Министерство на отбраната на Република България
Дирекция „Стратегическо планиране”

М О Д Е Л

за управление на риска при планиране на отбраната и въоръжените сили

гр. София
2011 г.

Министерство на отбраната на Република България
Дирекция „Стратегическо планиране”

М О Д Е Л

за управление на риска при планиране на отбраната и въоръжените сили

Обявен със заповед № 280/11.05.2011 г.
на министъра на отбраната на Република България

Разработването на Модела за управление на риска при планиране на отбраната и въоръжените сили е продиктувано от необходимостта да се отчита все по-нарастващата неопределеност на средата в процеса по планиране в отбраната, както и липсата на национална нормативна уредба по въпросите, по отношение на риска.

Целта на модела е да послужи като методологична основа, описваща процеса за управление на риска в системата на отбрана. В модела са представени елементите от теорията на управлението на риска, които очертават както теоретичните основи на материята, така и нейното практическо приложение.

Предназначен е за използване от широк кръг потребители и преди всичко за тези, които участват пряко в процеса на вземане на решения, свързани с ръководството и управлението на различни процеси, проекти и организационни структури.

Документът е разработен от авторски колектив
на дирекция „Стратегическо планиране”- МО,
в състав:

ръководител комодор Георги Фиданов

полковник Максим Любенов Карев, д-р
полковник Светослав Манев Чолаков
подполковник Светлан Василев Дюлгеров
подполковник Иво Георгиев Радулов, д-р
инж. Пламена Цанова Андреева, д-р

Издава: Военен географски център,
Печатна база гр. Троян

Моделът за управление на риска при планиране на отбраната и въоръжените сили е приет на основание чл. 4, ал. 1 и ал. 2 от Правилника на Съвета по отбранителни способности към министъра на отбраната на Република България (П-5/29.07.20010 г.) и решение на заседание на Съвета по отбранителни способности към министъра на отбраната на Република България (т. 1 от Протокол № 15/10.03.2011 г.). Същият е утвърден със заповед № 280/11.05.2011 г. на министъра на отбраната на Република България.

С Ъ Д Ъ Р Ж А Н И Е

1. Увод

Новата среда за сигурност, повлияна от трудно предвидими и динамични процеси от разнороден характер, както и обществената значимост на сектора за сигурност и отбрана, финансовите и материалните ресурси, влагани в него, придават на процеса на управление на риска изключителна важност за гарантиране на ефективно организационно управление и постигане на поставените цели. Добре оценението риск осигурява съществено и значимо предимство на управленския състав при формирането на обосновани и правилни решения.

Какво налага интереса към управлението на риска в планирането на отбраната и въоръжените сили? В света на глобалните предизвикателства точно дефинирани рискове и заплахи не съществуват, няма и универсални решения за противодействие, които да се прилагат еднакво за всеки специфичен случай от лицата, взимащи управленски решения. Именно все по-нарастваща неопределеност в средата на сигурност налага да се обърне по-голямо внимание на въпросите по управлението на риска.

По същество, управление на риска на най-високо ниво на абстракция не е нищо друго, освен систематичен отговор на неопределеността. От гледна точка на нуждите в сферата на отбраната и сигурността, неопределеността възниква от взаимното влияние между няколко независими една от друга променливи, част от които е изключително трудно да се анализират и оценят. По-конкретно управлението на риска, в контекста на отбраната и сигурността, е опит да се разкрият негативните последици от действието на носител на заплаха, използващ някои уязвими страни на конкретен субект (организация, процес, инфраструктура, ресурс и др.) с цел пагубно въздействие върху представляващата определена ценност на субекта (организация, процес, инфраструктура, ресурс и др.).

Съвременните рискове и заплахи имат променлив и често неконвенционален характер. Те са обусловени от процесите на глобализация и борбата за интереси и влияние, климатичните промени, емиграцията и утвърждаването на новите асиметрични заплахи. Ето защо рискът трябва да се управлява по ефективен начин, с цел ръководителите да бъдат подготвени в условия на кризисно управление – интензивен процес на изразходване на ресурси, който обикновено е ограничен от рестриктивната тенденция в свободата на избор.

За да бъде успешен процесът на управление на риска в планирането на отбраната и въоръжените сили, са необходими редица предпоставки, основните от които са:

1) изградена адекватна политика за управление на риска като неделима функция от процеса на вземане на решения;

2) налична методологична основа, включваща адекватни методи и средства за анализ, оценка и управление на риска;

3) подготвени специалисти в тази област.

Реалното състояние в отбраната показва, че все още не са осигурени условията за управлението на риска, които да обхващат всички нива на управление. Липсват и съответните ангажименти от страна на управленския състав за реализирането на такъв вид политика. Сериозен недостатък е и малкият брой подготвени специалисти по управление на риска в сектора, което се отразява на качеството на резултатите, основаващи се повече на интуицията и на професионалния опит на специалистите, отколкото на научно доказани теории и методи.

В отговор на това, разработеният модел е насочен главно към преодоляването на съществуващата липса на адекватен инструментариум за управление на риска, целящ повишаването на ефективността на мениджмънта в системата на отбраната. Същият няма за цел да запълни липсващите политики в областта на управлението на риска. Основното му предназначение е да предложи методологична основа за управлението на риска, базирана на научно-аналитична експертиза в помощ на управленския състав при вземането на решения. В модела са представени елементите от теорията на управлението на риска, така че да се

очертаят основите на материята – не само като научна теория, но и в контекста на нейното приложение.

В резултат се получава достатъчно изчерпателна картина за етапите, дейностите, подходите, методите и крайните резултати от целия процес на управлението на риска при планирането на отбраната и въоръжените сили.

Моделът може да се използва в целия спектър от задачи, свързани с планирането на отбраната и въоръжените сили, в случаите където трябва да се изследва влиянието на риска върху поставената цел. Това например са: 1) управление на риска на стратегическата среда за сигурност; 2) оценка на асоциираните най-критични рискови фактори за отделните сценарии; 3) управление на риска в прегледа на структурата на въоръжените сили; 4) анализ на риска при запазването и/или отказването от определени способности; 5) управление на риска при попълване на дефицитите от способности и поддържането им; 6) управление на риска при определянето на баланса между необходимите способности и ресурсното им осигуряване; 7) оценка на риска при управлението на проекти и т.н.

В приложенията на документа са предложени математически модели за оценка на риска, базирани на интелигентни технологии, адаптирани научни достижения и специализирани средства за моделиране и симулация, намерили конкретно приложение в дадените три примера. В тях чрез използването на съвременни математически методи (базирани на размита логика с отчитане на непълната определеност в количествените и качествените данни; PERT - Program Evaluation and Review Technique - техника за преглед и оценка на програми) и аналитичен софтуер е изследван риска за конкретни случаи на планиращи сценарии.

2. Предназначение на модела

Рисковете в мениджмънта на отбраната могат да произтичат от съдържанието и обхвата на изпълняваните дейности, както и да са свързани със законодателни, икономически, социални и други аспекти на средата, в която те се реализират. Независимо от условията на появата им, рисковете трябва да се идентифицират, дефинират, анализират и оценяват чрез използване на качествени и количествени методи. За редуцирането на тяхното влияние се разработват стратегии, съдържащи подходящи подходи и техники за намаляване на вероятността за поява на рискове и ограничаване на размерите на очакваните последици. Прилагането на тези стратегии гарантира във висока степен постигането на целите.

Предложеният модел дава възможност за практическо приложение и е отговор на съществуващата необходимост от инструментариум за управление на риска в цялостния процес на планиране на отбраната и въоръжените сили. Въвеждането му цели повишаване на ефективността на мениджмънта в системата на отбраната.

Документът съдържа необходимия минимум от знания за управлението на риска. При решаването на конкретна задача той може да бъде допълван и конкретизиран, но не и съкращаван.

3. Основни понятия

В специализираната научна литература [2, 14, 15, 22, 23] се срещат различни определения, свързани с понятието „риск”.

Под „риск” в предложения модел се разбира въздействие на несигурността върху целите на Организацията. Несигурността е състояние на недостиг от информация, свързана с разбирането и знанието за дадено въздействие, неговите последствия или вероятност. Целите могат да имат различни аспекти (финансови, здравни, свързани с безопасността, екологични)

и могат да се прилагат на различни нива (стратегическо, структурно звено, продукт или процес).

Причинителите на риска могат да бъдат природни сили, човешка дейност, пазарът и други. Голяма част от рисковете е възможно да бъдат предвидени. Те се наричат *известни рискове.* Рискове, които няма как да бъдат предвидени, се наричат *неизвестни*. Такива рискове могат да бъдат контролирани само с техники като предвиждане на **финансов, времеви или материален резерв.**

Терминът „заплаха” означава възможна надвиснала опасност или предупреждение за надвиснала опасност, например „терористична заплаха”. При военната заплаха, това е наличие на способност за нанасяне на поражения и намерение за изпълнението ú.

Под „опасност” се разбира източник на потенциална вреда. Опасността може да бъде източник на риск.

Терминът „сигурност” се разглежда като динамично състояние на дадена система, което осигурява неутрализирането и противодействието ѝ на външни и вътрешни фактори, оказващи влияние или можещи да въздействат деструктивно на системата (влошаване организационното състояние на системата или невъзможност за нейното функциониране и развитие).

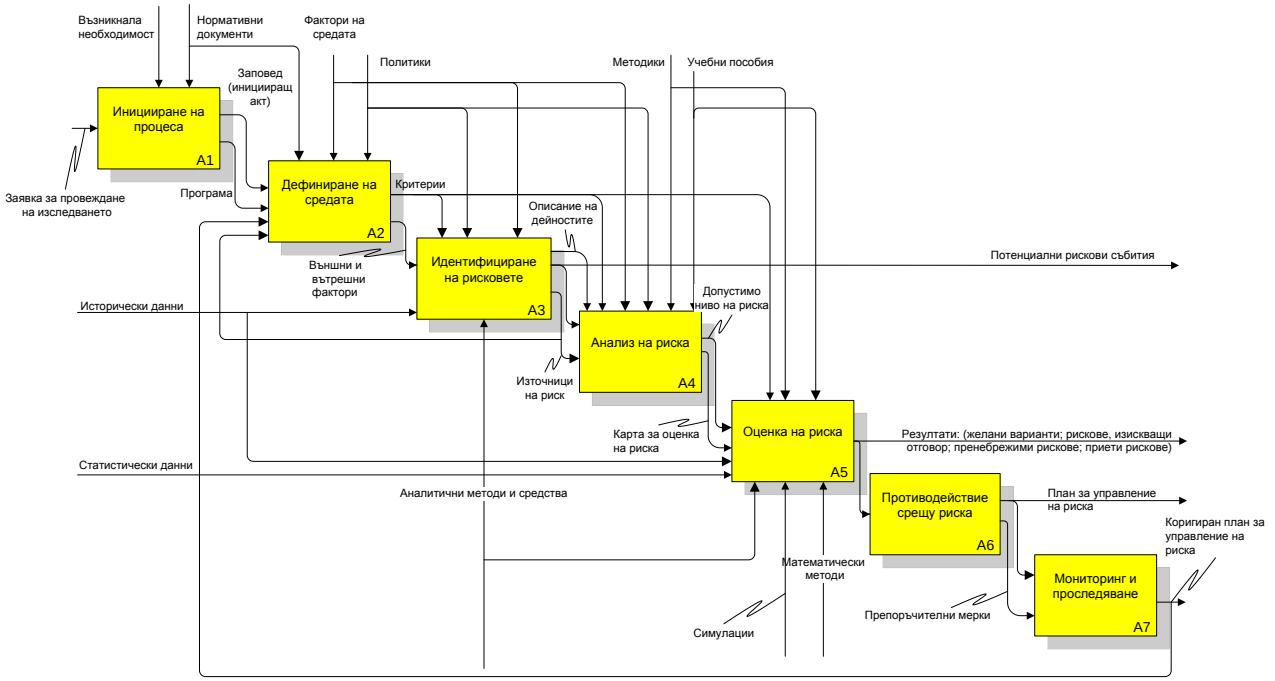
Представените основни понятия не изчерпват теоретичния обзор. Това са най-често употребяваните понятия, с които се говори за риск и за управление на риска. При описанието на модела са използвани и понятията, с техните обеми и съдържания, разкрити в „Терминологичен речник по управление на риска”, в края на документа.

4. Модел на дейностите по управление на риска

По дефиниция управлението на риска се разглежда като процес за идентифициране, анализ, противодействие, наблюдение и контрол на риска, насочен към максимизиране на резултатите от позитивните събития и минимизиране на ефектите от негативните [23]. В същността си управлението на риска е цикличен системен процес за ефективно редуциране влиянието на несигурността, която застрашава организационните цели.

Съществуват различни концепции относно съдържанието на процеса на управление на риска. Те се различават основно по групирането и структурирането на дейностите в процеса и в нивото им на декомпозиция [1, 2]. Най-широка популярност е придобила показаната на Фигура 1 разширена схема на процеса на управление на риска. В нея, с помощта на IDEF0 диаграма, са представени основните дейности от процеса по управление на риска, включващи накратко следното съдържание [3, 5, 12]:

- A1 - Иницииране на процеса. Поставят се началните условия на процеса и се съставят задание (заявка за провеждане), организационна заповед (иницииращ акт) за сформиране на екипите и провеждане, както и програма за реда, начина и периодичността за оценка на риска при планирането на отбраната и въоръжените сили;
- A2 - Дефиниране на средата (контекста). Определят се процесите, които са в обхвата на средата, заинтересованите страни и какви са техните цели. Това е рамката, в която ще се търсят рискове с цел тяхното управление. Крайни продукти от етапа са критериите за оценка и значимите външни и вътрешни фактори на средата [7, 14, 17];



Фигура 1. Основна диаграма на дейностите на процеса по управление на риска (A0)

- A3 - Идентифициране на рисковете. При идентифицирането на риска се изследват и определят рисковите области и източниците на риск за организационната дейност. Това се извършва с различни методи за идентификация на рисковите събития, които най-общо се изразяват чрез следните подходи: 1) Определяне на риска на базата на целите – определят се целите на организацията, а всички събития или обстоятелства, които могат частично или напълно да застрашат постигането на тези цели, се определят като рискове; 2) Определяне на риска на базата на сценарии – разиграват се различни сценарии за развитието на определено събитие или изпълнението на определен процес. Всяко събитие, което предизвиква реализирането на нежелан резултат, се третира като риск и/или заплаха; 3) Определяне на риска на базата на класификацията – определят се възможните източници на риск. На базата на тази класификация и на информацията за общо използваните добри практики се разработва въпросник, от отговорите на който се извличат рисковете, които трябва да се контролират. Крайните продукти от етапа са описание на дейностите от процеса, идентифициране на потенциалните рискове и източниците на риск.
- A4 - Анализ на риска. При анализа на риска се изследват идентифицираните рискове и причините за тях. Етапът е комплексен и е свързан с изграждането на работеща структура на процеса на оценката на риска. Анализът е насочен към изследване на параметрите на риска и потенциалните му влияния върху реализирането на другите специфични дейности по сценариите. Крайните продукти от етапа са: допустими нива на риска и карти за оценка на риска, съдържащи стойности на вероятностите за проява на рискове и стойности на последиците от проява на рисковете [8, 13, 24];
- A5 - Оценка на риска. Най-общо рисковете се оценяват спрямо потенциалните вредни последици и вероятността те да се случат. Това е най-критичният и един от най-трудните етапи от процеса на управление на риска. Например, сравнително лесно може да се изчисли размерът на загубата на някакъв материален актив, но не е толкова лесно той да се определи за нематериалните активи или да се оцени рискът за събития, свързани с въоръжени конфликти при отчитане на динамиката на бойните действия. Често изпълнението на етапа е затруднено и от липсата на адекватна информация, на която да се основават изследванията. В резултат от оценката на риска се изготвят варианти, описващи желаните възможности и рисковите събития, изискващи отговор, определят се и

възможностите за пренебрегване или приемане на определени рискови събития, без това да надхвърля допустимото ниво за риск [11, 16, 19, 20];

- А6 - Противодействие на риска. В този етап се прави определяне, оценка, избор и прилагане на подходящи техники за противодействие на идентифицираните и оценени рискове с цел намаляване на влиянието им до приемливи нива. Тези нива са определени предварително при дефинирането на допусканията и ограниченията за извършваната дейност. Противодействието на риска се осъществява по следните начини: **1) трансфер** – прехвърляне на риска към трета страна; **2) избягване** – да не се прави това, което евентуално би реализирало риска; **3) редуциране** – прилагат се механизми, чрез които да се намалят загубите; **4) приемане** – приемат се последствията (остатъчния риск), когато се случат. Обикновено се прилага за много малки или много големи рискове. Резултат от етапа е изготвянето на план за управление на риска [13, 20];
- А7 - Мониторинг и проследяване на процеса на управление на риска. Това е дейност за систематично следене и оценяване на прилаганите техники за противодействие на риска. На този етап могат да се разработват нови или да се усъвършенстват старите техники. Краен продукт от етапа е изготвянето на коригиран план за управление на риска.

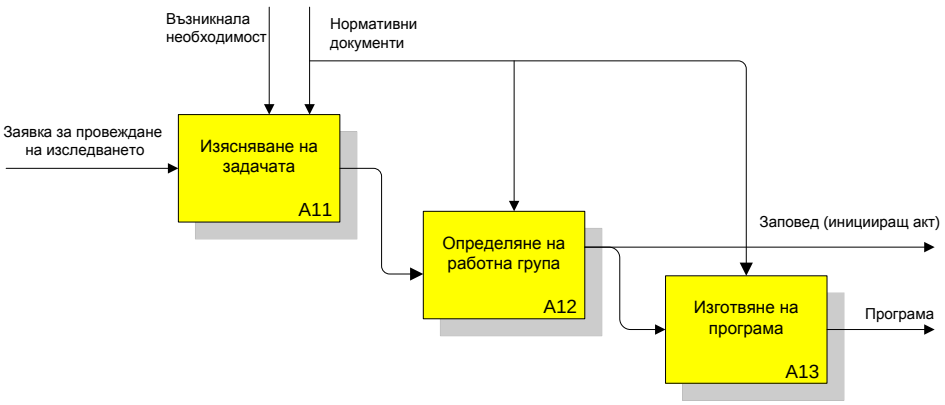
4.1. Иницииране на процеса – А1

С цел да се изясни въпросът и да се разширят познанията за процеса на управление на риска, основните дейности от диаграмата на Фигура 1 са декомпозирани, а същностите на етапите и видовете на изходните документи са описани детайлно в модела.

Етап А1 „Иницииране на процеса” е първият от процеса на управлението на риска и се състои основно от следните дейности:

- изясняване на задачата (А11);
- определяне на работните групи (А12);
- изготвяне на програма за дейността по оценяването на риска (А13).

Последователността на изпълнението им е показана на Фигура 2.



Фигура 2. Диаграма на дейността „Иницииране на процеса” (А1)

За начало на процеса се счита постъпването на заявка, указание или разпореждане за провеждане на изследването, което е водеща линия и фокус на извършваните дейности. Заявката трябва да съдържа рамката, в която следва да се идентифицират целите и да се отчете тяхното постигане. Като правило заявката се задава и уточнява от заявителя на изследването, който е целевият потребител. Промяната на параметрите в хода на работата е в състояние да обрече процеса на неуспех.

4.1.1. Изясняване на задачата - A11

Това е първата дейност от процеса, в която започва функционално изясняване на задачите, предполагащо ясна визия от самото начало за резултатите в края на всеки етап от процеса, както и за начина на изпълнение на всяка дейност. Етапът включва: 1) провеждане на детайлна и осмислена подготовка за изследването с цел безпрепятственото протичане на процеса; 2) създаване на цялостна организация за управление на процеса, отчитаща степента на централизираност или децентрализираност 23].

Изборът на подход за бъдещата работа е от особена важност и зависи от степента на зрелост на организацията по отношение на управлението на риска. Според стила на управление на организацията се прилагат централизиран и децентрализиран подход.

Централизираният подход за управление на риска се препоръчва в случай, когато екипите нямат достатъчен опит в областта и са в период на обучение. В този случай е целесъобразно да се създаде екип, който е отговорен за всички аспекти на управлението на риска – от разработването на план, през извършването на анализа и оценката, до определянето на подходящите техники за противодействие и следенето на постиганите резултати.

Децентрализираният подход за управление на риска позволява прилагането на експертиза в определените области. Степента на децентрализираност зависи от степента на делегиране на отговорности и от степента на подготовка на личния състав, който ще е отговорен за управлението на риска на съответното ниво.

Съществува и „хибриден” подход, в който делегирането на отговорности, по отношение на риска, може да бъде централизирана до определено ниво [23].

Независимо от схемата за организиране на процеса на управление на риска е необходимо да се спазват следните общи правила:

- управлението на риска да е интегрирана част от управлението;
- естеството на работата налага ръководителите, отговарящи за планирането, да участват пряко в цялостния процес по управлението на риска [23].

4.1.2. Определяне на работна група - A12

Дейностите по определяне на работната група включват формиране на екипи и разпределяне на ролите, правата и отговорностите между членовете на екипа, свързани с бъдещата работата по управлението на риска.

В зависимост от избрания подход за работа, работната група се определя съобразно естеството на конкретната задача и от поставените изисквания към изследването от страна на заявителя. В тази връзка, изследователите (оценителите) преценяват по целесъобразност състава на участниците в процеса, методите и подходите, които ще се използват и кои области ще се разглеждат.

При липса на административен капацитет за управлението на риска в дадена област/структура, към работната група се привличат подготвени специалисти от други административни структури и/или аналитични звена. Определянето на работната група за оценка на риска в процеса на планиране на отбраната се извършва с административен акт на министъра на отбраната (началника на отбраната), в който са посочени основните административни аспекти на процеса и с който се информират всички участници за необходимостта от тяхното съдействие в изпълнението на дейностите от процеса. В тази работна група е препоръчително да участват:

- експерти по отбранително планиране;
- експерти по управление на ресурсите за отбрана;
- експерти по отбранителна аквизиция;
- тесни специалисти от видовете въоръжени сили с експертиза за конкретните параметри на поставената задача;
- специалисти с подходящо техническо образование, запознати подробно с възможностите на наличната техника, въоръжение и работата с тях;
- експерти от служба „Военна информация”;
- експерти, притежаващи аналитични способности и математическа експертиза.

По собствена преценка ръководителят на процеса включва и други лица с необходими познания и опит за оценяване на риска при планирането на отбраната. В този контекст е целесъобразно административният акт да се съгласува предварително с всички заинтересовани структури и лица.

4.1.3. Изготвяне на програма - A13

Изготвянето на програма е последната дейност от етапа „Иницииране на процеса”.

Програмата служи за ръководство на работната група за извършване на изследването и за мониторинг на процеса, свързан с изпълнението на изискванията към резултатите и сроковете. Програмата е сборен документ и е предназначена преди всичко за изследователския екип. Документът трябва да съдържа задължителния минимум от данни, включващ [26]:

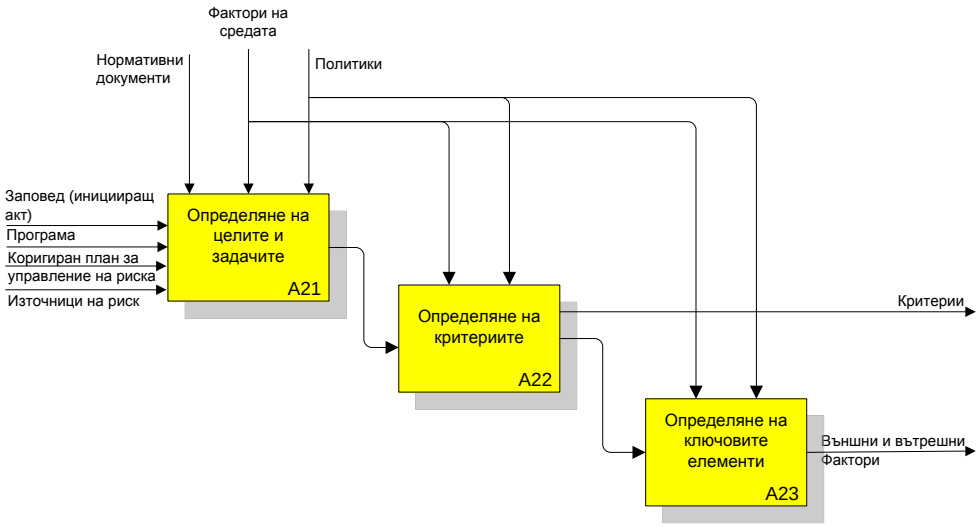
- организацията и координацията на дейностите по оценяването на риска;
- подходите и методите за извършване на оценката на риска, включително осигуряването на достоверност на резултатите и разработването при необходимост на подходящи за целта методи;
- оценителите на риска;
- необходимите ресурси за оценяването на риска;
- начините за осигуряване на информацията, обучение и консултации с оценителите;
- етапите, последователността и сроковете за оценяване на риска;
- начините за допитване, консултации, анкети и събеседване със специалистите за конкретното оценяване.

Примерен вариант на „Програма за дейността по оценяването на риска” е представен в Приложение 1.

4.2. Дефиниране на средата – A2

За да се идентифицира рискът, е необходимо предварително да бъдат дефинирани параметрите на средата (контекста) – вътрешни и външни, и рамките, в които ще се реализира изследването [2, 4].

На този етап се определят целите, задачите, критериите и ключовите елементи на изследването (Фигура 3).



Фигура 3. Диаграма на дейността „Дефиниране на средата” (A2)

Целите и задачите са основата на етапа „Дефиниране на средата”. За да се гарантира, че всички важни рискове ще бъдат овладени, е необходимо да се определят адекватни цели и задачи. Изпълнява се A21 – „Определяне на целите и задачите”. Целите направляват анализа. Те следва да дадат представа на заявителя/потребителите, какъв резултат ще бъде предоставен. Същевременно, добре формулираните, ясни и постижими цели очертават задачите. Заявителят утвърждава целите и задачите.

Следващата дейност от етапа „Дефиниране на средата” е A22 - „Определяне на критериите”. Критериите за успех са основните измерители за достигането на целите и се използват за измерване влиянието на променливите рискови фактори върху крайните резултати. Основните изисквания към критериите за успех са [22, 23]:

- да бъдат кратко и ясно формулирани;
- да обхващат всички области на организационната дейност;
- да позволяват количествени и/или качествени измервания на резултатите;
- да позволяват измерване влиянието на всеки риск отделно.

„Определянето на ключовите елементи” - A23, е последната дейност от етапа „Дефиниране на средата”. В нея компонентите на дейността се дефинират като ключови елементи и при тяхното декомпозиране се спазват определени стандарти. Тези компоненти се характеризират с по-малък обхват, но с по-голяма конкретност и дълбочина на описание и анализ [23, 25].

4.3. Идентифициране на рисковете – A3

Идентифицирането на риска е разкриване и дефиниране на рисковете и заплахите, които могат да възпрепятстват постигането на поставените цели. Точното и пълно идентифициране на рисковите събития е от особена важност за ефективното управление на риска.

Идентифицирането на наличните рискове и заплахи включва [23]:

1) Установяване на:
   - наличието на рискови събития;
   - обектите и субектите, които могат да бъдат застрашени;
   - възможни пътища и начини за въздействие.

2) Систематично проучване на всички аспекти на дейността чрез:
   - анализиране на всички дейности, които се извършват за оценявания обект;
   - отчитане на необичайните операции;
   - отчитане на непланирани, но предвидими събития;
   - отчитане на възможността за възникване на събития;
   - анализиране на конкретните нормативни документи.

3) Определяне на тези аспекти на дейността, които могат да причинят вреди.

4) Класифициране на идентифицираните опасности по групи, в зависимост от вида и естеството им.

В резултат от идентификацията на риска се определят потенциалните рискови събития, източниците на риск (включително формулиране на риска, механизми за отключване на риска и техните атрибути). Описват се дейностите. Обратната информация от тази стъпка може да доведе до актуализиране на факторите от средата и показателите за степените на риска. Източниците на риск и потенциалните рискови събития се нанасят в таблицата на факторите (Приложение 2).

Идентифицирането на риска се постига чрез прилагане на разнообразни методи и техники за откриване, дефиниране и документиране на възможните рискове. Най-използваните методи са показани в Приложение 3. Характерно за тях е, че могат да се използват самостоятелно, в комбинации помежду си или с други методи, в зависимост от избрания от оценяващия екип подход за работа.

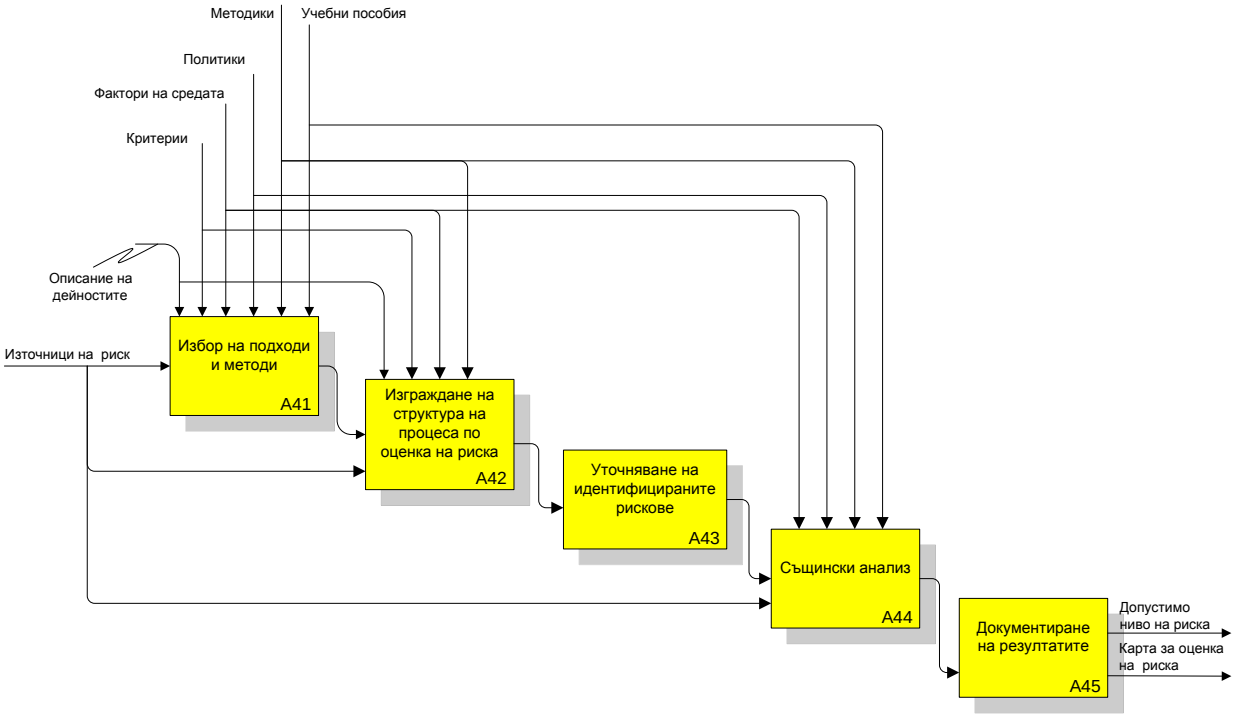
4.4. Анализ на риска – А4

Анализът на риска е комплексен въпрос за разбиране природата на риска и за определяне на неговото ниво. В този етап се изучават всички значими рискове посредством определянето на вероятността за появата им, експозицията и размера на очакваните последици за изследвания обект [22, 23, 25], т.е анализът на риска е разглеждане на идентифицираните рискове и класифицирането им на основата на очакваната вероятност и евентуалните последици. В редица източници анализът на риска включва и дейностите по идентифицирането и оценката на риска [9].

Препоръчително е анализът на асоциирания риск да става с участието на представители от всички структури, проявяващи интерес към резултатите от изследването.

За да се оцени ефективно рискът, на този етап се извършват следните основни дейности (Фигура 4):

- избор на подход и методи за оценка на риска (А41);
- изграждане на работеща структура на процеса за оценка на риска (А42);
- уточняване на идентифицираните рискове, асоциирани към дейностите на този процес (А43);
- анализиране на всеки идентифициран риск с цел определяне на вероятността за проява, очакваните последици, значимостта на тези последствия за достигане на организационните цели (А44);
- документиране на резултатите от анализа на риска (А45).



Фигура 4. Диаграма на дейността „Анализ на риска” (A4)

4.4.1. Изисквания към анализа

В хода на анализа на риска се определят още:

- стойностите на вероятностите за проява на рисковете;
- стойностите на експозицията;
- стойностите на последствията от проява на рисковете, изразени чрез разходите, времевите, качествените и други влияния върху целите;
- най-подходящите лица или организации, както и техники за реализиране на противодействието на риска;
- потенциалното влияние на риска върху реализирането на други организационни дейности.

Изходни продукти от етапа са:

- „Допустими нива на риска” - включват долни и горни гранични стойности;
- „Карта за оценка на риска” - съдържа съответните стойности на параметрите на риска с необходимите атрибути (Приложение 4).

4.4.2. Подходи за измерване на риска

Съществуват различни подходи за измерване и представяне на риска. В зависимост от ресурсите, с които разполага организацията, както и от възприетата от нея стратегия, оценката на риска може да се извършва на различни нива, които се асоциират с прилагането на различни методи и осигуряват различен по точност и надеждност резултат.

Най-общо нивата на оценяване на риска могат да бъдат:

- качествено описание;
- описание на риска чрез косвени характеристики;
- количествено измерване.

В зависимост от конкретната методология мярката може да бъде определена с различни термини – количествени, качествени, едномерни, многомерни или комбинации от

тях (Фигура 5). Във всички случаи използваният подход за измерване на риска трябва да бъде понятен и логичен. Изборът на подход е строго специфичен и варира в зависимост от вида на изследването, наличието и вида на данните за изследвания обект.

Фигура 5. Видове подходи за анализ на риска

При качествените подходи рискът се измерва в качествени термини, задавани с помощта на степени, които позволяват например вероятността за проява на риска да се оцени като “висока”, “средна” или “ниска”, експозицията, като „ниска”, средна” или „висока” и последиците като “средни”, “значими” и “катастрофални”. За тази цел се използват ординални скали. В практиката този подход се прилага по-често чрез методите[1], в които се използват техники, базирани на експертни оценки, обобщаващи опита на ангажираните с решаването на подобен род проблеми експерти от различните области. Обикновено поставените пред изследователите изисквания налагат да се взема решение в среда, характеризираща се с непълна определеност, което прави използването на интелигентните технологии подходящ инструмент за решаването на подобни проблеми.

При количествените подходи рискът се измерва с количествени измерители. Те се основават на математико-статистически модели, изискващи множество и различни по характер технически изпитания, опит и много висока квалификация на лицата, използващи модела. Този подход се характеризира с по-висока степен на детайлност, което дава възможност за оценка на неговото влияние върху реализирането на целите по критерии, като съдържание, качество, време, бойни загуби, ресурси и т.н.

Едномерните подходи разглеждат ограничен брой компоненти (изброените по дефиниция), докато при многомерните подходи се разглеждат допълнителни компоненти при измерването на риска, като видимост, надеждност, безопасност и т.н.

Технологията на работа се определя основно от характера на конкретната задача и от поставените изисквания към конкретното изследване. В тази връзка изследователите/ оценителите преценяват по целесъобразност методите и подходите, състава, областите, степента на изпълнение на дейностите от процеса на управление на риска и елементите на риска за конкретната задача.

Определянето на стойностите на елементите на риска се извършва най-често с помощта на:

- исторически данни (архиви, статистика), от които се извежда математическата зависимост на съществуващите/измерените данни. От тези данни се намира законът на разпределение;
- от експертни знания – лингвистично, посредством методи на мозъчна атака, дискусии и анкети и др. Тези стойности се кодират с числа за изчисляване на математическите зависимости или се моделират с известни функции от размитите множества[2] [21];

[1] Виж Таблица 3.1 от Приложение 3

[2] Теорията на Размитите множества е въведена от Л. Заде [21] и за разлика от точните множества, един елемент може да принадлежи (или не) на размитото множество със степен от интервала [0, 1] вместо само бинарните 1 (принадлежи напълно) или 0 (не принадлежи). Използва се изключително много при експертни системи, при описване на неясни, неточни или несигурни данни.

След определяне на елементите на риска се съставя базата от правила, имаща вида: „Ако експозицията на събитие А е x_1, а неговата вероятност за случване е x_2, то последиците са (обикновено) x_3. От изведените правила се генерира математическата зависимост на изходната величина от входните данни, в случая последицата от риска.

Определянето на тези зависимости (връзка между входа и изхода на модела) спомагат да се генерират множество примерни данни, с които се проследява поведението на модела. Това се постига на по-късен етап от изследването, например с Монте Карло симулации, при зададени допустими грешка/толеранс, праг на приемлив риск и др.

4.5. Оценка на риска – А5

Оценката на риска е специфичен вид дейност, в която се сравняват резултатите от анализа на риска с критериите за риск, за да се определи дали рискът и/или неговата величина са допустими или недопустими. Оценката на риска е свързана със степенуване на рисковете, за да се определи тяхното значение и приоритетност. Тя подпомага решението за въздействие върху риска. Резултатите от оценката на риска са база на всички останали дейности от процеса на управлението му. По своята същност и съдържание този етап е най-сложен, продължителен и критичен по отношение на постиганите крайни резултати.

Оценката на риска не е еднократно действие, а се извършва периодично в хода на изпълнение на дейностите и включва:

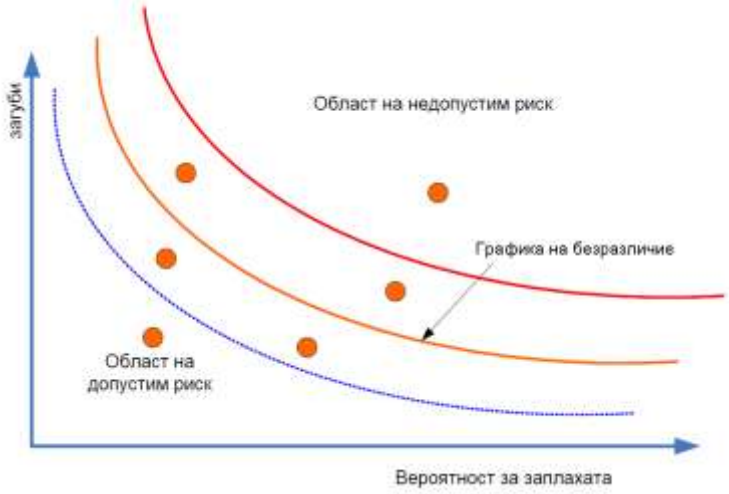
- оценяване на рисковете;
- градиране на рисковете;
- разглеждане на толерантността към риска;
- разглеждане на законите и другите изисквания.

Оценката на риска подпомага решението за въздействие върху риска.

При извършване на оценката на риска могат да се прилагат различни подходи, методи и техники. За всяка конкретна задача се избира подходящ математически инструментариум.

Крайната цел на оценката на риска е вземане на решение на кои рискове да се противодейства. Това е свързано с класифициране на идентифицираните и анализираните рискове към една от следните три категории [6, 23]:

- **приемливи рискове** – които към определен момент от реализирането на организационната дейност се приемат и не изискват прилагане на мерки за редуциране на тяхното влияние, като в същото време продължава следене на тяхното изменение – „област на допустим риск” от Фигура 6. За тези рискове се определят редът и периодичността на наблюдението и докладването на измененията, свързани с техните вероятности и последствия;
- **отхвърлени рискове** – тези, които са определени като несъществени или като несъществуващи за конкретната организационна дейност - графиката на безразличие от Фигура 6;
- **значими рискове** – тези, срещу които се изисква противодействие и които трябва да се приоритизират – „област на недопустим риск” от Фигура 6. В някои случаи рискът може да бъде толкова висок, че да изисква преоценка на реализируемостта на дейността като цяло. Наличието на подобни рискове трябва да се подчертава изрично в докладите пред ръководството на организацията [23].



Фигура 6. Криви на представяне на областите на риск, в зависимост от вероятността и последицата/ загубите.

Класифицирането и приоритизирането на рисковете се извършва по критерии, дефинирани в рамките на организационната политика в областта на управление на риска, които се отразяват в плана за управление на риска [23]. По този начин може да се направи първоначална оценка кои от идентифицираните рискове следва да се управляват.

Приоритизирането на рисковете се налага от ограничеността на ресурсите за реализиране на дейностите по планирането на отбраната и за управление на асоциираните към тях рискове. По тази причина е невъзможно предприемане на ефективни мерки за редуциране влиянието на всички идентифицирани рискове. Значимостта на различните рискове се изменя в хода на изпълнение на дейностите под влиянието на вътрешни и външни фактори и затова е важно във всеки момент да се познават значимите от тях, срещу които да се разработват мерки за противодействие. В повечето случаи критериите за приоритизиране на рисковете са субективни и са базирани на опита на експертите [23].

Съществуват четири случая, при които на идентифицираните рискове може да не се противодейства [22, 23]:

- при пренебрежимо малка вероятност за проява на рисковете;
- когато последствията от рисковете не са свързани с реализирането на дейността;
- когато размерите на очакваните последствия са незначителни за поставените цели;
- когато източниците на риск са извън рамките и обхвата на конкретната дейност.

Оценката на риска трябва да отчита чувствителността на извършваните изчисления към грешки. Склонността към поява на оптимизъм при субективната оценка на риска е друга особеност, която следва да се отчита. Прилагането на количествени методи при оценката на риска е в състояние да намали оптимистичната тенденция в оценките, тъй като в някои случаи тя може значително да повлияе върху обективността и точността. При определени обстоятелства се изисква разработване на кризисни планове за управление на рисковете, трансформирали се в проблеми. Това се налага при:

- достигане на критични точки в развитието на риска, без да е намерено ефективно противодействие;
- съществуване на вероятност да не се намери ефективно противодействие на някой от идентифицираните и анализирани рискове.

Когато срещу определен риск не са предприети мерки за редуциране на неговото влияние, следва да се определят индикатори за изменението и проявата на този риск.

Промените в индикаторите показват нарастване на вероятността за проява на риска и необходимостта от пристъпване към изпълнение на кризисния план за противодействие [23].

Мерките, предприети за редуциране на риска, могат да доведат до поява на вторични рискове, които следва също да се идентифицират и анализират. Оценката на вторичните рискове се извършва по описания начин.

4.6. Противодействие на риска – А6

Противодействието на рисковете е процес на избор и прилагане на мерки, целящи редуцирането на риска до определените приемливи нива. Този процес дефинира точното съдържание на мерките за противодействие, времето за което ще се изпълняват тези мерки, участниците в процесите и техните функции.

Мерките за противодействие на риска могат да бъдат насочени към намаляване на вероятността за проява на риска, към намаляване на експозицията, към ограничаване на размера на очакваните последици или и към трите.

Разработването на мерки за противодействие на риска може да изисква съвместна работа и сътрудничество с различни вътрешни и външни за организацията структури.

Основни изисквания към мерките за противодействие на риска са те да бъдат икономични, ефективни и ефикасни. Мерките са специфични за всяко рисково събитие и се свързват със съответна стратегия за противодействие. Нанасят се в таблицата на Препоръчителните мерки за управление и контрол на идентифицираните рискови събития, според оценката на риска (Приложение 6).

Противодействието на всеки свързан с определена дейност риск се асоциира със съответна стратегия за противодействие, включваща [6, 22, 23, 25]:

- ограничаване на риска до определено приемливо ниво в рамките на общите изисквания към дейността;
- трансфериране на рисковете от високо ниво към външни организации;
- смекчаване на риска посредством намаляване на влиянието му върху целите;
- приемане на риска без необходимост от предприемане на специални действия за контролирането му.

При избора на стратегия за противодействие срещу риска трябва да се отчитат [23]:

- възможността за прилагане на стратегията и постигане на целите;
- очакваната ефективност от прилагането на стратегията;
- рентабилност на прилагането на избраната стратегия от гледна точка на влаганите ресурси, необходимото допълнително време и др.

Основните подходи за противодействие на риска са [23]:

- редуциране на вероятността за проява на риска чрез извършване на промени в дейностите или в средата, в която тя се реализира;
- редуциране на размера на вероятните последици от риска чрез подходящи действия;
- избягване на риска посредством премахване на причините за него;
- трансфериране на риска чрез разпределяне на отговорностите за риска между други лица и организации, както и чрез застраховане, запасяване и т.н.

Тези изисквания и параметри се реализират чрез Плана за управление на риска[3] - краен продукт от дейността „Противодействие на риска” – А6 (Приложение 7).

[3] В някои литературни източници фигурира като „Регистър на риска”

4.7. Мониторинг и проследяване – A7

Асоциираният риск може да се промени под въздействието на нови външни и вътрешни фактори. Затова от съществена важност са непрекъснатото наблюдение и редовният преглед на действията, свързани с неговото управление. Честотата на прегледите на риска зависи от мащаба, обхвата и продължителността на организационната дейност. В идеалния случай тази честота е функция на времевите периоди и на възникнали значими за изпълнението събития. Като правило препоръчваната периодичност на прегледите на риска е два месеца [23]. Специални мерки за преглед на риска е необходимо да се вземат, когато:

- започва нов етап от реализацията на дейностите по сценариите;
- приет е нов подход или е променен обхватът на сценариите;
- налице са съществени промени в средата за реализиране на организационната дейност.

Системата за наблюдение на риска включва разработване на индикатори, с помощта на които се определят измененията в статуса на риска. Индикаторите служат за определяне степента на трансформация на риска в проблем, както и необходимостта от предприемане на управленски действия за редуциране на риска [23].

Всички коригирани изменения вследствие на промените в средата се нанасят в документа „Коригиран план за управление на риска”.

5. Роли

В таблица 1 са показани основните роли и отговорности на длъжностните лица, участващи в процеса на управление на риска. Предложената структура може да се различава по обем, обхват, състав и подход на работа и е специфична за всеки отделен случай.

Ролите могат да бъдат възложени на органи, структури и/или длъжности от различни нива, като вземането на решение с отчитане на риска е отговорност на всеки ръководител. Например ролята на „Съвет” може да бъде възложена на някои от съществуващите съвети в Министерството на отбраната, като „Съвет по отбранителни способности”, „Програмен съвет”, „Съвет по въоръженията” и др., ролята на „Ръководител” на директор на дирекция и т.н.

Таблица 1

Ръководител
• Основният служител, отговорен за цялостния процес по управление на риска. • Осигурява необходимите ресурси за изпълнение на процеса на управление на риска. • Възлага задачи и делегира пълномощия към съответните служители. • Отчита се пред „Заявителя” и „Съвета” по въпросите на управление на риска.
Координатор
• Разработва и поддържа политиката за управление на риска, процедурите и плановете. • Гарантира, координира и изпълнява процеса за управление на риска. • Осигурява или организира обучение по управление на риска за персонала, включен в дейностите по управление на риска. • Осигурява необходимите инструменти за управление на риска (контролни листове, план за управление на риска и т.н.). • Изготвя отчети за управлението на риска. • Осигурява съответствие с политиката и изискванията от по-високо ниво. • Подпомага ръководителя във всички дейности по управлението на риска,

включително със съвети за използване на ресурсите и възлагане на собствеността на риска. • Срочно докладва проблемите за управление на риска на ръководителя. • Оценява прилагането на управление на риска и наблюдава, контролира или одитира (евентуално чрез независими оценители) управлението на риска.
Заявител на изследването
• Изпълнява изготвената стратегия за риска. • Докладва за състоянието на притежавания от него риск (например чрез актуализиране на Плана за управление на риска) на Координатора. • Предлага промени в политиката за управление на риска, процедурите и плановете.
Съвет
• Координира дейностите по управление на риска. • Осигурява и разпределя необходимите ресурси, когато те са извън отговорностите на ръководителя.

6. Заключение

Представеният Модел за управление на риска при планирането на отбраната и въоръжените сили е разработен в контекста на стратегическото планиране на националната сигурност и дългосрочното планиране за развитието на способностите на въоръжените сили. В документа, управлението на риска е описано като формализиран процес, в рамките на който рисковете систематично се идентифицират, анализират, оценяват, въздейства им се, след което се следят промените и резултатите от тяхното развитие.

Моделът съответства на най-добрите съществуващи практики в областта на управлението на риска, а прилагането на предложените математическите методи дава не само теоретични насоки, но и практическа полза, изразяваща се в конкретни резултати при планирането на обраната и въоръжените сили. Тези подходи, методи и техники за оценка на риска при планирането на отбраната и въоръжените сили могат успешно да бъдат прилагани от експерти, ръководители и политически лица при развитието на стратегическия мениджмънт в сектора. Прилагането им позволява количествено да се оценят рисковете, както и да се изследват възможните им комбинации чрез симулации и анализ на чувствителността. Това намалява до минимум човешкия фактор и минимизира „недостатъка на средните стойности” [18][4] при вземането на решения, свързани с тяхното управление.

Приемането и утвърждаването на Модела за управление на риска при планирането на отбраната и въоръжените сили като официален документ ще запознае военната общественост с важността на този тип анализ и ще определи методическата рамка, свързана с изпълнението на тази комплексна задача. Важна негова роля е да подпомогне промяната в подходите за вземане на решения в областта на отбраната, като информира лицата, вземащи решения, че управлението на риска може да бъде полезен инструмент в стратегическия мениджмънт, само ако е добре организирано, провеждано и е интегрирана част от него.

---

[4] Savage, S, The Flaw of Averages: Why We Underestimate Risk in the Face of Uncertainty, John Wiley & Sons, Inc., Hoboken, New Jersey, 2009

Използвана литература

[1]. AFMC Pamphlet 63-101. Risk Management, 1997.
[2]. American Systems Corporation. Risk Management Process and Implementation, 2003.
[3]. Broadleaf Capital International PTY LTD. The Australian and New Zealand Standard on Risk Management, 2004.
[4]. Department of Commerce. Project Risk Management Guideline, 2004.
[5]. Enterprise Risk Management – Integrated Framework, 2004.
[6]. Georgiev V. Program and Project Management. Sofia. Avangard Prima, 2008, ISBN 978-954-323-387-8.
[7]. Grant Thornton. Risk – the Achilles heel of organizational progress, 2004.
[8]. Hillson, D., Use a Risk Breakdown Structure to Understand Your Risks, 2000.
[9]. ISO/IEC 31010: 2009, Risk management – Risk assessment techniques, 2009.
[10]. ISO/IEC Guide 73:2009. Risk management – Vocabulary, 2009.
[11]. Karel de Bakker. Risk Management Planning – How Much is Good Enough?, 2002.
[12]. NORSOK Standard. Risk and Emergency preparedness analysis, 2001.
[13]. PMI Standards Committee. A Guide to the Project Management Body of Knowledge, 1996.
[14]. Project Management Fundamentals, 2004.
[15]. Quantitative Risk Assessment System (QRAS) Version 1.6 User’s Guide, NASA, April 9, 2001.
[16]. Risk Management in Projects – 17 Steps to Success, 2004.
[17]. Risk Support Team. Risk Management Assessment Framework, 2004.
[18]. Savage, S, The Flaw of Averages: Why We Underestimate Risk in the Face of Uncertainty, Jnhn Wiley & Sons, Inc., Hoboken, New Jersey, 2009.
[19]. The Association for Project Management. Project Risk Analysis and Management, 2000.
[20]. University of Success. Risk Management Policy, 2005.
[21]. Zadeh, L. A., "Fuzzy sets", Information and Control, 8, 338–353, 1965.
[22]. Георгиев В. Програмно и проектно управление в отбраната и въоръжените сили. София. Авангард Прима, 2007.
[23]. Георгиев В. Управление на риска – учебно пособие. Военно издателство, 2005.
[24]. Георгиев В. Управлението на риска като инструмент на програмното управление. София. Военен журнал, 2005.
[25]. Георгиев В., Е. Тимева. Управление на проекти. Същност, съдържание, процеси и взаимодействие – учебно пособие. Военно издателство, 2006.
[26]. МО, Единна практическа методика за оценка на риска за здравето и безопасността при работа на кадровите военнослужещи и гражданските лица от Министерството на отбраната, Българската армия и структурите на подчинение на министъра на отбраната. София. Военно издателство, 2008.
[27]. Слатински Н., Лекция 3 от поредицата „Четири лекции” - „Увод в управлението на риска (В помощ на започващия дейността си риск-мениджър)”, http://nslatinski.org/?q=bg/node/297 , посетен октомври, 2010.
[28]. Стоянов В., Златева П., Киров Г., Стоянов К. „Приложение на размитата логика при прогнозиране на потенциалните загуби от природни бедствия”, Втора национална научно – практическа конференция по управление на извънредни ситуации и защита на населението, БАН, София, 2007.

Приложение 1

Утвърждавам:

……/……../

ПРОГРАМА

за реда, начина и периодичността за оценка на риска при планирането на отбраната и въоръжените сили

I. Организация и координация на дейностите по оценка на риска

1. Подбор на специалистите, които ще извършват оценката на риска - трябва да могат да анализират рисковите фактори и ситуации; да оценяват риска и да определят приоритетите; да оценяват наличните мерки; да предлагат достъпни и ефикасни мерки за предотвратяване и намаляване на риска; да работят в екип.
2. Координация на дейността съгласно програмата - при отделните етапи между различните нива и екипи, участващи в оценката на риска.
3. Формиране на основния екип (при централизирания способ за работа) и длъжностните лица, участващи от страна на поделения и дирекции.
4. Осигуряване на сътрудничество от страна на военнослужещите и цивилните служители чрез анкети, дискусии и консултации.
5. Създаване на стройна организация по спазване на сроковете, заложени в програмата и изготвяне на изискуемата в нормативните разпоредби документация.

II. Подходи и методи за оценяване на риска

1. Информационен - използване на богата база от данни от научна, техническа, законодателна и справочна литература.
2. Анкетен - провеждане на утвърдени тематични анкети сред личния състав, свързани с влиянието на факторите.
3. Адаптационен - адаптиране на методите за оценка на риска за конкретните нужди и спецификата на процеса.
4. Подбор на оценителите съгласно тяхната квалификация и опит.
5. Осигуряване на достоверност на резултатите.
6. Обзор и анализ на резултатите.

III. Оценители на риска

1. Ръководител
2. Координатор ……..
3. Специалист по ……..
4. Специалист по ……..

IV. Необходими ресурси

1. Информация по т. V от програмата.
2. Кадри по т. III от програмата.
3. Време за изпълнението и оценката на риска - до ……. г.
4. Финансови средства.

V. Осигуряване на информация на оценителите

1. Наблюдения върху работната среда.
2. Анкети.
3. Резултати от измервания.
4. Сведения.
5. Нормативни разпоредби.
6. Вътрешни правила и норми.
7. Ръководства и правилници.
8. Информация от национални институции.
9. Специализирани издания.

VI. Етапи, последователност и срокове за изпълнение

1. Определяне на обхвата на дейността, съгласно нормативните документи и спецификата на дейността.
2. Класифициране на дейностите с оглед вероятността за настъпване на рисково събитие.
3. Идентифициране на риска.
4. Структуриране на елементите на риска.
5. Определяне на степента на риска.
6. Изготвяне на приоритети на препоръчителните мерки.
7. Вземане на управленско решение за осъществяване на препоръчаните мерки. В зависимост от необходимите ресурси, финансовата стойност и значението им за отстраняване на рисковете.
8. Осъществяване на решенията.
9. Валидизиране на резултатите.

VII. Начини за допитване и консултации с личния състав

1. Анкетни листове – по видове фактори.
2. Обратна връзка.

Приложение 2

ФАКТОРИ И ПОТЕНЦИАЛНИ РИСКОВЕ

1. Мисия/Задача: ……..	**2. Дата/Час Група: …. ……..…… Начало: …… Край: ……**	**3. Дата на попълване: …….**
4. Попълнил: ……..……. (Звание, Име, Презиме, Фамилия, Заемана длъжност)		

5. Фактори	**6. Потенциални рискови събития**
I. Наименование на Фактор 1 1.1. Източник на риск 1.2. ……. 1.3. ……. …	1.1.1. ……. 1.1.2. ……. 1.1.3. …….
II. Наименование на Фактор 2 2.1. Източник на риск 2.2. ……. 2.3. ……. …	2.1.1. ……. 2.1.2. ……..……. 2.1.3. …….

При определянето на факторите и рисковите събития трябва да се търсят отговори и на следните групи въпроси:

1. Възможни ограничения/затруднения за дейностите
- Съществуват ли ограничения по отношение на политики, стратегии, планове, мисии и задачи?
- Какви са ресурсните ограничения?
- Какви други пречки може да възникнат пред осъществяването на набелязаните цели?

2. Възможни рискове, свързани с дейностите
- Какъв е рискът от непредприемане на нищо? (оставяне на нещата, както са)
- Може ли да се измери рискът? (количествена оценка)
- Къде (при кои дейности) и до каква степен/доколко голям риск е допустим?
- Има ли събития извън осъществявания контрол? Доколко те засягат желаните способности?

3. Основни заплахи, потенциални проблеми
- Какви мерки/действия са наложителни?
- Трябва ли веднага да се предприемат тези мерки (да се действа) или може да се изчака?
- Колко спешно е тяхното разрешаване?

Приложение 3

Сравнителен анализ на най-използваните методи и средства в дейностите на процеса по управление на риска

1. Приложение на методите и средствата

Първата класификация, от анализа, показва приложимостта на методите в следните основни дейности и поддейности от процеса по управление на риска [9]:

- идентифициране на риска (А3);
- анализ на риска (А4), при определянето на последствията, вероятността и допустимото ниво на риска;
- оценка на риска (А5).

В Таблица 3.1 е описана степента на приложимост на съответните методи и средства за изброените по-горе дейности от процеса по управление на риска.

2. Фактори, влияещи върху избора на методите и средствата

Следващата класификация, характеризира тези методи по отношение на [9]:

- сложността на проблема и необходимите методи за анализ;
- степента на несигурност на метода при управлението на риска;
- размера на вложените средства (време, ниво на експертиза, данни, цена и др.);
- способността на метода да осигурява количествено измерим изходен параметър.

Примери за методите за оценка на риска са изброени в Таблица 3.2, където за всеки метод са дадени оценки („високо”, „средно”, „ниско”) по отношение на тези критерии.

Таблица 3.1

Методи и средства	Дейности от процеса по управлението на риска				
	Идентификация на риска	Анализ на риска			Оценка на риска
		Последици	Вероятности	Допустимо ниво на риска	
Мозъчна атака	СП	НП	НП	НП	НП
Структурирани и полу-структурирани интервюта	СП	НП	НП	НП	НП
Метод Делфи	СП	НП	НП	НП	НП
Списък на рисковете	СП	НП	НП	НП	НП
Предварителен анализ на опасностите	СП	НП	НП	НП	НП
Изследване на опасностите и дейностите (HAZOP[5])	СП	СП	П	П	П
Анализ на опасностите и точките на критично управление	СП	СП	НП	НП	СП
Оценка на риска на заобикалящата среда	СП	СП	СП	СП	СП
Структуриран SWIFT[6] (какво, ако)	СП	СП	СП	СП	СП
Анализ на сценария	СП	СП	П	П	П
Анализ за влиянието на факторите върху работата	П	СП	П	П	П
Анализ на основната причина (анализ на единичната загуба)	НП	СП	СП	СП	СП
Анализ на способа на грешките и въздействието им (FMEA[7] и FMECA[8])	СП	СП	СП	СП	СП
Дърво на отказите	П	НП	СП	П	П
Дърво на събитията	П	СП	П	П	НП
Причинно-следствен анализ	П	СП	СП	П	П
Анализ на причината и въздействието	СП	СП	НП	НП	НП
Анализ на нивата за защита	П	СП	П	П	НП
Дърво на решенията	НП	СП	СП	П	П

[5] HAZOP – HAZard and OPerability study, техника за структурирано и систематично проучване на планираните или съществуващите процеси и дейности, с цел идентифициране и на проблеми, водещи до риск.
[6] SWIFT – Structured What-IF Technique
[7] FMEA – Failure Mode and Effects Analysis
[8] FMECA – Failure Mode and Effects Critical Analysis

Анализ на прага на издръжливост	СП	СП	СП	СП	П
Анализ „Папийонка”	НП	П	СП	СП	П
Надеждна поддръжка	СП	СП	СП	СП	СП
Скрит анализ	П	НП	НП	НП	НП
Модел на Марков	П	СП	НП	НП	НП
Монте Карло симулации	НП	НП	НП	НП	СП
Бейсови статистически методи и мрежи	НП	СП	НП	НП	СП
FN криви	П	СП	СП	П	СП
Индекси на риска	П	СП	СП	П	СП
Матрици на вероятностите/последиците	СП	СП	СП	СП	П
Разходи-ползи	П	СП	П	П	П
Многокритериален анализ	П	СП	П	СП	П
СП - Силно приложим НП - Неприложим П - Приложим					

Таблица 3.2

Наименование на метода/техниката за оценка на риска	**Описание**	**Връзка с въздействащите фактори**			**Предоставя количествен резултат**
		Ресурси и способности	**Същност и степен на неточност**	**Сложност**	
СПРАВОЧНИ МЕТОДИ					
Списък на рисковете	Проста форма за идентифициране на рисковете. Техника, която изброява типичните рискове, които трябва да се класифицират. Потребителите използват вече изготвени списъци, кодове или стандарти.	ниски	ниски	ниска	не
Предварителен анализ на опасностите	Прост индуктивен метод за анализ, чиято цел е да идентифицира опасностите, опасните ситуации и събитията, които могат да причинят вреда на дадена организация, процес, въоръжение или система.	ниски	високи	средна	не

Наименование на метода/техниката за оценка на риска	Описание	Връзка с въздействащите фактори			Предоставя количествен резултат
		Ресурси и способности	Същност и степен на неточност	Сложност	
ПОДДЪРЖАЩИ МЕТОДИ					
Структурирани интервюта и мозъчни атаки	Начин за набиране на идеи и оценки и/или ранговането им от експертен екип. Мозъчната атака може да бъде стимулирана чрез специфични техники за интервюиране на един или няколко експерта.	ниски	ниски	ниска	не
Метод Делфи	Начин за набиране на експертно мнение, което може да подкрепи източника и да окаже влияние върху идентификацията, оценката на вероятностите експозицията и последствията, оттам и върху оценката на риска. Това е универсална техника за изработване на консенсус между експертите.	средни	средни	средна	не
Структуриран SWIFT (какво, ако)	Система за мотивиране на екипа при идентифицирането на рисковете. Обикновено се използва по време на семинари и е свързан с анализа на риска и техниките за оценяване.	средни	средни	-	не
Анализ на прага на издръжливост	Той се изследва с влиянието на човешкия фактор върху разглеждания обект. Може да се използва за оценка на влиянието на човешките грешки върху работата на обекта.	средни	средни	средна	да
МЕТОДИ ЗА АНАЛИЗ НА СЦЕНАРИИТЕ					
Анализ на основната причина (анализ на единичната загуба)	Загубите (последствията) се анализират, за да се установи естеството на причините довели до тях. Набелязват се мерки за подобряване на системата. Анализът разглежда управлението на системата и начините за нейното подобрение.	средни	ниски	средна	не
Анализ на сценария	Създават се въображаеми или екстраполирани на действителността бъдещи сценарии, след което се обсъждат различните рискове в тях с презумпцията, че някои от тези рискови събития могат да се случат.	средни	средни	средна	не/да
Влияние на факторите върху работата	Тази техника предоставя анализ за това как рисковете оказват влияние върху дейността на организацията. В този анализ се идентифицират и определят необходимите за управлението ѝ способности.	средни	средни	средна	не

Наименование на метода/техниката за оценка на риска	Описание	Връзка с въздействащите фактори			Предоставя количествен резултат
		Ресурси и способности	Същност и степен на неточност	Сложност	
Дърво на отказите	Това е структурен модел, представящ в графична йерархична форма логиката на връзките между събитията, причиняващи отказите в сложна система. С този модел се анализира функционирането на системата по отношение поведението на изграждащите я елементи и във връзка със съставянето на крайна оценка за нейната надеждност и асоцииран риск.	високи	високи	средна	да
Дърво на събитията	Използва индуктивно мислене, за да определи вероятностите на различните начални събития във възможни резултати.	средни	средни	средна	да
Причинно-следствен анализ	Комбинация от анализ на дървото на грешките и на дървото на събитията, който позволява включване на времеви закъснения. Разглеждат се както причините, така и последствията от едно начално събитие.	високи	средни	висока	да
Анализ на причините и въздействието	Въздействието може да има редица допълващи го фактори, които могат да бъдат групирани в различни категории. Допълващите фактори често се идентифицират чрез мозъчна атака и се изобразяват с дървовидна или разклонена графика.	ниски	ниски	средна	не
МЕТОДИ ЗА ФУНКЦИОНАЛЕН АНАЛИЗ					
Способ на грешките и въздействието им (FMEA и FMECA)	FMEA (Failure Mode and Effect Analysis) Анализът на способа на грешките и въздействието им е техника, която идентифицира грешките, механизмите за възникването им и въздействието, което те оказват. Съществуват няколко вида анализ FMAE: продуктов, който се използва за елементи или продукти; системен - за системи; процесен – използван в производството; за услуги и софтуер.	средни	средни	средна	да
Скрит анализ (Sneak circuit analysis)	Методология за откриване на грешките в структурата. Служи за анализ на скрити (латентни) състояния в хардуер и/или софтуер, сложни системи и др., които да са причина за настъпването на нежелано събитие. Тези състояния се характеризират с произволна същност и способност да не бъдат откривани по време и на най-задълбочените системни тестове. Скритите състояния могат да причинят неточност в дейността, загуба на активи в системата, забавяния в програмите и дори смърт или нараняване на персонала.	средни	средни	средна	не

Наименование на метода/техниката за оценка на риска	Описание	Връзка с въздействащите фактори			Предоставя количествен резултат
		Ресурси и способности	Същност и степен на неточност	Сложност	
Изследване на опасностите и дейностите (HAZOP)	Основен процес за идентифициране на рисковете, с който се определят възможните отклонения от очакваната или желаната дейност на организацията. Използва система, основана на колонтитул. Оценява се сериозността на отклоненията.	средни	високи	високи	не
Анализ на опасностите и точките на критичното управление	Методична, проактивна и предупреждаваща система за оценяване на качеството на продукта, надеждността и сигурността на процесите чрез измерване и наблюдение на специфични свойства, удовлетворяващи определени норми.	средни	средни	средни	не
МЕТОДИ ЗА ОЦЕНКА И КОНТРОЛ НА УПРАВЛЕНИЕТО					
Анализ на нивата за защита	Известен още и като „Бариерен анализ”. Позволява оценяването на управлението и неговата ефективност.	средни	средни	средни	да
Метод на „Папийонката”	Под формата на графики, се описва и анализира пътя на риска - от опасности до последствия, както и слабостите в управлението. Може да се разглежда като комбинация от логиката на метода „Дървото на грешките”, анализиращ причините за дадено събитие (представени като възела на папийонката) и „Дърво на събитията”, анализиращо последствията.	средни	високи	средни	да
СТАТИСТИЧЕСКИ МЕТОДИ					
Модел на Марков	Известен и като анализ на състоянието и пространството. Използва се често за анализ на сложни системи, които могат да съществуват в различни състояния, включително разнообразни понижени състояния.	високи	ниски	високи	да
„Монте Карло” симулации	Симулацията „Монте Карло” се използва за установяване на сумата от измененията в системата, за определен брой входящи данни, където всяка притежава определено разпределение, като те са свързани с изходните данни чрез определени взаимоотношения. Анализът може да се използва за специфичен модел, където взаимодействията между отделните входящи данни могат да се определят математически. Входящите данни могат да се основават на разнообразни видове разпределение съгласно естеството на неточностите, които представляват. За оценка на риска често се използват триъгълни или бета разпределения.	високи	ниски	високи	да

Наименование на метода/техниката за оценка на риска	Описание	Връзка с въздействащите фактори			Предоставя количествен резултат
		Ресурси и способности	Същност и степен на неточност	Сложност	
Бейсови статистически методи и мрежи	Бейсовата статистика дава възможност да се оцени плътността на вероятностното разпределение на параметрите по наличните данни. За да се минимизира грешката се избира модел с такива параметри, при които плътността на вероятността е най-голяма. Структурата от елементи и факти, участващи в модела на качеството, се представя като ориентиран ацикличен граф, чиито върхове представят (несигурни) променливи с известни условни вероятностни разпределения, а дъгите показват отношенията между тези променливи. Моделиращата техника се основава на теоремата на Бейс. Мрежата на Бейс представя както количествени, така и качествени спецификации. Подходът дава полезни резултати дори при непълна и несигурна информация и е подходящ да бъде използван в ранните етапи на реализация на проекта, например при разработване на архитектура	високи	ниски	високи	да

Приложение 4

КАРТА ЗА ОЦЕНКА НА РИСКА

1. Мисия/Задача: ……..	**2. Дата/Час Група: ….** ……..…… **Начало: ……** **Край: ……**	**3. Дата на попълване:** …….

4. Изготвил:
……..…….
(Звание, Име, Презиме, Фамилия, Заемана длъжност)

Вид риск	**Вероятност (В)**	**Експозиция (Е)**	**Последица (П)**	**Риск (Р) Р=В*Е*П**	**Класификация**
5	**6**	**7**	**8**	**9**	**10**
I.Фактор 1.1 …….					
1.2 ...…..					
1.3 ……..					
II.Фактор 2.1 …….					
2.2 ...…..					
……					

Определянето на компонентите и нивото на риска за мисията/задачата, се определят в зависимост от избрания подход и метод за работа. При използването на качествени подходи за определянето им може да се използват степените със съответната им числова стойност от Таблици 5.1 – 5.4 в Приложение 5.

Приложение 5

ПРИМЕРИ ЗА МАТЕМАТИЧЕСКИ МОДЕЛ ЗА ОЦЕНКА НА РИСКА ПРИ ПЛАНИРАНЕ НА ОТБРАНАТА

Моделът за управление на риска при планирането на отбраната и въоръжените сили е апробиран с помощта на примери, в зависимост от това дали съществува, или не акумулиране на риск, т.е. дали появата на един риск може да води до появата на втори, а той от своя страна до появата на трети и т.н. За разгледаните примери са направени следните допускания:

1. Определена е работна група за оценката на риска по сценарии.
2. Изготвена е програма за дейността по оценяването на риска (Приложение 1). Програмата съдържа задължителния минимум от данни, описани в т. 4.1.3.
3. Дефинирани са параметрите на средата, ограниченията и допусканията, в които ще се реализира изследването. Определени са целите, задачите, критериите и ключовите елементи.
4. Идентифицирани са наличните рискове (Приложение 2).

В **пример 1** е демонстриран модел за оценка на риска, чрез използване на качествени подходи за измерване на риска. На практика са приложени основните дейности по управлението на риска, описани в модела на дейностите.

В **пример 2** е илюстриран математически модел за оценка на риска с използване на качествени и количествени подходи за изчисляване на риска в съчетание с техники и средства за математическо симулиране.

В **пример 3** е илюстрирано използването на конкретен математически метод за оценка на сценарий по време и неговото остойностяване [15]. Това става чрез Техниката за преглед и оценка на програми, PERT (Program Evaluation and Review Technique).

Всички примери от това приложение са демонстративни с цел представяне на различни методи, добри практики и известни техники при изпълнение на стъпките от предложения модел на дейностите. Те нямат характера на практическо ръководство за приложение на представения модел за управление на риска, нито задължават използването на посочения софтуер.

Пример 1 - без акумулиране на риск

В предложения пример е демонстриран модел за оценка на риска с използване на качествени методи за анализ. Примерът е реален и разработен през 2010 г. в отдел „Операционен анализ” при определянето на риска за реализирането на инициатива по въвеждането на „Концепция за прилагане на организационно-архитектурното моделиране в отбраната”.

В този случай определянето на елементите на риска – вероятност, експозиция (честота) и последици е извършено с лингвистични, качествени термини, с помощта на експерти. Рискът е функция от тези елементи и се измерва чрез степени, след съответно кодиране. Кодирането на лингвистичните експертни оценки служи за унифициране на тези оценки към една предварително избрана скала. Така кодираните коефициенти (числа) се използват за изчисленията в математическия модел. За всяка конкретна област се прилага експертиза, съответстваща на характерната за тази област. Например, експертното разбиране за „малка” последица в една област може да е загуба от 200 лв., но за друга – това да е загуба

от 5300 лв. И в двата случая оценките са правилно съобразени с обхвата, важността и характера на дейността, което води до единна стойност на коефициента.

Кодирането на вероятностите (В) с коефициенти е направено съгласно НАРЕДБА 5[9] за реда, начина и периодичността на извършване на оценка на риска, показано в Таблица 5.1.

Таблица 5.1

Коефициент	Описание на вероятността
0,2	Практически невъзможна
0,5	Малко вероятна
1,0	Възможна в определени случаи
3,0	Вероятността е под средната
5,0	Вероятността е средна
7,0	Вероятността е над средната
10,0	Висока

Експозицията (Е) се кодира, както е посочено в Таблица 5.2.

Таблица 5.2

Коефициент	Описание на експозицията
0,5	Твърде ниска, много рядка – под 1 път месечно
1,0	Много ниска – до 1 час седмично
2,0	Ниска - до 1 час дневно
3,0	Средна - до 1/3 от работното време
6,0	Достатъчно висока - до 1/3 от работното време
8,0	Много висока - над 1/3 от работното време
10,0	Непрекъснато - през цялото работно време

Последиците (П) се кодират, както е посочено в Таблица 5.3.

Таблица 5.3

Коефициент	Описание на последиците
1,0	Малки
3,0	Значителни
7,0	Сериозни
15,0	Опасни
40,0	Катастрофални

След като са определени елементите на риска се намира ранговото число на риска. То се получава по формулата:

$$P=B*E*П \qquad (5.1)$$

Забележка: В случаите, когато експозицията не участва във формула (5.1), то крайните оценки за ранговите числа на риска от таблица 5.4 се умножават с коригиращ коефициент 1/10.

[9] издадена от Министерство на труда и социалната политика и Министерство на здравеопазването, обн., ДВ, бр. 47 от 21 май 1999 г.

В зависимост от това в коя част на граничния интервал попада изчисленото рангово число, се извършва класифициране на риска. Това се прави с цел определяне на допустимостта и необходимостта от прилагане на мерки за противодействие.

Класифицирането на риска се извършва в степени по Таблица 5.4.

Таблица 5.4

Степен	Рангово число	Описание на риска
I	до 20	Незначителен, твърде ограничен риск
II	21-70	Приемлив, неголям риск – необходимо е внимание
III	71-200	Умерен риск – необходими са мерки за намаляването му
IV	201-400	Сериозен риск – следва незабавно предприемане на мерки
V	над 400	Висок риск – прекратяване на дейността до отстраняване на риска.

Всяко рисково събитие се класифицира по фактори, само за себе си. Недопустимо е стойностите на идентифицираните рискови събития да се сумират и след това да се сравняват по посочената класификация, както и да се осредняват техните стойности.

Всяка от стойностите в горните таблици може да се представи процентно, като се нормира към интервала 0 ÷ 100 %. Нормирането за стойностите от тези таблици се извършва по познатата формула:

$$NORMx_i = \frac{x_i - \min}{\max - \min}\%, \qquad (5.2)$$

където ***min*** и ***max*** са долната и горната граница на интервала, а x_i е текущата стойност, която се нормира. Така за елемента „вероятност” (от табл. 5.1) процентните стойности са:

Коефициент	Процентно съответствие
0,2	0,00%
0,5	3,06%
1	8,16%
3	28,57%
5	48,98%
7	69,39%
10	100,00%

От това съответствие се вижда, че средна вероятност за проявяване на дадено рисково събитие се кодира с „5” в интервала 0,5 ÷ 10, което отговаря на 48,98 % и съвпада напълно с експертното разбиране за средна вероятност.

Аналогично за останалите елементи на риска (табл. 5.2, 5.3 и 5.4) процентните стойности се изчисляват по формулата 5.2. В частност, за описаните степени на риска (таблица 5.4) те са: до 0,26% за I степен, до 13,42% за II степен, до 47,63% за III степен и над 48% имаме сериозен риск от IV степен. За последната степен V рискът е висок и се прекратяват всякакви дейности до отстраняването му.

.

Резултатите от определените елементи на риска със съответните пояснения и изчисления на ранговото число на риска – степен и описание – се получават за всяко рисково събитие. Същите се нанасят в Карта за оценка на риска. Формата на картата е дадена в Приложение 4.

За опростяване на работата на оценителите е целесъобразно да се работи със стойностите на коефициентите от таблиците, а при необходимост да се нормира само резултатът (стойността) на риска.

В Таблица 5.5 е дадена карта за оценка на идентифицираните рискове за конкретния пример, а в Таблица 5.6 – препоръчителните мерки за управление и контрол на идентифицираните рискови събития според оценката на риска.

За по-голяма нагледност на резултата се допуска обединяване на тези две таблици.

КАРТА ЗА ОЦЕНКА НА РИСКА

Таблица 5.5.

1. Задача: *„Концепция за прилагане на организационно-архитектурното моделиране в отбраната”*	**2. Дата/Час Група:** *ОА* *16.12.2009 г.* **Начало:** *09.30* **Край:** *17.00*	**3. Дата на попълване:** *16.12.2009 г.*

4. Попълнил: *подп. Иво Георгиев Радулов, главен експерт в отдел „Операционен анализ”, дирекция „Операции” - МО*
(Звание, Име, Презиме, Фамилия, Заемана длъжност)

Вид риск	**Вероятност (В)**	**Експозиция (Е)**	**Последици (П)**	**Риск (Р) Р=В*Е*П**	**Класификация (степен)**
5	**6**	**7**	**8**	**9**	**10**
I. Институционален					
1.1 Недостатъчна политическа воля за приемане на Концепцията	Средна (5,0)	-	Опасни (15,0) - Невъзможност за реализиране на Концепцията	(75,0) Умерен риск-необходими са мерки за намаляването му	III
1.2. Забавяне на процеса за внасяне на документите по създаването на нормативната база	Средна (5,0)	-	Малки (1,0) - Начало на въвеждането на Концепцията при незавършена нормативна база	(5,0) Незначителен, твърде ограничен риск	I
1.3. Забавяне на организационно-щатните промени на стратегическо ниво	Средна (5,0)	-	Сериозни (7,0) - Невъзможност за реализиране на концепцията	(35,0) Приемлив, неголям риск - необходимо е внимание	II
II. Нормативно-документален					
2.1. Забавяне приемането на нормативните документи	Висока (10,0)	-	Сериозни (7,0) - Невъзможност за стартиране на процеса	(70,0) Приемлив, неголям риск - необходимо е внимание	II
2.2. Забавяне разработването на вътрешно нормативните документи	Малко вероятна (0,5)	-	Малки (1,0) - Забавяне на процеса и некачествено реализиране на Концепцията	(0,5) Незначителен, твърде ограничен риск	I

III. Програмно-финансов					
3.1. Липса на воля за промяна в програмната структура за ресурсното осигуряване на процеса	Висока (10,0)	-	Опасни (15,0) - Нереализиране на Концепцията	(150,0) Умерен риск- необходими са мерки за намаляването му	III
3.2. Недостатъчни финансови средства за обезпечаване изпълнението на Концепцията	Висока (10,0)	-	Значителни (3,0) - Незавършеност и лошо качество за реализирането на Концепцията	(30,0) Приемлив, неголям риск - необходимо е внимание	II
IV. Организационен					
4.1. Липса на обособени организационни звена за работата с NAF	Висока (10,0)	-	Опасни (15,0) - Некачествено управление на процеса на промяната	(150,0) Умерен риск- необходими са мерки за намаляването му	III
4.2. Липса на обучен личен състав за работа в организационните звена	Средна (5,0)	-	Сериозни (7,0) - Некачествено управление на процеса на промяната	Приемлив, необходимо е внимание	II
4.3. Текучество в екипа, внедряващ и развиващ NAF	Средна (5,0)	-	Малки (1,0) - Забавяне на темпа за реализиране на Концепцията	(0,5) Незначителен, твърде ограничен риск	I
4.4. Съпротива от средния управленски персонал	Висока (10,0)	-	Опасни (15,0) - Подмяна на приоритетите	(150,0) Умерен риск- необходими са мерки за намаляването му	III
4.5. Ниска мотивация на служителите за реализация на Концепцията	Средна (5,0)	-	Малки (1,0) - Съпротива срещу промяната	(0,5) Незначителен, твърде ограничен риск	I

ПРЕПОРЪЧИТЕЛНИТЕ МЕРКИ ЗА УПРАВЛЕНИЕ И КОНТРОЛ НА ИДЕНТИФИЦИРАНИТЕ РИСКОВИ СЪБИТИЯ СПОРЕД ОЦЕНКАТА НА РИСКА

Таблица 5.6.

Идентифицирано рисково събитие	**Необходими мерки за управление и контрол на идентифицираните рискови събития**
I. Институционален риск	
1.1 Недостатъчна политическа воля за приемане на Концепцията	1.1.1. Ангажиране на политическото и военното ръководство в процеса по разработването на Концепцията
1.2. Забавяне на процеса за внасяне на документите по създаването на нормативната база	1.2.1. Ангажиране вниманието на военната общественост с потребността от нов подход и технология за работа
1.3. Забавяне на организационно-щатните промени на стратегическо ниво	1.3.1. Изграждане на екипи за реализиране
II. Нормативно-документален риск	
2.1. Забавяне приемането на нормативните документи	2.1.1. Популяризиране на идеята, като се ангажира вниманието на военната общественост с потребността от въвеждането на нов подход и съответна технология за работа
2.2. Забавяне разработването на вътрешно нормативните документи	2.2.1. Определяне и подготвяне на групите, разработващи документите
III. Програмно-финансов риск	
3.1. Липса на воля за промяна в програмната структура за ресурсното осигуряване на процеса	3.1.1. Представяне на идеите на Концепцията пред Съвета по ОС и Програмния съвет и търсене на алтернативи за финансиране
3.2. Недостатъчни финансови средства за обезпечаване изпълнението на Концепцията	3.2.1. Търсене на алтернативни източници и програми
IV. Организационен риск	
4.1. Липса на обособени организационни звена за работата с NAF	4.1.1. Създаване на ad-hoc групи за работа
4.2. Липса на обучен личен състав за работа в организац. звена	4.2.1. Провеждане на обучение
4.3. Текучество в екипа, внедряващ и развиващ NAF	4.3.1. Мотивация на личния състав
4.4. Съпротива от средния управленски персонал	4.4.1. Провеждане на качествено обучение, разпространяване на идеите и въвличане в процеса на промяната
4.5. Ниска мотивация на служителите за реализация на Концепцията	4.5.1. Провеждане на комплекс от мероприятия за повишаване на мениджърските умения на личния състав

Пример 2 - с акумулиране на риск

Използваният сценарий в пример 2 е разработен за провеждане на военна операция за прикриване на държавната граница на условна държава в условен регион. Целта е демонстриране на математически метод за анализ на сценариите, базиран на размита логика, с отчитане на непълната определеност в количествените и качествените данни.

Примерът описва конфликт между държавите Кесалония и Мидландия. За описания сценарий е оценен риска при разрешаване на военнополитическа криза с използване на пълния състав на въоръжените сили на Мидландия в операция по прикритие на държавната й граница.

ЕТИКЕТ НА СИТУАЦИОННИЯ СЦЕНАРИЙ

Географски обхват – Регионът, обхващащ територията на държавите Мидландия, Кесалония, Катол и Малония.
Характер на конфликта – Граничен между две съседни държави (Мидландия и Кесалония) с участието на криминални групировки и бандитски формирования.
Интензитет – Среден, с възможност за прерастване във висок.
Съюзна подкрепа – Мидландия е пълноправен член на Трансрегионалния Съюз за Отбрана и Сигурност - ТРАСОС.
Равнище на заплаха – Средно, с възможност за ескалация.
Равнище на амбиция – Мидландия участва в съюзна отбранителна операция или в действия за разрешаване на военнополитическата криза с основната част или пълния състав на въоръжените си сили.
Задача на ВС – Участие в съюзна отбранителна операция или в действия за разрешаване на военнополитическа криза в национален формат.
Основни операции – Съюзна отбранителна операция или действия за разрешаване на военнополитическа криза в национален формат.
Контингент – Основната част или пълният състав на Въоръжените сили.

ПОСТАНОВКА НА ЗАДАЧАТА

В следствие на вътрешни етно-политически противопоставяния през последната година в държавата Кесалония, която е в непосредствена близост до Република Мидландия, се забелязва нарастване на степента на насилие. Налице са спорадични преки стълкновения с използване на оръжие в приграничните райони. Отделни криминални елементи и въоръжени банди намират благоприятно поле за изява в резултат от нестабилната обстановка. Политическото ръководство, провокирано от създаденото вътрешно икономическо и политическо напрежение, търси начини за разрешаване на проблемите чрез провеждане на политика, насочена срещу съседните държави, предявяване на териториални и етнически претенции и създаване на условия за достигане на политическите си намерения. Налице е прегрупиране на съединения и части от въоръжените сили на страната (до 2-3 съединения) на едно направление, в близост до държавната граница на Република Мидландия.

С цел недопускане прехвърлянето и действието на враждебни елементи на мидландска територия, Мидландската армия (във взаимодействие с органите на гранична полиция) е развърнала за прикритие на държавната граница на застрашеното направление механизирани и поддържащи подразделения с общ състав до бригада, повишена е готовността на определени сили и средства, провеждат се мероприятията по усилване на бойното дежурство и по разузнаването. За да се спре по-нататъшното разрастване на

насилието в региона, Съвета на ОН гласува Резолюция за разполагане на военни контингенти в региона. **ТРАСОС** дава съгласие за развръщане на мироналагащи сили с мандат на ОН.

ЦЕЛ НА ЗАДАЧАТА

Целта е да се намерят асоциираните за този сценарий най-критичен рисков фактор за отбраната и общия риск за националната сигурност на Мидландия.

ОГРАНИЧЕНИЯ

За да се опрости задачата, без да се промени съществено дефинираната среда, се правят следните ограничения:

- Разглеждат се ограничен брой фактори на риск (до четири);
- Моделът за оценка на риска се състои от 2 йерархично свързани нива;
- Не се анализира динамиката на бойните действия;
- Поради липсата на достатъчно информация за някои управляеми и/или независими променливи и параметри, е възприета приблизителна точност на резултатите, удовлетворяваща анализа;
- Изследването е извършено на базата на експертни знания и информация от явни източници.

ИДЕНТИФИЦИРАНЕ НА РИСКОВЕТЕ

В съответствие с направените по-горе ограничения, факторното пространство е сведено до 4 типа основни рискови фактори. Същите са определени по метода на мозъчната атака и са дадени в Таблица 5.7.

Таблица 5.7.

1. Мисия/Задача: *„Прикритие на държавната граница на застрашено направление”*	**2. Дата/Час Група:** *ОА* *09.11.2010 г.* **Начало:** *10.30* **Край:** *11.00*	**3. Дата на попълване:** *09.11.2010 г.*
4. Попълнил: *подп. Иво Георгиев Радулов, главен експерт в отдел „Операционен анализ”, дирекция „Стратегическо планиране” - МО* (Звание, Име, Презиме, Фамилия, Заемана длъжност)		
5. Фактори	**6. Потенциални рискови събития**	
1. Релеф и метеорологични условия		
1.1. Наблюдение и разузнаване.	1.1.1. Лоши условия за добиване и обработка на информацията;	
1.2. Прикрития и условия за маскиране.	1.2.1. Липса на адекватни условия и средства.	
1.3. Препятствия на терена.	1.3.1. Наличие на изградени отбранителни и инженерни съоръжения в направлението на бойните действия;	
1.4. Ключов и критичен терен и инфраструктура.	1.4.1. Наличие на елементи от критичната инфраструктура.	
1.5. Пътна инфраструктура.		
1.6. Метеорологични условия (климатични особености за географската ширина).		

2. Войски и личен състав	
2.1. Физическо и емоционално състояние на личния състав;	
2.2. Планиране на операцията и организиране на участието на войсковите единици;	2.2.1. Недостатъчна подготовка; 2.2.2. Лоша комуникация; 2.2.3. Лошо взаимодействие между щабовете; 2.2.4. Недобра оперативна съвместимост; 2.2.5. Неадекватни бойни възможности.
2.3. Климатични особености, свързани с физическото оцеляване;	
2.4. Допълнителни трудности.	2.4.1. Слаба логистика; 2.4.2. Недобри условия на живот; 2.4.3. Лошо медицинско обслужване; 2.4.4. Недобра организация за евакуиране; 2.4.5. Липса на питейна вода и/или средства за пречистване на вода.
2.5. Продължителност на операцията.	2.5.1. Липса на способности за изпълнение на продължителна операция.
3. Време	
3.1. Време за действие;	3.1.1. Недостатъчно време за реакция;
3.2. Време за планиране на операцията;	3.2.1. Недостатъчно време за окомплектоване на силите (войсковите единици) 1/3, 2/3;
3.3. Време за подготовка;	3.3.1. Недостатъчно време за подготовка;
3.4. Време за изпълнение на операцията;	3.4.1. Липса на достатъчно време за изпълнението на операцията;
3.5. Метеорологични условия.	3.5.1. Недостиг от време поради лоши или специфични метеорологични условия.
4. Външна среда	
4.1. За военновременни операции;	4.1.1. Заплахи от възможни нови коалиции;
4.2. Вражески въздействия;	4.2.1. Сформиране на групировки и движения за дестабилизация (на територията на страната) на религиозен, етнически и/или крайно националистичен признак.
4.3. Криминогенна обстановка.	4.3.1. Криминални прояви; 4.3.2. Организирана престъпност.

РЕШЕНИЕ

Всеки модел представлява опростен, но отразяващ реалните характеристики, вариант на реална система, процес, план и т.н. След като вече са идентифицирани рисковите събития, се определя влиянието, което могат да окажат върху операцията.

За конкретното решение ще се използват качествени модели – с използване на размита логика (с помощта на лингвистични променливи и функции за принадлежност за всяка подобласт от пространството на допустимите стойности). За целите на изграждане на

модел на риска, при който има неопределеност и непълнота на необходимите входни данни, се прилага описание на базата от правила за реакцията/изхода на модела [28].

За всеки тип на идентифицираните рискови събития предварително се дефинират критерии, по които се определят последиците (работи се с лингвистичната скала от Таблица 5.3, но за всеки тип събитие количествените параметри на критерия са различни). За оценяване на влиянието на всеки тип рисково събитие се сумират отделните рискове на възможните независими елементи на този тип. Това става по формулата:

$$R_f = \sum_{i=1}^{n} R(A_i), \tag{5.3}$$

където R_f е сумарният риск на този фактор (от таблицата с потенциални рискови събития 5.5), а елементите на този фактор са от i = 1 до n на брой. R(Ai) е изчисленият риск на единичното събитие Ai.

За всяка заплаха (потенциално рисково събитие Ai) на основата на наличната количествена информация (априорна и апостериорна) и експертни знания се определя вероятността за възникване с отчитане на степента на интензивност. Предложено е единно оценяване на вероятността за възникване на различните рискови събития (изброени в таблица 5.5). Въвежда се експертна скала с лингвистични оценки за вероятността за възникване на събитие, съгласно Таблица 5.1.

Изчисляването на единичния риск R(Ai) от дадено събитие Ai се извършва по формулата (5.1) и приема вида:

$$R(A_i) = P(A_i).F(A_i).C(A_i), \tag{5.4}$$

където P(Ai) е вероятността за сбъдване на това единично събитие, F(Ai) е честотата/ интензитета на проявяване и C(Ai) е цената, или тежестта на последствията, които настъпването му ще окаже на цялата операция. При лингвистичните правила, знанията се задават с помощта на ***“If - Then” (Ако -То)*** формите.

Например:

If *[Последиците от рисково събитие А1 са Малки] и [Последиците от рисково събитие А2 са Средни]* ***Then*** *[Последиците от рисков фактор Х са Малки];*

Или:

If *[Вероятността от рисково събитие А1 е Под средната] и [Последиците от рисково събитие А1 са Малки]* ***Then*** *[Рискът от събитие А1е Незначителен]*.

При изграждане на правилата за модела има възможност да се избере конюнкцията (връзка И, ИЛИ, НЕ), както и оператор за сумиране, умножение, или друг вид импликация.

Оценката на риска на отделните фактори се извършва, като се използват данните за вероятността за възникване на неговите възможни събития, с определена интензивност и загуби. При този етап се определят преките загуби вследствие на възникналото независимо събитие.

Изчисляването на сумарния риск в модела се формира като се отчитат взаимодействията между отделните фактори в модела. Затова особено внимание следва да се отдели на правилното проследяване на връзките между отделните рискови събития в изграждане на модела. Често е налице причинно-следствена зависимост на един елемент/променлива от проявлението на друг рисков фактор. Функцията на зависимостта на крайния риск от влиянието на всички фактори f_j е означена с F(R(f)), където рисковото влияние на отделните фактори е изчислено по горната формула (5.3). Тази функция може да е просто сумиране, ако факторите са с равна тежест, или с множители на тежест за по-важните фактори. Общият вид на крайната оценка е:

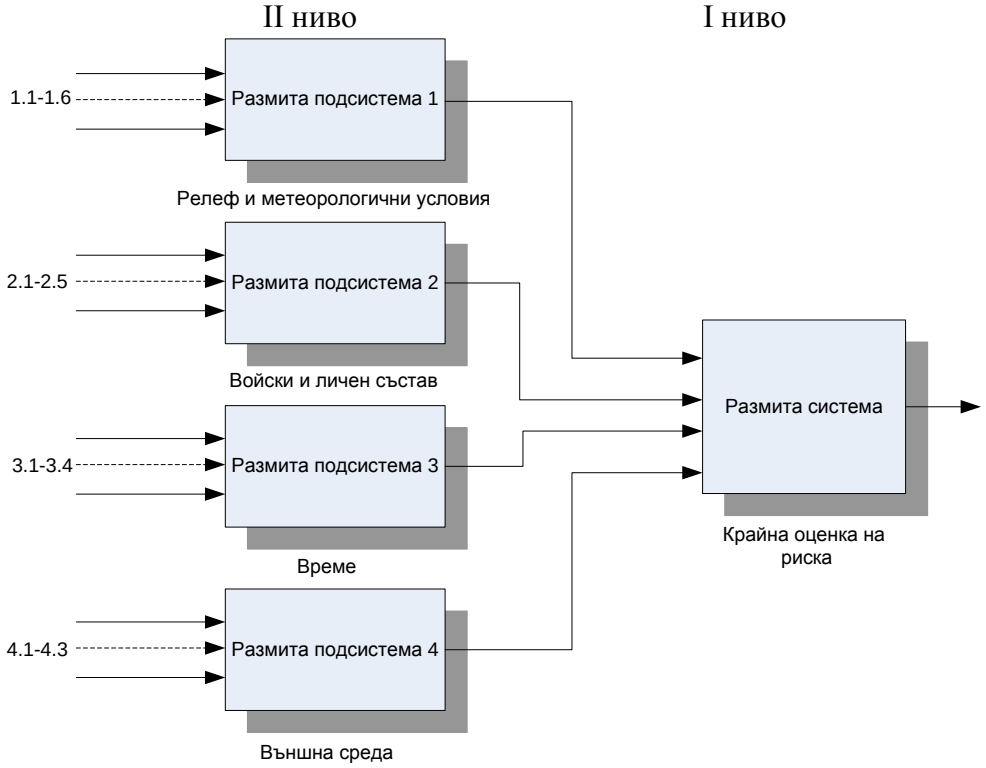
$$R = F(R(f_j)) \tag{5.5}$$

Посочените особености при изчисляването на риска в разглеждания случай, естествено водят до идеята за разработване на йерархична система.

Необходимо е да се подчертае отново, че изчисляването на потенциалната последица при случване на конкретно рисково събитие се базира на субективните знания на експертите относно интензивността и вероятността за случване на разглежданото събитие. Също така и самите оценки за интензивността на определено рисково събитие се представят чрез лингвистични променливи (малка, средна, голяма и катастрофална), които по своя характер са качествени, а не количествени променливи.

Както е показано на Фигура 5.1 моделът за оценка на риска се състои от 2 нива (съгласно направените ограничения), свързани йерархично. Всеки от факторите, влияещи на сумарния риск на разглежданата операция, се явява вход за моделираната система. Изход на размитата експертна система е крайният риск на цялата операция, изчислен по формула (5.4).

Йерархичната система, изградена на базата на размити експертни правила, е представена на Фигура 5.1. Второ ниво включва четири размити подсистеми, които съответстват на четирите типа фактори, разглеждани като източници на потенциални рискове за провеждането на операцията. Всеки от тези фактори от своя страна има за входове идентифицираните рискови събития от Таблица 5.5.



Фигура 5.1. Обобщен вид на размитата система.

Първото ниво се състои от една размита система, която формира комплексната оценка за степента на риск на операцията (сценария). Изходите на размитите подсистеми от второто ниво са входове за системата от първото ниво. Получаваната като изход оценка от първо ниво се обобщава с избран вид конюнкция и се получава крайната оценка за риска.

ИЗБОР НА СКАЛА

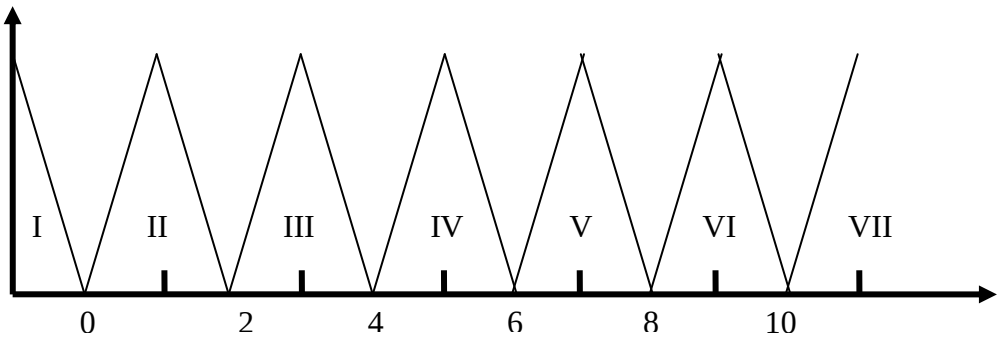
Дефинирането на скалата с качествени оценки за всеки от елементите на риска става въз основа на таблични стойности, приети в регламентиращи източници и наредби. Такава

скала, например е седем-степенната скала за описание на вероятността, с характеристики „*Практически невъзможна”; „Малко вероятна”; „Възможна в определени случаи”; „Вероятност под средната”; „Средна вероятност”; „Вероятност над средната”;* и „*Висока”*, както е дадена в НАРЕДБА 5[10].

За желана прецизност за всеки отделен случай на оценяване на риска е възможно друго определяне на скалата за качествени оценки. В термините на размитата логика се употребява най-често тристепенната скала (малко, средно, голямо), която съответства на широко прилаганата техника за размиване на една стойност чрез триъгълна функция на принадлежност, определена със средната ѝ (най-вероятна) стойност, долната (средната минус отклонението) граница и горната (средната плюс отклонението) граница. Като частен случай на тристепенната скала се явява 7-степенната с характеристики: *„Много малко”; „Малко”; „Под средно”; „Средно”; „Над средно”; „Голямо” и „Много голямо”*.

Добро покриване на целия възможен интервал (дефиниционна област) на заемани стойности се постига или чрез равномерно разположени степени на скалата, или чрез различна ширина/диапазон на отделните степени. Пример за равномерно разположени 7 степени, в интервала [0 ÷10], е изобразен на Фигура 5.2.

I степен (<0], II степен [0 ÷ 2], III степен [2 ÷ 4], IV степен [4 ÷ 6], V степен [6 ÷ 8], VI степен [8 ÷10] и VII степен [>10).



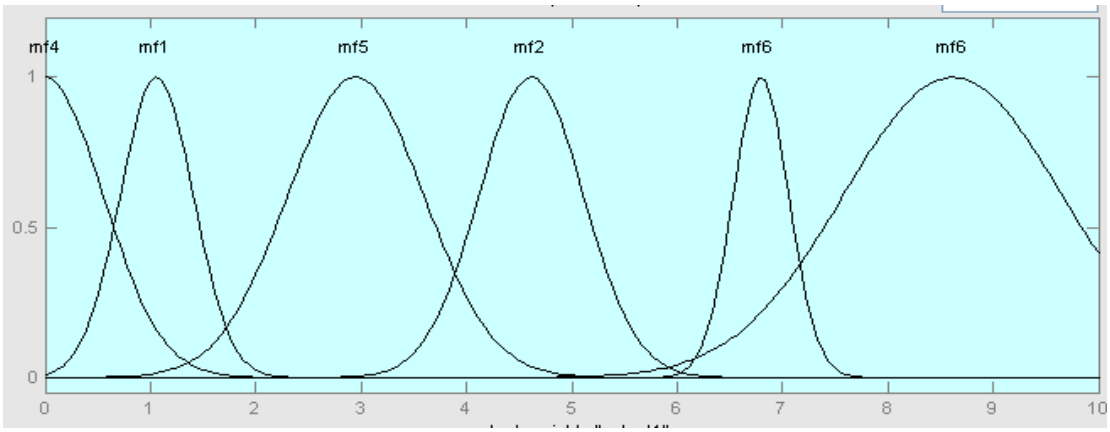
Фигура 5.2. Равномерно разпределение.

Неравномерно разположени 7 степени на скалата при интервал [0 ÷ 10] са изобразените на Фигура 5.3 интервали:

I степен [0 ÷ 0,2] II степен [0,2 ÷ 0,5] III степен [0,5 ÷ 1]
IV степен [1 ÷ 3] V степен [3 ÷ 5] VI степен [5 ÷ 7] и VII степен [7 ÷ 10].

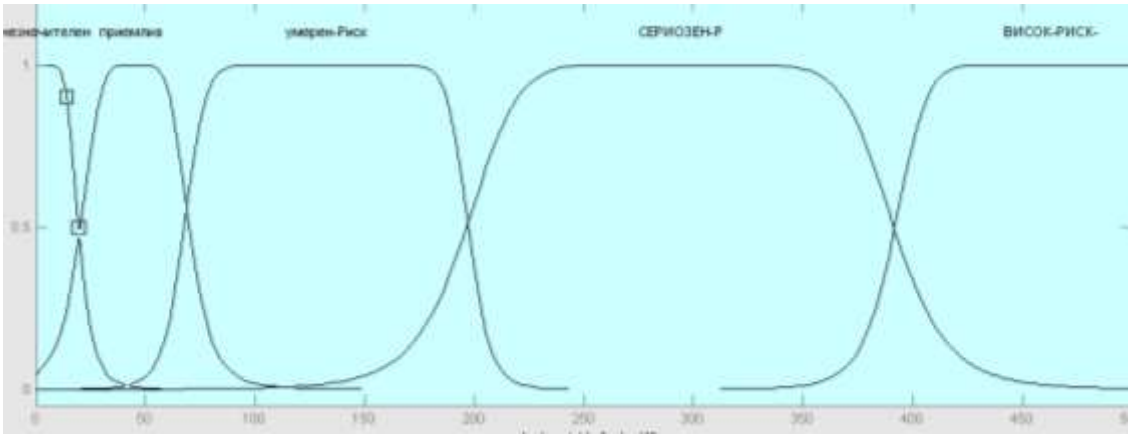
Изборът на различни функции на принадлежност позволява плавното преминаване от една степен в друга и добро покриване на целия интервал.

[10] НАРЕДБА № 5 от 11.05.1999 г. за реда, начина и периодичността на извършване на оценка на риска, издадена от министъра на труда и социалната политика и министъра на здравеопазването, обн., ДВ, бр. 47 от 21.05.1999 г.



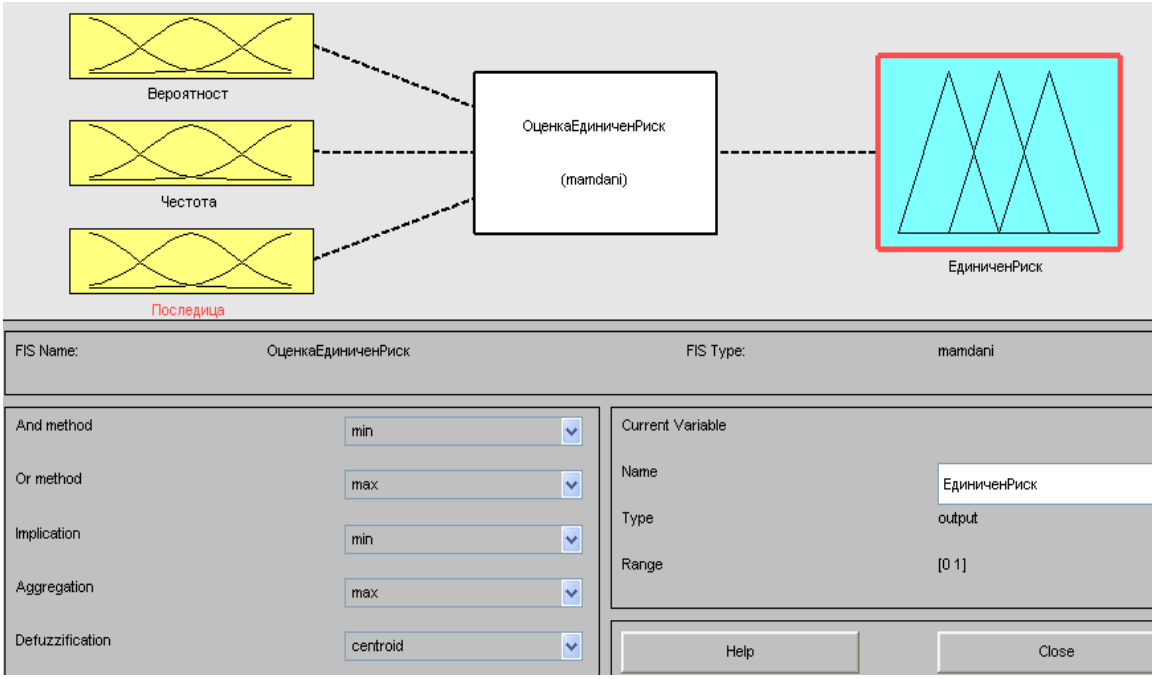
Фигура 5.3. Неравномерно разпределение.

Известно е от теорията на размитите множества, че лингвистичните променливи могат да приемат различни количествени или качествени значения (малко—голямо; ниско—високо; топло—студено и т.н.). В размитите модели тези променливи се разглеждат като множества (терми) с определена степен на принадлежност на конкретната величина. Дефинират се различни по форма функции на принадлежност (триъгълна, трапецовидна, Гаусова, и други), например тази от Фигура 5.4.



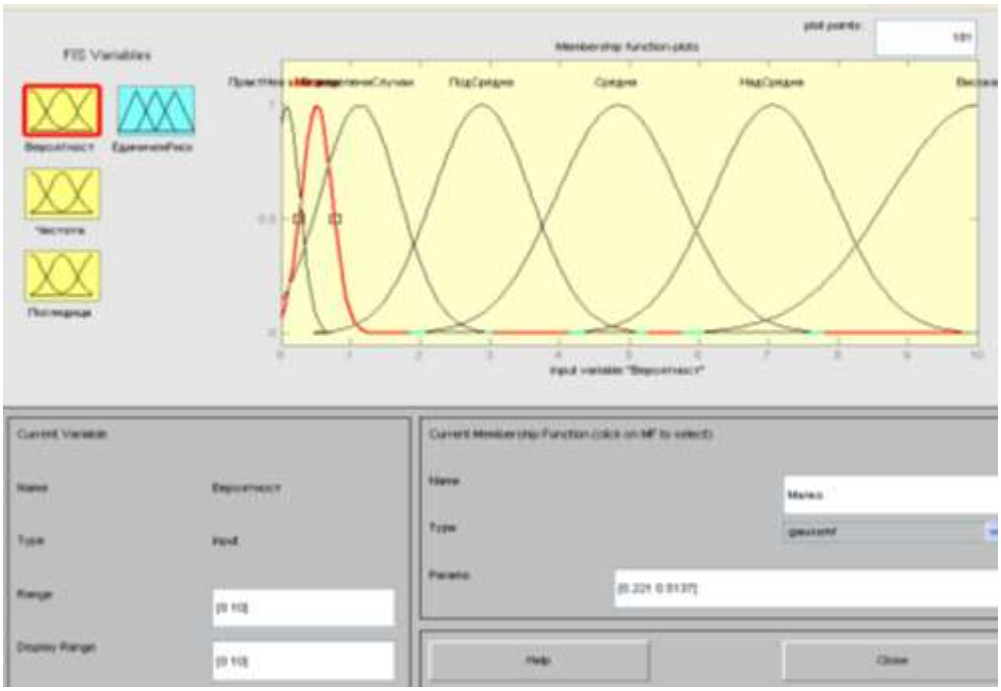
Фигура 5.4. Неравномерно разпределение при 5 степени на скалата.

В изграждания модел входните променливи от първото ниво са резултат от изхода (размит извод) на типичната формула (5.4) за оценка на единичен риск. Входовете за вероятност P(Ai); честота F(Ai) и последица/ цена C(Ai) се представят чрез еднакъв брой размити терма за всички подсистеми. За определяне на вероятността и експозицията се задават седем размити терма, които съответстват на Таблица 5.1 и 5.2. Още пет размити терма за определяне на последиците, които съответстват на Таблица 5.3. Моделът за оценка на единичния риск е показан на Фигура 5.5. Изходът на този модел е вход към второ ниво на йерархичната система от Фигура 5.1.



Фигура 5.5. Модел за оценка на единичен риск.

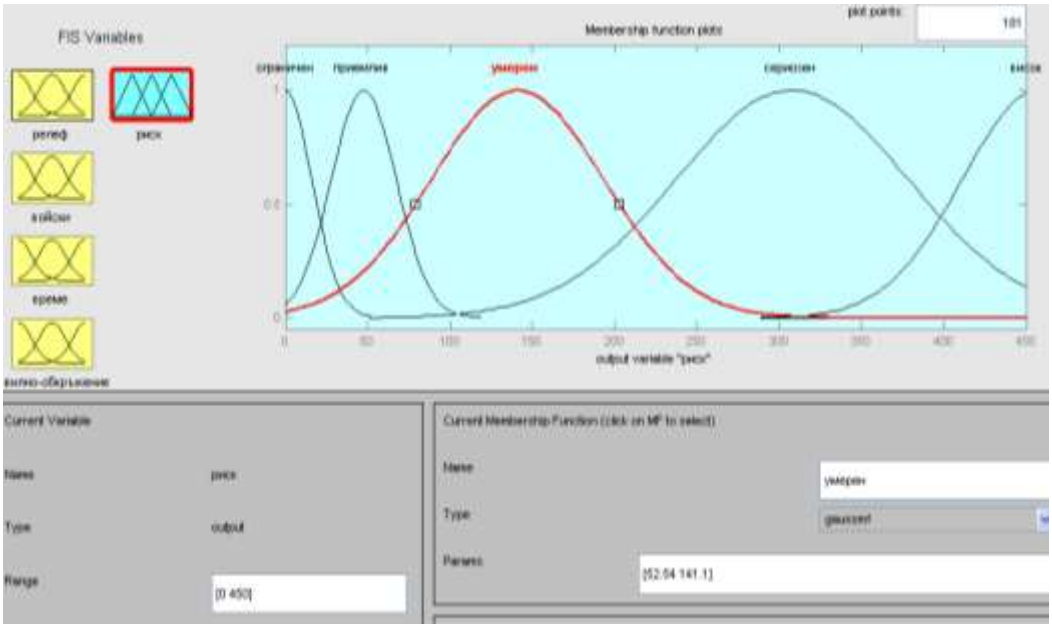
На Фигура 5.6. е показана входната променлива „*Вероятност”* от модела за оценка на единичния риск. Аналогично се представят останалите входове за този модел, в случая за „*Честота”* – в 7 терма; и за „*Последица”* – в 5 терма. Изходът на тази оценка е „*Единичният риск”*, който служи за вход на второ ниво на йерархичната система.



Фигура 5.6. Представяне на 7 размити терма за входната променлива „*Вероятност”* от модела за оценка на единичния риск.

Изходните променливи (четирите междинни и крайната комплексна оценка) на подсистемите от първото и второто ниво на йерархичната размита система (от Фигура 5.1) се

дефиниран с пет терма, съответстващи на Таблица 5.4 – „*Незначителен”; „Твърде ограничен риск”; „Приемлив”; „Неголям риск”; „Умерен риск”; „Сериозен риск”; „Висок риск”*. Тяхното представяне е показано на Фигура 5.7. Променливите са качествен резултат от размитите подсистеми за извод на базата на стойностите на входните лингвистични променливи.



Фигура 5.7. Размито представяне на изхода на първото ниво на йерархичната система.

Всички лингвистични променливи в модела се задават с Гаусова функция на принадлежност, както е показано на Фигура 5.7. Входните и изходните размити величини за елементите на *Единичен Риск* са в интервала [0 ÷ 10], а крайната комплексна оценка се изменя в интервала [0 ÷ 400]. В изграждания модел входните променливи от първото ниво се представят чрез седем размити терма за всички подсистеми, за определяне на вероятността, които съответстват на Таблица 5.1 – „*Практически невъзможна”; „Малко вероятна”; „Възможна в определени случаи”; „Под средната”; „Средна”; „Над средната”; „Висока”*. Още пет размити терма за определяне на тежестта/последиците, които съответстват на Таблица 5.3 – „*Малки”; „Значителни”; „Сериозни”; „Опасни”; „Катастрофални”*. Съответно седем размити терма за определяне на честотата.

Правилата за извод в базите знания се задават чрез “***If — Then”*** формите. За конкретния пример, при двувходовите размити подсистеми правилата са 35, а в тривходовите – 245. Някои от правилата са следните:

If *[Вероятността от рисково събитие А1 е Под средната] и [Последиците от рисково събитие А1 са Малки]* ***Then*** *[Рискът от събитие А1 е Приемлив]*.

If *[Вероятността от рисково събитие А1 е Средна] и [Последиците от рисково събитие А1 са Опасни]* ***Then*** *[Рискът от събитие А1 е Сериозен]*.

If *[Вероятността от рисково събитие А1 е Висока] и [Последиците от рисково събитие А1 са Значителни]* ***Then*** *[Рискът от събитие А1 е Висок]*.

Механизмите за извод (начинът за разсъждения *If ... Then ...*) в размитата логика зависят главно от вида на изхода от правилото и най-често се използват от тип Мамдани или Сугено. Основната разлика при механизмите за извод тип Сугено е, че изходните функции са линейни или константи.

Ако входовете на модела означим с матрица A с размерност $m_x n$ и общ член a_{ij} , с X (с размерност $n_x 1$ и общ член x_j) означим степените на проявяване на съответния вход (рисково събитие) и с B (с размерност $m_x 1$ и общ член b_i) означим съответно следствията (единичните рискове), то всеки елемент a_{ij} показва до колко причината j допринася за възникването на следствието i , при $1 \le i \le m$, $1 \le j \le n$.

Информацията за възможността да възникне всяко едно от m-те следствия (рискове, неизправности) се записва като m израза от вида:

If причината i се прояви със сила x_j ,
and следствието j зависи от нея със тегло a_{ij}
or причината $i+1$ се прояви със сила x_{j+1} ,
and следствието j зависи от нея със тегло $a_{i+1,j}$
or ... .
Then следствието j ще се прояви със сила b_i.

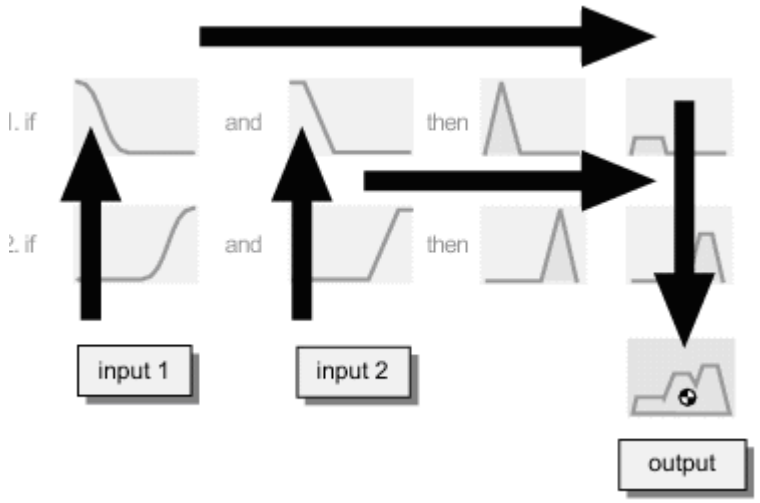
Компактният запис е аналогичен на система линейни уравнения, в която операциите умножение и събиране са заменени с логическото „И” и „ИЛИ”.

$$\begin{vmatrix} (a_{11} \wedge x_1) & \vee \ldots \vee & (a_{1n} \wedge x_n) & = b_1 \\ & \ldots \quad \ldots \quad \ldots . \quad \ldots & & \\ (a_{m1} \wedge x_1) & \vee \ldots \vee & (a_{mn} \wedge x_n) & = b_m \end{vmatrix} \qquad (5.6)$$

където $A = \begin{bmatrix} a_{11} & \ldots & a_{1n} \\ \ldots & \ldots & \ldots \\ a_{m1} & \ldots & a_{mn} \end{bmatrix}$, $X = \begin{bmatrix} x_1 \\ \ldots \\ x_n \end{bmatrix}$, $B = \begin{bmatrix} b_1 \\ \ldots \\ b_m \end{bmatrix}$

Композицията $B=AX$ може да бъде изпълнена с помощта на различни композиционни закони, но за разглеждания случай се прилага ***min-max*** композицията на правилата. Това означава, че от 2 стойности, свързани с логическо „И”, се взема минималната, а от няколко стойности, свързани с логическо „ИЛИ”, се взема максималната.

Тъй като моделът е изграден от няколко правила, комплексната оценка за степента на риска е комбинация от изходите на всичките активни (които се засягат, влизат в действие) правила. Комбинираната или агрегирана функция за изхода от първото ниво формира комплексната оценка за риска (Фигура 5.8).



Фигура 5.8. Модел на правилата.

Второто ниво има толкова подсистеми, колкото са типовете фактори за потенциални източници на риск.

Всички подсистеми са изградени във вариант Мамдани размити системи. Използват се класически min/max процедури за обработване на правилата и метод на деразмиване — център на тежестта. Конкретната стойност на изхода на йерархичната размита система представлява крайната комплексна оценка за потенциалните рискове за операцията.

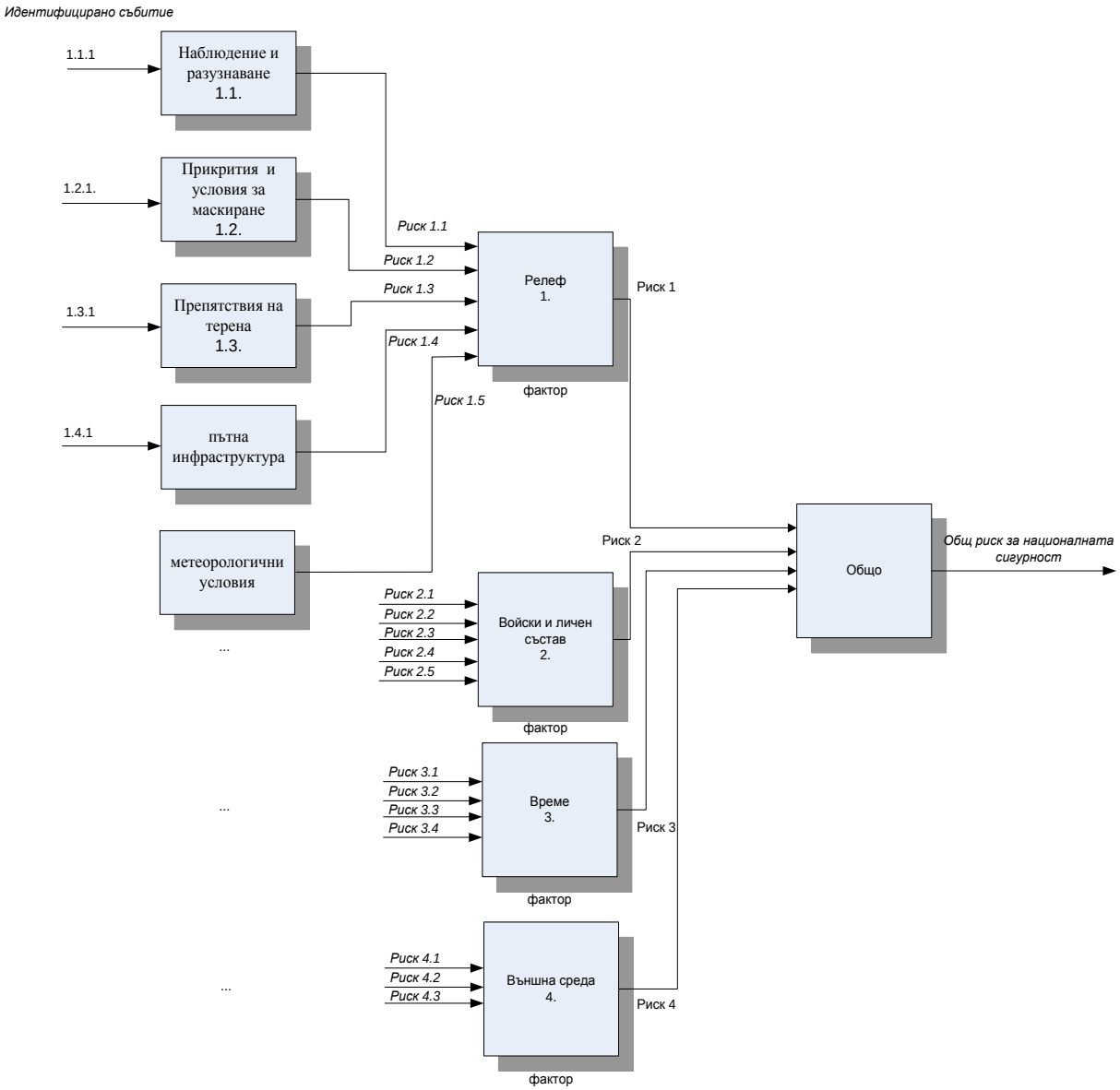
СИМУЛАЦИОННИ РЕЗУЛТАТИ

Разработената йерархична размита експертна система е проектирана в среда на MatLab[11] при използване на Fuzzy Toolbox.

Работоспособността и полезността на предложения интелигентен подход за комплексна оценка на рисковете за конкретна операция се доказва чрез моделиране и симулационни изследвания на формирания модел.

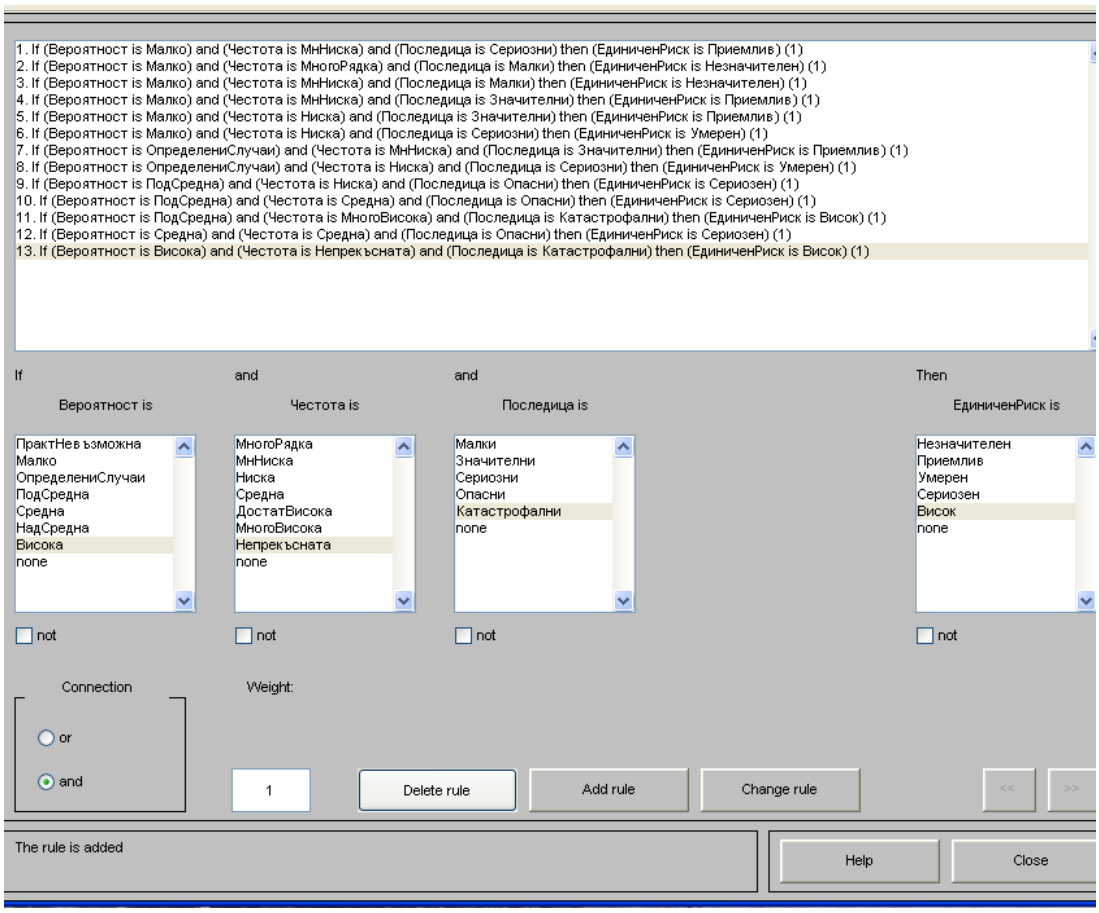
В този модел са разгледани определените четири типа рискови фактори за една операция. Изследва се степента на риска за всеки фактор. Структурата на системата е дадена на Фигура 5.9. Всеки вход съответства на потенциалните рискове за операцията, които произтичат от определения фактор. На фигурата подробно са разписана йерархичната размита система, асоциирана към фактора „*Релеф и метеорологични условия*”, характеризираща се с две нива, с 5 входа и две подсистеми. По аналогия се построяват и останали три фактора –„*Войски и личен състав”*; „*Време”* и „*Външна среда*”. Тези оценки от своя страна се явяват входове за крайната оценка на йерархичната система. Изходът е комплексна оценка за степента на риска, вследствие на изследваните фактори и техните идентифицирани събития.

[11] MATLAB е запазена марка на програмен продукт на фирмата MATHWORKS, USA.

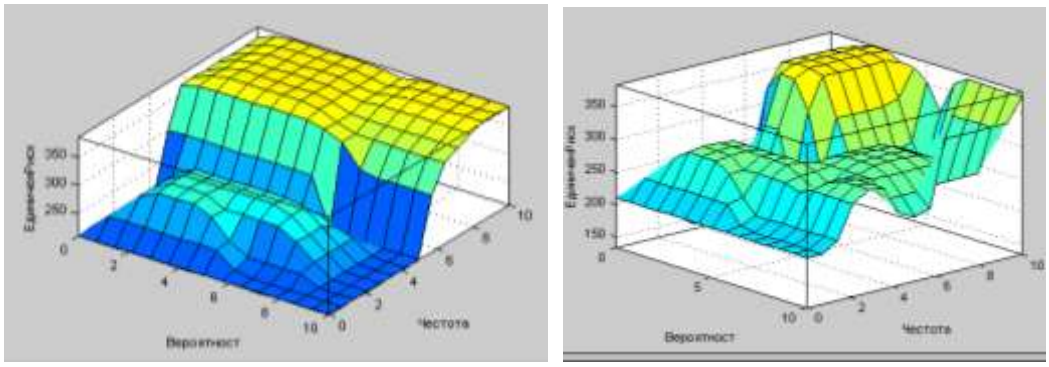


Фигура 5.9. Размита система с 2 подсистеми за оценка на риска от фактора *Релеф*. Петте входа съответстват на идентифицираните рискови събития от този тип фактор.

Извършена е симулация на множеството от пространствени състояния на изхода на модела и е изследвана интерактивната обратна връзка за настройка на правилата, показана на Фигура 5.10. Повърхнината на изчисления риск от единично събитие е показана на Фигура 5.11. Тази повърхнина съответства на показаните правила на Фигура 5.10.



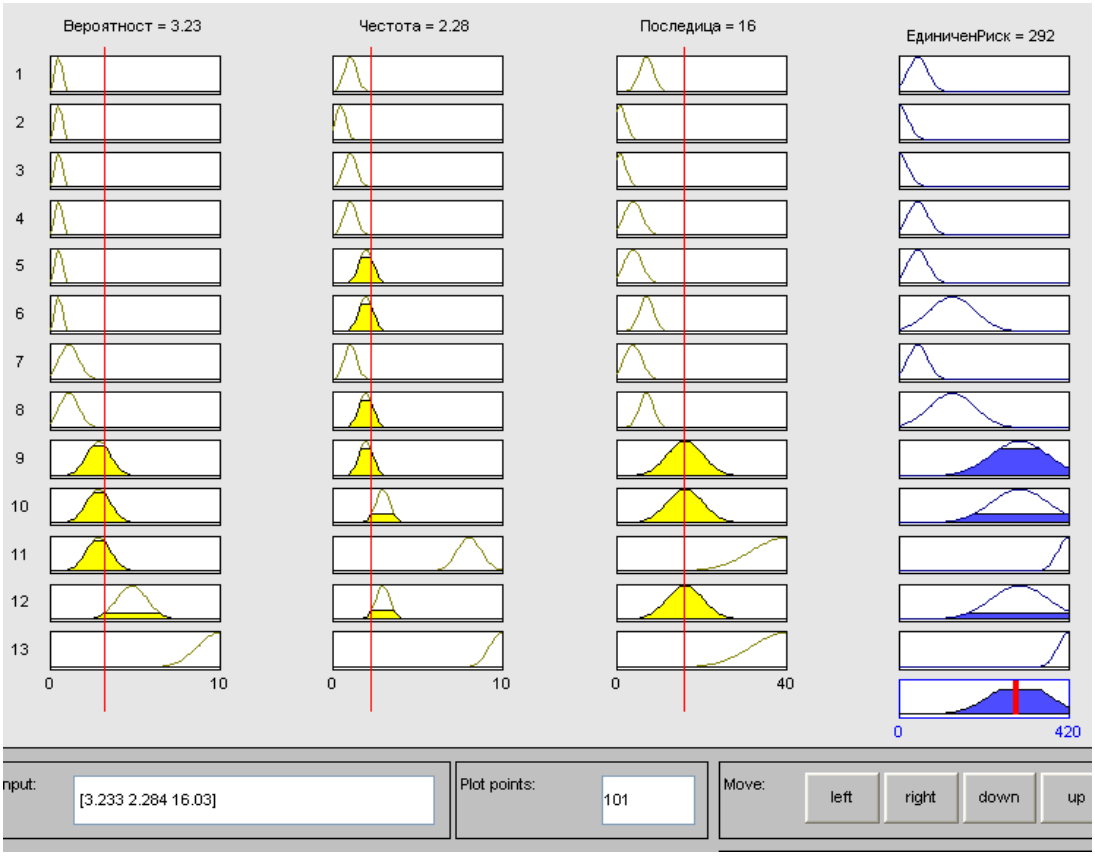
Фигура 5.10. Настройка на правилата за оценка на риск.



Фигура 5.11. Симулационни резултати. Повърхнина на изчислен риск на единично събитие „Налично Време_Изпълнение” за фактора ***Време***

От интерактивното представяне на модела с правила за изхода за йерархичната система може да се проиграват различни ситуации и да се изследва чувствителността на модела. На Фигура 5.12 е показан изходът за оценка на риска от единично събитие. Първите три колонки от този екран съответстват на трите входа на изградения модел (показан на Фигура 5.5). Последната колонка е изходът на модела. Броят на въведените от експертите правила (показани на Фигура 5.10) съответства на броя редове. Чрез преместване на червената гранична линия за всяка от колоните се избира различна стойност за този вход и съответните правила се изпълняват в различна степен – показано в жълто оцветяване. Възможно е и директно въвеждане на конкретната стойност за входовете в полето input долу вляво, с което интерактивно се показва изчислената стойност за оценката на риска. В случая

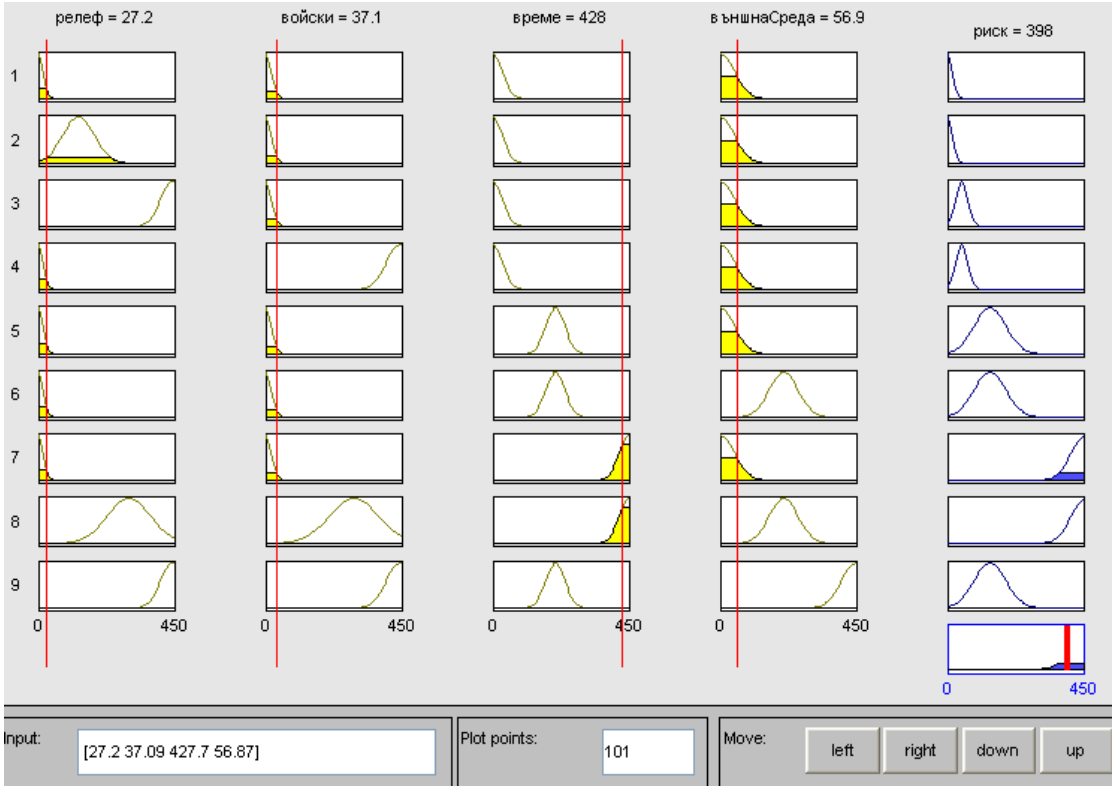
на Фигура 5.12 това е Единичен Риск – 292. Визуално се изобразява площта на сумарния комплексен риск (оцветена в синьо област, най-долу под колоната за изход).



Фигура 5.12. Симулационен резултат за оценка на риска – червената стойност вдясно долу, изчислена по метода на център на гравитация.

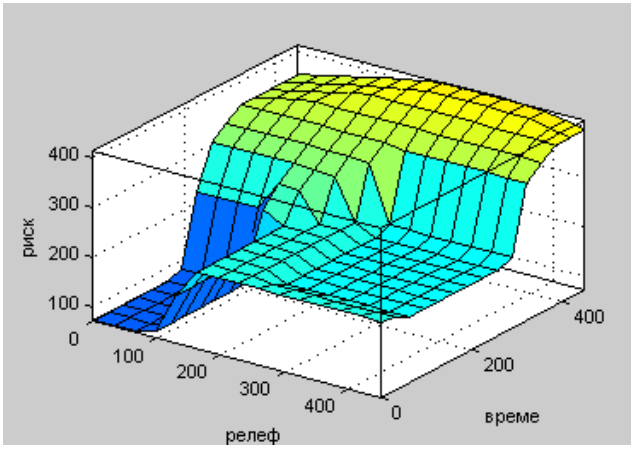
Получените симулационни резултати – крайните комплексни оценки за рисковете на четирите фактора (Фигура 5.13.), показват, че фактор 3 (Време) е най-критичен, т.е. потенциалните му последици за разглежданата операция са най-големи. Обратно, потенциалните рискове от фактор 1 са най-малки, т.е. факторът „Релеф” има най-ниска комплексна оценка за риск при провеждането на операцията (Фигура 5.14.).

Тъй като за триизмерното представяне на графиките се разглеждат само два от входните фактори (по двете оси X, Y), а изхода е по третата ос Z, то се налага по отделно разглеждане на всеки две 2 двойки входове. Крайното обобщено представяне на всички влияещи фактори е от вида, показан на фигура 5.13.



Фигура 5.13. Симулационен резултат за оценка на риска – изход от второ ниво на йерархичната система.

При добро покриване на правилата за целия диапазон на входните променливи се генерира пълната повърхнина на поведение на модела и се дава нагледна представа за критичните области на превключване и за възможните реакции и посоки на желано управление. Достигането до целево състояние на модела (напр. стойности на риска под предварително определени прагови) става чрез „пълзене” по тази повърхнина.



Фигура 5.14. Повърхнина за изчислен риск - отношение на риска за факторите „Релеф” – „Време”

Разработеният модел дава възможност да се изследва **влиянието на несигурността** чрез извършване на експерименти с реална система, за много по-кратък период от време. Подобно на метода Монте Карло, чрез използването на вградените функции на

разпределение в Fuzzy Toolbox, се извършват множество симулации с модела на анализираната операция, като включените в него случайни променливи приемат стойност на случаен принцип от вероятностните им разпределения. По този начин едновременно се извършват множество анализи от типа „***Какво-Ако***”.

Математическият модел, базиран на размитата логика, спомага за описване на неясни, неточни или несигурни данни. По този начин се отчита непълната определеност в количествените и качествените данни. Съществуват различни програмни продукти, с които може да се изградят моделите и да се визуализират резултатите, но в илюстрирания пример не се акцентира върху това, кой точно продукт ще се използва, а се цели само представяне на една възможност.

Пример 3

Примерът илюстрира използването на конкретен математически метод PERT (Project/Program Evaluation of Resources and Time) за оценка на сценарий по време и неговото остойностяване, като същевременно се отчита риска на всеки етап от развитието на ситуацията.

ЕТИКЕТ НА СИТУАЦИОННИЯ СЦЕНАРИЙ

Географски обхват – Регионът, обхващащ територията на държавите Мидландия, Кесалония, Катол и Малония.
Характер на кризата – Културно-ценностен между държави с население, което изповядва различни културни и религиозни ценности (Мидландия и Кесалония) с участието на криминални групировки и лобистски среди от трети страни, които имат икономически интереси в района.
Интензитет – Нисък, с възможност за прерастване в среден.
Съюзна подкрепа - Мидландия е пълноправен член на Трансрегионалния Съюз за Отбрана и Сигурност - ТРАСОС.
Равнище на заплаха – Ниско, с възможност за ескалация.
Равнище на амбиция – Мидландия предприема действия за разрешаване на социалнополитическата криза основно с политически и дипломатически средства, но има готовност, в случай на нужда да използва и военнополитически средства.
Задача на ВС – Осигурява предприетите действия за разрешаване на социалнополитическа криза в национален формат с повишено внимание гарантиране на въздушния и морски суверенитет на страната и недопускане на действия отвън, целящи задълбочаване на икономическата криза.
Основни операции – Действия за недопускане на нарушаване на въздушното пространство от типа „Ренегат” в национален формат.
Контингент – Част от състава на въоръжените сили, по-конкретно състава на ВВС и сили за ПВО, участващи в охрана на въздушното пространство на националната територия.

ПОСТАНОВКА НА ЗАДАЧАТА

В следствие на вътрешни етно-политически противопоставяния през последната година в държавата Кесалония, която е в непосредствена близост до Република Мидландия, се забелязва нарастване на степента на насилие. Налице са спорадични преки стълкновения с използване на оръжие в приграничните райони. Отделни криминални елементи и въоръжени банди намират благоприятно поле за действие. Установени са данни за подготовка на

терористични клетки, както на територията на Мидландия, така и в няколко други държави, включително едната от тях е Кесалония, като в тях са включени и няколко лица, които притежават бревети за управление на малки граждански самолети.

Целта е да се оцени риска за националната сигурност на Мидландия, в случай на възникване на заплаха от тип „Ренегат”, да се остойности планирането на поддържане на способност за ефективно неутрализиране на заплаха от този тип и се направят препоръки за ефективно вземане на решение и управление на риска.

Допускания (всички те са условни за целите на примера):

Използваното въздухоплавателно средство с терористична цел е граждански самолет с пътници на борда и достатъчно гориво в резервоарите. В случай, че самолетът удари обект (сграда, определена площ или друго съоръжение), поражението е еквивалентно на удар с авиационна бомба (ОФАБ) калибър от 250 до 500 кг, при което смъртоносни поражения върху хора на закрито се очакват в радиус до 30 м и на открито до 250 м; тежки поражения върху сгради от търговски тип в радиус до 50 м и на усилени железобетонни конструкции в радиус до 10 м от центъра на кинетичния удар; площта на пораженията не надвишава полоса с размери 100х400 м. Самолетът е с реактивни двигатели, крейсерска скорост 800 км/ч, крейсерска височина на полета 10 000 м и на борда си има монтирано стандартно за своя клас радионавигационно оборудване. При обстрел с управляема ракета клас „въздух-въздух” или „земя-въздух”, същият пада неконтролируемо (цял или на отломки) върху площ, чиито координати могат предварително да се определят с достатъчна точност за да се каже попадат ли в границите на населено място или не.

Вероятността за поражение при огнево въздействие върху самолета-цел е над 85%.

Вероятността за неизпълнение на задачата е 20%.

Вероятността за пряко попадане на гражданския самолет върху планираната от терористите цел, ако липсва противодействие, е 70%.

Изтребителите за ПВО могат да действат във всякакви метеорологични условия, денем и нощем в целия височинен и скоростен диапазон на самолета, радиусът им на действие покрива цялата територия на страната от летището на което са базирани, като скоростта на изтребителя спрямо скоростта на гражданския самолет при насочване и сближение с него е в диапазона от 1,2:1 до 1,5:1, което осигурява успешно сближение дори на догон при попътни и попътно пресичащи се курсове и подаване на предупредителни сигнали от изтребителя преди крайния рубеж за въздействие върху самолета „Ренегат”.

Огнево въздействие върху гражданския самолет се осъществява само в краен случай, когато всички други алтернативи са изчерпани, има ясни и доказуеми признаци за намеренията на терористите и съществува реална заплаха от последици с недопустим риск (отнемане на човешки живот, застрашаване на живота и здравето на гражданите на Мидландия в особено голяма степен, нанасяне на неприемливи материални щети, застрашаване на енергийната сигурност на Мидландия, водещо до неприемливи икономически загуби). Оценката на тези рискове се прави от длъжностно(и) лице(а), по предварително изготвен, узаконен и въведен за изпълнение алгоритъм.

ПОСЛЕДОВАТЕЛНОСТ НА ДЕЙСТВИЯ

1) Определяне на най-уязвимите обекти и степента на поражения в случай на използване на гражданско въздухоплавателно средство с терористична цел.

На територията на Мидландия са определени 15 обекта, които имат потенциално висок риск, ако срещу тях се използва заплаха от въздуха от тип „Ренегат”. Същите са разположени сравнително равномерно върху цялата територия на Мидландия, като най-голям е броят им на територията и в непосредствена близост до столицата и разположеното

до нея гражданско летище. Това са сгради и съоръжения, както и елементи от инфраструктури (административни, обществени, търговски, промишлени - енергетика, химическа промишленост, складове).

Така определените обекти се нанасят на карта, върху която съобразно трасетата и наличната актуална аеронавигационна информация се определят максималните и минимални отдалечения на рубежите за визуално сближение и огнево въздействие (в случай на необходимост), както и най-близките летища за принудително кацане на самолета, нарушил правилата на полетите спрямо всеки един от най-уязвимите обекти. За обектите, за които в зависимост от случая (когато времето за предупреждение и реакция е по-голямо от времето за достигане на гражданския самолет до обекта), като крайна мярка за защита, се определя и назначава обектово прикритие със зенитно-ракетен комплекс (ЗРК) за близко действие, позволяващо огнево въздействие върху самолета „Ренегат” на крайния етап и в най-късен момент, преди същият да порази защитавания обект. Времето за реакция на ЗРК е възможно най-малкия от анализираните в модела времеви интервали. Вероятността то да надвишава времето, необходимо за оценка на обстановката, вземане на решение и подаване на команди за действие е нищожна, поради което считаме с достатъчна за практиката точност, че то няма да бъде критично за изпълнението на задачата по неутрализиране на заплаха от въздуха от тип „Ренегат”.

Още на този етап може да се направи извода и препоръката, че в самото начало и на възможно най-ранен етап трябва да се приведе цялата система за ПВО на страната в най-висока готовност с особено внимание обектовото зенитно-ракетно прикритие на посочените по-горе обекти.

2) Определяне на степента на физическия риск за всеки обект поотделно и за групи обекти, ако са разположени на малко разстояние един от друг.

Определя се по отделна методика, не представлява цел на настоящия модел и не оказва влияние върху решаваната задача.

3) Определяне на рисковите фактори, описване, анализ, изготвяне и поддържане на бази данни.

Рисковите фактори биват количествени и качествени. Определят се от експерти и се нанасят в регистър на рисковите фактори, подобно на таблица 5.7. Примерен вид на този регистър е показан на Таблица 5.8.

Таблица 5.8.

Поле	Описание
Идентификатор на риска	Обикновено уникален алфа цифрова препратка
Наименование на риска	Кратко наименование за означаване на същността
Категория на риска	Използва се като метод за групиране на подобни типове риск (пример ‘Ресурс’ или ‘Финанси’)
Описание на риска	Детайли, включващи контекста, причината и въздействието на риска. (в табличен вид поотделно)
Риск мениджър	Лицето, носещо отговорност и притежаващо пълномощия и ресурси, за да осъществи качествен анализ и ефективно управление на риска
Вероятност	Процентна стойност за индикация на вероятността за поява на риска
Време на въздействие, цена на въздействие и проява на	За качествен анализ се изброяват подреждането и връзката (Висок, Среден, Нисък и т.н.)

Поле	Описание
въздействие	
Действие за намаляване на въздействието на рисковия фактор	Описание на мерките за намаляване на вредното действие на риска, включително и носителя на риска, лицето, което носи отговорност за прилагане на мерките, както и началото и края на действията
Вероятност след прилагане на действието за намаляване на рисковия фактор/Време за въздействие/Цена на въздействие/Стойности на проявяването на въздействието	Прогнозируеми стойности след прилагане на мерките за намаляване на вредното действие на риска
Планове за противодействие на рисковия фактор	Какви дейности са планирани в случай на поява на риска, кога ще се вземе решение за противодействие (може би преди появата на риска)

4) Дефиниране на критериите за успех и на критериите за ефективност. **Критериите** за успех и за ефективност могат да бъдат:

- Ранно предупреждение за наличие на заплаха от въздуха от тип „Ренегат”;
- Своевременно вдигане на изтребителите;
- Успешно насочване на изтребителите;
- Успешно визуално сближение на изтребителя с гражданския самолет;
- Успешно подаване на сигнали, съгласно „Инструкция за действия”;
- Успешно принудително кацане на гражданския самолет;
- Установяване на комуникация с екипажа на гражданския самолет и последващи адекватни действия от негова страна (на всеки етап от изпълнение на задачата);
- Успешно огнево поразяване на самолета, източник на заплахата и недопускане на съпътстващи загуби (да бъде извън границите на населени места и промишлени обекти с потенциално висок риск);
- Използване на минимум ресурси за решаване на задачата;
- Доказване на превъзходство в решаването на такъв тип ситуация и принуждаване на опонента да изхвърли от арсенала си на действия подобни терористични действия.

5) Дефиниране и приоритизация на сценарии по ясно различаващи се критерии за различие. Оптимистичен, песимистичен, най-вероятен, най-малко вероятен и един случаен с най-голяма степен на неопределеност.

Това по-скоро са типове частни ситуации, които описват по-обстойно дадения сценарий. Като такива можем да определим: източникът на заплаха действа от най-близкото международно гражданско летище на територията на Мидландия; източникът на заплаха действа от други летища и нарушаването на режима на полета става по време на транзитен полет над територията на Мидландия; нарушаването на режима на полета става на етап излитане/кацане в Мидландия; нарушаването на режима на полета става на фона на имитация на отказ или авария и др. Колкото повече такива частни ситуации се анализират и проиграят, толкова по-качествен ще бъда крайният резултат.

6) Анализ на действията, които се описват от процедура, която детайлно е регламентирана в съответните инструкции и правила за действия, както и правомощия за вземане на решение. Характерно за тази последователност е, че в зависимост от конкретната ситуация, действията ще се извършват в крайно съкратени срокове от порядъка на минути при недостиг на време и достатъчно изчерпателна информация за обстановката, която ще бъде бързоизменяща се. Предварително отработените действия и подготовката на личния състав имат първостепенно значение за успешно решаване на ситуация от типа „ренегат”.

7) Въвеждане на всички входни данни в цялостен логически модел и математическа обработка на данните. След като бъдат идентифицирани „*рисковите фактори*” (рисковите събития) по таблица 5.8, на база на исторически данни се определя влиянието, което могат да окажат върху операцията. Така могат да се дефинират **вероятностните разпределения** на необходимите разходи и време за реализирането на отделните дейности. Те определят каква е вероятността разходите и продължителността на дейностите да приемат дадена стойност. Различните дейности могат да имат свои специфични разпределения. След това различните разпределения се акумулират, в зависимост от ограниченията, за да бъдат изчислени с по-добра предвидимост на времето и цената на операцията. Техниката е особено полезна, когато има на разположение специализиран софтуер.

За оптимистичния, песимистичния и най-вероятния сценарий се определят **взаимовръзките** между отделните дейности. За точното и прецизно определяне на разходите и отклоненията от графика е необходимо правилното определяне на вида и степента на връзката между дейностите на операцията.

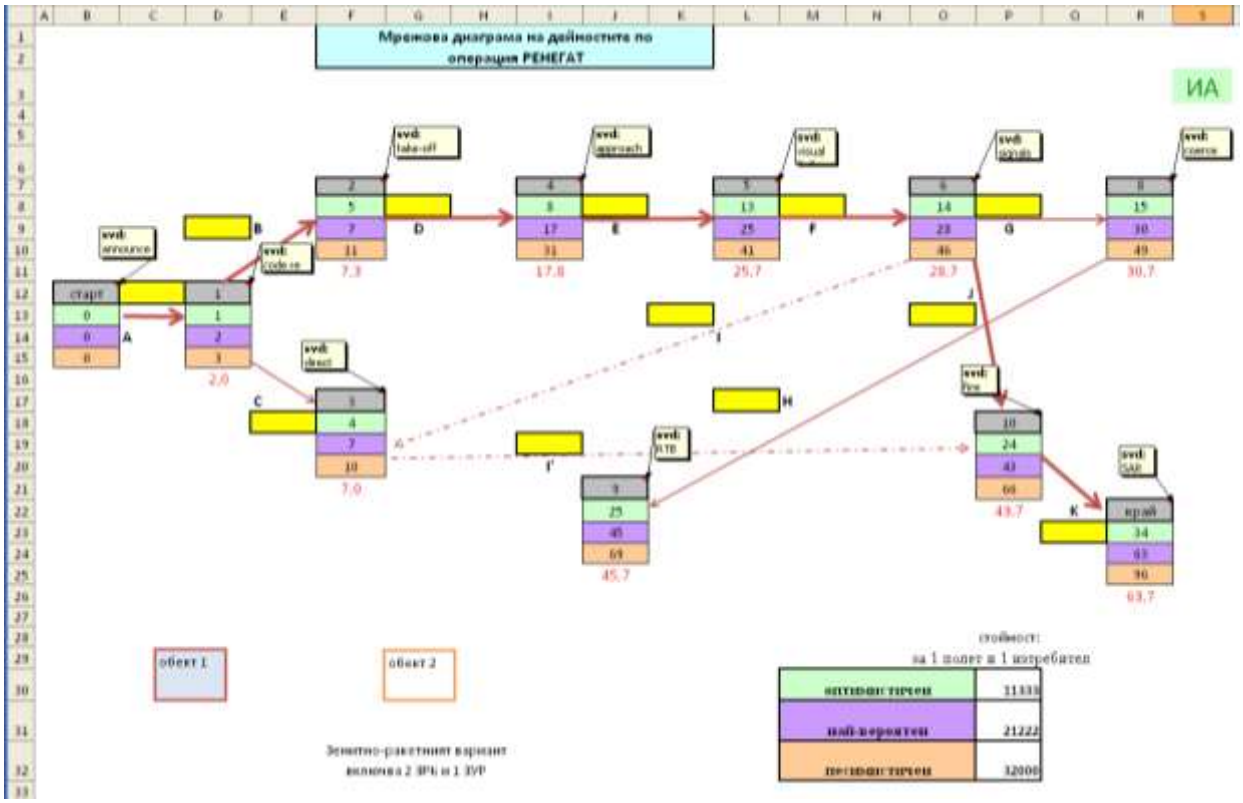
За оценка на конкретния сценарий от гледна точка на критичния фактор време (който носи риск, ако определени времеви параметри излязат от допустими интервали) се използва метода PERT. Той е *количествен* метод, даващ възможност за построяване на мрежова диаграма на дейностите. Предварително е налична информация за граничните времена на всяка дейност по сценария. Използвайки метода PERT, можем да остойностим дейностите, включени в изпълнението на сценария, както и да определим в какви граници да планираме необходимите за осигуряване успешното изпълнение на задачата финансови ресурси (на годишна база). Този метод повишава точността на оценката чрез отчитане на несигурността и риска. За определянето на очакваната стойност на разходите се използва формулата:

$$E = (B + 4M + W)/6 \qquad (5.7)$$

където: E – очаквана стойност, B – оптимистичен вариант, M – реалистичен вариант, W – песимистичен вариант. Специфичните дейности и събития, описващи най-добре сценария, са определени от експертите. Те са:

A. Оповестяване.
B. Привеждане на системата за ПВО в най-висока готовност.
C. Вдигане на изтребителите**.**
D. Сближение.
E. Насочване.
F. Визуално опознаване.
G. Подаване на предупредителни сигнали и сигнали за принудително кацане.
H. Водене на гражданския самолет и изпълнение на принудително кацане.
I. В случай, че не изпълни командите, осъществяване на огнево въздействие**.**
J. Прибиране на изтребителите на летището за базиране или на запасно летище.
K. Търсене и спасяване (при необходимост).

Въз основа на логическата връзка между тях се определя последователността на изпълнение и се построява мрежова диаграма, показана на фигура 5.15:



Фигура 5.15. Мрежова диаграма на дейностите.

Оценяваме времето, което е необходимо за изпълнението на всяка отделна дейност.

Оптимистично време - е най-краткото време, за което е възможно да бъде изпълнена определената дейност;

Най-вероятното време – това, което има най-голяма вероятност да бъде необходимо за изпълнение на определената дейност. То е различно от *Очакваното време*;

Песимистично време – най-дългото време, за да бъде изпълнена определената дейност. Обикновено се използват три стандартни отклонения от средното, за да се даде стойността на песимистичното време.

Методът PERT предполага бета разпределение на вероятността. Стандартното отклонение се изчислява по формулата:

$$\sigma = \frac{b-a}{6} \qquad (5.8)$$

където b е горната граница на времевия интервал, а a е долната граница на този интервал за конкретната дейност.

Общата продължителност на операцията е случайна функция, чиято стойност е между минималната и максималната продължителност на дейностите. Тази функция ще бъде нормално разпределена, тъй като е сбор от няколко случайни променливи.

Изчисляването на критичния път се получава като сума от времената на дейностите от построения модел. Резултатите от модела, реализиран в Excel са показани на фигура 5.15, където с удебелените стрелки е представен критичният път.

От натрупаните статистически данни (главно от "Мейнландконтрол") годишно във въздушното пространство на страните от Регионалния Съюз имаме няколкостотин докладвани случаи на нарушаване на връзката с летателни апарати, като само малка част от тях са реални нарушения на режима на полетите на граждански въздухоплавателни средства, което отнесено пропорционално към площта на територията на Мидландия и плътността на въздушния трафик ни дава крайна величина, която ще бъде един от оценяваните фактори. Нека нейната стойност отбележим с N. Цифрата, която ще изразява броя на вдигнатите изтребители за охрана на въздушното пространство ще бъде 2xN, тъй като задачата се изпълнява с двойка изтребители. Тези величини имат най-голямо значение при остойностяване на полетите за охрана на въздушното пространство и съответно планиране на необходимите за това ресурси. Остойностяването извършваме на база стойност на един час полет на самолет (Цовп) за нуждите на охрана на въздушното пространство.

След като се остойности (по трите варианта: оптимистичен, най-вероятен и песимистичен) при стойност от 20 000 мидландски лири за един час полет на един изтребител и очаквано число от 3 полета годишно за успешното неутрализиране на заплаха от тип "Ренегат" с двойка изтребители, се получават съответно:

- оптимистичен вариант 34 мин. и общ разход от 68 000 мидландски лири,
- най-вероятен вариант 63 мин. и общ разход от 127 333 мидландски лири,
- песимистичен вариант 96 мин. и общ разход от 192 000 мидландски лири.

Получените цифри могат успешно да бъдат използвани за нуждите на планиране на отбраната като финансово изражение на поддържането на съответната военна способност по сценария, съобразно разгледания пример.

Като следваща стъпка, съгласно основната диаграма на дейностите от модела по управление на риска (от фигура 1), за сценария се определя риска във всеки един момент спрямо измененията в обстановката и наличните ресурси. Оценката на риска се извършва по сценарии (съгласно споменатите по-горе типови ситуации, спрямо всеки отделен рисков фактор, спрямо всеки конкретен обект или група обекти). Предполага максимална конкретизация.

Последната стъпка (А6 от основната диаграма на дейностите) е изготвяне на план за управление на риска. Планът за управление на риска, в конкретния случай, включва следната информация: степен на риска и идентификационен номер (според регистъра на рисковете); превантивни действия; дата и изпълнител. Тази информация е попълнена в таблица от вида:

Степен	ID	Превантивни действия	Действа	Дата за действие	Предварителни действия	Действа	Дата за действие
Много висок	2.2	Ясно дава количествени параметри на положителни действия	Заявител	*xx/yy/zz*	Измерва действителните положителни параметри	Ръководител	*xx/yy/zz*
Висок	1.2	Дефинира ясни изисквания	Ръководител	*xx/yy/zz*	Прави преглед	Ръководител	*xx/yy/zz*

Като крайна стъпка се изготвят изводи и препоръки. За тяхното изготвяне допълнително следва да се отчете влиянието на следните фактори, определящи в най-голяма степен ефективността на действия в случай на ренегат:

- Време за предупреждение Тпр (t_1);
- Време за вземане на решение Твр (t_2);
- Време за реакция Тре (t_3);
- Координати, характер и динамика на действия в пространството (височина на полета, скорост, маневриране, безопасни разстояния и височини) на летателния апарат, нарушил режима на полети.
- Комуникация с този летателен апарат (наличност или не, какви данни са обменят и с кого, има ли и каква опасност на борда за пътниците и екипажа, реакция при предупредителни сигнали и действия от страна на изтребителя или боен вертолет и др.).
- Състояние на времето като качество, метеорологични условия, годишно време, коя част от денонощието.
- Състояние на системата за ПВО.
- Ниво на подготовка на личния състав.
- Състояние на летищната инфраструктура (има ли работещо запасно летище за кацане).
- Отдалеченост на рубежите за прехват (визуално сближение) от потенциално най-рисковите обекти на територията на страната.
- Възможности на авиационната техника.
- Възможности по управление, приемане/предаване на управлението, взаимодействие при прелитане на държавната граница.
- География (релеф, водни басейни, инфраструктура, промишлени сгради и съоръжения).
- Политика (политически форуми, заявления, отправени заплахи, наличие на допълнителна актуална информация в реално време в медийното пространство и др.).

Посредством обективното оценяване на риска по изпълнение на операцията и използване на създадения модел има възможност да се отрази реалната стойност на всяка дейност през различните фази на провежданата операция. Това позволява по-точни и прецизни оценки за необходимите разходи и време за реализиране на целите, което спомага вземането на решения.

Крайните резултати от оценката на риска са определените пространствени параметри (рубежи и височини, разстояния и обеми), времеви (срокове и нормативи, честота) и вероятностни (събития, възможност за реакция), а дейностите по управление на риска – организационни, технически, административни и законодателни.

Ефективността на мениджмънта на риска зависи пряко от автоматизирането на дейностите, включването на мотивирани експерти в работните групи, използване на известните техники за анализ и обективна оценка на идентифицираните рискови фактори по отношение на заложената цел. Изборът на софтуерно приложение, с което да се реализират стъпките от модела, допълнително спомага за точното и правилно изграждане на такъв модел, но най-важният елемент си остава осъзнаването на проблемите, свързани с риска, техният адекватен анализ чрез предложените в модела техники, както и изборът на информирано решение за вариантите на действие.

Апробирането на получените резултати дава необходимата увереност за надеждността и практическата приложимост на ефектите от разработените „Математически модели за оценка на риска”. Но най-голямата полза ще се извлече при прилагането им в цялостния процес на отбранителния мениджмънт.

Приложение 6

ПРЕПОРЪЧИТЕЛНИ МЕРКИ ЗА УПРАВЛЕНИЕ И КОНТРОЛ НА ИДЕНТИФИЦИРАНИТЕ РИСКОВИ СЪБИТИЯ СПОРЕД ОЦЕНКАТА НА РИСКА

Идентифицирано рисково събитие	**Необходими мерки за управление и контрол на идентифицираните рискови събития**
1	**2**
I. Фактор 1 1.1 ……. 1.2 ……. 1.3 …….	 1.1.1. ……. 1.1.2. ……. 1.1.3. …….
II. Фактор 2 2.1 …….	 2.1.1. ……. 2.1.2. ……. 2.1.3. …….

Приложение 7

ПРИМЕРНО СЪДЪРЖАНИЕ НА ПЛАН ЗА УПРАВЛЕНИЕ НА РИСКА

1. Въведение.
1.1. Цел на плана за управление на риска.
- Осигуряване управлението на дейностите по идентифициране, анализ, оценка и противодействие срещу рисковете за постигане на целите на организацията, при планирането на отбраната и въоръжените сили.
- Създаване, поддържане и докладване на информация в областта на управление на риска.

1.2. За кого е предназначен планът.
- Планът за управление на риска или части от него могат да бъдат предназначени за ръководството на Министерството на отбраната, за екипа, извършващ дейността и за други вътрешни или външни участници.

2. Организационна политика в областта на управление на риска.
2.1. Общи положения.
- Съответствие със съществуващите стандарти в областта на управление на риска.

2.2. Цели пред управлението на риска.
- Идентифициране и подходящо представяне на приетите цели, свързани с управлението на риска.

2.3. Критерии.
- Представят се критериите, които ще се използват при оценката на рисковете.

3. Организация в областта на управление на риска.
3.1. Роли, права и отговорности.
- Идентифицират се всички роли в процеса на управление на риска и техните права и отговорности.

3.2. Ресурси в интерес на управлението на риска.
- Определят се източниците за осигуряване на ресурси в интерес на управлението на риска, начина за финансиране и контрола върху изразходването на тези ресурси.

3.3. Структура на организацията в областта на управление на риска.
- Определят се структурните звена и състава на участниците в управлението на риска, както и взаимодействието с други лица и организации, извън екипа.

4. Изследване на риска.
4.1. Идентифициране и дефиниране на риска.
- Описание на методите и дейностите, извършвани при идентифициране и дефиниране на рисковете.

4.2. Анализ на риска.
- Описание на методите и дейностите, извършвани при анализа на рисковете.

4.3. Оценяване на риска.
- Описание на методите и дейностите, извършвани при оценяването на рисковете.

5. Взаимодействие и координация.
5.1. Наблюдение на рисковете.
- Ангажименти и организация на наблюдението на рисковете, включително и на тези, които са оценени като приемливи.

5.2. Прегледи на рисковете.
- Определяне на честотата на прегледите и начините за тяхното извършване.

5.3. Докладване на измененията на рисковете, както и за появата на нови или вторични рискове.

- Определя се съдържанието, честотата и предназначението на изготвяните доклади в областта на управлението на риска.

5.4. Координиране с други свързани дейности.

- Извършва се при необходимост, когато са налице подобни организационни дейности, изпълнявани по същото време.

6. Регистър на рисковете.

- Най-често се разработва като отделен документ, но въпреки това се разглежда като част от плана за управление на риска.
- Всеки идентифициран риск се включва в регистъра на рисковете на отделна страница, но също така се разработва обобщение на регистъра, което се използва при подготовка на докладите за управление на риска.
- За всеки от рисковете, включени в регистъра, се разработват мерки за противодействие и редуциране, както и кризисен план за действие след реализирането му.

Терминологичен речник по управление на риска [27]

А

● **Акумулиране на риска** - разглеждане на рискове в комбинация, изразяваща се в това, че един риск може да води до появата на втори, а той от своя страна до появата на трети и т.н., докато накрая се стигне до провал при постигане на поставените цели.

● **Анализ на риска** - процес за разбиране на природата на риска и за определяне нивото на риска. Включва всички дейности за идентифициране на източниците на риска, за неговото описание и измерване, за прогнозиране на неговото време на проявление, честота, вероятност и последствия.

● **Антипатия към риска** - нагласа за избягване на риска.

● **Апетит за риск** - величината и видът на риска, които една организация е готова да търси, запази или приеме.

Пояснение: Апетитът за риск (склонност към риск) е свързан с предела (максимума) на риска като вероятност, ущърб, време и честота на реализиране, до който рискът може да се допусне и толерира.

Б

● **Безопасност** - състояние на защитеност на жизненоважните интереси на личност, организация, предприятие, общество от потенциално или реално съществуващи заплахи.

● **Бизнес риск** - риск, свързан с основните дейности на организацията.

В

● **Величина на риска** - количествена (в числа) или качествена (чрез думи – напр. „нисък”, „висок”) оценка, получена след обобщаване на данните от измерването на риска.

● **Вероятност** (математическа) - мярка за възможността нещо да се случи, изразена като число между 0 и 1, където 0 означава невъзможност, а 1 – абсолютна сигурност.

● **Вероятност** (на риска) - възможност нещо да се случи.

Пояснение: Количественият израз на възможността даден риск да се реализира се нарича вероятност (математическа) на този риск. Изразява се чрез вероятността за трансформиране на риска в проблем. Количествено се изразява като абсолютна стойност в интервала от 0 до 1 и като относителна стойност в проценти от 0% до 100%.

● **Влияние на риска** - изразява се в невъзможност за постигане на част от предварително поставените цели. Влиянието на риска се отразява върху области, свързани с разходите на ресурси, времевите хоризонти за реализацията и някои други аспекти като сигурност, ефективност, ефикасност на дейностите и т.н. Влиянието на риска намира изражение посредством последствията за реализиране на организационните дейности. Последствията от риска могат да се оценяват качествено като пренебрежими, малки, средни, значими и катастрофални или количествено с помощта на различни скали.

● **Въздействие върху риска** - процес за промяна на риска. Включва дейности, насочени към предотвратяване на риска или минимизиране на щетите от него

Пояснение: Въздействието върху риска може да включва:

- Избягване на риска, посредством решение да не се започва или да не продължава дейността, която може да породи риск.

- Приемане или увеличаване на риска с цел възползване от благоприятна възможност. - Премахване на източника на риск.

- Промяна на вероятността.
- Промяна на последствията. - Споделяне на риска с друго лице или лица (включително чрез договори и финансиране на риска).
- Запазване на риска чрез осъзнат избор.

Въздействието върху риска, насочено към преодоляване на негативните последствия, понякога се определя като „смекчаване на риска”, „елиминиране на риска”, „превенция на риска” или „намаляване на риска”. Въздействието върху риска може да породи нови рискове или да видоизмени съществуващи рискове.

● **Външен контекст** - външната среда, в която организацията се стреми да постигне своите цели.

Пояснение: Външният контекст може да включва:

- културната, социалната, политическата, правната, регулативната, финансовата, технологичната, икономическата, природната и конкурентната среда – международна, национална, регионална или местна.
- ключовите движещи сили и тенденции, оказващи въздействие върху целите на организацията.
- отношения със и възприятия и ценности на външните заинтересовани лица.

● **Вътрешен контекст** - вътрешната среда, в която организацията се стреми да постигне своите цели

Пояснение: Вътрешният контекст може да включва:

- управление, организационна структура, роли и отговорности.
- политики, цели, както и стратегии, които се прилагат за постигането им.
- способности, разбирани като ресурси и знания (напр. капитал, време, хора, процеси, системи и технологии).
- информационни системи, информационни потоци и процеси за вземане на решения (както формални, така и неформални).
- отношения със и възприятия и ценности на вътрешните заинтересовани лица.
- организационната култура.
- стандарти, насоки и модели, одобрени във организацията.
- форма и обхват на договорните отношения.

● **Вътрешни одитори** - отдел, звено, консултантски екип или други организация, която предоставя независими, обективни услуги за даване на увереност на ръководството и консултантски услуги, предназначени да добавят стойност и да подобряват оперативната дейност на организацията. Вътрешните одитори помагат на организацията да постигне своите цели чрез използването на систематичен и дисциплиниран подход за оценяване и подобряване на ефективността на процесите за управление на риска, за контрол и управление.

Г

● **Гъвкава устойчивост** - адаптивният капацитет на организацията в сложна и променяща се среда.

Д

● **Диверсифициране на риска** - дейности, при които рискът се разпределя между различни партньори или контрагенти.

● **Добавяне на стойност при вътрешния одит** - увеличената стойност се изразява в подобряване на възможностите за постигане на целите на организацията, идентифициране на оперативни подобрения и/или намаляване на потенциалните рискове и се осигурява посредством предоставянето на одиторски и консултантски услуги.

Е

● **Експозиция (на риск)** - степента, честотата и продължителността, до които една организация и/или заинтересовано лице са изложени на рисков фактор.

● **Ефект на риска** - количествен израз на негативните или позитивните последствия от реализирането на даден риск.

З

● **Заинтересовано лице** - личност или организация, които могат да засегнат, да бъдат засегнати или да се почувстват, че са засегнати от дадено решение или дейност.

Пояснение: Всеки, който взема решения може да бъде заинтересовано лице.

● **Запазване на риска** - приемане на потенциалната полза от печалба или на тежестта от загуба от определен риск.

Пояснение: Запазването на риска включва приемане на остатъчните рискове. Нивото на запазения риск може да зависи от критериите за риск.

● **Заплаха** - възможна надвиснала опасност или предупреждение за надвиснала опасност, например „терористична заплаха”.

И

● **Идентифициране на риска** - процес на намиране, разпознаване и описание на рисковете. Включва определяне на основните рискове за организацията, чрез изясняване на това - какво, къде, кога, защо и как могат да възникнат рискове, чрез описване на възможните рискове и характеризиране на техните елементи.

Пояснение: Идентифицирането на риска съдържа идентифициране на източниците на риска, на събитията и на техните причини и потенциални последствия. То може да се прави на базата на исторически данни, теоретични анализи, обосновани и експертни мнения, и на потребностите на заинтересовани лица.

● **Избягване на риска** - обосновано решение да не се поеме ангажимент с или за оттегляне от дадена дейност, с цел да не се допусне излагане на определен риск или въвличане в рискова ситуация, ако това се случи – да се създадат условия за минимизиране на последиците от риска или за излизане от рисковата ситуация.

Пояснение: Избягването на риска може да се основава върху резултатите от оценката на риска и/или правните и регулаторни задължения.

● **Измерване на риска** - определяне на стойности за вероятността и последствията от даден риск.

● **Източник на риск (рисков фактор)** - елемент, който сам или в комбинация има присъщ потенциал за възникването на отделен риск.

Пояснение: Източникът на риск (рисковият фактор) може да бъде материален или нематериален.

● **Индекс на риска** - персонален идентификационен показател на риска, който служи за подреждането му в приоритизирания списък на идентифицираните рискове. В най-елементарния случай индекса на риска се определя като произведение от оценките на вероятността за реализиране и размера на очакваните последствия.

К

● **Карта на рисковете (Risk Profile)** - документ (форма) със съответен формат за вписване на рисковете и техните количествени и качествени характеристики (напр. название, идентифициране, вероятност, ефект, оценка, мерки). Служи за детайлизирана оценка на

рисковете и за приоритизиране на дейностите по тяхното управление. Позволява да се опишат приложимите методи за контрол над рисковете и да се определят зоните на отговорност по отношение на рисковете и да се разпределят необходимите за тяхното управление човешки и финансови ресурси.

● **Комуникиране и консултиране (при риск)** - непрекъснати и повтарящи се процеси, които вземащите решения в организацията провеждат, за да се предостави, сподели или придобие информация, и за да се влезе в диалог със заинтересованите лица и други такива по отношение на управлението на риска. Тази информация може да се отнася до съществуването, характера, природата, формата, вероятността, сериозността, оценката, статуса, допустимостта и други аспекти на управлението и контрола на риска.

● **Контрол (на риска)** - мярка, която променя риска.

Включва всички дейности по прилагането на решенията, свързани с управлението на риска, т.е. дейности, насочени към понижаване на вероятността от реализиране на риска и намаляване на последствията, ако рискът се материализира (дейности, насочени към подобряване на статуса на риска).

Пояснение: Контролът включва всеки процес, политика, устройство, практика или други действия, които променят риска. Контролът може да доведе до планирания или предполагаемия ефект на промяна на риска.

● **Контролен риск** - рискът, предприетите управленски мерки да са неадекватни/ неефективни.

● **Контролни механизми** - политиките, процедурите и дейностите, част от контролната рамка, които са създадени да гарантират, че рисковете са ограничени в допустимите граници на толерантност, определени в процеса на управление на риска.

● **Кредитен риск** - риск, свързан с кредитния рейтинг на организацията и способността ѝ да обслужва своите кредитни задължения.

● **Критерии за риск** - основни положения (норми, изисквания, параметри или величини), спрямо (чрез) които се оценява значимостта (значението) на риска.

Пояснение: Критериите за риск се основават на организационните цели, външния и вътрешния контекст. Те могат да бъдат изведени от стандартите, законите, политиките и други изисквания.

М

● **Матрица на риска** - инструмент за степенуване и представяне на рисковете чрез дефиниране на диапазони за последствието и вероятността.

● **Мониторинг (на риска)** - непрекъснати проверки, надзор, критично наблюдение или определяне на състоянието, с цел да се установят промените от гледна точка на изискваното и очакваното равнище на изпълнение.

Месечни, тримесечни, полугодишни или годишни прегледи (анализи) с оценка на съдържанието, реализацията и ефективността от дейностите по управление на рисковете, с цел идентифициране на възможностите за оптимизирането им, предприемане на необходимите мерки и актуализиране на списъка от рисковете и техния статус.

Процесът на наблюдение трябва да потвърди наличието на необходимите контроли за дейността на организацията и че процедурите се разбират и изпълняват. Промените в организацията и средата, в която тя осъществява дейността си, трябва да се идентифицират и да се отразяват с необходимите промени в системата.

Пояснение: Мониторингът може да бъде приложен към рамката на управление на риска, процеса за управление на риска, риска или контрола.

Н

● **Неутрализиране на риска** - дейности, при които се осъществява елиминиране или потискане на риска.

● **Ниво на риска** - величина на даден риск, изразена като комбинация от последствия и техните вероятности.

Пояснение: Нивото на риска може да бъде изразено чрез количествена (в числа) или качествена (чрез думи – напр. „нисък”, „висок”) оценка, получена след обобщаване на данните от измерването на риска.

О

● **Одит на управлението на риска** - систематичен, независим и документиран процес за получаване на доказателства и за тяхното обективно оценяване, с цел да се определи степента, до която рамката на управление на риска или всяка отделно взета част от нея е адекватна и ефективна.

● **Опасност** - източник на потенциална вреда.

Пояснение: Опасността може да бъде източник на риск.

● **Оперативен риск** - риск, свързан с начина, по който ежедневно се осъществяват процесите в организацията (и отделните стъпки в процесите).

● **Определяне на риска** - цялостен процес на идентифициране на риска, анализ на риска и оценка на риска.

Пояснение: Определянето на риска се базира на научни знания и технологични изисквания.

● **Оптимизиране на риска** - дейности, при които се осъществява минимизиране на щетите и максимизиране на ползите от риска.

● **Остатъчен риск** - риск, останал след въздействието върху риска.

Рискът, който остава да съществува, след като ръководството е предприело действия за намаляване на ефекта и вероятността от настъпването на неблагоприятно събитие.

Пояснение: Остатъчният риск може да съдържа неидентифицирани рискове. Остатъчният риск може да бъде известен също като „запазен риск”.

● **Отношение към риска** - подход на организацията за определяне на риска и за това дали евентуално рискът да се търси, да се запази, да се приеме или да се избегне.

● **Отчет за риска** - начин за комуникация, предназначен да информира определени вътрешни или външни заинтересовани лица чрез предоставяне на информация относно текущото състояние на риска и неговото управление.

Пояснение: Отчетът за риска се осъществява главно чрез документи, подготвени за акционерите и заинтересованите лица, за мениджърите и служителите на организацията, както и за обществеността, с цел разясняване на политиката на организацията по управление на рисковете и за повишаване на знанието и осведомеността за рисковете.

● **Оценка на риска** - процес на сравняване на резултатите от анализа на риска с критериите за риск, за да се определи дали рискът и/или неговата величина са допустими или приемливи.

Пояснение: Оценката на риска е свързана със степенуване на рисковете, за да се определи тяхното значение и приоритетност. Тя подпомага решението за въздействие върху риска.

● **Оценител на риска** - лице което оценява риска.

П

● **Пакетиране на риска** - дейности, при които даден риск се обединява с друг риск, който има противоположен ефект.

● **Парцелиране на риска** - дейности, при които рискът се разпределя между няколко структурни звена в организацията и по този начин се намалява.

● **План за управление на риска** - план, влизащ в рамката на управление на риска, определящ подхода, управленските компоненти и ресурсите, които трябва да бъдат вложени в управлението на риска.

Пояснение: Управленските компоненти обикновено включват процедури, практики, възлагане на отговорности, последователност и синхронизиране на дейностите. Планът за управление на риска може да бъде приложен към отделен продукт, процес и проект, към част от организацията или към цялата организация.

● **Политика за управление на риска** - деклариране на общите намерения и насоки на организацията, свързани с управлението на риска.

● **Последствие от риска** - резултатът от дадено събитие, което въздейства върху целите.

Пояснение: Едно събитие може да доведе до редица последствия. Последствията могат да бъдат изразени качествено или количествено. Първоначалните последствия могат да ескалират чрез верижни ефекти.

● **Превенция на риска** - дейности, които целят въздействие върху (неутрализиране на вече) възникнал риск, докато той е още с нисък статус, т.е. е незначителен и не е нараснал във времето.

● **Преглед (на риска)** - дейност, предприета за определяне доколко е подходящ, адекватен и ефективен подходът на действие за постигане на поставените цели.

Пояснение: Прегледът може да бъде приложен към рамката на управление на риска, процеса за управление на риска, риска или контрола. Той се осъществява главно чрез месечни, тримесечни, полугодишни или годишни прегледи (анализи) с оценка на съдържанието, реализацията и ефективността от дейностите по управление на рисковете, с цел идентифициране на възможностите за оптимизирането им, предприемане на необходимите мерки и актуализиране на списъка от рисковете и техния статус.

● **Предпазни мерки при риск** - практики, процедури или механизми за снижаване на вероятността от риск или за намаляване на щетите от него.

● **Приемане на риска** - обосновано решение да се допусне реализирането на даден риск и да се изконсумират последствията от неговото реализиране.

Пояснение: Приемането на риска може да настъпи без въздействие върху риска или в процеса на въздействие върху риска. Приетите рискове са обект на наблюдение и преглед. Приемането на риска и реагирането на последствията от него се нарича „общуване с риска”.

● **Приемлив риск** - статус на остатъчен риск, който удовлетворява собственика на риска, т.е. рискът се характеризира с допустимо ниво на вероятност от реализиране и допустимо ниво на щетите, ако се реализира.

● **Присъщ риск** - рискът, преди да бъдат проведени дейностите по неговото управление.

● **Проблем** - представлява риск, който се е реализирал. След реализиране на риска и свързаните с него последствия се изменя състоянието на организацията.

● **Профил на рисковете** - описание на всяка съвкупност от рискове.

Пояснение: Съвкупността от рискове може да включва онези рискове, които се отнасят до цялата организация, до част от нея или както е определено по някакъв друг начин.

● **Процес за управление на риска** - систематично прилагане на политиките за управление, процедурите и практиките към дейностите за комуникиране, консултиране, установяване на контекста и идентифициране, анализиране, оценяване, въздействие, мониторинг и преглед на риска.

Р

● **Раздробяване на риска** - дейности, при които се разделят пространствено или времево източниците на риска или обектите, които могат да претърпят щети при неговото реализиране.

● **Рамка на управлението на риска** - съвкупност от компоненти, които осигуряват основите и организационните разпоредби за проектиране, внедряване, мониторинг, преглед и непрекъснато подобряване на управлението на риска в организацията.

Пояснение: Основите включват политиката, целите, мандата и ангажимента за управление на риска. Организационните разпоредби включват планове, отношения, отговорности, ресурси, процеси и дейности. Рамката на управление на риска е вградена в цялостните стратегически и операционни политики и практики на организацията.

● **Ранно сигнализиране на риска** - дейности, които позволяват диагностициране на Организацията и нейните процеси, така че да се определят възможните „уязвимости”, поради които е възможно да възникнат рискове.

● **Редуциране на риска** - дейности, свързани с намаляване на вероятността и/или на негативните последствия от даден риск.

● **Риск** - въздействие на несигурността върху целите на Организацията.

Пояснение: Въздействието върху целите на организацията може да бъде позитивно или негативно. Несигурността е състояние на недостиг от информация, свързана с разбирането и знанието за дадено въздействие, неговите последствия или вероятност. Целите могат да имат различни аспекти (финансови, здравни, свързани с безопасността, екологични) и могат да се прилагат на различни нива (стратегическо, структурно звено, продукт или процес).

● **Риск мениджър** - човекът, които управлява даден риск.

● **Рисков фактор** - ситуация, събитие, въздействие или процес, които могат да доведат до възникването на отделен риск.

С

● **Сигурност** - функционалното състояние на дадена система, което осигурява неутрализирането и противодействието ѝ на външни и вътрешни фактори, оказващи влияние или можещи да въздействат деструктивно на системата (влошаване организационното състояние на системата или невъзможност за нейното функциониране и развитие).

● **Симптоми на риска** - събития или сценарии, които способстват превръщането (трансформирането) на риска в проблем. Някои автори наричат симптомите на риска с понятието “спусъци” на риска.

● **Склонност към риск** - предел (максимум) на риска като вероятност, ущърб, време и честота на реализиране, до който, според собственика на риска, рискът може да се допусне и толерира. Базира се на управленската философия за допускане на приемливо ниво на риск на приемлива цена.

● **Собственик на риск** - упълномощено лице или организационна единица, отговорни за спазването на всички изисквания и предписания по прилагането на политиката на организацията в управлението на рисковете и по управлението на съответния риск

● **Споделяне на риска** - форма на въздействие върху риска, включваща договорено разпределение на риска с други участници.

Споделяне на риска - дейности, при които част от щетите от риска се прехвърлят частично или напълно (трансферират се) върху друга организация – чрез аутсорсинг, застраховане, хеджиране и или други видове договори.

Пояснение: Правни или регулаторни изисквания могат да ограничат, да забранят или да дадат мандат за споделяне на риска. Степента, до която рискът е споделен може да зависи от надеждността и яснотата на споразуменията за споделяне. Трансферът на риск е форма на споделяне на риска.

● **Статус на риска** - оценка на риска в даден момент, използва се за сравнение с предишни оценки за този риск.

● **Степенуване на рисковете** - сравняване на измерените рискове помежду им на базата на дадени критерии, за да се определи тяхното значение и приоритетност за Организацията.

● **Стратегически риск** - риск, възникващ на нивото на висшия мениджмънт на организацията и свързан със стратегическите цели на организацията и устойчивостта на резултатите от нейната дългосрочна дейност.

● **Схващане за риска** - виждане на заинтересованото лице за даден риск.

Пояснение: Схващането за риска отразява потребности, проблеми, знания, убеждения и ценности на заинтересованото лице. То отразява и начина, по който собственикът на риска се отнася към риска на базата на своите отговорности, цели, опит и знание. Схващането за риска може да се различава от обективните данни за неговата вероятност и възможните последствия от него.

● **Събитие** - възникване или промяна на определена съвкупност от обстоятелства.

Пояснение: Едно събитие може да възникне от една или повече ситуации и може да има няколко причини. Едно събитие може да представлява нещо, което не се е случило. Едно събитие може понякога да бъде определено като „произшествие” или като „злополука”. Едно събитие без последствия може също да бъде определено като “едва избягнато”, “инцидент”, “за малко да ни удари” или “разминаване на косъм”.

Т

● **Толерантност към риска** - готовността на организацията или заинтересованото лице да приеме риска след въздействието върху него с оглед постигане на своите цели.

Пояснение: Толерантността към риска може да бъде повлияна от юридически или регулаторни изисквания.

У

● **Управление на риска (Риск-мениджмънт)** - съгласувани дейности за ръководство и контрол на една организация по отношение на риска. Управлението на риска по своята същност е процес на идентифициране, оценяване, управляване и контролиране на потенциални събития или ситуации (рискове), предназначен да даде разумно ниво на увереност, че целите на организацията ще бъдат постигнати.

Управлението на риска съчетава култура, структура, процеси, практики и защитни мерки, които са насочени към идентифициране, оценка, вземане на решения и осъществяване на дейности по отношение на рисковете в Организацията с цел въздействие върху рисковете.

● **Услуги за даване на увереност** - обективен преглед на доказателствата с цел да се даде независима оценка на процесите за управление на риска, контрол и управление в организацията. Примери за такива услуги включват финансов одит, оперативен одит, одит за съответствие, проверка на сигурността на системата и преглед на състоянието (due diligence).

● **Установяване на контекста** - определяне на външните и вътрешни параметри, които трябва да бъдат отчетени при управлението на риска и при установяването на обхвата и критериите за риск на политиката за управление на риска.

● **Уязвимост** - присъщи свойства на нещо, пораждащи податливост към източник на риск, в резултат на което може да има някакво последствие.

Ф

● **Финансиране на риска** - начин на въздействие върху риска, включващ разпоредби по отношение на непредвидени събития, с цел осигуряване на средства за посрещане и смекчаване на финансовите последствия, ако такива настъпят, както и за покриване на разходите по управлението на рисковете.

Финансирането на риска се осъществява като правило чрез създаване на фонд за компенсиране на щетите от рисковете и за покриване на разходите по управлението на рисковете.

● **Финансов риск** - риск, свързан с ефективното управление и контрол на финансите на организацията и с влиянието на вътрешни и външни фактори върху тях като наличие на кредитен ресурс, валутни курсове, движение на лихвените проценти и др.

Ч

● **Честота** - мярка за вероятността на дадено събитие, изразена като брой събития или резултати за определена единица време.

Забележка: Терминологичният речник по управление на риска е съобразен с Наръчника ISO/lEC Guide 73:2009, „Речник за Риск-мениджмънта“ [10].