Nowoczesne Systemy Zarządzania
Zeszyt 13 (2018), nr 4 (październik-grudzień)
ISSN 1896-9380, s. 89-104

Instytut Organizacji i Zarządzania
Wydział Cybernetyki
Wojskowa Akademia Techniczna
w Warszawie

Modern Management Systems
Volume 13 (2018), No. 4 (October-December)
ISSN 1896-9380, pp. 89-104

Institute of Organization and Management
Faculty of Cybernetics
Military University of Technology

Koncepcja narzędzia informatycznego wspomagającego budowę scenariuszy zdarzeń niekorzystnych

Functional assumptions of an IT tool to assist in the construction of adverse event scenarios

Michał Wiśniewski
Politechnika Warszawska, Wydział Zarządzania,
Katedra Systemów Zarządzania

Abstrakt. W artykule przedstawiono koncepcję oraz wymagania funkcjonalne narzędzia informatycznego wspomagającego budowę scenariuszy zdarzeń niekorzystnych oraz umiejscowienie tego narzędzia w procesie planowania cywilnego. Ponadto artykuł przedstawia procedury: opracowania scenariuszy zdarzeń niekorzystnych, budowy problemu decyzyjnego oraz weryfikacji zabezpieczeń zaproponowanych w ramach reakcji na rozpoznane zagrożenia, na które podatny jest rozpatrywany obiekt.
Słowa kluczowe: planowanie cywilne, scenariusz zdarzenia niekorzystnego, model sytuacji zasobu, problem decyzyjny, weryfikacja zabezpieczeń, infrastruktura krytyczna.

Abstract. The paper presents the concept and functional requirements of an IT tool to assist in the development of adverse event scenarios and the location of this IT tool in the process of civil planning. In addition, the paper provides procedures: development of adverse events scenarios, determination of a decision problem and verification of safeguards proposed in response to identified threats to which the object under consideration is exposed.
Keywords: Civilian Planning, Adverse Event Scenario, Resource Situation Model, Decision Problem, Security Verification, Critical Infrastructure.

Wstęp

Utrzymanie bezpieczeństwa publicznego jest jednym z podstawowych obowiązków państwa. Osiągnięcie tego celu uzależnione jest od wyczerpującej identyfikacji

zagrożeń, analizowania ryzyka, które wyrażają, jak również podejmowania działań prewencyjnych wobec zagrożeń oraz działań naprawczych wobec incydentów i sytuacji kryzysowych. Obecnie w Polsce bezpieczeństwo publiczne jest zapewniane m.in. w ramach tzw. planowania cywilnego (PC).

Odpowiednia reakcja na rozpoznane zagrożenia wymaga połączenia wiedzy dotyczącej zagrożeń oraz skuteczności działań podejmowanych w celu eliminacji skutków zdarzenia niekorzystnego[1]. Gromadzona wiedza powinna m.in. uwzględniać współzależności zagrożeń[2] oraz funkcjonalności[3] rozpatrywanych zasobów.

Określenie charakterystyki rozpatrywanego obiektu uwzględniającej listę zagrożeń wraz z identyfikacją wzajemnych powiązań między zagrożeniami jest podstawą opracowania prognozy rozprzestrzeniania się zdarzeń niekorzystnych, która pozwala odpowiednio dobrać siły i środki do zaistniałej sytuacji. Obserwacja ta stała się przyczyną zaproponowania zasad budowy scenariuszy zdarzeń niekorzystnych, które opracowano na bazie analizy wymogów formalno-prawnych, zagranicznych metodyk oceny ryzyka na potrzeby zarządzania kryzysowego oraz metod i technik organizatorskich, analitycznych i projektowych stosowanych w biznesie (Wiśniewski, Kisilowski, Marczewski, 2016, s. 97-110). Procedurę budowy scenariuszy zdarzeń niekorzystnych poddano weryfikacji za pomocą eksperymentu obliczeniowego, przeprowadzonego na bazie danych pochodzących z Planów Zarządzania Kryzysowego (PZK)Województwa Mazowieckiego i Podlaskiego z 2015 r. (Wiśniewski, 2017).

Ocena procedury budowy scenariuszy zdarzeń niekorzystnych wykazała potrzebę uzupełnienia jej o procedurę budowy problemu decyzyjnego oraz procedurę weryfikacji zabezpieczeń. Zabieg ten pozwala na realizację funkcji zarządzania w obszarze zarządzania bezpieczeństwem[4] rozpatrywanego obiektu.

Realizacja opracowanych procedur budowy scenariuszy zdarzeń niekorzystnych, budowy problemu decyzyjnego oraz weryfikacji zabezpieczeń wymaga wsparcia ze strony narzędzia informatycznego[5]. Celem artykułu jest przedstawienie koncepcji narzędzia informatycznego wspomagającego budowę scenariuszy zdarzeń niekorzystnych na tle wymogów stawianych planom zarządzania kryzysowego

---

1 Zdarzenie niekorzystne – zdarzenie będące efektem spełnienia się zagrożenia, mające negatywne skutki dla organizacji, procesu gospodarczego, środowiska naturalnego lub ludności.

2 Wymóg zapisany w NPOIK i Europejskim Programie Ochrony IK.

3 Wymóg zapisany w dyrektywie NIST z dnia 21 kwietnia 2016 r. w sprawie bezpieczeństwa sieci i systemów teleinformatycznych opublikowanej przez Radę UE i zatwierdzonej przez Unijny Parlament 6 lipca 2016.

4 Zarządzanie bezpieczeństwem obiektu jest rozumiane jako zespół działań lub procedur realizowanych w obszarze planowania, organizowania, weryfikacji i realizacji, wykonywanych dla osiągnięcia wymaganego poziomu bezpieczeństwa zasobu uzależnionych od sytuacji, w jakiej zasób się znajduje.

5 Narzędzie informatyczne – oprogramowanie umożliwiające interakcję człowieka z komputerem, przeznaczone do wykonywania czynności oraz rozwiązywania problemów zadanych przez tego użytkownika.

(PZK) i planom ochrony infrastruktury krytycznej (POIK). Koncepcja narzędzia informatycznego została opracowana w ramach projektu rozwojowego NCBiR pt. Wysokospecjalistyczna platforma wspomagająca PC i ratownictwo w administracji publicznej RP oraz jednostkach organizacyjnych KSRG[6].

1. Koncepcja narzędzia informatycznego

Ze względu na zapewnienie możliwości szybkiego wdrażania funkcjonalności narzędzia informatycznego wspierającego opracowywanie scenariuszy zdarzeń niekorzystnych oraz możliwość rozłożenia kosztów budowy oprogramowania na kilka etapów proponuje się aby projektowane narzędzie informatyczne miało budowę modułową (rys. 1) złożoną z:

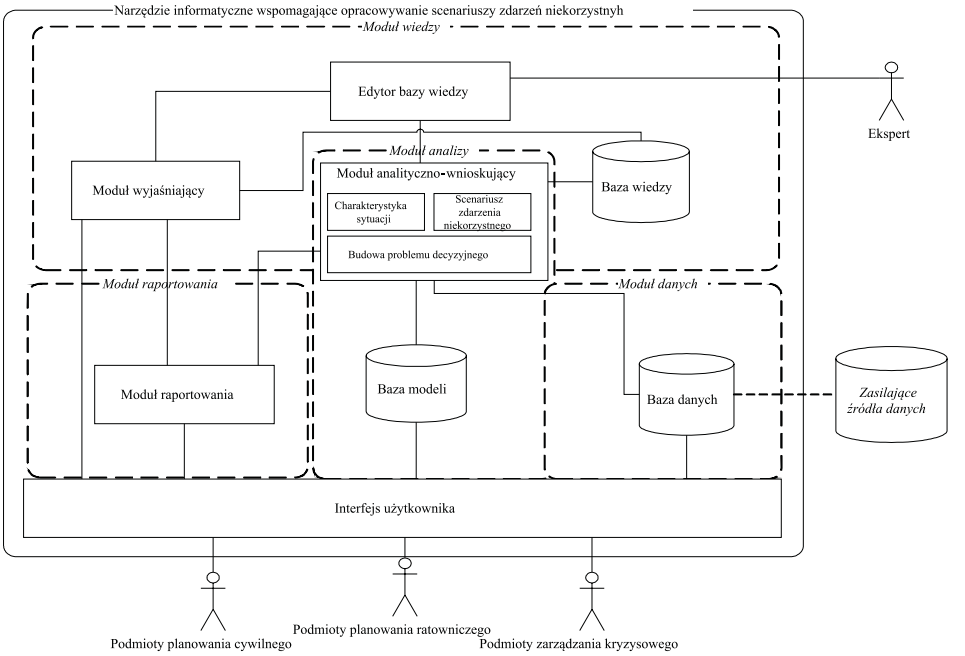
- moduł danych – odpowiadającej za pozyskiwanie, gromadzenie i udostępnianie danych,
- moduł analizy – przetwarzającej dane do postaci informacji, wspomagającej podejmowanie decyzji w PC tzn.:
  - przetwarzającej zgromadzone dane w model sytuacji rozpatrywanego zasobu,
  - umożliwiającej symulację przebiegu zdarzenia niekorzystnego,
  - umożliwiającej zbudowanie problemu decyzyjnego,
  - moduł wiedzy – przetwarzającej zgromadzone dane i informacje do postaci sprawdzonych przypadków zastosowania zabezpieczeń przed rozpatrywanymi zagrożeniami oraz umożliwiającej ich porównanie z rozpatrywaną sytuacją zasobu,
  - moduł raportowania – odpowiadającej za dopasowane do potrzeb użytkownika dokumentowanie wyników prowadzonych analizy.

W proponowanym rozwiązaniu warstwa danych składa się bazy danych oraz powiązań integracyjnych z:

- zasilającymi źródłami danych tj. Centralna Aplikacja Raportująca, Baza danych Państwowej Straży Pożarnej czy projektowana Wysokospecjalistyczna platforma wspomagająca PC i ratownictwo w administracji publicznej RP oraz w jednostkach organizacyjnych KSRG,
- interfejsem użytkownika,
- modułem analityczno-wnioskującym.

[6] Umowa nr DOB – BIO7/11/02/2015, na wykonanie projektów w zakresie badań naukowych i projektów rozwojowych na rzecz obronności i bezpieczeństwa państwa, przez konsorcjum: Politechnika Warszawska (Wydział Zarządzania), Medcore sp. z o.o.

Dane, zgromadzone dzięki warstwie danych, trafiają przez moduł analityczny do modułu raportowania, bądź do bazy wiedzy. Stąd jest to newralgiczny element narzędzia, decydujący o poprawności jego funkcjonowania.



Rys. 1. Model struktury narzędzia informatycznego wspomagającego procedurę budowy scenariuszy zdarzeń niekorzystnych

Źródło: opracowanie własne

Warstwa analizy obejmuje bazę modeli oraz moduł analityczno-wnioskujący, współużytkowany przez warstwę wiedzy. Warstwa analizy stanowi rdzeń projektowanego narzędzia, integrujący pozostałe jego warstwy. Komunikuje się zarówno z warstwą danych, przez którą jest zasilana, jak i z generatorem raportów oraz interfejsem użytkownika, do których zwraca wyniki analiz. Pełni też funkcję usługową dla warstwy wiedzy, implementując sprawdzone przypadki skutecznych zabezpieczeń jako reguły dla bazy wiedzy oraz realizując proces weryfikacji zabezpieczeń. Składa się z dwóch zasadniczych elementów:

- bazy modeli – implementującej modele analityczne, które umożliwiają utworzenie modelu sytuacji rozpłatywanego zasobu,
- modułu analityczno-wnioskującego – realizującego procedury:
  - odwzorowania sytuacji zasobu,
  - opracowanie scenariusza zdarzenia niekorzystnego,
  - budowy problemu decyzyjnego.

Warstwa wiedzy odpowiada w projektowanym rozwiązaniu za gromadzenie, przetwarzanie i udostępnianie wiedzy dotyczącej przypadków zdarzeń niekorzystnych, które wystąpiły w przeszłości oraz zastosowanych wówczas zabezpieczeń. Przy czym wiedza ta może być pozyskiwana od eksperta (i w początkowej fazie funkcjonowania narzędzia jest to niezbędny element) albo syntetyzowana na podstawie wyników analiz realizowanych w warstwie analizy. Będzie to możliwe, pod warunkiem zgromadzenia odpowiedniej liczby danych o incydentach i związanych z nimi stratach. Wiedza eksperta jest dostarczana do narzędzia przez edytor bazy wiedzy i składowana w postaci reguł. Baza reguł jest porównywana z nowo wprowadzanym przypadkiem w module wnioskującym. Przez mechanizmy dopasowania tworzone są zestawienia przypadków, które odpowiadają zaistniałym zdarzeniom. Przypadki podobne wskazują na działania, które powinny być podjęte w związku z zaistniałą sytuacją.

Moduł raportowania służy jako generator raportów rozsyłanych dostępnymi kanałami dystrybucji do uprawnionych użytkowników. Moduł raportowania należy traktować, jako narzędzie komunikacji dla podmiotów planowania cywilnego.

Projektowane narzędzie informatyczne, wspomagające realizację zadań PC[7] (Dz.U. 2017 poz. 209, art. 4), zakłada obsługę trzech obszarów funkcjonalnych:

- generowania scenariuszy zdarzeń niekorzystnych – procedura budowy scenariuszy zdarzeń niekorzystnych,
- podejmowania decyzji dotyczących zabezpieczeń przed rozpoznanymi zagrożeniami – procedura budowy problemu decyzyjnego,
- weryfikacji zaproponowanych zabezpieczeń – procedura weryfikacji zabezpieczeń.

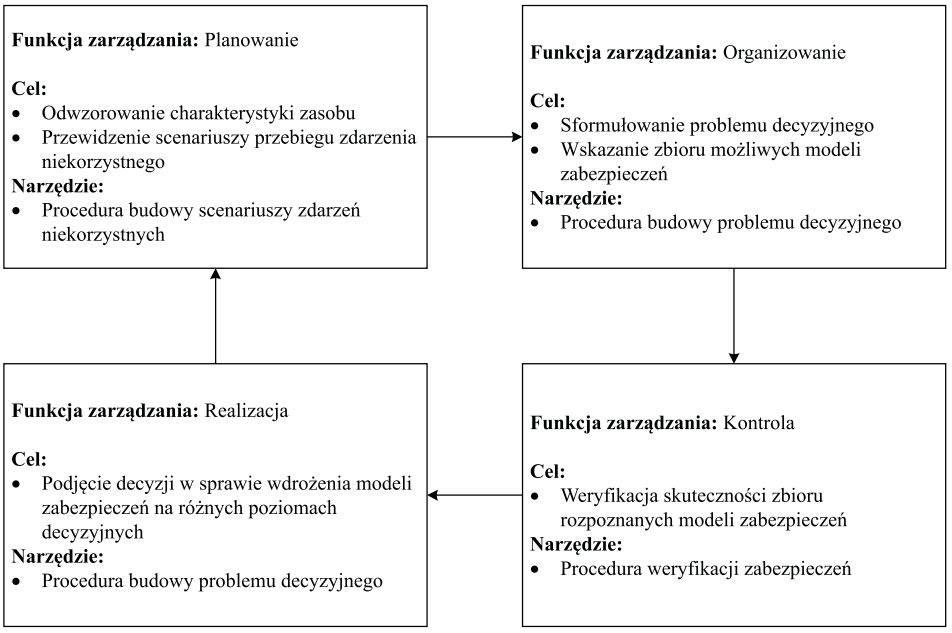
Procedura budowy scenariuszy zdarzeń niekorzystnych może zostać wykorzystana do dokładniejszego przygotowania PZK, które będą uwzględniały nie tylko wykaz zagrożeń, na jakie narażony jest rozpatrywany obiekt, ale również zależności występujące między tymi zagrożeniami. Pozwoli to na rozpoznanie szerszego zbioru zdarzeń niekorzystnych, na wypadek których należy przygotować struktury uruchamiane w sytuacjach kryzysowych, oraz efektywniej (pod względem kosztów utrzymania) dobrać siły i środki niezbędne do wykonania celów zarządzania kryzysowego[8]. Produktem procedury budowy scenariuszy zdarzeń niekorzystnych jest charakterystyka rozpatrywanego obiektu dostarczająca wiedzy na temat zagrożeń,

[7] Planowanie cywilne obejmuje całokształt przedsięwzięć organizacyjnych mających na celu przygotowanie administracji publicznej do zarządzania kryzysowego, planowania w zakresie wspierania Sił Zbrojnych RP w razie ich użycia oraz planowanie wykorzystania Sił Zbrojnych RP do realizacji zadań z zakresu zarządzania kryzysowego (Dz.U. 2017 poz. 209, art. 3, pkt 4).

[8] 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).

przed którymi należy chronić obiekt. Rozpoznany zbiór zagrożeń stanowi problem decyzyjny, którego rozwiązaniem jest zbiór zabezpieczeń realizujący funkcję celu określoną przez podmiot odpowiedzialny za bezpieczeństwo obiektu.

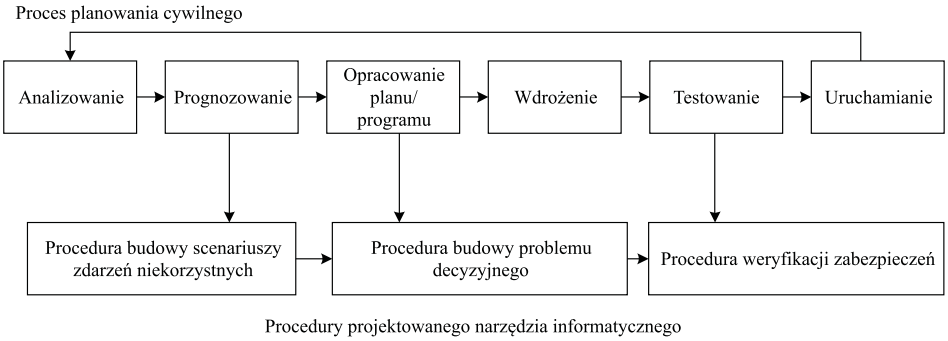
Procedura budowy problemu decyzyjnego może zostać wykorzystana do przygotowania odpowiednich struktur uruchamianych w sytuacjach kryzysowych. Zwykle podmioty odpowiedzialne za bezpieczeństwo rozpatrywanego obiektu mają do wyboru kilka możliwości zabezpieczenia się przed rozpoznanym zagrożeniem, jednak ze względów kosztowych nie mogą zastosować ich wszystkich. Powstaje więc pytanie, jaki zestaw zabezpieczeń zastosować dla rozpoznanego zbioru zagrożeń, na które podatny jest obiekt. Projektowane narzędzie pozwoli utworzyć model problemu decyzyjnego uwzględniającego zagrożenia (obszary decyzyjne) oraz zabezpieczenia (decyzje elementarne) dla sytuacji[9], w której znajduje się rozpatrywany obiekt. Rozwiązanie problemu decyzyjnego pozwoli wskazać zestaw zabezpieczeń, spełniający przyjętą funkcję celu, np. minimalizujący czas przywrócenia funkcjonalności[10] obiektu.



Rys. 2. Koncepcja Integralnego Modelu Bezpieczeństwa
Źródło: opracowanie własne

[9] Sytuacją nazywamy zbiór węzłów (zasobów) V {V1, …, Vn}, związanych ze sobą skierowanymi połączeniami (zagrożeniami) Z {Z1, …, Zn}.

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



Rys. 3. Umiejscowienie projektowanego narzędzia informatycznego w procesie PC

Źródło: opracowanie własne (Dz.U. 2017 poz. 209)

Procedura weryfikacji zabezpieczeń ma pozwolić na określenie, czy zaproponowany zestaw zabezpieczeń będzie skuteczny[11]. Zakłada się, że weryfikacja będzie dokonywana na podstawie analizy przypadków z przeszłości, w których wystąpiły podobne[12] zagrożenia i zastosowane były podobne zabezpieczenia.

Wymienione procedury można przedstawić na planie funkcji zarządzania (rys. 2), gdzie czynnością inicjującą cykl jest określenie charakterystyki rozpatrywanego obiektu (funkcja planowanie). Realizacja cyklu prowadzi do wdrożenia zabezpieczeń przed rozpoznanymi zagrożeniami (funkcja realizacja), co wpływa na obiekt, wymuszając ponowne określenie jego charakterystyki.

Analiza celów poszczególnych kroków PC wykazała, że projektowane narzędzie informatyczne powinno wspomagać realizację etapów: programowanie, opracowanie planu/programu oraz testowanie (rys. 3).

2. Procedura opracowywania scenariuszy zdarzeń niekorzystnych

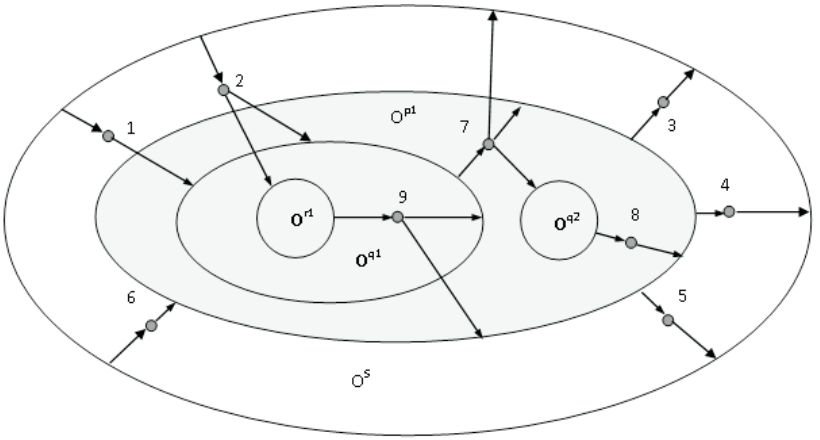
Scenariusze zdarzeń niekorzystnych realizują się w systemie połączonych ze sobą zasobów (rys. 4), które zapewniają dostęp do funkcjonalności niezbędnych do działania systemu, którego są składowymi.

Zasoby można opisać zestawem funkcjonalności oraz zestawem zagrożeń, na które podatny jest zasób. Przyjmując to założenie, opracowano model sytuacji zasobu (MSZ)

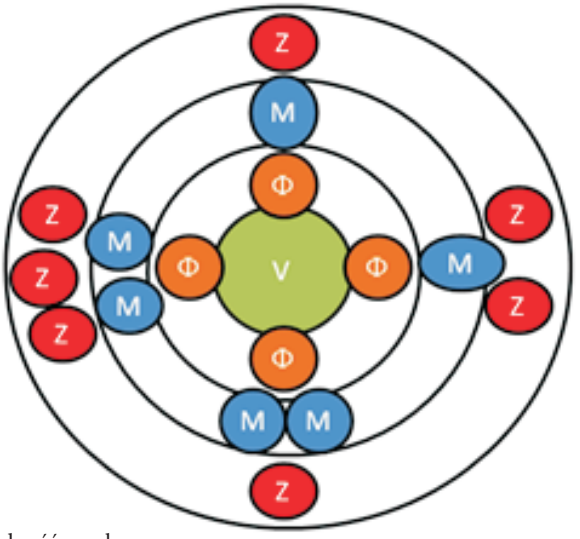
[11] Skuteczność zabezpieczenia jest rozumiana jako wyeliminowanie skutków zagrożenia poprzez zastosowane zabezpieczenie, np. utrzymanie dostępności energii elektrycznej dla szpitala, umożliwiające jego funkcjonowanie, w wyniku zastosowania agregatu prądotwórczego na wypadek utraty zasilania z miejskiej sieci energetycznej.

[12] Podobieństwo – wskaźnik określający stopień równoważności dwóch obiektów w przestrzeni ocenianych kryteriów.

(rys. 5), który stanowi podstawowy element pozwalający określić charakterystykę rozpatrywanego systemu, w którym realizują się scenariusze zdarzeń niekorzystnych (Wiśniewski, 2016, s. 297-310).



Rys. 4. Przykład hipergrafowej struktury zasobów i łączące je kanały
Źródło: (Krupa, 2015, s. 7793)



gdzie:

- V – zasób,
- Φ – funkcjonalność zasobu,
- Z – zagrożenia oddziałujące na funkcjonalność,
- M – modele zabezpieczeń funkcjonalności.

Rys. 5. Model sytuacji zasobu
Źródło: (Wiśniewski, 2016, s. 301)

Pomiędzy zasobami istnieją połączenia, które można zdefiniować w postaci kanału łączącego dwa zasoby (Krupa, 2013, s. 89-102). Znajomość organizacji procesu, w którym wykorzystywany jest zasób, w połączeniu funkcjonalnościami zasobów, pozwala na wskazanie wzajemnych powiązań (rys. 4).

Na bazie MSZ opracowano procedurę projektowania scenariuszy zdarzeń niekorzystnych:

- Krok 1 – opis charakterystyki rozpatrywanego zasobu;
- Krok 2 – opis zagrożeń, na które podatny jest zasób;
- Krok 3 – określenie wpływu zagrożeń;
- Krok 4 – przygotowanie struktury systemu;
- Krok 5 – przygotowanie opisów scenariuszy.

Przykład realizacji omawianej procedury został przedstawiony w artykule pt. „Weryfikacja stosowalności zasad budowy scenariuszy zdarzeń niekorzystnych – raport z badań" (Wiśniewski, 2017).

3. Procedura budowy problemu decyzyjnego

Zbiór zagrożeń zapisany w postaci MSZ lub wyłoniony przez scenariusz zdarzenia niekorzystnego stanowi problem decyzyjny, którego rozwiązaniem jest zbiór zabezpieczeń, jakie należy zastosować w celu minimalizacji lub eliminacji skutków zagrożeń. Do budowy i rozwiązania problemów decyzyjnych może posłużyć metoda analizy powiązanych obszarów decyzyjnych (ang. Analysis of Interconnected Decision Areas – AIDA), która zakłada realizację trzech zasadniczych etapów (Krupa, Ostrowska, 2012, s. 26):

- zbudowanie modelu problemu decyzyjnego:
  - wydzielenie obszarów decyzyjnych i ich elementarnych decyzji,
  - zaznaczenie par elementarnych decyzji będących w relacji pełnej sprzeczności,
  - wyznaczenie wag istotności Vi obszarów decyzyjnych Di na skali procentowej oraz wag istotności vji (kosztów do sumy 1 w każdym obszarze decyzyjnym Di) elementarnych decyzji dji na skali (0...1),
- wygenerowanie zbioru dopuszczalnych decyzji niezawierających par elementarnych decyzji znajdujących się w relacji pełnej sprzeczności,
- dokonanie wyboru i podjęcie decyzji:
  - przeprowadzenie oceny kosztowej wszystkich poprawnie utworzonych decyzji i uporządkowanie ich w malejącej kolejności kosztów,
  - analiza uzyskanych rozwiązań, wytypowanie grupy najbardziej pożądanych wariantów decyzji, dokonanie wyboru jednej z nich i wykonanie decyzji,
  - analiza skutków podjętej (wykonanej) decyzji.

W przypadku procesu PC problem decyzyjny to zbiór zagrożeń, na jakie zasób jest podatny. Występujące w problemie decyzyjnym obszary decyzyjne to pojedyncze zagrożenia, a decyzje elementarne w ramach obszarów decyzyjnych ilustrują dostępne środki reakcji na rozpoznane zagrożenie.

Relacje sprzeczności między decyzjami elementarnymi interpretuje się jako ograniczenie w zastosowaniu danej kombinacji zabezpieczeń. Ograniczenie to może wynikać np. z uwarunkowań technicznych, organizacyjnych, finansowych itp. Wygenerowane kombinacje decyzji elementarnych, uwzględniające relacje sprzeczności, stanowią zbiór zabezpieczeń przed rozpoznanymi zagrożeniami.

Opisując obszary decyzyjne prawdopodobieństwem wystąpienia zagrożenia, a decyzje elementarne np. kosztem wdrożenia zabezpieczenia, możliwe jest dokonanie oceny kosztowej wszystkich modeli zabezpieczeń. Pozwala to na ich uporządkowanie i podjęcie decyzji zgodnie z przyjętą funkcją celu.

W zależności od przyjętego parametru wartościującego decyzję elementarną, ocena kosztowa rozwiązania problemu decyzyjnego może być różnie interpretowana. Jeśli decyzje elementarne zostaną opisane parametrem odnoszącym się do kosztów wdrożenia zabezpieczenia, to możliwe jest poszukiwanie rozwiązania o najniższych kosztach. W przypadku opisania decyzji elementarnej parametrem opisującym ograniczenie ofiar wśród ludzi, możliwe jest poszukiwanie modelu zabezpieczeń, który zapewni najwyższy odsetek osób chronionych.

Przykład realizacji procedury budowy problemu decyzyjnego został przedstawiony w opracowaniu Concept of Situational Management of Safety Critical Infrastructure of State (Wiśniewski, 2016, s. 305-309).

4. Procedura weryfikacji zabezpieczeń

Realizacja funkcji kontroli jest zapewniana dzięki procedurze weryfikacji zabezpieczeń opracowanej na bazie metody analizy przypadków (ang. Case-based reasoning – CBR). Metoda CBR bazuje na obserwacji rozumowania eksperta, który szukając rozwiązania problemu, odwołuje się do doświadczeń z przeszłości i wzoruje swoje decyzje na wówczas podjętych. CBR określa przypadek jako parę <problem : rozwiązanie>. W przypadku PC przypadek rozumie się jako parę <zagrożenie : zabezpieczenie>.

Przypadki są niezależne, są zapisami rzeczywistych zdarzeń inicjowanymi w konkretnych sytuacjach, które mogą zostać opisane odpowiednim zestawem danych. Istota CBR sprowadza się do stwierdzenia, że możliwe jest rozwiązanie bieżącego problemu przez adaptację rozwiązań zastosowanych w przeszłości (Riesbeck, Schank, 1989, s. 32; Surma, 2010, s. 33). W metodzie wyróżnia się następujące etapy (Aamodt, Plaza, 1994, s. 47):

– wyszukanie – w bazie przypadków odnajduje się przypadek najbardziej podobny do rozpatrywanego,

- propozycja rozwiązania – sposób rozwiązania znalezionego przypadku staje się potencjalnym rozwiązaniem obecnego problemu,
- weryfikacja – znane rozwiązanie dopasowuje się do rozpatrywanego problemu,
- zapamiętanie – problem oraz rozwiązanie zapamiętuje się jako nowy przypadek.

Na potrzeby PC konieczne jest wprowadzenie kryteriów podobieństwa sytuacji, na podstawie których określany będzie stopień podobieństwa sytuacji zasobu (sytuacji bazowej) z przypadkami z przeszłości (tab. 1). Bazując na MSZ kryteriami podobieństwa mogą być:

- podobieństwo zasobów,
- podobieństwo funkcjonalności,
- podobieństwo zagrożeń,
- podobieństwo zabezpieczeń.

Na podstawie kryteriów podobieństwa w bazie zarejestrowanych przypadków wyszukiwane są sytuacje podobne. Następnie sprawdza się, jaka była skuteczność zastosowanych w przeszłości zabezpieczeń. Dzięki temu można przewidywać, czy zaproponowany zbiór zabezpieczeń będzie skutecznie chronił zasób przed zagrożeniami.

Podobieństwo zasobów (PW) określa się na podstawie zasobów występujących w dwóch porównywanych przypadkach. Podobieństwo określane jest na skali 0-100%, gdzie 0 oznacza brak wspólnych zasobów w rozpatrywanych sytuacjach, a 100 oznacza, że w obu sytuacjach występują dokładnie takie same zasoby.

Przykład ilustrujący określenie podobieństwa zasobów przedstawiono w tabeli 1. Sytuacja bazowa zawiera osiem zasobów od v1 do v8. W przypadku 1 podobieństwo wynosi PW = 0%, ponieważ nie występują zasoby zbieżne z przypadkiem bazowym. W przypadku 2 stopień podobieństwa wynosi PW = 100%, mimo że w przypadku występuje dodatkowy zasób v10. Dzieje się tak, ponieważ w procedurze weryfikacji zabezpieczeń do oceny stopnia podobieństwa brana jest pod uwagę tylko przestrzeń zasobów przypadku bazowego (oznaczona na szaro). W przypadku 3 stopień podobieństwa wynosi PW = 75% (zgodność 6 zasobów z przypadkiem bazowym). Ta sama logika określania stopnia podobieństwa jest stosowana dla pozostałych wskazanych kryteriów.

Tabela 1. Przykład określenia stopnia podobieństwa w obszarze kryterium zasobów

Wyszczególnienie	Podobieństwo	Zasoby											
	PW	v_1	v_2	v_3	v_4	v_5	v_6	v_7	v_8	v_9	v_{10}	v_{11}	v_{12}
Przypadek bazowy	100%	1	1	1	1	1	1	1	1	0	0	0	0
Przypadek 1	0%	0	0	0	0	0	0	0	0	1	1	1	1
Przypadek 2	100%	1	1	1	1	1	1	1	1	0	1	0	0
Przypadek 3	75%	1	1	1	1	1	1	0	0	0	0	1	0

Źródło: opracowanie własne

Realizacja omówionej procedury weryfikacji zabezpieczeń wymaga opracowania repozytorium, które będzie gromadziło dane o zdarzeniach niekorzystnych, mających miejsce w przeszłości, według struktury danych wyznaczonej przez MSZ.

5. Wymagania funkcjonalne

Zgodnie z definicją, wymagania funkcjonalne dotyczą tego, co ma być realizowane przez projektowane narzędzie informatyczne: jakie ma spełniać funkcje, jakich dostarczać usług, jak zachowywać się w określonych sytuacjach (Socha, 2010, s. 52). Zestaw wymagań funkcjonalnych, wynikający z omówionych procedur budowy scenariuszy zdarzeń niekorzystnych, budowy problemu decyzyjnego oraz weryfikacji zabezpieczeń, został przedstawiony w tabeli 2.

Tabela 2. Wykaz wymagań funkcjonalnych

Symbol	Opis funkcjonalności
Funkcjonalności wynikające z procedury budowy scenariuszy zdarzeń niekorzystnych	
FP1	odwzorowanie charakterystyki rozpatrywanego zasobu w konwencji MSZ, co oznacza możliwość opisania zasobu poprzez: • nazwę zasobu • realizowane funkcjonalności • zagrożenia, na które jest podatny • zabezpieczenia, jakie są stosowane na wypadek materializacji zagrożeń • inne kategorie danych wymagane przepisami prawa (zał. A)
FP2	odwzorowanie charakterystyki zagrożeń poprzez: • nazwę zagrożenia • określenie rodzaju zagrożenia • określenie typu zagrożenia • określenie skutku materializacji zagrożenia dla każdej funkcjonalności realizowanej przez rozpatrywany zasób • określenie prawdopodobieństwa materializacji zagrożenia • wykaz zabezpieczeń stosowanych w celu minimalizacji lub eliminacji skutków zagrożenia • wykaz zabezpieczeń jakie można zastosować w celu minimalizacji lub eliminacji skutków zagrożenia
FP3	odwzorowanie charakterystyki zabezpieczeń: • nazwa zabezpieczenia • możliwość stosowania przeciwko zagrożeniu • wpływ zabezpieczenia na podatność zasobu na zagrożenie • cel zarządzania kryzysowego
FP4	określenie zależności między zagrożeniami
FP5	wygenerowanie struktury sytuacji rozpatrywanego zasobu na podstawie modeli sytuacji analizowanych zasobów i danych dotyczących powiązań między zagrożeniami
FP6	wygenerowanie i zapis listy scenariuszy zdarzeń niekorzystnych
FP7	obliczenie wartości ryzyka dla scenariuszy zdarzeń niekorzystnych

cd. tab. 2

Symbol	Opis funkcjonalności
FP8	możliwość sortowania scenariuszy zdarzeń niekorzystnych według kryterium prawdopodobieństwa i wartości ryzyka
Funkcjonalności wynikające z procedury budowy problemu decyzyjnego	
FP9	możliwość utworzenia na podstawie MSZ lub na podstawie scenariusza zdarzenia niekorzystnego problemu decyzyjnego
FP10	możliwość automatycznego przekształcenia zbioru zagrożeń wynikającego z MSZ w zbiór obszarów decyzyjnych
FP11	możliwość ręcznego dodawania i usuwania obszarów decyzyjnych do utworzonego problemu decyzyjnego
FP12	możliwość tworzenia i usuwania poziomów decyzyjnych
FP13	możliwość dodawania i usuwania obszarów decyzyjnych do poziomu decyzyjnego
FP14	możliwość automatycznego generowania decyzji elementarnych dotyczących zabezpieczeń przed rozpoznanymi zagrożeniami na podstawie MSZ
FP15	możliwość ręcznego dodawania i usuwania decyzji elementarnych do obszarów decyzyjnych
FP16	możliwość określenia funkcji celu
FP17	możliwość przypisywania wartości obszarom decyzyjnym
FP18	możliwość przypisywania wartości decyzjom elementarnym
FP19	możliwość przypisywania wartości problemom decyzyjnym
FP20	możliwość oznaczenia par elementarnych decyzji sprzecznych
FP21	możliwość generowania decyzji rozwiązujących problem decyzyjny
FP22	przekształcanie decyzji rozwiązujących problem decyzyjny w równanie macierzowe
FP23	obliczenie wartości decyzji rozwiązujących problem decyzyjny
FP24	oznaczenie decyzji realizujących funkcję celu
FP25	prezentacja wyników w postaci wykresów
Funkcjonalności wynikające z procedury weryfikacji zabezpieczeń	
FP26	możliwość porównywania zbioru zasobów wyznaczonego przez model rozpatrywanej sytuacji zasobu lub scenariusz zdarzenia niekorzystnego ze zbiorami zasobów zarejestrowanych sytuacji przeszłych
FP27	możliwość porównywania zbioru funkcjonalności wyznaczonego przez model rozpatrywanej sytuacji zasobu lub scenariusz zdarzenia niekorzystnego ze zbiorami funkcjonalności zarejestrowanych sytuacji przeszłych
FP28	możliwość porównywania zbioru zagrożeń wyznaczonego przez model rozpatrywanej sytuacji zasobu lub scenariusz zdarzenia niekorzystnego ze zbiorami zagrożeń zarejestrowanych sytuacji przeszłych
FP29	możliwość porównywania zbioru zabezpieczeń wyznaczonego przez model rozpatrywanej sytuacji zasobu lub scenariusz zdarzenia niekorzystnego ze zbiorami zabezpieczeń zarejestrowanych sytuacji przeszłych
FP30	możliwość prezentacji stopni podobieństwa rozpatrywanych sytuacji przeszłych z sytuacją bazową dla zdefiniowanych kryteriów podobieństwa

Źródło: opracowanie własne

W tabeli 3 przedstawiono przypisanie poszczególnych funkcjonalności do wymaganych elementów PZK i POIK, powstających w wyniku planowania cywilnego.

Tabela 3. Zestawienie elementów PZK i POIK z realizującymi je funkcjonalnościami narzędzia informatycznego

Wyszczególnienie			
Elementy PZK	Symbol wymagania funkcjonalnego	Elementy POIK	Symbol wymagania funkcjonalnego
Plan główny zawierający: • charakterystykę zagrożeń oraz ocenę ryzyka ich wystąpienia, w tym dotyczących IK, oraz mapy ryzyka i mapy zagrożeń, • zadania i obowiązki uczestników zarządzania kryzysowego w formie siatki bezpieczeństwa, • zestawienie sił i środków do wykorzystania w sytuacjach kryzysowych, • zadania określone planami działań krótkoterminowych, o których mowa w art. 92 ustawy z dnia 27 kwietnia 2001 r. – Prawo ochrony środowiska.	FP1-FP8	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 i siedziba, 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.	FP1
Zespół przedsięwzięć na wypadek sytuacji kryzysowych, a w tym: • zadania w zakresie monitorowania zagrożeń, • tryb uruchamiania niezbędnych sił i środków, uczestniczących w realizacji planowanych przedsięwzięć na wypadek sytuacji kryzysowej, • procedury reagowania kryzysowego, określające sposób postępowania w sytuacjach kryzysowych, • współdziałanie między siłami, o których mowa w lit. b.	FP9-FP25	Dane IK: • charakterystykę i podstawowe parametry techniczne, • plan (mapę) z naniesieniem lokalizacji obiektów, instalacji lub systemu, • połączenia z innymi obiektami, instalacjami, urządzeniami lub usługami.	FP1
		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.	FP2-FP8

cd. tab. 3

<table>
<tr><th colspan="4">Wyszczególnienie</th></tr>
<tr><th>Elementy PZK</th><th>Symbol wymagania funkcjonalnego</th><th>Elementy POIK</th><th>Symbol wymagania funkcjonalnego</th></tr>
<tr><td rowspan="2">Załączniki funkcjonalne planu głównego określające:
• procedury realizacji zadań z zakresu zarządzania kryzysowego, w tym związane z ochroną IK,
• organizację łączności,
• organizację systemu monitorowania zagrożeń, ostrzegania i alarmowania,
• zasady informowania ludności o zagrożeniach i sposobach postępowania na wypadek zagrożeń,
• organizację ewakuacji z obszarów zagrożonych,
• organizację ratownictwa, opieki medycznej, pomocy społecznej oraz pomocy psychologicznej,
• organizację ochrony przed zagrożeniami charakterystycznymi dla danego obszaru,
• wykaz zawartych umów i porozumień związanych z realizacją zadań zawartych w planie zarządzania kryzysowego,
• zasady oraz tryb oceniania i dokumentowania szkód,
• procedury uruchamiania rezerw państwowych,
• wykaz IK znajdującej się odpowiednio na terenie województwa, powiatu lub gminy, objętej planem zarządzania kryzysowego,
• priorytety w zakresie ochrony oraz odtwarzania IK.</td><td rowspan="2">FP26-FP30</td><td>Zasadnicze warianty:
• działania w sytuacji zagrożenia lub zakłócenia funkcjonowania IK,
• zapewnienia ciągłości funkcjonowania IK,
• odtwarzania IK.</td><td>FP6, FP9-FP25</td></tr>
<tr><td>Zasady współpracy z właściwymi miejscowo:
• centrami zarządzania kryzysowego,
• organami administracji publicznej.</td><td>FP26-FP30</td></tr>
</table>

Źródło: opracowanie własne na podstawie Dz.U. 2017 poz. 209, art. 5, pkt 2 i Dz.U. 2010 nr 83 poz. 542, § 2, ust. 3

Podsumowanie

Artykuł stanowi opis koncepcji budowy narzędzia informatycznego wspomagającego: generowanie scenariuszy zdarzeń niekorzystnych, podejmowanie decyzji dotyczących zabezpieczeń przed rozpoznanymi zagrożeniami oraz weryfikację skuteczności zaproponowanych zabezpieczeń.

Przedstawiono w nim koncepcję integracji działań związanych z bezpieczeństwem rozpatrywanego obiektu od momentu rozpoznania zagrożeń, na które jest podatny, poprzez opracowanie prognozy rozwoju zagrożeń, do zaproponowania zabezpieczeń przed rozpoznanymi zagrożeniami i weryfikacji ich skuteczności. Ponadto wskazano wymagania funkcjonalne oraz koncepcję budowy narzędzia informatycznego wspomagającego generowanie scenariuszy zdarzeń niekorzystnych, podejmowanie decyzji dotyczących zabezpieczeń przed rozpoznanymi zagrożeniami oraz weryfikację zaproponowanych zabezpieczeń.

Zaprezentowana koncepcja narzędzia informatycznego stanowi perspektywę dalszego rozwoju powstającej wysokospecjalistycznej platformy wspomagającej PC i ratownictwo w administracji publicznej RP oraz jednostkach organizacyjnych KSRG.

BIBLIOGRAFIA

[1] Aamodt A., Plaza E., 1994, *Case-Based Reasoning: Foundational Issues, Methodological Variations and System Approaches Artificial Intelligence Communications*, 7(1), pp. 39-59.

[2] Krupa T., 2013, *V.A. Gorbatov Theory of Characterization – Solutions and Examples Foundations of Management*, Vol. 5, No. 3, pp. 89-102.

[3] Krupa T., 2015, *Semiotyka kluczowych pojęć tezaurusa ciągłości działania w infrastrukturze krytycznej*, „Logistyka", nr 4, s. 7793-7802.

[4] Krupa T., Ostrowska T., 2012, *Decision – Making in Flat and Hierarchical Decision Problems Foundations of Management*, Vol. 4, No. 2, pp. 23-36.

[5] Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie planów ochrony infrastruktury krytycznej (Dz.U. 2010 nr 83 poz. 542).

[6] Riesbeck C., Schank R., 1989, *Inside Case-Based Reasoning*, New Jersey: Hillsdale.

[7] Socha K., 2010, *Inżynieria oprogramowania*, PWN, Warszawa.

[8] Surma J., 2010, *Rola analogii w podejmowaniu decyzji w zarządzaniu strategicznym małych i średnich przedsiębiorstw*, Oficyna Wydawnicza SGH, Warszawa.

[9] Ustawa z dnia 26 kwietnia 2007 roku o zarządzaniu kryzysowym (Dz.U. 2017 poz. 209).

[10] Wiśniewski M., 2016, *Concept of Situational Management of Safety Critical Infrastructure of State Foundation of Management*, Vol. 8, annual 2016, pp. 297-310.

[11] Wiśniewski M., 2017, *Weryfikacja stosowalności zasad budowy scenariuszy zdarzeń niekorzystnych – raport z badań*, Studia i Materiały "Miscellanea Oeconomicae", 4/2017, UJK.

[12] Wiśniewski M., Kisilowski M., Marczewski M., 2016, *Zasady budowy scenariuszy zdarzeń niekorzystnych w publicznym zarządzaniu kryzysowym*, [w:] M. Ćwiklicki, M. Jabłoński, S. Mazur (red.), *Współczesne koncepcje zarządzania publicznego. Wyzwania modernizacyjne sektora publicznego*, Fundacja GAP, Kraków, s. 97-110.