

**СТРАТЕГИЯ
ЗА УПРАВЛЕНИЕ НА РИСКА
В ОТБРАНИТЕЛНИТЕ ПРОГРАМИ
НА МИНИСТЕРСТВОТО НА ОТБРАНАТА,
СТРУКТУРИТЕ НА ПРЯКО ПОДЧИНЕНИЕ НА
МИНИСТЪРА НА ОТБРАНАТА И БЪЛГАРСКАТА
АРМИЯ**

Стратегията за управление на риска в отбранителните програми на МО, структурите на пряко подчинение на министъра на отбраната и БА е разработена в отдел „Програмиране на отбранителните ресурси”, дирекция „Планиране, програмиране и бюджет“

Основание за разработване на Стратегията за управление на риска в отбранителните програми на МО, структурите на пряко подчинение на министъра на отбраната и БА: “Закон за финансово управление и контрол в публичния сектор”, „Доктрина за финансово осигуряване” (НП-8, издание А) и „Ръководство за планиране, програмиране, бюджетиране, изпълнение и отчет на отбранителните програми в МО, структурите на пряко подчинение на министъра на отбраната и БА” и Указания на министъра на финансите за управление на риска в организациите от публичния сектор.

Стратегията е въведена със Заповед на министъра на отбраната:

Отговорна структура за разработване и поддържане на документа:
дирекция „Планиране, програмиране и бюджет” - МО.

Таблица за внесени промени:

Дата за внасяне на промените	Дата на приемане на промените	Дата за влизане в сила на промените	Отговорник за внесената промяна

СЪДЪРЖАНИЕ:

1. Въведение	4
2. Цел и обхват на Стратегията	4
3. Дефиниции	5
4. Организиране на процеса за управление на риска в отбранителните програми	8
4.1. Съдържание на процеса за управление на риска в отбранителните програми	8
4.2. Фактори, влияещи върху изпълнението на отбранителните програми и водещи до поява на рискове	10
4.3. Участници, органи и отговорности за управление на риска в отбранителните програми	11
5. Етапи на процеса за управление на риска в отбранителните програми	16
5.1. Първи етап „Създаване на условия за управление на риска“	16
5.2. Втори етап „Идентифициране на рисковете“	18
5.3. Трети етап „Анализ и оценка на рисковете“	23
5.4. Четвърти етап „Противодействие на значимите рискове“	29
5.5. Пети етап „Наблюдение, документиране и докладване на резултатите от управлението на риска в отбранителните програми“	23
Приложение 1 Описание на техники за идентифициране, оценка на рисковете и за дефиниране на техники за реакции	37

1. ВЪВЕДЕНИЕ

Управлението на риска представлява управленска дейност, оказваща влияние върху реализирането на организационните цели и проекти, и подпомагаща ръководителите при вземане на обосновани и рационални решения.

Съгласно съвременните разбирания в областта на мениджмънта управлението на риска представлява част от цялостното управление на организацията и структурата. То не е отделна функция, а е елемент от процеса на организационно планиране и изпълнение на предварително поставените цели, приоритети и задачи.

В тази връзка управлението на риска в отбранителните програми представлява структуриран процес, в рамките на който съществуващите рискове за изпълнението на целите на отбранителните програми в Министерството на отбраната (МО), структурите на пряко подчинение на министъра на отбраната и Българската армия (БА) се идентифицират, анализират, оценяват, планират и наблюдават с помощта на интуитивни, интуитивно-научни и научни методи. За противодействие срещу значимите рискове в отбранителните програми се дефинират, избират и прилагат ефективни дейности, целящи снижаване до приемливи нива на степента на влияние и вероятност за проявление.

Необходимостта от процес на управление на риска в отбранителните програми в рамките на Интегрираната система за управление на ресурсите за отбрана се налага от наличието на много на брой, разнообразни по своята същност и значими по мащаби рискови събития, произтичащи от характера на целите, дейностите, проектите и структурите, включени в отбранителните програми на МО, структурите на пряко подчинение на министъра на отбраната и БА.

Управлението на риска представлява инструмент, подпомагащ управлението на ресурсите за отбрана и допринасящ за успешното изпълнение на отбранителните програми. Неговата ефективност се определя от нивото на организираност, задълбочеността, изчерпателността и качеството на изпълняваните процедури, както и подготовката на ръководния и експертния състав.

Основните параметри на рисковете в отбранителните програми са:

- вероятност за проявление;
- влияние (степен на влияние);
- обща оценка на риска
- време за проявление;
- вероятни причини за проявление (спусъци).

Оценката на рисковете в отбранителните програми е комплексна и включва едновременно оценяване на всички параметри.

Управлението на риска в отбранителните програми включва всички рискови области при планиране, програмиране, бюджетиране, отчет и изпълнение на отбранителните програми и дейностите на структурите в МО, структурите на пряко подчинение на министъра на отбраната и БА.

2. ЦЕЛ И ОБХВАТ НА СТРАТЕГИЯТА

Съгласно Закона за финансовото управление и контрол в публичния сектор (ЗФУКПС) Управлението на риска е един от взаимосвързаните елементи на системите за финансовото управление и контрол (Системите за вътрешен контрол - СВК) в организациите от публичния сектор. Управлението на риска се основава на проучване на добри практики в областта на финансовото управление и контрол в публичния сектор и анализ на текущото състояние на финансовото управление и контрол в публичния сектор в България. Управлението и оценката на риска трябва да бъдат основа за вземането на ключови решения от ръководството на МО. Предизвикателството пред ръководителите на организациите е как да определят рисковете, да оценят вероятността от настъпването им, тяхното влияние и да решат какви мерки трябва да се

предприемат, какви контролни дейности да организират, за да ограничат рисковете до едно приемливо ниво.

Стратегията за управление на риска в отбранителните програми на МО, структурите на пряко подчинение на министъра на отбраната и БА е разработена в съответствие с изискванията на Закон за финансовото управление и контрол в публичния сектор. Стратегията за развитие на вътрешния контрол в публичния сектор на Р България за периода 2018-2020 г., актуалната Интегрирана рамка за вътрешен контрол (COSO 2013) и Концепцията на трите линии на защита, Указания за управление на риска в организациите от публичния сектор, утвърдени със Заповед № ЗМФ 184/06.03.2020 г. на министъра на финансите, Методически насоки по елементите на финансовото управление и контрол. Тя е съобразена с вътрешноведомствените документи: Доктрина за финансово осигуряване (НП-8, издание А), въведена за изпълнение с МЗ № ОХ-433/07.05.2019 г., Ръководство за планиране, програмиране, бюджетиране, изпълнение и отчет на отбранителните програми в МО, структурите на пряко подчинение на министъра на отбраната и БА, въведено за изпълнение с МЗ № ОХ-531/18.06.201 г. и Ръководство за планиране на отбраната, базирано на способности, въведено за изпълнение с МЗ № ОХ-322/29.03.2019 г.

Целта на Стратегията за управление на риска е да дефинира процедурите, практиките и дейностите за управление на риска при изпълнение на отбранителните програми за ефективно и ефикасно управление на ресурсите за отбрана. Обхватът на Стратегията за управление на риска е управление на риска в отбранителните програми (структури) на МО, структурите на пряко подчинение на министъра на отбраната и БА.

Стратегията за управление на риска позволява да бъдат разработени процедури за идентифициране на рисковете, анализ, оценка, наблюдение, контрол и докладване на значимите рискове на съответните нива от програмната структура.

Факторите, от които зависи ефективността на процеса на управление на риска в отбранителните програми са както следва:

- организационна политика за управление на риска;
- навременна подготовка на вътрешноведомствени документи за управление на риска;
- подготвени програмни екипи и екипи за управление на риска.

Стратегията за управление на риска обхваща управлението на риска в отбранителните програми и включва:

- етапи на процеса на управление на риска и тяхното съдържание;
- участници в процеса на управление на риска и техните правомощия и отговорности;
- подходи и методи за организиране и изпълнение на дейностите от етапите на процеса на управление на риска;
- начините за документиране на процеса;
- начина, по който ще се осъществява мониторинг на дейностите по управление на риска;
- ред за докладване;
- съдържание на документите, разработвани за управление на риска и сроковете за тяхното утвърждаване и изпълнение.

3. ДЕФИНИЦИИ

При осъществяване на дейността и изпълнение на функциите си ръководството на организациите в публичния сектор – ръководството на МО и ръководителите на отбранителните програми (ОП) се сблъскват с рискове (потенциални събития), които могат да затруднят тяхната дейност. Възникването на подобни събития в случаите, в които те не са били предвидени и оценени, принуждава ръководителите на ОП да предприемат мерки, а понякога и да разходват

значителни по размер публични средства за премахване на последиците от тях. Като цяло рискът и вероятността за неговата реализация се свързват със случайния характер на събитието и несигурността на възможните крайни резултати от неговата реализация, наличието на различни решения и подходи, възможността да се предвидят, а в определени случаи и да се изчислят вероятностите за един или друг изход (резултат) от събитието, както и наличието на възможности за реализиране на загуба или печалба при дадено развитие на събитието.

Съществуват различни видове техники за управление на рисковете. По-голямата част от тях, в това число и тези, използвани от вътрешните и външните одитори за целите на тяхната одиторска работа, включват количествена и качествена оценка на рисковете. Тази оценка трябва да позволи идентифицирането на дейностите, функциите и задачите, които съдържат най-много рискове и последващата класификация на тези рискове, с оглед на тяхната важност. Тук могат да се споменат и периодичните анализи на икономически и технологични фактори, релевантни за дейността, заседанията на ръководството за целите на стратегическото и оперативното планиране на дейността и заседанията, на които се прави анализ на средата, в която организацията упражнява своята дейност.

3.1. Интегрираната рамка за вътрешен контрол COSO 2013 въвежда четири принципа на Управление на риска:

- Ръководителите на съответната структура или ОП, определят целите с достатъчна яснота, за да позволят идентифицирането и оценката на рисковете, свързани с тях.
- Ръководителите на съответната структура или ОП идентифицират рисковете за постигане на целите си и ги анализират от гледна точка на определяне на подходите и начините за тяхното управление.
- Ръководителите на съответната структура или ОП разглеждат възможностите за измами при оценката на риска и тяхното влияние при постигане на целите.
- Ръководителите на съответната структура или ОП идентифицират и оценяват промените, които биха могли да повлияят значително на системата за вътрешен контрол.

3.2. Концепция за трите линии на защита.

Работната група на Мрежата по вътрешен контрол в публичния сектор (РГМВКПС), в издадената през 2017 г. позиция за трите линии на защита в публичния сектор, прави следното описание на отговорностите по управление на риска и разпределението им в трите линии на защита:

- В първата линия на защита, отговорността на оперативните ръководители в организацията, в качеството им на собственици на риска, е да осигуряват и следят прилагането на вътрешните контроли в организацията. По този начин оперативните (редови) ръководители в организациите от публичния сектор са отговорни за управлението на рисковете.

- Втората линия на защита помага на управлението чрез разработване на конкретни части от рамката за управление на риска, чрез наблюдение и улесняване на прилагането ѝ от оперативното управление, функционирането на ефективни практики за управление на риска и чрез подпомагане на собствениците на риска да докладват адекватна информация, свързана с риска. Субектите от втората линия не притежават риска, но се фокусират върху подпомагане на собствениците на риска.

- Третата линия на защита е независимият вътрешен одит на организациите от публичния сектор, който изпълнява своите отговорности по отношение на Управлението на риска.

Добри практики при управление на риска:

Конкретни насоки за видовете планови документи, техните характеристики и процеса на целеполагане са дадени в Методологията за стратегическо планиране на Република България, одобрена от Съвета за административната реформа. Тяхното прилагане от организациите от публичния сектор ще допринесе за формулирането на ясни, конкретни и измерими цели. Колкото по-ясно са определени целите, които следва да бъдат постигнати, толкова по-лесно ще бъдат идентифицирани рисковете, които могат да застрашат тяхното постигане.

3.3. Въз основа на дефинициите и на добрите практики при управление на риска могат да се изведат следните основни характеристики на управлението на риска:

- Това е процес, свързан с изпълнението на поставените стратегически и оперативни цели;
- Това е динамичен процес;
- Осъществява се на всички йерархични нива;
- Осъществява се в тясно взаимодействие с вътрешния одит на организацията, който предоставя увереност по отношение начина на управлението на риска.

Допълнителни насоки за формулиране на ясни, конкретни и измерими цели съдържа концепцията на SMART целите, според която целите трябва да отговарят на следните критерии:

- Специфични/конкретни (Specific) – да са ясно и точно определени, а не общи цели;
- Измерими (Measurable) – целите да могат да бъдат измерени в единици, да са измерими с преследваните резултати;
- Достижими (Achievable) – целите трябва да са обективно постижими, с оглед на обстоятелствата и разполагаемите ресурси;
- Уместни (Relevant) – целите следва да са обвързани с компетентността, професионалния опит на служителите и с времето за тяхното изпълнение; трябва да са полезни от гледна точка на разглежданата политика, както и да съвпадат с общата визия и мисия на организацията;
- Своевременни (Time-bound) – целите да са формулирани с определен срок на изпълнение (да има поставен краен срок).

3.4. Динамичен процес

Процесът по управление на риска е динамичен процес, обвързан с непрекъснато променящата се среда, в която организацията функционира. Различните фази на процеса се осъществяват непрекъснато във времето и отразяват настъпващите промени. В тази връзка актуализацията на целите, вероятността от настъпване на риск и възможното влияние, мерките, които се определят за реакция на рисковете, са също динамични и трябва да се наблюдават и актуализират непрекъснато.

3.5. Осъществяване на всички йерархични нива

Процесът по управление на риска е отговорност на ръководителя на организацията - МО, но конкретни функции и отговорности по неговото изпълнение съществуват на всички йерархични нива от структурата и от програмната структура. От изключителна важност за ефективността на процеса е ангажираността и разбирането на ръководството и служителите на организацията. Детайлно описание на ролите и отговорностите по управление на риска е дадено в следващата част от Стратегията за управление на риска.

3.6. Други дефиниции

С оглед осъществяването на ефективно управление на риска в настоящата стратегия се използват следните термини, отразяващи както националното законодателство, така и приложимите добри практики:

- Риск е събитие, което ще повлияе върху постигане на целите на организацията. Рискът се измерва с неговия ефект и с вероятността от настъпването му;
- Разумна увереност – задоволително ниво на увереност, което изисква разходите за вътрешен контрол да не надхвърлят очакваните ползи от него. Концепцията за разумна увереност е признание, че не е възможно да се твърди абсолютно и със сигурност, че дадено неблагоприятно събитие няма да се случи въпреки взетите мерки и предприетите действия. Никой не може да постигне абсолютна (100%) увереност поради многобройни фактори, произтичащи от ограничените финансови и други ресурси, ограниченията на източниците на информация, човешките грешки и т.н.;

- Идентифициране на риска – идентифициране на вътрешни и външни събития, които могат да застрашат постигането на целите на организацията;
- Оценка на риска – процес, състоящ се от определяне на степен на вероятност от сбъдването на идентифицирания риск и определяне на степен на влияние (ефект) върху целите на организацията при неговото настъпване;
- Вероятност – представлява възможността дадено събитие да се случи или с други думи колко е вероятно дадено събитие да се прояви;
- Ефект (влияние-степен на влияние) – представлява описание и оценка на това какви биха могли да бъдат последствията/въздействието от настъпило събитие. Ефектът може да бъде както отрицателен, така и положителен;
- Присъщ риск – рискът, свързан с естеството на дейността на организацията при липса на каквито и да е действия (контроли) за смекчаване на вероятността или на ефекта от неговото проявление;
- Остатъчен риск – нивото на влияние и вероятност от риск, което остава след реакцията (контрола) на ръководството към риска. След предприемане на конкретни действия (реакция на риска) продължава да съществува риск, който се нарича остатъчен риск, и по същество изразява факта, че рискът не може да бъде премахнат изцяло. Отговорност на ръководителя е да реши дали равнището на остатъчния риск е приемливо за организацията или е необходимо да бъдат предприети допълнителни действия за неговото намаляване;
- Реакция на риска – мерки/действия за противодействие на риска: за приемане, ограничаване, прехвърляне или прекратяване на риска;
- Риск апетит – нивото на риск, което организацията е склонна да приеме при изпълнение на своята мисия, без да бъде застрашено постигането на целите.

4. ОРГАНИЗИРАНЕ НА ПРОЦЕСА ЗА УПРАВЛЕНИЕ НА РИСКА В ОТБРАНИТЕЛНИТЕ ПРОГРАМИ

4.1. Съдържание на процеса за управление на риска в отбранителните програми

Определение за „риск” - Риск е възможността да настъпи събитие, което ще повлияе върху постигане на утвърдените и планирани цели на структурата (организацията) или отбранителната програма. Рискът се измерва с неговото влияние (степен на влияние) и вероятност за проявление.

Управлението на риска е процесът по идентифициране, анализ, оценяване, мониторинг, противодействие и докладване на рисковете, които могат да повлияят върху постигане на целите на организацията и въвеждането на необходимите контролни дейности, с цел ограничаване на рисковете до едно приемливо равнище.

Управлението на риска в отбранителните програми (структурите) е непрекъснат процес, осигуряващ добро разбиране на потенциалните заплахи, действия или събития, които могат положително или отрицателно да повлияят на способността на отбранителната програма (структурата) да постигне своите планирани цели и дейности.

Управлението на риска е задължителна част от мениджмънта на отбраната и управлението на ресурсите за отбрана и е ключова дейност, допринасяща за постигане на целите на отбранителната програма и на МО като организация.

Основна предпоставка за ефективното управление на риска е определянето на ясни, измерими цели и тяхното разбиране. Правилното управление на риска е невъзможно да бъде извършено, ако в отбранителната програма (структурата) не е въведен адекватен процес на целеполагане. Трябва да съществуват цели, преди да се идентифицират рисковете, които ги застрашават и да се вземат мерки за тяхното управление. Целите трябва да бъдат утвърдени от ръководителите на отбранителни програми, като целите следва да съответстват със

стратегическите и оперативните цели на организацията - МО. Целите на отбранителните програми се постигат чрез изпълнението на конкретни дейности и задачи в определени срокове.

Процесът на Управлението на риска е предназначен да даде разумна увереност, че целите на организацията ще бъдат постигнати. В тази връзка ефективното управление на риска е невъзможно и безсмислено, без предварително да са ясно определени целите на съответната организация от публичния сектор. Процесът по управление на риска следва да е съобразен със стратегическите и оперативните цели на организацията.

Целите на Министерството на отбраната се дефинират, както следва:

- Стратегическа цел на отбранителната политика на Министерството на отбраната. Стратегическите цели се илюстрират обикновено с формулировката „КАКВО трябва да постигне организацията след няколко години?“. КАКВА искаме да бъде организацията след няколко години? Такива са целите, заложи в стратегическите планиращи документи на организацията.

- Основни цели на областите на политика в сектор „Отбрана“ (отбранителни политики). Основните цели на областите на политика са оперативни цели на организацията. Оперативните цели се илюстрират с формулировката „КОИ са стъпките, които трябва да се предприемат и КАК да се постигне това, което искаме или сме планирали?“. Основните цели детайлизират стратегическите цели, определят точния критерий за оценка на изпълнението им и времето за това изпълнение. Насочени са към отделни области и дейности в организацията – финанси, отбранителни способности, човешки ресурси, публичност, вътрешен контрол и др. Една основна цел може да служи за постигането на повече от една стратегическа цел.

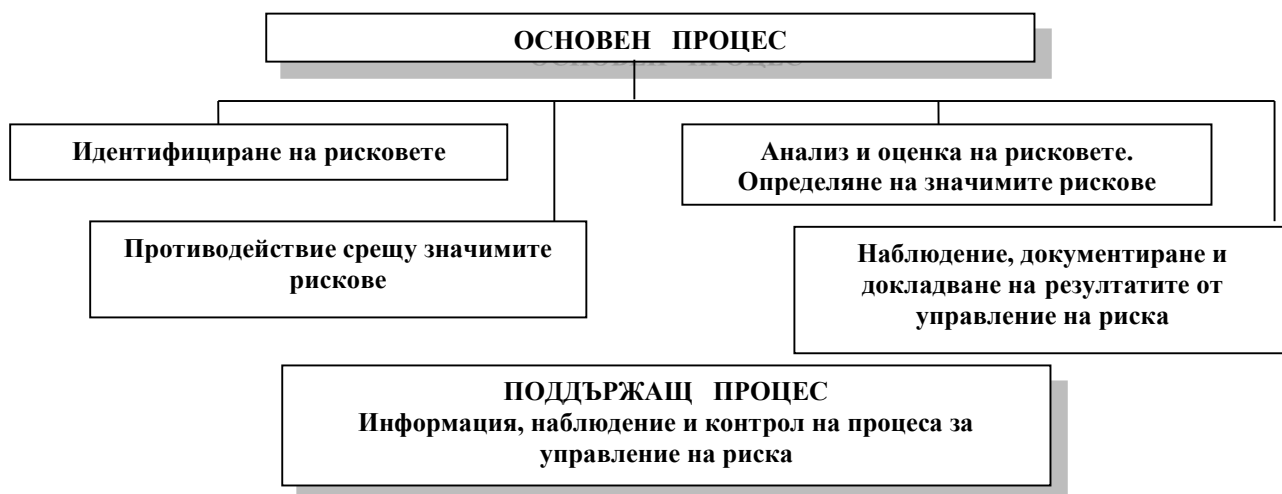
- Главни и допълнителни (спомагателни или поддържащи) цели на отбранителните програми, трябва да подпомагат изпълнението на основните цели на отбранителните политики в сектор „Отбрана“. Това са оперативни цели на ниво отбранителни програми.

Документите, в които се утвърждават целите на отбранителните политики и отбранителните програми (структурите) в МО са: дългосрочна Програма за развитие на отбранителните способности на Въоръжените сили (ВС) 2032 (Програма 2032), Указания на министъра на отбраната по отбранителната политика, План за развитие на ВС за средносрочен период – План за развитие на ВС до 2026 г. (План 2026), Национален план за повишаване на разходите за отбрана на 2% от Брутният вътрешен продукт на Република България до 2024 г. (Национален план), Указания за програмиране на министъра на отбраната за шестгодишен период, Меморандум на програмните решения за шестгодишен период и програмните меморандуми на отбранителните програми в МО, структурите на пряко подчинение на министъра на отбраната и БА за шестгодишен период.

Въвеждането на управлението на риска осигурява на ръководителите достатъчно предварителна информация за потенциалните събития, застрашаващи целите и за дейностите за противодействие за намаляване на негативното им влияние и вероятността за проявлението им.

Процесът за управление на риска в МО, структурите на пряко подчинение на министъра на отбраната и БА включва следните процеси:

- **основен процес** - определяне на областите и категориите за проявление на рисковете; идентифициране на рисковете; анализ и оценка на идентифицираните рискове; определяне на значимите рискове и планиране на дейности за противодействие срещу значимите рискове; реакции на риска, наблюдение, документиране и докладване на резултатите от управлението на риска;
- **поддържащ процес** - информация, наблюдение и контрол на измененията в рисковете.



Фиг. 1 Съдържание на процеса за управление на риска

При прилагане на етапите и практиките на процеса на управление на риска се използва смесен подход, включващ централизиран и децентрализиран подход на различните нива на програмната структура. Прилагането на смесения подход, изисква непрекъснато повишаване на подготовката на експертите, участващи в процеса на управление на риска.

При управлението на риска до ниво основна програма се прилага децентрализиран подход. Във всяка отбранителна програма (структура) индивидуално се изпълняват дейностите от етапите за управление на риска, въз основа на Указанията за програмиране на министъра на отбраната и указанията на ръководителя на отбранителната програма.

При управлението на риска в МО се прилага централизиран подход. При него резултатите се включват в обобщена карта на рисковете, обобщен риск регистър и обобщен План за управление на риска в отбранителните програми в МО и структурите на пряко подчинение на министъра на отбраната и БА и обхващат утвърдените значими рискове за МО. Тези документи се изготвят на базата на картата на рисковете, риск-регистъра на всяка основна отбранителна програма, както и план за управление на риска на всяка основна програма за бюджетната година.

4.2. Фактори, влияещи върху изпълнението на отбранителните програми и водещи до поява на рискове

Рисковете могат да бъдат определени в хода на дългосрочното, средносрочното и краткосрочното планиране на дейността на организацията (структурата). Няма значение какъв ще бъде методът за определяне на рисковете. Важното е ръководството да взема под внимание факторите, които могат да допринесат за появата на даден риск или за увеличаване на степента на важност на вече идентифициран риск. Като нагледен пример основни фактори в случая могат да бъдат:

- непостигането на предходни планирани цели;
- компетентност на персонала;
- географско разпределение на упражняваните функции и дейности;
- сложност на извършваните операции;
- степен на важност на операциите и др.;
- промени в законодателството, текучество на персонала и други, които оказват влияние върху организацията.

Факторите, които влияят върху изпълнението на отбранителните програми (структурите) и върху постигането на планираните цели, приоритети и задачи са разпределени в три основни групи:

- Външни фактори за МО - влияят косвено върху изпълнението на отбранителните програми. Те могат да бъдат: военно - политически; икономически; правно-нормативни; ниво на научно-техническото развитие; свързани с опазване на околната среда и др.

Външните фактори са свързани с икономическото развитие на страната и макроикономическите показатели, с политиката на правителството в областта на отбраната, управленската програма на правителството, средносрочна бюджетна прогноза за тригодишен период, Закона за държавния бюджет на Р България за бюджетната година и постановлението на Министерския съвет за изпълнение на държавния бюджет. Те са: нивото на бюджета на МО като процент от Брутният вътрешен продукт (БВП); ограничения върху бюджета на МО, наложени от противоепидемичната обстановка в страната; осигуряване на целевите средства в Централния бюджет за изпълнение на приоритетните инвестиционни проекти за модернизация на ВС, изпълнение на Националния план.

- Вътрешни фактори за МО - влияят пряко върху изпълнението на отбранителните програми. Те са: разпределение на бюджета на МО по области на политика и отбранителни програми; разпределението на бюджета на МО по направления на разходите; нивото на капиталовите разходи; програмната структура; необходимите отбранителни способности на ВС; утвърдените приоритети за МО; поетите ангажменти към НАТО и ЕС; декларирани сили и способности за НАТО и Обща политика за сигурност и отбрана на ЕС (ОПСО на ЕС); участващи формирования от ВС в операции и мисии извън територията на страната; видове осигуряване и поддръжка; инфраструктура; обучение и капацитет на личния състав и др.

- Вътрешните фактори за отбранителните програми (структури) са следните: командване и управление; структура на военните формирования; инфраструктура; логистично осигуряване и поддръжка; приета програмна структура; капацитет на програмните екипи; системи за комуникационно-информационно осигуряване; обучение и подготовка; разпределение на финансовите ресурси по направления на разходите; окомплектоване с личен състав; изпълнение на инвестиционните проекти за модернизация на ВС и др.

4.3. Участници, органи и отговорности за управление на риска в отбранителните програми

4.3.1. Ръководители на организациите от публичния сектор

Предвид нормативните разпоредби, както и в съответствие с добрите практики, отговорностите на ръководителите на организациите по отношение на управлението на риска могат да се систематизират по следния начин:

1. Ръководителите трябва да демонстрират с поведението си разбиране на важността и подкрепа за дейностите по управление на риска;

2. Ръководителите отговарят за определяне на мисията, визията и стратегическите цели на организацията. Те трябва да създадат условия за формулиране на ясни, конкретни и измерими цели, осигурени с конкретни по размер и източник ресурси, в съответствие със съществуващите нормативни изисквания и добри практики. Предвид значението на правилното целеполагане за ефективността на СВК и в частност на управлението на риска (описано подробно в Методическите насоки по елементите на финансовото управление и контрол), тези отговорности на ръководителите на организациите са ключови за реалното функциониране на управлението на риска;

3. Част от отговорността по целеполагане на ръководителите е утвърждаването на Стратегически план (Бизнес-план или програма и др.), който да отразява общите (стратегически) цели на организацията и да бъде съгласуван с целите на други организации, обхващащи дейността на няколко организации и др. Стратегическият план следва да обхваща период не по-малък от 3 години;

4. Ръководителят на организацията утвърждава Стратегия за управление на риска, която се актуализира периодично (на всеки три години), както и при настъпване на съществени промени в рисковата среда;

5. Ръководителят на организацията трябва да определи Риск-мениджмънт, както и да разпредели ясно отговорностите по управление на риска сред средното ниво на ръководството на организацията и служителите;

6. Отговорност на ръководителя на организацията е да осигури предприемане на коригиращи действия на база на информацията от мониторинга на риска.

Звено/лице, отговорно за управлението на риска (риск-мениджмънт)

Съгласно модела на трите линии на защита ръководството на организацията установява дейности по управление на риска, които да помогнат при изграждането и/или мониторинга на контролите на първата линия на защита. В зависимост от спецификите на организацията и сектора, формата на тези дейности може да варира, но най-често втората линия на защита включва структура (звено или комитет) или служител, който координира управлението на риска. В МО е създаден Комитет за управление на риска. Председател на Комитета за управление на риска е директорът на дирекция „Планиране, програмиране и бюджет“.

Целта на тази структура или служител е да дава увереност на ръководството, че първата защитна линия е изградена правилно и функционира според очакванията, във връзка с управлението на риска в организацията.

Ръководителят на организацията може да определи, назначи или да създаде Риск-мениджмънт (звено/комитет за управление на риска, Риск-ръководител/мениджър или служител по управление на риска). За да разполага с нужната позиция за изпълнение на функциите си, Риск-ръководителят следва да бъде ръководител на високо ниво в организацията и да познава добре структурата и дейността на организацията, нейните стратегически и годишни цели, както и да има познания за същността на процеса по управление на риска.

Риск-мениджмънтът има отговорности по:

1. Създаване на организация за разработване на Стратегията за управление на риска, съответно нейната актуализация;

2. Координиране, организиране и информационно обезпечаване на дейностите по идентифициране и оценка на риска и определяне на реакции на риска;

3. Осигуряване на отразяването на рисковете и тяхната оценка, на резултатите от извършените по управление на риска действия, сроковете, в които действията ще бъдат предприети и отговорните лица, в специален документ – риск-регистър, както и да се подсигури неговото редовно актуализиране;

4. Консултиране, организиране и провеждане на обучения по теми, свързани с управлението на риска;

5. Организиране и координиране на обмяната на знания и информация по отношение на управлението на риска между трите линии на защита;

6. Организиране на осъществяването на мониторинг на управлението на риска. Целта на мониторинга е да се установи дали след прилагането на избраната реакция, рискът е бил намален до приемливо за организацията равнище и ако е необходимо да се изберат подходящи допълнителни действия. В резултат от мониторинга, управлението на риска се наблюдава непрекъснато на всеки един етап като част от общия процес на управление, заедно с текущите промени, които могат да повлияят на целите или на възможността те да бъдат постигнати, за да придобие увереност, че процесът по управление на риска е ефективен и ефикасен;

7. Докладване на ръководителя на организацията на обобщена информация по отношение управлението на риска под формата на отчети (доклади). При необходимост от предприемане на

коригиращи действия, в резултат от мониторинга, Риск-мениджмънтът докладва на ръководителя на организацията, организира и координира тяхното разработване в съответствие със Стратегията за управление на риска.

4.3.2. Ръководители на структурни звена в организацията (оперативно ръководно ниво)

Оперативните ръководители или средното ниво на ръководство формират първата линия на защита. В тази връзка те са пряко отговорни за управлението на рисковете, както и за прилагането на коригиращи действия при наличие на недостатъци в процесите и контрола. Според позицията на Международния институт на вътрешните одитори (The IIA) оперативното ръководство идентифицира, оценява, контролира и ограничава рисковете в процеса на развиване и прилагане на вътрешни политики и процедури в цялостното управление на дейностите, уверявайки се, че те функционират в съответствие с предварително заложените цели. Отговорностите на ръководителите на структурни звена (отбранителни програми) в организациите от публичния сектор включват:

1. Всеки ръководител на структурно звено (отбранителна програма) в организациите от публичния сектор е „собственик на риска“ по отношение на целите, функциите и дейностите, стоящи за изпълнение пред ръководеното от него звено;

2. Като собственици на риска ръководителите на структурни звена в организациите идентифицират и оценяват рисковете съобразно подхода избран от организацията и утвърден със Стратегията за управление на риска. Отговорността на всеки риск-собственик е преди всичко по отношение на идентифицирането и оценката на рискове, които стоят пред ръководеното от него звено/дейност и на второ място по отношение на идентифицирането и оценката на рисковете, стоящи пред организацията като цяло;

3. Ръководителите на структурни звена (отбранителни програми) са отговорни за анализ и актуализация на контролните дейности, целящи ограничаването на идентифицираните и оценени рискове, спрямо които съответното структурно звено трябва да реагира, предвид възприетото ниво на риск апетита в цялата организация;

4. Ръководителите на структурни звена са отговорни да провеждат мониторинг на резултатите от управлението на риска в ръководените от тях звена/дейности. Те докладват резултатите на Риск-ръководителя, който е отговорен за предприемането на по-нататъшни действия. При нужда от предприемане на коригиращи действия, ръководителите на структурни звена участват съобразно компетентността си в тяхното разработване.

4.3.3. Служители на организацията

Служителите на организацията са тези, които прилагат ежедневно контролните дейности, разработени за управление на рисковете. В тази връзка те са в позиция да установят първи евентуални слабости, нередности или проявления на рискове.

Отговорностите на служителите са, както следва:

1. Да подпомагат оперативните ръководители в процеса на управление на риска, като осигуряват нужната за целта информация и участват активно в дейностите по оценка на идентифицираните рискове и въведените контролни процедури;

2. Да докладват на оперативното ръководство за възникващи проблеми, които могат да застрашат постигането на целите;

3. Да докладват на оперативното ръководство за потенциални възможности за подобрене на СВК.

4.3.4. Вътрешен одит

Съгласно Стандартите, вътрешният одит задължително трябва да оценява ефективността и да допринася за подобряването на процесите на управление на риска. Когато подпомагат ръководството при изграждането или подобряването на процесите по управление на риска, вътрешните одитори задължително трябва да не поемат управленска отговорност за практическото управление на рисковете. В този смисъл отговорността на вътрешния одит е да предоставя обективно мнение по отношение на управлението на риска чрез извършване на одитни ангажменти при спазване на приложимата нормативна рамка и Стандартите.

4.3.5. В процеса на управление на риска на различните нива в МО участват:

В Министерството на отбраната:

- Програмнен съвет към министъра на отбраната;
- Комитет за управление на риска в отбранителните програми на МО, структурите на пряко подчинение на министъра на отбраната и БА;
- Дирекция „Планиране, програмиране и бюджет”.

В отбранителните програми:

- ръководители на отбранителни програми;
- програмни екипи;
- екипи за управление на риска в отбранителните програми.

Председателят на Програмния съвет към министъра на отбраната ръководи процеса на управление на риска, като обсъжда и предлага на министъра на отбраната за утвърждаване „План за управление на риска в отбранителните програми на МО, структурите на пряко подчинение и БА” с приложения „Риск-регистър на значимите рискове” и „Карта на значимите рискове”.

Програмният съвет обсъжда и предлага на министъра на отбраната периодични Доклади за резултатите от управлението на риска в отбранителните програми за шестмесечието и деветмесечието на текущата година и годишен за предходната година. Приема и обсъжда ежесмесечна информация за „Изменение на нивата на значимите рискове в отбранителните програми на МО и влиянието им върху изпълнението на целите, приоритетите и задачите“ (при необходимост).

Директорът на дирекция „Планиране, програмиране и бюджет” непосредствено организира, планира, координира и контролира дейностите по управление на риска в МО и в отбранителните програми на МО, структурите на пряко подчинение на министъра на отбраната и БА. Обикновено той е председател на Комитета за управление на риска в МО.

Дейността на Комитета за управление на риска е свързана с изпълнението на следните функции:

- Координация на въпросите, свързани с управлението на риска в отбранителните програми (структурите) в МО, структурите на пряко подчинение на министъра на отбраната и БА;
- Управление на значимите рискове за МО;
- Подготовката на длъжностите лица (експертите) от екипите за управление на риска в отбранителните програми;
- Съгласуване на методите и подходите за управление на риска в МО в отбранителните програми (структурите);
- Подготовката на всички документи по управление на риска в отбранителните програми и внасянето им в Програмнен съвет към министъра на отбраната.

Ръководителите на отбранителни програми (структури) са отговорни за организиране, планиране, координиране и контролиране на дейностите по управление на риска, касаещи съответната отбранителна програма.

Органите за управление на риска се формират със заповеди на министъра на отбраната за състава и структурата на Комитета за управление на риска в отбранителните програми на МО,

структурите на пряко подчинение на министъра на отбраната и БА и за състава и структурата на екипите за управление на риска в основните програми и програмите на МО, структурите на пряко подчинение на министъра на отбраната и БА.

Органите за управление на риска в отбранителните програми се формират със заповеди (разпореждания, възлагане на допълнителни отговорности) на ръководителите на отбранителните програми (структури) и включват състава и структурата на екипите за управление на риска на всички подчинени нива от програмната структура.

Комитетът за управление на риска в отбранителните програми на МО осъществява постоянен мониторинг, контрол и докладване за процеса на управление на риска в отбранителните програми на МО, структурите на пряко подчинение на министъра на отбраната и БА. Председателят на Комитета внася на заседания на Програмния съвет към министъра на отбраната годишния План за управление на риска в отбранителните програми за бюджетната година и периодичните доклади за резултатите от управлението на риска в отбранителните програми.

Екипите за управление на риска включват в състава си ръководител на екипа, секретар и членове (броя на членовете е в зависимост от състава на отбранителната програма). Екипите трябва да отговарят на следните условия:

- да бъдат съставени от експерти, които да имат познания (да работят) в структури, отговорни за поддържане/изграждане на отбранителни способности на ВС, области от способности и елементи на отбранителните способности съгласно Плана за развитие на ВС до 2026 г. и приети в НАТО или да работят в различни области и дейности, свързани с отбранителната програма;
- да могат да формират решения в областта на управление на риска и да ги предлагат на ръководителите на отбранителни програми;
- по възможност екипът за управление на риска в отбранителната програма да не включва членове на програмния екип.

5. ЕТАПИ НА ПРОЦЕСА ЗА УПРАВЛЕНИЕ НА РИСКА В ОТБРАНИТЕЛНИТЕ ПРОГРАМИ

Процесът на управление на риска обхваща пет етапа, съгласно Схема 1.

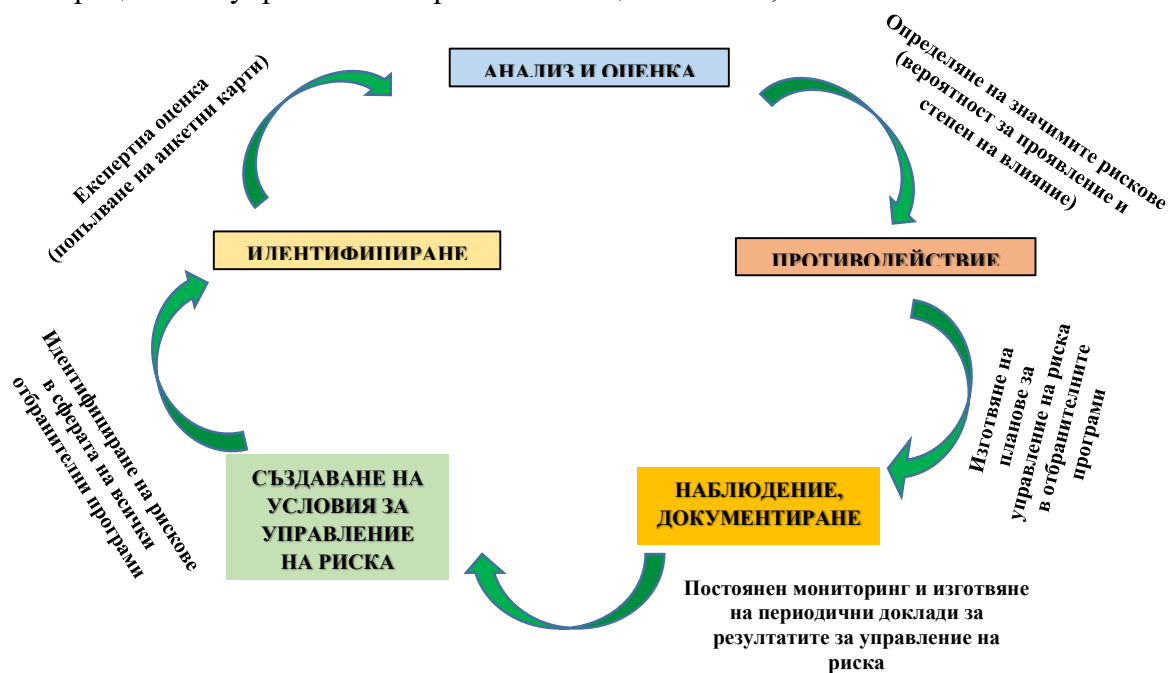


Схема 1 - „Етапи на процеса за управление на риска”

Редът за работа на екипите за управление на риска през етапите на процеса на управление на риска и съдържанието на документите подробно са посочени по стъпки и с примери в разработеното „Методическо пособие за разработване на документи по управление на риска в отбранителните програми на МО”.

5.1. Първи етап „Създаване на условия за управление на риска“

През този етап не се изпълняват ежегодно всички документи, касаещи управлението на риска. Издават се ежегодно Указания за програмиране на министъра на отбраната за шестгодишен период, Меморандум на програмните решения за шестгодишен период и се разработват програмни меморандуми на отбранителните програми за шестгодишен период.

Създаването на условия за управление на риска е предпоставка за ефективно идентифициране и оценка на рисковете, застрашаващи целите на организацията или на отбранителната програма и за предприемане на адекватни реакции на тези рискове. Извършването на дейностите, включени в тази стъпка, е отговорност на ръководителя на организацията от публичния сектор. За да създаде условия за ефективно управление на риска, ръководителят на организацията от публичния сектор трябва да предприеме следните действия:

1. Да утвърди стратегически план на организацията - МО, който да отразява общите (стратегически) цели на МО, отбранителните програми и структурите. В Методическите насоки по елементите на финансовото управление и контрол и Указанията за управление на риска се съдържат достатъчно указания по отношение на стратегическия план. В МО са разработени и утвърдени стратегически планиращи документи Програма 2032, приета с решение на Народното събрание и План 2026 (ПМС № 183/07.05.2021 г., ДВ бр. 38/11.05.2021 г.).

2. Да утвърди Стратегия за управление на риска. Стратегията за управление на риска трябва да съдържа описание на:

- подхода и методите, които ще бъдат използвани в процеса на управлението на рисковете;
- начините за документиране на процеса;
- начина, по който ще се осъществява мониторинг на дейността по управление на рисковете;
- реда за докладване;
- отговорностите на лицата, изпълняващи дейности по управление на риска.

Съгласно изискванията на ЗФУКПС Стратегията се актуализира на всеки три години или при настъпване на съществени промени в рисковата среда. Разработването на Стратегията и докладването ѝ на ръководителя на организацията за утвърждаване, както и предприемането на действия по нейното актуализиране, е отговорност на Риск ръководителя, в МО – на Председателя на Комитета за управление на риска.

3. Да определи Риск-мениджмънта и отговорностите по управление на риска. В Методическите насоки по елементите на финансовото управление и контрол и в Указанията за управление на риска в организациите от публичния сектор се съдържат достатъчно указания по отношение на изискванията и процеса на определяне на Риск мениджмънта и по определяне на останалите отговорности по управление на риска.

4. Да утвърди риск-апетита на организацията.

5. Да осигури необходимите ресурси във връзка с изпълнение на задълженията по управление на риска.

Разработването и прилагането на контролни дейности, представляващи една от възможните и най-често прилаганата реакция на риска, предполага осигуряването на нужните ресурси – човешки, финансови, информационни и т.н. В тази връзка и предвид факта, че управлението на

риска е неразделна част от планирането и определянето на целите и годишните приоритети на ОП (структурите), е важно процесът на управление на риска да се обвърже с процеса на изготвяне на бюджетите на ОП (структурите). За разпоредителите с бюджет това означава да се съобразят със сроковете и дейностите по бюджетната процедура за съответната година, съгласно Закона за публичните финанси и други.

По-конкретно следва да се имат предвид следните дейности:

- При изготвянето на средносрочните бюджетни прогнози следва да се съобразят и да се координират целите, заложи в стратегическия средносрочен план – План за развитие на ВС до 2026 г., както и Меморандум на програмните решения за шестгодишен период;
- Ръководителите на ОП трябва да обвържат стратегическите и годишните цели на ОП с областите на политики/функционални области;
- Трябва да се предвидят нужните финансови средства за изпълнението на целите на организацията, включително средства за разработването и прилагането на контролни дейности, представляващи реакция на риска;
- Заедно с отчитането на бюджета трябва да се извършва преглед на риск-регистъра и на база на резултатите от мониторинга трябва да се обсъжда ефективността на предприетите реакции на рисковете и съответно да се извършва актуализация на идентифицирането и оценката на рисковете и на съответните реакции.

6. Да осигури необходимите условия Стратегическият план, Стратегията за управление на риска, както и всяка друга относима информация да бъдат ефективно комуникирани със служителите на организацията.

Публикуването на информацията на КИС „ЩИТ“ за даване на достъп до документите е минимално изискуемото, но не е достатъчно за ефективна комуникация и създаване на култура на управление на риска. Ръководният състав на организацията и програмните ръководители трябва да демонстрират с поведението си разбиране на важността и подкрепа за дейностите по управление на риска.

За целта ръководителите на отбранителни програми трябва да инициират регулярно активни дискусии по въпросите на управление на риска, да използват проактивно резултатите от мониторинга на риска, да демонстрират разбиране между целите на програмата (структурата) и рисковете и да комуникират тази връзка със служителите на програмата (структурата).

5.2. Втори етап „Идентифициране на рисковете“

Идентифицирането на риска в отбранителните програми представлява втори етап от процеса на неговото управление. Изразява се в прилагане на разнообразни техники за откриване, дефиниране и документиране на възможните области на несигурност, неопределеност или промяна по отношение на изпълнението на отбранителните програми.

Идентифицирането на риска се заключава в разкриване и дефиниране на рисковете, които могат да окажат влияние върху постигане на целите, приоритетите и планираните резултати на програмата. Идентифицирането на рисковете в отбранителните програми започва по време на разработването на програмните меморандуми на всички нива от програмната структура. Програмните екипи при планиране на ресурсите за отбрана в меморандумите на отбранителните програми разкриват и идентифицират възможни рискове, които дават отражение върху отбранителната програма.

Всеки собственик на риска изготвя риск-регистър за своите рискове и на тази база се изготвя риск-регистър на цялата организация с т.н. хоризонтални рискове – валидни за цялата организация. За относително малките организации – може да се изготви един общ риск-регистър. Идентифицираните рискове се документират от Риск-ръководителя в Риск-регистъра, съдържащ Стратегическите и оперативните цели на организацията и идентифицираните до момента рискове, които могат да застрашат постигането на тези цели.

Идентифицирането на рисковете трябва да се извърши по отношение на всяка стратегическа или оперативна цел. Ако различните структурни звена на организацията са дефинирали своите оперативни цели за постигане на стратегическите цели, идентифицирането на рисковете по всяка оперативна цел ще осигури и идентифициране на рисковете за всяко структурно звено. През този етап риск-собствениците трябва да идентифицират присъщите рискове, които биха могли да повлияят на постигането на всяка отделна оперативна цел от списъка на целите. При идентифицирането на рисковете, застрашаващи постигането на поставените цели, е от ключово значение да се обхванат всички аспекти на средата, в която съществува организацията, на самата организация и на дейността ѝ. За целта се използват предварително установени класификации на рисковете, като при идентификацията риск-собствениците преглеждат и работят по всички категории, с цел идентифициране на съществуващите рискове от различни категории.

Идентифицираните рискове се представят в текстова форма и включват: описание на риска, вероятни причини за проявление на риска (спусъци), определение, съдържание, последствия при евентуално проявление на риска, източници и области за проявление и др.

Неидентифицирани рискове в отбранителните програми не могат да се управляват. Органите (екипите) за управление на риска са длъжни да идентифицират всички възможни рискове, които могат да окажат влияние или да доведат до неизпълнение на определени цели, задачи и приоритети в отбранителните програми.

Рисковете за отбранителните програми може да се класифицират на вътрешни и външни рискове за отбранителните програми.

- Външни рискове – рискове, свързани с външни обстоятелства, като например: политически събития, законодателни промени, промени в икономиката, природни явления, външни организации – партньори, контрагенти, медии и др.;

- Вътрешни рискове – рискове, свързани с правно-организационната форма, спецификата на дейността и процеса на работа на програмите, като например: рискове, свързани със системата за обмен на данни, проблеми, свързани с човешките ресурси, промени в работните задачи, неефикасно управление и др.

Възможни са и други класификации на рисковете, които да улеснят идентифицирането на конкретните рискове. Като примерни рискови области могат да се посочат следните:

- Стратегически рискове – те могат да повлияят върху постигането на стратегическите цели на организацията;

- Оперативни рискове – тези, с които организацията се сблъсква ежедневно и заплашват изпълнението на оперативни процеси и дейности;

- Политически рискове – възникват от промяна в правителството и провеждане на нови политики;

- Икономически рискове – породени от особеностите и/или промяната на икономическата система (инфлация, конкуренция и др.). Това може да се отрази на нивото на търсене на някои услуги, да повлияе на разходите или да доведе до намаляване размера на наличното финансиране (бюджета на организацията);

- Репутационни рискове – причинени от слаби връзки с обществеността, от неуспех при предоставянето на услуги или при задоволяване на обществени потребности, при работа с граждани, с колеги, медиен скандал, в който са замесени служители на организацията;

- Технологични рискове – причинени от използването на стари технологии, от пробив в сигурността или от използването на нови информационни системи, които не са достатъчно изпробвани или служителите не са обучени на необходимото ниво;

- Рискове за сигурността – причинени от кражби или злоупотреби с материални активи, парични средства или други финансови активи или нерегламентиран достъп до информация, поради неадекватна защита на информационната система;
- Правни/регулаторни рискове – възникващи от промяна в националното или на ЕС законодателство, както и промяна във вътрешноевропейската нормативна база;
- Финансови рискове – причинени от недостатъчно финансиране или от незаконосъобразно, неефективно, неефикасно или неикономично разходване на средствата. Финансовите рискове могат да се проявят и по отношение на приходната част на бюджета – незаконосъобразно/неефикасно определяне/събираемост на приходите за организацията;
- Екологични и здравни рискове – възникващи в резултат на въвеждането на нови екологични стандарти или поради настъпили екологични катастрофи, промени в климата, пандемии и др.;
- Управленски рискове – причинени от грешни управленски решения или от незадоволителни мерки за вътрешен контрол, честа промяна в ръководния състав на организацията;
- Договорни или партньорски рискове – възникващи от неуспех на партньор или доставчик на обществена услуга, както и неизпълнение на договори.

При идентифицирането на рисковете следва да се има предвид факта, че голяма част от целите на организацията МО се изпълняват от нейните подчинени структури (отбранителни програми и разпоредители с бюджет от втора и по-ниска степен). В тези случаи настъпването на риск на нивото на подчинени структури може да засегне изпълнението на целите на организацията – първостепенен/второстепенен разпоредител с бюджет. В тази връзка, организацията - МО трябва да идентифицира потенциалните рискове на ниво подчинени структури, да ги обсъди с ръководителите на отбранителни програми (структури) и да потърси подходящи мерки за контрол на риска.

Това не означава, че организацията – първостепенен разпоредител с бюджет, следва да прегледа в цялост процедурите по управление на риска в подчинените си структури, нито да включи в собствения си риск-регистър всички рискове, идентифицирани от тях.

Последователността при идентифициране на рисковете е следната:

- Определяне на експерти за идентифициране на рисковете в отбранителните програми.

Основна роля при идентифициране на рисковете имат програмните екипи, които планират ресурсите за отбрана в програмните меморандуми на отбранителните програми. Допълнително е необходимо да се определят експерти, които ще вземат участие при идентифициране на рисковете, като те трябва да са от екипите за управление на риска в съответната отбранителна програма.

Препоръчително е експертите да имат познания (да работят) в структури, отговорни за поддържане/изграждане на отбранителни способности на ВС по области от способности и по елементите на отбранителната способност съгласно План 2026 и приети в НАТО.

Отбранителните програми, които не поддържат/изграждат отбранителни способности е необходимо да привличат експерти за идентифициране на рисковете свързани с целите, дейностите и задачите на програмата.

Практиката е доказала, че колкото повече области (дейности, задачи) се изпълняват в отбранителната програма, толкова по-голям е броят на идентифицираните рискове. Няма ограничение за броя на идентифицираните рискове.

- Идентифициране на рисковете в отбранителната програма.

Експертите участващи в процеса на идентифициране на рисковете, трябва точно да определят рисковете в съответната област, дейност (задача) на отбранителната програма, които биха застрашили изпълнението на целите и приоритетите или планираните резултати на програмата.

При идентифициране на риска е необходимо да се определи следната информация (изходни данни): наименование и описание на риска, вероятни причини за проявление на риска (спусъци), очаквани последствия при проявление на риска, източници, области, елементи и дейности в които може да се прояви и върху кои цели и приоритети, свързани с изпълнението на отбранителната програма ще повлияе. Необходимо е идентифицираните рискове да бъдат кратко и ясно формулирани, без излишни обяснения и описания.

Входните и изходните данни при идентифициране на рисковете в отбранителните програми са показани на Схема 2:



Схема 2 - „Входни и изходни данни при идентифициране на рисковете”

- Разработване и попълване на индивидуална анкетна карта.

Ръководителят на екипа за управление на риска в отбранителната програма определя експерти, които да отговарят за изготвяне на анкетните карти и обобщаване на резултатите.

За попълване на анкетните карти е необходимо да бъдат привлечени определен брой експерти от различни области. Колкото броят на експертите, попълващи анкетните карти е по-голям, толкова резултатите, получени от анкетните карти ще бъдат по-реалистични.

За попълване на анкетните карти е необходимо:

- Да бъдат предварително подготвени анкетни карти, включващи всички идентифицирани рискове за отбранителната програма;

- При идентифициране на голям брой рискове за отбранителната програма се допуска тези рискове да бъдат групирани по определените области и категории. В този случай анкетните карти трябва да включват идентифицираните рискове, подготвени по области;

- Участниците в анкетата е необходимо да определят рангове на рисковете, като рискът с най-голямо значение да получи най-висок ранг;

- Всеки риск е необходимо да получи ранг;

- Допуска се експертите да дават един и същи ранг на повече от един риск, т.е. в анкетните карти може да има два и повече риска със съвпадащи рангове.

- Обобщаване на резултатите от индивидуалните анкетни карти.

След попълване на индивидуалните анкетни карти от експертите, резултатите се обобщават от екипа за управление на риска. Подготвя се обобщена анкетна карта, която включва резултатите от индивидуалните анкетни карти на експертите. В случаи, когато идентифицираните рискове са голям брой се подготвят обобщени анкетни карти по приетите области и категории. При попълване на обобщените анкетни карти е необходимо да се нанесат коректно резултатите на всеки експерт от индивидуалната анкетна карта.

Отчитайки основната слабост на качествената оценка – субективизмът при присъждане на съответните словесни или числови показатели за оценка на вероятността и ефекта, е препоръчително да се използват различни техники за снижаване на нивото на субективизъм или за унифициране на разбирането на оценяващите. Представените в Приложение 1 на стратегията техники, съдържат различни похвати за смекчаване на крайните субективни оценки, въз основа на балансираното участие на достатъчен брой служители. Подобна техника е използването на подходящи критерии, които да показват в какви ситуации каква тежест на вероятност или ефект следва да се присъди.

За да могат да се използват на практика подобни критерии, те трябва предварително да се дефинират за използването от организацията категории рискове. Самият процес по дефинирането им подпомага повишаването на разбирането на оценяващите и намалява субективизма. Друга примерна техника за намаляване на субективизма е използването на историческа информация за вероятността и ефекта на сходни събития.

Примерни източници на такава информация са:

- Минал опит (в личен и институционален аспект);
- Бенчмаркинг (сравнение с информация на сходни организации);
- Използване на индикатори (единици и мерки):
 - за вероятността – тя може да бъде определена в конкретна времева рамка - всеки ден, месечно и т.н.;
 - относно въздействието – финансови прагове, процент от финансови или физически показатели, ниво на разпространение на въздействието (на ниво проект, на ниво мярка или приоритет).
- Използване на стандарти и насоки (например насоки на ЕС за финансови корекции).

За идентифициране на рисковете се използват следните по-характерни методи:

- мозъчна атака - експертите идентифицират рискове във всяка област и категория, съгласно притежаваното ниво на компетенции и опит във своята област (дейност, в която работи);
- контролни карти - експертите идентифицират рисковете от предварително подготвени карти с източници на риска за специфични рискови области;
- интервюиране на експерти - провеждане на разговори с експерти, участвали в процеса на планиране, програмиране и бюджетиране за минали периоди;
- метод „Ринги“ - експертите от програмните екипи се разпределят по области, като техните резултати се сравняват с резултатите получени в екипа за управление на риска и се изготвя единна позиция. Този метод се приема като класически при идентифициране на рисковете;
- метод „Черна кутия“ - за идентифициране на рисковете, предварително се изготвя въпросник на който експертите отговарят. За идентифицираните рискове се провежда обща дискусия по зададените въпроси от въпросника. Методът е по-малко приложим;
- метод „Синектика“ - рисковете се идентифицират от една страна от ръководителя на екипа за управление на риска и от друга от експертите, след което се обсъждат и се формира общо мнение;
- „SWOT“ анализът - анализа включва силните и слабите страни, благоприятните възможности и заплахите при изпълнение на отбранителните програми;

- „Делфи“ метод – представлява инструмент за формиране на резултати от група. Решението се взема на основата на голямо количество събрана информация. Процедурата се развива на етапи (кръгове).

В Приложение 1 на стратегията са описани техники за идентифициране, оценка на рисковете и за дефиниране на техники за реакция.

5.3. Трети етап „Анализ и оценка на рисковете”

Оценка на рисковете

Поради необходимостта да се отдели сериозно внимание на основните рискове, с които се сблъсква организацията МО, по принцип не е възможно да бъдат идентифицирани и управлявани повече от 20-30 риска в МО. Ето защо е необходимо вниманието да се концентрира към идентифициране на най-важните (съществените) рискове. Това са тези рискове, за които съществува най-голяма вероятност да настъпят и са с най-голямо потенциално влияние върху стратегическите и оперативни цели на МО. Основната задача на този етап е рисковете да бъдат анализирани и оценени, за да могат да бъдат определени съществените (значимите) рискове и да се вземе решение как да се контролират и какво въздействие трябва да бъде оказано върху тях – каква трябва да бъде реакцията на риска. Рисковете се оценяват по два показателя – вероятност и влияние (дефиниция за същите е налична в раздел 3 от настоящата стратегия).

Осъществяването на дейностите на организациите от публичния сектор е динамичен процес поради непрекъснатите промени в обществените потребности и в средата, в която се осъществява дейността. Следователно природата на риска се променя непрекъснато. От тук следва, че вероятността от настъпване на риска и възможното влияние са също динамични и трябва да се наблюдават непрекъснато.

Методи и техники за оценка

При оценката на риска могат да бъдат използвани количествени и/или качествени методи. Количествените методи обикновено носят по-голяма точност, но могат да се използват само по отношение на определени рискове, подлежащи на количествено измерване (например финансови рискове) и предполагат използването на по-сложни техники. Такива техники са статистическите техники на интервални оценки или на използване на съотношения. Освен нуждата от специфични познания, те предполагат наличието на достатъчни като количество и точност статистически данни. Качествените методи могат да се приложат, когато рисковете не подлежат на количествено измерване (например репутационни рискове) или когато липсват достатъчно достоверни статистически данни. Качествените методи са субективни, но се прилагат по-лесно. При използването на качествени методи, вероятността и ефектът (влиянието) на рисковете се оценяват чрез качествени показатели, които могат да бъдат словесни (висок, среден, нисък) или числови (като скалата може да е от 1 до 3 или от 10 до 40).

Подход за оценка на риска

Както и при идентифицирането на рисковете, оценката на рисковете се извършва от риск-собствениците, като съществуват различни подходи – включване във формална (постоянно действаща или временна) работна група, работеща с ясни правила и процедури, работни заседания и др. В МО оценката на риска се извършва от Комитет за управление на риска в МО, създаден със заповед на министъра на отбраната.

В оценката на рисковете трябва да бъдат ангажирани всички ръководители на отбранителни програми. Първоначално се оценяват идентифицираните присъщи рискове и след това се пристъпва към оценка на остатъчните рискове.

За да се оценят остатъчните рискове, риск-собствениците трябва да идентифицират контролните механизми (дейности за противодействие), които имат за цел да намалят вероятността и/или ефекта на всеки риск. След идентифицирането на контролите, риск-

собствениците оценяват ефективността на всяка съществуваща контрола поотделно, както по отношение на нейното влияние върху вероятността, така и по отношение на влиянието върху ефекта на риска.

Анализът на риска в отбранителните програми представлява системен процес, включващ изучаването на идентифицираните рискове, определяне на значимите рискове и взаимовръзките им с целите, приоритетите и задачите на програмата, изразяване на степента на влияние върху изпълнението на програмата, вероятността за проявление и размера на очакваните последствия за отбранителната програма.

В анализа и оценката на риска се определят:

- оценки за вероятност за проявление на рисковете;
- оценки за влияние (степен на влияние) на рисковете;
- общо ниво на риска;
- най-общите дейности за противодействие на значимите рискове;
- влияние на значимите рискове върху реализирането на целите, приоритетите и задачите на отбранителните програми (структурите).

Основната задача през този етап е идентифицираните рискове да бъдат анализирани, оценени и да бъдат определени значимите рискове, както и да се оцени как да се контролират рисковете и какво въздействие трябва да бъде оказано върху тях. Рисковете не могат да бъдат премахнати напълно, но могат да бъдат значително намалени чрез предприемане на подходящи действия. Необходимо е рисковете да се оценят чрез използване на два показателя – степен на влияние и вероятност за проявление. Степента на влияние показва, какви са очакваните последствия (въздействието) от настъпване на събитието за постигането на целите на отбранителните програми (структурите), а вероятността за проявление характеризира предполагаемата честота за настъпване на неблагоприятното събитие.

Оценка на риска е процес, състоящ се от определяне на вероятността от сбъдването на идентифицирания риск и определяне на ефекта (степен на влияние) върху целите на организацията при неговото настъпване.

Влияние (степен на влияние) - след възникване на риска, какво ще бъде въздействието му върху постигането на целите, приоритетите и задачите на отбранителните програми (структурите).

Нивата за влияние на риска са съгласно скалата, представена в таблицата:

Оценка	Описание
Нисък	Несъществено
Среден	Умерено
Висок	Изключително голямо

Оценките за влияние на рисковете са следните:

Влияние	
Числова оценка	Степен
10-20	Ниско
21-30	Средно
31-40 и повече	Високо

Вероятност за проявление на риска - показва до каква степен рискът може да се прояви през периода на изпълнение на отбранителната програма. Може да се използва опитът от проявили се рискове. Всеки риск трябва да бъде оценен от гледна точка на вероятността рискът да се сбъдне / прояви.

Нивата за вероятност за проявление са съгласно скалата в таблицата:

Оценка	Описание
Ниска	Не е вероятно
Средна	Възможно (Вероятно)
Висока	Почти сигурно

Оценките за вероятност за проявление на рисковете са следните:

Вероятност за проявление	
Числова оценка	Степен
10-20	Ниска
21-30	Средна
31-40 и повече	Висока

Общо ниво на риска - оценява се по два начина:

- общо ниво на риска, получено от средноаритметичните теглови коефициенти на степента на влияние и вероятността за проявление:

Общо ниво на риска	
Числова оценка	Степен
10-20	Нисък риск
21-30	Среден риск
31-40 и повече	Висок риск

- общо ниво на риска, получено от комбинация на степента на влияние и вероятността за проявление:

Общо ниво на риска	
Оценка	Описание
Нисък риск	ниско влияние и средна вероятност
	средно влияние и ниска вероятност
	ниско влияние и ниска вероятност
Среден риск	ниско влияние и висока вероятност
	средно влияние и средна вероятност
	високо влияние и ниска вероятност
Висок риск	високо влияние и висока вероятност
	средно влияние и висока вероятност
	високо влияние и средна вероятност

Входните и изходните данни при анализ и оценка на рисковете в отбранителните програми са представени на Схема 3:

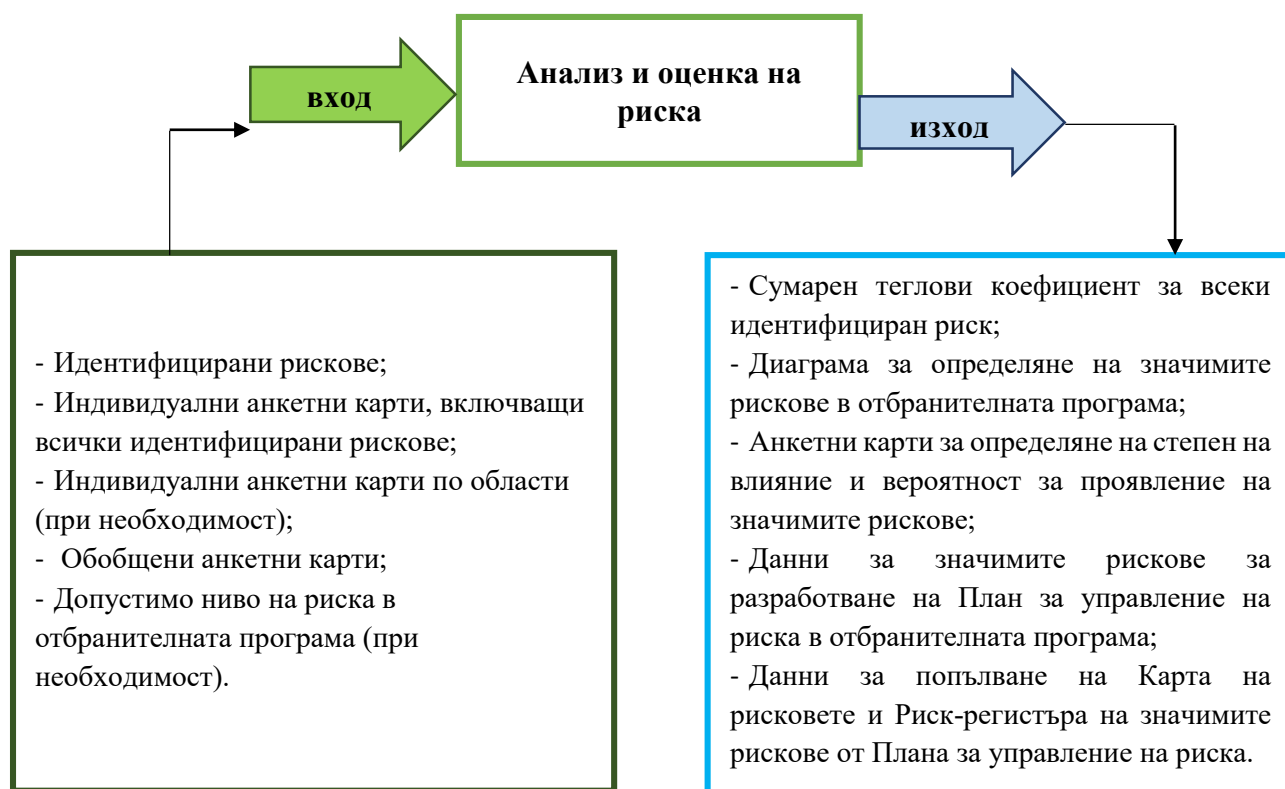


Схема 3 - „Входни и изходни данни при анализ и оценка на риска”

Последователност на дейностите на екипите за управление на риска при анализа и оценката на рисковете е следната:

- Определяне на експерти за анализ и оценка на рисковете в отбранителните програми.

Препоръчително е експертите да имат познания (да работят) в структури, отговорни за поддържане/изграждане на отбранителни способности по области от способности или по елементите на отбранителната способност съгласно План 2026 и приети в НАТО.

Отбранителните програми (структури), които не поддържат/изграждат отбранителни способности е необходимо да привличат експерти за анализ и оценка на рисковете, свързани с дейностите и задачите на програмата (структурата).

- Определяне на сумарен теглови коефициент на идентифицираните рискове.

При определяне на сумарния теглови коефициент на идентифицираните рискове се изравняват тегловите коефициенти на ранговете, определени от всеки един от експертите. Изравняването се налага поради това, че след попълване на анкетните карти от експертите за някои от рисковете има съвпадения на ранговете. Изравняването на ранговете се извършва от екипа за управление на риска на съответната отбранителна програма.

Определянето на крайния теглови коефициент се извършва по този ред за резултатите на всеки експерт. Резултатите се нанасят в обобщената таблица.

Тегловите коефициенти не се изравняват ако в съответната анкетна карта няма повторение на ранговете. Тези теглови коефициенти се нанасят директно в обобщената таблица.

За контрол (проверка) на получените крайни теглови коефициенти може да се използва формулата:

$$\sum_{i=1}^n x_{ij} = \frac{1}{2} n(n+1)$$

където: **n** - брой на идентифицираните рискове

X_{ij} - сума на тегловите коефициенти в j-та анкетна карта

- Попълване на обобщена таблица с крайните теглови коефициенти на всички експерти.

Обобщената таблица с крайните теглови коефициенти се попълва от екипа за управление на риска на отбранителната програма. Сумарният теглови коефициент се получава като сума от крайните теглови коефициенти на всички експерти.

- Разработване на диаграма с резултатите от анализа и оценката на идентифицираните рискове и определяне на значимите рискове на отбранителната програма.

Екипът за управление на риска в отбранителната програма разработва диаграма, на която се нанасят сумарните теглови коефициенти. На диаграмата по хоризонталата се нанасят броя на идентифицираните рискове, а по вертикалата се нанасят получените сумарни теглови коефициенти за всеки идентифициран риск.

Определянето на значимите рискове в отбранителната програма се извършва чрез определяне и начертаване на „средна линия“, която е половината (50%) от стойността на най-високия сумарен теглови коефициент (Схема 4).

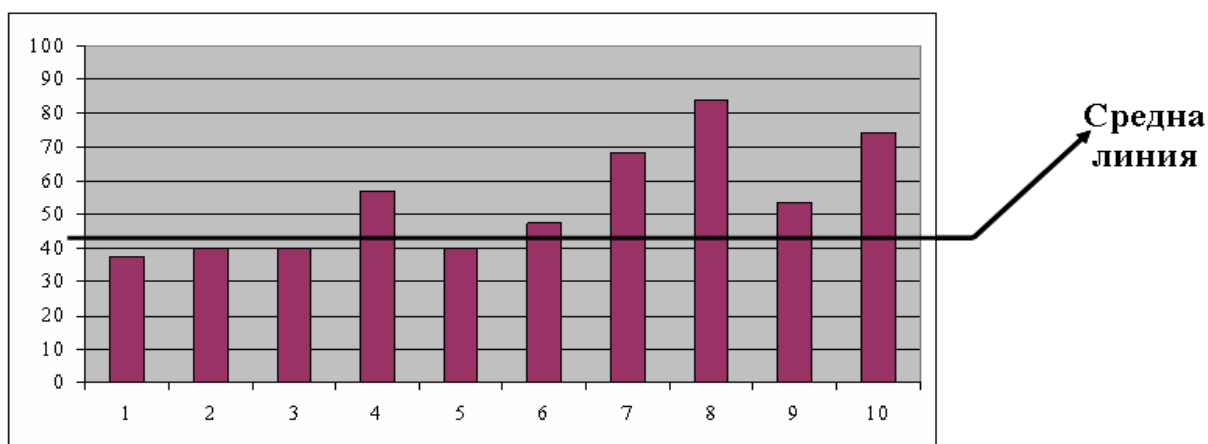


Схема 4 „Диаграма за определяне на значимите рискове”

Всички рискове, които са със сумарни теглови коефициенти над средната линия се определят като значими рискове за отбранителната програма (структурата). Тези значими рискове се включват в Плана за управление на риска на отбранителната програма, в Риск-регистър и в Карта на рисковете за отбранителната програма.

Останалите рискове, които са под средната линия са незначими за отбранителната програма (структурата), но подлежат на наблюдение, защото на определен етап могат да повишат степента на влияние и вероятността за проявление. Тези рискове също се описват в Плана за управление на риска на отбранителната програма.

- Разработване и попълване на анкетна карта за оценяване на степента на влияние и вероятността за проявление на определените за отбранителната програма значими рискове.

Екипът за управление на риска разработва анкетна карта, в която се изписват само определените значими рискове.

Анкетните карти се попълват от определен брой експерти, като се използват посочените по-горе оценки и степени. Всеки експерт е длъжен да постави оценка и да определи степента на влияние и вероятността на проявление на всеки от определените значими рискове на отбранителната програма.

- Попълване на обобщена таблица с оценките за влияние и вероятност за проявление на значимите рискове и определяне на общото ниво на всеки риск.

Екипът за управление на риска попълва обобщената таблица с оценките за влияние и вероятност за проявление на значимите рискове, дадени от всеки от експертите и се определя средноаритметичната оценка на значимите рискове.

При определен голям брой значими рискове се допуска рисковете да бъдат разпределени по определени области и категории.

При определяне на значимите рискове за съответната отбранителна програма се анализират значимите рискове, определени в по-ниското програмно ниво и идентифицираните рискове от съответната отбранителна програма.

- Попълване на матрица на риска със степента на влияние и вероятността за проявление.

В схемата „матрица на риска” по хоризонталата се нанасят степента на влияние на риска, а по вертикалата се нанася вероятността за проявление на рисковете (Схема 5).

ВЕРОЯТНОСТ	висока	жълто	червено	червено
	средна	зелено	жълто	червено
	ниска	зелено	зелено	жълто
		ниско	средно	високо
		ВЛИЯНИЕ		

Схема 5 - „Матрица на риска”

Значението на зоните в матрицата на риска са, както следва:

- Червена зона - рискът е със средни и високи степен на влияние и вероятност за проявление. При транспонирането им върху скалата - рисковете, оценени като високи/високи и високи/средни при оценяването на вероятността и влиянието, ще попаднат в червената област. Те би трябвало да се смятат за съществени и да се управляват активно чрез предприемане на действия за намалението им. Тези рискове не могат да се елиминират напълно. Трябва да бъдат предприети конкретни и навременни дейности за противодействие, които да намалят степента на влияние и вероятността за проявление на риска, с цел същият да премине в жълтата зона.

- Жълта зона - рискът е с ниски, средни и високи степени на влияние и вероятност за проявление. Рисковете, оценени като средни/средни или ниски/високи, или високи/ниски попадат в жълтата област на скалата и са все още значителни рискове. Тези рискове се наблюдават отблизо, като се прилагат действия за контролирането им или за предотвратяване на преминаването им в по-висока рискова категория. Необходимо е да бъдат предприети дейности за противодействие, които да попречат на риска да премине в червената зона. Рискът трябва да остане в жълтата зона или да премине в зелената зона.

- Зелена зона - рискът е с ниски и средни степен на влияние и вероятност за проявление. Рисковете, оценени като ниски/ниски или ниски/средни попадат в зелената област. Тези рискове могат да се смятат като ниско приоритетни и следователно рискове, които се „приемат“. При предприемане на допълнителни действия да се има предвид, че разходите за осъществяване на контрол могат да надвишат ползата от намалението на риска. Тези рискове трябва да бъдат наблюдавани, защото в определен момент могат да повишат степента на влияние и вероятността за проявление и да преминат в жълтата зона.

Методите и подходите за анализ и оценка на риска са, както следва:

- подробен и задълбочен анализ - позволява определяне на последствията за цялостното изпълнение на целите на отбранителната програма (структурата). Този метод се прилага за

всички рискове, с цел да се определят онези от тях, които притежават висока степен на влияние върху постигане на целите, приоритетите и планираните резултати на отбранителната програма (структурата);

- вероятностен анализ - определя се разпределението на вероятностите за проявление на отделните рискове и се отчита комбинираното влияние на всички рискове върху постигане на целите и приоритетите на отбранителната програма (структурата);

- диаграми на влиянието - използват се като потребителски интерфейс в компютърни средства за анализ на риска. Заклучава се в разработване на комплексни математически модели, с които да се сравняват и анализират параметрите на ресурсите за отбрана и времето за изпълнение на отбранителните програми;

- дърво на решенията - представлява графичен метод за анализ на рискове, представящ възможните начини за действие и очакваните резултати. Прилага се най-често за анализ на риска по отношение на разходите в отбранителната програма (структурата);

- очаквана парична стойност - измерва се чрез вероятността за проявление на рисковете и размерите на загубите на ресурси за отбрана (финансови средства) при евентуално проявление на риска. Може да се използва като входна информация при други методи за анализ;

- статистически метод - статистическият метод е най-разпространеният метод и се основава на точни и конкретни изчисления. Методът се прилага в три стъпки: анализ на продължителността; анализ на стойността; анализ на ефективността на отбранителната програма (структурата);

- симулации - могат да се използват симулативни модели за определяне на нивата на риска при изпълнение на отбранителните програми. Популярна форма за симулация е разчетната симулация, базираща се на метода на статистическото моделиране;

- експертни оценки - представляващи интуитивно-научен метод, с помощта на който рисковете могат да бъдат оценени по отношение на тяхното влияние и вероятност за проявление. Този метод е най-приложим при управление на ресурсите за отбрана и изпълнение на отбранителните програми;

- метод на сценария - прави се подробен анализ на всички дейности, възможните вероятности за възникване на рискове, разиграват се всички варианти и се достига до най-вероятния вариант, който се предлага на ръководителя на екипа за управление на риска.

5.4. Четвърти етап „Противодействие на значимите рискове”

Етапът „Противодействие на значимите рискове” представлява процес на определяне и прилагане на дейности за противодействие на значимите рискове. Прилаганите дейности трябва да доведат до намаляване на степента на влияние и вероятността за проявление на значимите рискове до нива, които не оказват съществено влияние върху изпълнението на целите, приоритетите и планираните резултати на отбранителната програма.

Реакции на ръководителите на отбранителни програми срещу значимите рискове

След като бъдат идентифицирани и оценени рисковете чрез методите и техниките, описани по-горе, организацията трябва да прецени какви мерки и действия за реакция или отговор на идентифицираните и оценени рискове трябва да бъдат предприети. Процесът се организира от Риск-ръководителя, но отново всеки ръководител на отбранителна програма е отговорен да предложи мерки, които да бъдат реакция на рисковете, отнасящи се до ръководената от него програма (звено) или дейност. Възможни са следните варианти за реакция: ограничаване, прехвърляне, приемане и прекратяване на риска. При избора на подходящи действия (реакция) се взема предвид изискването разходите за тях да не надхвърлят очакваните ползи. Този избор зависи и от преценката на ръководителя на организацията за нивото на остатъчните рискове, които организацията може да приеме, без да се предприемат допълнителни действия и без да се

застраши постигането на целите (риск апетита). Възможните реакции, които могат да бъдат предприети са:

- Ограничаване на риска - ограничаването на риска представлява намаляване или третиране на риска чрез прилагане на контроли (например, чрез законодателство, партньорство и сътрудничество, повишаване на ефикасността на контрола чрез засилване на съществуващите контроли или въвеждането на нови и т.н.). Решението за ограничаване на значимите рискове изисква: адекватен избор на действията в съответствие с оценката на риска; вътрешен контрол; внимателно анализиране на разходите и ползите от контрола; дефиниране на специфични дейности за ограничаване или третиране на риска и ясно определяне на роли и отговорности.

- Прехвърляне (трансфериране) или споделяне на риска - ръководството на организацията - МО може да прецени, че рискът е твърде висок и трябва да го „прехвърли” към друга организация. Класическият начин за прехвърляне на риска е застраховането. Ако дейността, свързана с определени цели на организацията е предмет на застраховане, като например опазване на имуществото на организацията, опазване живота и здравето на служители, извършващи високорискови дейности – е препоръчително да се предприемат такива мерки. Друг способ за прехвърляне на риска е сключването на споразумение с друга организация, по силата на което се прехвърля дейността заедно със съответните рискове, по общо съгласие на страните.

Прехвърлянето (трансферирането) или споделянето на значимите рискове означава да се влезе в партньорство с трета страна, така че рискът да бъде управляван съвместно. Подобна схема позволява достъп до допълнителен ресурс (например контролни дейности или опит и квалификация), като в същото време се ограничава възможността от загуба на контрол над дейностите за противодействие. Ръководителите на отбранителни програми (структури) продължават да бъдат отговорни за управлението на прехвърления (споделения) риск.

- Толериране (приемане) на риска - толерирането на даден риск означава, че отбранителната програма (структурата) приема риска без да предприеме конкретни мерки за управлението му. Причините да се толерира даден риск без по-нататъшни действия за управлението му могат да бъдат: действията по ограничаване на риска са свързани със съществени контролни дейности; приемането на риска е свързано със самото развитие на отбранителната програма (структурата); управлението на риска е извън контрола на ръководството, което означава преустановяване на дейности, които са от ключова важност за отбранителната програма (структурата). Такава реакция на приемане на риска е възможна само ако определени рискове имат ограничено (незначително) влияние върху постигане на целите или ако разходите за предприемане на действия превишават потенциалните ползи. Такива рискове, обаче, трябва да бъдат постоянно наблюдавани. Възможно е различни външни или вътрешни фактори да окажат въздействие върху вероятността и влиянието и да изместят риска в друга по-висока категория.

- Прекратяване (избягване) на риска - прекратяването (избягването) на даден риск означава да се прекратят дейностите за противодействие. Разглеждат се и възможности за избягване на риска в определена степен, т.е. дадени цели или дейности да бъдат частично променени или преустановени, както и да се установят възможностите поставените цели да бъдат постигнати по различен от предвидения начин. Някои рискове могат да се намалят или ограничат до приемливо равнище единствено чрез прекратяване на дейността. Бездействието на организацията също може да е риск, защото при него не могат да се постигнат целите, за които е създадена. В публичния сектор възможностите за прекратяване на риска са твърде ограничени, тъй като стратегическите цели на организациите в повечето случаи се определят в нормативни актове, стратегически планиращи документи на национално ниво и на ниво организация (МО) и правителствени програми.

Дефиниране на реакции по отношение на рисковете

Следва да се отбележи, че към един и същи риск могат да бъдат предприети действия, включващи комбинация от горепосочените реакции на риска, като при последващ преглед на риск-регистъра определената реакция към даден риск може да се наложи да бъде променена. Дейностите и методите, които са необходими за намаляване на съответните рискове могат да се дефинират на работно заседание на ръководителите на отбранителни програми (риск собствениците) или на заседание на Комитета за управление на риска под координацията на председателя на Комитета за управление на риска.

Дефинирането на мерки за реакция (противодействие) включва и преценка доколко съществуващите контролни процедури са подходящи за управление на идентифицираните рискове. При необходимост се дефинират нови мерки за реакция на риска. При оценката на съществуващите контролни механизми и при разработването на нови, трябва да се разбира, че ниво на остатъчен риск винаги ще съществува, не само заради ограничените ресурси, но и заради вътрешно присъщите ограничения от различен характер (човешки фактор, несъвършенство на технологиите и др.) на контролните механизми. В тази връзка не трябва да се изпада в крайности, като разработване и въвеждане на свръхконтроли в опит за пълно ограничаване на риска.

Противодействието срещу влиянието и вероятността за проявление на значимите рискове представлява процес на дефиниране, избор и прилагане на методи и средства за противодействие, с цел редуциране на риска до приемливи нива, които не оказват влияние върху изпълнението на целите, приоритетите и планираните резултати на отбранителните програми (структурите). На етапа „Противодействие на значимите рискове” е необходимо да се определят: значимите рискове, на които ще се противодейства; определяне на дейности за противодействие; срока за противодействието; отговорност за провеждане на дейностите за противодействие; методи и средства за провеждане на противодействието.

Противодействието на значимите рискове в отбранителните програми (структурите) е насочено в следните направления:

- намаляване на вероятността за проявление на значимите рискове;
- намаляване на влиянието - размера на очакваните последствия от проявлението на значимите рискове;
- едновременно намаляване или изключване на вероятността за проявление на значимите рискове и размера на очакваните последствия.

Противодействието на значимите рискове е необходимо да доведе до следните резултати:

- снижаване на риска до определеното приемливо ниво за отбранителна програма (структурата);
- намаляване на степента на влияние и вероятността за проявление на значимите рискове от високо ниво чрез разпределяне на влиянието им между съставните части на отбранителната програма (структурата) или пренасочване към трета страна;
- приемане на риска без предприемане на действия за управлението му.

За противодействие на значимите рискове е необходимо да се извършат следните дейности:

- да се определят отговорности за прилагане на дейностите за противодействие на значимите рискове;
- да се изготви подробно описание на значимите рискове;
- да се опишат взаимовръзките на значимия риск с останалите рискове;
- да се определят начините за намаляване на степента на влияние и вероятността за проявление на рисковете;
- да се изберат методи и подходи за противодействие на значимите рискове;

- да се изготвят критерии за измерване на очакваната ефективност на прилаганите дейности за противодействие на значимите рискове;
- разработване на кризисен план за действие в случай, че избраните и прилагани дейности за противодействие на значимите рискове се окажат недостатъчно ефективни (при необходимост);
- изготвяне на времеви график за противодействие на значимите рискове.

Входните и изходните данни при противодействие на значимите рискове в отбранителните програми са представени на Схема 6:

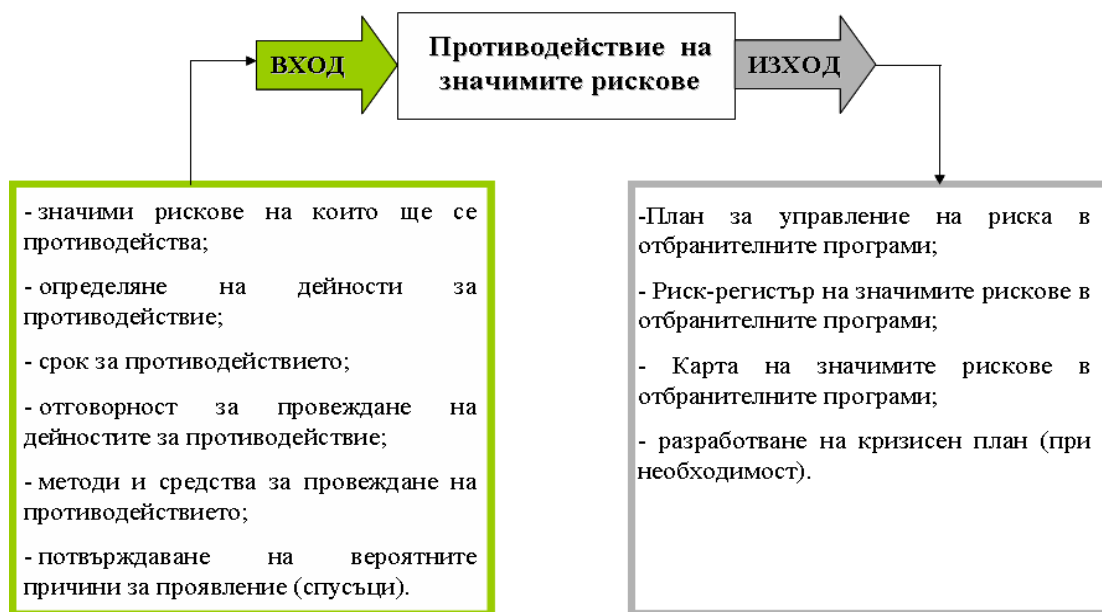


Схема 6 - „Входни и изходни данни за противодействие на значимите рискове”

През етапа „Противодействие на значимите рискове” се разработва План за управление на риска в отбранителната програма за бюджетната година.

Целите на разработване на Плана за управление на риска са следните:

- да се определят значимите рискове и да се дефинират отговорностите на ръководителите на отбранителни програми по наблюдение (мониторинг) на значимите рискове;
- подпомагане на ръководството на МО и ръководителите на основни програми на МО, структурите на пряко подчинение на министъра на отбраната и БА за ограничаване или недопускане на негативното влияние на рисковете при управление на ресурсите за отбрана и цялостното управление на процесите в МО;
- подпомагане на процеса на програмиране на ресурсите за отбрана за поддържане/изграждане на способности на ВС;
- провеждане на периодични прегледи на значимите рискове и предприемане на адекватни дейности за противодействие на рисковете.

Планът за управление на риска на отбранителната програма се разработва след приемане и утвърждаване от министъра на отбраната на Меморандум на програмните решения за шестгодишен период и обхваща първата година от периода на програмиране (бюджетната година). Планът се разработва от екипа за управление на риска и се утвърждава от ръководителя на отбранителната програма.

Планът за управление на риска в отбранителните програми в МО, структурите на пряко подчинение на министъра на отбраната и БА се разработва от дирекция „Планиране,

програмиране и бюджет” и се приема в Комитета за управление на риска в отбранителните програми на МО и от Програмния съвет към министъра на отбраната, след което се утвърждава от министъра на отбраната.

Риск-регистър на значимите рискове в отбранителната програма - риск регистърът съдържа - главна цел и цели на отбранителните програми; планирани мисии и задачи; наименование на значимите рискове, определени за всяка мисия и задача; вероятни причини за проявление на рисковете (спусъци); степен на влияние и вероятност за проявление на рисковете; обобщена степен на рисковете; дейности за противодействие на значимите рискове и отговорници за изпълнение на дейностите.

Карта на рисковете съдържа - област на действие на рисковете; категория; наименование на значимите рискове и описание на рисковете.

Пример за формата и съдържанието на План за управление на риска на отбранителна програма е посочен в „Методическо пособие за разработване на документи по управление на риска в отбранителните програми на МО”.

Методите и подходите, прилагани за противодействие на значимите рискове са следните:

- общи методи и средства - разработва се План за управление на риска в отбранителните програми с Риск-регистър на значимите рискове за отбранителните програми и Карта на значимите рискове;
- кризисно планиране - планиране на методи и средства за противодействие при възникване на нови рискове в отбранителните програми;
- разработване на алтернативни методи и средства - влияние на значимите рискове може да се предотврати или избегне чрез смяна на методите и средствата за противодействие.

5.5. Пети етап „Наблюдение, документиране и докладване на резултатите от управлението на риска в отбранителните програми”

Осигуряването на ефективност на процеса по управление на рисковете изисква текущо наблюдение (мониторинг) на всеки негов етап и периодично докладване на идентифицираните рискове и предприетите действия за тяхното намаляване (реакции). За целите на периодичното докладване на идентифицираните рискове, ръководителят на организацията създава условия, както е описано в частта за идентифициране на рисковете.

Следва да се има предвид, че мониторингът на процеса по управление на риска е част от системата за мониторинг, като един от петте елемента на вътрешния контрол. В този смисъл е формулиран и един от принципите на елемента Мониторинг, въведен с Интегрираната рамка за вътрешен контрол COSO 2013: „Организацията избира, разработва и извършва текущи и/или отделни оценки, за да се установи дали компонентите на вътрешния контрол присъстват и функционират“.

В тази връзка, ръководителят на организацията и Риск-ръководителят трябва да използват всички инструменти, въведени като част от Мониторинга, като елемент на вътрешния контрол, в т.ч. вътрешния одит, за да следят и оценяват ефективността, ефикасността и икономичността на управлението на риска.

За осъществяване на систематично наблюдение Риск-ръководителят и риск-собствениците преглеждат периодично целия риск-регистър. Определени рискове могат да бъдат прегледани по-често, в зависимост от тяхната специфика или особена значимост. Някои съществени рискове могат да изискват и ежедневен преглед. При възникване на внезапни събития риск-регистърът може да се разглежда извънредно без да се чака редовния преглед. Прегледът на рисковете трябва да се документира адекватно. Целта на процеса по мониторинг и докладване е да наблюдава дали рисковият профил (вероятността и влиянието) на идентифицираните рискове се променя, дали се пораждат нови, неидентифицирани преди

рискове и да дава увереност на ръководителя на организацията, че процесът по управление на риска остава ефективен във времето и са предприети необходимите действия за намаляване на риска до приемливо за организацията ниво.

Един от важните инструменти за мониторинг върху изменението на рисковия профил са ключовите риск-индикатори (КРИ). Предвид факта, че мониторингът на управлението на риска е част от елемента Мониторинг, който използва и други видове индикатори, по-детайлна информация за характера и използването на КРИ се съдържа в Указанията за ключови индикатори и процедури за мониторинг в организациите от публичния сектор, издадени от министъра на финансите. За успешното наблюдение и оценяване на процеса по управление на рисковете в организацията Стратегията по управление на риска следва да съдържа процедури, които да описват:

- комуникацията и обмена на информация между всички нива и служители в организацията относно идентифицираните рискове;
- реда и сроковете за извършване на регулярните прегледи на риск – регистъра;
- реда и сроковете за докладване на всички значими рискове, предприетите действия и ефекта от тях, както и за нововъзникнали събития. Например за едни рискове срокът за докладване може да бъде веднъж годишно, а за критични рискове – ежемесечно или дори ежедневно;
- отговорностите по управление на риска сред средното ниво на ръководството на организацията и служителите.

В зависимост от големината и структурата на съответната организация от публичния сектор, ръководителят може да изисква от отбранителните програми (отделните звена) или от подчинените структури (в това число разпоредители с бюджет от втора и по-ниска степен, дъщерни търговски дружества и др.), изготвянето на доклади за управлението на риска.

Етапът „Наблюдение, документиране и докладване” който включва преглед на Плана за управление на риска в отбранителната програма, анализ и оценка на рисковете (идентифицирани, значими и новопоявили се) и изготвяне на периодични доклади.

Основната задача на етапа „Наблюдение, документиране и докладване” е своевременно реагиране при изменения в степента на влияние и вероятността за проявление на рисковете в отбранителната програма, документиране в периодичните доклади и докладване за състоянието на рисковете в екипа за управление на риска.

В хода на изпълнение на отбранителните програми рисковете се изменят под въздействието на външни и вътрешни фактори, включващи променени или нови изисквания, промени в законодателната база, в икономическата среда и т.н. В тази връзка от съществена важност са непрекъснатото наблюдение на риска и редовният преглед на плановете за управление на риска и на риск-регистъра.

Наблюдението на рисковете в отбранителните програми представлява непрекъснат процес, който включва следните дейности:

- наблюдение на степента на влияние и вероятността за проявление на значимите рискове в отбранителните програми;
- наблюдение на рисковия профил на идентифицираните и значимите рискове;
- наблюдение на вероятните причини за проявление на значимите рискове (спусъци);
- непрекъснато прилагане на нови дейности за противодействие на тези рискове, които променят степента на влияние и вероятността за проявление;
- непрекъснат контрол и промяна на отговорностите по управление на рисковете;
- наблюдение на всички идентифицирани рискове за повишаване на степените им;
- наблюдение за новопоявили се рискове при изпълнение на отбранителните програми.

Входните и изходните данни при наблюдение, документиране и докладване на значимите рискове в отбранителните програми са показани на Схема 7:



Схема 7 - „Входни и изходни данни при наблюдение, документиране и докладване на значимите рискове”

Н

аблюдението (мониторинга) на рисковете включва информация за: промените на наименования и описания на рисковете; изменения на степента на влияние и вероятността за проявление на рисковете; изменения на вероятните причини за проявление (спусъци) на рисковете; приложени нови дейности за превенция на рисковете; нововъзникнали рискове и рискове, които са се проявили.

Промените в параметрите на рисковете се включват в периодичните доклади за резултатите от управление на риска. Тези периодични доклади са, както следва:

- разработване на ежесмесчна информация „Изменения на нивата на значимите рискове в отбранителните програми на МО и влиянието им върху изпълнението на целите, приоритетите и задачите” – при възникване на промяна в значимите рискове и приложени дейности за противодействие от ръководителите на отбранителните програми за управление на риска;
- - разработване на периодични „Доклади за резултатите от управлението на риска в отбранителните програми на МО, структурите на пряко подчинение на министъра на отбраната и БА” – за шестмесечието и деветмесечието на текущата година за предходната бюджетна година след изтичане на годината.

Ежесмесчната информация се разработва от екипите за управление на риска в основните програми и се обобщава от дирекция „Планиране, програмиране и бюджет” и се внася за разглеждане в Програмен съвет към министъра на отбраната при необходимост. Екипите за управление на риска е необходимо да включват в ежесмесчната информация измененията, настъпили в управлението на рисковете при изпълнение на отбранителните програми. Направените предложения за промени в Единния финансов план за материално-техническо осигуряване и Единния поименен списък на обектите за строителство и строителни услуги за съответните отбранителни програми трябва да бъдат посочени като дейности, прилагани от ръководителите на отбранителните програми за управление на риска.

Формата и съдържанието на ежемесечната информация са посочени в Методическото пособие за разработване на документи по управление на риска в отбранителните програми.

Периодичните доклади се разработват от екипите за управление на риска в основните програми. Дирекция „Планиране, програмиране и бюджет” обобщава докладите на основните отбранителни програми и изготвя обобщен Доклад за резултатите от управлението на риска в отбранителните програми на МО, структурите на пряко подчинение на министъра на отбраната и БА. Обобщеният доклад за резултатите от управлението на риска се внася за разглеждане в Програмен съвет към министъра на отбраната и се представя на министъра на отбраната. Периодичните доклади за резултатите от управлението на риска се изготвят след издаване на Указания на постоянния секретар на отбраната за шестмесечието и деветмесечието на текущата година и за предходната бюджетна година след изтичане на годината.

В Докладите за резултатите от управление на риска се предоставя следната информация:

- предприетите действия във връзка с процеса по управление на рисковете;
- изпълнението на планираните действия, заложи в регистрите на рисковете, информация за ефективността им и в случай, че те не са били ефективни, анализ на причините за това;
- прилагани нови дейности за противодействие
- настъпила ли е промяна в описаните в регистрите рискове;
- нововъзникнали обстоятелства, които могат да предизвикат промяна в отразените в регистрите рискове;
- нововъзникнали и проявили се рискове;
- компетентността на служителите по отношение управлението на рисковете (информация за преминати обучения, придобиване на сертификати за управление на риска);
- спазени ли са срокове за изготвяне на докладите.

Формата и съдържанието на периодичните доклади за резултатите от управление на риска за шестмесечието и деветмесечието на текущата година и за предходната бюджетна година след изтичане на годината на отбранителните програми са посочени в Методическото пособие за разработване на документи по управление на риска в отбранителните програми на МО.

„Описание на техники за идентифициране, оценка на рисковете и за дефиниране на техники за реакция“

„БРЕЙНСТОРМИНГ“ (МЕТОД НА МОЗЪЧНАТА АТАКА)

Брейнстормингът" представлява традиционен подход за извършване на оценката на риска, който стимулира първичното даване на нови, полезни идеи и използването на груповия творчески потенциал за вземане на оптимални решения и повишаване на творческото мислене. Тази техника може да бъде използвана като помощно средство за:

- дефиниране на задачата, върху която се работи;
- определяне на конкретни проблеми;
- намиране на примерни решения и изследване на тяхната надеждност.

„Брейнстормингът" е подходящ за срещите на работните групи по оценка на риска, тъй като всеки от членовете на тези работни групи има възможност да дава спонтанни идеи, което дава възможност за извличане на максимален брой идеи от различните области на компетентност на съответните експерти.

В случай, че в процеса на работа бъде избрана тази техника, трябва да се вземат под внимание и да бъдат следвани някои основни правила като:

1. Наблягане на количеството: Това правило спомага за увеличаването на разнородността на идеите чрез максимата „количеството повишава качеството“. Предполага се, че колкото по-голям е броят на генерираните идеи, толкова по-голям е шансът за намиране на радикално и ефективно решение.

2. Ограничаване на критиката: Идеите, които изникват не бива да бъдат критикувани, като по този начин се стимулира нестандартното, новаторско мислене на участниците. Те трябва да се фокусират върху разширяването и добавянето на идеи, а едва на по-късен етап – в аналитичната фаза, идеите следва да бъдат анализирани.

3. Посрещане на нестандартни идеи: За да се постигне изчерпателен списък от идеи, нестандартните идеи следва да бъдат насърчавани. Те могат да бъдат генерирани посредством откриването на нови перспективи или отхвърлянето на предположения, като по този начин могат да бъдат открити правилните решения.

4. Комбиниране и оптимизиране на идеи: Няколко добри идеи могат да бъдат обединени в една по-добра чрез мотото „1 + 1 = 3“. Тази практика допринася за откриването на правилните решения чрез помощта на асоциация.

ТЕХНИКА НА ПРОВЕЖДАНЕ НА „БРЕЙНСТОРМИНГ“

1. Формулиране на проблема

За успешното провеждане на „брейнсторминг“ сесия е от особено значение предварителното ясно дефиниране на проблема. Проблемът трябва да бъде ясен, не твърде обширен, но не и твърде конкретен въпрос.

2. Избор на участници

Организаторът съставя „брейнсторминг“ група, състояща се от участници и ръководител, събиращ идеите. При съставянето на групите следва да се има предвид, че по-малки групи, състоящи се от максимум 10 участника, обикновено са по-продуктивни. Съставът на групата за провеждане на „брейнсторминг“ сесия може да бъде следния:

- Лица, които са основни участници в проекта;
- Външни за проекта лица;
- Ръководител, който записва предложенията.

3. Създаване на пояснителна бележка

Встъпителната бележка е покана и информационна брошура за участниците, съдържаща името на заданието, темата, часа, датата и мястото. Листовката се изпраща предварително с цел участниците да имат време да помислят над проблема.

4. Стъпки на провеждане

Стандартните стъпки в „брейнсторминг“ сесията са:

- Встъпителна част, в която участниците се адаптират към отсъствието на критика, като се дискутира неангажиращо общ проблем;
- Ръководителят представя основния проблем и дава допълнителни разяснения, ако това е необходимо;
- Ръководителят призовава участниците да представят своите идеи;
- В случай на липса на идеи от страна на участниците, ръководителят предлага насочващи идеи, които да стимулират творческото мислене в групата;
- Всички участници представят своите идеи, които биват записани;
- За да се осигури яснота, участниците могат да разясняват своите идеи;
- Когато сесията приключи, водещият организира идеите тематично с оглед на целта на „брейнсторминга“ и насърчава дискусията;
- Идеите се категоризират;
- Целият списък се преглежда с цел изясняване на изложените идеи;
- Отстраняват се неприложимите/повтарящи се предложения;
- Ръководителят благодари на всички участници.

Основни въпроси, които могат да бъдат засегнати по време на „брейнсторминга“ - т.нар. техника на „Трите перспективи“. Тази техника се основава на разбирането, че погледът върху даден проблем от различни гледни точки е от важно значение при търсенето на неговото решение. За да бъде приложена тази стратегия е необходимо да се отговори на **три основни въпроса**, в следствие на което да се потърсят **техните взаимовръзките или несъответствия**. Следва да се постигне разбиране по отношение на:

А. Описание - търси се отговор на въпросите: Каква е темата?; Какви са нейните компоненти?; Какви са нейните отличителни характеристики?; Какви са особеностите ѝ?;

Б. Проследяване - а именно: Каква е предисторията?; Какви са промените, които са настъпили в процеса на развитие?; Кои са факторите, които са оказали влияние и довели до изменения?;

В. Скициране - тук следва да бъде разяснено: С какво е свързан проблемът?; От какво е повлиян?; Кой са засегнатите страни?; Какви решения са взимани в сходни ситуации?; По какъв начин техните решения могат да бъдат съпоставени?

ТЕХНИКА НА „НОМИНАЛНАТА ГРУПА“

Техниката на „Номиналната група“ е структуриран метод за работа към постигане на консенсус. Силата ѝ е в това, че дава на всеки в екипа равен глас при споделяне на идеите.

Основни принципи

Когато се използва тази процедура, участниците се събират в групи, но не разговарят помежду си. Групата е номинална, тъй като членовете са в групова обстановка, но не им се позволява да си взаимодействат. Всеки член на групата бива подканен да формулира своите виждания за проблема, който се разглежда (в случая идентифициране или оценка на рисковете). Членовете на работната група излагат своите предложения в предварително подготвени форми/формуляри (за целта могат да се използват приложените примерен „Формуляр за идентифициране на риска“ и примерен „Формуляр за индивидуална оценка на рисковете“). След това идеите на всеки се разпространяват сред останалите в структуриран формат и предложенията се разискват, за да бъдат доразяснени.

Методът на номиналната група има следните преимущества:

- независимата работа на всеки от членовете на Работната група;
- възможността за участие на всеки от членовете на Работната група;
- отнетата възможност на когото и да било да доминира в дискусиата;
- контрол върху изразходваното време;
- наличие на стимул да се допринася максимално за работата на Работната група, когато и другите правят същото.

Ключови техники

Има няколко характеристики на техниките при номиналната група, които еднозначно ѝ позволяват да минимизира много от проблемите, дискутирани в тази глава. Те са:

1. Тъй като не е позволено никакво взаимодействие между членовете на групата, има по-малка възможност доминиращите индивиди да контролират групата. В стандартните групи е възможно важни измерения на проблема да не бъдат идентифицирани от групата, тъй като доминиращите индивиди биха наложили своите идеи без да оставят възможност на другите да правят предложения;

2. Докато всички рискове не бъдат идентифицирани, обсъдени и приети, няма да се прави никаква оценка. Когато оценката се прави преждевременно, някои аспекти на даден проблем могат да бъдат игнорирани. Това от своя страна може да доведе до неправилно идентифициране и формулиране на рисковете;

3. Тъй като всеки индивид трябва да идентифицира рисковете самостоятелно, е по-вероятно да бъдат изложени и взети под внимание аспекти на рисковете, които никога не биха били дискутирани иначе. В нормално взаимодействаща си група някои участници предпочитат да ограничат участието си до това да реагират на идеите на другите. Тъй като това не е възможно за участниците в номиналната група, е вероятно да бъдат идентифицирани по-голям брой идеи.

Техниката на номиналната група осигурява балансирано участие.

Стандартни стъпки в техниката на номинална група:

- Риск-ръководителят дава насоки, обръща внимание на целите, въвежда участниците в процеса;
- Риск-ръководителят разпространява предварително подготвените формуляри и призовава участниците да опишат своите идеи;

- Всички участници описват идеите си (рисковете) без да обсъждат помежду си;
- Когато времето за описание приключи, Риск-ръководителят събира попълнените предварително подготвени формуляри.

Тук техниката за номиналната група в тесен смисъл спира, но би могло да има още няколко стъпки за по-ефективни резултати:

- Риск-ръководителят категоризира/обобщава събраните идеи/рискове и за целта той моли участниците за някои разяснения на техните идеи;
 - Премахват се неподходящи/повтарящи се формулировки;
- Като краен резултат, Риск-ръководителят подготвя обобщен списък на идеите/рисковете.

„КРОФЪРД МЕТОД“

„Крофърд методът“ е предназначен за събиране на идеи от голям кръг хора. Чрез него могат да се събират предложения от всички служители на организацията извън риск-собствениците, участващи пряко в процеса за идентифициране и оценка на риска, и служи за сверяване и допълване на идеите (рискове/оценки), генерирани от риск-собствениците.

Същността на „Крофърд метода“ се състои в следното:

Чрез предварително подготвени форми на хартиен и електронен носител, в предварително определен срок се събират предложения за рискови фактори от служители на организацията. Целта е да се получи информация за разбирането на всички служители, неучастващи пряко в процеса по идентифициране на рисковете.

Предимствата на „Крофърд метода“, в сравнение с другите методи за първоначално събиране на информация, са:

- Служи за бързо и анонимно събиране на идеи;
 - Изключва групов интeрактивност;
 - Генерира голям брой идеи;
 - Позволява разработването на идеи, покриващи множество категории от определена тема;
 - Водещият процеса (Риск-ръководителят) подготвя определени категории по темата, на които участниците отговарят;
 - Отговорите на участниците отразяват тяхното знание и виждане по определения въпрос.
- „Крофърд методът“ се прилага, когато:
- целта е да се съберат идеи от голяма група от хора;
 - има недостиг на време или възможност за обсъждането на идеи, а се цели главно събирането на различни мнения от участниците;
 - целта е да бъде въввлечен широк кръг служители и да се създаде чувство на ангажираност.
- „Крофърд методът“ се прилага за:
- Създаване на списък от потенциални проблематични области;
 - Създаване на списък от възможни подобрения;
 - Идентифициране на възможните причини за възникване на даден проблем;
 - Генериране на възможни решения за даден проблем;
 - Спомагане създаването на подробни документи, адресиращи гореспоменатите приложения.

„ДЕЛФИ МЕТОД“

Методът „Делфи“ представлява инструмент за формиране на резултати от група. При него решението се взема на основата на голямо количество събрана информация.

Процедурата се развива на етапи (кръгове).

- На първия етап, чрез предварително подготвени работни документи, се събират мнения от всеки един от членовете на съответната Работна група (РГ);
- Всеки член на РГ попълва сам предоставения му работен документ;
- Впоследствие тези работни документи се обобщават и се изчислява средноаритметичното от оценките на всеки един от членовете на работната група;
- С цел да бъде избегнато „изкривяване“ на оценката, ако само един от членовете на РГ даде оценка със значително по-голяма разлика от останалите, може да се определи разлика над или под която съответната разлика не се включва в изчисляването на средноаритметичната стойност;
- На втория етап на членовете на РГ се подава обратна информация за резултатите от първия тур и те попълват отново работния документ за дефиниране на контролни механизми, като вземат предвид обратната информация и мотивират промяната в позицията си, в сравнение с тази, формирана през първия етап.

Процесът продължава докато не достигне предварително определен критерий - например брой етапи (кръгове), постигане на консенсус, стабилност на резултатите и т.н. Средноаритметичните резултати от финалния етап определят резултатите.