., Kiureghian, A., 2017. Reliability Assessment of Critical Infrastructure Using Bayesian Networks. *Journal of Infrastructure Systems*. vol. 23, issue: 4.

[80] Trajer, J., Paszek, A., Iwan, S., 2012. *Zarządzanie wiedzą*. Warszawa: PWE.

[81] Tyburska, A., Nalepski, M., 2008. *Ochrona infrastruktury krytycznej.* Szczytno.

[82] Tyburska, A., 2009. Ochrona infrastruktury krytycznej – potrzeby edukacyjne. W: T. Białas, M. Grzybowski, J. Tomaszewski, 2009. *Zarządzanie bezpieczeństwem w sektorze publicznym i biznesie*. Gdynia. ss. 83–102.

[83] Tyburska, A., 2011. Policja a ochrona infrastruktury krytycznej. *Zeszyty naukowe WSOWL*, nr 3, ss. 143–162.

[84] Winiarski, J., 2007. Zarządzanie ryzkiem w przedsięwzięciach informatycznych. *Polskie Stowarzyszenie Zarządzania Wiedzą: Studia i Materiały,* nr 8., ss. 181–190.

[85] Wiśniewski, M., 2015. *Doskonalenie zarządzania kryzysowego z wykorzystaniem zarządzania wiedzą i jego informatycznych narzędzi.* Logistyka: czasopismo dla profesjonalistów, nr 4/2015, ss. 8511–8521.

[86] Wiśniewki, M., 2016a. Autorska koncepcja sytuacyjnych modeli: zasobu IK, procesów podejmowania decyzji oraz szacowania ryzyka i kompensacji zagrożeń. *Studia i Materiały „Miscellanea Oeconomicae*", nr 1/2016, UJK, ss. 429–444.

[87] Wiśniewski, M., 2016b. Concept of Situational Management of Safety Critical Infrastructure of State. *Foundations of Management*, vol. 8, 2016, ss. 297–310.

[88] Wiśniewski, M., Kisilowski, M., Marczewski, M., 2016. *Zasady budowy scenariuszy zdarzeń niekorzystnych w publicznym zarządzaniu kryzysowym.* W: M. Ćwiklicki, M. Jabłoński, S. Mazur, 2016. *Współczesne koncepcje zarządzania publicznego. Wyzwania modernizacyjne sektora publicznego*, Kraków: Fundacja GAP, ss. 97–110.

[89] Wiśniewski M., Ostrowska T., 2016. *Wyzwania i dobre praktyki zarządzania bezpieczeństwem infrastruktury krytycznej.* W: M. Ćwiklicki, M. Jabłoński, S. Mazur, 2016. *Współczesne koncepcje zarządzania publicznego. Wyzwania modernizacyjne sektora publicznego*, Kraków: Fundacja GAP. ss. 111–125.
[90] Wójtowicz, W, 2006. *Bezpieczeństwo infrastruktury krytycznej.* Warszawa: Departament Polityki Obronnej MON.
[91] Wróblewski, D., (red.), 2015. *Zarządzanie ryzykiem – przegląd wybranych metodyk*. Józefów: Wydawnictwo CNBOP-PIB.
[92] Zasadzińska-Baraniewska, A., 2017. Zarządzanie kryzysowe wobec nowego typu zagrożeń – spotkanie eksperckie w Rządowym Centrum Bezpieczeństwa. *Biuletyn RCB*. Nr 19.
[93] Zadeh, L., A., Fuzzy sets. *International and Control*. nr 8 (3), ss. 338–353.
[94] Zawiła-Niedźwiecki, J., 2013. *Zarządzanie ryzykiem operacyjnym w zapewnianiu ciągłości działania organizacji.* Kraków: edu-Libri.
[95] Zieliński, E., 2001. *Administracja rządowa w Polsce*. Warszawa.

Akty prawne/plany

[96] *A Framework for Major Emergency Management, A Guide to Risk Assessment In Major Emergency Management,* 2010. Irlandia: Department of the Environment, Heritage and Local Government.
[97] *All Hazards Risk Assessment Methodology Guidelines*, 2013. Kanada: Defence Research and Development Canada.
[98] *Biała księga bezpieczeństwa narodowego RP*, 2013. Warszawa: Biuro Bezpieczeństwa Narodowego.
[99] *Decyzja Parlamentu Europejskiego i Rady Nr 1313/2013/EU z dnia 17 grudnia 2013 r. w sprawie Unijnego Mechanizmu Ochrony Ludności* (Dz.U.UE. 2013 nr 347 poz. 924).
[100] *Dyrektywa Rady 2008/114/WE z dnia 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceeny potrzeb w zakresie jej ochrony* (Dz.U.UE 2008 nr 345 poz. 75).
[101] *Dyrektywa Parlamentu Europeiskiego I Rady (UE) 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii.* (Dz.U.UE 2016 nr 194 poz. 1).
[102] *Europeiska strategia bespieczeństwa,* 2003. Bruksela: Rada Europejska.
[103] *Europejski Program Ochrony Infrastruktury Krytycznej*, 2006. Rada Europejska.
[104] *Guide to Risk and Vulenerability Analyses*, 2012. Szwecja: Swedish Civil Contingencies Agency.
[105] *Method of Risk Analysis for Civil Protection*, 2011. Niemcy: Federal Office of Civil Protection and Disaster Assistance.
[106] *Multi Hazard Identification and Risk Assessment A Cornerstone of the National Mitigation Strategy,* 1997. U.S.A: Federal Emergency Management Agency.
[107] *Norma PN-EN ISO 31000:2012 Zarządzanie ryzykiem – Zasady i wytyczne.*
[108] *Norma ISO/IEC 31010 – Praktyczne metody oceny ryzyka.*

[109] *Narodowy Program Ochrony Infrastruktury Krytycznej*, 2015. Warszawa: Rządowe Centrum Bezpieczeństwa.
[110] *National Emergency Risk Assessment Guidelines*, 2015. Australia: Australian Institute for Disaster Resilience.
[111] *Procedura opracowywania raportu cząstkowego do raportu o zagrożeniach bezpieczeństwa narodowego*, 2010. Warszawa: Rządowe Centrum Bezpieczeństwa.
[112] *Rozporządzenie Ministra Nauki i Szkolnictwa Wyższego z dnia 4 stycznia 2011 r. w sprawie sposobu zarządzania przez Narodowe Centrum Badań i Rozwoju realizacją badań naukowych lub prac rozwojowych na rzecz obronności i bezpieczeństwa państwa* (Dz.U. 2011 nr 18 poz. 91).
[113] *Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 513/2014 z dnia 16 kwietnia 2014 r. ustanawiające, w ramach Funduszu Bezpieczeństwa Wewnętrznego, instrument na rzecz wsparcia finansowego współpracy policyjnej, zapobiegania i zwalczania przestępczości oraz zarządzania kryzysowego oraz uchylające decyzję Rady 2007/125/WSiSW.* (Dz.U.UE 2014 nr 150 poz. 93).
[114] *Rozporządzenie Prezesa Rady Ministrów z dnia 14 lipca 2010 r. w sprawie pełnomocnika do spraw ochrony infrastruktury krytycznej* (Dz.U. 2010 nr 135, poz. 906).
[115] *Rozporządzenie Rady Ministrów z dnia 27 kwietnia 2004 r. w sprawie przygotowania systemu kierowania bezpieczeństwem narodowym* (Dz.U. 2004 nr 98 poz. 978).
[116] *Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie planów ochrony infrastruktury krytycznej* (Dz.U. 2010 nr 83 poz. 542).
[117] *Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie Raportu o zagrożeniach bezpieczeństwa narodowego* (Dz.U. 2010 nr 83 poz. 540).
[118] *Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 w sprawie Narodowego Programu Ochrony Infrastruktury Krytycznej* (DZ.U. 2010 nr 83, poz. 541).
[119] *Strategia bezpieczeństwa narodowego RP*, 2014. Warszawa: Biuro Bezpieczeństwa Narodowego.
[120] *Strategia rozwoju kraju 2020*, 2012. Warszawa: Ministerstwo Rozwoju Regionalnego.
[121] *Strategia rozwoju systemu bezpieczeństwa narodowego RP 2022*, 2013. Warszawa: Ministerstwo Obrony Narodowej.
[122] *Strategia sprawne państwo 2020*, 2013. Warszawa: Ministerstwo Cyfryzacji.
[123] *Swedish National Risk Assessment 2012*, 2013. Szwecja: Swedish Civil Contingency Agency.
[124] *Ustawia z dnia 22 sierpnia 1997 r. o ochronie osób i mienia* (Dz.U. 1997 nr 114, poz. 740).
[125] *Ustawa z dnia 26 kwietnia 2007 roku o zarządzaniu kryzysowym* (Dz.U. 2017, poz. 209).
[126] *Ust*awa z dnia 18 marca 2010 r. o szczególnych uprawnieniach ministra właściwego do spraw energii oraz ich wykonywaniu w niektórych spółkach kapitałowych lub grupach kapitałowych prowadzących działalność w sektorach energii elektrycznej, ropy naftowej oraz paliw gazowych (Dz.U. 2010 Nr 65 poz. 404).
[127] *Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych* (Dz.U. 2016, poz. 904).
[128] *Using HAZUS-MH for Risk Assessment,* 2004. U.S.A: International Decade for Natural Disaster Reduction.

[129] *Working with Scenarios, Risk Assessment and Capabilities in the National Safty and Security Strategy of Netherlands*, 2009. Holandia: Ministry of Security and Justice.
[130] *Zielona Księga w sprawie Europejskiego Programu Ochrony Infrastruktury Krytycznej,* 2005. Komisja Wspólnot Europejskich.

Źródła internetowe

[131] Fendolite MII <www.strazak.waw.pl/zabezpieczenie-ognioochronne-tunelach--rafineriach/rafinerie-zaklady-petrochemiczne/> [dat odczytu 04.04.2018 r.].
[132] *Grupa orlen*, <www.orlen.pl/PL/OFirmie/StrukturaGrupyORLEN/Strony/default.aspx?pl> [data odczytu 13.02.2018 r.].
[133] Korzeniowska, S., *Cyberbezpieczeństwo Infrastruktury Krytycznej*, LSW – Leśnodorski Ślusarek i Wspólnicy. Dostępne <www.lsw.com.pl> [data odczytu 29.08.2016 r.].
[134] Lotos – Informacja o występujących zagrożeniach <m.*odpowiedzialny.lotos.pl/repository/39634/*> [data odczytu 04.04.2018 r.].
[135] *Plan Zarządzania Kryzysowego Powiatu Płockiego*, <powiat-plock.pl/attachments/article/44/powiatowy_plan_zk_sp_plock.pdf>, [data odczytu 28.12.2017 r.].
[136] Stefanowski, J., *Sztuczne sieci neuronowe*. www.cs.put.poznan.pl/jstefanowski/aed/TPDANN.pdf, [data odczytu 14.11.2017 r.].
[137] *Terminal-LNG*, <gaz-system.pl/terminal-lng/finansowanie> [data odczytu 7.06.2017].
[138] *Veturilo nie działa* <warszawa.naszemiasto.pl/artykul/veturilo-nie-dziala-padly--serwery-zdjecia,1891508,artgal,t,id,tm.html > [data odczytu: 07.08.2017 r.].
[139] UEEX <www.iturri.com/pl/rozwiazania/rozwiazania-przeciwpozarowe/rozwiazania-przeciwpozarowe-w-przemysle> [data odczytu 04.04.2018 r.].
[140] Woityto, D., Kulma, W., 2017. Zastosowanie systemów informatycznych do dokumentowania zdarzeń kryzysowych < http://www.ptzp.org.pl/files/konferencje/kzz/artyk_pdf_2017/T2/t2_800.pdf >, [data odczytu 13.07.2017 r.].
[141] www.encyklopedia.pwn.pl [data odczytu 17.03.2017 r.].

Tezaurus pojęć[122]

administracja publiczna – całokształt struktur organizacyjnych w państwie oraz ludzi zatrudnionych w tych strukturach spełniających zadania publiczne, zbiorowe i indywidualne, reglamentacyjne i świadczące oraz organizatorskie podmiotów kierowniczych i decyzyjnych [Zieliński, 2001, s.12]

administracja samorządowa – terenowa reprezentacja lokalnych grup społecznych, które zgodnie z przepisami mają samodzielnie realizować funkcje administracji publicznej [AON, 2008, s. 6]

agregacja – kombinacja kilku rodzajów ryzyka przeprowadzania opisowo w celu uzyskania szerszego spojrzenia na całość ryzyka lub wartościowo w celu określenia łącznej wartości oceny ryzyka [Kosieradzka, Zawiła-Niedźwiecki, 2016, s. 359]:

- **agregacja pozioma** – realizowana w celu przewidywania skutków wystąpienia SZN.
- **agregacja pionowa** – realizowana w celu wyznaczania zakresu odpowiedzialności i współdziałania szczebli administracji publicznej w zarządzaniu kryzysowym

analiza ryzyka – metoda badania procesów polegająca na rozpatrywaniu związków zachodzących między poszczególnymi elementami tych procesów, potencjalnych skutków oraz prawdopodobieństwa ich wystąpienia [Kosieradzka, Zawiła-Niedźwiecki, 2016, s. 359]

akceptowalna wartość ryzyka – wartość ryzyka, przy którym podmioty odpowiedzialne za bezpieczeństwo IK nie podejmują dalszych działań zmierzających do ograniczenia ryzyka lub jego eliminacji. Wartość ta stanowi różnicę pomiędzy bieżącą dostępnością funkcjonalności IK a wyznaczonym dla niej progiem bezpieczeństwa.

akt normatywny – tekst zawierający sformułowane w języku prawnym i zapisane w postaci przepisów normy prawne. Normy te mają najczęściej charakter generalny i abstrakcyjny. Niekiedy pod tym pojęciem rozumie się także wszelkie teksty formułujące normy postępowania. Wydają je podmioty, które mają kompetencje do działań prawotwórczych [encyklopedia.pwn.pl; data odczytu 17.03.2017]

bazowy problem decyzyjny – problem decyzyjny wynikający z modelu sytuacji IK lub SZN dla którego wskazano zbiór zabezpieczeń, który to zbiór zabezpieczeń poddawany jest weryfikacji pod względem skuteczności

[122] Definicje pojęć niezawierające wskazania źródła zostały sformułowane przez autora na potrzeby rozprawy w ramach realizacji projektu pt. Metodyka oceny ryzyka na potrzeby systemu zarządzania kryzysowego RP.

bezpieczeństwo – stan, w którym ludzie (społeczeństwo) mają pewność, że nie zagrażają im żadne negatywne zdarzenia spowodowane przyczynami losowymi (naturalnymi) lub nielosowymi (celowymi), które stanowiłyby przeszkodę do stabilnego rozwoju i normalnej egzystencji [Sobolewski, 2010]

bezpieczeństwo fizyczne – zespół działań proceduralnych, organizacyjnych i technicznych mających na celu minimalizację ryzyka zakłócenia funkcjonowania IK w następstwie działań osób, które w sposób nieautoryzowany podjęły próbę dostania się lub znalazły się na terenie IK. Składają się na nie m.in. bezpośrednia ochrona fizyczna oraz zabezpieczenia techniczne (elektroniczne i mechaniczne) [NPOIK, 2015, zał. 1, s. 22]

bezpieczeństwo IK – stan powstały w wyniku zastosowania zabezpieczeń przed zagrożeniami, w którym ryzyko utraty funkcjonalności jest niższe niż wynika to z akceptowanej wartości ryzyka jej utraty

bezpieczeństwo narodowe – jedna z podstawowych dziedzin funkcjonowania (aktywności) państwa, mająca zapewnić możliwości przetrwania, ale przede wszystkim rozwoju i swobody realizacji interesów narodowych w konkretnym środowisku (warunkach) bezpieczeństwa, poprzez podejmowanie wyzwań, wykorzystywanie szans, redukowanie ryzyka oraz przeciwdziałanie wszelkiego rodzaju zagrożeniom dla jego interesów [AON, 2008, s. 17]

bezpieczeństwo publiczne – stan na obszarze państwa powstały w wyniku zorganizowanej obrony i ochrony osób i mienia przed zagrożeniami na lądzie, morzu i w powietrzu [AON, 2008, s. 19]

bezpieczeństwo osobowe – zespół przedsięwzięć i procedur mających na celu minimalizację ryzyka związanego z osobami, które przez autoryzowany dostęp do obiektów, urządzeń, instalacji i usług infrastruktury krytycznej mogą spowodować zakłócenia w jej funkcjonowaniu [NPOIK, 2015, zał. 1, s. 59]

bezpieczeństwo prawne – zespół przedsięwzięć mających na celu minimalizację ryzyka związanego z działalnością osób fizycznych lub innych podmiotów gospodarczych (państwowych lub prywatnych), których działania mogą prowadzić do zakłócenia w funkcjonowaniu obiektów, urządzeń, instalacji i usług IK [NPOIK, 2015, zał. 1, s. 113]

bezpieczeństwo techniczne – zespół działań organizacyjnych i technicznych mających na celu minimalizację ryzyka zakłócenia funkcjonowania IK w następstwie zaburzenia realizowanych procesów technologicznych [NPOIK, 2015, zał. 1, s. 42]

bezpieczeństwo teleinformatyczne – zespół działań organizacyjnych i technicznych mających na celu minimalizację ryzyka zakłócenia funkcjonowania IK w następstwie nieautoryzowanego oddziaływania na aparaturę kontrolną oraz systemy i sieci teleinformatyczne, włączając w to akty szeroko rozumianej cyberprzestępczości i cyberterroryzmu a także przypadkowych (niecelowych) działań użytkowników [NPOIK, 2015, zał. 1, s. 67]

brak bezpieczeństwa IK – występuje, gdy prognozowana dostępność funkcjonalności IK spada poniżej progu bezpieczeństwa

ciągłość działania – zdolność organizacji do przewidywania i reagowania na incydenty i zakłócenia w prowadzonej działalności w celu jej kontynuowania na akceptowalnym poziomie [Staniec, Zawiła-Niedźwiecki, 2008, s. 261]

cel zarządzania kryzysowego – zapobieganie sytuacjom kryzysowym, przygotowanie do przejmowania nad nimi kontroli w drodze zaplanowanych działań, reagowanie w przypadku wystąpienia sytuacji kryzysowych, usuwanie ich skutków oraz odtwarzanie zasobów i infrastruktury krytycznej [Dz.U. 2013 poz. 1166, art. 2]

cykl planowania – to okresowe realizowanie etapów: analizowania, programowania, opracowywania planu lub programu, jego wdrażanie, testowanie i uruchamianie [Dz.U. 2013 poz. 1166, art. 3, pkt 7]

dane – to zapis faktów, obrazów, tekstów i dźwięków, umożliwiający ich następne odtwarzanie i przetwarzanie, w tym również technikami komputerowymi [Trajer, Paszek, Iwan, 2012]

dane obligatoryjne – wymagane obowiązującymi przepisami prawnymi, które należy zgromadzić lub do których należy się odnieść, proponując działania ochronne dla IK, w postaci PZK lub POIK

dane opcjonalne – wynikające z dokumentów planistycznych, tj. strategii, programów, itp., które wskazują kierunki rozszerzenia zbioru danych obligatoryjnych

dostępność funkcjonalności – stopień, w jakim społeczeństwo może skorzystać z usługi /produktu zapewnianego przez rozpatrywany zasób, system

decyzja – zbiór decyzji elementarnych po jednej z każdego obszaru decyzyjnego w ramach rozpatrywanego problemu decyzyjnego [Krupa, Ostrowska, 2012, s. 25]

decyzja dopuszczalna – rozwiązanie problemu decyzyjnego niezawierające par sprzecznych decyzji elementarnych [Krupa, Ostrowska, 2012, s. 26]

decyzja elementarna – element obszaru decyzyjnego niepodlegający dalszej dekompozycji i będący jego niepowtarzalnym rozwiązaniem w granicach całego problemu decyzyjnego (np. zabezpieczenie przed określonym zagrożeniem) [Krupa, Ostrowska, 2012, s. 26]

działanie korygujące – działanie podejmowane w wyniku stwierdzenia niezgodności, polegające na wprowadzaniu zmian, które uniemożliwiają lub ograniczają skutki powtórnego wystąpienia zagrożenia [Kosieradzka, Zawiła-Niedźwiecki, 2016, s. 360]

europejska IK – należy przez to rozumieć systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia i instalacje kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców, wyznaczone w systemach infrastruktury krytycznej w zakresie energii elektrycznej, ropy naftowej i gazu ziemnego oraz transportu drogowego, kolejowego, lotniczego, wodnego śródlądowego, żeglugi oceanicznej, żeglugi morskiej bliskiego zasięgu i portów, zlokalizowane na terytorium państw członkowskich Unii Europejskiej, których zakłócenie lub

zniszczenie miałoby istotny wpływ na co najmniej dwa państwa członkowskie [Dz.U. 2017 poz. 209 , art. 3]

funkcja – własność związana zastosowaniem, przeznaczeniem lub zadaniem z obiektem, urządzeniem lub osobą [Fayol, 1930]

funkcje zarządzania – zespoły czynności, jakie pełni zarządzanie w każdej organizacji. wyróżnia się cztery funkcje [Fayol, 1916, s. 15]:

- planowanie i podejmowanie decyzji – plany wyznaczają cele organizacji, programy jej działania i określają sposób ich osiągnięcia. Podejmowanie decyzji wymaga dokonywania wyborów pomiędzy celami, posiadanymi zasobami i możliwościami realizacji zadań,
- organizowanie – zaprojektowanie i wdrożenie działań, które zapewnią skuteczne wykonanie planów, np.: zapewnienie obsady na stanowiskach pracy, dobór środków realizacji zadań, budowanie relacji z otoczeniem, budowanie struktur organizacyjnych,
- realizacja – motywowanie i pobudzanie członków organizacji do działania,
- kontrolowanie – określanie mierników efektywności, pomiaru bieżącej efektywności i porównania jej z wyznaczonymi miernikami, podjęcia działań korygujących, jeśli są konieczne

funkcjonalność – zdolność zasobu do zaspokajania potrzeb użytkownika w określonych warunkach

Grupa Orlen – grupa firm wchodzących w skład PKN Orlen S.A., w tym m.in.: rafineria PKN Orlen S.A w Płocku, Basell Orlen Polyolefins sp. z o.o., Zakład Produkcyjny Orlen Oil sp. z o.o. w Płocku [Grupa Orlen, data odczytu 13.02.2018]

hierarchiczny problem decyzyjny – zbiór obszarów decyzyjnych wyznaczonych przez zagrożenia, na które podatna jest IK, których ryzyko nie pozwala na osiągnięcie założonego progu bezpieczeństwa, dla których rozstrzygnięcie o zabezpieczeniach nie zapada na jednym poziomie decyzyjnym – zagrożenia są wyznaczane na podstawie sytuacji rozpatrywanej IK lub SZN

incydent – zdarzenie będące efektem spełnienia się zagrożenia, mające negatywne skutki dla organizacji lub procesu [Kosieradzka, Zawiła-Niedźwiecki, 2016, s. 362]

infrastruktura – to urządzenia, budynki, sieci komunikacyjne, systemy i instytucje usługowe niezbędne do należytego funkcjonowania społeczeństwa i produkcyjnych działów gospodarki.

infrastruktura krytyczna (IK) – to systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców [Dz.U. 2013 poz. 1166, art. 3, pkt 2]

infrastruktura państwa – to główne obiekty, instalacje i urządzenia stałe wraz z instytucjami usługowymi utrzymujące je w sprawności technicznej, niezbędne do należytego

funkcjonowania produkcyjnych działów gospodarki oraz życia (w tym bezpieczeństwa) ludności kraju [AON, 2008, s. 56]

infrastruktura publiczna – to dobra publiczne majce charakter dóbr podstawowych, o strategicznym znaczeniu dla całej gospodarki i społeczeństwa, umożliwiające przemieszczanie mediów (energii, pojazdów, wody, informacji), osób i rzeczy, udostępniane bezpłatnie lub za odpłatnością, częściową, pozostające w gestii władz publicznych (państwowych lub lokalnych), na których spoczywa obowiązek tworzenia infrastruktury i utrzymania jej w odpowiednim stanie [Brzozowska, 2009, s. 18]

instalacja technologiczna – zestaw urządzeń służących do przesyłania mediów takich jak prąd elektryczny, woda, gaz ziemny, paliwo, ścieki czy inne substancje. Na instalację składają się zwykle elementy liniowe odpowiednie do transportu danego medium takie jak rury czy przewody elektryczne oraz dodatkowe elementy służące do monitorowania i sterowania przepływem medium, tj. pompy, zawory, liczniki, bezpieczniki i inne

instalacja pianowa – instalacja technologiczna rozpylająca pianę gaśniczą, która odcina dopływ powietrza do ogniska pożaru, powodując jego wygaszanie

integralność – występuje, gdy dane dotyczące kanonu IK stanowią dane wejściowe dla metod IM-BIK. Natomiast wprowadzenie przez podmiot odpowiedzialny za bezpieczeństwo IK nowych zabezpieczeń definiuje zmianę sytuacji IK

integralny model bezpieczeństwa IK – zbiór pojęć umożliwiający modelowe odwzorowanie sytuacji IK należącej do dowolnego systemu IK, rozpoznanie przebiegu zdarzeń niekorzystnych, oszacowanie ryzyka wynikającego z zagrożeń, na które podatna jest IK oraz określenie problemu decyzyjnego dotyczącego zabezpieczeń IK przed rozpoznanymi zagrożeniami

interesariusz wewnętrzny – osoby lub jednostki organizacyjne nadzorujące funkcjonowanie zasobów, od sprawności których zależą funkcjonalności IK [Kosieradzka, Zawiła-Niedźwiecki, 2016, s. 363]

interesariusz zewnętrzny – jednostki administracji publicznej oraz służby powołane do niesienia pomocy wskazane w aktach normatywnych związane z opracowaniem planów ochrony IK [Kosieradzka, Zawiła-Niedźwiecki, 2016, s. 363]

kanon IK – podstawowy zbiór obszarów charakteryzujących sytuację dowolnej IK, tj. zasoby składowe, realizowane funkcjonalności, zagrożenia, na które podatne są zasoby i stosowane zabezpieczenia

katastrofa – dowolna sytuacja, która ma lub może mieć poważne negatywne skutki dla ludzi, środowiska naturalnego lub mienia, w tym dziedzictwa narodowego [Kosieradzka, Zawiła-Niedźwiecki, 2016, s. 363]

klaster – zbiór zasobów/obiektów tego samego typu

kompetencje – ogół wiedzy, umiejętności, doświadczeń, postaw i gotowości pracownika do działania w danych warunkach [Glinkowska, 2012, s. 126–133]

krotka – rozwiązanie problemu decyzyjnego zawierające liczbę i decyzji elementarnych $M_{\alpha,\beta,\lambda}$ równą liczbie j obszarów decyzyjnych $Z_{\alpha,\beta}$ (po jednej decyzji elementarnej z każdego obszaru decyzyjnego). Krotki są wyznaczane na podstawie iloczynu kartezjańskiego wszystkich obszarów decyzyjnych $Z_{\alpha,\beta}$

kryzys – nieakceptowany stan rozpatrywanej IK, który polega na ograniczeniu dostępności funkcjonalności IK [Kosieradzka, Zawiła-Niedźwiecki, 2016, s. 363]

luka informacyjna – to rozbieżność między danymi niezbędnymi do pełnego opisu zjawiska a informacjami dostępnymi w danym momencie [Bogdanienko, 2002, s. 150]

mapa ryzyka – to mapa lub opis przedstawiający potencjalnie negatywne skutki oddziaływania zagrożenia na ludzi, środowisko, mienie i infrastrukturę [Dz.U. 2013 poz. 1166, art. 3, pkt 10]

mapa zagrożenia – to mapa przedstawiająca obszar geograficzny objęty zasięgiem zagrożenia z uwzględnieniem różnych scenariuszy zdarzeń [Dz.U. 2013 poz. 1166, art. 3, pkt 9]

materializacja zagrożenia – to fizyczne wystąpienie zagrożenia, mające skutki dla rozpatrywanego obiektu

metoda ekspercka – metoda polegająca na podejmowaniu decyzji na podstawie doświadczeń i opinii ekspertów z danej dziedziny [Kosieradzka, Zawiła-Niedźwiecki, 2016, s. 111]

metoda symulacyjna – dokonywanie na podstawie danego modelu obliczeń, które stanowią podstawę do wnioskowania o zachowaniu się opisywanego przez model sytemu [Gajda, 2017, ss. 16–20]

metodyka zarządzania sytuacyjnego bezpieczeństwem IK – zbiór etapów pozwalających na: określnie sytuacji IK, oszacowanie wartości ryzyka wynikającego z sytuacji IK oraz sformułowanie problemu decyzyjnego mającego na celu wskazać zabezpieczenia utrzymujące dostępność funkcjonalności powyżej progu bezpieczeństwa, gdzie wyniki uzyskane z wykonania etapu poprzedzającego stanowią dane wejściowe dla kolejnego etapu

model – zbiór elementów rzeczywistości przyjętych jako istotne dla danego zagadnienia oraz reguł, które nim rządzą [Kosieradzka, Zawiła-Niedźwiecki, 2016, s. 364]

model sytuacji IK – obejmuje elementy kanonu IK rozszerzone o zbiór wzbudzanych zagrożeń oraz zależności z innymi obiektami

model zabezpieczeń – uporządkowany zgodnie z celami zarządzania kryzysowego zbiór zasobów i/lub procedur obniżających podatność zasobu IK na zagrożenie w ramach wymaganych przepisami prawa obszarów ochrony IK

monitoring parametrów technologicznych – obserwacja stanu parametrów, związanych z technologią wytwarzania produktów ropopochodnych, w poszukiwaniu wartości zagrażających monitorowanej instalacji

monitoring stanu napełnienia zbiorników – system czujników chroniący przed nadmiernym wypełnieniem zbiornika przechowującego produkty petrochemiczne, które może doprowadzić do jego uszkodzenia np. rozszczelnienia

niepewność – polega na tym, że obserwator dowolnego zjawiska, w danym miejscu i czasie, nie może być pewien dalszego biegu tego zjawiska. Stopień niepewności jest związany z mechanizmem zjawiska, które zawsze jest przypadkowe, a z perspektywy człowieka lub systemu będącego wytworem ludzkim, jest związany z niedoskonałością percepcji czynników zjawiska, właściwą specyfice subiektywnego postrzegania przez człowieka [Zawiła-Niedźwiecki, 2013, s. 33]

niezawodność – własność obiektu mówiąca o tym, czy funkcjonuje on poprawnie (spełnia wszystkie funkcje) przez wymagany czas i w określonych warunkach eksploatacji [Iwaszkiewicz, 2005, ss. 27–30]

ocena ryzyka – proces obejmujący wyznaczenie wartości ryzyka zgodnie z przyjętym modelem oraz metodami kalkulacji, a kończący się analizą tych wartości skutkującą akceptacją lub odrzuceniem ryzyka [Kosieradzka, Zawiła-Niedźwiecki, 2016, s. 365]

odporność – zdolność obiektu do realizacji funkcjonalności przy oddziaływaniu zakłóceń

obszary, obiekty, urządzenia, transporty podlegające obowiązkowej ochronie – to obszary, obiekty, urządzenia i transporty ważne dla obronności, interesu gospodarczego państwa, bezpieczeństwa publicznego i innych ważnych interesów państwa, które podlegają obowiązkowej ochronie przez specjalistyczne uzbrojone formacje ochronne lub odpowiednie zabezpieczenie techniczne [Dz.U. 1997 nr 114 poz. 740, art. 5, ust. 1]

obszar decyzyjny – zbiór wzajemnie alternatywnych decyzji elementarnych [Krupa, Ostrowska, 2012, s. 26]

obszary ochrony IK – bezpieczeństwo fizyczne, bezpieczeństwo techniczne, bezpieczeństwo osobowe, bezpieczeństwo teleinformatyczne, bezpieczeństwo prawne, ciągłość działania [NPOIK, 2015, zał. 1, s. 5]

obwałowanie zbiornika – sposób zabezpieczenia wałami ziemnymi zbiorników przechowujących produkty petrochemiczne przed niekontrolowanym rozprzestrzenianiem powstałych wycieków

ochrona IK – to wszelkie działania zmierzające do zapewnienia funkcjonalności, ciągłości działań i integralności infrastruktury krytycznej w celu zapobiegania zagrożeniom, ryzykom lub słabym punktom oraz ograniczenia i neutralizacji ich skutków oraz szybkiego odtworzenia tej infrastruktury na wypadek awarii, ataków oraz innych zdarzeń zakłócających jej prawidłowe funkcjonowanie [Dz.U. 2013 poz. 1166, art. 3, pkt 3]

odporność – niewrażliwość na działanie niekorzystnych czynników (np. zagrożeń) [Pilich, 1989, s. 326]

okładziny ognioodporne – materiały stosowane w urządzeniach, instalacjach przeznaczonych do pracy w wysokiej temperaturze lub w obecności ognia

operator IK – właściciel oraz posiadacz samoistny i zależny obiektów, instalacji, urządzeń i usług infrastruktury krytycznej [§ 1, Dz.U. Nr 83, poz. 541], operatorami IK są zarówno podmioty prywatne, podmioty stanowiące własność państwa, jak i sama administracja [NPOIK, 2013, s. 9]

planowanie cywilne – działania mające na celu przygotowanie administracji publicznej do zarządzania kryzysowego, planowania w zakresie wspierania Sił Zbrojnych Rzeczpospolitej Polskiej w razie ich użycia oraz planowanie wykorzystania Sił Zbrojnych Rzeczpospolitej Polskiej do realizacji zadań z zakresu zarządzania kryzysowego [Dz.U. 2017 poz. 209, art. 3, pkt 4]

plan ochrony IK – dokument zgodny z wytycznymi zawartymi w Rozporządzeniu Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie planów ochrony infrastruktury krytycznej [Dz.U. 2010 nr 83 poz. 542.]

plan zarządzania kryzysowego – dokument zgodny z wytycznymi określonymi w art. 5 Ustawy z dnia 26 kwietnia 2017 r. o zarządzaniu kryzysowym [Dz.U. 2017 poz. 209]

płaski problem decyzyjny – zbiór obszarów decyzyjnych wyznaczonych przez zagrożenia, na które podatna jest IK, których ryzyko nie pozwala na osiągnięcie założonego progu bezpieczeństwa i w stosunku do których rozstrzygnięcia zapadają na jednym poziomie decyzyjnym – zagrożenia są wyznaczane na podstawie sytuacji rozpatrywanej IK lub SZN

pochodnia gazowa – instalacja umożliwiająca spalenie gazu niezagospodarowanego lub jego nadmiaru. Spalanie gazu w pochodniach stosuje się głównie z dwóch powodów: zabezpieczenia otoczenia (lokalnego) przed skutkami niekontrolowanej migracji gazu, (np. przed wybuchem, zatruciami, odorem), globalnej ochrony środowiska (przez zastąpienie emisji bardziej szkodliwych gazów palnych emisją mniej szkodliwych spalin)

podatność IK – prawdopodobieństwo zmiany dostępności funkcjonalności IK w wyniku wystąpienia rozpatrywanego zagrożenia, wynikające z cech konstrukcyjnych IK

podejście sytuacyjne – jedna z koncepcji nauk o zarządzaniu, korzystająca z osiągnięć koncepcji systemowych, w której szczególną uwagę zwraca się na pojęcie otoczenia rozumiane bardzo szeroko. Podstawową przesłanką podejścia sytuacyjnego jest relatywizm zasad i reguł organizacyjnych, czyli założenie, że mają one zastosowanie ograniczone jedynie do pewnych klas sytuacji [Stabryła, Trzcieniecki, 1986, s. 183–184]

podmioty odpowiedzialne za bezpieczeństwo IK – jednostki operacyjne realizujące zadania dotyczące bezpieczeństwa IK na określonych poziomach decyzyjnych określone w Ustawie z dnia 26 kwietnia 2017 r. o zarządzaniu kryzysowym [Dz.U. 2007 nr 89 poz. 590]

postępowanie z ryzykiem – przyjęcie jednej z strategii działania: redukcja zagrożeń, ograniczenie skutków, transfer ryzyka, podjęcie ryzyka [Zawiła-Niedźwiecki, 2013, ss. 81–84].

potrzeba – stan osoby doznającej poczucia niespełnienia, wg Maslowa potrzeby są klasyfikowane w obszarze: fizjologicznym, bezpieczeństwa, afiliacji, szacunku i uznania oraz samorealizacji [Maslow, 2016, ss. 115–119]

poziom decyzyjny – umowny podział kompetencji decyzyjnych w ramach procesu zarządzania bezpieczeństwem IK:

- **centralny –** Rządowe Centrum Bezpieczeństwa,
- **administracyjny –** Rada Ministrów, urzędy centralne, wojewódzkie, powiatowe, gminne centra zarządzania kryzysowego,
- **operatora IK –** przedsiębiorstwa w ramach, których funkcjonują zasoby uznane za IK. W ramach poziomu operatora IK może występować wiele poziomów decyzyjnych uzależnionych od wzajemnego usytuowania rozpatrywanych IK

poziomy gotowości technologicznej – stosowane do oceny badań naukowych lub prac rozwojowych na rzecz obronności i bezpieczeństwa państwa [Dz.U. 2011 nr 18 poz. 91, zał.]

problem decyzyjny – zbiór obszarów decyzyjnych [Krupa, Ostrowska, 2012, s. 26]

proces – ciąg czynności realizowanych jedna po drugiej lub współbieżnie, który prowadzi do wytworzenia wyrobu lub usługi zgodnie z przyjętymi wymaganiami [Bitkowska, 2009, s. 54]

proces decyzyjny – stanowi proceduralno-technologiczną cechę procesu zarządzania o wielorakich uwarunkowaniach [Targalski, 1986, s. 194] (identyfikacja sytuacji decyzyjnej, sformułowanie problemu decyzyjnego, zbudowanie modelu decyzyjnego, wyznaczenie decyzji dopuszczalnych i decyzji wystarczających lub decyzji optymalnych, podjęcie ostatecznej decyzji)

prognoza – hipoteza dotycząca przyszłości, formułowana na podstawie uzasadnionych przesłanek ustalonych w toku badań naukowych, służąca jako wytyczna do dalszego postępowania [Bogdanienko, 2002, s. 139]

prognozowana dostępność funkcjonalności – różnica dostępności funkcjonalności i ryzyka jej utraty związanego z rozpatrywanym zagrożeniem

próg bezpieczeństwa – poziom funkcjonalności uznany przez operatora IK za wystarczający do realizacji zadań IK wynikających z zobowiązań wobec społeczeństwa

raport zagrożeń bezpieczeństwa narodowego – dokument zgodny z wytycznymi zawartymi w Rozporządzeniu Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie Raportu o zagrożeniach bezpieczeństwa narodowego [Dz.U. Z 2010, Nr 83, poz. 540]

ryzyko – wartość liczbowa wyrażająca procentowo przewidywany stopień utraty funkcjonalności IK, jaki może powstać w wyniku materializacji zagrożenia [Kosieradzka, Zawiła-Niedźwiecki, 2016, s. 367]

ryzyko inherentne – wyznaczane bez uwzględniania zabezpieczeń [Kosieradzka, Zawiła-Niedźwiecki, 2016, s. 369]

ryzyko rezydualne – uwzgledniające wpływ istniejących zabezpieczeń [Kosieradzka, Zawiła-Niedźwiecki, 2016, s. 369]

ryzyko utraty dostępności funkcjonalności – miara wyznaczana jako iloczyn prawdopodobieństwa wystąpienia zagrożenia, szacowanej procentowej utraty dostępności funkcjonalności oraz różnicy podatności na zagrożenie i szacowanego wpływu zabezpieczeń na podatność zasobu na zagrożenie

scenariusz zdarzenia niekorzystnego – opis zdarzeń mogących wywołać sytuację kryzysową, pozwalający na określenie sposobu reagowania w przypadku zmaterializowania się zagrożeń [Kosieradzka, Zawiła-Niedźwiecki, 2016, s. 368]

siatka bezpieczeństwa – zestawienie potencjalnych zagrożeń ze wskazaniem podmiotu wiodącego [Dz.U. 2013 poz. 1166, art. 3, pkt 8]

sieć zależności – zbiór powiązań występujący między infrastrukturami krytycznymi i zagrożeniami wyrażany za pomocą wirtualnych kanałów

skierowane połączenie – odwzorowanie zależności dwóch obiektów, kierunek połączenia symbolizuje sekwencję oddziaływania

skuteczność – zdolność organizmu, urządzenia, systemu do wykonania określonych czynności skutkujących uzyskaniem spodziewanego efektu [Kosieradzka, Zawiła-Niedźwiecki, 2016, s. 368]

skutek – rezultaty oddziaływania zagrożenia na ludzi, środowisko, mienie, funkcjonowanie państwa lub społeczeństwa

służby powołane do niesienia pomocy – policja, straż pożarna, pogotowie ratunkowe

sprawność – skalarna bezwymiarowa wielkość fizyczna określająca, w jakim stopniu urządzenie, organizm lub proces przekształca energię występującą w jednej postaci w energię w innej postaci [Kosieradzka, Zawiła-Niedźwiecki, 2016, s. 368]

struktura IK – stanowi ilustrację siatki powiązań między zasobami (powiązania odwzorowują wzajemny wpływ zasobów identyfikowany na podstawie realizacji tych samych funkcjonalności)

system – całość złożoną z wielu powiązanych ze sobą podukładów i elementów, wchodzącą w relacje z środowiskiem, w którym sią znajduje [Bogdanienko, 2002, s. 30]

system IK – układ wzajemnie powiązanych elementów IK, stanowiących logicznie uporządkowaną całość, realizujący zbiór funkcjonalności: system zaopatrzenia w energię, surowce energetyczne i paliwa, system łączności, system sieci teleinformatycznych, system finansowy, system zaopatrzenia w żywność, system zaopatrzenia w wodę, system ochrony zdrowia, system transportowy, system ratowniczy, system zapewniający ciągłość działania administracji publicznej, system produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych [Dz.U. 2017 poz. 1566, art. 3, pkt 2]

system powiązanych IK – system złożony z przynajmniej jednej IK, jej otoczenia uwzględniający relacje podrzędności i nadrzędności oraz zależności składowych

sytuacja – aktualnie obowiązująca wielopoziomowa charakterystyka zasobu, organizacji [Krupa, 2006, s. 43]

sytuacja IK – aktualnie obowiązująca charakterystyka IK określana w obszarze zasobów, funkcjonalności, zagrożeń oraz zabezpieczeń, uwzględniająca zależność rozpatrywanej IK z powiązanymi IK

sytuacja kryzysowa – należy przez to rozumieć sytuację wpływającą negatywnie na poziom bezpieczeństwa ludzi, mienia w znacznych rozmiarach lub środowiska, wywołującą znaczne ograniczenia w działaniu właściwych organów administracji publicznej ze względu na nieadekwatność posiadanych sił i środków [Dz.U. 2017 poz. 1566, art. 3, pkt 1]

szacowanie ryzyka – obliczanie wartości ryzyka na podstawie przyjętego wzoru, co prowadzi do nadania mu umownej wartości [Kosieradzka, Zawiła-Niedźwiecki, 2016, s. 369]

terroryzm – teoria i praktyka określająca różnie umotywowane ideologicznie, planowane i zorganizowane działania pojedynczych osób lub grup, skutkujące naruszeniem istniejącego porządku prawnego, podjęte w celu wymuszenia od władz, państw i społeczeństw określonych zachowań i świadczeń, często naruszające dobra osób postronnych [AON, 2008, s. 147]

typ zagrożenia – zbiór zagrożeń o jednakowym zestawie skutków

typ zasobu – zbiór zasobów o jednakowym zestawie cech

wirtualny kanał – zależność między zasobem i zagrożeniem lub między zagrożeniem i zagrożeniem:

- zależności IK – komunikacja podatności $U_{\alpha,\beta}$ IK V_{α} i prawdopodobieństwa wystąpienia zagrożenia $P_{\alpha,\beta}$ wyrażona na skali <0, 1>, określająca prawdopodobieństwo utraty funkcjonalności po uwzględnieniu podatności IK na rozpatrywane zagrożenie, co można zapisać $P(P_{\alpha,\beta}|U_{\alpha,\beta})$, gdzie: α – indeks IK; β – indeks zagrożenia,
- zależności zagrożeń – komunikacja prawdopodobieństwa zagrożenia $P_{\alpha,\beta}$ pod warunkiem wystąpienia innego zagrożenia $P'_{\alpha,\beta}$ wyrażona na skali <0, 1>, określająca prawdopodobieństwo materializacji rozpatrywanej pary zagrożeń, co można zapisać $P(P_{\alpha,\beta}|P'_{\alpha,\beta})$ gdzie: α – indeks IK; β – indeks zagrożenia

wzbudzenie zagrożenia – zaistnienie sprzyjających warunków do materializacji zagrożenia

względna istotność decyzji elementarnej – stosunek istotności rozpatrywanej decyzji elementarnej do innych decyzji elementarnych możliwych do podjęcia w obszarze decyzyjnym

względna istotność obszaru decyzyjnego – stosunek istotności rozpatrywanego obszaru decyzyjnego do innych obszarów decyzyjnych zawartych w problemie decyzyjnym

zabezpieczenie – działania, systemy lub zasoby stosowane w reakcji na rozpoznane zagrożenie w celu wyeliminowania lub ograniczenia ryzyka z nim związanego

zagrożenie – spodziewane oddziaływanie na zasoby lub między zasobami, w wyniku realizacji którego mogą ulec degradacji ich cechy funkcjonalno-strukturalne

zagrożenie wewnętrzne – zagrożenie oddziałujące na rozpatrywany zasób generowane przez rozpatrywany zasób

zagrożenie zewnętrzne – zagrożenie oddziałujące na rozpatrywany zasób generowane przez inny zasób

zakłócenie – zdarzenie powodujące nieplanowane i negatywne odchylenie od spodziewanego rezultatu, stanu lub sposobu działania organizacji. Zakłócenie może mieć ograniczony zasięg lub być katastrofą. W ujęciu organizacyjnym polega na utracie zasobów lub utracie kontroli nad zasobami (w tym funkcjami realizowanymi przez zasoby) [Kosieradzka, Zawiła-Niedźwiecki, 2016, s. 370]

zależność – związek przyczynowo-skutkowy wynikający z wzajemnych powiązań pomiędzy grupami zasobów, podsystemami i systemami, ujawniający się w momencie materializacji zagrożenia

zarządzanie – to proces polegający na podejmowaniu decyzji zapewniających wykorzystanie określonych zasobów dla osiągnięcia pożądanych celów (…) oraz na koordynowaniu aktywności mających współpracować ze sobą ludzi [Bogdanienko, 2002, s. 12]

zarządzanie bezpieczeństwem IK – procedura realizowana w ramach procesu planowania cywilnego polegająca na zebraniu przez Rządowe Centrum Bezpieczeństwa Raportów Zagrożeń Bezpieczeństwa Narodowego z wymaganych ustawą o zarządzaniu kryzysowym poziomów administracji publicznej i opracowaniu na ich podstawie PZK przez wszystkie szczeble administracji publicznej oraz POIK przez operatorów IK [na podstawie NPOIK, 2015 oraz Dz.U. 2017 poz. 209]

zarządzanie sytuacyjne bezpieczeństwem IK – zespół działań realizowanych w obszarze funkcji zarządzania, uzależnionych od sytuacji IK, w celu osiągnięcia wymaganego progu bezpieczeństwa

zarządzanie kryzysowe – działalność organów administracji publicznej będąca elementem kierowania bezpieczeństwem narodowym, która polega na zapobieganiu sytuacjom kryzysowym, przygotowaniu do przejmowania nad nimi kontroli w drodze zaplanowanych działań, reagowaniu w przypadku wystąpienia sytuacji kryzysowych, usuwaniu ich skutków oraz odtwarzaniu zasobów i infrastruktury krytycznej [Dz.U. 2017 poz. 209, art. 2]

zarządzanie ryzykiem – koordynowanie działań w zakresie zarządzania bezpieczeństwem z uwzględnieniem ryzyka [Kosieradzka, Zawiła-Niedźwiecki, 2016, s. 371]

zarządzanie sytuacyjne – działanie realizujące funkcje zarządzania dla osiągnięcia wyznaczonego celu uwzględniające aktualną sytuację organizacji

zasób – fragment rzeczywistości materialnej (fizycznej) lub wirtualnej (np. pojęciowej, informacyjnej, metajęzykowej) o niepustym zbiorze funkcjonalności

zawór bezpieczeństwa – samoczynnie upuszcza czynnik w przypadku wzrostu ciśnienia powyżej nastawionej wartości (ciśnienia nastawy), chroniąc zbiornik ciśnieniowy lub instalację przed rozerwaniem. Po ustabilizowaniu się ciśnienia poniżej wartości zadanej następuje zamknięcie zaworu i zanik wypływu czynnika. Zgodnie z dyrektywą ciśnieniową PED 2014/68/UE tego rodzaju zawory zalicza się do osprzętu zabezpieczającego

zdarzenie niekorzystne – zdarzenie będące efektem spełnienia się zagrożenia, mające negatywne skutki dla organizacji, środowiska naturalnego lub ludności

Skróty i oznaczenia stosowane w tekście

α – indeks zasobu

β – indeks zagrożenia,

γ – indeks funkcjonalności

λ – indeks zabezpieczenia

Φ – zbiór funkcjonalności IK

ϕ^{PB} – wartość progu bezpieczeństwa

A – cel zarządzania kryzysowego realizowany przez zabezpieczenie

i – liczba decyzji elementarnych w obszarze decyzyjnym

j – liczba obszarów decyzyjnych w problemie decyzyjnym

n – indeks porządkowy

$\Delta\Phi$ – zmiana dostępności funkcjonalności

$\ni$ – symbol zawierania się zbioru

AIDA – Analysis of Interconnected Decision Areas (Analiza Powiązanych Obszarów Decyzyjnych)

ARGUS – System szybkiego ostrzegania o zagrożeniach dla IK w ramach UE

BIA – Business Impact Analysis (Analiza Wpływu Zdarzenia na Biznes)

$D_{\alpha,\beta}$ – istotność obszaru decyzyjnego

$d_{\alpha,\beta,\lambda}$ – istotność decyzji elementarnej

DC – decyzja elementarna na rozpatrywanym poziomie decyzyjnym

dc – wartość decyzji elementarnej na rozpatrywanym poziomie decyzyjnym

G_n – zbiór zależności rozpatrywanej IK z innymi IK

GZZK – Gminny Zespół Zarządzania Kryzysowego

EEPR – European Energy Programme for Recovery (Europejski program energetyczny na rzecz naprawy gospodarczej)

ELIKSIR – System wspierania planowania działań w czasie kryzysu na poziomie gminy

EIK – Europejska Infrastruktura Krytyczna

EPOIK – Europejski Program Ochrony Infrastruktur Krytycznej

ETA – Event Tree Analysis (analiza drzewa zdarzeń)

H_n – zbiór zagrożeń wywoływanych

IN – zagrożenie wewnętrzne

IK – Infrastruktura Krytyczna

IM-BIK – Integralny Model Bezpieczeństwa Infrastruktury Krytycznej

KPZK – Krajowy Plan Zarządzania Kryzysowego

LPR – Lotnicze Pogotowie Ratunkowe

LNG – Liquefied Natural Gas (skroplony gaz ziemny)

$M_{\alpha,\beta,\lambda}$ – nazwa/symbol modelu zabezpieczeń

$m_{\alpha,\beta,\lambda}$ – wartość podniesienia odporności rozpatrywanej IK o indeksie α na zagrożenie o indeksie β związana z zabezpieczeniem o indeksie λ

NFZ – Narodowy Fundusz Zdrowia

NIST – National Institute of Standards and Technology (Narodowy Instytut Standaryzacji i Technologii)

NPOIK – Narodowy Program Ochrony Infrastruktury Krytycznej

O – obszar ochrony IK zabezpieczany przez rozpatrywany środek ochronny

OUT – zagrożenie zewnętrzne

$P_{\alpha,\beta}$ – prawdopodobieństwo wystąpienia zagrożenia

PGT – Poziom Gotowości Technologicznej

PHA – Process Hazard Analysis (analiza zagrożeń procesu)

POIK – Plan Ochrony Infrastruktury Krytycznej

PZK – Plan Zarządzania Kryzysowego

PZZK – Powiatowy Zespół Zarządzania Kryzysowego

$R_{\alpha,\beta}$ – wartość ryzyka związanego z zagrożeniem o indeksie β, na które podatna jest IK o indeksie α

R^i – wartość ryzyka inherentnego

R^r – wartość ryzyka rezydualnego

RCB – Rządowe Centrum Bezpieczeństwa

RP – Rzeczypospolita Polska

RZBN – Raport o Zagrożeniach Bezpieczeństwa Narodowego

RZZK – Rządowy Zespół Zarządzania Kryzysowego

S – sytuacja rozpatrywanej IK

SARNA – system służący do monitorowania zagrożeń epidemiologicznych

SPIK – System Powiązanych Infrastruktur Krytycznych

SWOT – Strong, Weak, Opportunity, Threat (silne strony, słabe strony, szanse, zagrożenia)

SZN – scenariusz zdarzenia niekorzystnego

TELDAT – system wsparcia dowodzenia i działania wojsk

V_{α} – rozpatrywana IK (zasób)

$U_{\alpha,\beta}$ – poziom podatności zasobu o indeksie α na zagrożenie o indeksie β

$U'_{\alpha,\beta}$ – podatność IK o indeksie α na zagrożeniem o indeksie β po uwzględnieniu dodatkowych zabezpieczeń

UE – Unia Europejska

UMOL – Unijny Mechanizm Ochrony Ludności

USA – United States of America (Stany Zjednoczone Ameryki)

WZZK – Wojewódzki Zespół Zarządzania Kryzysowego

$Z_{\alpha,\beta}$ – zagrożenie, na które podatna jest IK

ZR – zbiór możliwych rezultatów

$Z_{\alpha,\beta}$-D – oznaczenie wzbudzenia zagrożenia

$Z_{\alpha,\beta}$-P – oznaczenie materializacji zagrożenia bez negatywnych skutków dla IK

$Z_{\alpha,\beta}$-R – oznaczenie materializacji zagrożenia z negatywnymi skutkami dla IK

ZRZBN – zbiorczy raport o zagrożeniach bezpieczeństwa narodowego

ZS-BIK – zarządzanie sytuacyjne bezpieczeństwem infrastruktury krytycznej

Spis rysunków

Rysunek 1.1a. Zależność pojęć bezpieczeństwo narodowe – planowanie cywilne – infrastruktura krytyczna 12
Rysunek 1.1b. Cykl planowania cywilnego 15
Rysunek 1.1c. Schemat procesu planowania cywilnego 16
Rysunek 1.1d. Proces zarządzania kryzysowego 17
Rysunek 1.1e. Podmioty odpowiedzialne za bezpieczeństwo IK 19
Rysunek 1.2a. Cykl metodyki ZS-BIK 23
Rysunek 1.2b. Elementy IM-BIK 24
Rysunek 1.2c. Zależność etapów metodyki ZS-BIK od elementów modelu IM-BIK .. 24
Rysunek 1.3a. Klasyfikacja danych stosowanych w POIK i PZK do charakterystyki IK 26
Rysunek 1.4a. Struktura sytuacji 30
Rysunek 1.4b. Przykład diagramu szacowania zagrożeń metodą ETA 39
Rysunek 1.4c. Pomiar ryzyka – podejścia, metody, techniki 42
Rysunek 1.5a. Schemat wykorzystania danych zebranych w istniejących systemach informatycznych wspierających proces planowania cywilnego i zarządzania kryzysowego przez elementy IM-BIK 45
Rysunek 2.1a. Koncepcja IM-BIK 48
Rysunek 2.2a. Przykład sytuacji wg modelu Kłykowa 50
Rysunek 2.2b. Przykład graficznej ilustracji zależności IK 52
Rysunek 2.4a. Przykład identyfikacji zależności IK w rozpatrywanym SPIK 63
Rysunek 2.4b. Przykład implementacji SPIK przedstawionego rys. 2.4a w narzędziu informatycznym umożliwiającym symulację SZN 68
Rysunek 2.4c. Przykład ilustrujący podatności zasobu V_1 na zagrożenia 69
Rysunek 2.5a. Przykład problemu decyzyjnego sformułowanego dla sytuacji IK – rafineria 75
Rysunek 3.2a. Procedura realizacji metodyki ZS-BIK dla płaskiego problemu decyzyjnego 92
Rysunek 3.3a. Procedura realizacji metodyki ZS-BIK dla hierarchicznego problemu decyzyjnego 94
Rysunek 3.3b. Przykład hierarchicznego problemu decyzyjnego 95
Rysunek 4.2a. Graficzna ilustracja zależności rafinerii PKN ORLEN S.A., Basell Orlen Polyolefins sp. z o.o. oraz Zakładu Produkcyjnego ORLEN OIL sp. z o.o. w Płocku 103

Rysunek 4.2b. Graficzna ilustracja SPIK rafinerii PKN ORLEN S.A., Basell Orlen Polyolefins sp. z o.o. oraz Zakładu Produkcyjnego ORLEN OIL sp. z o.o. w Płocku 106
Rysunek 4.2c. Fragment SPIK rafinerii PKN ORLEN S.A., Basell Orlen Polyolefins sp. z o.o. oraz Zakładu Produkcyjnego ORLEN OIL sp. z o.o. w Płocku zaimplementowany w IBM WebSphere Business Modeler 7.0 108
Rysunek 4.2d. Ilustracja rozpatrywanego problemu decyzyjnego dotyczącego IK V_1 113
Rysunek 4.2e. Ilustracja zapisu rozpatrywanego problemu decyzyjnego operatora IK V_1 w narzędziu informatycznym 114
Rysunek 4.3a. Ilustracja rozpatrywanego problemu decyzyjnego dotyczącego SZN nr 28 123
Rysunek 4.3b. Ilustracja rozwiązania rozpatrywanego problemu decyzyjnego dotyczącego SZN nr 28 124
Rysunek A.1. Przykład ilustrujący implementację modelu sytuacji IK oraz procedurę SZN c.1 167
Rysunek A.2. Przykład ilustrujący implementację modelu sytuacji IK oraz procedurę symulacji SZN c.2 168
Rysunek B.1. Okno główne aplikacji pozwalającej na rozwiązanie problemu decyzyjnego 173
Rysunek B.2. Wygenerowanie zbioru rozwiązań problemu decyzyjnego 174
Rysunek B.3. Wartości oceny kosztowej dla rozwiązań problemu decyzyjnego 174
Rysunek C.1. Przykład graficznej ilustracji zależności IK 178
Rysunek C.2. Przykład identyfikacji zależności IK w rozpatrywanym SPIK 179
Rysunek C.3. Przykład problemu decyzyjnego bazującego na SZN nr 7 dla IK V1 i V2 188
Rysunek F.1. Proces zarządzania ryzykiem wg normy ISO 31000:2009 205

Spis tabel

Tabela 1.1a. Zestawienie systemów IK w UE i Polsce 14
Tabela 1.2a. Wykaz etapów działań rozpatrywanych metodyk oceny ryzyka na potrzeby zarządzania kryzysowego 21
Tabela 1.4a. Metody wykorzystywane w ocenie ryzyka na potrzeby zarządzania kryzysowego 28
Tabela 1.4b. Ocena metod możliwych do zastosowania w obszarze odwzorowania charakterystyki IK 31
Tabela 1.4c. Ocena metod możliwych do zastosowania w obszarze generowania SZN 34
Tabela 1.4d. Ocena metod możliwych do zastosowania w obszarze formułowania problemu decyzyjnego 38
Tabela 1.4e. Ocena metod możliwych do zastosowania w obszarze szacowania ryzyka 43
Tabela 2.2a. Podstawowe atrybuty zasobu 53
Tabela 2.2b. Podstawowe atrybuty zagrożenia 53
Tabela 2.2c. Podstawowe atrybuty zależności zagrożeń 54
Tabela 2.2d. Podstawowe atrybuty funkcjonalności 54
Tabela 2.2e. Podstawowe atrybuty modelu zabezpieczeń 54
Tabela 2.2f. Podstawowe atrybuty odwzorowujące zależność IK 55
Tabela 2.2g. Zapis zależności zagrożeń dla elementów IK: V_1 – szpital, V_3 – środowisko naturalne 55
Tabela 2.2h. Przykład syntetycznego zapisu sytuacji IK (V_1 – szpital) 56
Tabela 2.3a. Przykład przedziałów określających postępowanie z ryzykiem 62
Tabela 2.4a. Ideowy zapis odwzorowujący podatności składowych SPIK na zagrożenia 66
Tabela 2.4b. Ideowy zapis odwzorowujący zależności zagrożeń w SPIK 66
Tabela 2.4c. Przykład opisu SZN dla zagrożenia $Z_{3,1}$ – susza 67
Tabela 2.5a. Wykaz możliwych celów problemów decyzyjnych w kontekście kryteriów przekrojowych 72
Tabela 2.5b. Macierz możliwych rozwiązań problemu decyzyjnego 76
Tabela 2.5c. Przykład obliczenia wartości oceny kosztowej rozwiązań problemu decyzyjnego przedstawionego na rys. 2.5a 77
Tabela 2.5d. Zestawienie wartości ryzyka utraty funkcjonalności i wartości funkcjonalności dla rozwiązań problemu decyzyjnego przedstawionego na rys. 2.5a 77

Tabela 2.5e. Opisu SZN nr 7 dla zagrożenia $Z_{3,1}$ – susza 78
Tabela 3.1a. Matryca kompetencji zespołu analitycznego 85
Tabela 3.1b. Charakterystyka etapu metodyki ZS-BIK – powołanie zespołu 86
Tabela 3.1c. Charakterystyka etapu metodyki ZS-BIK – określenie progu bezpieczeństwa 87
Tabela 3.1d. Charakterystyka etapu metodyki ZS-BIK – odwzorowanie charakterystyki IK 88
Tabela 3.1e. Charakterystyka etapu metodyki ZS-BIK – szacowanie ryzyka 88
Tabela 3.1f. Charakterystyka etapu metodyki ZS-BIK – wygenerowanie SZN 89
Tabela 3.1g. Charakterystyka etapu metodyki ZS-BIK – sformułowanie problemu decyzyjnego 90
Tabela 3.1h. Charakterystyka etapu metodyki ZS-BIK – wdrożenie zabezpieczeń 90
Tabela 3.2a. Opis elementów charakteryzujących procedurę zastosowania metodyki ZS-BIK 91
Tabela 3.3a. Zapis macierzowy zależności wartości decyzji elementarnych poziomu powiatu od wartości decyzji elementarnych poziomu gmin 96
Tabela 3.5b. Przykład zapisu macierzowego hierarchicznego problemu decyzyjnego 97
Tabela 4.2a. Syntetyczny zapis zależności pomiędzy rafinerią PKN ORLEN S.A., Basell Orlen Polyolefins sp. z o.o. oraz Zakładem Produkcyjnym ORLEN OIL sp. z o.o. w Płocku 103
Tabela 4.2b Syntetyczny zapis sytuacji rafinerii PKN ORLEN S.A., Basell Orlen Polyolefins sp. z o.o. oraz Zakładu Produkcyjnego ORLEN OIL sp. z o.o. w Płocku 104
Tabela 4.2c. Syntetyczny zapis ryzyka utraty funkcjonalności dla rozpatrywanych IK 105
Tabela 4.2d. Opis oddziaływania zagrożeń na SPIK rafinerii PKN ORLEN S.A., Basell Orlen Polyolefins sp. z o.o. oraz Zakładu Produkcyjnego ORLEN OIL sp. z o.o. w Płocku 107
Tabela 4.2e. Opis wzajemnego oddziaływania zagrożeń dla SPIK rafinerii PKN ORLEN S.A., Basell Orlen Polyolefins sp. z o.o. oraz Zakładu Produkcyjnego ORLEN OIL sp. z o.o. w Płocku 107
Tabela 4.2f. Wykaz SZN dla SPIK rafinerii PKN ORLEN S.A., Basell Orlen Polyolefins sp. z o.o. oraz Zakładu Produkcyjnego ORLEN OIL sp. z o.o. w Płocku agregujących 80% przypadków negatywnie wpływających na IK 109
Tabela 4.2g. Szacunkowy wpływ dodatkowych zabezpieczeń dostępnych dla operatora IK V_1 na podatność rozpatrywanej IK 112
Tabela 4.2h. Macierz dopuszczalnych decyzji rozwiązujących rozpatrywany problem decyzyjny operatora IK V1 115
Tabela 4.2i. Ocena kosztowa dopuszczalnych decyzji dla problemu decyzyjnego operatora IK V_1 116
Tabela 4.2j. Wykaz decyzji realizujących cel operatora IK V_1 117

Tabela 4.2k. Syntetyczny zapis sytuacji rafinerii PKN ORLEN S.A. po wdrożeniu nowych zabezpieczeń ... 118
Tabela 4.2l. Syntetyczny zapis ryzyka utraty funkcjonalności dla IK V_1 po wdrożeniu nowych zabezpieczeń ... 119
Tabela 4.3a. Charakterystyka SZN negatywnie wpływającego na rafinerię PKN ORLEN S.A. oraz Zakład Produkcyjny ORLEN OIL sp. z o.o. w Płocku ... 120
Tabela 4.3b. Syntetyczny zapis podatności V_1 i V_3 na zagrożenia ze SZN nr 28 ... 120
Tabela 4.3c. Szacunkowy wpływ dodatkowych zabezpieczeń na podatność rozpatrywanej IK V_1 i V_3 na zagrożenia ... 122
Tabela 4.3d. Zapis macierzowy rozpatrywanego hierarchicznego problemu decyzyjnego dotyczącego SZN nr 28 ... 125
Tabela 4.3e. Syntetyczny zapis podatności V_1 i V_3 na zagrożenia ze SZN nr 28 po zastosowaniu dodatkowych zabezpieczeń ... 126
Tabela 4.4a. Powiązanie etapów metodyki ZS-BIK z etapami procesu planowania cywilnego ... 129
Tabela 4.4b. Zestawienie elementów POIK z realizującymi je etapami ZS-BIK ... 130
Tabela 4.4c. Zestawienie elementów PZK z realizującymi je etapami ZS-BIK ... 130
Tabela A.1. Notacja używana przez program IBM Websphere Business Modeler wersja 7.0 ... 166
Tabela B.1. Wykaz wartości względnej istotności obszarów decyzyjnych i decyzji elementarnych ... 172
Tabela B.2. Wagi istotności decyzji dla przykładu problemu decyzyjnego ... 175
Tabela C.1. Przykład syntetycznego zapisu sytuacji IK V_1 i V_2 ... 177
Tabela C.2. Przykład syntetycznego zapisu zależności zagrożeń i IK ... 178
Tabela C.3. Przykład opisu oddziaływania zagrożeń wewnętrznych na rozpatrywany system ... 181
Tabela C.4. Przykład opisu zależności zagrożeń ... 181
Tabela C.5. Podsumowanie przypadków SZN dla zagrożenia $Z_{3,1}$ – susza ... 182
Tabela C.6. Macierz możliwych rozwiązań problemu decyzyjnego bazującego na SZN nr 7 dla IK V_1 i V_2 ... 189
Tabela C.7. Obliczenie wartości możliwych rozwiązań problemu decyzyjnego bazującego na SZN nr 7 dla IK V_1 i V_2 ... 189
Tabela C.8. Zestawienie wartości ryzyka utraty funkcjonalności i wartości funkcjonalności dla rozwiązań problemu decyzyjnego ... 189
Tabela D.1. Wykaz SZN dla SPIK rafinerii PKN ORLEN S.A., Basell Orlen Polyolefins sp. z o.o. oraz Zakładu Produkcyjnego ORLEN OIL sp. z o.o. w Płocku ... 190
Tabela E.1. Wykaz danych obligatoryjnych procesu zarządzania bezpieczeństwem IK ... 202
Tabela E.2. Wykaz elementów planowanych dla procesu zarządzania bezpieczeństwem IK ... 203

Tabela F.1. Przykład parametrów opisu scenariusza zdarzeń niekorzystnych stosowanych w niemieckiej metodyce oceny ryzyka na potrzeby zarządzania kryzysowego 209
Tabela F.2. Obszary i wskaźniki wykorzystywane w irlandzkiej metodyce oceny ryzyka na potrzeby zarządzania kryzysowego 211
Tabela F.3. Opis scenariusza zdarzenia wg AHRA 213
Tabela G.1. Wpływ systemu zaopatrzenia w energię, surowce energetyczne i paliwa na inne systemy IK 221
Tabela G.2. Wpływ systemów IK na system zaopatrzenia w energię, surowce energetyczne i paliwa 221
Tabela G.3. Wpływ systemu produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągów substancji niebezpiecznych na inne systemy IK 222
Tabela G.4. Wpływ innych systemów IK na system produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągów substancji niebezpiecznych 222
Tabela G.5. Wpływ systemu transportu na inne systemy IK 223
Tabela G.6. Wpływ systemów IK na system transportu 223
Tabela G.7. Wpływ systemu łączności na inne systemy IK 224
Tabela G.8. Wpływ systemów IK na system łączności 224
Tabela G.9. Wpływ systemu sieci teleinformatycznych na inne systemy IK 225
Tabela G.10. Wpływ systemów IK na system sieci teleinformatycznych 225
Tabela G.11. Wpływ systemu finansowego na inne systemy IK 226
Tabela G.12. Wpływ systemów IK na system finansowy 226
Tabela G.13. Wpływ systemu zapewniania ciągłości działania administracji publicznej na inne systemy IK 227
Tabela G.14. Wpływ systemów IK na system zapewniania ciągłości działania administracji publicznej 227
Tabela G.15. Wpływ systemu zaopatrzenia w żywność na inne systemy IK 228
Tabela G.16. Wpływ systemów IK na system zaopatrzenia w żywność 228
Tabela G.17. Wpływ systemu zaopatrzenia w wodę na inne systemy IK 229
Tabela G.18. Wpływ systemów IK na system zaopatrzenia w wodę 230
Tabela G.19. Wpływ systemu ratownictwa na inne systemy IK 231
Tabela G.20. Wpływ systemów IK na system ratownictwa 231
Tabela G.21. Wpływ systemu ochrony zdrowia na inne systemy IK 232
Tabela G.22. Wpływ systemów IK na system ochrony zdrowia 232

Załączniki

Niniejsza cześć monografii stanowi uzupełnienie treści przedstawionych w poszczególnych rozdziałach, które omawiały jedynie kluczowe fragmenty przeprowadzonych badań, istotne dla opracowania IM-BIK oraz metodyki ZS-BI. Monografia zawiera siedem załączników dotyczących trzech obszarów prowadzonych badań:

- implementacja opracowanych rozwiązań w narzędziach informatycznych – zał. A – B,
- weryfikacja użyteczności opracowanych rozwiązań – zał. C – D,
- badania literaturowe – zał. E – G.

W zał. A omówiono uwarunkowania pozwalające na implementację modelu sytuacji IK (rozdz. 2.2) oraz metody generowania SZN (rozdz. 2.4) w narzędziu informatycznym. Wybrane narzędzie informatyczne (IBM Websphere Business Modeler) pozwala na modelowanie oraz symulację przebiegu procesów biznesowych w przestrzeni zamodelowanych warunków decyzyjnych.

W ramach zał. B przedstawiono autorskie narzędzie informatyczne implementujące procedurę formułowania problemu decyzyjnego (rozdz. 2.5). Opracowane narzędzie informatyczne pozwala na opisanie danymi ilościowymi zaobserwowanego problemu decyzyjnego, oznaczenie par decyzji elementarnych pozostających w sprzeczności, wyznaczenie możliwych wariantów decyzyjnych stanowiących rozwiązanie problemu decyzyjnego oraz wyznaczenie oceny kosztowej decyzji dopuszczalnych.

W zał. C przedstawiono przykłady obliczeniowe ilustrujące zastosowanie elementów IM-BIK: modelu sytuacji IK – część A, metody generowania SZN – część B, metody szacowania ryzyka – część C oraz metody formułowania problemu decyzyjnego – część D.

W zał. D przedstawiono wykaz SZN możliwych do zaistnienia w rafinerii PKN ORLEN S.A.

Zał. E zawiera wykaz danych obligatoryjnych i opcjonalnych z zakresu zarządzania bezpieczeństwem IK pozyskanych z obowiązujących aktów normatywnych oraz opracowań planistycznych, tj. strategie, programy i raporty publikowane przez Komisję Europejską, rządy państw lub jednostki powołane do ochrony IK.

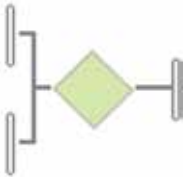
W zał. F przedstawiono szczegółowy opis wybranych metodyk oceny ryzyka na potrzeby zarządzania kryzysowego. W ramach załącznika przedstawione zostały metodyki stosowane w: Austrii, Szwecji, Republice Federalnej Niemiec, Iralndii, Kanadzie, Holandii i USA. Załącznik zawiera również opis procedur oceny ryzyka na potrzeby zarządzania kryzysowego stosowane w Polsce, przy opracowaniu których uczestniczył autor rozprawy.

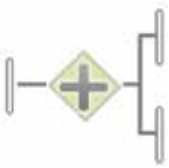
Natomiast w zał. G przedstawiono powiązania między polskimi systemami IK, które stanowią nośnik rozprzestrzeniania się zdarzeń niekorzystnych.

Załącznik A – Implementacja modelu sytuacji IK w narzędziu symulacyjnym

W zał. A omówiono uwarunkowania pozwalające na implementację modelu sytuacji IK (rozdz. 2.1) oraz procedury symulacji SZN (rozdz. 2.2) w narzędziu informatycznym. Do przeprowadzenia badań wybrane zostało narzędzie informatyczne (IBM Websphere Business Modeler wersja 7.0), które pozwala na modelowanie oraz symulację przebiegu procesów biznesowych w przestrzeni zamodelowanych warunków decyzyjnych. W badaniach wykorzystano zdolność programu do odwzorowania sytuacji rozpatrywanej IK oraz wskazania elementów modelu, które były uaktywnione w ramach konkretnego scenariusza. Było to możliwe dzięki przyjęciu założenia, że obiekty dostępne w ramach IBM Websphere Business Modeler odwzorowują elementy IK (tab. A.1). Stosując takie dostosowanie możliwe jest wykorzystanie innego środowiska umożliwiającego przeprowadzenie stymulacji procesu.

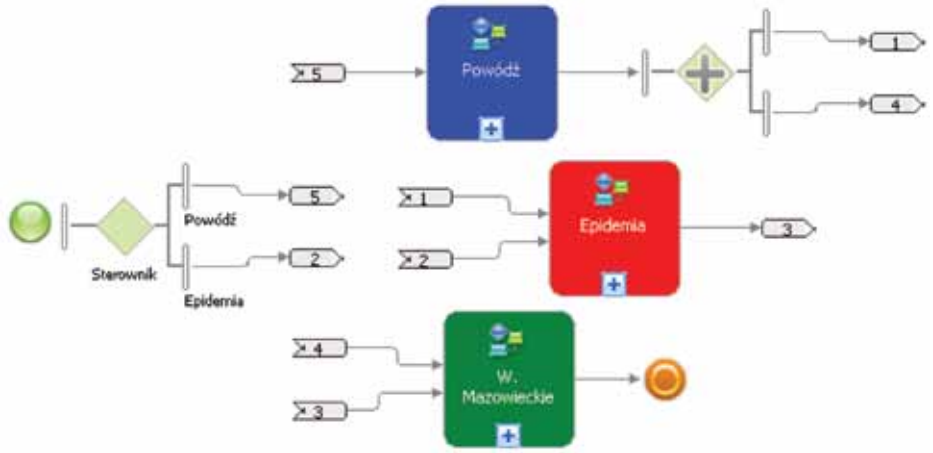
Tabela A.1. Notacja używana przez program IBM Websphere Business Modeler wersja 7.0

Rodzaj elementu	Opis zastosowania	Reprezentacja graficzna
Węzły początkowe oraz końcowe	Węzeł początkowy procesu wskazuje początek procesu i jest wymagany do uruchomienia symulacji. Węzeł końcowy procesu wskazuje koniec procesu i jest wymagany do zakończenia symulacji. Węzeł końcowy przepływu wskazuje koniec wątku symulacji.	Początek procesu  Koniec procesu  Koniec przepływu 
Zadanie	Reprezentuje zdarzenia w procesie, jest to najniższy poziom reprezentacji pracy. W eksperymencie element ten oznacza zagrożenie, na które podatny jest zasób.	Zadanie 
Decyzja	Element modelu procesu umożliwiający podział ścieżki przebiegu procesu na gałęzie alternatywne. Możliwe jest generowanie decyzji złożonych (posiadających więcej niż dwa rozgałęzienia). W eksperymencie element używany do określenia prawdopodobieństwa wystąpienia zagrożenia lub podatności zasobu na zagrożenie.	Decyzja prosta  Decyzja z wielokrotnym wyborem 
Scalenie alternatywne	Element służący połączeniu gałęzi alternatywnych (Decyzji).	

Rodzaj elementu	Opis zastosowania	Reprezentacja graficzna
Rozdzielenie	Element umożliwiający podział ścieżki przebiegu procesu na gałęzie współbieżne. W eksperymencie element wykorzystywany do wzbudzenia zagrożeń wywoływanych przez wystąpienie określonego zagrożenia.	
Podproces	Element służący powiązaniu modelu podprocesu z elementami modelu procesu nadrzędnego. Podprocesy w eksperymencie są wykorzystywane do ograniczania złożoności diagramów na jednym poziomie.	

Źródło: opracowanie własne.

Implementacja modelu sytuacji IK (rozdz. 2.2) oraz uwarunkowań wynikających z procedury symulacji SZN (rozdz. 2.4) w narzędziu informatycznym została omówiona na podstawie przykładu, który ilustruje rys. A.1. Implementacja polega na przyjęciu autorskiej interpretacji elementów udostępnionych w narzędziu informatycznym oraz wyników przeprowadzonych symulacji. Na potrzeby ilustracji logiki postępowania przyjęto, że rolę obiektu IK pełni województwo mazowieckie.

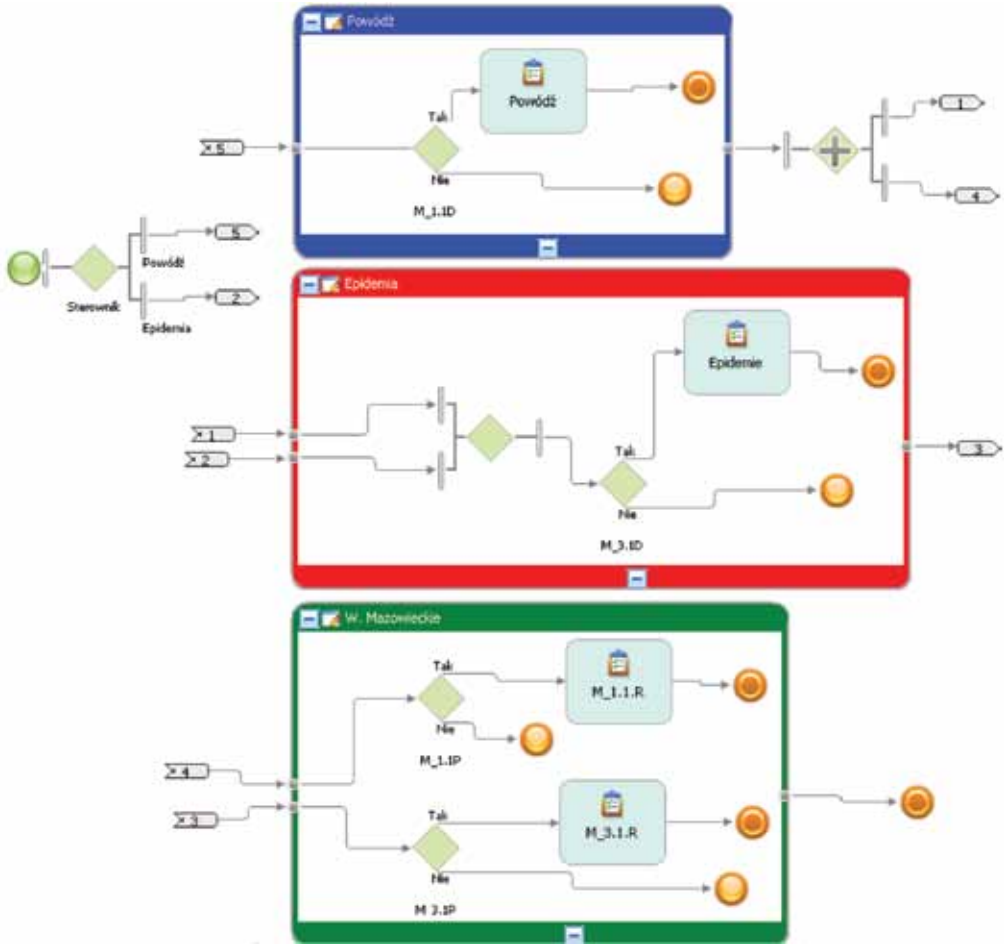


Rysunek A.1. Przykład ilustrujący implementację modelu sytuacji IK oraz procedurę SZN c.1
Źródło: opracowanie własne.

Na rys. A.1 przedstawiono trzy okna (podprocesy), w których zamknięto elementy opisujące prawdopodobieństwo wystąpienia zagrożenia oraz podatność województwa na zagrożenia (rys. A.2):

- okno niebieskie – oznaczające zagrożenie powodzi dla województwa mazowieckiego,
- okno czerwone – oznaczające zagrożenie epidemii dla województwa mazowieckiego,

- okno zielone – symbolizujące województwo mazowieckie i podatności województwa na zagrożenie powodzi i zagrożenie epidemii.



Rysunek A.2. Przykład ilustrujący implementację modelu sytuacji IK oraz procedurę symulacji SZN c.2

Źródło: opracowanie własne.

Zabieg ten został zastosowany ze względu na zwiększenie czytelności modeli sytuacji IK. Ponadto na rys. A.2 umieszczony jest element o nazwie „sterownik" służący do określania, z jakim prawdopodobieństwem wzbudzane są zagrożenia w ramach prowadzonych symulacji, np. ustawienie wartości 100% dla przepływu oznaczonego jako „epidemia" pozwoli na wzbudzenie tego zagrożenia określoną liczbę razy bez wzbudzania zagrożenia „powódź".

W oknie niebieskim znajdują się cztery elementy:

- decyzja prosta M_1.1D – element pozwalający wpisać prawdopodobieństwo materializacji zagrożenia „powódź", z elementu wychodzą dwa przepływy: „tak" oznacza-

jący, że zagrożenie zostało wzbudzone i zmaterializowało się, „nie" oznaczający, że zagrożenie zostało wzbudzone, ale nie zmaterializowało się,
- zadanie „powódź" – element służący do odnotowania, że zagrożenie zostało zmaterializowane, dzięki temu elementowi zmaterializowane zagrożenie jest widoczne w raporcie symulacji,
- węzeł końcowy procesu – element pozwalający na zakończenie podprocesu i powrót symulacji do procesu głównego, element zwraca wartość dodatnią oznaczającą, że zagrożenie „powódź" zmaterializowało się,
- węzeł końcowy przepływu – element pozwalający zakończyć wątek symulacji, zwracający wartość ujemną oznaczającą, że zagrożenie „powódź" mimo wzbudzenia nie zmaterializowało się.

W oknie czerwonym znajduje się pięć elementów:
- scalenie – pozwalające na połączenie wątków symulacji wzbudzających zagrożenie „epidemia", element sterujący, służący do łączenia przepływów alternatywnych,
- decyzja prosta M_3.1D – element pozwalający wpisać prawdopodobieństwo materializacji zagrożenia „epidemia", z elementu wychodzą dwa przepływy: „tak" oznaczający, że zagrożenie zostało wzbudzone i zmaterializowało się, „nie" oznaczający, że zagrożenie zostało wzbudzone, ale nie zmaterializowało się,
- zadanie „epidemia" – element służący do odnotowania, że zagrożenie zmaterializowało się, dzięki temu elementowi zmaterializowane zagrożenie jest widoczne w raporcie symulacji,
- węzeł końcowy procesu – element pozwalający na zakończenie podprocesu i powrót symulacji do procesu głównego, element zwraca wartość dodatnią oznaczającą, że zagrożenie „epidemia" zmaterializowało się,
- węzeł końcowy przepływu – element pozwalający zakończyć wątek symulacji, zwracający wartość ujemną oznaczającą, że zagrożenie „epidemia" mimo wzbudzenia nie zmaterializowało się.

W oknie zielonym znajduje się osiem elementów:
- decyzja prosta M_1.1P – element pozwalający wpisać wartość podatności województwa na zagrożenie „powódź", z elementu wychodzą dwa przepływy: „tak" oznaczający, że województwo ucierpiało w wyniku materializacji zagrożenia, „nie" oznaczający, że województwo nie ucierpiało w wyniku materializacji zagrożenia,
- decyzja prosta M_3.1P – element pozwalający wpisać wartość podatności województwa na zagrożenie „epidemia", z elementu wychodzą dwa przepływy: „tak" oznaczający, że województwo ucierpiało w wyniku materializacji zagrożenia: „nie" oznaczający, że województwo nie ucierpiało w wyniku materializacji zagrożenia,
- zadanie M_1.1.R – element służący do odnotowania, że województwo zostało poszkodowane na skutek wystąpienia zagrożenia „powódź", w ramach tego elementu można wpisać wartości charakteryzujące zagrożenie tj. średni czas/przedział czasu trwania powodzi, średnie koszty/przedział kosztów generowanych wystąpieniem zagrożenia „powódź",
- zadanie M_3.1.R – element służący do odnotowania, że województwo ucierpiało na skutek wystąpienia zagrożenia „epidemia", w ramach tego elementu można wpisać

wartości charakteryzujące zagrożenie, tj. średni czas/przedział czasu trwania epidemii, średnie koszty/przedział kosztów generowanych wystąpieniem zagrożenia „epidemia",
- dwa węzły końcowe procesu – elementy pozwalające na zakończenie podprocesu i powrót symulacji do procesu głównego, elementy zwracają wartość dodatnią oznaczającą, że województwo ucierpiało na skutek zagrożenia,
- dwa węzły końcowe przepływu – elementy pozwalające na zakończenie wątków symulacji, zwracające wartość ujemną oznaczającą, że województwo mimo wystąpienia zagrożenia nie poniosło uszczerbku (zastosowane zabezpieczenia skutecznie ochroniły województwo).

Funkcjonowanie przykładowego modelu sytuacji IK (rys. A.2) zostanie opisane na przykładzie wzbudzenie pojedynczego zagrożenia „powódź". W tym celu w elemencie „sterownik" na przepływie „powódź" ustawiana jest wartość 100%. Zabieg ten pozwala wzbudzić zagrożenie „powódź" (przepływ oznaczony na rys. A.2 nr 5). Następnie element sterujący M_1.1D decyduje (na podstawie zapisanego prawdopodobieństwa), czy zagrożenie „powódź" zmaterializuje się czy nie. W przypadku niezmaterializowania się zagrożenia „powódź" wykonywany jest węzeł końcowy przepływu i symulacja kończy się (ten przypadek oznacza, że zagrożenie „powódź" ostatecznie nie doszło do skutku).

W przypadku materializacji zagrożenia wykonywane jest zadanie „powódź" oraz węzeł końcowy procesu. Dzięki temu w raporcie symulacji odnotowywane jest, że zagrożenie „powódź" miało miejsce w rozpatrywanym scenariuszu. Ponadto na wyjściu podprocesu pojawia się sygnał inicjujący element „rozdzielenie".

Inicjacja elementu „rozdzielenie" powoduje dwa zdarzenia w modelu:
1. Sygnał jest przekazywany do podprocesu, w którym określona jest podatność województwa na zagrożenie „powódź" (przepływ oznaczony na rys. A.2 nr 4).
2. Sygnał jest przekazywany do podprocesu wzbudzającego zagrożenie „epidemia" (przepływ oznaczony na rys. A.2 nr 1 zależność ustalona na podstawie PZK województwa mazowieckiego).

W przypadku przepływu oznaczonego nr 4 sygnał jest odbierany przez element M_1.1P, w którym określono wartość podatności województwa mazowieckiego na zagrożenie „powódź". W przypadku, gdy na podstawie podatności województwo ucierpi w wyniku zagrożenia „powódź", realizowany jest element M_1.1R oraz węzeł końcowy procesu. Działanie to pozwala na odnotowanie faktu uszczerbku województwa mazowieckiego w wyniku materializacji zagrożenia „powódź" w raporcie symulacji oraz przekaże sygnał do procesu głównego, który zakończy ten wątek trwającej symulacji. Alternatywą jest sytuacja, w której z elementu M_1.1P wyjdzie sygnał (przepływ „nie") oznaczający, że mimo materializacji zagrożenia „powódź" województwo nie ucierpiało. Taka sytuacja jest interpretowana jako zdarzenie materializacji zagrożenia „powódź", którego negatywne skutki zostały wyeliminowane dzięki stosowanym zabezpieczeniom.

W przypadku przepływu oznaczonego nr 1 sygnał jest odbierany przez podproces epidemia (okno czerwone). Następnie sygnał dzięki elementowi „scalenie" jest przekazywany do elementu M_3.1D, w którym określono prawdopodobieństwo wystąpienia zagrożenia „epidemia". W tym przypadku podproces epidemia oraz jego składowe zachowują się dokładnie tak jak podproces powódź opisany wcześniej.

W przypadku materializacji zagrożenia „epidemia" sygnał jest przekazywany do podprocesu województwo mazowieckie (zielone okno) przepływem oznaczonym nr 3. Następnie, podobnie jak w przypadku zagrożenia „powódź", na podstawie podatności województwa na zagrożenie „epidemia" model decyduje, czy województwo ucierpi czy też nie w wyniku materializacji zagrożenia. Zakończenie wątku zagrożenia „epidemia" kończy symulację przebiegu scenariusza zdarzenia niekorzystnego „powódź".

Przedstawiony przykład obrazuje logikę funkcjonowania modeli sytuacji IK, a także modelu SPIK złożonego z modeli sytuacji różnych IK.

Załącznik B – Implementacja procedury budowy problemu decyzyjnego w narzędziu informatycznym

W zał. B omówiono uwarunkowania pozwalające na implementację problemu decyzyjnego (rozdz. 2.5) w autorskim narzędziu informatycznym. Opracowane narzędzie informatyczne pozwala na:

- określenie liczby obszarów decyzyjnych w ramach problemu decyzyjnego,
- określenie decyzji elementarnych w ramach obszaru decyzyjnego,
- przypisanie wartości względnej istotności do obszaru decyzyjnego,
- przypisanie wartości względnej istotności do decyzji elementarnej,
- wskazanie par decyzji sprzecznych,
- usunięcie decyzji zawierających pary decyzji sprzecznych ze zbioru decyzji rozwiązujących problem decyzyjny,
- obliczenie wartości oceny kosztowej decyzji rozwiązujących problem decyzyjny.

Wymienione funkcjonalności narzędzia informatycznego zaprezentowano na bazie przykładu obliczeniowego dla problemu decyzyjnego opublikowanego w artykule [Krupa, Ostrowska, 2012, ss. 25–31].

Rozpatrywany problem decyzyjny dotyczy trzech obszarów decyzyjnych D_i i ∋{1,2,3}. W każdym obszarze decyzyjnym wskazano zbiór decyzji elementarnych. Wartości względnej istotności obszarów decyzyjnych oraz decyzji elementarnych przedstawiono w tab. B.1.

Tabela B.1. Wykaz wartości względnej istotności obszarów decyzyjnych i decyzji elementarnych

Obszary decyzyjne		
D_1 ($V_1 = 20$)	D_2 ($V_2 = 30$)	D_3 ($V_3 = 50$)
Decyzje elementarne		
d_{11} ($v_{11} = 0{,}75$)	d_{12} ($v_{12} = 0{,}50$)	d_{13} ($v_{13} = 0{,}40$)
d_{21} ($v_{21} = 0{,}25$)	d_{22} ($v_{22} = 0{,}10$)	d_{23} ($v_{23} = 0{,}30$)
	d_{32} ($v_{32} = 0{,}40$)	d_{33} ($v_{33} = 0{,}30$)

Źródło: Krupa, Ostrowska, 2012, s. 26.

Określono decyzje elementarne pozostające w relacji sprzeczności: $d_{11} - d_{32}$, $d_{21} - d_{12}$, $d_{21} - d_{33}$, $d_{22} - d_{13}$, $d_{12} - d_{23}$ [Krupa, Ostrowska, 2012, s. 25].

Ocena kosztowa pojedynczej decyzji Q jest liczona jako suma iloczynów wag istotności obszarów decyzyjnych i wag istotności elementarnych decyzji z odpowiadających im obszarów decyzyjnych wg wzoru [Krupa, Ostrowska, 2012, s. 26]:

$$Q = \Sigma V_i * v_{ji} \tag{B.1}$$

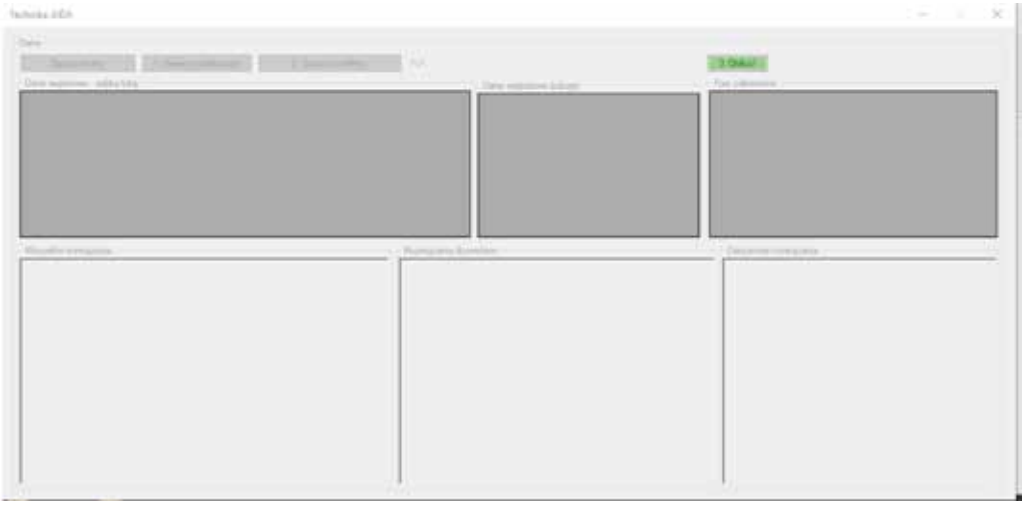
gdzie:

- V_i – relatywna waga istotności obszaru decyzyjnego D_i na skali otwartej <0%, 100%>
- v_{ji} – relatywna waga istotności elementarnej decyzji d_{ji} na skali otwartej <0, 1>,
- Q – waga istotności pojedynczej decyzji (wariantu decyzyjnego).

Na przykład ocena kosztowa wariantu decyzyjnego <{d_{21}},{d_{32}},{d_{23}}> wynosi:

$$Q = V_1 \text{ x } v_{21} + V_2 \text{ x } v_{32} + V_3 \text{ x } v_{23} = 20 \text{ x } 0{,}25 + 30 \text{ x } 0{,}40 + 50 \text{ x } 0{,}30 = 32$$

Na rys. B.1 zaprezentowano ekran główny opracowanego narzędzia.



Rysunek B.1. Okno główne aplikacji pozwalającej na rozwiązanie problemu decyzyjnego *Źródło: opracowanie własne.*

W oknie na rys. B.1 widocznych jest sześć obszarów odpowiedzialnych za:

- edycję danych wejściowych (Dane wejściowe – edytuj tutaj),
- odczyt danych wejściowych po zakończonej edycji (Dane wejściowe – odczyt),
- odczyt par zabronionych (Pary zabronione),
- odczyt wszystkich możliwych rozwiązań wraz z parami zabronionymi (Wszystkie rozwiązania),
- odczyt rozwiązań dozwolonych, bez rozwiązań zawierających pary zabronione (Rozwiązania dozwolone),
- odczyt rozwiązań z parami zabronionymi (Odrzucone rozwiązania).

Ponadto okno aplikacji zawiera przyciski:

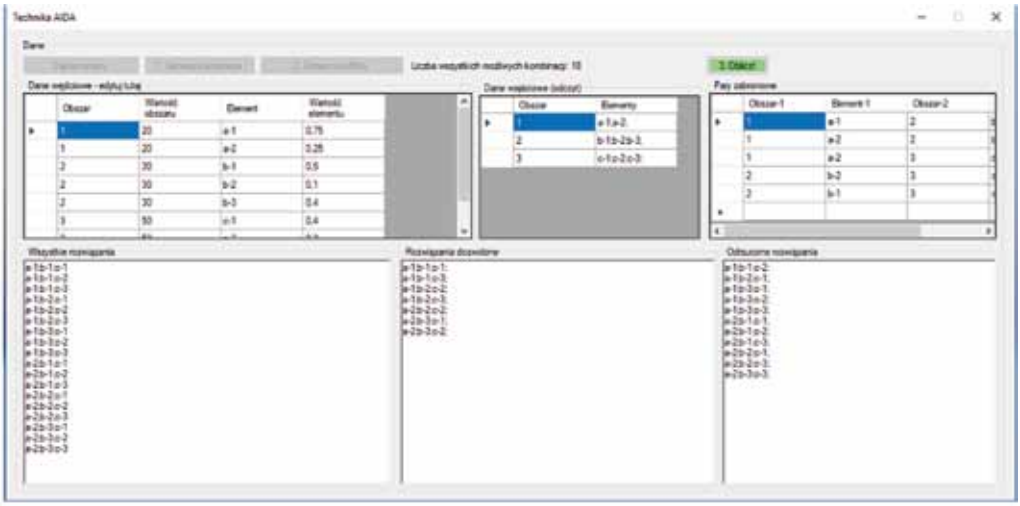
- generuj kombinacje – przycisk pozwala na wygenerowanie kombinacji decyzji elementarnych po jednej z każdego obszaru decyzyjnego,
- oznacz konflikty – przycisk usuwający decyzje zawierające pary sprzeczne ze zbioru rozwiązań problemu decyzyjnego,
- oblicz – przycisk umożliwiający wygenerowanie wartości oceny kosztowej dozwolonych rozwiązań.

W pierwszej kolejności do aplikacji wprowadza się liczbę obszarów decyzyjnych. Następnie wprowadza się wartości istotności dla kolejnych obszarów decyzyjnych oraz liczbę i wartości istotności decyzji elementarnych dla każdego obszaru decyzyjnego. Po tym kroku aplikacja sprawdza czy wartości istotności decyzji elementarnych sumują się do wartości 1. W przypadku, gdy sumy się nie zgadzają, aplikacja generuje odpowiedni komunikat informujący o błędzie.

Wprowadzenie liczby obszarów decyzyjnych dla rozpatrywanego problemu decyzyjnego oraz liczby decyzji elementarnych dla poszczególnych obszarów decyzyjnych

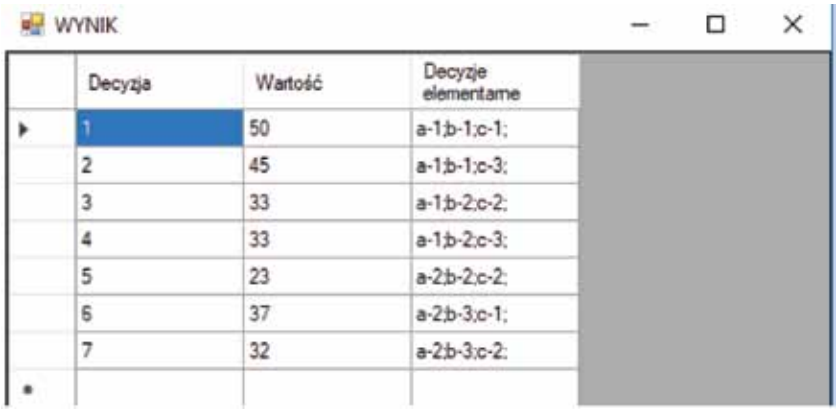
i przypisanie im wartości istotności umożliwia zdefiniowanie zbioru par pozostających w relacji sprzeczności.

W kolejnym kroku aplikacja pozwala na odczyt wprowadzonych danych oraz ich edycję, jeśli istnieje taka potrzeba, a także na wygenerowanie możliwych wszystkich kombinacji rozwiązań poprzez wciśnięcie przycisku „Generuj kombinację" i usunięcie z tego zbioru rozwiązań zawierających pary sprzeczne w wyniku wciśnięcia przycisku „Oznacz konflikty" (rys. B.2).



Rysunek B.2. Wygenerowanie zbioru rozwiązań problemu decyzyjnego
Źródło: opracowanie własne.

Na tym etapie wciśnięcie przycisku „Oblicz" pozwala wygenerować wartości oceny kosztowej decyzji rozwiązujących problem decyzyjny możliwych do zastosowania, tzn. z wyłączeniem decyzji zawierających pary w relacji sprzeczności (rys. B.3).



Decyzja	Wartość	Decyzje elementarne
1	50	a-1;b-1;c-1;
2	45	a-1;b-1;c-3;
3	33	a-1;b-2;c-2;
4	33	a-1;b-2;c-3;
5	23	a-2;b-2;c-2;
6	37	a-2;b-3;c-1;
7	32	a-2;b-3;c-2;

Rysunek B.3. Wartości oceny kosztowej dla rozwiązań problemu decyzyjnego
Źródło: opracowanie własne.

Uzyskane wyniki oraz liczba możliwych decyzji rozwiązujących problem decyzyjny jest zgodna w wynikami opisanymi w artykule [Krupa, Ostrowska, 2012, ss. 25–31] (tab. B.2).

Tabela B.2. Wagi istotności decyzji dla przykładu problemu decyzyjnego

Nr decyzji	Decyzja	Waga istotności decyzji
1	$<\{d_{11}\},\{d_{12}\},\{d_{13}\}>$	$Q_1 = 20 \times 0{,}75 + 30 \times 0{,}50 + 50 \times 0{,}40 = 50$
2	$<\{d_{11}\}\{d_{12}\}\{d_{33}\}>$	$Q_2 = 20 \times 0{,}75 + 30 \times 0{,}50 + 50 \times 0{,}30 = 45$
3	$<\{d_{21}\}\{d_{22}\}\{d_{23}\}>$	$Q_3 = 20 \times 0{,}25 + 30 \times 0{,}10 + 50 \times 0{,}30 = 23$
4	$<\{d_{21}\}\{d_{32}\}\{d_{13}\}>$	$Q_4 = 20 \times 0{,}25 + 30 \times 0{,}40 + 50 \times 0{,}40 = 37$
5	$<\{d_{21}\}\{d_{32}\}\{d_{23}\}>$	$Q_5 = 20 \times 0{,}25 + 30 \times 0{,}40 + 50 \times 0{,}30 = 32$
6	$<\{d_{11}\}\{d_{22}\}\{d_{23}\}>$	$Q_6 = 20 \times 0{,}75 + 30 \times 0{,}10 + 50 \times 0{,}30 = 33$
7	$<\{d_{11}\}\{d_{22}\}\{d_{33}\}>$	$Q_7 = 20 \times 0{,}75 + 30 \times 0{,}10 + 50 \times 0{,}30 = 33$

Źródło: Krupa, Ostrowska, 2012, s. 27.

Załącznik C – Przykłady obliczeniowe zastosowania elementów IM-BIK

Część A – Odwzorowanie charakterystyki IK za pomocą modelu sytuacji

Przykładem ilustrującym określenie charakterystyki IK za pomocą modelu sytuacji IK jest system dwóch IK funkcjonujących w obrębie jednego miasta.

Niech V_1 oznacza szpital, a V_2 rafinerię naftową. Natomiast V_3 otoczenie rozpatrywanych IK (miasto), które może wpływać na IK i na które mogą oddziaływać IK V_1 i V_2.

Szpital IK V_1 jest podatny na zagrożenie:

- pożaru ($Z_{1,1}$),
- suszy ($Z_{1,2}$),
- skażenia środowiska – silne zadymienie ($Z_{1,3}$),
- ograniczenia personelu ($Z_{1,4}$).

Operator V_1 w odpowiedzi na rozpoznane zagrożenia wprowadził następujące zabezpieczenia:

- system środków gaśniczych – koc gaśniczy, gaśnica typu A, B, hydrant z wężem gaśniczym na każdym piętrze ($M_{1,1,1}$),
- własne ujęcie wody pitnej ($M_{1,2,1}$),
- system filtrów powietrza ($M_{1,3,1}$),
- możliwość mobilizacji personelu niebędącego na dyżurze ($M_{1,4,1}$).

Szpital charakteryzuje się trzema funkcjonalnościami:

- oddziałem leczenia oparzeń ($\Phi_{1,1}$),
- lądowiskiem dla LPR ($\Phi_{1,2}$),
- dostępnością personelu ($\Phi_{1,3}$).

Rafineria IK V_2 podatna jest na zagrożenie:

- pożaru ($Z_{2,1}$),
- suszy ($Z_{2,2}$),
- awarii technicznej ($Z_{2,3}$).

Operator V_2 w odpowiedzi na rozpoznane zagrożenia wprowadził następujące zabezpieczenia:

- zakładową straż pożarną ($M_{2,1,1}$),
- system środków gaśniczych ($M_{2,1,2}$),
- kombinezony ochronne ($M_{2,1,3}$),
- zapas wody pitnej ($M_{2,2,1}$),
- dział utrzymania ruchu ($M_{2,3,1}$).

Rafineria charakteryzuje się trzema funkcjonalnościami:

- instalacją produkcji olefin ($\Phi_{2,1}$),
- oczyszczaniem spalin ($\Phi_{2,2}$),
- bezpieczeństwem personelu ($\Phi_{2,3}$).

Dodatkowo otoczenie szpitala i rafinerii (V_3) wzbudza zagrożenie suszy ($Z_{3,1}$) z prawdopodobieństwem 0,2 i podatnością $U_{3,1} = 0{,}11$, na które obie IK są podatne. Ponadto zagrożenie $Z_{2,1}$ – pożaru wzbudza zagrożenie $Z_{3,2}$ – skażenia środowiska – silne zadymienie, którego prawdopodobieństwo wynosi 0,1 i na które podatne jest otoczenie V_3 ($U_{3,2} = 0{,}32$).

W sposób syntetyczny charakterystyka IK V_1 oraz V_2 została zobrazowana w tab. C.1 przedstawiającej dane dotyczące: zasobów, funkcjonalności, zagrożeń oraz zabezpieczeń.

Tabela C.1. Przykład syntetycznego zapisu sytuacji IK V_1 i V_2

IK	Funkcjonalności		Zagrożenia									Podatność na zagrożenie
								Zabezpieczenie				
	Symbol	Wartość	Symbol	Rodzaj	Wzbudzane zagrożenie	Prawdopodobieństwo	Ograniczenie funkcjonalności IK	Symbol	Stopień obniżenia podatności	Cel zarządzania kryzysowego	Obszar ochrony IK	
V_1	$\Phi_{1,1}$	70%	$Z_{1,1}$	IN	–	0,3	-30%($\Phi_{1,1}$) -20%($\Phi_{1,3}$)	$M_{1,1,1}$	0,05	Przejmowanie kontroli	Bezpieczeństwo techniczne	0,5
			$Z_{1,2}$	OUT	awaria techniczna	0,4	-10%($\Phi_{1,3}$)	$M_{1,2,1}$	0,9	Zapobieganie	Ciągłość działania	0,8
	$\Phi_{1,2}$	100%	$Z_{1,3}$	OUT	awaria techniczna zwiększona liczba poszkodowanych	0,05	-100%($\Phi_{1,2}$) -15%($\Phi_{1,3}$)	$M_{1,3,1}$	0,3	Zapobieganie	Bezpieczeństwo techniczne	0,7
	$\Phi_{1,3}$	85%	$Z_{1,4}$	OUT	–	0,65	-50%($\Phi_{1,1}$) -5%($\Phi_{1,3}$) -10%($\Phi_{1,2}$)	$M_{1,4,1}$	0,04	Przejmowanie kontroli	Ciągłość działania	0,65
V_2	$\Phi_{2,1}$	85%	$Z_{2,1}$	IN	skażenie środowiska silne zadymienie zwiększona liczba poszkodowanych	0,5	-100%($\Phi_{2,1}$)	$M_{2,1,1}$	0,4	Zapobieganie	Bezpieczeństwo techniczne	0,7
							-50%($\Phi_{2,2}$)	$M_{2,1,2}$	0,1	Przejmowanie kontroli	Bezpieczeństwo techniczne	
							-30%($\Phi_{2,3}$)	$M_{2,1,3}$	0,05	Reagowanie w przypadku wystąpienia	Bezpieczeństwo fizyczne	
	$\Phi_{2,2}$	100%	$Z_{2,2}$	OUT	awaria techniczna	0,4	-10%($\Phi_{2,3}$)	$M_{2,2,1}$	0,1	Reagowanie w przypadku wystąpienia	Ciągłość działania	0,8
	$\Phi_{2,3}$	90%	$Z_{2,3}$	IN	pożar	0,35	-40%($\Phi_{2,1}$) -35%($\Phi_{2,2}$) -15%($\Phi_{2,3}$)	$M_{2,3,1}$	0,35	Zapobieganie Reagowanie w przypadku wystąpienia	Bezpieczeństwo techniczne Ciągłość działania	0,65

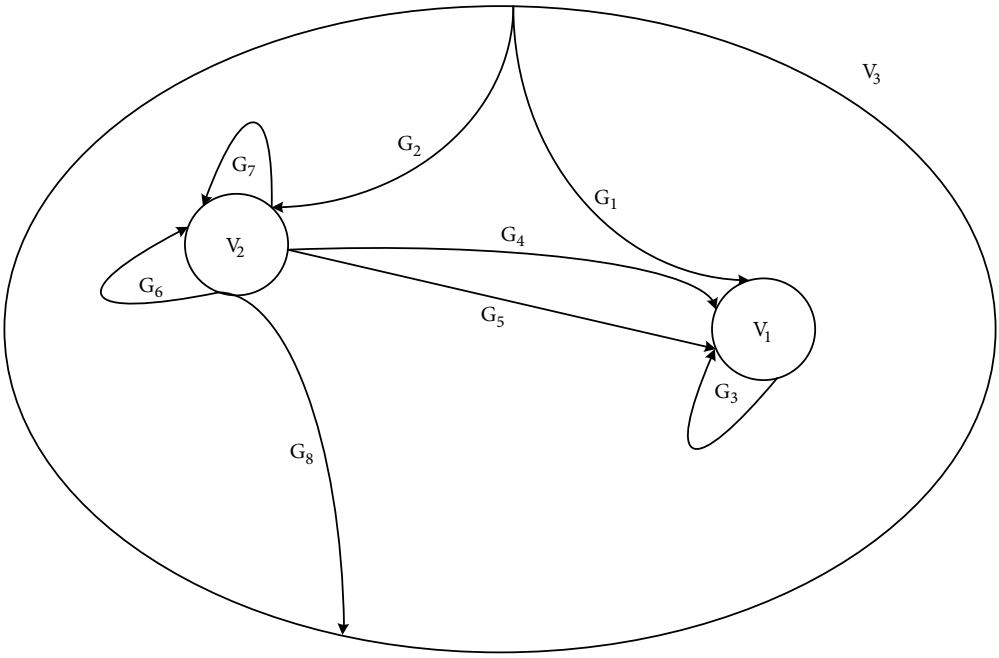
Źródło: opracowanie własne.

Uzupełnieniem modeli sytuacji V_1 i V_2 jest tab. C.2 ilustrująca zależności między IK. Graficzną ilustrację IK V_1 i V_2, z uwzględnieniem otoczenia V_3, przedstawia rys. C.1.

Tabela C.2. Przykład syntetycznego zapisu zależności zagrożeń i IK

Symbol zasobu:	**V_3**	
Symbol zależności	**Zasób zależny**	**Zagrożenie wpływające**
G_1	V_1	Susza
G_2	V_2	
Symbol zasobu:	**V_1**	
G_3	V_1	Pożar
Symbol zasobu:	**V_2**	
G_4	V_1	Zwiększona liczba poszkodowanych
G_5	V_1	Skażenie środowiska - silne zadymienie
G_6	V_2	Pożar
G_7	V_2	Awaria techniczna
G_8	V_3	Skażenie środowiska - silne zadymienie

Źródło: opracowanie własne.



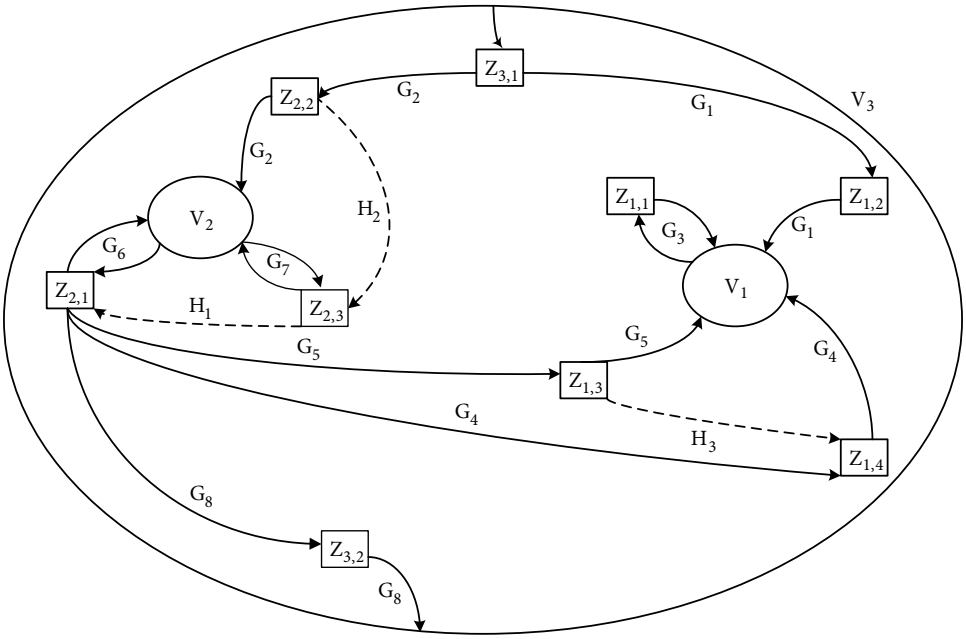
Rysunek C.1. Przykład graficznej ilustracji zależności IK

Źródło: opracowanie własne.

Sformułowanie modelu sytuacji IK pozwala na określenie charakterystyki pojedynczej IK jak i zbioru IK, co obrazuje przedstawiony przykład (tab. C.1). Określenie sytuacji grupy IK pozwala na przeanalizowanie wzajemnego oddziaływania IK (rys. C.1) i daje możliwość przewidzenia przebiegu zdarzenia niekorzystnego.

Część B – Scenariusze rozwoju zdarzeń niekorzystnych

Rysunek C.2 przedstawia rozpatrywany w części A przykład sytuacji IK szpitala (V_1), rafinerii (V_2) oraz ich otoczenia (V_3). Na rys. C.2 oznaczono zależności rozpatrywanych IK (strzałki ↓, zależność: G_1; G_2; G_3; G_4; G_5; G_6; G_7; G_8). Zagrożenia oznaczone w modelu sytuacji IK jako wewnętrzne (rys. C.2, strzałki ↑↓, zależności G_3; G_6; G_7) są wywoływane przez rozpatrywaną IK i wpływają bezpośrednio na nią (rys. C.2, zagrożenia: $Z_{1,1}$; $Z_{2,1}$; $Z_{2,3}$). Strzałki przerywane oznaczają zależności zagrożeń wynikające z modelu sytuacji IK (tab. C.1, zależność H_1; H_2; H_3).



Elipsy oznaczają IK (V_α), prostokąty oznaczają zagrożenia ($Z_{\alpha,\beta}$), strzałki ciągłe oznaczają zależności rozpatrywanych IK (G_n), strzałki przerywane oznaczają zależność zagrożeń (H_n)

Rysunek C.2. Przykład identyfikacji zależności IK w rozpatrywanym SPIK

Źródło: opracowanie własne.

Analizując rys. C.2, można rozpoznać część zależności IK wskazanych w tab. C.2. Zależności te wynikają z zagrożeń wewnętrznych wskazujących, że rozpatrywana IK oddziałuje sama na siebie (rys. C.2, zależności: G_3, G_6 i G_7). Pozostałe zależności wynikają z informacji o zagrożeniach wzbudzanych przez materializację zagrożeń, na które podatne są IK.

Przykładem jest zagrożenie $Z_{2,1}$ – pożaru w rafinerii, które oprócz negatywnych skutków dla funkcjonalności rafinerii wzbudza zagrożenie $Z_{1,3}$ – skażenia środowiska – silne zadymienie. Na to zagrożenie podatny jest szpital, dla którego jest ono zagrożeniem zewnętrznym. Pożar w rafinerii tworzy warunki sprzyjające wystąpieniu zdarzenia niekorzystnego ($Z_{1,3}$) oddziałującego na szpital co wskazuje na istnienie zależności (G_5) między rafinerią a szpitalem.

Zależności między IK chociaż wynikają z rozpatrywanych modeli sytuacji IK to jednak nie mogą być generowane automatycznie. Przykładem jest zagrożenie $Z_{1,1}$ – pożaru, na które jest podatny szpital (V_1). Materializacja tego zagrożenia, podobnie jak w przypadku zagrożenia $Z_{3,1}$ – suszy powinna wzbudzić zagrożenie $Z_{2,1}$ – pożaru, na który podatna jest rafineria. Jednak SPIK przedstawiony na rys. C.2 nie uwzględnia takiej zależności. Zależność ta została pominięta ze względu na zbyt dużą odległość szpitala (V_1) od rafinerii (V_2). W takich przypadkach dużą rolę odgrywa doświadczenie osoby konstruującej SPIK na podstawie modeli sytuacji IK, która musi zinterpretować dostępne dane i zdecydować, czy istnieje zależność.

Innym przykładem braku oddziaływania zdarzenia niekorzystnego na zasób jest przypadek zagrożenia $Z_{1,3}$ – skażenie środowiska – silne zadymienie, którego wystąpienie wzbudza zagrożenie awarii technicznej oraz ograniczenia personelu. Na rys. C.2 oznaczono możliwość wzbudzenia przez zagrożenie $Z_{1,3}$ zagrożenia $Z_{1,4}$ – ograniczenia personelu, pomijając zagrożenie awarii technicznej. Stało się tak, ponieważ w modelu sytuacji IK (V_1) nie wskazano, że jest ona podatna na to zagrożenie.

Sposób rozpoznawania zależności składowych SPIK wskazuje na dwie reguły:

- jeśli rozpatrywane zagrożenie wzbudza inne zagrożenie, na które podatne są składowe SPIK, to istnieje potencjalna zależność między składowymi SPIK, która musi być zweryfikowana i potwierdzona przez podmiot odpowiedzialny za bezpieczeństwo IK,
- jeżeli rozpatrywane zagrożenie wzbudza inne zagrożenie, na które nie są podatne składowe SPIK, to nie istnieje zależność między składowymi SPIK.

W tab. C.3 przedstawiono syntetyczny zapis podatności składowych SPIK (rys. C.2) na zagrożenia, przygotowany na podstawie tab. C.2.

W tab. C.4 przedstawiono syntetyczny zapis zależności zagrożeń[123] występujących w SPIK (rys. C.2), przygotowany na podstawie tab. C.2.

Zebrane w tab. C.3 i C.4 dane pozwoliły na opracowanie modelu SPIK, który zaimplementowano w narzędziu informatycznym, zgodnie z zasadami opisanymi w zał. A. Na podstawie symulacji przeprowadzonej na próbie 1000 wzbudzeń zagrożenia $Z_{3,1}$ – suszy uzyskano 18 SZN, z których 11 zakończyło się negatywnymi skutkami dla szpitala, rafinerii lub ich otoczenia. Dane dotyczące wszystkich uzyskanych SZN przedstawiono w tab. C.5.

[123] Dane zawarte w tab. 2.3d należy interpretować następująco, np. zagrożenie $Z_{1,3}$ wzbudza zagrożenie $Z_{1,4}$. Prawdopodobieństwo wystąpienia pary tych zagrożeń razem wynosi 0,0325 ($P_{1,3} * P_{1,4}$).

Tabela C.3. Przykład opisu oddziaływania zagrożeń wewnętrznych na rozpatrywany system

Wyszczególnienie	V_1		V_2		V_3	
	P	U	P	U	P	U
		M		M		M
$Z_{1,1}$	0,30	0,50				
		0,05				
$Z_{1,2}$	0,40	0,80				
		0,90				
$Z_{1,3}$	0,05	0,70				
		0,30				
$Z_{1,4}$	0,65	0,65				
		0,04				
$Z_{2,1}$			0,50	0,70		
				0,4+0,1+0,05		
$Z_{2,2}$			0,40	0,8		
				0,10		
$Z_{2,3}$			0,35	0,65		
				0,35		
$Z_{3,1}$					0,20	0,11
						0
$Z_{3,2}$					0,10	0,32
						0

Źródło: opracowanie własne.

Tabela C.4. Przykład opisu zależności zagrożeń

Zagrożenie	$Z'_{1,1}$		$Z'_{1,2}$		$Z'_{1,3}$		$Z'_{1,4}$		$Z'_{2,1}$		$Z'_{2,2}$		$Z'_{2,3}$		$Z'_{3,1}$		$Z'_{3,2}$	
$Z_{1,1}$																		
$Z_{1,2}$																		
$Z_{1,3}$							$P'_{1,4}$	0,65										
							$P_{1,3}$	0,05										
$Z_{1,4}$																		
$Z_{2,1}$					$P'_{1,3}$	0,05	$P'_{1,4}$	0,65									$P'_{3,2}$	0,10
					$P_{2,1}$	0,50	$P_{2,1}$	0,50									$P_{2,1}$	0,50
$Z_{2,2}$													$P'_{2,3}$	0,35				
													$P_{2,2}$	0,40				
$Z_{2,3}$									$P'_{2,1}$	0,50								
									$P_{2,3}$	0,35								
$Z_{3,1}$			$P'_{1,2}$	0,40							$P'_{2,2}$	0,40						
			$P_{3,1}$	0,20							$P_{3,1}$	0,20						
$Z_{3,2}$																		

Źródło: opracowanie własne.

Dane zamieszczone w tab. C.5 należy odczytywać w następujący sposób:

- pojedynczy element scenariusza oznaczony literą „D" oznacza, że zagrożenie $Z_{\alpha,\beta}$ zostało wzbudzone, tzn. zaistniały warunki sprzyjające jego wystąpieniu. Jeżeli w kolejnej kolumnie nie ma elementu $Z_{\alpha,\beta}$ oznaczonego literą „P", tzn. że mimo warunków sprzyjających zagrożenie nie zmaterializowało się;
- sekwencję elementów scenariusza $Z_{\alpha,\beta}$-D, $Z_{\alpha,\beta}$-P, należy odczytywać jako zaistnienie sprzyjających warunków i materializację zagrożenia $Z_{\alpha,\beta}$. Jeżeli w kolejnej kolumnie nie ma elementu $Z_{\alpha,\beta}$ oznaczonego literą „R", tzn. że mimo materializacja zagrożenia zasób V_α nie ucierpiał, tzn. funkcjonalności zasobu V_α są dostępne na poziomie sprzed materializacji zagrożenia. Taka sytuacja oznacza, że zasób V_α okazał się odporny na zagrożenie $Z_{\alpha,\beta}$;
- sekwencję elementów scenariusza $Z_{\alpha,\beta}$-D, $Z_{\alpha,\beta}$-P, $Z_{\alpha,\beta}$-R należy odczytywać jako materializację zagrożenia $Z_{\alpha,\beta}$, w wyniku którego zasób V_α ucierpiał, tzn. poziom funkcjonalności zasobu V_α jest niższy niż przed materializacją zagrożenia lub całkowicie utracono funkcjonalność rozpatrywanej IK.

Tabela C.5. Podsumowanie przypadków SZN dla zagrożenia $Z_{3,1}$ – susza

Wyszczególnienie	Sekwencja zdarzeń			Liczba przypadków	Rozkład
	Wzbudzenie	Materializacja	Skutek		
Scenariusz 1	$Z_{2,2}$-D	$Z_{2,2}$-P	$Z_{2,2}$-R	25	2,50%
	$Z_{2,3}$-D				
	$Z_{1,2}$-D				
	$Z_{3,1}$-D	$Z_{3,1}$-P			
Scenariusz 2	$Z_{2,2}$-D	$Z_{2,2}$-P	$Z_{2,2}$-R	15	1,50%
	$Z_{2,3}$-D				
	$Z_{1,2}$-D	$Z_{1,2}$-P			
	$Z_{3,1}$-D	$Z_{3,1}$-P			
	$Z_{1,2}$-P				
Scenariusz 3	$Z_{2,1}$-D			10	1,00%
	$Z_{2,2}$-D	$Z_{2,2}$-P	$Z_{2,2}$-R		
	$Z_{2,3}$-D	$Z_{2,3}$-P			
	$Z_{1,2}$-D	$Z_{1,2}$-P			
	$Z_{3,1}$-D				
Scenariusz 4	$Z_{2,1}$-D			14	1,40%
	$Z_{2,2}$-D	$Z_{2,2}$-P	$Z_{2,2}$-R		
	$Z_{2,3}$-D	$Z_{2,3}$-P			
	$Z_{1,2}$-D				
	$Z_{3,1}$-D	$Z_{3,1}$-P			

Wyszczególnienie	Sekwencja zdarzeń			Liczba przypadków	Rozkład
	Wzbudzenie	Materializacja	Skutek		
Scenariusz 5	$Z_{2,1}$-D	$Z_{2,1}$-P		1	0,10%
	$Z_{2,2}$-D	$Z_{2,2}$-P			
	$Z_{2,3}$-D	$Z_{2,3}$-P			
	$Z_{1,2}$-D	$Z_{1,2}$-P			
	$Z_{1,3}$-D				
	$Z_{1,4}$-D	$Z_{1,4}$-P	$Z_{1,4}$-R		
	$Z_{3,1}$-D	$Z_{3,1}$-P			
	$Z_{3,2}$-D				
Scenariusz 6	$Z_{2,1}$-D			1	0,10%
	$Z_{2,2}$-D	$Z_{2,2}$-P			
	$Z_{2,3}$-D	$Z_{2,3}$-P	$Z_{2,3}$-R		
	$Z_{1,2}$-D				
	$Z_{3,1}$-D	$Z_{3,1}$-P			
Scenariusz 7	$Z_{2,1}$-D	$Z_{2,1}$-P		1	0,10%
	$Z_{2,2}$-D	$Z_{2,2}$-P			
	$Z_{2,3}$-D	$Z_{2,3}$-P	$Z_{2,3}$-R		
	$Z_{1,2}$-D				
	$Z_{1,3}$-D				
	$Z_{1,4}$-D	$Z_{1,4}$-P	$Z_{1,4}$-R		
	$Z_{3,1}$-D	$Z_{3,1}$-P			
	$Z_{3,2}$-D				
Scenariusz 8	$Z_{2,1}$-D	$Z_{2,1}$-P		1	0,10%
	$Z_{2,2}$-D	$Z_{2,2}$-P			
	$Z_{2,3}$-D	$Z_{2,3}$-P			
	$Z_{1,2}$-D				
	$Z_{1,3}$-D				
	$Z_{1,4}$-D	$Z_{1,4}$-P	$Z_{1,4}$-R		
	$Z_{3,1}$-D	$Z_{3,1}$-P			
	$Z_{3,2}$-D				
Scenariusz 9	$Z_{2,1}$-D			1	0,10%
	$Z_{2,2}$-D	$Z_{2,2}$-P	$Z_{2,2}$-R		
	$Z_{2,3}$-D	$Z_{2,3}$-P			
	$Z_{1,2}$-D	$Z_{1,2}$-P			
	$Z_{3,1}$-D	$Z_{3,1}$-P			

Wyszczególnienie	Sekwencja zdarzeń			Liczba przypadków	Rozkład
	Wzbudzenie	Materializacja	Skutek		
Scenariusz 10	$Z_{2,1}$-D			1	0,10%
	$Z_{2,2}$-D	$Z_{2,2}$-P			
	$Z_{2,3}$-D	$Z_{2,3}$-P	$Z_{2,3}$-R		
	$Z_{1,2}$-D	$Z_{1,2}$-P			
	$Z_{3,1}$-D	$Z_{3,1}$-P			
Scenariusz 11	$Z_{2,1}$-D	$Z_{2,1}$-P		1	0,10%
	$Z_{2,2}$-D	$Z_{2,2}$-P			
	$Z_{2,3}$-D	$Z_{2,3}$-P	$Z_{2,3}$-R		
	$Z_{1,2}$-D				
	$Z_{1,3}$-D				
	$Z_{1,4}$-D				
	$Z_{3,1}$-D	$Z_{3,1}$-P			
	$Z_{3,2}$-D				
Scenariusz 12	$Z_{3,1}$-D			811	81,10%
Scenariusz 13	$Z_{2,2}$-D			60	6,00%
	$Z_{1,2}$-D				
	$Z_{3,1}$-D	$Z_{3,1}$-P			
Scenariusz 14	$Z_{2,2}$-D			44	4,40%
	$Z_{1,2}$-D	$Z_{1,2}$-P			
	$Z_{3,1}$-D	$Z_{3,1}$-P			
Scenariusz 15	$Z_{2,1}$-D	$Z_{2,1}$-P		1	0,10%
	$Z_{2,2}$-D	$Z_{2,2}$-P			
	$Z_{2,3}$-D	$Z_{2,3}$-P			
	$Z_{1,2}$-D				
	$Z_{1,3}$-D				
	$Z_{1,4}$-D				
	$Z_{3,1}$-D	$Z_{3,1}$-P			
	$Z_{3,2}$-D				
Scenariusz 16	$Z_{2,2}$-D	$Z_{2,2}$-P		7	0,70%
	$Z_{2,3}$-D				
	$Z_{1,2}$-D				
	$Z_{3,1}$-D	$Z_{3,1}$-P			
Scenariusz 17	$Z_{2,2}$-D	$Z_{2,2}$-P		4	0,40%
	$Z_{2,3}$-D				
	$Z_{1,2}$-D	$Z_{1,2}$-P			
	$Z_{3,1}$-D	$Z_{3,1}$-P			

Wyszczególnienie	Sekwencja zdarzeń			Liczba przypadków	Rozkład
	Wzbudzenie	Materializacja	Skutek		
Scenariusz 18	$Z_{2,1}$-D			2	0,20%
	$Z_{2,2}$-D	$Z_{2,2}$-P			
	$Z_{2,3}$-D	$Z_{2,3}$-P			
	$Z_{1,2}$-D				
	$Z_{3,1}$-D	$Z_{3,1}$-P			
Wszystkie przypadki				1000	100,00%

Źródło: opracowanie własne.

Interpretację danych zawartych w tab. C.5 przedstawiono na przykładzie scenariusza 7 (przykład scenariusza o negatywnych skutkach dla składowych SPIK) oraz scenariusza 18 (przykład scenariusza bez negatywnych skutków dla składowych SPIK).

W ramach scenariusza 7, który wystąpił jeden raz, zostało wzbudnych osiem zagrożeń ($Z_{1,2}$; $Z_{1,3}$; $Z_{1,4}$; $Z_{2,1}$; $Z_{2,2}$; $Z_{2,3}$; $Z_{3,1}$ i $Z_{3,2}$). W wyniku zaistnienia sprzyjających warunków pięć zagrożeń zmaterializowało się ($Z_{1,4}$; $Z_{2,1}$; $Z_{2,2}$; $Z_{2,3}$ i $Z3_{,1}$), w wyniku czego zasób V_1 – szpital i zasób V_2 – rafineria zostały narażone na negatywne skutki objawiające się obniżeniem dostępności funkcjonalności. Materializacja zagrożeń wywołała zdarzenia niekorzystne ($Z_{1,4}$ i $Z_{2,3}$) dla zasobu V_1 (zagrożenie $Z_{1,4}$ – ograniczenia personelu wywołało negatywne skutki określone w tab. C.1) i zasób V_2 (zagrożenie $Z_{2,3}$ – awarii technicznej wywołało negatywne skutki określone w tab. C.1)

W ramach scenariusza 18, który wystąpił dwa razy, zostało wzbudnych pięć zagrożeń ($Z_{1,2}$; $Z_{2,1}$; $Z_{2,2}$; $Z_{2,3}$ i $Z_{3,1}$). W wyniku zaistnienia sprzyjających warunków zmaterializowały się dwa zagrożenia ($Z_{2,2}$; $Z_{2,3}$ i $Z_{3,1}$), w wyniku czego zasób V_2 – rafineria został narażony na negatywne skutki. Materializacja zagrożeń nie wywołała jednak zdarzenia niekorzystnego skutkującego obniżeniem dostępności funkcjonalności rozpatrywanej IK.

Część C – Szacowanie ryzyka dla SZN

Obliczenie wartości ryzyka związanego z rozpatrywanym zagrożeniem, na które podatna jest IK wymaga określenia przez podmiot odpowiedzialny za bezpieczeństwo IK jaka funkcjonalność jest narażona na negatywne skutki materializacji zagrożenia. SZN realizujący się w SPIK może integrować wiele IK, czego przykładem jest scenariusz 7 (tab. C.5). W takim przypadku wspólna funkcjonalność dla zbioru IK występujących w scenariuszu może nie istnieć. Nie stanowi to przeszkody dla obliczenia ryzyka związanego ze SZN.

W przypadku gdy tak jak w scenariuszu 7 nie istnieje wspólna funkcjonalność dla składowych SPIK, podmiot odpowiedzialny za bezpieczeństwo IK decyduje, która funkcjonalność spośród zbioru funkcjonalności rozpatrywanych IK znajduje się w kręgu jego zainteresowań. Po wyborze funkcjonalności stosowany jest wzór na ryzyko 2.3c[124]

[124] Wyjątkiem jest sytuacja, w której tylko jedno zagrożenie występujące w SZN ma wpływ na rozpatrywaną IK. Wówczas do obliczenia ryzyka utraty funkcjonalności stosuje się wzór 2.3b.

uwzględniający wszystkie IK zawarte w SZN, które mają wpływ na rozpatrywaną funkcjonalność ($\Delta\Phi \neq 0$).

Istotna zmiana w stosunku do obliczania wartości ryzyka dla modelu sytuacji IK i SZN dotyczy parametru odpowiedzialnego za prawdopodobieństwo wystąpienia zagrożenia. Zagrożenia zawarte w SZN wpływają na IK w wyniku materializacji innych zagrożeń. Skąd znając wynik SZN (tzn. zagrożenia, które negatywnie wpłynęły na rozpatrywaną funkcjonalność IK) należy zastosować twierdzenie Bayesa w celu ustalenia prawdopodobieństwa materializacji rozpatrywanego zagrożenia pod warunkiem zaistnienia innych zagrożeń, które do niego doprowadziły.

Przykład ilustrujący obliczenie wartości ryzyka dla SZN wykorzystuje dane ze scenariusza 7 (tab. C.5). W ramach eksperymentu obliczeniowego badany jest wpływ zagrożeń występujących w scenariuszu na funkcjonalność instalacji produkcji olefin ($\Phi_{2,1}$). Scenariusz 7 zakłada, że zostało wzbudnych osiem zagrożeń ($Z_{1,2}$; $Z_{1,3}$; $Z_{1,4}$; $Z_{2,1}$; $Z_{2,2}$; $Z_{2,3}$; $Z_{3,1}$ i $Z_{3,2}$). W wyniku zaistnienia sprzyjających warunków pięć zagrożeń zmaterializowało się ($Z_{1,4}$; $Z_{2,1}$; $Z_{2,2}$; $Z_{2,3}$ i $Z_{3,1}$), co spowodowało, że zasób V_1 – szpital i zasób V_2 – rafineria zostały narażone na negatywne skutki, objawiające się obniżeniem poziomu funkcjonalności. Materializacja zagrożeń wywołała zdarzenia niekorzystne ($Z_{1,4}$ i $Z_{2,3}$) dla zasobu V_1 (zagrożenie $Z_{1,4}$ – ograniczenia personelu wywołało negatywne skutki określone w tab. C.1) i zasobu V_2 (zagrożenie $Z_{2,3}$ – awarii technicznej wywołało negatywne skutki określone w tab. C.1). Z punktu widzenia rozpatrywanej funkcjonalności $\Phi_{2,1}$ istotne jest tylko zagrożenie $Z_{2,3.}$ Wykorzystując model SPIK przedstawiony na rys. C.2, można odtworzyć przebieg SZN i ustalić, że wystąpienie zagrożenia $Z_{2,3}$ było poprzedzone zagrożeniem $Z_{2,2}$ i $Z_{3,1}$. Pozwala to na obliczenie prawdopodobieństwa wystąpienia zagrożenia $Z_{2,3}$ pod warunkiem materializacji zagrożeń $Z_{2,2}$ i $Z_{3,1}$.

$$P(Z_{2,3}|Z_{2,2}; Z_{3,1}) = \frac{P_{2,3} * 0,(3)}{0,(3) * [(P_{2,3}) + (P_{2,2}) + (P_{3,1})]} = 0,316$$

Uzyskany wynik prawdopodobieństwa wystąpienia zagrożenia $Z_{2,3}$ pod warunkiem materializacji zagrożeń $Z_{2,2}$ i $Z_{3,1}$ podstawiony do wzoru na ryzyko (2.3b) pozwala na obliczenie ryzyka utraty funkcjonalności $\Phi_{2,1}$, jakie jest związane ze SZN nr 7.

$$R_{2,3} = P_{1,1} * |\Delta\Phi_{2,1}| * (U_{2,3} - M_{2,3,1}) = 0,316 * |-40\%| * (0,65 - 0,35) = 3,792\%$$

Z przeprowadzonego eksperymentu obliczeniowego wynika, że ryzyko utraty funkcjonalności $\Phi_{2,1}$ – instalacji produkcji olefin wynikające ze scenariusza 7 wynosi 3,792%.

W analizowanym przypadku tylko zagrożenie $Z_{2,3}$ zmaterializowało się i oddziaływało negatywnie na funkcjonalności $\Phi_{2,1}$. Stąd wartość ryzyka dla tego zagrożenia stanowi jednocześnie wartość ryzyka dla funkcjonalności $\Phi_{2,1}$ wynikającego ze SZN nr 7.

Część D – Przykład problemu decyzyjnego wynikającego ze SZN

Problem decyzyjny dla SZN sformułowano na podstawie scenariusza nr 7 (tab. C.5), w którym:

- zagrożenie $Z_{1,4}$ – ograniczenia personelu negatywnie wpływa na IK V_1 – szpital,
- zagrożenie $Z_{2,3}$ – awarii technicznej negatywnie wpływa na IK V_2 – rafineria.

Celem założonym przez operatorów rozpatrywanych IK jest maksymalne obniżenie podatności SPIK utworzonego z IK V_1 i V_2 na zagrożenia wynikające ze SZN nr 7. Jednocześnie poziom podatności na zagrożenie nie może przekroczyć wartości 0,2 dla żadnej z rozpatrywanych IK.

Na potrzeby eksperymentu obliczeniowego przyjmuje się stan wynikający z modeli sytuacji IK V_1 i V_2 (tab. C.1). Oznacza to, że bazowa podatność:

- IK V_1 na zagrożenie $Z_{1,4}$ wynosi $U_{1,4} = 0{,}65$,
- IK V_2 na zagrożenie $Z_{2,3}$ wynosi $U_{2,3} = 0{,}65$.
- operator IK V_1 stosuje zabezpieczenie przed zagrożeniem $Z_{1,4}$ w postaci $M_{1,4,1}$ – mobilizacji personelu niebędącego na dyżurze, które obniża podatność IK V_1 na zagrożenie $Z_{1,4}$ o 0,04 do poziomu $U'_{1,4} = 0{,}61$,
- operator IK V_2 stosuje zabezpieczenie przed zagrożeniem $Z_{2,3}$ w postaci $M_{2,3,1}$ – działu utrzymania ruchu, które obniża podatność IK V_2 na zagrożenie $Z_{2,3}$ o 0,35 do poziomu $U'_{2,3} = 0{,}3$.

Przyjmując założenia dotyczące podatności IK V_1 i V_2 na zagrożenia $Z_{1,4}$ i $Z_{2,3}$ oraz wpływ zabezpieczeń obliczono względną istotność obszarów decyzyjnych (wg wzoru 2.5d).

$$D_{1,4} = \frac{U'_{1,4}}{U'_{1,4} + U'_{2,3}} * 100 = \frac{0{,}61}{0{,}61 + 0{,}3} * 100 \approx 67$$

$$D_{2,3} = \frac{U'_{2,3}}{U'_{1,4} + U'_{2,3}} * 100 = \frac{0{,}3}{0{,}61 + 0{,}3} * 100 \approx 33$$

Dodatkowymi zabezpieczeniami możliwymi do zastosowania w reakcji na rozpoznane zagrożenia są:

- dla zagrożenia $Z_{1,4}$:
  - zabezpieczenie $M_{1,4,2}$ – transport poszkodowanych do innych szpitali, które obniża podatność IK V_1 na zagrożenie $Z_{1,4}$ o $m_{1,4,2} = 0{,}45$,
  - zabezpieczenie $M_{1,4,3}$ – mobilizacja personelu z innych szpitali, które obniża podatność IK V_1 na zagrożenie $Z_{1,4}$ o $m_{1,4,3} = 0{,}42$,
  - zabezpieczenie $M_{1,4,4}$ – mobilizacja wojskowego personelu medycznego, które obniża podatność IK V_1 na zagrożenie $Z_{1,4}$ o $m_{1,4,4} = 0{,}35$,
- dla zagrożenia $Z_{2,3}$:
  - zabezpieczenie $M_{2,3,2}$ – produkcja na innym urządzeniu, które obniża podatność IK V_2 na zagrożenie $Z_{2,3}$ o $m_{2,3,2} = 0{,}2$,
  - zabezpieczenie $M_{2,3,3}$ – zlecenie produkcji innemu zakładowi, które obniża podatność IK V_2 na zagrożenie $Z_{2,3}$ o $m_{2,3,3} = 0{,}1$.

Przyjmując założenia dotyczące zabezpieczeń przed zagrożeniami $Z_{1,4}$ i $Z_{2,3}$, obliczono względną istotność decyzji elementarnych w obszarach decyzyjnych, stosując wzór 2.5b.

$$d_{1,4,2} = \frac{m_{1,4,2}}{\sum_{\lambda=2}^{4} m_{1,4,\lambda}} = \frac{0,45}{0,45+0,42+0,35} \approx 0,37$$

$$d_{1,4,3} = \frac{m_{1,4,3}}{\sum_{\lambda=2}^{4} m_{1,4,\lambda}} = \frac{0,42}{0,45+0,42+0,35} \approx 0,34$$

$$d_{1,4,4} = \frac{m_{1,4,4}}{\sum_{\lambda=2}^{4} m_{1,4,\lambda}} = \frac{0,35}{0,45+0,42+0,35} \approx 0,29$$

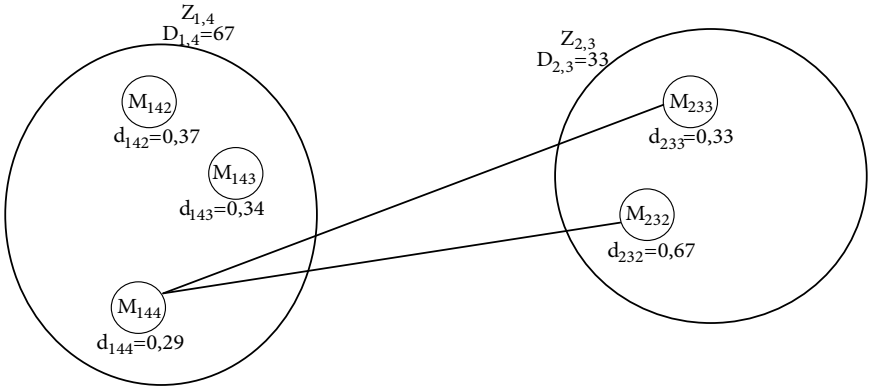
$$d_{2,3,2} = \frac{m_{2,3,2}}{\sum_{\lambda=2}^{3} m_{2,3,\lambda}} = \frac{0,2}{0,2+0,1} \approx 0,67$$

$$d_{2,3,3} = \frac{m_{2,3,3}}{\sum_{\lambda=2}^{3} m_{2,3,\lambda}} = \frac{0,1}{0,2+0,1} \approx 0,33$$

Dla rozpatrywanego problemu decyzyjnego, wskazano pary w relacji sprzeczności[125]:

- $M_{1,4,4} - M_{2,3,2}$
- $M_{1,4,4} - M_{2,3,3}$

Rysunek C.3 ilustruje problem decyzyjny wynikający z SZN nr 7 dla IK V_1 i V_2.



Rysunek C.3. Przykład problemu decyzyjnego bazującego na SZN nr 7 dla IK V_1 i V_2

Źródło: opracowanie własne.

Uwzględniając sprzeczność par decyzji elementarnych, wskazano macierz krotek rozwiązujących problem decyzyjny (tab. C.6).

[125] Sprzeczność w tym przypadku wynika z faktu, że zastosowanie zabezpieczenia $M_{1,4,4}$ nie pozwala na obniżenie podatności IK V_1 do wymaganego poziomu. Oznaczenie ww. par sprzecznych decyzji elementarnych pozwala na ograniczenie zbioru rozwiązań tylko do tych, które spełniają warunek minimum funkcji celu. Podobny efekt można osiągnąć poprzez wykluczenie zabezpieczenia $M_{1,4,4}$ ze zbioru możliwych rozwiązań dla obszaru decyzyjnego $Z_{1,4}$.

Tabela C.6. Macierz możliwych rozwiązań problemu decyzyjnego bazującego na SZN nr 7 dla IK V_1 i V_2

	$M_{1,4,\lambda}$	$M_{2,3,\lambda}$
Decyzja 1	$d_{1,4,2}$	$d_{2,3,2}$
Decyzja 2	$d_{1,4,2}$	$d_{2,3,3}$
Decyzja 3	$d_{1,4,3}$	$d_{2,3,2}$
Decyzja 4	$d_{1,4,3}$	$d_{2,3,3}$

Źródło: opracowanie własne.

Podstawiając wartości względnej istotności poszczególnych decyzji elementarnych oraz przemnażając uzyskaną macierz przez macierz względnej istotności obszarów decyzyjnych, uzyskano ocenę kosztową poszczególnych decyzji (tab. C.7).

Tabela C.7. Obliczenie wartości możliwych rozwiązań problemu decyzyjnego bazującego na SZN nr 7 dla IK V_1 i V_2

	$d_{1,4,\lambda}$	$d_{2,3,\lambda}$		$D_{\alpha,\beta}$		Ocena kosztowa
Decyzja 1	0,37	0,64		67		46,9
Decyzja 2	0,37	0,64	*	33	=	35,68
Decyzja 3	0,34	0,36				44,89
Decyzja 4	0,34	0,64				33,67

Źródło: opracowanie własne.

Z danych przedstawionych w tab. C.7 wynika, że zabezpieczenie transportu poszkodowanych do innych szpitali oraz produkcji na innym urządzeniu najefektywniej realizuje założony cel (maksymalnie obniża podatności SPIK utworzonego z IK V_1 i V_2, na zagrożenia wynikające ze SZN nr 7 oraz utrzymanie podatność IK na każde z rozpatrywanych zagrożeń poniżej poziomu 0,2). Podatności IK V_1 i V_2 po wdrożeniu sugerowanych zabezpieczeń przedstawia tab. C.8.

Tabela C.8. Zestawienie wartości ryzyka utraty funkcjonalności i wartości funkcjonalności dla rozwiązań problemu decyzyjnego

Decyzja	Ocena kosztowa	Wartość podatności uwzględniająca nowe zabezpieczenia V_1	Wartość podatności uwzględniająca nowe zabezpieczenia V_2
1	**46,9**	**0,16**	**0,1**
2	35,68	0,16	0,2
3	44,89	0,19	0,1
4	33,67	0,19	0,2

Źródło: opracowanie własne.

Załącznik D – Wykaz scenariuszy zdarzeń niekorzystnych dla rafinerii PKN ORLEN S.A.

W tab. D.1 przedstawiono SZN, w wyniku których przewiduje się utratę funkcjonalności dla przynajmniej jednej z rozpatrywanych IK.

Tabela D.1. Wykaz SZN dla SPIK rafinerii PKN ORLEN S.A., Basell Orlen Polyolefins sp. z o.o. oraz Zakładu Produkcyjnego ORLEN OIL sp. z o.o. w Płocku

Wyszczególnienie	Wzbudzenie	Materializacja	Skutek	Liczba przypadków	Rozkład
Scenariusz 1	Z2,1-D	Z2,1-P		14	1,4%
	Z2,2-D				
	Z2,3-D				
	Z3,1-D	Z3,1-P			
	Z3,2-D				
	Z3,3-D				
	Z1,1-D	Z1,1-P	Z1,1-R		
	Z1,2-D	Z1,2-P			
	Z1,3-D	Z1,3-P			
Scenariusz 2	Z2,1-D			16	1,6%
	Z2,2-D	Z2,2-P	Z2,2-R		
Scenariusz 3	Z2,1-D	Z2,1-P		4	0,4%
	Z2,2-D				
	Z2,3-D				
	Z3,1-D	Z3,1-P			
	Z3,2-D	Z3,2-P			
	Z3,3-D				
	Z1,1-D	Z1,1-P			
	Z1,2-D	Z1,2-P	Z1,2-R		
	Z1,3-D	Z1,3-P			
Scenariusz 4	Z2,1-D			2	0,2%
	Z3,1-D	Z3,1-P			
	Z3,2-D				
	Z3,3-D				
	Z1,1-D	Z1,1-P	Z1,1-R		
	Z1,2-D				
	Z1,3-D				
Scenariusz 5	Z2,1-D			21	2,1%
	Z3,1-D				
	Z1,1-D	Z1,1-P			
	Z1,2-D	Z1,2-P	Z1,2-R		
	Z1,3-D				

Wyszczególnienie	Wzbudzenie	Materializacja	Skutek	Liczba przypadków	Rozkład
Scenariusz 6	Z2,1-D	Z2,1-P		6	0,6%
	Z2,2-D				
	Z2,3-D				
	Z3,1-D	Z3,1-P			
	Z3,2-D				
	Z3,3-D				
	Z1,1-D	Z1,1-P	Z1,1-R		
	Z1,2-D				
	Z1,3-D	Z1,3-P			
Scenariusz 7	Z2,1-D	Z2,1-P		4	0,4%
	Z2,2-D	Z2,2-P			
	Z2,3-D				
	Z3,1-D	Z3,1-P			
	Z3,2-D				
	Z3,3-D				
	Z1,1-D	Z1,1-P			
	Z1,2-D	Z1,2-P	Z1,2-R		
	Z1,3-D	Z1,3-P			
Scenariusz 8	Z2,1-D	Z2,1-P		1	0,1%
	Z2,2-D				
	Z2,3-D				
	Z3,1-D	Z3,1-P			
	Z3,2-D				
	Z3,3-D				
	Z1,1-D	Z1,1-P			
	Z1,2-D	Z1,2-P	Z1,2-R		
	Z1,3-D				
Scenariusz 9	Z2,1-D	Z2,1-P		74	7,4%
	Z2,2-D				
	Z2,3-D				
	Z3,1-D	Z3,1-P			
	Z3,2-D				
	Z3,3-D				
	Z1,1-D	Z1,1-P			
	Z1,2-D	Z1,2-P	Z1,2-R		
	Z1,3-D	Z1,3-P			
Scenariusz 10	Z2,3-D	Z2,3-P	Z2,3-R	18	1,8%

Wyszczególnienie	Wzbudzenie	Materializacja	Skutek	Liczba przypadków	Rozkład
Scenariusz 11	Z2,1-D	Z2,1-P		15	1,5%
	Z2,2-D				
	Z2,3-D				
	Z3,1-D	Z3,1-P			
	Z3,2-D				
	Z3,3-D				
	Z1,1-D	Z1,1-P			
	Z1,2-D				
	Z1,3-D	Z1,3-P	Z1,3-R		
Scenariusz 12	Z1,3-D	Z1,3-P	Z1,3-R	11	1,1%
Scenariusz 13	Z2,1-D	Z2,1-P		7	0,7%
	Z2,2-D				
	Z2,3-D				
	Z3,1-D	Z3,1-P			
	Z3,2-D				
	Z3,3-D				
	Z1,1-D	Z1,1-P			
	Z1,2-D	Z1,2-P	Z1,2-R		
	Z1,3-D	Z1,3-P	Z1,3-R		
Scenariusz 14	Z2,1-D	Z2,1-P		6	0,6%
	Z2,2-D				
	Z2,3-D				
	Z3,1-D				
	Z1,1-D	Z1,1-P			
	Z1,2-D	Z1,2-P	Z1,2-R		
	Z1,3-D	Z1,3-P			
Scenariusz 15	Z1,1-D			8	0,8%
	Z1,2-D	Z1,2-P	Z1,2-R		
Scenariusz 16	Z2,1-D	Z2,1-P		5	0,5%
	Z2,2-D				
	Z2,3-D				
	Z3,1-D	Z3,1-P			
	Z3,2-D				
	Z3,3-D				
	Z1,1-D	Z1,1-P	Z1,1-R		
	Z1,2-D	Z1,2-P	Z1,2-R		
	Z1,3-D	Z1,3-P			

Wyszczególnienie	Wzbudzenie	Materializacja	Skutek	Liczba przypadków	Rozkład
Scenariusz 17	Z2,1-D	Z2,1-P		4	0,4%
	Z2,2-D				
	Z2,3-D				
	Z3,1-D	Z3,1-P			
	Z3,2-D	Z3,2-P	Z3,2-R		
	Z3,3-D				
	Z1,1-D	Z1,1-P	Z1,1-R		
	Z1,2-D	Z1,2-P			
	Z1,3-D	Z1,3-P			
Scenariusz 18	Z2,1-D			11	1,1%
	Z3,1-D	Z3,1-P			
	Z3,2-D				
	Z3,3-D				
	Z1,1-D	Z1,1-P			
	Z1,2-D	Z1,2-P	Z1,2-R		
	Z1,3-D	Z1,3-P			
Scenariusz 19	Z2,1-D			2	0,2%
	Z3,1-D	Z3,1-P			
	Z3,2-D				
	Z3,3-D				
	Z1,1-D	Z1,1-P	Z1,1-R		
	Z1,2-D	Z1,2-P			
	Z1,3-D	Z1,3-P			
Scenariusz 20	Z2,1-D	Z2,1-P		1	0,1%
	Z2,2-D				
	Z2,3-D				
	Z3,1-D	Z3,1-P			
	Z3,2-D	Z3,2-P	Z3,2-R		
	Z3,3-D				
	Z1,1-D	Z1,1-P	Z1,1-R		
	Z1,2-D				
	Z1,3-D	Z1,3-P			
Scenariusz 21	Z2,1-D	Z2,1-P		3	0,3%
	Z2,2-D				
	Z2,3-D				
	Z3,1-D	Z3,1-P			
	Z3,2-D				
	Z3,3-D				
	Z1,1-D	Z1,1-P	Z1,1-R		
	Z1,2-D	Z1,2-P	Z1,2-R		
	Z1,3-D	Z1,3-P	Z1,3-R		

Wyszczególnienie	Wzbudzenie	Materializacja	Skutek	Liczba przypadków	Rozkład
Scenariusz 22	Z2,1-D			3	0,3%
	Z3,1-D				
	Z1,1-D				
	Z1,2-D	Z1,2-P			
	Z1,3-D	Z1,3-P	Z1,3-R		
Scenariusz 23	Z2,1-D	Z2,1-P		2	0,2%
	Z2,2-D				
	Z2,3-D				
	Z3,1-D	Z3,1-P			
	Z3,2-D	Z3,2-P	Z3,2-R		
	Z3,3-D				
	Z1,1-D	Z1,1-P	Z1,1-R		
	Z1,2-D	Z1,2-P	Z1,2-R		
	Z1,3-D	Z1,3-P			
Scenariusz 24	Z2,1-D			2	0,2%
	Z3,1-D	Z3,1-P			
	Z3,2-D				
	Z3,3-D				
	Z1,1-D	Z1,1-P	Z1,1-R		
	Z1,2-D				
	Z1,3-D	Z1,3-P			
Scenariusz 25	Z2,1-D			4	0,4%
	Z3,1-D	Z3,1-P			
	Z3,2-D				
	Z3,3-D				
	Z1,1-D	Z1,1-P			
	Z1,2-D	Z1,2-P	Z1,2-R		
	Z1,3-D				
Scenariusz 26	Z2,1-D			1	0,1%
	Z3,1-D	Z3,1-P			
	Z3,2-D				
	Z3,3-D				
	Z1,1-D	Z1,1-P	Z1,1-R		
	Z1,2-D	Z1,2-P			
	Z1,3-D				
Scenariusz 27	Z2,1-D			3	0,3%
	Z3,1-D				
	Z1,1-D	Z1,1-P			
	Z1,2-D	Z1,2-P	Z1,2-R		
	Z1,3-D	Z1,3-P			

Wyszczególnienie	Wzbudzenie	Materializacja	Skutek	Liczba przypadków	Rozkład
Scenariusz 28	Z2,1-D			2	0,2%
	Z2,2-D				
	Z2,3-D				
	Z3,1-D	Z3,1-P			
	Z3,2-D	Z3,2-P	Z3,2-R		
	Z3,3-D				
	Z1,1-D	Z1,1-P	Z1,1-R		
	Z1,2-D	Z1,2-P			
	Z1,3-D	Z1,3-P	Z1,3-R		
Scenariusz 29	Z2,1-D	Z2,1-P		1	0,1%
	Z2,2-D	Z2,2-P	Z2,2-R		
	Z2,3-D				
	Z3,1-D	Z3,1-P			
	Z3,2-D				
	Z3,3-D				
	Z1,1-D	Z1,1-P	Z1,1-R		
	Z1,2-D	Z1,2-P			
	Z1,3-D	Z1,3-P			
Scenariusz 30	Z2,1-D	Z2,1-P		3	0,3%
	Z2,2-D	Z2,2-P	Z2,2-R		
	Z2,3-D				
	Z3,1-D	Z3,1-P			
	Z3,2-D				
	Z3,3-D				
	Z1,1-D	Z1,1-P			
	Z1,2-D	Z1,2-P	Z1,2-R		
	Z1,3-D	Z1,3-P			
Scenariusz 31	Z2,1-D			2	0,2%
	Z3,1-D				
	Z1,1-D	Z1,1-P			
	Z1,2-D				
	Z1,3-D	Z1,3-P	Z1,3-R		
Scenariusz 32	Z2,1-D	Z2,1-P		6	0,6%
	Z2,2-D				
	Z2,3-D				
	Z3,1-D	Z3,1-P			
	Z3,2-D	Z3,2-P	Z3,2-R		
	Z3,3-D				
	Z1,1-D	Z1,1-P			
	Z1,2-D	Z1,2-P	Z1,2-R		
	Z1,3-D	Z1,3-P			

Wyszczególnienie	Wzbudzenie	Materializacja	Skutek	Liczba przypadków	Rozkład
Scenariusz 33	Z2,1-D	Z2,1-P		1	0,1%
	Z2,2-D				
	Z2,3-D				
	Z3,1-D				
	Z1,1-D	Z1,1-P	Z1,1-R		
	Z1,2-D				
	Z1,3-D	Z1,3-P			
Scenariusz 34	Z2,1-D			1	0,1%
	Z3,1-D	Z3,1-P			
	Z3,2-D	Z3,2-P			
	Z3,3-D				
	Z1,1-D	Z1,1-P			
	Z1,2-D	Z1,2-P	Z1,2-R		
	Z1,3-D	Z1,3-P			
Scenariusz 35	Z3,1-D			15	1,5%
	Z3,2-D	Z3,2-P	Z3,2-R		
Scenariusz 36	Z2,1-D			1	0,1%
	Z3,1-D				
	Z1,1-D	Z1,1-P	Z1,1-R		
	Z1,2-D	Z1,2-P			
	Z1,3-D				
Scenariusz 37	Z2,1-D	Z2,1-P		1	0,1%
	Z2,2-D				
	Z2,3-D				
	Z3,1-D	Z3,1-P			
	Z3,2-D				
	Z3,3-D				
	Z1,1-D	Z1,1-P	Z1,1-R		
	Z1,2-D				
	Z1,3-D				
Scenariusz 38	Z2,1-D	Z2,1-P		4	0,4%
	Z2,2-D				
	Z2,3-D				
	Z3,1-D	Z3,1-P			
	Z3,2-D				
	Z3,3-D				
	Z1,1-D	Z1,1-P			
	Z1,2-D	Z1,2-P			
	Z1,3-D	Z1,3-P	Z1,3-R		
Scenariusz 39	Z2,1-D			1	0,1%
	Z3,1-D				
	Z1,1-D	Z1,1-P	Z1,1-R		
	Z1,2-D				
	Z1,3-D	Z1,3-P			

Wyszczególnienie	Wzbudzenie	Materializacja	Skutek	Liczba przypadków	Rozkład
Scenariusz 40	Z2,1-D	Z2,1-P		1	0,1%
	Z2,2-D	Z2,2-P	Z2,2-R		
	Z2,3-D				
	Z3,1-D				
	Z1,1-D	Z1,1-P	Z1,1-R		
	Z1,2-D				
	Z1,3-D	Z1,3-P			
Scenariusz 41	Z2,1-D	Z2,1-P		1	0,1%
	Z2,2-D				
	Z2,3-D				
	Z3,1-D				
	Z1,1-D	Z1,1-P	Z1,1-R		
	Z1,2-D	Z1,2-P			
	Z1,3-D				
Scenariusz 42	Z2,1-D			2	0,2%
	Z3,1-D	Z3,1-P			
	Z3,2-D	Z3,2-P	Z3,2-R		
	Z3,3-D				
	Z1,1-D	Z1,1-P			
	Z1,2-D				
	Z1,3-D	Z1,3-P	Z1,3-R		
Scenariusz 43	Z2,1-D	Z2,1-P		2	0,2%
	Z2,2-D	Z2,2-P	Z2,2-R		
	Z2,3-D				
	Z3,1-D	Z3,1-P			
	Z3,2-D				
	Z3,3-D				
	Z1,1-D	Z1,1-P			
	Z1,2-D	Z1,2-P	Z1,2-R		
	Z1,3-D	Z1,3-P	Z1,3-R		
Scenariusz 44	Z2,1-D	Z2,1-P		1	0,1%
	Z2,2-D	Z2,2-P			
	Z2,3-D				
	Z3,1-D	Z3,1-P			
	Z3,2-D				
	Z3,3-D				
	Z1,1-D	Z1,1-P	Z1,1-R		
	Z1,2-D	Z1,2-P			
	Z1,3-D	Z1,3-P			

Wyszczególnienie	Wzbudzenie	Materializacja	Skutek	Liczba przypadków	Rozkład
Scenariusz 45	Z2,1-D			1	0,1%
	Z3,1-D	Z3,1-P			
	Z3,2-D	Z3,2-P	Z3,2-R		
	Z3,3-D				
	Z1,1-D	Z1,1-P			
	Z1,2-D	Z1,2-P	Z1,2-R		
	Z1,3-D	Z1,3-P			
Scenariusz 46	Z2,1-D			1	0,1%
	Z3,1-D				
	Z1,1-D	Z1,1-P	Z1,1-R		
	Z1,2-D	Z1,2-P			
	Z1,3-D	Z1,3-P			
Scenariusz 47	Z3,3-D	Z3,3-P	Z3,3-R	4	0,4%
Scenariusz 48	Z2,1-D	Z2,1-P		1	0,1%
	Z2,2-D				
	Z2,3-D				
	Z3,1-D	Z3,1-P			
	Z3,2-D	Z3,2-P	Z3,2-R		
	Z3,3-D				
	Z1,1-D	Z1,1-P			
	Z1,2-D	Z1,2-P			
	Z1,3-D	Z1,3-P	Z1,3-R		
Scenariusz 49	Z2,1-D	Z2,1-P		1	0,1%
	Z2,2-D				
	Z2,3-D				
	Z3,1-D				
	Z1,1-D	Z1,1-P			
	Z1,2-D	Z1,2-P	Z1,2-R		
	Z1,3-D	Z1,3-P	Z1,3-R		
Scenariusz 50	Z2,1-D	Z2,1-P		1	0,1%
	Z2,2-D				
	Z2,3-D				
	Z3,1-D	Z3,1-P			
	Z3,2-D	Z3,2-P			
	Z3,3-D				
	Z1,1-D	Z1,1-P			
	Z1,2-D				
	Z1,3-D	Z1,3-P	Z1,3-R		

Wyszczególnienie	Wzbudzenie	Materializacja	Skutek	Liczba przypadków	Rozkład
Scenariusz 51	Z2,1-D	Z2,1-P		1	0,1%
	Z2,2-D				
	Z2,3-D				
	Z3,1-D	Z3,1-P			
	Z3,2-D				
	Z3,3-D				
	Z1,1-D	Z1,1-P	Z1,1-R		
	Z1,2-D	Z1,2-P			
	Z1,3-D	Z1,3-P	Z1,3-R		
Scenariusz 52	Z2,1-D	Z2,1-P		1	0,1%
	Z2,2-D				
	Z2,3-D				
	Z3,1-D				
	Z3,2-D				
	Z3,3-D				
	Z1,1-D	Z1,1-P			
	Z1,2-D	Z1,2-P	Z1,2-R		
	Z1,3-D	Z1,3-P	Z1,3-R		
Scenariusz 53	Z2,1-D			1	0,1%
	Z3,1-D	Z3,1-P			
	Z3,2-D				
	Z3,3-D				
	Z1,1-D	Z1,1-P			
	Z1,2-D				
	Z1,3-D	Z1,3-P	Z1,3-R		
Scenariusz 54	Z2,1-D			1	0,1%
	Z3,1-D	Z3,1-P			
	Z3,2-D				
	Z3,3-D				
	Z1,1-D	Z1,1-P			
	Z1,2-D				
	Z1,3-D	Z1,3-P	Z1,3-R		
Scenariusz 70	Z2,1-D	Z2,1-P		3	0,3%
	Z2,2-D	Z2,2-P	Z2,2-R		
	Z2,3-D				
	Z3,1-D				
	Z1,1-D				
Scenariusz 74	Z2,1-D			1	0,1%
	Z3,1-D	Z3,1-P			
	Z3,2-D	Z3,2-P	Z3,2-R		
	Z3,3-D				
	Z1,1-D	Z1,1-P			
	Z1,2-D				
	Z1,3-D	Z1,3-P			

Wyszczególnienie	Wzbudzenie	Materializacja	Skutek	Liczba przypadków	Rozkład
Scenariusz 83	Z2,1-D			2	0,2%
	Z3,1-D	Z3,1-P			
	Z3,2-D	Z3,2-P	Z3,2-R		
	Z3,3-D				
	Z1,1-D				
Scenariusz 85	Z2,1-D			1	0,1%
	Z3,1-D	Z3,1-P			
	Z3,2-D	Z3,2-P	Z3,2-R		
	Z3,3-D				
	Z1,1-D	Z1,1-P			
	Z1,2-D	Z1,2-P			
	Z1,3-D	Z1,3-P			
Scenariusz 88	Z2,1-D	Z2,1-P		1	0,1%
	Z2,2-D				
	Z2,3-D				
	Z3,1-D	Z3,1-P			
	Z3,2-D	Z3,2-P	Z3,2-R		
	Z3,3-D				
	Z1,1-D				
Scenariusz 90	Z2,1-D	Z2,1-P		1	0,1%
	Z2,2-D	Z2,2-P	Z2,2-R		
	Z2,3-D				
	Z3,1-D	Z3,1-P			
	Z3,2-D				
	Z3,3-D				
	Z1,1-D	Z1,1-P			
	Z1,2-D				
	Z1,3-D	Z1,3-P			
Scenariusz 91	Z2,1-D	Z2,1-P		1	0,1%
	Z2,2-D	Z2,2-P	Z2,2-R		
	Z2,3-D				
	Z3,1-D	Z3,1-P			
	Z3,2-D				
	Z3,3-D				
	Z1,1-D				

Źródło: opracowanie własne.

Załącznik E – Wybrane akty normatywne i planistyczne dotyczące zarządzania bezpieczeństwem IK

W załączniku zawarto wykaz danych obligatoryjnych i opcjonalnych związanych z procesem zarzadzania bezpieczeństwem IK pozyskane z aktów normatywnych oraz planistycznych. Dane obligatoryjne pochodzą z:

- Dyrektywy Rady 2008/114/WE z 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania EIK oraz oceny potrzeb w zakresie poprawy jej ochrony;
- Dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii;
- Decyzji Parlamentu Europejskiego i Rady Nr 1313/2013/EU z dnia 17 grudnia 2013 r. w sprawie Unijnego Mechanizmu Ochrony Ludności;
- Ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym;
- Ustawy z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych;
- Rozporządzenia Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie Raportu o zagrożeniach bezpieczeństwa narodowego;
- Rozporządzenia Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie Narodowego Programu Ochrony Infrastruktury Krytycznej;
- Rozporządzenia Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie planów ochrony infrastruktury krytycznej;
- Rozporządzenia Prezesa Rady Ministrów z dnia 14 lipca 2010 r. w sprawie pełnomocnika do spraw ochrony infrastruktury krytycznej;
- Procedury opracowywania raportu cząstkowego do raportu o zagrożeniach bezpieczeństwa narodowego.

Dane opcjonalne zostały pozyskane z:

- Europejskiej Strategii Bezpieczeństwa;
- Europejskiego Programu Ochrony Infrastruktury Krytycznej;
- Strategii bezpieczeństwa narodowego RP;
- Strategii rozwoju kraju 2020;
- Strategii sprawne państwo 2020;
- Strategii rozwoju systemu bezpieczeństwa narodowego RP 2022;
- Narodowego Programu Ochrony Infrastruktury Krytycznej;
- Białej księgi bezpieczeństwa narodowego RP.

Przeanalizowane akty normatywne wskazują, jakie kategorie danych muszą być zgromadzone w ramach procesu zarządzania bezpieczeństwem IK. Ich zestawienie ilustruje tab. E.1.

Tabela E.1. Wykaz danych obligatoryjnych procesu zarządzania bezpieczeństwem IK

Lp.	Kategoria danych	Źródło
1	wykaz obiektów, urządzeń, instalacji oraz usług kluczowych dla bezpieczeństwa państwa	• Dz.U.UE 2016 nr 194 poz. 1, art. 23, pkt 2 • Dz.U. 2017 poz. 209, art. 3, pkt 2 • Dz.U.UE 2008 nr 345 poz. 75, zał II, art. 2 • DZ.U. 2010 nr 83, poz. 541, § 4, ust. 3 • Dz.U. 2010 nr 83 poz. 542, § 2, ust. 3
2	zestawienie potencjalnych zagrożeń wraz z ich charakterystyką	• Dz.U. 2017 poz. 209, art. 3, pkt 8 • Dz.U. 2016 poz. 904, art. 4, pkt 1 • Dz.U. 2004 nr 98 poz. 978, § 3 ust. 1–24 • Dz.U. 2010 nr 83 poz. 540, § 4 • Procedura opracowywania raportu cząstkowego do RZBN, ss. 4–5
3	ocena ryzyka wystąpienia zagrożeń	• Dz.U.UE. 2016 nr 194 poz. 1, art. 6 • Dz.U. 2017 poz. 209, art. 11, pkt 2 • Dz.U.UE. 2008 nr 345 poz. 75, zał II, art. 2 • Dz.U.UE. 2013 nr 347 poz. 924, art. 5 • DZ.U. 2010 nr 83, poz. 541, § 5, ust 1
4	skutki wystąpienia zagrożenia	• Dz.U.UE. 2016 nr 194 poz. 1, art. 6, pkt 1 • Dz.U. 2017 poz. 209, art. 3, pkt 10 • DZ.U. 2010 nr 83, poz. 541, § 7, ust 2 • Dz.U. 2010 nr 83 poz. 542, § 2, ust 3 • Procedura opracowywania raportu cząstkowego do RZBN, ss.10–18
5	obszar geograficzny objęty zasięgiem zagrożenia	• Dz.U. 2017 poz. 209, art. 3, pkt 10 • Dz.U.UE. 2013 nr 347 poz. 924, art. 5 • Dz.U. 2010 nr 83 poz. 540, § 5 ust. 1
6	wykaz wariantów zasięgu zagrożeń	• Dz.U. 2017 poz. 209 art. 3, pkt 9
7	wykaz sił i środków potrzebnych do zażegnania zdarzenia niekorzystnego lub sytuacji kryzysowej	• Dz.U. 2017 poz. 209, art. 5, pkt 2 • Dz.U. 2016 poz. 904, art. 5, pkt 1 • Dz.U. 2004 nr 98 poz. 978, § 4 ust. 2 • DZ.U. 2010 nr 83, poz. 541, § 4, ust. 3 • Procedura opracowywania raportu cząstkowego do RZBN, ss. 20–21
8	wykaz podmiotów odpowiedzialnych za usuwanie zagrożeń	• Dz.U. 2017 poz. 209, art. 4, pkt 3 • Dz.U. 2016 poz. 904, art. 5, pkt 1
9	wykaz struktur uruchamianych w sytuacjach kryzysowych	• Dz.U. 2017 poz. 209, art. 4, pkt 2 • DZ.U. 2010 nr 83, poz. 541, § 4, ust 3 • Dz.U. 2010 nr 83 poz. 542, § 2, ust
10	wykaz zadań i obowiązków uczestników zarządzania kryzysowego	• Dz.U. 2017 poz. 209, art. 5, pkt 2
11	wykaz zawartych umów porozumień związanych z realizacją zadań zawartych w planie zarządzania kryzysowego	• Dz.U. 2017 poz. 209, art. 5, pkt 2
12	wykaz zadań dotyczących monitorowania zagrożeń	• Dz.U. 2017 poz. 209, art. 5, pkt 2

Lp.	Kategoria danych	Źródło
13	scenariusze rozwoju sytuacji kryzysowych	• Dz.U.UE 2016 nr 194 poz. 1, s.7 • Dz.U.UE 2008 nr 345 poz. 75, zał II, art. 2 • Procedura opracowywania raportu cząstkowego do RZBN, ss. 10–18
14	wykaz istniejących rozwiązań służących ochronie IK	• Dz.U.UE 2008 nr 345 poz. 75, zał II, art. 2 • Dz.U.UE 2013 nr 347 poz. 924, art. 8 i 1 • Dz.U. 2004 nr 98 poz. 978, § 3 ust. 1–24
15	analiza podatności IK na zagrożenia	• Dz.U.UE 2008 nr 345 poz. 75, zał II, art. 2
16	procedury komunikacji wewnętrznych służb ochrony z Policją i jednostkami ochrony przeciwpożarowej, obrony cywilnej i strażami gminnymi i miejskimi	• Dz.U. 2010 nr 83 poz. 542, § 2, ust. 3
17	wykaz celów strategicznych dotyczących ochrony IK	• Dz.U. 2010 nr 83 poz. 540, § 4 • Procedura opracowywania raportu cząstkowego do RZNB, ss. 20–21

Źródło: opracowanie na podstawie przeanalizowanych aktów normatywnych.

Przeanalizowane dokumenty planistyczne, tj. strategie, programy i raporty publikowane przez Komisję Europejską, rządy państw lub jednostki powołane do ochrony IK, np. RCB, pozwoliły na ustalenie danych opcjonalnych dla procesu zarządzania bezpieczeństwem IK. Dane te wskazują kierunek w jakim będzie się rozszerzał zbiór danych obligatoryjnych. Ich podsumowanie stanowi tab. E.2.

Tabela E.2. Wykaz elementów planowanych dla procesu zarządzania bezpieczeństwem IK

Lp.	Kategoria danych	Źródło
1	większa koncentracja na zagrożeniach niemilitarnych	• Europejska Strategia Bezpieczeństwa • Strategia rozwoju kraju 2020 • Strategia rozwoju systemu bezpieczeństwa narodowego RP 2022 • NPOIK
2	efektywne wykorzystanie sił i środków	• Europejska Strategia Bezpieczeństwa • Strategia bezpieczeństwa narodowego RP • Strategia rozwoju kraju 2020 • NPOIK
3	zwiększenie spójności działań uczestników procesu zarządzania bezpieczeństwem IK	• Europejska Strategia Bezpieczeństwa • EPOIK • Strategia rozwoju kraju 2020 • Strategia sprawne państwo 2020 • Strategia rozwoju systemu bezpieczeństwa narodowego RP 2022 • Biała księga bezpieczeństwa narodowego RP
4	zwiększenie efektywności obiegu informacji	• Europejska Strategia Bezpieczeństwa • EPOIK • Strategia bezpieczeństwa narodowego RP • Strategia sprawne państwo 2020 • NPOIK

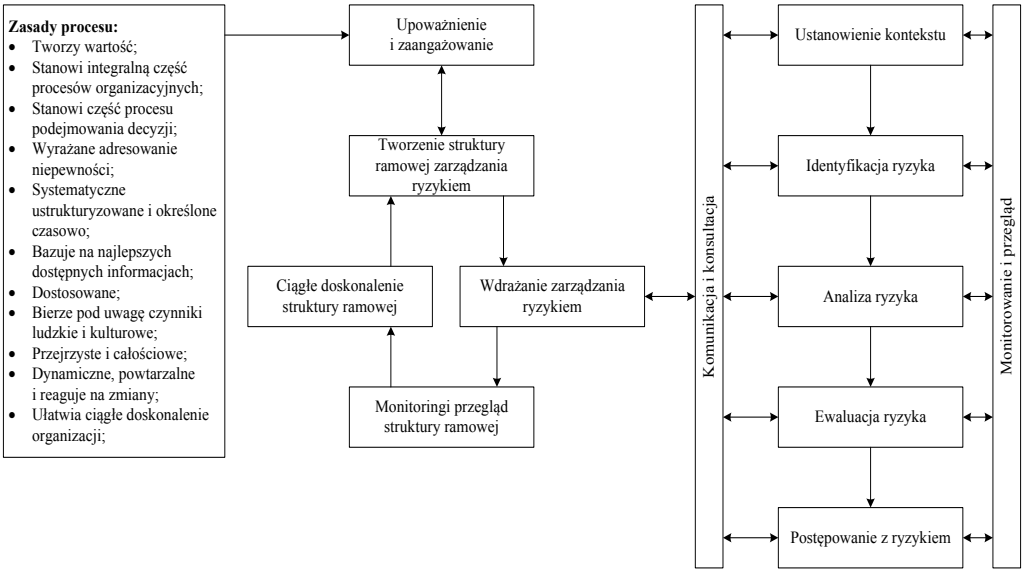
Lp.	Kategoria danych	Źródło
5	opracowanie procedur rozpoznawania współzależności IK	• EPOIK • NPOIK
6	opracowanie planów ciągłości działania	• EPOIK • NPOIK
7	opracowanie procedur określania skutków uszkodzenia lub zniszczenia IK w sferze: społecznej, ekologicznej, ekonomicznej, politycznej, psychologicznej, zdrowia publicznego	• EPOIK
8	wprowadzenie integralnych metod wyznaczania zabezpieczeń przed rozpoznanymi zagrożeniami	• Strategia sprawne państwo 2020 • Strategia rozwoju systemu bezpieczeństwa narodowego RP 2022 • NPOIK
9	wprowadzenia metod weryfikacji modeli zabezpieczeń	• Strategia sprawne państwo 2020 • Strategia rozwoju systemu bezpieczeństwa narodowego RP 2022 • NPOIK
10	procedury odtwarzania IK	• NPOIK
11	przygotowanie wykazu interesariuszy procesu zarządzania bezpieczeństwem IK	• NPOIK • EPOIK
12	uwzględnienie poziomu podatności na zagrożenia	• Biała księga bezpieczeństwa narodowego RP
13	uwzględnienie funkcjonalności IK	• Biała księga bezpieczeństwa narodowego RP • NPOIK
14	uwzględnienie złożoności struktury administracyjnej uczestników procesu zarządzania bezpieczeństwem IK	• Biała księga bezpieczeństwa narodowego RP
15	uwzględnienie celów biznesowych operatorów IK	• Biała księga bezpieczeństwa narodowego RP

Źródło: opracowanie na podstawie przeanalizowanych dokumentów planistycznych.

Załącznik F – Charakterystyka metodyk oceny ryzyka na potrzeby zarządzania kryzysowego

Metodyka Australii

W Australii zasady oceny ryzyka na potrzeby zarządzania kryzysowego zostały zebrane w dokumencie *National Emergency Risk Assessment Guidelines* (NERAG). Zarządzanie kryzysowe w tym kraju jest realizowane zgodnie z wytycznymi normy *ISO 31000:2009 Zarządzanie ryzykiem – Zasady i wytyczne*. Norma zawiera wytyczne w zakresie projektowania, wdrażania, monitorowania, dokonywania przeglądów i ciągłego doskonalenia zarządzania ryzykiem w organizacji. Standard ten może być zastosowany zarówno w sektorze publicznym, jak i prywatnym. Nie jest przeznaczony dla konkretnej branży czy stylu zarządzania. Norma ISO 31000:2009 jako jedna z pierwszych zaproponowała opis procesu zarządzania ryzykiem, który przedstawiono na rys. F.1.



Rysunek F.1. Proces zarządzania ryzykiem wg normy ISO 31000:2009

Źródło: NERAG, 2015, s. 10.

Australijski model oceny ryzyka na potrzeby zarządzania kryzysowego jest ciągle doskonalony pod wpływem zbieranych doświadczeń. Sama metodyka jest podzielona na dwa etapy [Wróblewski, 2015, s. 169]:

- ocena bazowa w celu identyfikacji i szybkiego ukazania ryzyka – ocena, której dokonać mogą osoby o zróżnicowanym poziomie umiejętności technicznych i dysponujące czasem w różnym wymiarze,
- szczegółowa analiza – wymaga specjalnych metod w postaci wykorzystania rekomendowanych modeli lub scenariuszy zdarzeń.

Metodyka australijska stosowana jest na wszystkich szczeblach administracji publicznej. Zalecaną formą identyfikacji zagrożeń są warsztaty, w których uczestniczą przedstawiciele administracji publiczne, operatorzy IK, organizacje pozarządowe oraz społeczność lokalna. Podczas warsztatów wymieniane są informacje dotyczące bieżącej działalności i zdarzeń kryzysowych. Na tej podstawie aktualizowana jest lista zagrożeń. W trakcie warsztatów uczestnicy mają dostęp do [NERAG, 2015, s. 38]:

- wiedzy specjalistycznej odpowiadającej zakresowi tematycznemu warsztatów,
- procedur procesu oceny ryzyka,
- właściwych informacji i baz danych,
- wyników prac studyjnych.

Zakłada się, że warsztaty skutkują: pogłębieniem wiedzy o poszczególnych etapach oceny ryzyka, zdobywaniem doświadczenia w rozwiązywaniu złożonych zagadnień w ramach analizowanych scenariuszy zagrożeń, doskonaleniem pracy zespołowej, przygotowaniem personelu zarówno uczestników warsztatów, jak i obserwatorów.

W ramach metodyki australijskiej wykorzystuje się następujące narzędzia wspierające proces rozpoznawania zagrożeń [NERAG, 2015, ss. 16–22]:

- rejestr zagrożeń, skutków oraz możliwych środków zapobiegawczych,
- skalowanie przestrzenne,
- scenariusze zdarzeń w całym procesie oceny ryzyka,
- usystematyzowane podejście do identyfikacji mechanizmów kontroli i możliwość zastosowania adekwatnych rozwiązań,
- wykaz interesariuszy związanych z danym zagrożeniem,
- ustandaryzowane opisy konsekwencji i prawdopodobieństwa wystąpienia zagrożenia,
- powiązanie przyczyn zagrożenia i jego skutków w postaci diagramu bow-tie,
- ustandaryzowane matryce tolerancji ryzyka,
- kryteria oraz poziomy klasyfikacji ryzyka.

Wybór metody analizy ryzyka jest określony przez kontekst analizy danego zagrożenia oraz dostępne źródła informacji. Stosuje się metody ilościowe, jakościowe lub ilościowo-jakościowe. Metody jakościowe polegają na wykorzystaniu tablic, matryc i wykresów. Metody ilościowe wymagają wykorzystania programów komputerowych, kalkulacji i przeliczeń, które pozwolą określić i zrozumieć parametry ryzyka prezentowane liczbowo.

Rezultatem metodyki jest decyzja o postępowaniu z ryzykiem. Decyzję podejmuje się na podstawie rejestru ryzyka, który jest okresowo aktualizowany. W przypadku konieczności podjęcia działań w reakcji na ocenione ryzyko podejmuje się decyzję o wykonaniu analizy pogłębionej, której wynik wskazuje się działania zapobiegające zagrożeniom lub minimalizujące ryzyko.

Metodyka Szwecji

Z punktu widzenia procesu oceny ryzyka na potrzeby zarządzania kryzysowego w Szwecji istotne są dwa dokumenty. Pierwszy z nich został opublikowany w 2012 roku – *Guide to Risk and Vulenerability Analyses* (GRVA), a drugim jest *Swedish Naional Risk Assessment 2012* (SNRA).

Przewodnik opisuje cztery etapy procesu zarządzania ryzykiem. Wśród nich znalazły się działania z zakresu [GRVA, 2012, ss. 13–77]:

- wdrożenia prewencyjnych i przygotowawczych środków bezpieczeństwa,
- definiowania ról i obszarów odpowiedzialności,
- realizacji procesu analizy ryzyka i podatności,
- wykorzystania metod i narzędzi ułatwiających identyfikację oraz analizę ryzyka.

Swedish Naional Risk Assessment 2012 jest dokumentem, który miał podsumować zrealizowane do chwili jego wydania działania związane z rozwijaniem umiejętności zapobiegania i zarządzania zdarzeniami kryzysowymi na poszczególnych szczeblach zarządzania państwem. Celem tego dokumentu było uzyskanie powszechnego zrozumienia najpoważniejszych zagrożeń dla Szwecji i punktu wyjścia dla wytycznych w zakresie priorytetów dla zasobów krytycznych oraz wdrożenia środków kontroli i brakujących zabezpieczeń [SNRA, 2013, ss. 15–16].

Przewodnik definiuje kluczowe cele oceny ryzyka na potrzeby planowania kryzysowego [GRVA, 2012, s. 7]:

- zmniejszenie ryzyka i skutków poważnych zakłóceń, kryzysów oraz wypadków,
- zapewnienie bezpieczeństwa zdrowotnego i osobistego społeczeństwa,
- zapobieganie lub minimalizację skutków zniszczenia majątku i środowiska.

Proces oceny ryzyka w metodyce szwedzkiej został podzielny na etapy [GRVA, 2012, s.14]:

- Punty startowe – działania dotyczące określenia roli i obszaru odpowiedzialności uczestników procesu oraz określenia metody i perspektywy analiz ryzyka;
- Ocena ryzyka – działania dotyczące oceny, analizy oraz ewaluacji ryzyka;
- Ocena podatności – działania dotyczące oceny zdolności reagowania na zagrożenia oraz analizy podatności na zagrożenia;
- Postępowanie z ryzykiem – działania dotyczące wskazania ocen i wniosków oraz ciągłej pracy na rzecz ulepszania planów ochrony oraz prawidłowego zabezpieczenia odpowiedniej ilości sił i środków niezbędnych do reakcji na sytuacje kryzysowe.

Metodyka szwedzka wymaga, aby zarządzanie ryzykiem było realizowane w ustrukturyzowany i systematyczny sposób. Wytyczne do procesu oceny ryzyka zawarte w przewodniku rozpoczynają się od etapu identyfikacja ryzyka. Według szwedzkiego podejścia identyfikacja ryzyka powinna polegać na rozpoznaniu scenariuszy rozwoju zagrożeń w celu weryfikacji, co może się wydarzyć. Bezpośrednim uzasadnieniem dla powyższego rozwiązania według autorów metodyki jest fakt, że trudniej jest zidentyfikować źródło ryzyka bez świadomości potencjalnych scenariuszy rozwoju zagrożeń [Skomra, 2015, s. 22].

Proces opracowywania scenariuszy wspomagany jest szerokim wyborem narzędzi oraz metodyk, tj. wielowymiarową analizą aktywności (MVA), analizą zagrożeń i wrażliwości (ROSA) czy metodą IBERO [GRVA, 2012, s. 61]. Jedną z praktyk stosowanych w tych metodach jest rozpoczęcie analizy od systematycznego i kompleksowego opisania procesu czy zasobu. Taki opis jest wykonywany najczęściej przy użyciu dwóch typów modeli: strukturalnego lub funkcjonalnego.

Model strukturalny opisuje części organizacji, natomiast funkcjonalny skupia się na zadaniach, procesach lub funkcjach przedsiębiorstwa. W trakcie identyfikacji źródeł ryzyka

lub scenariuszy istotnym jest zidentyfikowanie incydentów i okoliczności, których źródło znajduje się poza organizacją, a może mieć na nią wpływ. Dzięki tym informacjom można dokonać podziału na grupy zdarzeń, m.in.: wypadki, katastrofy naturalne, awarie infrastruktury i/lub systemów wspierających, zagrożenia przeciwstawne, niepokoje społeczne.

Podczas analizy ryzyka szczególny nacisk kładzie się na ocenę prawdopodobieństwa wystąpienia danego scenariusza i jego konsekwencji. Stosuje się kilka metod opisu prawdopodobieństwa wystąpienia scenariusza, tj. analizę drzewa zdarzeń (ETA), drzewa zdarzeń i nadzoru nad ryzykiem (HAZOP), technikę przeglądu zarządzania bezpieczeństwem i organizacją (SMORT), analizę zależności (RIB) oraz bazy danych statystycznych na temat katastrof [GRVA, 2012, s. 71].

Wynikiem metodyki szwedzkiej są decyzje dotyczące priorytetów oraz środków bezpieczeństwa, wskazane na podstawie wyników procesu oceny ryzyka. W metodyce szwedzkiej na uwagę zasługuje zastosowanie podejścia scenariuszowego obejmującego analizę podatności. Rozwiązanie to pozwala na dokładniejsze oszacowanie niezbędnych sił i środków, jakie należy zastosować w wyniku reakcji na rozpoznane zagrożenia oraz dokładniejsze opracowanie planów ochrony IK.

Metodyka Niemiec

Niemiecka metodyka oceny ryzyka na potrzeby zarządzania kryzysowego została przedstawiona w dokumencie *Method of Risk Analysis for Civil Protection* (MRACP). Przyczyną jej opracowania było ogłoszenie w 2002 r. *Nowej strategii ochrony ludności w Niemczech*. Na jej podstawie rządy poszczególnych landów opracowały lokalne ankiety na potrzeby szacowania ryzyka w trzech kategoriach, ryzyko: techniczne, antropogeniczne, naturalne. Zakładano, że zdarzenia mieszczące się w tych grupach stanowią najczęściej przyczyny zdarzeń kryzysowych o dużej skali i charakteryzujące się długim czasem trwania. W 2006 r. zdecydowano o opracowaniu pełnej metodyki umożliwiającej analizę czynników wpływających na prawdopodobieństwo wystąpienia zagrożenia i jego skutki [MRACP, 2011, ss. 11–17].

Opracowana w 2011 r. metodyka miała wspomóc systematyczną analizę ryzyka bazującą na mierzalnych i porównywalnych kryteriach, a także umożliwiać graficzne raportowanie ryzyka. Metodyka miała być zgodna z wydanymi międzynarodowymi standardami ISO 31000:2009 Risk management – Principles and guidelines oraz ISO 31010:2009 Risk management – Risk assessment. Ostatecznie metodyka niemiecka realizowana jest w pięciu etapach [MRACP, 2011, ss. 23–40]:

1. Opis zdefiniowanego obszaru.
2. Selekcja zagrożenia i opis scenariuszy.
3. Szacownie prawdopodobieństwa.
4. Szacowanie wpływu.
5. Identyfikacja i wizualizacja ryzyka.

Pierwszym krokiem metodyki niemieckiej jest wykonanie szczegółowego opisu obszaru, którym może być całe terytorium Niemiec, pojedyncze landy lub lokalne społeczności. Dane zbierane na tym etapie dotyczą: lokalizacji geograficznej, klimatu, populacji zamieszkującej region, środowiska, ekonomii, mediów (np. źródła wody pitnej,

zasilanie) [MRACP, 2011, s. 24]. Opis analizowanego obszaru może być uzupełniony adekwatnymi mapami (również tymi opartymi na systemach GIS).

Drugim krokiem metodyki niemieckiej jest wybór zagrożenia i opis scenariusza jego rozwoju. Metodyka dostarcza wzorcową, otwartą listę zawierającą przykładowy katalog zagrożeń. Opracowanie scenariusza jest punktem startowym do przeprowadzenia analizy ryzyka. Scenariusz powinien opisywać zdarzenie szczegółowo, aby zapewnić dane na potrzeby wskazania oceny prawdopodobieństwa wstąpienia zdarzenia niekorzystnego. Trzeba zebrać dane dotyczące rozmiarów, intensywności i czasu trwania zdarzenia. Jeśli to możliwe, należy dostarczyć dane statystyczne lub wynikające z badań naukowych. Braki danych mogą być zastępowane opiniami eksperckimi. Tam, gdzie to możliwe, sugeruje się używanie miar ilościowych [MRACP, 2011, ss. 25–26].

Trzecim krokiem metodyki niemieckiej jest ocena prawdopodobieństwa wystąpienia scenariusza zdarzenia. W omawianej metodyce zaproponowano pięciostopniową skalę częstotliwości zdarzeń w przedziale od 1 na 100 000 lat (bardzo nieprawdopodobne) do 1 na 10 lat (bardzo prawdopodobne) [MRACP, 2011, s. 27]. W zamyśle autorów metodyki ma ona dać się zaadaptować na każdym szczeblu zarządzania sektora administracji publicznej. Metodyka zakłada możliwość użycia zarówno danych ilościowych, jak i jakościowych.

Czwartym korkiem opisanym w metodyce jest ocena skutków, podczas której wskazywane są negatywne konsekwencje scenariusza zdarzenia. Parametry negatywnych skutków zostały przypisane do pięciu kategorii: człowiek, środowisko, ekonomia, dostawy mediów, skutki niematerialne. Poniższy katalog (tab. F.1) stanowi przykład i otwarty zbiór parametrów, które powinny być każdorazowo uzupełniane.

Tabela F.1. Przykład parametrów opisu scenariusza zdarzeń niekorzystnych stosowanych w niemieckiej metodyce oceny ryzyka na potrzeby zarządzania kryzysowego

Wyszczególnienie	Kategorie danych
Człowiek	ofiary śmiertelne, osoby ranne, osoby potrzebujące opieki powyżej 14 dni, osoby potrzebujące opieki poniżej 14 dni;
Środowisko	skażenie chronionego terenu, skażenie zbiorników wodnych, skażenie wód gruntowych, skażenie terenów rolniczych;
Ekonomia	zniszczenia fizyczne (np. majątku), zniszczenie będące konsekwencją innego zdarzenia, zakłócenia działalności operacyjnej, utrata zyskowności (np. z tytułu wpływów podatkowych);
Dostawy mediów	zakłócenie dostaw wody, zakłócenie dostaw energii elektrycznej, zakłócenie dostaw gazu, zakłócenie usług telekomunikacyjnych;
Skutki niematerialne	wpływ na publiczny porządek i bezpieczeństwo, skutki polityczne, skutki psychologiczne, straty w dziedzictwie kulturowym;

Źródło: MRACP, 2011, ss. 30–31.

Metodyka niemiecka wymaga określenia progów akceptacji ryzyka oddzielnie dla poszczególnych parametrów. Mogą one być ustanawiane na podstawie obowiązujących przepisów prawa lub też kryteriów dla konkretnych systemów IK.

Wynikiem niemieckiej metodyki oceny ryzyka na potrzeby zarządzania kryzysowego jest matryca ryzyka obrazująca sytuację dla analizowanego obszaru. Wartość ryzyka

określana jest na podstawie prawdopodobieństwa wystąpienia zdarzenia oraz jego skutków. Następnie porównuje się ze sobą różne scenariusze rozwoju sytuacji kryzysowej i na ich podstawie planuje zabezpieczenia lub środki reakcji na zagrożenie.

Podsumowując, metodyka niemiecka kładzie nacisk na analizę obszaru, w którym występuje zagrożenie. Identyfikowane są infrastruktury, które mogą ulec uszkodzeniu. Następnie określa się ich podatność na zagrożenia występujące w danym scenariuszu i na tej podstawie dobiera się środki zapobiegawcze lub minimalizujące ryzyko. Metodyka niemiecka nie wskazuje konkretnych metod analizy zagrożeń czy budowy scenariuszy. Jednak jej zgodność z normą ISO 31000:2009 sugeruje możliwość wykorzystywania rekomendowanych przez nią metod, tj. burzy mózgów, wywiadu ustrukturalizowanego, metody delfickiej, listy kontrolnej, podstawowej analizy zagrożeń, analizy zagrożeń i zdolności operacyjnych, analizy zagrożeń i krytycznych punktów kontroli, oceny ryzyka środowiskowego itp. [Wróblewski, 2015, ss. 58–60].

Metodyka Irlandii

Dokumentem opisującym irlandzką metodykę oceny ryzyka na potrzeby zarządzania kryzysowego jest *A Framework for Major Emergrncy Management, A Guide to Risk Assessment In Major Emergency Management* (FMEM). U podstaw irlandzkiej metodyki oceny ryzyka leżały analiza kontekstu zarządzania sytuacjami kryzysowymi występującymi w przeszłości, jak i bieżąca sytuacja ekonomiczna, a także geopolityczna tego kraju. Globalne zdarzenia takie jak kryzys paliwowy, choroby ludzi i zwierząt, erupcja islandzkiego wulkanu Eyjafjallajökull czy zagrożenie terrorystyczne wymusiły na władzach Irlandii wykonywanie oceny ryzyka w różnych obszarach zarządzania bezpieczeństwem państwa. Irlandzka metodyka oceny ryzyka z założenia ma korzystać z danych ilościowych (tam, gdzie możliwe jest ich pozyskanie i analiza). Opracowanie tej metodyki było koordynowane przez Office of Emergency Planning przy wsparciu Szkoły Biznesu DCU oraz we współpracy ze wszystkimi ważnymi jednostkami i agendami rządowymi [FMEM, 2010, s. 11].

Zgodnie z wytycznymi ocena ryzyka w Irlandii ma być wykonywana na wszystkich szczeblach administracji publicznej. Proces ten został podzielony na dwie części. Pierwsza część szczegółowo omawia cztery kroki oceny ryzyka: ustanowienie kontekstu, identyfikację zagrożeń, ocenę ryzyka, zapisanie potencjalnych zagrożeń na matrycy ryzyka. Druga część opisuje wytyczne z zakresu planowania i postępowania z ryzykiem [FMEM, 2010, ss. 21–26].

Pierwszym krokiem metodyki irlandzkiej jest *ustanowienie kontekstu,* konieczne jest opisanie charakterystyki obszaru, dla którego wykonywana jest ocena ryzyka. Informacja ta jest ważna zarówno ze względu na potrzeby wskazania prawdopodobieństwa, jak i skutków poważnych zdarzeń kryzysowych. Ustanowienie kontekstu umożliwia lepsze zrozumienie podatności oraz odporności obszaru na zdarzenia kryzysowe. Zespół odpowiedzialny za realizację tego etapu powinien zapewnić konsultacje z zespołami eksperckimi z organizacji odpowiadających za ochronę środowiska, bezpieczeństwo życia i zdrowia, bezpieczeństwo żywności, żeglugę morską i śródlądową oraz transport lotniczy. Budując wiedzę o potencjalnych scenariuszach zagrożeń, należy wziąć pod

uwagę następujące obszary oraz istotne dla nich wskaźniki (tab. F.2). W ramach tego etapu używa się m.in. map GIS oraz danych historycznych i statystycznych.

W ramach korku *identyfikacja zagrożeń* zagrożenia powinny zostać rozpoznane zarówno na poziomie lokalnym, jak i centralnym. Zgodnie z wytycznymi metodyki, zagrożenia mają być grupowane w cztery kategorie: naturalne, związane z transportem, technologiczne, związane z ludnością [FMEM, 2010, s. 23]. Następnie do każdego zidentyfikowanego zagrożenia z ww. kategorii konieczne jest przyporządkowanie elementu związanego ze społecznością, który jest podatny na dane zagrożenie.

Tabela F.2. Obszary i wskaźniki wykorzystywane w irlandzkiej metodyce oceny ryzyka na potrzeby zarządzania kryzysowego

Wyszczególnienie	Elementy opisu
Społeczeństwo	opis demografii, pochodzenia etnicznego, uwarunkowania socjoekonomiczne; informacje o rozmieszczeniu geograficznym poszczególnych społeczności; istnienie potencjalnie podatnych na zagrożenia grup w społeczności; identyfikacja wydarzeń kulturalnych i sportowych, w trakcie których na terenie danej społeczności pojawiają się duże skupiska ludzi (np. koncerty, imprezy sportowe); informacja o umiejętności radzenia sobie społeczności z sytuacjami kryzysowymi; charakterystyka społeczności pod kątem istnienia grup związanych z wolontariatem;
Środowisko	charakterystyka obszaru i ocena, czy jest on miejski, wiejski czy mieszany; istnienie na tym terenie czynników ryzyka stanowiących element podatności; istnienie obszarów dużego zagęszczenia ludności; istnienie wrażliwych obszarów środowiska; historia zdarzeń kryzysowych na danym obszarze;
Infrastruktura	sposób konfiguracji infrastruktury na danym obszarze – w zakresie: transport (drogi, tory kolejowe, korytarze powietrzne, drogi morskie); krytyczne łańcuchy dostaw; lokalizacje krytyczne na poziomie lokalnym, regionalnym czy narodowym zapewniające podstawowe usługi (np. węzły telekomunikacyjne, generatory prądu); czynniki istotne z punktu widzenia gospodarki/ekonomii regionu;
Lokalizacje niebezpieczne	rodzaje niebezpiecznych instalacji w regionie; rozlokowanie niebezpiecznych instalacji w odniesieniu do miejsc zamieszkałych przez lokalne społeczności; obszary ważne z punktu widzenia ochrony środowiska.

Źródło: FMEM, 2010, ss. 22–23.

W ramach kroku *oceny ryzyka* przeprowadzane jest badanie skutków, ich dotkliwości oraz wpływu na zdrowie lub życie, majątek oraz infrastrukturę, a także środowisko. Przy ocenie prawdopodobieństwa wystąpienia zdarzenia pod uwagę bierze się dostępne dane ilościowe oraz opinie centrów kompetencji. Metodyka irlandzka proponuje stosowanie pięciostopniowych skal skutków i prawdopodobieństwa [FMEM, 2010, s. 23].

Ostatnim etapem irlandzkiej metodyki jest *prezentacja zagrożeń na matrycy ryzyka*. Matryca opisana jest przez prawdopodobieństwo wystąpienia zagrożenia oraz jego skutki. Prawdopodobieństwo określa się na podstawie miernika charakteryzującego zagrożenie jako występujące raz na określona liczbę lat. Poziom skutków określa się w czterech kategoriach: rodzaj szkody, wartość liczbowa, wartość finansowa, czas niedostępności usług [FMEM, 2010, ss. 24–25]. W przypadku oceny ryzyka bierze się również pod uwagę powiązania poszczególnych zagrożeń, które mogą powodować powstanie zdarzeń niekorzystnych.

Metodyka irlandzka zwraca uwagę na konieczność ustalenia kontekstu analizowanego zagrożenia poprzez umieszczenie go w określonym środowisku społecznym, gospodarczym i obszarze geograficznym. Takie podejście ułatwia określenie poziomu podatności analizowanego obszaru na rozpoznane zagrożenie. Na uwagę zasługuje również fakt, że w ramach obrazowania ryzyka na matrycy ryzyka wskazane są te zagrożenia, które wymagają reakcji w postaci uruchomienia odpowiednich planów ochrony infrastruktury, ludności czy środowiska.

Metodyka Kanady

Kanadyjska metodyka oceny ryzyka na potrzeby zarządzania kryzysowego została opisana w dokumencie *All Hazards Risk Assessment Methodology Guidelines* (AHRA). Celem tej metodyki jest umożliwienie wykonywania oceny ryzyka przy użyciu jednolitych zasad i kroków przez wszystkich uczestników procesu. Zgodnie z metodyką ocena ryzyka na szczeblu centralnym jest wykonywana raz w roku. Ocena ryzyka ma skupiać się na najbardziej prawdopodobnych i mających duże skutki zdarzeniach [AHRA, 2013, s. 1–2]. Założenie to pozwala na koncentrację działań na zagrożeniach występujących najczęściej. Z drugiej strony pomijane są zagrożenia nietypowe, które mogą również przynieść negatywne skutki w znacznych rozmiarach. Pominięcie tych zagrożeń sprawia, że nie istnieją plany reakcji, co może potęgować negatywne skutki ich wystąpienia.

Proces zarządzania ryzykiem opisany w kanadyjskiej metodyce odnosi się do zapisów normy ISO 31000:2009 Risk Management – Principles and Guidelines i realizowany jest w ramach następujących kroków [AHRA, 2013, s. 4]:

- ustanowienie kontekstu – wskazanie celów organizacji i zdefiniowanie zewnętrznych i wewnętrznych parametrów, które powinny być brane pod uwagę w trakcie zarządzania ryzykiem. W ramach tego etapu wykorzystywane są: plany i raporty dotyczące zagrożeń i sposobów przeciwdziałania, dane dotyczące środowiska, dane historyczne, raporty dotyczące korelacji między zagrożeniami [AHRA, 2013, ss. 9–10];
- identyfikacja ryzyka – proces rozpoznawania i dokumentowania ryzyka. W ramach tego etapu wykorzystywane są: burze mózgów, analiza powiązań, analiza źródeł ryzyka, check-listy, analiza scenariuszy, analiza SWOT [AHRA, 2013, s. 13];
- analiza ryzyka – proces zrozumienia natury i wartości ryzyka w kontekście jego skutków i prawdopodobieństwa. W ramach tego etapu wykorzystywane są: dane historyczne, dane dotyczące częstotliwości występowania zagrożenia, symulacje rozwoju sytuacji kryzysowej [AHRA, 2013, s. 20];
- ewaluacja ryzyka – proces porównywania wyników analizy ryzyka z kryteriami ryzyka w celu określenia, czy ryzyko jest akceptowane/tolerowane. W ramach tego etapu wykorzystywane są dane dotyczące prawdopodobieństwa wystąpienia zagrożenia oraz skutków wystąpienia zagrożenia [AHRA, 2013, s. 53];
- postępowanie z ryzykiem – proces identyfikacji i rekomendowania rozwiązań kontrolujących lub umożliwiających postępowanie z ryzykiem. W ramach tego etapu wykorzystywane są: wyniki etapu ewaluacji ryzyka, graficzne reprezentacje danych etapu analizy ryzyka i ewaluacji ryzyka oraz różne wskaźniki opisujące ryzyko [AHRA, 2013, s. 57];

Metodyka AHRA do oceny ryzyka wykorzystuje podejście scenariuszowe. Podczas realizacji pierwszego etapu powinny zostać wskazane zagrożenia mogące zmaterializować się w ciągu 5 lat oraz zagrożenia, które mogą pojawić się w czasie od 5 do 25 lat [AHRA, 2013, s. 11]. Jedną z metod identyfikacji zagrożeń jest Risk Event Scenario Development, która ma na celu wyeliminowanie nieprecyzyjnych założeń i niepewności. Zastosowanie tej metody ma wpływ na dokładność wyników analizy ryzyka. Metodyka dostarcza szczegółowych informacji dotyczących zdarzenia skupiając się na kontekście i działaniach ograniczających ryzyko [AHRA, 2013, ss. 13–15]. W tab. F.3 znajduje się ramowy wykaz kategorii danych dotyczących zagrożeń oraz scenariuszy ich rozwoju wykorzystywany w metodyce kanadyjskiej.

Tabela F.3. Opis scenariusza zdarzenia wg AHRA

Metryka dokumentu	
Nazwa scenariusza zdarzenia	krótki opis zdarzenia
Kod zagrożenia dla zdarzenia wiodącego	odniesienie do nazewnictwa zagrożeń opisanego w metodyce AHRA
Kod zagrożenia dla zdarzenia wtórnego	pole opcjonalne dla zdarzeń następujących w wyniku zdarzenia wiodącego
Jednostka wiodąca	jednostka wskazana w dokumencie Federal Emergency Response Plan jako wiodąca w reagowaniu na zdarzenie
Jednostki wspierające	jednostka wskazana w dokumencie Federal Emergency Response Plan zapewniające wsparcie eksperckie lub specyficzne zasoby
Kluczowe źródła informacji nt. scenariusza zdarzenia	dokumentacja wspierająca niezbędna zwłaszcza przy wykorzystaniu danych ilościowych i jakościowych na potrzeby analizy ryzyka
Opis scenariusza zdarzenia	
Opis zdarzenia (kontekst, przyczyna, źródło, natura, skala)	faktyczne informacje o możliwości i warunkach materializacji zdarzenia; orientacyjny czas pojawienia się zdarzenia zgodnie z wymaganiami AHRA – krótkoterminowy (w ciągu kolejnych 5 lat) lub długoterminowy (pomiędzy 5 a 25 lat); wskazanie adekwatnych kategorii skutków: ludzie, środowisko, gospodarka, bezpieczeństwo terytorialne, reputacja kraju itp.
Incydenty pośrednie	pole opcjonalne
Rozważania geograficzne	pole opcjonalne (długość i szerokość geograficzna), kraj, prowincja itp.
Naturalne środowisko	charakterystyka otoczenia fizycznego/środowiskowego
Warunki meteorologiczne	warunki, które mogą mieć wpływ na wystąpienie zdarzenia
Sezonowość	pole opcjonalne
Charakterystyka zagrożenia	charakterystyka chemicznych, biologicznych, radiologicznych czynników pojawiających się w scenariuszu, które umożliwiają ocenę złożoności i czasy trwania zdarzenia
Natura i podatność dotkniętego obszaru (kontekst, populacja, gęstość zaludnienia, kluczowa infrastruktura itp.)	na podstawie tych informacji eksperci dziedzinowi mogą ocenić wartość ryzyka
Inne ważne wnioski i założenia	pole opcjonalne
Niepewność w opisie scenariusza zdarzenia	pole opcjonalne; jeśli w przypadku zdarzenia istnieją obszary niepewności i nieprzewidywalności, powinny zostać opisane w tym polu

Inne adekwatne informacje, notatki komentarze	inne komentarze dotyczące zdarzenia
Ocena prawdopodobieństwa	
Czas/horyzont czasowy, w którym zdarzenie może wystąpić	wyjaśnienie danych dotyczących prawdopodobieństwa wystąpienia zdarzenia
Niepewność w ocenie prawdopodobieństwa	nieznane czynniki, które mogą mieć wpływ na ocenę prawdopodobieństwa
Inne adekwatne informacje	inne dane dotyczące wstępnej oceny prawdopodobieństwa
Ocena skutków	
Kategorie skutków: natura i skala	
Ludzie	specyficzne wskaźniki wpływu zdarzenia na ludzi; orientacyjne wartości, ilość ofiar śmiertelnych, poważnie rannych itp.
Gospodarka	bezpośrednie i pośrednie straty finansowe, koszty naprawy/ /odtworzenia
Środowisko	wskaźniki charakteryzujące wpływ zdarzenia na środowisko
Bezpieczeństwo terytorialne	wskaźniki opisujące warunki, w których rząd nie może zapewnić bezpieczeństwa granic i zapewnić bezpieczeństwo obywateli
Reputacja kraju	w oparciu o ocenę ekspercką opis potencjalnej reakcji międzynarodowej
Społeczeństwo	wskaźniki niezadowolenia społecznego, protesty, zamieszki, wandalizm
Inne adekwatne informacje	inne dodatkowe informacje dotyczące konsekwencji zdarzenia
Wstępne planowanie postępowania z ryzykiem	
Podstawowy plan postępowania z ryzykiem	pole opcjonalne; jednostki centralne mogą wykorzystywać je do oceny istniejących rozwiązań w zakresie zarządzania kryzysowego
Mierniki wdrożonych działań związanych z postępowaniem z ryzykiem	metodyka AHRA bierze pod uwagę faktycznie wdrożone i funkcjonujące zabezpieczenia, należy je wymienić w tym polu
Poziom, do którego ryzyko (prawdopodobieństwo i skutki) może być zredukowane	pole zawierać powinno ocenę planowanego do wdrożenia zabezpieczenia
Dodatkowe zasoby niezbędne do postępowania z ryzykiem	dodatkowe informacje związane z postępowaniem z ryzykiem
Inne adekwatne informacje	inne adekwatne informacje dotyczące oceny skutków/konsekwencji

Źródło: AHRA, 2013, ss. 65–69.

Podsumowując metodyka kanadyjska kładzie nacisk na wykonywanie systematycznych ocen ryzyka w cyklu roczny przy wykorzystaniu wielu metod wspomagających zaadaptowanych z różnych obszarów zarządzania. Ponadto zapisy metodyki różnicują prawdopodobieństwo wystąpienia zagrożenia w okresie od 5 do 25 lat. Pozwala to lepiej dostosować plany działań do specyfiki zagrożenia.

Metodyka Holandii

Holenderska metodyka oceny ryzyka na potrzeby zarządzania kryzysowego została opublikowana w dokumencie *National Risk Assessment Method Guide* (NRAMG) w 2008 r. Rok później wydano *Working with scenarios, risk assessment and capabilities*

In the National Safty and Security Strategy of Netherlands, który stanowi jej rozszerzenie (WSRAC). Holenderska metodyka oceny ryzyka została opracowana w celu realizacji Narodowej Strategii Bezpieczeństwa Holandii. Punktem wyjścia w metodyce holenderskiej jest określenie ról i odpowiedzialności wszystkich podmiotów uwzględnionych w narodowej strategii oraz zaangażowanych w realizację kolejnych przedsięwzięć wynikających z faz metodyki. Cała metodyka składa się z następujących faz: opracowanie scenariuszy, ocena ryzyka, ocena zdolności reakcji na zagrożenie, opracowanie raportu podsumowującego i rekomendacji [WSRAC, 2009, s. 12].

W ramach fazy *opracowanie scenariuszy* budowane są prognozy zagrożeń dla bezpieczeństwa narodowego w perspektywie średnioterminowej do 5 lat. Opracowany scenariusz jest opisem potencjalnego zagrożenia (pojedynczego lub złożonego). Opisy zagrożeń odnoszą się do stopnia podatności i odporności, w kontekście: zasobów ludzkich, obiektów oraz społeczeństwa. Dodatkowo opis scenariusza zawiera wykaz konsekwencji zdarzenia niekorzystnego, wykaz podjętych działań w ramach reakcji na zdarzenie, wykaz stosowanych środków kontroli oraz konsekwencje w stosunku do ciągłości funkcjonowania IK. Wypracowane scenariusze dzieli się na dwie kategorie. Scenariusze, które mogą wydarzyć się w każdej chwili oraz scenariusze zdarzeń niekorzystnych, które mogą się wydarzyć w wyniku zaistnienia określonych warunków, np. w wyniku wzrostu poziomu życia społeczeństwa lub zmian demograficznych czy migracji ludności [WSRAC, 2009, ss. 17–20].

Potencjalną wadą metodyki holenderskiej jest założenie, że scenariusze sytuacji niekorzystnych mają mieć zasięg krajowy, co powoduje odrzucenie scenariuszy o zasięgu regionalnym, które również mogą mieć poważne konsekwencje. Ponadto każdy scenariusz musi być unikatowy, różnić się skalą, intensywnością zdarzeń, prawdopodobieństwem, lokalizacją itp.

Kolejnym krokiem w metodyce holenderskiej jest *ocena ryzyka*, która jest podzielona na podetapy: sprawdzenie kompletności opisu scenariusza, oszacowanie wpływu scenariusza, oszacowanie prawdopodobieństwa scenariusza, prezentacja wyników analiz [WSRAC, 2009, ss. 25–26]. Ryzyko w metodyce holenderskiej ocenia się w kategoriach: bezpieczeństwo terytorialne, bezpieczeństwo fizyczne, ekonomiczne oraz stabilność społeczno-polityczna. Wskaźnik syntetyczny oszacowania wpływu opracowuje się w wyniku agregacji danych cząstkowych i wylicza się wartość wpływu całkowitego (z wykorzystaniem sumy ważonej) [WSRAC, 2009, ss. 99–102]. Szacowanie prawdopodobieństwa wystąpienia scenariusza dobywa się przez określenie dolnej i górnej granicy prawdopodobieństwa. Ponadto uwzględnia się niepewność określenia kategorii prawdopodobieństwa dla każdego scenariusza incydentu wraz ze wskazaniem źródła niepewności. Prawdopodobieństwo zdarzeń niekorzystnych w metodyce holenderskiej określane jest na podstawie danych historycznych, studiów przypadków z wykorzystaniem analiz sieciowych i drzew decyzyjnych oraz szacunków eksperckich i analiz trendów. Wyniki oceny ryzyka prezentowane są jako dwuwymiarowy diagram ryzyka.

Kolejną fazą metodyki holenderskiej jest *ocena zdolności reakcji na zagrożenie*. Ma ona doprowadzić do uzyskania odpowiedzi na pytanie: jakie są słabości analizowanego sytemu w kontekście posiadanych sił i środków redukcji ryzyka. Na podstawie analizy scenariuszy ustala się, które zdolności systemu muszą zostać wzmocnione na potrzeby

redukcji prawdopodobieństwa ich wystąpienia. Oceny dokonuje się w kategoriach: bezpieczeństwo terytorialne, bezpieczeństwo fizyczne, bezpieczeństwo ekonomiczne, ochrona środowiska, stabilność społeczna i polityczna [WSRAC, 2009, s. 29]. Faza ta wykorzystuje predefiniowane check-listy, zestawienia tabelaryczne oraz mapy GIS.

Ostatnia faza metodyki *opracowanie raportu podsumowującego i rekomendacji* polega na zebraniu danych i opracowań z poprzednich faz i utworzeniu syntetycznego raportu. Następnie raport ten jest przekazywany rządowi holenderskiemu, który podejmuje decyzje o dalszych działaniach. W raporcie do prezentacji danych wykorzystywane są głównie diagramy ryzyka [WSRAC, 2009, ss. 63–66].

Podsumowując, metodyka holenderska rozpoczyna się od analizy scenariuszy rozwoju zdarzenia niekorzystnego, co wyróżnia ją spośród pozostałych metodyk. Inne metodyki swoją ocenę ryzyka uzależniały przede wszystkim od listy zagrożeń, w uzasadnionych przypadkach uwzględniając scenariusze. W metodyce holenderskiej scenariusze rozwoju sytuacji niekorzystnej przedstawiają kompleksowy obraz niepewności oraz czynników wpływających na decyzje dotyczące planów reakcji na zagrożenie.

Metodyka USA

Metodyka oceny ryzyka na potrzeby zarządzania kryzysowego w Stanach Zjednoczonych Ameryki Północnej została opublikowana w dokumencie *Multi Hazard Identification and Risk Assessment A Cornerstore of the National Mitigation Strategy* (HAZUS) w 1997 r. Obejmuje ona całość terytorium USA. Celem metodyki jest oszacowanie potencjalnych strat poniesionych w wyniku wystąpienia sytuacji kryzysowej za pomocą ustandaryzowanych procedur. Na podstawie szacowanych strat podejmuje się decyzje dotyczące zastosowania zabezpieczeń osłabiających skutki materializacji zagrożeń lub utrzymywania stanów gotowości i reagowania na zdarzenia niepożądane i sytuacje kryzysowe. W 2004 r. wydano dokument *Using HAZUS-MH for Risk Assessment* (UHAZUS), który dostarcza wiedzy użytkownikowi, w jaki sposób zrealizować założenia i wytyczne metodyki HAZUS. Metodyka implementuje modele służące do estymacji potencjalnych strat powodowanych przez: trzęsienia ziemi, powodzie i huragany [HAZUS, 1997, s. II]. Estymacja jest dokonywana w obszarach strat fizycznych, ekonomicznych oraz społecznych. Analizy są wspierane systemami typu GIS.

Metodyka HAZUS jest częścią procesu planowania ograniczania szkodliwości zagrożeń. Proces ten realizuje cztery fazy [UHAZUS, 2004, s. XII]:

- identyfikację zasobów;
- szacowanie ryzyka:
  - identyfikacja zagrożeń – wynikiem etapu jest charakterystyka regionu, mapa regionu w systemie GIS oraz lista rozpoznanych zagrożeń,
  - opis zagrożeń – wynikiem etapu jest profil zagrożeń, syntetyczna mapa zagrożeń oraz lista zagrożeń uporządkowana według priorytetów,
  - klasyfikacja zagrożeń – wynikiem etapu są dane o zagrożeniach uzupełnione przez lokalne zasoby danych oraz informacje o źródłach tych danych,
  - szacowanie strat – wynikiem etapu jest wykaz możliwych strat poniesionych w ramach różnych scenariuszy rozwoju sytuacji niepożądanej,

  - wskazanie możliwych działań – wynikiem etapu jest lista możliwych działań łagodzących skutki rozpoznanych zagrożeń;
- opracowanie planów łagodzenia ryzyka,
- implementację planów łagodzenia ryzyka.

Amerykańska metodyka oceny ryzyka na potrzeby zarządzania kryzysowego stosuje podział zagrożeń na dwie główne kategorie [HAZUS, 1997, ss. 1–292]:

- zagrożenia naturalne:
  - zagrożenia atmosferyczne,
  - zagrożenia geologiczne,
  - zagrożenia hydrologiczne,
  - zagrożenia sejsmiczne,
  - inne naturalne zagrożenia (wybuchy wulkanów, burza ogniowa),
- zagrożenia technologiczne:
  - awarie zabezpieczeń systemu,
  - pożary w centrach danych,
  - wypadki z materiałami niebezpiecznymi,
  - wypadki z udziałem materiałów jądrowych.

Metodyka stosowana w USA ma budowę modułową. Dzięki takiemu podejściu możliwe jest jej stosowanie na terytorium całego państwa. Jednocześnie metodyka pozostaje elastyczna, zachowując możliwość dostosowania do lokalnych warunków, dzięki czemu odpowiada na potrzeby użytkowników końcowych. Modułowa budowa umożliwią również rozbudowę metodyki o nowe elementy, jeśli zachodzi taka potrzeba. Podstawowymi modułami HAZUS są [HAZUS, 1997, s. 301]:

- potencjalne zagrożenia geologiczne,
- dostępne zasoby,
- szkody bezpośrednie,
- bezpośrednie straty ekonomiczno-społeczne,
- straty pośrednie.

Każdy z wymienionych modułów podstawowych jest dekomponowany na podmoduły dotyczące obiektów szczegółowych znajdujących się w obszarze decyzyjnym modułu nadrzędnego.

Metodyka HAZUS oprócz systemów GIS wykorzystuje matryce ryzyka, check-listy, systemy symulacyjne (np. do przewidywania skutków trzęsień ziemi), dane historyczne oraz statystyczne, a także analizy scenariuszowe.

Wynikiem metodyki oceny ryzyka na potrzeby zarządzania kryzysowego stosowanej w USA są możliwe do zastosowania zabezpieczenia łagodzące lub zapobiegające negatywnym skutkom wystąpienia sytuacji niepożądanej lub kryzysowej. Decyzję o wdrożeniu konkretnych rozwiązań podejmowane są przez rząd federalny w porozumieniu z władzami poszczególnych stanów. Wyróżnikiem metodyki HAZUS jest jej silne uzbrojenie w dedykowane narzędzia informatyczne wspierające poszczególne etapy prowadzące od rozpoznania analizowanego obszaru poprzez wskazanie możliwych zagrożeń aż do etapu zaproponowania działań łagodzących potencjalne skutki wystąpienia zagrożenia.

Metodyka Polski

Polska metodyka oceny ryzyka, tak jak omówione metodyki zagraniczne, jest częścią procesu zarządzania kryzowego, który został zdefiniowany w ustawie z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (rys. 1.1c). Obecnie funkcjonujący w Polsce model zarządzania kryzysowego wykorzystuje dane z przygotowywanych co dwa lata RZBN. Obowiązek sporządzenia raportów mają ministerstwa, urzędy centralne oraz wojewodowie. W procesie tym opcjonalnie mogą uczestniczyć powiaty oraz gminy. Fakt ten utrudnia zbieranie wiarygodnych danych na temat zagrożeń występujących na poszczególnych poziomach administracyjnych oraz ich agregację na poziomy wyższe. Potwierdzenie tego spostrzeżenia stanowią zapisy NPOIK, gdzie stwierdzono, że najlepszą wiedzę dotyczącą zagrożeń IK oraz metod przeciwdziałania zagrożeniom mają operatorzy IK [NPOIK, 2015, s. 9]. Grupa ta nie ma ustawowego obowiązku przygotowywania RZBN. Brak takiego obowiązku prowadzi do sytuacji, w której wiedza o zagrożeniach nie pochodzi ze źródła ich powstawania.

Koordynatorem procesu opracowywania RZBN jest RCB, które na podstawie zabranych RZBN sporządza KPZK. Dokument ten jest następnie przedstawiany Radzie Ministrów, która przyjmuje go w postaci uchwały. Wnioski z RZBN oraz KPZK stanowią podstawę do opracowania PZK na poziomach samorządów. W ramach obowiązującej procedury zarządzania kryzysowego powstaje również NPOIK określający zadania i obowiązki dotyczące ochrony IK [Krupa, Wiśniewski, 2015, s. 94].

Przygotowanie PZK jest realizowane w ramach procedury planowania cywilnego. Podobnie jak proces zarządzania kryzysowego procedura planowania cywilnego jest uregulowana zapisami ustawy o zarządzaniu kryzysowym. Cel oraz schemat procesu planowania cywilnego został przedstawiony w rozdz. 1.1. W ramach procesu planowania cywilnego opracowywane są m.in.: mapy ryzyka, cele strategiczne dotyczące przeciwdziałania zagrożeniom, wskazywane są priorytety reagowania na określone zagrożenie, wykazy dostępnych sił i środków, zadania w zakresie poprawy bezpieczeństwa, wnioski zawierające hierarchicznie uporządkowaną listę przedsięwzięć niezbędnych do osiągnięcia celów strategicznych [Abgarowicz, 2015, s. 15].

Metodykę oceny ryzyka na potrzeby zarządzania kryzysowego RP należy bezpośrednio powiązać z etapem *analizowania* i *prognozowania* procesu planowania cywilnego. W ramach etapu analizowania dokonuje się m.in. identyfikacji zagrożeń, opisu podatnych na zagrożenia obiektów oraz szacowanie ryzyka. W ramach etapu prognozowania podejmowane są próby wskazania scenariuszy rozwoju zdarzeń niekorzystnych i sytuacji kryzysowych. Wyniki tych dwóch etapów stanowią podstawę do przygotowania planów reagowania na rozpoznane zagrożenia.

Przeprowadzone prace nad Polską metodyką oceny ryzyka doprowadziły do powstania dwóch komplementarnych rozwiązań:

- rozwiązanie pierwsze – metodyka ceny ryzyka na potrzeby zarządzania kryzysowego RP [Skomra, 2015],
- rozwiązanie drugie – zaawansowana metodyka oceny ryzyka w publicznym zarządzaniu kryzysowym [Kosieradzka, Zawiła-Niedźwiecki, 2016].

Metodyka oceny ryzyka na potrzeby zarządzania kryzysowego RP wykorzystuje metodę listy pytań kontrolnych, gdzie użytkownik metody odpowiadając na kolejne pytania

jest w stanie określić, na jakie zagrożenia podatny jest analizowany obiekt. Zastosowanie tej metody jest pożądane ze względu na zróżnicowany poziom wiedzy osób odpowiedzialnych za ocenę ryzyka na poszczególnych szczeblach administracyjnych kraju. Metoda wykorzystująca wiedzę ekspercką, zawartą w liście pytań uzależnionych od odpowiedzi użytkownika jest intuicyjna i nie wymaga specjalistycznych szkoleń. Metodyka ceny ryzyka na potrzeby zarządzania kryzysowego RP realizowana jest w pięciu krokach [Skomra, 2015, ss. 121–212]:

- ustalenie kontekstu – w ramach tego kroku powstaje opis podmiotu chronionego zawierający dane podmiotu sporządzającego analizę, cele analizy ryzyka oraz sposób zarządzania nimi, opis podatności na zagrożenia w różnych kontekstach, np. położenia geograficznego czy podziału administracyjnego;
- identyfikacja zagrożeń – w ramach tego kroku powstaje wykaz zagrożeń, na które podatny jest analizowany obiekt, wykaz ten powstaje na podstawie danych historycznych, statystycznych oraz wniosków ekspertów;
- analiza – w ramach tego kroku dokonuje się klasyfikacji zagrożeń, dzięki czemu określa się możliwe skutki ich wystąpienia oraz możliwe działania łagodzące skutki lub zapobiegawcze, dokonuje się również prognozy przebiegu zdarzenia niekorzystnego
- szacowanie – w ramach tego kroku szacuje się ryzyko związane z rozpoznanymi zagrożeniami w obszarze: ofiary śmiertelne, ranni, ewakuowani. Dalej określa się straty materialne i wpływ na środowisko oraz wskazuje się skutki społeczne i polityczne uszkodzenia IK. Szacunku ryzyka dokonuje się na podstawie prawdopodobieństwa i spodziewanych skutków wystąpienia zagrożenia;
- ocena jest ostatnim etapem, w ramach którego powstaje matryca ryzyka oraz mapy zagrożeń.

Zaawansowana metodyka oceny ryzyka w publicznym zarządzaniu kryzysowym została opracowana z myślą o niestandardowych zagrożeniach, których identyfikacja nie jest możliwa za pomocą metody listy kontrolnej. Metodyka ta jest rekomendowana do prowadzenia wnikliwej i wszechstronnej analizy ryzyka. Wykorzystuje ona podejście metodyczne i dorobek nauk o zarządzaniu, w szczególności uwzględnione zostały metody: analizy interesariuszy, analizy strategicznej, benchmarking, foresight, metody eksperckie, metody twórczego rozwiązywania problemów, podejście procesowe, podejście zasobowe, podejście systemowe, zarządzanie wiedzą, TQM i modele doskonałości organizacji.

Cele metody zaawansowanej osiągane są w wyniku realizacji dziewięciu modułów [Kosieradzka, Zawiła Niedźwiecki, 2016, ss. 159–318]:

- moduł 1 – organizacja pracy zespołu oceny ryzyka – w ramach tego modułu przeprowadzana jest analiza interesariuszy, tworzony jest zespół projektowy, weryfikowane są kompetencje członków zespołu oraz wskazywany jest model pracy;
- moduł 2 – charakterystyka podmiotu chronionego – w ramach tego modułu powstaje szczegółowy opis podmioty chronionego, identyfikowana jest IK, identyfikowane są procesy i zasoby niezbędne do ich realizacji;
- moduł 3 – wyznaczenie podsystemów i grup zasobów IK państwa – w ramach tego modułu identyfikuje się systemy IK na analizowanym obszarze, wyznacza się podsystemy oraz grupy zasobów w ramach rozpoznanych systemów IK;

- moduł 4 – obliczenie zmiennych ryzyka – w ramach tego modułu identyfikuje się i selekcjonuje zmienne ryzyka, dobiera się metodę obliczania zmiennych ryzyka, przyjmuje procedurę pionowej (między szczeblami administracji państwowej) i poziomej (na tym samym szczeblu administracyjnym) agregacji ryzyka;
- moduł 5 – identyfikacja zagrożeń oraz analiza i oszacowanie ryzyka – w ramach tego modułu dokonuje się przeglądu i doboru metod identyfikacji zagrożeń, rozpoznaje się zagrożenia według przyjętych metod, dokonuje się klasyfikacji zagrożeń, wskazuje powiązania między zagrożeniami, oblicza się wartość ryzyka oraz prezentuje wyniki oceny na potrzeby dalszych analiz;
- moduł 6 – kryteria akceptowalności ryzyka – w ramach tego modułu definiuje się kryteria klasyfikacji ryzyka oraz poziomy akceptowalności ryzyka, opracowuje się mapę ryzyka, a także wskazuje wytyczne postępowania z ryzykiem;
- moduł 7 – uwzględnienie zależności w ocenie ryzyka oraz prognozowanie rozprzestrzeniania się zagrożeń – w ramach tego modułu weryfikuje się listę zagrożeń na podstawie wypracowanych i przyjętych kryteriów, wskazuje potencjalne luki w liście zagrożeń oraz prognozuje się rozprzestrzenianie sytuacji niekorzystnych;
- moduł 8 – ustalenie kryteriów przejścia zagrożenia w sytuację kryzysową – w ramach tego modułu wskazuje się typowe zagrożenia, na podstawie których tworzy się wzorce zagrożeń dla kolejnych cykli analiz, ustala i opisuje się kryteria charakteryzujące wystąpienie sytuacji kryzysowych i zagrożeń dla bezpieczeństwa narodowego, wskazuje się wartości poszczególnych kryteriów, których spełnienie kwalifikuje wystąpienie zagrożenia jako sytuację kryzysową;
- moduł 9 – sprawozdawczość i międzyszczeblowe przekazywanie oceny ryzyka – w ramach tego modułu dokonuje się standaryzacji oceny ryzyka, kontroluje jakość przeprowadzonej oceny ryzyka, agreguje się wartości ryzyka oraz prezentuje ustalenia innym uczestnikom procesu.

W ramach prac nad Polską metodyką oceny ryzyka na potrzebny zarządzania kryzysowego RP powstało również dedykowane narzędzie wspierające realizację poszczególnych etapów wersji podstawowej oraz zaawansowanej. Obie metodyki wykorzystują podobną różnorodność metod i narzędzi służących do realizacji celów szczegółowych poszczególnych kroków. W szczególności do tej grupy należy zaliczyć: metodę burzy mózgów, mapę myśli, wykres Ishikawy, metodę 5 x dlaczego, diagram konfliktu, drzewo decyzyjne, diagram pokrewieństwa [Skomra, 2015, ss. 48–80; Kosieradzka, Zawiła-Niedźwiecki, 2016, ss. 89–133].

Obie polskie metodyki oceny ryzyka na potrzeby zarządzania kryzysowego są zgodne z międzynarodowymi przepisami dotyczącymi obowiązku ochrony państwa, zarządzania kryzysowego i bezpieczeństwa IK. Stanowią komplementarną całość, a zakres ich stosowalności wzajemnie się uzupełnia. Można tu dostrzec analogie między metodyką australijską, gdzie również występują dwa etapy oceny ryzyka (ocena bazowa oraz szczegółowa). W przypadku zaawansowanej metodyki oceny ryzyka w publicznym zarządzaniu kryzysowym widać również zapożyczenia z metodyki stosowanej w USA odnoszące się do budowy modułowej.

Załącznik G – Wykaz zależności i współzależności systemów IK

Tabela G.1. Wpływ systemu zaopatrzenia w energię, surowce energetyczne i paliwa na inne systemy IK

System podatny	Podatność
System łączności	• brak energii uniemożliwia funkcjonowanie systemu podatnego
System sieci teleinformatycznych	• brak energii utrudnia poprawne funkcjonowanie systemu podatnego
System finansowy	• brak energii utrudnia poprawne funkcjonowanie systemu podatnego
System zaopatrzenia w żywność	• brak energii utrudnia poprawne funkcjonowanie systemu podatnego
System zaopatrzenia w wodę	• brak energii uniemożliwia funkcjonowanie systemu podatnego
System ochrony zdrowia	• brak energii utrudnia poprawne funkcjonowanie systemu podatnego
System transportowy	• brak energii uniemożliwia funkcjonowanie systemu podatnego
System ratowniczy	• brak energii utrudnia poprawne funkcjonowanie systemu podatnego
System zapewniający ciągłość działania administracji publicznej	• brak energii uniemożliwia funkcjonowanie systemu podatnego
System produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych	• brak energii uniemożliwia poprawne funkcjonowanie systemu podatnego

Źródło: opracowanie własne na podstawie Kisilowski, Pomierny, Wojtkiewicz, 2014.

Tabela G.2. Wpływ systemów IK na system zaopatrzenia w energię, surowce energetyczne i paliwa

System oddziałujący	Oddziaływanie
System łączności	• błędy w komunikacji i zarządzaniu instalacjami energetycznymi • brak możliwości usunięcia usterek w systemie
System sieci teleinformatycznych	• błędy w sterowaniu infrastrukturą instalacji energetycznych • brak możliwości usunięcia usterek w systemie energetycznym
System finansowy	• brak środków finansowych niezbędnych do funkcjonowania systemu energetycznego • brak środków na zakup części zamiennych i materiałów • brak środków na naprawę usterek w systemie energetycznym • brak środków dla pracowników
System zaopatrzenia w wodę	• brak wody technologicznej do poprawnego funkcjonowania systemu zaopatrzenia w energię, surowce energetyczne i paliwa • wrażliwość na zmiany zapasów wody w systemie hydrologicznym
System transportowy	• brak stałych dostaw paliw, surowców, materiałów i części zamiennych • ograniczone możliwości dokonania napraw i rozbudowy instalacji • ograniczone możliwości dojazdu pracowników
System ratowniczy	• brak możliwości ewakuacji personelu, którego życie lub zdrowie jest zagrożone
System zapewniający ciągłość działania administracji publicznej	• błędy w sterowaniu infrastrukturą instalacji energetycznych • brak planów rozbudowy i utrzymania infrastruktury energetycznej • błędne prognozy i niewłaściwe planowanie

Źródło: opracowanie własne na podstawie Kisilowski, Pomierny, Wojtkiewicz, 2014.

Tabela G.3. Wpływ systemu produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągów substancji niebezpiecznych na inne systemy IK

System podatny	Podatność
System zaopatrzenia w żywność	• możliwość skażenia, zanieczyszczenia i zniszczenia żywności
System zaopatrzenia w wodę	• możliwość skażenia i zanieczyszczenia wody
System ochrony zdrowia	• gwałtowne zaburzenia w systemie ochrony zdrowia

Źródło: opracowanie własne na podstawie Kisilowski, Pomierny, Wojtkiewicz, 2014.

Tabela G.4. Wpływ innych systemów IK na system produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągów substancji niebezpiecznych

System oddziałujący	Oddziaływanie
System zaopatrzenia w energię, surowce energetyczne i paliwa	• brak energii niezbędnej do napędzania poszczególnych urządzeń instalacji substancji niebezpiecznych • błędy w sterowaniu infrastrukturą instalacji substancji niebezpiecznych
System łączności	• błędy w zarządzaniu instalacjami substancji niebezpiecznych • brak możliwości usunięcia usterek
System sieci teleinformatycznych	• błędy w sterowaniu infrastrukturą instalacji substancji niebezpiecznych • brak możliwości usunięcia usterek instalacji substancji niebezpiecznych
System finansowy	• brak środków finansowych niezbędnych do funkcjonowania instalacji substancji niebezpiecznych • brak środków na zakup części zamiennych i materiałów • brak środków na naprawę usterek • brak środków dla pracowników
System transportowy	• brak stałych dostaw materiałów i części zamiennych • ograniczone możliwości dokonania napraw i rozbudowy instalacji • ograniczone możliwości dojazdu pracowników
System ratowniczy	• brak możliwości usunięcia lub minimalizacji skutków katastrofy ekologicznej • brak możliwości ewakuacji personelu, którego życie lub zdrowie jest zagrożone
System zapewniający ciągłość działania administracji publicznej	• błędy w sterowaniu infrastrukturą instalacji substancji niebezpiecznych • brak planów rozbudowy i utrzymania infrastruktury instalacji substancji niebezpiecznych

Źródło: opracowanie własne na podstawie Kisilowski, Pomierny, Wojtkiewicz, 2014.

Tabela G.5. Wpływ systemu transportu na inne systemy IK

System podatny	Podatność
System zaopatrzenia w energię, surowce energetyczne i paliwa	• zakłócenia transportu uniemożliwiają poprawne funkcjonowanie systemu podatnego
System łączności	
System sieci teleinformatycznych	
System finansowy	
System zaopatrzenia w żywność	
System zaopatrzenia w wodę	
System ochrony zdrowia	
System ratowniczy	
System zapewniający ciągłość działania administracji publicznej	
System produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych	

Źródło: opracowanie własne na podstawie Kisilowski, Pomierny, Wojtkiewicz, 2014.

Tabela G.6. Wpływ systemów IK na system transportu

System oddziałujący	Oddziaływanie
System zaopatrzenia w energię, surowce energetyczne i paliwa	• zakłócenia w zasilaniu systemu transportu kolejowego • zakłócenia w zasilaniu urządzeń i instalacji komunikacyjnych • brak dostaw paliw pędnych
System łączności	• błędy w komunikacji i zarządzaniu systemem transportowym • brak możliwości usunięcia usterek w systemie transportowym
System sieci teleinformatycznych	• błędy w sterowaniu infrastrukturą systemu transportowego • brak możliwości usunięcia usterek w systemie transportowym
System finansowy	• brak środków finansowych niezbędnych do funkcjonowania systemu transportowego • brak środków na zakup części zamiennych i materiałów • brak środków na naprawę usterek • brak środków dla pracowników
System zaopatrzenia w żywność	• zakłócenia w zaopatrzeniu środków transportu w żywność (samoloty, statki, pociągi)
System zaopatrzenia w wodę	• wrażliwość transportu wodnego na stan wód w systemie hydrologicznym
System ratowniczy	• brak możliwości ewakuacji personelu, którego życie lub zdrowie jest zagrożone
System zapewniający ciągłość działania administracji publicznej	• błędy w założeniach systemu sterowania infrastrukturą transportową • brak planów rozbudowy i utrzymania infrastruktury transportowej • błędne prognozy i niewłaściwe planowanie • brak odpowiednich prognoz meteorologicznych

Źródło: opracowanie własne na podstawie Kisilowski, Pomierny, Wojtkiewicz, 2014.

Tabela G.7. Wpływ systemu łączności na inne systemy IK

System podatny	Podatność
System zaopatrzenia w energię, surowce energetyczne i paliwa	• zakłócenia systemu łączności utrudniają poprawne funkcjonowanie systemu podatnego
System sieci teleinformatycznych	
System finansowy	
System zaopatrzenia w żywność	
System zaopatrzenia w wodę	
System ochrony zdrowia	
System transportowy	
System ratowniczy	
System zapewniający ciągłość działania administracji publicznej	
System produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych	

Źródło: Pijanowski, Marczewski, Staniszewski, 2014.

Tabela G.8. Wpływ systemów IK na system łączności

System oddziałujący	Oddziaływanie
System zaopatrzenia w energię, surowce energetyczne i paliwa	• zakłócenia systemu utrudniają lub uniemożliwiają poprawne funkcjonowanie systemu łączność
System sieci teleinformatycznych	
System transportowy	
System zapewniający ciągłość działania administracji publicznej	

Źródło: opracowanie własne na podstawie Pijanowski, Marczewski, Staniszewski, 2014)

Tabela G.9. Wpływ systemu sieci teleinformatycznych na inne systemy IK

System podatny	Podatność
System zaopatrzenia w energię, surowce energetyczne i paliwa	• zakłócenia systemu sieci teleinformatycznych utrudniają lub uniemożliwiają poprawne funkcjonowanie systemu podatnego • zniszczenie systemu sieci teleinformatycznych uniemożliwia poprawne funkcjonowanie systemu podatnego
System łączności	• zakłócenia systemu sieci teleinformatycznych utrudniają lub uniemożliwiają poprawne funkcjonowanie systemu podatnego • zniszczenie systemu sieci teleinformatycznych uniemożliwia poprawne funkcjonowanie systemu podatnego
System finansowy	• zakłócenia systemu sieci teleinformatycznych utrudniają lub uniemożliwiają poprawne funkcjonowanie systemu podatnego • zniszczenie systemu sieci teleinformatycznych uniemożliwia poprawne funkcjonowanie systemu podatnego
System zaopatrzenia w żywność	• zakłócenia systemu sieci teleinformatycznych utrudniają poprawne funkcjonowanie systemu podatnego
System zaopatrzenia w wodę	• zakłócenia systemu sieci teleinformatycznych utrudniają poprawne funkcjonowanie systemu podatnego
System ochrony zdrowia	• zakłócenia systemu sieci teleinformatycznych utrudniają poprawne funkcjonowanie systemu podatnego
System transportowy	• zakłócenia systemu sieci teleinformatycznych utrudniają poprawne funkcjonowanie systemu podatnego
System ratowniczy	• zakłócenia systemu sieci teleinformatycznych utrudniają lub uniemożliwiają poprawne funkcjonowanie systemu podatnego • zniszczenie systemu sieci teleinformatycznych uniemożliwia poprawne funkcjonowanie systemu podatnego
System zapewniający ciągłość działania administracji publicznej	• zakłócenia systemu sieci teleinformatycznych utrudniają lub uniemożliwiają poprawne funkcjonowanie systemu podatnego • zniszczenie systemu sieci teleinformatycznych uniemożliwia poprawne funkcjonowanie systemu podatnego
System produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych	• zakłócenia systemu sieci teleinformatycznych utrudniają poprawne funkcjonowanie systemu podatnego

Źródło: opracowanie własne na podstawie Pijanowski, Marczewski, Staniszewski, 2014)

Tabela G.10. Wpływ systemów IK na system sieci teleinformatycznych

System oddziałujący	Oddziaływanie
System zaopatrzenia w energię, surowce energetyczne i paliwa	• zakłócenia systemu utrudniają lub uniemożliwiają poprawne funkcjonowanie systemu sieci teleinformatycznych
System łączności	
System transportowy	
System zapewniający ciągłość działania administracji publicznej	

Źródło: opracowanie własne na podstawie Pijanowski, Marczewski, Staniszewski, 2014)

Tabela G.11. Wpływ systemu finansowego na inne systemy IK

System podatny	Podatność
System zaopatrzenia w energię, surowce energetyczne i paliwa	• zakłócenia systemu finansowego utrudniają lub uniemożliwiają poprawne funkcjonowanie systemu podatnego
System łączności	
System sieci teleinformatycznych	
System zaopatrzenia w żywność	
System zaopatrzenia w wodę	
System ochrony zdrowia	
System transportowy	
System ratowniczy	
System zapewniający ciągłość działania administracji publicznej	
System produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych	

Źródło: opracowanie własne na podstawie Pijanowski, Marczewski, Staniszewski, 2014.

Tabela G.12. Wpływ systemów IK na system finansowy

System oddziałujący	Oddziaływanie
System zaopatrzenia w energię, surowce energetyczne i paliwa	• zakłócenia systemu finansowego mogą destabilizować poprawne funkcjonowanie systemu finansowego
System łączności	
System sieci teleinformatycznych	
System transportowy	
System zapewniający ciągłość działania administracji publicznej	

Źródło: opracowanie własne na podstawie Pijanowski, Marczewski, Staniszewski, 2014.

Tabela G.13. Wpływ systemu zapewniania ciągłości działania administracji publicznej na inne systemy IK

System podatny	Podatność
System zaopatrzenia w energię, surowce energetyczne i paliwa	• zakłócenie w funkcjonowaniu systemu zapewniania ciągłości działania administracji publicznej może doprowadzić do poważnych utrudnień lub paraliżu funkcjonowania systemu podatnego
System łączności	
System sieci teleinformatycznych	
System finansowy	
System zaopatrzenia w żywność	
System zaopatrzenia w wodę	
System ochrony zdrowia	
System transportowy	
System ratowniczy	
System produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych	

Źródło: opracowanie własne na podstawie Pijanowski, Marczewski, Staniszewski, 2014.

Tabela G.14. Wpływ systemów IK na system zapewniania ciągłości działania administracji publicznej

System oddziałujący	Oddziaływanie
System zaopatrzenia w energię, surowce energetyczne i paliwa	• zakłócenia systemu utrudniają lub uniemożliwiają poprawne funkcjonowanie systemu zapewniania ciągłości działania administracji publicznej
System łączności	
System sieci teleinformatycznych	
System finansowy	
System zaopatrzenia w żywność	
System zaopatrzenia w wodę	
System ochrony zdrowia	
System transportowy	
System ratowniczy	
System produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych	

Źródło: opracowanie własne na podstawie Pijanowski, Marczewski, Staniszewski, 2014.

Tabela G.15. Wpływ systemu zaopatrzenia w żywność na inne systemy IK

System podatny	Podatność
System zaopatrzenia w wodę	• możliwe skażenie ujęć wody ze względu na złą utylizację skażonej żywności, surowców rolno-spożywczych i pasz
System ochrony zdrowia	• możliwy wpływ na ograniczenie dostaw żywności placówek żywienia zbiorowego (szpitali)

Źródło: opracowanie własne na podstawie Obiedzińska, Kochanek, Kiślowski, 2014.

Tabela G.16. Wpływ systemów IK na system zaopatrzenia w żywność

System oddziałujący	Oddziaływanie
System zaopatrzenia w energię, surowce energetyczne i paliwa	• utrudniony dostęp do zakupu paliw • utrudniony transport surowców rolno-spożywczych, żywności i pasz • zakłócony przepływ surowców rolno-spożywczych i żywności między operatorami łańcucha żywnościowego • ograniczona produkcja żywności • utrudniony dostęp bądź brak zasilania w obiektach biorących udział w funkcjonowaniu łańcucha żywnościowego • utrudnione funkcjonowanie podmiotów łańcucha żywnościowego
System łączności	• ograniczenie lub brak możliwości kontroli zakupu i sprzedaży surowców rolno-spożywczych, żywności i pasz
System sieci teleinformatycznych	• niedostępne systemy teleinformatyczne prowadzące do dezorganizacji łańcucha żywności
System finansowy	• ograniczenie lub brak możliwości dokonania operacji finansowych dotyczących zakupu i lub sprzedaży surowców rolno-spożywczych, żywności i pasz oraz komunikacji pomiędzy ogniwami łańcucha żywnościowego
System zaopatrzenia w wodę	• ograniczona produkcja żywności • utrudniony dostęp bądź brak zasilania wody w obiektach biorących udział w funkcjonowaniu łańcucha żywnościowego • utrudnione funkcjonowanie podmiotów łańcucha żywnościowego
System transportowy	• ograniczony dostęp do surowców rolno-spożywczych do produkcji żywności • zakłócona ciągłość produkcji roślinnej i zwierzęcej
System produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych	• skażenie środowiska naturalnego • ograniczony dostęp do żywności, pasz, surowców rolnych spełniających wymogi bezpieczeństwa i jakości żywności i pasz • ograniczony dostęp do surowców paszowych niezbędnych do żywienia zwierząt • ograniczony dostęp do surowców rolno-spożywczych do produkcji żywności • zakłócona ciągłość produkcji roślinnej i zwierzęcej • zakłócony przepływ surowców i informacji między operatorami łańcucha żywnościowego

Źródło: opracowanie własne na podstawie Obiedzińska, Kochanek, Kiślowski, 2014.

Tabela G.17. Wpływ systemu zaopatrzenia w wodę na inne systemy IK

System podatny	Podatność
System zaopatrzenia w energię, surowce energetyczne i paliwa	• brak wody do celów produkcyjnych (wytwarzania pary do turbin, chłodzenia itp.) • brak wody do celów transportowych • brak wody do mycia i konserwacji budynków • brak wody do mycia i konserwacji urządzeń • brak wody do celów składowania odpadów • brak możliwości odprowadzenia ścieków i odpadów • brak wody do picia i mycia dla pracowników
System łączności	• brak wody do mycia i konserwacji budynków • brak wody do mycia i konserwacji urządzeń • brak możliwości odprowadzenia ścieków i odpadów • brak wody do picia i mycia dla pracowników
System finansowy	• brak wody do mycia i konserwacji budynków • brak wody do mycia i konserwacji urządzeń • brak możliwości odprowadzenia ścieków i odpadów • brak wody do picia i mycia dla pracowników
System ochrony zdrowia	• brak wody niezbędnej dla leczenia pacjentów (np. w czasie operacji i zabiegów) • brak wody do utrzymywania należytych warunków higienicznych • brak wody do mycia i konserwacji urządzeń • brak możliwości odprowadzenia ścieków i odpadów • brak wody do picia i mycia dla pacjentów i pracowników
System transportowy	• brak wody do mycia i konserwacji urządzeń • brak możliwości odprowadzenia ścieków i odpadów • brak wody do picia i mycia dla pracowników
System ratowniczy	• brak wody do prowadzenie akcji ratowniczej (np. gaszenia pożarów lub usuwania wycieków substancji szkodliwych) • brak wody do utrzymywania należytych warunków higienicznych (głównie w przypadku ratownictwa medycznego) • brak wody do mycia i konserwacji urządzeń • brak możliwości odprowadzenia ścieków i odpadów • brak wody do picia i mycia dla poszkodowanych i pracowników
System zapewniający ciągłość działania administracji publicznej	• brak wody do mycia i konserwacji budynków • brak wody do mycia i konserwacji urządzeń • brak możliwości odprowadzenia ścieków i odpadów • brak wody do picia i mycia dla klientów i pracowników
System produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych	• brak wody do celów produkcyjnych • brak wody do celów transportowych • brak wody do mycia i konserwacji budynków • brak wody do mycia i konserwacji urządzeń • brak wody do celów składowania odpadów • brak możliwości odprowadzenia ścieków i odpadów • brak wody do podjęcia akcji ratowniczej na wypadek awarii • brak wody do picia i mycia dla pracowników

Źródło: opracowanie własne na podstawie Obiedzińska, Kochanek, Kiślowski, 2014.

Tabela G.18. Wpływ systemów IK na system zaopatrzenia w wodę

System oddziałujący	Oddziaływanie
System zaopatrzenia w energię, surowce energetyczne i paliwa	• brak energii niezbędnej do napędzania urządzeń infrastruktury wodnej • błędy w sterowaniu infrastrukturą • błędy w komunikacji i zarządzaniu • brak możliwości usunięcia usterek • brak lub ograniczenia w transporcie wody, ścieków i/lub substancji koniecznych do działania infrastruktury wodnej • brak dostaw materiałów i części zamiennych • ograniczone możliwości dokonania napraw i rozbudowy systemu zaopatrzenia w wodę • ograniczone możliwości dojazdu pracowników
System łączności	• błędy w sterowaniu infrastrukturą • błędy w komunikacji i zarządzaniu • brak możliwości usunięcia usterek
System finansowy	• brak środków finansowych niezbędnych do utrzymania produkcji i dystrybucji wody oraz transportu i oczyszczania ścieków • brak środków na zakup części zamiennych i materiałów • brak środków na naprawę usterek • brak środków dla pracowników
System ochrony zdrowia	• brak pracowników • potencjalna konieczność budowy nowej (często tymczasowej) infrastruktury, gdy ośrodki zdrowia zostają na czas kryzysu przeniesione w inne miejsce • zwiększone pobory wody i ilości ścieków w sytuacjach kryzysowych (np. w przypadku epidemii, wojny, katastrofy przemysłowej itp.) • konieczność niestandardowego działania w przypadku zanieczyszczenia wody przez odpady medyczne
System transportowy	• brak stałych dostaw materiałów i części zamiennych • ograniczone możliwości dokonania napraw i rozbudowy systemu zaopatrzenia w wodę • ograniczone możliwości dojazdu pracowników
System ratowniczy	• brak możliwości usunięcia lub minimalizacji skutków katastrofy ekologicznej (np. w przypadku wycieku z infrastruktury wodnej skażonej wody do środowiska lub poboru skażonego surowca ze środowiska przez infrastrukturę zaopatrzenia w wodę) • brak możliwości naprawy zniszczeń lub uszkodzeń infrastruktury wodnej (spowodowanej np. aktem terroryzmu, katastrofą naturalną) • brak możliwości ewakuacji personelu, którego życie lub zdrowie jest zagrożone
System zapewniający ciągłość działania administracji publicznej	• błędy w sterowaniu infrastrukturą • błędy w komunikacji i zarządzaniu • brak środków finansowych niezbędnych do utrzymania produkcji i dystrybucji wody oraz transportu i oczyszczania ścieków • brak środków finansowych na wynagrodzenia pracowników • brak planów rozbudowy i utrzymania infrastruktury wodnej lub plany są niewłaściwe
System produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych	• potencjalna możliwość zanieczyszczenia naturalnego środowiska wodnego (surowca dla infrastruktury wodnej) • możliwość zanieczyszczenia wody będącej już w obiegu (np. skażenie wody podczas uzdatniania lub dystrybucji) • potencjalna konieczność opuszczenia skażonych budynków przez personel zajmujący się infrastrukturą wodną • nieodwracalne zniszczenie infrastruktury wodnej poprzez skażenie (np. radiologiczne)

Źródło: opracowanie własne na podstawie Obiedzińska, Kochanek, Kiślowski, 2014.

Tabela G.19. Wpływ systemu ratownictwa na inne systemy IK

System podatny	Podatność
System zaopatrzenia w energię, surowce energetyczne i paliwa	• zakłócenie w systemie ratownictwa ogranicza bądź uniemożliwia udzielenie pomocy w sytuacjach kryzysowych
System łączności	
System sieci teleinformatycznych	
System finansowy	
System zaopatrzenia w żywność	
System zaopatrzenia w wodę	
System ochrony zdrowia	
System transportowy	
System zapewniający ciągłość działania administracji publicznej	
System produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych	

Źródło: opracowanie własne na podstawie Obiedzińska, Kochanek, Kiślowski, 2014.

Tabela G.20. Wpływ systemów IK na system ratownictwa

System oddziałujący	Oddziaływanie
System zaopatrzenia w energię, surowce energetyczne i paliwa	• utrudniona realizacja funkcji w sytuacjach kryzysowych
System łączności	• brak informacji o sytuacjach kryzysowych
System zaopatrzenia w żywność	• utrudniona realizacja funkcji na skutek wystąpienia ograniczeń w sferze zasobów ludzkich
System zaopatrzenia w wodę	• utrudniona realizacja funkcji na skutek wystąpienia ograniczeń w sferze zasobów ludzkich
System ochrony zdrowia	• brak możliwości dotarcia do poszkodowanych
System transportowy	• brak możliwości wypełniania niektórych działań ratowniczych
System produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych	• awaria tego systemu może uniemożliwić działanie elementów systemu ratownictwa (np. utrudniony dostęp do miejsc skażonych)

Źródło: opracowanie własne na podstawie Obiedzińska, Kochanek, Kiślowski, 2014.

Tabela G.21. Wpływ systemu ochrony zdrowia na inne systemy IK

System podatny	Podatność
System zaopatrzenia w energię, surowce energetyczne i paliwa	• organicznie możliwości wypełniania funkcji na skutek wystąpienia braków w sferze zasobów ludzkich
System łączności	
System sieci teleinformatycznych	
System finansowy	
System zaopatrzenia w żywność	
System zaopatrzenia w wodę	
System transportowy	
System ratowniczy	
System zapewniający ciągłość działania administracji publicznej	
System produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych	

Źródło: opracowanie własne na podstawie Obiedzińska, Kochanek, Kiślowski, 2014.

Tabela G.22. Wpływ systemów IK na system ochrony zdrowia

System oddziałujący	Oddziaływanie
System zaopatrzenia w energię, surowce energetyczne i paliwa	• w przypadku jednostek nieposiadających własnego, alternatywnego źródła zasilania zaburzenie działania tego systemu spowoduje brak możliwości wykonywania większości procedur medycznych
System łączności	• powoduje brak możliwości kontaktu z jednostkami świadczącymi usługi medyczne
System sieci teleinformatycznych	• może wywoływać brak możliwości identyfikacji danych o pacjencie
System zaopatrzenia w żywność	• brak możliwości zapewnienia aprowizacji personelowi i pacjentom
System zaopatrzenia w wodę	• brak możliwości wykonywania niektórych procedur medycznych
System transportowy	• brak możliwości dotarcia do pacjenta i pacjenta do jednostki udzielającej świadczenia medyczne
System ratowniczy	• brak możliwości udzielania pomocy medycznej w sytuacjach kryzysowych
System produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych	• awaria tego systemu może uniemożliwić działanie elementów systemu ochrony zdrowia

Źródło: opracowanie własne na podstawie Obiedzińska, Kochanek, Kiślowski, 2014.

Dr inż. Michał Wiśniewski - pracownik naukowo-dydaktyczny zatrudniony na Wydziale Zarządzania Politechniki Warszawskiej. Absolwent studiów licencjackich w Kolegium Nauk Ekonomicznych i Społecznych Politechniki Warszawskiej filia w Płocku oraz studiów inżynierskich i magisterskich na Wydziale Zarządzania Politechniki Warszawskiej. Stopień naukowy doktora w dyscyplinie nauk o zarządzaniu uzyskał w 2018 r.

W latach 2011-2012 pracował przy projekcie finansowanym przez MNiSW pt. „Model optymalizacji organizacji zarządzania policji w obszarze kosztów, transportu i gospodarowania nieruchomościami". W 2013-2014 odbył czteromiesięczny staż w firmie MyIT pracując nad projektem systemu eksperckiego służącego do zarządzania ryzykiem operacyjnym. W latach 2013-2015 brał udział w projekcje finansowanym przez NCBiR pt. „Metodyka oceny ryzyka na potrzeby systemu zarządzania kryzysowego RP". W latach 2015-2018 pracował przy projekcie finansowanym przez NCBiR pt. „Wysokospecjalistyczna platforma wspomagająca planowanie cywilne i ratownictwo w administracji publicznej Rzeczypospolitej Polskiej oraz w jednostkach organizacyjnych Krajowego Systemu Ratowniczo Gaśniczego". W kadencji 2016-2020 członek Rady Wydziału Zarządzania.

Autor lub współautor ponad czterdziestu opracowań naukowych z obszaru nauk o zarządzaniu dotyczących zarządzania procesowego, chmury obliczeniowej, zarządzania bezpieczeństwem infrastruktury krytycznej. Laureat nagród naukowych i organizacyjnych Rektora Politechniki Warszawskiej.

„Autor opracował oryginalny model IM-BIK, będący jego autorskim pomysłem. Model zawiera wiele nowych opracowanych przez autora elementów rozszerzających metody analizy ryzyka. Autor wprowadził ilościowy miernik zmiennej losowej jaką jest funkcjonalność oraz zinterpretował mierniki podatności i wpływu zabezpieczeń. To, co jest również istotne to uwzględnienie w modelu wzajemnych zależności między poszczególnymi rodzajami IK oraz między różnymi zagrożeniami. Autor adoptował model sytuacji Kłykowa, ustalając kanon sytuacji IK. Zdefiniował podstawowe atrybuty zagrożeń ich zależności, podstawowe atrybuty funkcjonalności oraz atrybuty zależności IK, a także atrybuty zabezpieczeń. Taki zabieg pozwolił autorowi „wyjść" na ilościową analizę ryzyka w oparciu o zmodyfikowany wzór na ryzyko. Z IM-BIK nierozerwalnie związane są procesy decyzyjne, które w ujęciu autora, bazując na zaproponowanej przez niego analizie ryzyka, również mają charakter ilościowy. Model jest na tyle uniwersalny, że może być zastosowany w wielu obszarach bezpieczeństwa w szczególności bezpieczeństwa na terenie jednostek administracji publicznej (nie tylko z punktu widzenia IK) (…)"

Z recenzji prof. dr hab. Jerzego Wolanina

„Oczywistym osiągnięciem autora jest stworzenie całkiem udanej konstrukcji modelu bezpieczeństwa infrastruktury krytycznej oraz metodyki zarządzania sytuacyjnego bezpieczeństwem infrastruktury krytycznie. W zakresie wyników badań należy stwierdzić, że otrzymane rezultaty potwierdziły użyteczność opracowanego modelu i metodyki".

Z recenzji prof. dr hab. inż. Jacka Szołtyska