ZESZYTY NAUKOWE WSOWL

Nr 4 (162) 2011 ISSN 1731-8157

Dariusz BECMER[*]
Dariusz SKORUPKA[**]

ZARZĄDZANIE RYZYKIEM W ORGANIZACJI MILITARNEJ WEDŁUG POGLĄDÓW AMERYKAŃSKICH

Autorzy w swym opracowaniu omawiają metodę zarządzania ryzykiem stosowaną w procesie podejmowania decyzji oraz podczas przygotowania i realizacji działań przez dowódców różnych szczebli armii Stanów Zjednoczonych. Metoda ta jest stosowana zarówno w działaniach militarnych i niemilitarnych, jak również w szkoleniu, w bieżącej działalności służbowej i pozasłużbowej. Ma ona na celu zredukowanie lub całkowite wyeliminowanie ryzyka związanego z występowaniem różnorodnych zagrożeń w wymienionych działaniach.

Słowa kluczowe: *zarządzanie ryzykiem, ryzyko, decyzje, podejmowanie decyzji, Kompleksowe Zarządzanie Ryzykiem, wojsko – Stany Zjednoczone*

WSTĘP

Podstawowym elementem procesu zarządzania ryzykiem, dotyczącego wszelkich form aktywności, jest zapewnienie bezpieczeństwa realizowanych przedsięwzięć. Jest to istotne nie tylko w działalności gospodarczej, ale także organizacji społeczeństw, funkcjonowania samorządów i innych instytucji, a w tym m.in. działalności sił zbrojnych, policji, szpitali czy szkół. Wraz z postępem globalizacji oraz wzrostem ilości zagrożeń, a wśród nich dużym natężeniem klęsk żywiołowych i katastrof naturalnych, którym towarzyszą coraz bardziej nasilające się zmiany klimatyczne, a także bardzo groźnego zjawiska międzynarodowego terroryzmu, ujawniają się nowe rodzaje ryzyka, które praktycznie dotykają każdą organizację.

Zarządzanie ryzykiem to technika zarządcza, do której przekonuje się obecnie coraz więcej organizacji. Jest to temat nośny, dlatego też ukazało się już wiele podręczników dotyczących tej techniki [1, 2, 6, 9, 19, 21]. Co więcej, w Polsce organizacje sek-

[*] mjr mgr inż. Dariusz BECMER – Instytut Dowodzenia Wyższej Szkoły Oficerskiej Wojsk Lądowych

[**] płk dr hab. inż. Dariusz SKORUPKA, prof. nadzw. WSOWL – Wydział Zarządzania Wyższej Szkoły Oficerskiej Wojsk Lądowych

tora publicznego od niedawna zobowiązane są do stosowania zaawansowanych technik zarządczych, w tym zarządzania ryzykiem. Organizacje sektora publicznego zaczynają więc wdrażać systemy zintegrowanego zarządzania ryzykiem. Jednak z obserwacji ich wysiłków w tym zakresie wynika, że nie jest to łatwe zadanie. Badanie przeprowadzone przez firmę JDS Consulting, opisane w opracowaniu K. M. Klimczaka [7], dotyczące doświadczeń jednostek związanych z próbami wdrażania zarządzania ryzykiem wykazało, że większość respondentów nie prowadziła zarządzania ryzykiem lub czyniła to w niewielkim stopniu.

W Siłach Zbrojnych RP podczas realizacji przedsięwzięć procesu dowodzenia nie występuje taki element, jak ocena ryzyka. Wprawdzie rozpatruje się zagrożenia związane z działaniem przeciwnika, szeroko pojętym środowiskiem i innymi czynnikami mogącymi ujemnie wpływać na działania wojsk własnych, ale rozważania te mają bardziej charakter orientacyjny, bez rzetelnej oceny prawdopodobieństwa oraz skutków ich wystąpienia [12, 17]. Tymczasem analiza i ocena wymienionych czynników, wzbogacona o możliwość oceny skutków wystąpienia zagrożeń wpływających na osiągnięcie celu końcowego mogłaby pozwolić na dokładniejszą weryfikację opracowanych wariantów działania.

W literaturze przedmiotu wprawdzie wspomina się o możliwościach zastosowania techniki zarządzania ryzykiem w niektórych obszarach działalności organizacji militarnych, jak również proponuje się pewne rozwiązania metody oceny ryzyka, jednakże nie wychodzą one poza prezentacje przedstawione w określonych opracowaniach [13, 16].

Analizując metody identyfikacji ryzyka oraz zarządzania nim, z punktu widzenia zastosowań w wojsku, można stwierdzić, że są one najbardziej popularne w armii amerykańskiej. Amerykanie wykorzystują procedury zarządzania ryzykiem praktycznie na każdym szczeblu dowodzenia. Do bardziej znanych należy procedura opisana pierwotnie w regulaminie *FM 100-14, Risk Management* [4], w którym opisano genezę zarządzania ryzykiem, elementy procesu zarządzania ryzykiem oraz możliwość implementacji procedury zarządzania ryzykiem w procesie decyzyjnym. W kolejnym, poprawionym, wydaniu tego regulaminu *FM 5-19, Composite Risk Management* [5] proponowane jest nowe podejście do zarządzania ryzykiem, które swym zakresem obejmuje nie tylko szkolenie bojowe oraz wszelkiego rodzaju działania taktyczne i operacje, ale również działania niemilitarne, a także aktywność pozasłużbową. Wymienione instrukcje nie są jedynymi poświęconymi problematyce zarządzania ryzykiem [15], ponieważ praktycznie w większości obecnie wydawanych regulaminach w armii Stanów Zjednoczonych, dotyczących określonych działań, istnieje rozdział poświęcony zarządzaniu ryzykiem. Ocenę ryzyka realizuje się także w oddziałach wsparcia armii amerykańskiej[1].

Kompleksowe Zarządzanie Ryzykiem (ang. *Composite Risk Management* – CRM) jest metodą stosowaną w Armii Stanów Zjednoczonych i jednocześnie podstawowym elementem procesu podejmowania decyzji służącym do identyfikacji zagrożeń oraz kontroli związanego z nimi ryzyka w całym spektrum działań i przedsięwzięć re-

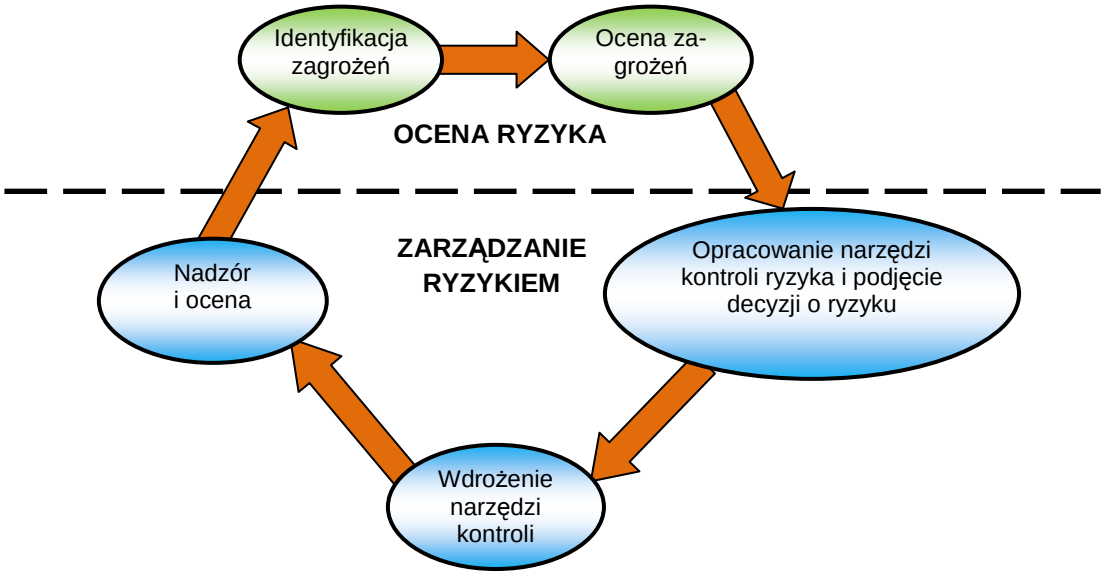
[1] Przykładowo amerykańskie wojska inżynieryjne (*The US Army Corps of Engineers -USACE*) rozwijają metodę oceny ryzyka zwaną *Component Level Risk Assessment Methodology* dla potrzeb budowy i eksploatacji mostów.

alizowanych przez Armię USA. Głównym celem stosowania procesu CRM jest redukowanie poziomu ryzyka dotyczącego wszystkich zagrożeń, które mogą powodować obrażenia lub śmierć personelu, uszkodzenie lub zniszczenie uzbrojenia i sprzętu wojskowego oraz mogą ujemnie wpłynąć na efektywność realizowanej misji [5].

CRM jest procesem złożonym z pięciu następujących etapów (rys. 1):

1. Identyfikacja zagrożeń.
2. Ocena zagrożeń.
3. Opracowanie narzędzi kontroli ryzyka[2] i podjęcie decyzji o ryzyku.
4. Wdrożenie narzędzi kontroli ryzyka.
5. Nadzór i ocena [4, 5].

Etap pierwszy i drugi są etapami oceny ryzyka, etapy od trzeciego do piątego są elementami zarządzania ryzykiem.



Rys. 1. Proces CRM

Źródło: Opracowanie własne na podstawie Field Manual 5-19 (100-14), Composite Risk Management, Department of the Army, Washington 2006, s. 1-4

W kolejnych zagadnieniach autorzy przedstawią szczegółowo poszczególne etapy procesu CRM.

1. IDENTYFIKACJA ZAGROŻEŃ

Zagrożenie, według regulaminu armii amerykańskiej to okoliczność, sytuacja, zdarzenie lub czynnik mogące powodować obrażenia, choroby oraz śmierć personelu, uszkodzenie lub utratę wyposażenia, uzbrojenia lub innego mienia, jak również utrata zdolności bojowej, porażka lub niewykonanie zadania [3, 5]. Zagrożenia dotyczą różnych form działalności armii: działań bojowych, operacji stabilizacyjnych, zabezpieczenia baz, szkolenia, działalności służbowej (w garnizonie) i działalności pozasłużbowej.

[2] Narzędzia kontroli ryzyka – działania podjęte w celu wyeliminowania zagrożeń lub zredukowania ryzyka z nimi związanymi.

W metodzie CRM identyfikacja zagrożeń polega na poszukiwaniu ich w obszarach powiązanych z takimi czynnikami, jak: misja (zadanie), przeciwnik, teren i pogoda (środowisko), wojska własne i wspierające, czas, aspekt cywilny (METT-TC)[3]. Czynniki te są związane z podstawowym, bojowym przeznaczeniem armii, ale w podobny sposób rozpatruje się ryzyko występujące podczas realizacji zadań niemilitarnych. Różnica polega na tym, że w tym przypadku rozpatrywane są zagrożenia związane z następującymi czynnikami: przedsięwzięcie, zakłócenia, teren i pogoda (środowisko), ludzie, czas i aspekt prawny (rys. 2)[4].

Rys. 2. Czynniki-źródła zagrożeń i ryzyka

Źródło: FM 5-19 (100-14), Composite Risk Management, Department of the Army, Washington 2006, s. 1-4

Zadanie (mission)

Zadania w zależności od charakteru misji bojowej mogą być mniej lub bardziej niebezpieczne. Rozpatrując ten aspekt, dowódca powinien poszukiwać zagrożeń wynikających ze złożoności zadania lub stopnia skomplikowania planów działania i rozkazów przełożonych, np. szczególnie skomplikowanego schematu manewru. Sposób lub forma postawienia zadania również może powodować pewne zagrożenia, np. wydanie wstępnego zarządzenia bojowego zamiast szczegółowo opracowanego, kompletnego rozkazu bojowego wraz ze wszystkimi załącznikami zwiększa ryzyko niewłaściwego zrozumienia zamiaru przełożonego [5].

Przedsięwzięcie (activity)

Ten czynnik dotyczy bieżącej działalności służbowej w jednostce oraz działalności pozasłużbowej. Identyfikacja i ocena ryzyka może być prowadzona podczas pla-

[3] METT-TC: ang.: Mission, Enemy, Terrain And Weather, Troops And Support Available, Time Available, And Civil Considerations.

[4] ang.: Activity, Disrupters, Terrain And Weather, People, Time, Legal.

nowania przedsięwzięć dla podwładnych w ramach długiego wolnego weekendu, który może być spędzany w formie rekreacji, wydarzenia sportowego, wyjazdu, przepustki lub też pełnienia służby. Istotną rolę pełnią w tym przypadku dowódcy niższych szczebli dowodzenia, którzy są odpowiedzialni za dokonywanie ocen indywidualnych cech charakteru poszczególnych podwładnych. Szczególnej uwagi wymagają wydarzenia, podczas których będzie spożywany alkohol lub będzie możliwość przyjmowania innych używek [5].

Przeciwnik (Enemy)

Informacyjne przygotowanie pola walki (ang. *Intelligence preparation of the battlefield* - IPB), jako dynamiczny element procesu podejmowania decyzji, jest istotne dla zidentyfikowania zagrożeń, których źródłem jest przeciwnik. Oceniając przeciwnika, rozważa się elementy mogące stanowić zagrożenie dla operacji lub zadania. Zalicza się do nich: jego położenie, skład i możliwości bojowe oraz przewidywany sposób działania. W ramach tej oceny poszukuje się odpowiedzi na pytanie: *co przeciwnik może zrobić, aby udaremnić działanie mojego oddziału?*, czyli dąży się do ustalenia najbardziej prawdopodobnego lub najgroźniejszego w danej sytuacji sposobu jego działania. IPB jest narzędziem wspierającym ocenę zagrożeń, będącą podstawą oceny ryzyka, poprzez identyfikację szans i ograniczeń, które tworzy środowisko pola walki zarówno dla przeciwnika, jak i wojsk własnych. Jednocześnie jest narzędziem odzwierciedlającym możliwości i słabości przeciwnika [5].

Zakłócenia (Disrupters)

Przez zakłócenia rozumie się czynniki będące odpowiednikiem przeciwnika w walce zbrojnej, ale rozpatrywane w aspekcie działalności służbowej w jednostce lub działań niemilitarnych, a ujmowane jako zewnętrzne działanie, mające ujemny wpływ na planowane przedsięwzięcie lub działanie [5].

Teren i warunki atmosferyczne (Terrain and Weather)

Oceniając teren, w celu zidentyfikowania i oceny zagrożeń mających wpływ na sposób wykonania zadania, dokonuje się analizy następujących elementów:

- warunków prowadzenia obserwacji i ognia *(observation and fields of fire)*;
- pokrycia terenu i warunków maskowania *(cover and concealment)*;
- przeszkód terenowych naturalnych i sztucznych *(obstacles)*;
- terenu kluczowego i o decydującym znaczeniu *(key and decisive terrain)*;
- dróg podejścia *(avenues of approach)* [5].

Powszechne zagrożenia związane z terenem wynikają z takich parametrów, jak: wysokość nad poziomem morza, niski pułap chmur, nawierzchnia dróg, nierówności terenowe, stopień pochylenia oraz pojemność terenu. Zagrożenia związane z warunkami atmosferycznymi dotyczą takich kategorii, jak: zimno, pokrywa lodu, śnieg, deszcz, mgła, ciepło, wilgotność, wiatr, widoczność i oświetlenie. Warunki atmosferyczne mogą również kreować specyficzne zagrożenia [5].

Podczas rozpatrywania zagrożeń wynikających ze specyfiki środowiska w działaniach niemilitarnych bierze się pod uwagę te same parametry.

Wojska własne (ludzie)i dostępne wsparcie (Troops (or People) and Equipment)

W odniesieniu do oceny ryzyka podczas działań bojowych z pojęciem wojska własne wiąże się rozważenie takich czynników, jak: poziom wyszkolenia, stopień ukompletowania obsady etatowej stanowisk, utrzymanie i stan techniczny uzbrojenia, sprzętu i wyposażenia. Ponadto rozpatruje się również morale, dostęp do zaopatrzenia i zapasów środków bojowych i materiałowych, dostęp do służb zabezpieczających działania taktyczne wojsk, łącznie z medycznymi [5].

W odniesieniu do działań niebojowych termin „ludzie" obejmuje żołnierzy, ich podwładnych, pracowników cywilnych oraz innych związanych lub nie z podejmowanym działaniem. Zagrożenia, które mogą być brane pod uwagę to m.in. napaść na tle seksualnym, przemoc w rodzinie, nadużywanie środków odurzających, choroby przenoszone drogą płciową oraz inne zagrożenia medyczne lub związane z postępowaniem ludzi [5].

Czas (time)

Ilość czasu dostępnego na przygotowanie misji ma kluczowe znaczenie, gdyż jego niedobór często zmusza dowódców do zaakceptowania większego poziomu ryzyka podczas planowania, przygotowania i realizacji działania. Aby uniknąć lub zmniejszyć poziom ryzyka w warunkach ograniczonego czasu przeznaczonego na planowanie, dowódcy powinni działać zgodnie z zasadą 1/3 czasu dla mnie, 2/3 dla podwładnych, co oznacza, że w tak kalkulowanym czasie po upływie jego 1/3 części powinien być wydany rozkaz bojowy. Pozostałe 2/3 jest przeznaczone na planowanie i organizowanie działań przez podwładnych oraz jednocześnie jest czasem, w którym następuje faza kontroli polegająca na monitorowaniu sytuacji w podległych pododdziałach i reagowaniu w przypadku występowania problemów[5].

W działaniach niebojowych ograniczony czas jest częściej kwestią pośpiechu niż możliwości dysponowania nim. Przykładem może być okres długiego weekendu, gdzie celem młodych żołnierzy jest szybkie dotarcie do domu nawet kosztem dostatecznego odpoczynku. Szczególnego znaczenia nabiera ten czynnik wtedy, gdy taki zmęczony żołnierz jest kierowcą samochodu, którym powraca do domu [5].

Aspekt cywilny lub prawny (Civil or Legal Considerations)

W omawianym aspekcie obszar rozważań obejmuje ryzyko wystąpienia strat, wśród populacji cywilnej oraz wojskowego personelu niewalczącego podczas wykonywania zadania w rejonie prowadzonej operacji. Powszechnym trendem jest dążenie do ich ograniczania. Zagrożenia dotyczące tego czynnika są związane z obecnością określonej społeczności w rejonie prowadzonych działań oraz z intensywnością ruchu jej członków. Duże nasilenie ruchu mieszkańców może powodować zagrożenia dla przemieszczających się kolumn oraz zaplanowanych manewrów taktycznych. Podczas oceny zagrożeń należy rozważyć także takie elementy, jak partyzanci, możliwość wystąpienia zamieszek oraz działalność kryminalną [5].

W działaniach niebojowych w ramach aspektu prawnego pod uwagę bierze się względy prawne oraz polityczne, które mogą wpływać na pożądany lub ograniczony sposób działania lidera grupy lub innych ludzi.

Zgodnie z literaturą [5] podczas identyfikacji zagrożeń można wykorzystywać następujące źródła i narzędzia:

- doświadczenie własne oraz innych ekspertów;
- regulaminy, podręczniki, standardowe procedury działania, teorię sztuki wojennej;
- dane dotyczące wypadków, które wydarzyły się w przeszłości;
- gry wojenne (rozpatrywane według scenariusza akcja-reakcja);
- macierze oceny ryzyka;
- ocena gotowości bojowej;
- diagramy przyczyn i efektów;
- analizy zmian;
- analizy ścieżek i barier przepływu energii;
- diagramy logiczne;
- techniki mapowania;
- ocenę wyszkolenia;
- przegląd działania (ang. *After-action reviews*-AARs) [5].

Zagrożenia mogą pojawiać się w wielu obszarach. Mogą być związane z działalnością przeciwnika, możliwością wystąpienia wypadków, warunkami atmosferycznymi i środowiska, zdrowiem, warunkami sanitarnymi, działaniem uzbrojenia i wyposażenia. Straty w ludziach, wyposażeniu, sprzęcie lub środkach bojowych wywołane przez jakiekolwiek zagrożenie mają destrukcyjny wpływ na gotowość i możliwości wykonania zadania niezależnie od źródła. Jednostka (żołnierz, człowiek) ma większy wpływ na wywołanie zmian związanych z zagrożeniami wynikającymi z przestrzegania pewnych zasad, możliwości wypadków, działaniem uzbrojenia i wyposażenia niż tych związanych z działaniem przeciwnika [5].

2. OCENA ZAGROŻEŃ

W etapie tym używa się liczb i zestawień oraz wykresów, aby przedstawić metodologię zmierzającą do oceny prawdopodobieństwa oraz stopnia trudności w osiągnięciu właściwego poziomu ryzyka. Należy jednak pamiętać, że matematyczny opis i tabele mają wspierać dowódcę, ale nie powinny być decydującym elementem podczas podejmowania decyzji. Jest to narzędzie, które nie powinno wykluczać kompetentnych decyzji, bazujących na doświadczeniu bojowym.

Poziom ryzyka jest określany na podstawie oszacowania prawdopodobieństwa wystąpienia danego zagrożenia oraz konsekwencji (dotkliwości) i wpływu na funkcjonowanie pododdziału (oddziału), jeżeli takie zagrożenie wystąpi. Oceny te w większości przypadków są oparte na doświadczeniach członków sztabu z działań prowadzonych w przeszłości oraz doświadczeń zbieranych w ramach tzw. *Lesson learned.* W etapie tym poszukuje się odpowiedzi na pytanie: *Jakie jest prawdopodobieństwo wystąpienia niesprzyjającego zdarzenia i jakie będą jego konsekwencje, jeśli to zdarzenie wystąpi?* [5].

Zagrożenia i związane z nimi ryzyko są rozpatrywane w ramach procesu podejmowania decyzji oraz podczas przygotowania (w tym synchronizacji) i realizacji działań (rys. 3). Końcowym rezultatem analiz jest wstępne oszacowanie ryzyka w odniesie-

niu do każdego zidentyfikowanego zagrożenia w kategoriach: ekstremalnie wysokie (ang. *extremely high*), wysokie (*high*), umiarkowane (*moderate*), niskie (*low*) (tabela 1).

Etap ten polega na wykonaniu trzech następujących czynności:

– ocena prawdopodobieństwa wystąpienia niesprzyjającego zdarzenia;
– oszacowanie wagi konsekwencji, jakie mogą nastąpić w rezultacie wystąpienia zdarzenia;
– określenie poziomu ryzyka dla danego prawdopodobieństwa i wagi konsekwencji przy użyciu standardowej tabeli oceny ryzyka [5].

Proces podejmowania decyzji (MDMP) i proces zarządzania ryzykiem w amerykańskiej organizacji militarnej

Proces podejmowania decyzji (MDMP)	Proces zarządzania ryzykiem				
	1.Identyfikacja zagrożeń	2.Ocena zagrożeń	3.Opracowanie narzędzi kontroli ryzyka i podjęcie decyzji o ryzyku	4.Wdrożenie narzędzi kontroli ryzyka	5.Nadzór i ocena
Etap 1: Otrzymanie zadania	X				
Etap 2: Analiza zadania	X	X			
Etap 3: Opracowanie wariantów działania	X	X	X		
Etap 4: Rozważenie wariantów działania (Gra wojenna)	X	X	X		
Etap 5: Porównanie wariantów działania			X		
Etap 6: Wybór wariantu działania - decyzja			X		
Etap 7: Opracowanie rozkazu (bojowego)			X	X	
Przygotowanie	X	X	X	X	X
Realizacja zadania	X	X	X	X	X

Rys. 3. Przebieg procesu CRM podczas procesu podejmowania decyzji

Źródło: Opracowanie własne na podstawie Field Manual No. 5-19 (100-14), Composite Risk Management, Department of the Army, Washington 2006

Tabela 1. Ocena ryzyka w amerykańskiej organizacji militarnej

MACIERZ OCENY RYZYKA						
Dotkliwość – Skutki oddziaływania		Prawdopodobieństwo				
		Częste	Prawdopodobne	Sporadyczne	Rzadkie	Małoprawdopodobne
		A	B	C	D	E
Katastrofalne	I	E	E	H	H	M
Krytyczne	II	E	H	H	M	L
Marginalne	III	H	M	M	L	L
Nieistotne	IV	M	L	L	L	L
E - Ekstremalnie wysokie ryzyko **H** - Wysokie ryzyko **M** - Umiarkowane ryzyko **L** - Niskie ryzyko						

Źródło: Opracowanie własne na podstawie Field Manual No. 5-19 (100-14), Composite Risk Management, Department of the Army, Washington 2006

2.1. Ocena prawdopodobieństwa wystąpienia niesprzyjającego zdarzenia

Prawdopodobieństwo jest rozumiane jako możliwość wystąpienia zdarzenia. Ocena jest dokonywana na podstawie informacji i doświadczenia, które posiada dowódca i sztab. Poziom prawdopodobieństwa dla każdego z zagrożeń jest określany w zależności od zadania, opracowanych wariantów działania lub częstotliwości występowania podobnych zdarzeń.

Dla celów metody CRM przyjęto następujące kategorie prawdopodobieństwa:

- częste *(frequent)* – zagrożenie występuje bardzo często, wręcz regularnie; jeśli np. stwierdzono około 500 podobnych sytuacji, w których wystąpiło nieprzyjemne zdarzenie, można oczekiwać, że w podobnym działaniu na pewno się wydarzy (do takich zdarzeń można zaliczyć dachowanie samochodu, kolizje w postaci najechania na siebie samochodów, urazy, otarcia będące wynikiem prowadzenia treningu fizycznego podczas upałów lub z niezaaklimatyzowanymi żołnierzami) [5];
- prawdopodobne *(likely)* – zagrożenie występuje wielokrotnie, powszechnie; dla przykładu, jeśli ujawniono około 100 przypadków ekspozycji na określone zagrożenie bez odpowiednich działań eliminujących zagrożenie lub redukujących ryzyko, można oczekiwać, że takie zagrożenie wydarzy się (zaliczyć do nich można prowizoryczne urządzenia wybuchowe, zaczepienie o linię wysokiego napięcia przez samolot, nieumyślne rozładowanie broni poprzez wystrzał) [5];
- sporadyczne *(occasional)* – sytuacje zagrożenia występują sporadycznie, ale nie są powszechne (zaliczyć można do nich niewypały i niewybuchy oraz straty powodowane przez ogień wojsk własnych – ang. *fratricide*) [5];
- rzadkie *(seldom)* – wystąpienie groźnych sytuacji jest możliwe w najmniejszym stopniu (np. śmierć w wyniku upału) [5];
- mało prawdopodobne *(unlikely)* – można założyć, że sytuacja groźna nie wystąpi, ale nie jest to niemożliwe (np. detonacja amunicji podczas transportu) [5].

2.2. Oszacowanie oczekiwanych rezultatów lub dotkliwości konsekwencji wystąpienia zdarzenia

Dotkliwość wyrażana w stopniach określa rozmiar skutków zdarzenia, które może ujemnie wpłynąć na zdolność bojową lub możliwość wykonania zadania. Stopień dotkliwości oszacowany dla każdego z zagrożeń bazuje na znajomości rezultatów podobnych zdarzeń z przeszłości. Zgodnie z literaturą [5] podczas wypełniania arkusza oceny ryzyka wskazuje się następujące poziomy dotkliwości:

a) katastrofalne *(catastrophic)* [5]:
   - całkowita klęska misji (zadania) lub utrata poziomu zdolności niezbędnego do ukończenia misji (zadania);
   - śmierć lub trwały ogólny brak zdolności do działań;
   - utrata głównych lub decydujących o wykonaniu misji systemów walki lub elementów sprzętu i uzbrojenia;
   - dewastacja głównych lub pomocniczych obiektów, nieruchomości *(facility)*;

- poważne zniszczenia środowiska;
- zdecydowany brak ochrony (bezpieczeństwa) misji;
- nieakceptowanie straty wśród ludności cywilnej;

b) krytyczne *(critical)* [5]:
- dotkliwie obniżona zdolność bojowa pododdziałów lub obniżone możliwości wykonania misji (zadania);
- trwały częściowy brak zdolności lub tymczasowy (okresowy) całkowity brak zdolności (przekraczający 3 miesiące);
- rozległe poważne uszkodzenia wyposażenia i systemów;
- znaczące zniszczenia obiektów i środowiska;
- brak ochrony (bezpieczeństwa) misji;
- znaczące straty wśród ludności cywilnej;

c) marginalne *(marginal)* [5]:
- obniżone możliwości wykonania misji (zadania) lub zdolności bojowej pododdziałów;
- nieznaczne uszkodzenia sprzętu i systemów, obiektów, lub środowiska;
- wykluczenie z walki z powodu obrażeń i chorób nieprzekraczające okresu trzech miesięcy;

d) nieistotne *(negligible)* [5]:
- mały lub brak wpływu działania przeciwnika na możliwości wykonania misji;
- obrażenia z poziomu pierwszej pomocy lub wymagające nieznacznej kuracji;
- drobne uszkodzenia sprzętu i systemów, nieograniczające ich funkcjonalności i obsługiwalności;
- drobne lub brak zniszczeń obiektów lub środowiska.

2.3. Określenie wyspecyfikowanego poziomu ryzyka

Prawdopodobieństwo i dotkliwość konsekwencji każdego ze zidentyfikowanych zagrożeń, przy użyciu tabeli oceny ryzyka (tabela 1), są przetransferowane w konkretny poziom ryzyka, przy czym należy pamiętać, że tabela przedstawia tylko ocenę ryzyka, ale nie należy jej traktować jako niepodważalnego pewnika. Może być wskaźnikiem względnego zagrożenia danej operacji lub innego przedsięwzięcia. Poziomy ryzyka wyspecyfikowane u dołu tabeli, zgodnie z literaturą [5] są rozumiane w sposób przedstawiony następująco:

- ekstremalnie wysokie ryzyko *(extremely high risk)* – utrata zdolności do wypełnienia misji, w przypadku wystąpienia zagrożenia podczas jej prowadzenia; ten poziom ryzyka wskazuje, że ryzyko związane z daną misją, aktywnością lub przedsięwzięciem pozasłużbowym może stanowić dotkliwe konsekwencje dotyczące nie tylko danej misji lub przedsięwzięcia, a decyzja o kontynuowaniu musi być rozważona szczególnie w aspekcie możliwości osiągnięcia ewentualnych korzyści w przypadku jej kontynuowania; dotyczy *częstego* lub *prawdopodobnego* prawdopodobieństwa wystąpienia *katastrofal-*

nych skutków (IA i IB) lub *częstego* prawdopodobieństwa wystąpienia *krytycznych* konsekwencji (IIA) [5];

- wysokie ryzyko *(high risk)* – znaczne obniżenie możliwości wypełnienia misji w kategoriach utrzymania pożądanych standardów zadania, zdolności do wypełnienia wszystkich etapów misji lub zdolności do wykonania misji na określonym poziomie w przypadku wystąpienia zagrożenia; poziom ten wskazuje, że wystąpienie zagrożenia grozi poważnymi (dotkliwymi) konsekwencjami, co oznacza, że decyzja o kontynuowaniu misji również musi być szczególnie rozważona w aspekcie osiągnięcia ewentualnych korzyści w przypadku jej kontynuowania; dotyczy *sporadycznego* i *rzadkiego* prawdopodobieństwa wystąpienia *katastrofalnych* strat (IC i ID), *prawdopodobnego* i *sporadycznego* prawdopodobieństwa wystąpienia strat *krytycznych* oraz *częstego* prawdopodobieństwa wystąpienia strat *marginalnych* [5];
- umiarkowane ryzyko *(moderate risk)* – przewidywane obniżenie możliwości w kategoriach osiągnięcia pożądanych parametrów zadania lub zmniejszenie tych możliwości w przypadku wystąpienia zagrożenia; dotyczy *mało prawdopodobnego prawdopodobieństwa* wystąpienia strat *katastrofalnych* (IE), *rzadkiego* prawdopodobieństwa wystąpienia *krytycznych* strat (IID) oraz *prawdopodobnego i sporadycznego* prawdopodobieństwa strat *marginalnych* (IIIB i IIIC), a także *częstego* prawdopodobieństwa strat *nieistotnych* [5];
- niskie ryzyko *(low risk)* – przewidywane straty mają mały lub nie mają wpływu na wypełnienie misji; obrażenia, zniszczenia lub choroby nie są oczekiwane, jednakże mogą wystąpić w nieznacznym zakresie bez długotrwałych skutków lub wpływu na wypełnienie misji; dotyczy to występowania *mało prawdopodobnego* wystąpienia strat *krytycznych* (IIIE), *rzadkiego* i *małoprawdopodobnego* wystąpienia strat *marginalnych* (IIID i IIIE) oraz *prawdopodobnego* wystąpienia strat *nieistotnych* (od IVB do IVE) [5].

3. OPRACOWANIE NARZĘDZI (PROCEDUR) KONTROLI RYZYKA I PODJĘCIE DECYZJI O AKCEPTACJI RYZYKA

W etapie trzecim opracowuje się i wprowadza procedury kontroli ryzyka, mające na celu wyeliminowanie zagrożenia lub zredukowanie ryzyka z nimi związanego. Następnie zagrożenia są ponownie szacowane w celu określenia ryzyka rezydualnego (pozostałego)[5]. Podstawą podjęcia decyzji o akceptacji ryzyka jest poziom ryzyka rezydualnego. Proces opracowania i wprowadzania procedur kontroli ryzyka oraz ponownego szacowania ryzyka jest prowadzony dopóki nie zostanie osiągnięty akceptowalny poziom ryzyka lub wszystkie ryzyka nie zostaną zredukowane do poziomu, w którym korzyści przewyższają poniesione koszty. Ten etap powinien być dokonywany podczas opracowania, rozważania i porównania wariantów działania oraz wyboru wariantu działania, czyli podjęcia decyzji (rys. 3).

[5] Ryzyko rezydualne - Poziom danego ryzyka, jaki pozostał po zastosowaniu wobec niego zaplanowanych działań [14]; Ryzyko rezydualne to ten poziom ryzyka, który pozostaje mimo podjęcia najlepszych i najbardziej starannych metod postępowania oraz stosownej kontroli [8].

3.1. Opracowanie narzędzi (procedur) kontroli ryzyka

Po oszacowaniu każdego zagrożenia, dowódca (sztab) opracowują jedną lub więcej procedur eliminujących lub zmniejszających ryzyko (prawdopodobieństwo i/lub dotkliwość) wystąpienia groźnych zdarzeń. W czasie opracowywania tych procedur dowódcy (liderzy) muszą skupić uwagę na przyczynach powodujących wystąpienie zagrożeń, a nie na zagrożeniach, jako samych w sobie. Procedury narzędzia kontroli ryzyka mogą przyjąć różne formy, ale zazwyczaj grupowane są w trzy podstawowe kategorie:

- naukowe *(educational (awareness) controls)* – bazujące na wiedzy i umiejętnościach jednostek, organizacji i żołnierzy. Obejmują ich świadomość zagrożenia i jego kontroli. Efektywną naukową procedurę kontroli ryzyka wprowadza się poprzez indywidualne i zbiorowe szkolenie, które powinno zapewnić jej wykonanie na wymaganym poziomie [5];
- fizyczne *(fhysical controls)* – przybierające formę barier i osłon lub oznak (sygnałów) ostrzegających ludzi, jednostki lub organizacje o istnieniu zagrożenia. Właściwy nadzorca lub personel nadzorujący zaliczany jest również do tych narzędzi [5];
- unikania/eliminacji *(avoidance/elimination controls)* – obejmują działania pozytywne w celu zapobieżenia zetknięcia się ze zidentyfikowanym zagrożeniem lub całkowitej eliminacji zagrożenia [5].

Aby spełnić wymaganie efektywności, każde z narzędzi musi sprostać następującym kryteriom:

- przydatność *(suitability)* – musi usunąć zagrożenie lub zmniejszyć ryzyko rezydualne do akceptowalnego poziomu;
- wykonalność *(feasibility)* – dana organizacja, jednostka musi posiadać możliwości wdrożenia danego narzędzia;
- akceptowalność *(acceptability)* – korzyści osiągnięte po wprowadzeniu narzędzi kontroli ryzyka muszą uzasadniać koszty środków materiałowych i czasu. To kryterium należy do najbardziej subiektywnych [5].

Źródłami, które mogą dostarczyć lub zidentyfikować efektywne procedury kontrolujące ryzyko w odniesieniu do określonych przedsięwzięć, operacji lub misji mogą być: doświadczenie personelu, wnioski z AAR *(After Action Review)*, dane o wypadkach ze zautomatyzowanego systemu zarządzania ryzykiem dostępne poprzez Centrum Gotowości Bojowej Armii Stanów Zjednoczonych (ang. *United States Army Combat Readiness Center* - USACRC), SOP-y i regulaminy, metody, techniki i procedury (ang. *tactics, technics and procedures* - TTP) oraz doświadczenia zbierane w ramach *lesson learned* z operacji prowadzonych w przeszłości. Ponadto arkusze CRM *(Composite Risk Management)* wykonywane w ramach poprzednich misji mogą stanowić kolejne źródło wyselekcjonowania określonych mierników efektywności. Kluczem efektywności procedur kontroli jest zredukowanie skutków lub eliminacja zidentyfikowanego zagrożenia.

Efektywne środki (narzędzia) kontroli muszą precyzować: kto?, co?, gdzie?, kiedy i jak? Poniżej przedstawionych jest kilka przykładów procedur, mających obniżyć

ryzyko w określonych sytuacjach, zaczerpniętych z instrukcji *Field Manual No. 5-19 (100-14), Composite Risk Management* [5].

a) niezabezpieczone/niestabilne ładunki
   - KTO?: Przełożeni, liderzy (dowódcy, kierownicy), kierowcy, operatorzy;
   - CO?: Powinni się upewnić się, że ładunki są zabezpieczone zgodnie z planem załadowania i stosownymi instrukcjami;
   - GDZIE?: W rejonie załadowania;
   - KIEDY?: Zanim pojazd otrzyma zezwolenie na wyjazd;
   - JAK?: Zwrócić uwagę na położenie środka ciężkości ładunku, amunicji i środków pozoracji pola walki;

b) niezabezpieczone włazy/rampy
   - KTO?: Przełożeni, liderzy (dowódcy, kierownicy), kierowcy, operatorzy;
   - CO?: Powinni skontrolować i usunąć niebezpieczną okoliczność;
   - GDZIE?: W rejonie rozmieszczenia lub w PST;
   - KIEDY?: Przed rozpoczęciem działania;
   - JAK?: Zabezpieczyć poprzez użycie sworznia blokującego lub zasuwy, zatrzasku;

c) niewłaściwe wyprzedzanie
   - KTO?: Przełożeni, liderzy (dowódcy, kierownicy), kierowcy, operatorzy;
   - CO?: Powinni ustalić i wprowadzić określone normy, ćwiczyć czynność wyprzedzania innych pojazdów tylko w bezpiecznych miejscach i czasie przy uwzględnieniu widoczności i intensywności ruchu drogowego;
   - GDZIE?: W rejonie rozmieszczenia lub w PST;
   - KIEDY?: Podczas szkolenia operatorów i kierowców przed wydaniem uprawnień, instruowanie operatorów i kierowców przed rozpoczęciem działania;
   - JAK?: Zweryfikować, czy operatorzy i kierowcy są wyszkoleni, wymusić standardowe zachowania;

d) niewłaściwe kierowanie ruchem pojazdów (przez ustawiającego pojazdy)
   - KTO?: Przełożeni, liderzy (kierownicy), kierowcy, operatorzy, żołnierze;
   - CO?: Ustalić i wprowadzić normy działania pojazdów w zatłoczonych rejonach (obóz, obsługa, rejon rozmieszczenia i na pozycji bojowej);
   - GDZIE?: W rejonie rozmieszczenia lub w PST;
   - KIEDY?: Przed wydaniem uprawnień kierowcom i operatorom, przed ćwiczeniami;
   - JAK?: Wymagać wzywania pomocy innych żołnierzy podczas operowania pojazdem w warunkach ograniczonej widoczności, cofania pojazdu, poruszania się w rejonie obozu, obsługi, rozmieszczenia lub pozycji bojowej;

3.2. Ponowne oszacowanie ryzyka

Wraz z wdrożeniem procedur kontroli - ryzyko powinno być ponownie oszacowane w celu określenia ryzyka rezydualnego (pozostałego) odnośnie poszczególnych zagrożeń oraz całkowitego ryzyka rezydualnego w odniesieniu do misji.

Ryzyko rezydualne to ryzyko pozostające po wprowadzeniu procedur kontroli ryzyka wyselekcjonowanych dla określonych zagrożeń. Ryzyko rezydualne można uznać za prawdziwe tylko wtedy, gdy wybrane procedury jego wyeliminowania lub zredukowania zostały wdrożone. Kiedy tylko określone procedury dla zidentyfikowanych zagrożeń zostaną wyselekcjonowane, zagrożenia są ponownie oszacowane i poziom ryzyka jest ponownie weryfikowany. Należy się liczyć z możliwością, że zastosowanie wybranych procedur nie będzie wystarczające, aby znacząco obniżyć poziom ryzyka.

Całkowite ryzyko rezydualne musi być określone poprzez rozważenie poszczególnych ryzyk rezydualnych odnoszących się do każdego zidentyfikowanego zagrożenia. Ryzyko rezydualne dla każdego zagrożenia może być różne, zależne od prawdopodobieństwa i dotkliwości zagrażającego zdarzenia. Przyjmuje się, że całkowite ryzyko rezydualne powinno być równe lub większe największemu zidentyfikowanemu ryzyku, które dotyczący któregoś ze zidentyfikowanych zagrożeń. Należy również wziąć pod uwagę ilość i charakter istniejących zagrożeń. W niektórych przypadkach dowódca może zdecydować, że całkowite ryzyko rezydualne jest wyższe niż którekolwiek z zagrożeń. Podstawą podjęcia takiej decyzji jest liczba zagrożeń o niższym ryzyku, jeśli w połączeniu prezentują większe zagrożenie. Przykładowo wynikiem oceny ryzyka w określonej misji może być umiarkowane ryzyko rezydualne dla poszczególnych zidentyfikowanych zagrożeń. Jednakże mając na względzie złożoność wymaganych procedur kontrolujących ryzyko oraz efekt synergiczny wszystkich zagrożeń, dowódca może zdecydować, że ryzyko rezydualne dla całej misji jest wysokie [5].

3.3. Podjęcie decyzji o akceptacji ryzyka *(Risk Decision)*

Celem procesu oceny i zarządzania ryzykiem (CRM) jest stworzenie podstaw do podjęcia optymalnej decyzji odnośnie akceptacji ryzyka lub jej braku. Kluczowym elementem do podjęcia tej decyzji jest określenie akceptowalnego poziomu ryzyka. Ryzyko lub możliwość potencjalnych strat muszą być zbalansowane oczekiwanymi korzyściami. Decyzja akceptacji poziomu ryzyka zawsze musi być podjęta na właściwym dla danej operacji, zadania szczeblu dowodzenia lub kierownictwa, a podstawę do jej podjęcia stanowi poziom istniejącego ryzyka [5] (ryzyka rezydualnego – przyp. autora).

4. WDROŻENIE PROCEDUR KONTROLI RYZYKA

W etapie tym dowódcy i ich sztaby zapewniają scalenie i przekształcenie procedur kontrolujących ryzyko w standardowe procedury operacyjne (SOP) oraz wydanie związanych z tym pisemnych i ustnych decyzji i instrukcji. Decydującym sprawdzianem dla tego etapu jest upewnienie się, że procedury (narzędzia) kontrolujące ryzyko zostały przekształcone w jasne i proste decyzje (rozkazy). Wdrożenie procedur (narzędzi) kontroli ryzyka, zgodnie z literaturą [5], obejmuje koordynację i komunikację (kontakt) z:

- bezpośrednim przełożonym, sąsiednimi oraz podległymi jednostkami, organizacjami i podwładnymi;

- organizacjami działającymi w ramach Programu Wzmocnienia Logistyki Cywilnej (ang. *Logistics Civil Augmentation Program* - LOGCAP), agencjami cywilnymi wchodzącymi w skład sił prowadzących daną operację (przedsięwzięcie) lub tymi, na których funkcjonowanie będą wpływać działania sił, zagrożenia związane z misją lub procedury kontrolujące ryzyko;
- mediami i organizacjami pozarządowymi (NGO), jeśli ich obecność wpływa na daną misję lub działania sił prowadzących misję wywierają wpływ na daną organizację [5].

Dowódcy lub tzw. liderzy są zobowiązani do wyjaśnienia, w jaki sposób zostaną wprowadzone procedury kontroli ryzyka. Wśród przykładowych sposobów i narzędzi służących temu celowi w armii Stanów Zjednoczonych wyróżnia się:

- nakładki (oleaty) i grafiki;
- ćwiczenia w identyfikacji sylwetek pojazdów i lotnictwa;
- odprawy poświęcone synchronizacji działań oraz ćwiczenia poligonowe;
- treningi dla załóg i obsług z pododdziałów przeciwpancernych i przeciwlotniczych dotyczące działania po ogłoszeniu alarmu bojowego oraz „odświeżające" pamięć sylwetek pojazdów i samolotów wojsk własnych;
- odprawy informacyjne dla nowego personelu (zmieniającego poprzedni);
- instalacja i utrzymywanie łączności z organizacjami cywilnymi;
- organizacja konwojów z nakazana minimalną (optymalną) ilością pojazdów;
- nakaz noszenia broni oraz kamizelek kuloodpornych i hełmów podczas przebywania poza bazą;
- uświadamianie o możliwości wystąpienia wypadków, instruktaże oraz szkolenia dotyczące bezpieczeństwa wojsk własnych [5].

5. NADZÓR I OCENA

W etapie piątym dąży się do uzyskania potwierdzenia, że procedury kontroli ryzyka zostały wprowadzone zgodnie z narzuconymi standardami, że wyselekcjonowano właściwe środki kontroli, aby osiągnąć pożądane cele i wyniki. Nadzór i ocena podjętych decyzji jest nieodłącznym elementem podczas prowadzenia każdego etapu operacji lub przedsięwzięcia. Stały proces kontroli, bazujący na osiąganych wynikach w zmieniającej się sytuacji, ma zapewnić zdolność identyfikacji niedociągnięć i wprowadzania zmian oraz korekt w procedurach kontroli ryzyka [5].

5.1. Nadzór

W wyniku prowadzonego nadzoru uzyskuje się potwierdzenie, że podwładni właściwie zrozumieli, w jaki sposób, kiedy i gdzie miały być wprowadzone procedury kontroli ryzyka, jak również, że wspomniane procedury zostały wprowadzone, są utrzymywane i monitorowane. Istotnym elementem w procesie CRM podczas identyfikacji zagrożeń jest świadomość sytuacyjna[6], która ma równie ważne znaczenie w czasie realizacji nadzoru. Jej właściwy poziom zapewnia monitoring takich czynników, jak:

[6] Świadomość sytuacyjna (*situational awareness* - wiedza o obszarze działania (operacji) oraz o położeniu, działaniu i zamiarach sił własnych i przeciwnika) [22].

samozadowolenie, zmęczenie, dostępność i możliwości obsługowe sprzętu i wyposażenia, warunki atmosferyczne i środowiskowe, odchylenia od wprowadzonego planu oraz naruszenia procedur kontroli ryzyka. Monitorowanie to pozwala na zredukowanie zagrożeń związanych z wymienionymi czynnikami i obniżenie ich ujemnego wpływu na osiągnięcie celu. Nadzór i przegląd sytuacji pozwala również dowódcom i liderom, dzięki ich właściwemu poziomowi świadomości sytuacyjnej przewidywać, identyfikować i szacować nowe zagrożenia oraz rozwijać lub modyfikować procedury kontroli według potrzeb [5].

W etapie piątym jest wymagane utrzymywanie jak najwyższego stopnia dyscypliny niepozwalającego popadać w samozadowolenie i zbytnią pewność będącą wynikiem znużenia, spowodowanego sytuacją, w której personel, podwładni wykonują rutynowe powtarzające się czynności. Procedury kontroli ustanowione i wdrożone na długi okres niejednokrotnie mogą być ignorowane z powodu zbyt dużej pewności siebie. Przykładowo, podczas działań stabilizacyjnych, już na początku operacji mogą zostać zidentyfikowane zagrożenia spowodowane istnieniem min lądowych, a w następstwie tego można ustanowić i wdrożyć określone procedury kontroli. Jednakże z czasem, wraz z osiąganym powodzeniem (brakiem jakichkolwiek wypadków i groźnych zdarzeń), przeświadczenie o braku zagrożeń może wzrosnąć, czego wynikiem może być spadek efektywności ustanowionych procedur. Kiedy personel mieszka lub działa w rejonie uważanym za rejon o niskim zagrożeniu lub w rejonie o wysokim zagrożeniu, ale przez długi czas nie odnotowuje żadnego wypadku, wtedy istnieje ryzyko utraty właściwego poziomu świadomości sytuacyjnej i utrzymania odpowiedniej czujności [5].

Inne długotrwałe zagrożenia, które mogą z czasem powodować spadek efektywności procedur kontroli ryzyka to: ekstremalne warunki klimatyczne, zagrożenia związane z bronią masowego rażenia oraz zanieczyszczeniami i niebezpiecznymi odpadami, jak również choroby pochodzące z rejonu działania lub tubylcze społeczeństwo.

5.2. Ocena

Oceny (szacowania) dokonuje się w całym zakresie działania, jako część tzw. *After Action Review* (AAR) – przeglądu i oceny działania, który następuje po zakończeniu operacji lub przedsięwzięcia. Proces oceny służy do osiągnięcia następujących celów:

- identyfikacji zagrożeń, które nie zostały rozpoznane podczas wstępnej oceny zagrożeń, a które uwidoczniły się w toku operacji lub przedsięwzięcia (np. za każdym razem, kiedy personel, sprzęt i wyposażenie, środowisko lub misja zmieni wstępną analizę oceny ryzyka, procedury jego kontroli powinny być ponownie poddane ewaluacji) [5];
- oceny efektywności wspomagania osiągania celów operacyjnych i głównych. *Czy procedury kontroli pozytywnie lub negatywnie wpłynęły na przygotowanie lub ukończenie misji? Czy procedury kontroli potwierdzają istniejące doktryny, techniki, metody i procedury operacyjne?* [5];
- oceny wdrożenia, wykonania oraz komunikatywności procedur kontroli;
- oceny trafności określenia poziomu ryzyka rezydualnego oraz efektywności procedur kontroli w eliminowaniu zagrożeń i kontrolowania ryzyka [5];

– zapewnienia zgodności z regułami procesu CRM. *Czy proces ten jest integralną częścią wszystkich faz operacji? Czy decyzja o akceptacji ryzyka była właściwa? Czy została podjęta na właściwym szczeblu dowodzenia? Czy pojawiło się jakieś zbędne ryzyko i czy korzyści w szkoleniu i w czasie przewyższały koszty liczone w dolarach? Czy proces ten jest cykliczny czy stały przez całą operację?*[5].

Dowódcy, przywódcy i indywidualni żołnierze ponoszą odpowiedzialność za nadzór i ocenę zarówno działań taktycznych, jak i przedsięwzięć niemilitarnych czy pozasłużbowych. Techniki przez nich stosowane w tym celu mogą obejmować badania wyrywkowe, inspekcje, raporty sytuacyjne (SITREP – ang. *situation report*), kontrole, bezpośredni nadzór oraz tzw. przegląd działania (AAR – *After Action Review*), który dostarcza danych (wniosków do przedstawienia w szerszym gronie), na bazie których cała misja lub inne przedsięwzięcie może być ocenione. W przeglądzie działania powinna być ujęta również ocena efektywności procesu CRM [5].

PODSUMOWANIE

Celem autorów niniejszego opracowania było przybliżenie metody zarządzania ryzykiem stosowanej w armii Stanów Zjednoczonych. W metodzie tej oceny prawdopodobieństwa wystąpienia danego zagrożenia oraz konsekwencji (dotkliwości) i wpływu na działanie, jeżeli takie zagrożenie wystąpi, w większości przypadków są oparte na doświadczeniach członków sztabu z działań prowadzonych w przeszłości oraz doświadczeń zbieranych w ramach tzw. *Lesson learned*. Niewątpliwą zaletą stosowania tej metody w procesie podejmowania decyzji jest to, że rozpatruje się skutki wystąpienia określonych zagrożeń, co pozwala dowódcom na szerszą ocenę sytuacji oraz podjęcie decyzji racjonalnej lub optymalnej, w przeciwieństwie do naszych sił zbrojnych, w których nie ocenia się ryzyka. Na uwagę zasługuje fakt, że w regulaminie opisującym tę metodę zawarto informację, że ocena ryzyka ma tylko wspomóc dowódcę podczas podejmowania decyzji, a nie narzucać ostatecznego rozwiązania problemu, nie może wykluczać kompetentnych decyzji wynikających z doświadczenia bojowego. Jednakże wątpliwości autorów wzbudza sposób kategoryzacji skutków wystąpienia zagrożenia, który pozwala dowódcom na pewną dowolność interpretacji poszczególnych kategorii (zdaniem autorów zbyt dużą).

LITERATURA

[1] Chong Y. Y., Brown E. M., *Zarządzanie ryzykiem projektu*, Oficyna Ekonomiczna, Kraków 2001.

[2] Damodaran A., *Ryzyko strategiczne: podstawy zarządzania ryzykiem*, Wydawnictwa Akademickie i Profesjonalne, Warszawa 2009.

[3] *Field Manual No. 1-02 (101-5-1) Operational Terms and Graphics*, Headquarters Department of the Army, Washington 2004.

[4] *Field Manual No. 100-14, Risk Management*, Department of the Army, Washington 1998.

[5] *Field Manual No. 5-19 (100-14), Composite Risk Management*, Department of the Army, Washington 2006.

[6] Kaczmarek T. T., *Ryzyko i zarządzanie ryzykiem. Ujęcie interdyscyplinarne,* Centrum Doradztwa i Informacji Difin, Warszawa 2008.

[7] Klimczak K. M., *Wdrażanie zarządzania ryzykiem w jednostkach sektora finansów publicznych,* [w:] „Przegląd Organizacji", nr 5/2009, s. 23 – 26.

[8] Knypl K., *Redukcja ryzyka rezydualnego w chorobach układu krążenia,* KARDIOPROFIL VOL. 7/NR 1(28)/2009, [online]. [dostęp: 04.05.2010]. Dostępny w Internecie: http://www.mededu.plk.

[9] Kulińska E., Dornfeld A., *Zarządzanie ryzykiem procesów: identyfikacja, modelowanie, zastosowanie*, Politechnika Opolska, Opole 2009.

[10] Liedel K., *Zarządzanie przyszłością i analiza ryzyka jako narzędzia w walce z terroryzmem,* [w:] *Zagrożenia i wyzwania dla bezpieczeństwa. Tom II*, pod red. Żuber M., Wrocław 2009.

[11] Matkowski P., *Zarządzanie ryzykiem operacyjnym*, Oficyna Ekonomiczna - Wolters Kluwer Polska, Kraków 2006.

[12] Michniak J., *Dowodzenie i łączność*, AON, Warszawa 2003.

[13] Moczulski J., *Zarządzanie ryzykiem*, [w:] „Przegląd Wojsk Lądowych", nr 4/2005, (550), s. 38 – 42.

[14] *M_o_R® (Management of Risk) Glossary Of Terms – Polish (Słownik – Polski),* The APM Group 2010, 12 February 2010; [online]. [dostęp: 04.05.2010]. Dostępny w Internecie: http://www.mor-officialsite.com/.

[15] *ORM 0-1, Operational Risk Management,* Headquarters Marine Corps, Washington 2002.

[16] Pałetko O., *Zarządzanie ryzykiem – narzędzie do planowania systemu ochrony bazy wojskowej (na podstawie doświadczeń IV zmiany PKW w Iraku),* [w:] „Przegląd Wojsk Lądowych", nr 7/2006, s. 39 – 42.

[17] *Podstawy dowodzenia*, pod red. Kręcikij J., Wołejszo J., AON, Warszawa 2007.

[18] Skorupka D., Nogalski B., *Zarządzanie ryzykiem realizacji inwestycji budowlanych,* [w:] „Zeszyty Naukowe, Problemy Zarządzania, Finansów i Marketingu", nr 8, Uniwersytet Szczeciński 420/8/2006, Szczecin 2006, s. 71 – 84.

[19] Skorupka D., *Metoda identyfikacji i oceny ryzyka realizacji przedsięwzięć budowlanych,* WAT, Warszawa 2007.

[20] Strzelczak S., *Operational Risk Management*, Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa 2008.

[21] Tarczyński W., Mojsiewicz M., *Zarządzanie ryzykiem*, Polskie Wydawnictwo Ekonomiczne, Warszawa 2001.

[22] Wrzosek M., *Uwarunkowania amerykańskiej lądowej operacji interwencyjnej XXI wieku w aspekcie rozpoznania,* [w:] „Zeszyty Naukowe AON", nr 4/2003, (53), s. 241 – 251.

COMPOSITE RISK MANAGEMENT – METHOD OF RISK MANAGEMENT IN US MILITARY ORGANISATION

Summary

In their article the authors depict the method of risk management used by US Army commanders in the military decision-making process, the preparation and the execution of an operation. The method is applied to combat operations, stabilisation operations, training, garrison activities and off-duty activities. The purpose of Composite Risk Management is to mitigate or eliminate risks associated with all the hazards related to the abovementioned operations and activities.

Key words: *risk management, risk, decisions, decision making, Composite Risk Management, armed forces – United States*