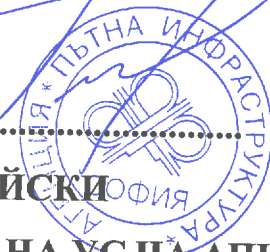




МИНИСТЕРСТВО НА РЕГИОНАЛНОТО
РАЗВИТИЕ И БЛАГОУСТРОЙСТВОТО
АГЕНЦИЯ "ПЪТНА ИНФРАСТРУКТУРА"

УТВЪРДИЛ.....
ГЕОРГИ ТЕРЗИЙСКИ
ПРЕДСЕДАТЕЛ НА УС НА АПИ



МЕТОДОЛОГИЯ
ЗА
ОЦЕНКА НА РИСКА НА
УСТАНОВЕНИТЕ КРИТИЧНИ ИНФРАСТРУКТУРИ И
ОБЕКТИТЕ ИМ

София 2019 г.

Съдържание

I. Въведение.....	3
1. Основни определения и понятия.....	4
2. Цели на методологията	4
3. Общи положения.....	5
II. Процес по управление на риска на установените критични инфраструктури.....	6
1. Оценка на риска	6
1.1 Анализ на риска	7
1.2 Изчисляване на риска.....	10
1.3 Намаляване на риска	11
2. Контрол върху риска	13
3. Документиране на процеса по анализ и оценка на риска.....	13
4. Същност на процеса по управление на риска в установените критични инфраструктури и обектите им, попадащи в управлението на Агенция „Пътна инфраструктура“.....	13
4.1 Идентифициране на критичната инфраструктура попадаща в управлението на Агенция „Пътна инфраструктура“.....	13
4.2 Идентифициране, описание (характеризиране) и оценка на заплахи.....	13
4.3 Изчисляване на риска	14
4.3.1 Оценка на преките загуби от присъщия риск.....	14
4.3.2 Определяне на стандартното отклонение на риска.....	16
4.3.3 Оценка на взаимното влияние между обектите от КИ – непреки загуби от присъщия риск.....	17
4.3.4 Определяне на общата оценка на риска.....	19
4.3.5 Определяне на Рейтинга на присъщия риск.....	19
4.3.6 Определяне на ефективността и адекватността на контрола.....	20
4.3.7 Определяне Рейтинга на остатъчния риск.....	21
4.3.8 Определяне на риск апетит (праг на търпимост)	22
5. Контрол върху риска.....	22
5.1 Реакция на риска.....	22
5.1.1 Подбор на действията в съответствие с оценката на преките загуби от риска.....	23
5.1.2 Разработване на контролни дейности.....	24
5.1.3 Анализ на разходите и ползите от контрола.....	25
5.2 Мониторинг и докладване.....	28
5.2.1 Форма и съдържание на докладите.....	28
6. Документиране на процеса.....	29
6.1 Изготвяне на документи по управление на риска.....	29
6.2 Поддържане на единна база данни за управление на риска.....	30
Приложение 1: Речник на термините.....	31
Приложение 2: Примерен списък достоверни опасности, които биха повлияли негативно върху сигурността на обекта от КИ.....	33
Приложение 3: Оценка на риска на обект/група обекти от КИ	34
Приложение 4: Оценка на непреките загуби на обект/група обекти от КИ.....	35
Приложение 5: Оценка на ефективността на контрола.....	36
Приложение 6: Риск-регистър на обект/група обекти от КИ.....	37
Приложение 7: План за ограничаване въздействието на риска.....	38

I. Въведение

Настоящата Методология е разработена на основание чл. 12, ал. 2 от Наредбата за реда, начина и компетентните органи за установяване на критичните инфраструктури и обектите им и оценка на риска за тях (приета с ПМС № 256 от 17.10.2012 г., обн., ДВ, бр. 81 от 23.10.2012 г., изм. и доп. ДВ. бр.19 от 26 Февруари 2013г., изм. ДВ. бр.27 от 5 Април 2016г., в сила от 05.04.2016 г.).

Наредбата за реда, начина и компетентните органи за установяване на критичните инфраструктури и обектите им и оценка на риска за тях (Наредбата) е приета на основание чл. 8а, ал. 1 от Закона за защита при бедствия (ЗЗБ).

Методологията се прилага от собствениците/операторите на установени КИ и обектите им за секторите и подсекторите, съгласно Списък със секторите и подсекторите с критична инфраструктура в Република България (*Приложение № 1 към чл. 2, ал. 1 от Наредбата*). Подсектор „Автомобилен транспорт и пътна инфраструктура“ е от компетентността на Агенция „Пътна инфраструктура“.

Мерките за намаляване уязвимостта на обектите от природни и причинени от човека опасности се определят с Наредбата по чл. 10, ал. 2 от ЗЗБ.

1. Основни определения и понятия.

По смисъла на Наредбата и ЗЗБ са дадени следните определения:

- **"Критична инфраструктура" /КИ/** е система или части от нея, които са от основно значение за поддържането на жизненоважни обществени функции, здравето, безопасността, сигурността, икономическото или социалното благосъстояние на населението и чието нарушаване или унищожаване би имало значителни последици за Република България в резултат на невъзможността да се запазят тези функции (*§ 1, т. 1 от Наредбата и § 1, т. 15 от допълнителните разпоредби на ЗЗБ*).
- **"Обект на критична инфраструктура"** е организационно и/или икономически обособена част от критичната инфраструктура, която е ключова за нормалното функциониране, непрекъснатостта и целостта ѝ (*§ 1, т. 2 от Наредбата*).
- **"Собственици/оператори на критични инфраструктури"** са физически или юридически лица, които отговарят за инвестирането или за нормалното

функциониране, непрекъснатостта и целостта на определена система или част от нея, установена като критична инфраструктура в Република България (§ 1, т. 3 от Наредбата).

- **"Защита"** е съвкупност от дейности, целящи гарантиране на нормалното функциониране, непрекъснатостта и целостта на критичните инфраструктури с цел възпиране, намаляване, смекчаване или неутрализиране на заплахите, рисковете или уязвимостта им.
- **"Уязвимост"** е показател за степента на податливост на дадена територия или обект на различните опасности.
- **"Опасност"** е природно явление или събитие, причинено от човешката дейност, което може да причини вредни последици за населението и имуществото му, околната среда, икономиката и културните и материалните ценности.
- **"Риск"** е вероятност от възникване на вредни последици за населението и имуществото му, икономиката и околната среда в резултат на опасността и уязвимостта за дадена територия/обект.
- **"Анализ и оценка на риска"** е определяне същността и размера на риска като функция на /опасността, уязвимостта и вероятността/ вероятността и въздействието.

За нуждите на настоящата Методология се използват понятия описани в Приложение 1 – „Речник на термините“.

2. Цели на методологията

Методологията е етап от цялостен подход, включващ установяването на критичните инфраструктури и обектите им, анализа на риска за тях и прилагането на конкретни мерки за намаляване на уязвимостта им. Главната цел на този подход е да се осигури надеждна и оптимална защита от всички възможни за КИ и обектите им опасности, чрез цялостно изграждане на най-подходящата структурна организация за сигурност. Тази организация трябва да изпълнява ефективно целите и задачите на сигурността, да реагира своевременно и изпреварващо при екстремни ситуации, да е оптимална и функционално самоусъвършенстваща се, да е снабдена с модерни технически средства и изградена от професионалисти. Структурната организация трябва да е разработена и съгласно действащото в страната нормативно законодателство в тази област с разбирането, че пълното или частично нарушаване на обекта или неговото разрушаване може да доведе до значителни загуби за населението, икономиката, околната среда.

Целта на Методологията е да се определят заплахите и уязвимостите за КИ и обектите им, да се оценят рисковете, да се приоритизират по тяхната критичност, да се установят наличните мерки за защита и ефективно се комбинират, като се усъвършенстват или добавят нови такива при необходимост и да се извърши правилна оценка на остатъчния риск. Изхождайки от това да се вземат адекватни и обосновани технически и управленски решения, с цел елиминирание или минимизиране на възможните щети, предизвикани от въздействието върху тези инфраструктури и обекти.

Управлението на риска е възприет в световен мащаб основен подход към критичните инфраструктури. Той обхваща всички дейности, целящи идентифициране и намаляване на рисковете, произтичащи от зависимостта на обществото от КИ и обектите им в случаи на бедствия, аварии, катастрофи, терористични актове. Управлението на риска е съвкупност от процеси, методи и инструменти, които осигуряват дисциплинирана околна среда и подпомагат вземането на решения за това да се определя кои рискове са първостепенни за справяне, да се преценява постоянно какво може да се обърка и да се вземат съответните мерки. Управлението на риска само по себе си не гарантира успех - то ни дава възможност да вземем правилните решения, да предвидим и предотвратим изненади, да подобрим шанса за успех. Добре информирани решения могат да се вземат само ако се разбираат рисковете.

3. Общи положения

Инфраструктурите и обектите, които се третират от настоящата методология са установени за КИ и обекти към тях, съгласно Наредбата. Оценката на риска изисква определяне на характеристиките им, които при наличие на наблюдения могат да бъдат получени с помощта на точни вероятностни методи или по експертен път. Методологията дава препоръки относно условията и реда за оценка на риска на КИ и обектите им и установяване на приоритетите им за защита. Обобщената оценка на риска се основава на съчетанието на три параметъра – опасност, уязвимост и вероятност. Опасността става риск само когато е налице уязвимо място в инфраструктурата, което тя може да атакува.

Управлението на риска идентифицира опасностите и уязвимостите, както и вероятностния подход за тяхното проявление за да се приложи подходящ контрол и средства за минимизиране на риска, за да се предотвратят инцидентите или да се намалят последиците от тях (природни, човешки, технологични). Необходимо е да се извърши експертна оценка за критичност на всеки обект на КИ, касаеща неговата уязвимост, защитеност, възстановяемост, зависимост, взаимозависимост и др. Необходимо е и да се разгледат възможните сценарии за прекъсване на доставките, причинени от срив на основни инфраструктури и да се оценят вероятните последици от тези сценарии. След това е необходимо да се въведат мерки за укрепване на инфраструктурата (физически, организационни и други за да се намали уязвимостта на елементите от инфраструктурата, включително евентуалното ѝ подсилване).

Намаляването на уязвимостта на КИ и обектите им се разглежда като динамично състояние на дадена система, което осигурява неутрализирането и противодействието на външни и вътрешни фактори. Управлението на риска не избягва или премахва рискът. То разбира какви са рисковете, какво е вероятното им въздействие, ако се материализират и как да се управлява това.

заплахи, които са резултат от човешка дейност, технологични заплахи и природни бедствия.

В Агенция „Пътна инфраструктура“, оценката на риска за установените КИ и обектите им се извършва от дирекция „Анализ на риска и оперативен контрол“.

При необходимост за анализа и оценяването на риска на КИ, дирекцията може да привлече специалисти от други структурни звена на АПИ, както и външни специалисти.

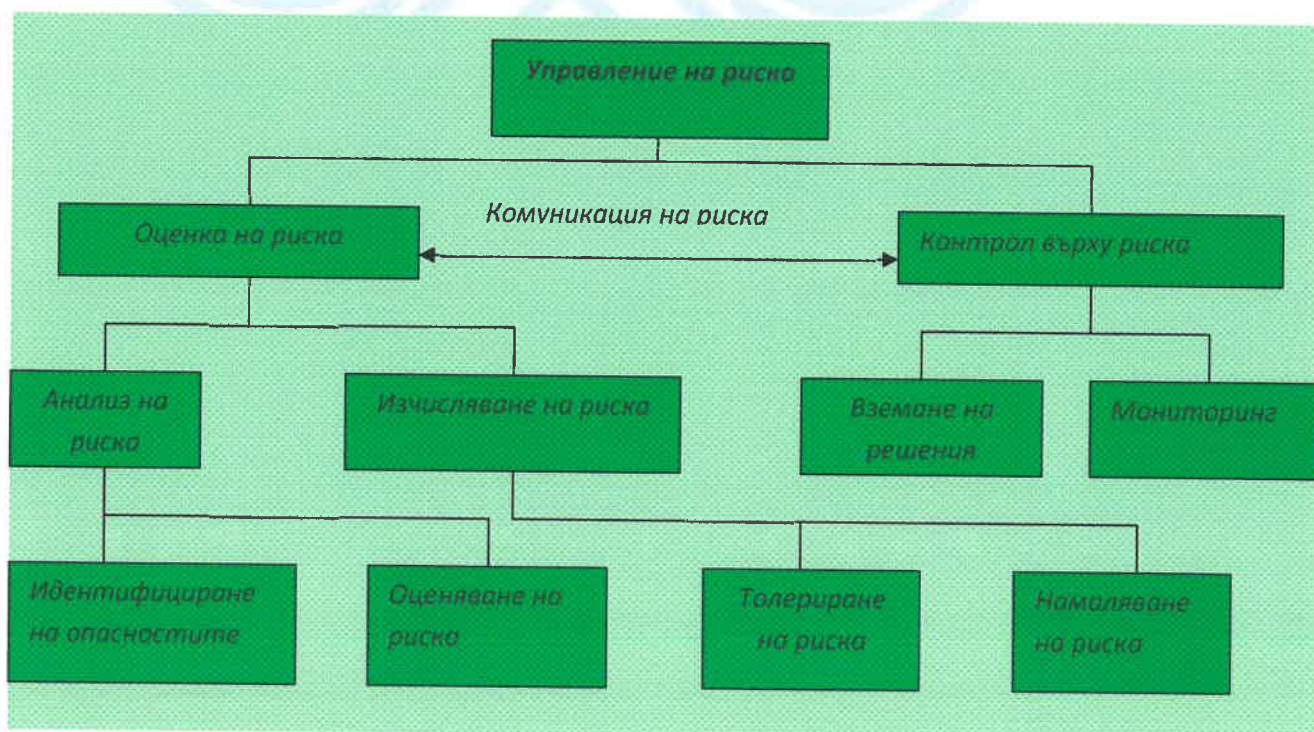
Управлението на риска на установените КИ включва идентифициране, анализ и оценка на рисковете (заплахите). Въз основа на извършената оценка на риска следва да се прецени необходимостта от ограничаване на риска, чрез въздействие върху него, като се планират и прилагат мерки за сигурност на установените КИ и обектите им. През целия този системен и логичен процес непрекъснато се наблюдава и документира риска, с цел гарантиране неговото надеждно управление.

Способите за предотвратяване на опасностите и за защитата на КИ и обектите им са: анализът и оценката на риска (оценка на опасностите за защитата на КИ и обектите им) и мерките за намаляване на уязвимостта на обектите от КИ с цел подобряване на тяхната защита. Целта на способите е създаването на ефективни методи за противодействие на опасностите за защитата на КИ и обектите им и ключовите им елементи чрез използване на защитни мерки.

При извършването на дейности по изпълнение на тази методология, свързани с достъп до класифицирана информация, се прилагат изискванията на Закона за защита на класифицираната информация.

II. Процес по управление на риска на установените критични инфраструктури.

Основните компоненти на управление на риска и съответните основни понятия са посочени в диаграма на фигура 1:



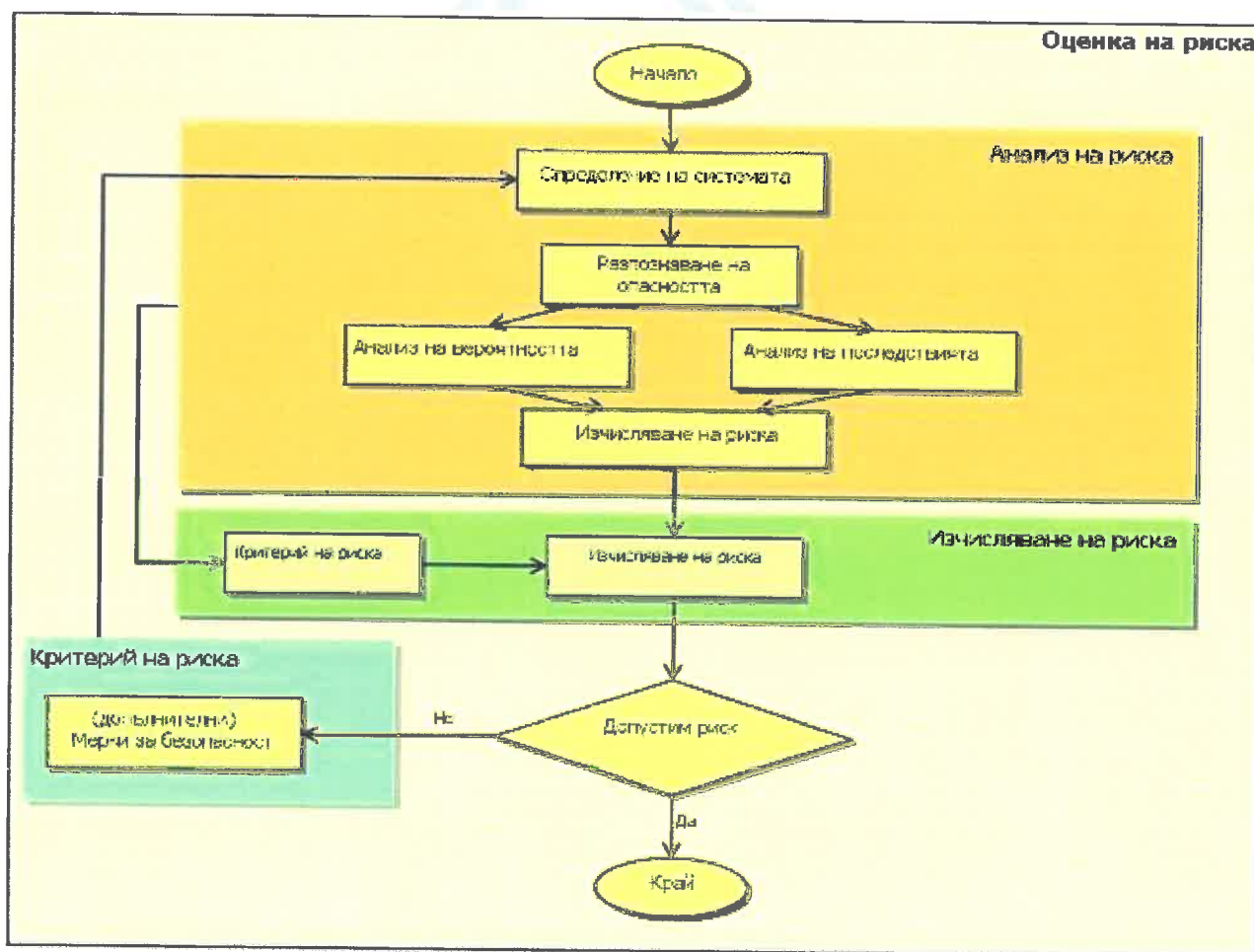
фигура 1

1. Оценка на риска

Процедурата за анализ на риска може да се раздели на следните три стъпки:

- Идентификация на опасностите: Систематичен процес за идентифициране и структуриране на всички възможни опасности и за анализиране на съответните последици.
- Анализ на вероятностите: Определяне на вероятностите за съответните събития/рискове.
- Въздействие върху риска и избор на вариант на мерки за защита.
- Анализ на последиците.

Опростената диаграма на фигура 2 илюстрира основните стъпки на процеса на оценка на риска.



фигура 2 - Схема на процедурата по оценка на риска

Трябва да се отбележи, че на фигура 2 са показани само основните характерни елементи на процеса на оценка на риска; когато се анализира безопасността на определен обект от КИ може да са необходими по-подробни диаграми, допълнителни елементи и допълнителни взаимни връзки.

Процесът на оценка на риска включва следните ключови елементи:

1.1. Анализ на риска

Анализът на риска е систематичен подход за анализиране на последиците и взаимоотношенията при потенциални заплахи, който по този начин установява слабите места в системата и определя възможни мерки за подобряване.

Анализът на риска има за цел да даде отговор на основния въпрос: „Какво може да се случи и какви ще бъдат последиците?“. Анализът на риска включва: анализ на средата за сигурност; разглеждането на причините и източниците на риск, както и техните положителни и отрицателни последствия и вероятността да се случат; установяване на ключовите елементи и начина на защита и/или охрана; анализ на съществуващите мерки за защита; разглеждане на различни сценарии за действие при сериозни опасности; въз основа на сценариите отчитане на последствията и уязвимостите за КИ и обектите им, както и на потенциалните последици за населението, икономиката, околната среда и социално-политическо въздействие от нарушаването или унищожаването им.

Анализът на риска може да се осъществи по качествен или по количествен начин или като комбинация от двата начина. При количествения анализ се оценяват възможностите за реализиране на заплахите и техните последици (например от гледна точка на смъртни случаи, наранявания, материални щети и прекъсване на услугите) и свързаните с тях рискове. Анализът се осъществява посредством събиране на подробна информация за идентифициране на ключовите елементи (ценности) на КИ и обектите им, може да се извърши по един или комбинация от следните методи: използване на въпросници, отнасящи се до планирани и приложени мерки за сигурност; провеждане на интервюта с различни категории служители; разглеждане на налична документация; използване на специализирани програмни или технически средства и др. Определянето на риска изисква задълбочено познаване на средата, в която функционират КИ и обектите им във всички аспекти – околна среда, физическа среда, техническа среда, организационна среда и др.

Началният етап от анализът на риска е **идентифициране и оценка на опасностите**.

➤ Идентифицирането на риска обхваща:

- идентифициране на природните и причинени от човека опасности водещи до нарушаването или унищожаването на КИ и обектите им, техните източници и причини и вероятността да се случат;
- за всяка идентифицирана опасност определяне уязвимостта за КИ и обектите им и потенциалните последици от това, както и вероятността да се случат;
- идентифициране на опасностите и уязвимостите не само за дадената КИ и обектите им, но и възможното влияние, взаимодействие и въздействие с други инфраструктури и обекти с цел минимизиране на каскадните ефекти.

Правилното описание на опасностите и уязвимите места за КИ и обектите им е важна част от успешното изготвяне на анализа и оценката на риска и определянето на системата от мерки за защита.

✓ **Идентифицирането на риска** цели установяване на всякаква заплаха или вреда в резултат на бедствия и аварии, нерегламентиран достъп, опит за нерегламентиран достъп, терористична дейност или саботаж, технологични фактори, както и влиянието и последиците при тяхното проявление.

✓ **Идентифицирането на опасностите за КИ и обектите им** е идентифициране на възможността за реализиране на случайна или целенасочена опасност за нарушаване функционирането на КИ и обектите им. За да се разберат и определят опасностите за конкретните КИ и обектите им е необходимо те да бъдат разделени по категории според източника им: причинени от природни бедствия и аварии; причинени от човешка намеса; технологични (неизправности и отказ на технически средства). Освен това всяка опасност, причинена от човешка намеса, може да бъде вследствие на случайна (непреднамерена) или преднамерена човешка намеса. Преднамерените опасности могат да възникнат вследствие на умишлено използване на пропуски и слабости в проектирането и експлоатацията на КИ и обектите им. Непреднамерените опасности могат да възникнат поради неумишлени пропуски и слабости в проектирането и експлоатацията на КИ и обектите им, както и на недобре обучен персонал. Преднамерените и непреднамерените заплахи могат да бъдат вътрешни и външни.

✓ **Идентифицирането на риска** е процес на намиране, разпознаване и описание на рисковете, като им се състави изчерпателен списък. Включва определяне на основните рискове за КИ и обектите им, чрез изясняване на това - къде, кога, защо и как могат да възникнат рискове, описание и характеризиране на техните елементи. Идентифицирането на риска съдържа идентифициране на източниците на риска, на събитията и на техните причини и потенциални последствия. То може да се прави на базата на исторически данни, теоретични анализи, обосновани експертни мнения, както и на потребностите на заинтересовани лица. От решаващо значение е да се идентифицират всички рискове, защото риск неидентифициран на този етап, няма да бъде включен в по-нататъшния анализ. След като се идентифицира това, което може да се случи, трябва да се проверят възможните причини и сценарии за евентуални последствия, като бъдат проучени всички значителни причини и последствия. При идентифицирането на риска от съществено значение е използваната информация да бъде постоянно актуализирана и да участват служители, които притежават съответните познания.

✓ **Идентифицирането на уязвимостите за КИ и обектите им е идентифицирането на слабостите в тях.** Уязвимостите, това са слабостите на КИ и обектите им, там където те са податливи на различните опасности. Уязвимостите могат да се дължат на пропуски и слабости в проектирането и експлоатацията на КИ и обектите им, на недобрата им устойчивост на работа, на занижен надзор и физическа защита, може да бъдат от техническо, технологично, организационно или процедурно естество. Прилагането на мерките за защита намаляват вероятните загуби от реализирането на евентуална опасност.

✓ **Определянето степента на вероятност на опасността** е определяне на вероятността определена опасност да използва потенциална уязвимост на КИ и обектите им при наличие на приложени и/или планирани мерки за защита и да въздейства върху тях. Трябва да се вземат под внимание следните фактори: мотивация и възможности на източниците на заплахи; характер и природа на съществуващите уязвимости; съществуващи средства за контрол и управление т.е. преглед и отчитане на ефективността на приложените вече мерки за защита спрямо възможните заплахи за КИ и обектите им.

✓ **Организацията на дейността на процеса по оценка на риска трябва да:** обхваща всички елементи, осигуряващи функционирането, непрекъснатостта и целостта на КИ и обектите им с цел установяване на всички възможни опасности, уязвимости и рискове; установява подходите и методите за извършване оценката на риска, включително осигуряване достоверност на резултатите; съдържа описание на източниците на информация за оценката на риска.

Процесът по оценката на риска трябва да е непрекъснат, цялостен и аналитично-информационен по събирането на данни и техния анализ, оценка от гледна точка на защитата на КИ и обектите им, идентифицирането, анализа и оценката на риска.

➤ **Оценка на взаимното влияние между обектите от КИ – непреки загуби.**

Оценка на взаимовръзката между секторите

Определят се загубите в стоки и услуги за стопанството и населението вследствие на взаимното влияние между обектите от КИ, т.е. непреките загуби. Взаимното влияние може да се прояви като зависимост и взаимозависимост.

- **Зависимост:** Свързване или връзка между две инфраструктури, чрез която състоянието на едната инфраструктура влияе или е свързано със състоянието на другата.

- **Взаимозависимост:** Двустранна зависимост между две инфраструктури, чрез която състоянието на всяка една влияе или е свързано със състоянието на другата. По-общо казано, две инфраструктури са взаимозависими, когато всяка една от тях е зависима от другата.

Взаимозависимостите между обектите могат да бъдат:

▪ **Физически:** Две инфраструктури са физически взаимозависими, ако състоянието на всяка една е зависимо от материалния изход(и) на другата: стока произведена или модифицирана от една инфраструктура (изход) е необходима за работата на друга (вход). Вследствие на това, рискът от повреда или отклонение от нормалното работно състояние в едната инфраструктура може да бъде функция от риска в друга инфраструктура.

▪ **Кибернетични:** Една инфраструктура има кибер-взаимозависимости, ако състоянието ѝ зависи от информацията, пренасяна по информационната инфраструктура. Вследствие на това, състоянието на тази инфраструктура зависи от изходите на информационната инфраструктура.

▪ **Географски:** Дадени инфраструктури са географски взаимозависими, ако събитие в обкръжаващата ги среда може да създаде промени в състоянието на всички тях. При географска близост на обекти, събития като експлозия или пожар могат да причинят взаимосвързани повреди или промени в тях. Взаимозависимостта се дължи единствено на близостта; състоянието на дадена инфраструктура не се влияе от състоянието на друга.

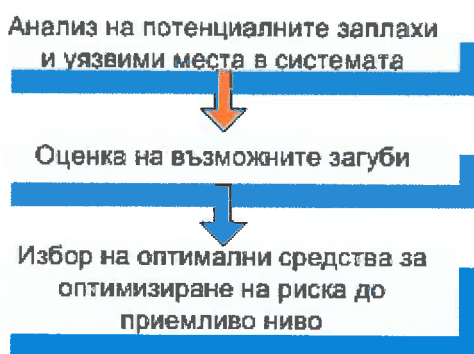
▪ **Логически:** Две инфраструктури са логически взаимозависими, ако състоянието на всяка една зависи от другата чрез механизъм, който не е физически, кибер или географска връзка. Основна роля при логическите взаимозависимости играят човешките решения. Например, ако се понижи цената на бензина може да доведе до пренатоварване на магистралите и задръствания на движението. В този случай логическата връзка между петролната и транспортната инфраструктури се дължи на човешки решения и действия и не е резултат от физически процес.

Непреките загуби са резултат от намалението на производството и доставянето на **стоки и услуги** вследствие излизане от строя и взаимно влияние на обекти и системи (сектори), осигуряващи нормалната жизнена среда на населението.

1.2. Изчисляване на риска:

Изчисляването на риска е определяне размера на риска като функция на опасността, уязвимостта и вероятността чрез сравняване нивото на риска установено в процеса на анализа с приемливите му критерии, за да се проучи необходимостта от въздействие върху риска. Установява се степента на застрашеност и уязвимост на обекта.

На базата на резултатите от анализа на риска целта на изчисляването на риска е да се подпомогне Агенция „Пътна инфраструктура“ при вземането на решения за необходимостта от въздействие върху риска и приоритета при внедряване на въздействието. Решенията трябва да се вземат, като се спазват изискванията на нормативните актове и други изисквания. В някои случаи изчисляването на риска може да доведе до решение да се предприеме по задълбочен анализ или до решение да не се въздейства върху риска.



Изчисляването на риска се изготвя на база информацията за опасностите за обекта и уязвимостта му от тях. Оценката на всеки един елемент е необходимо да се извърши от експерти имащи опит в теренни, технологични и други функции и дейности. Оценката на риска дава информация за компетентни управленски решения относно мерките за защита на КИ и обектите им и тяхното приоритизиране. Трябва да се класифицират ключовите елементи на обектите по важност, както и необходимите финансови средства за постигане на всяко определено ниво на сигурност и др.

За правилното изчисление на риска може да се използват средства за моделиране на външни опасности в/у КИ и обектите им – природни бедствия в цялата им съвкупност характерна за района, аварии, терористични атаки и др. и оценка на пораженията, включително и отразяване на взаимовръзките между обектите на КИ при определени външни опасности. Предварителната оценка на пораженията и загубите ще спомогне за определяне на мерките за сигурност, начините за действия за отстраняване на последствията и др., както и на финансови разчети за достигане на определено ниво на сигурност на КИ и обектите им от различните въздействия – природни бедствия, човешка намеса, технологични фактори.

Резултатът от тази стъпка е определяне на нивото на риска, което може да се определи като Високо, Средно или Ниско.

Изчисляването на риска е насочено към въпроса за приемливостта. То трябва да даде отговор на следния въпрос „Дали изчисленият риск е допустим?“. За системно и изпълнимо изчисляване на риска трябва да се дефинират критерии за риска и да се установи дали дадено ниво на риск е приемливо или не.

1.3. Намаляване на риска / Планиране на (допълнителни) мерки за безопасност: Планирането на мерките за безопасност трябва да отговори на въпроса „Кои мерки са необходими, за да се получи безопасна (рентабилна) система?“. Ако изчисленият риск се смята за недопустим, трябва да се предложат допълнителни мерки за безопасност.

При високо ниво на риска трябва да бъдат предприети незабавни намаляващи нивото му действия и да се извърши последващата му оценка. При средно ниво на риска са необходими действия за намаляване на нивото му в определен оптимален срок и да се извърши последващата му оценка. При ниско ниво на риска следва да се определи дали са необходими неутрализиращи действия или е възможно риска да бъде приет.

✓ **Въздействието върху риска включва повтарящ се процес за:** оценяване на въздействието върху риска; решение дали нивата на остатъчния риск са допустими; когато нивата на остатъчния риск не са допустими, пораждање на ново въздействие върху риска; оценяване на ефикасността на въздействието върху риска.

✓ **Възможностите за въздействие могат да включват:** избягване на риска, чрез вземане на решение да не се започва или продължава дейност, която поражда риск; поемане или нарастване на даден риск с цел да се постигне благоприятна възможност; премахване на източника на риск; изменение на възможност; изменение на последствията; споделяне на риска с друга или други страни; поддържане на риска, основано на аргументиран избор.

Изборът на най-подходящата възможност за въздействие върху риска включва сравняване на разходите и усилията за внедряване по отношение на получените ползи (напр. за рискове с много отрицателни последствия, но редки проявления - въздействието върху тях може да не е оправдано по икономически причини), както и задълженията, произтичащи от изискванията на нормативните актове и други изисквания. Определен брой варианти за въздействие върху риска може да бъдат изследвани и прилагани самостоятелно или в комбинация. Трябва да се разгледа дали самото въздействие върху риска може да породи рискове. Слабостта или неефикасността на мерките за въздействие върху риска може да представлява значителен риск. За да се гарантира, че мерките са ефикасни, наблюдението трябва да бъде неразделна част на процеса по управление на риска.

Важно е да се разбере природата на рисковете, с които се сблъскват КИ и обектите им. В някои случаи рисковете са изцяло или в голяма степен под контрол. Тогава може да се определя колко риск може да се поеме. По принцип винаги може да се намали риска като се създадат повече контролни и предпазни механизми. Но това има своята цена. Управлението на риска означава да се претеглят допълнителните разходи срещу намаления риск, за да се вземе добре информирано решение. В други случаи рисковете са напълно или преобладаващо извън контрол. За този тип рискове ударението пада най-вече върху преценката на вероятността от възникване на проблема и определяне на начина, по който да се управлява, ако това стане. За повечето дейности по КИ и обектите им има редица рискове, някои от които са в рамките на контрол, а други не са.

След определяне на начина на въздействие върху риска, следва да се предприемат мерки за подобряване на защитата на КИ и обектите им .

Нормативното определяне на мерките за намаляване на уязвимостта на обектите от критичната инфраструктура на природни и причинени от човека опасности е определено с наредбата по чл. 8а, ал. 3 от ЗЗБ.

Установяването, подборът и подреждането по приоритети на мерките за сигурност, необходими за защитата на обекта се извършва, като се отчитат алтернативните решения, включително новостите по съответните проблеми, осъществимостта на решенията и възможността за инвестиции.

Мерките за намаляване на уязвимостта се предприемат за предотвратяване, намаляване или ограничаване на рисковете, оценени над приемливите им нива. Изборът на вариант на мерките за намаляване на уязвимостта отчита съществуващите мерки, алтернативните решения, осъществимостта на вариантите и възможностите за инвестиции.

Не се изисква допълнително въвеждане на мерки за намаляване на уязвимостта ако се установи, че вече има въведени ефикасни такива.

Мерките за подобряване на защитата на КИ и обектите им са постоянни и допълнителни. Мерките имат за цел:

- своевременно установяване и противодействие при нарушаване или при опит за нарушаване на въведените мерки за подобряване на защитата на КИ и обектите им;

- предотвратяване на нерегламентиран достъп или на опит за нерегламентиран достъп до ключовите елементи на КИ и обектите им;

- запазване на функционалното състояние на съоръженията и оборудването в КИ и обектите им.

- определяне на контролирани периметри;

- наличие при необходимост на непрекъсната охрана;

- наличие на алармена система против проникване и/или сили за реагиране, които след постъпване на сигнал за нарушение пристигат на мястото за време по-малко от необходимото за преодоляване на техническите мерки за достъп до ключовите елементи.

2. Контрол върху риска

Необходимо е анализиране и актуализиране на процеса по управление на риска, периодично или при необходимост, включващо: преразглеждане и преоценка на риска, идентифициране и оценка на нововъзникнали и остатъчни рискове с възможното им проявление, описание на остатъчните заплахи и тяхното допустимо проявление, необходимост от внедряване на допълнителни защитни механизми.

Наличието на остатъчни рискове трябва да бъде ясно отбелязано, тъй като може да се приеме, че ако остатъчният риск не бъде приведен до приемливо ниво, то трябва да се извърши отново анализ и оценка на дадения риск с цел намиране на други пътища за понижаването му.

Мониторингът на риска се осъществява чрез наблюдение и координиране на процесите по управление на риска и постигнатите резултати. Основната функция на процеса по мониторинг на управлението на риска е да осигури информацията относно:

- Наличие и достатъчност на мерки за управление на риска;
- Необходимост от създаване на нови мерки за нови критични рискове;
- Необходимост от промяна на мерките за управление на риска, където предприетите мерки са се оказали недостатъчни;
- Необходимост от намаляване на мерките за управление на риска, когато те са ненужни;

3. Документиране на процеса по анализ и оценка на риска

Необходимо е документирането на процеса по анализ и оценка на риска, включващо и избраните варианти на мерки за защита с описание на приложените мерки за предотвратяването, намаляването и ограничаването на риска, отчитайки съществуващите такива. Документират се и периодичните проверки, преразглеждане и преоценка на риска, включително за нововъзникнали и остатъчни рискове с възможното им проявление и мерки за защита.

4. Същност на процеса по управление на риска в установените критични инфраструктури и обектите им, попадащи в управлението на Агенция „Пътна инфраструктура“.

4.1. Идентифициране на критичната инфраструктура попадаща в управлението на Агенция „Пътна инфраструктура“

Потенциалните обекти за включване в регистъра на критичната инфраструктура, попадаща в управлението на АПИ, се определят на база утвърдени от Председателя на УС на АПИ „Правила за определяне на критичните инфраструктури и обектите им на територията на Република България, попадащи в управлението на АПИ“.

4.2. Идентифициране, описание (характеризиране) и оценка на заплахи.

Анализа и оценката на риска се извършва от дирекция „Анализ на риска и оперативен контрол“ в АПИ, като при необходимост могат да се ползват експерти от други дирекции и независими експерти, които следва да притежават добро разбиране и експертни познания относно изискванията за безопасност на установените КИ, умения и опит за оценяване и управление на комплексни рискови фактори.

Оценката на заплахата е възлов момент както по отношение на критичната инфраструктура, така и за защитата на населението.

Експертните оценки се определят на базата на анализ на прогностичните данни за очаквани природни явления, които биха предизвикали определени бедствия. При оценката се вземат предвид географските характеристики на региона – местоположение, релеф, климат, почви, наличие на опасни водоеми в близост, а също така и техническата инфраструктура, която ще поеме въздействията (пътища, мостове и др.). Оценката на очакваните техногенни бедствия се извършва на основата на анализа на данните за обектите от техническата инфраструктура – местоположение, сектор на КИ, използвана технология, брой на персонала, опасни (рискови) производства, складове с химически и опасни вещества, анализ на причините и следствията от минали аварии и др.

В процеса на определяне на рисковете може да се ползва примерен списък достоверни опасности, които биха повлияли негативно върху сигурността на КИ (Приложение №2). При идентификацията на рисковете акцентът трябва да бъде поставен върху сравнително малък брой значими рискове, което е необходимо за ефективното им управление.

На база осъщественият анализ на риска се изготвя регистър на идентифицираните общи рискове .

4.3. Изчисляване на риска

4.3.1. Оценка на преките загуби от присъщия риск

На този етап се определят преките загуби вследствие на възникналото конкретно бедствие. Оценката на уязвимостта на елементите на КИ се извършва, като се използват данните за вероятността за възникване на бедствие с определена интензивност. Оценката на пораженията се извършва за човешки и материални загуби. По този начин може по-ясно да се определи характера и особеността на обекта от КИ.

Въз основа на съображенията относно влиянието на честотата на събитията и размера на щетите, се извършва оценка на очакваните рискове и се определя величината на идентифицираните рискове.

Оценката на риска се извършва на базата на двуфакторен модел, където оценяваните фактори са:

Вероятност за реализация на риска;

Влияние (въздействие) на събитието, в случай, че рискът се реализира.

На всяка опасност от списъка на идентифицираните рискове се определя категория на „вероятност на събитието” и категория на „влияние на събитието”, като се оценяват със съответен брой точки.

➤ Оценка на фактор - „вероятност на събитието”

Оценката се определя по скалата от таблица 1.

Вероятност	Описание	Процентна вероятност	Точки
Почти сигурно	Много често срещано явление	Над 85%	9
Вероятно	Често срещано явление	51-85%	7
Възможно	Случва се	21-50%	5
Рядко	Може да се случи, но не много често	1-20%	3
Не е вероятно	Теоретически възможно, но появата не се очаква да се случи	По-малко от 1%	1

таблица 1 - Вероятност на събитието

➤ **Оценка на фактор - „влияние на събитието”**

По аналогичен начин, като оценка на честотата на събитията следва да се определи размера на щетите по отношение на телесните повреди и материалните щети. На база експертна оценка следва да се прогнозираат последиците от реализирането на риска, от гледна точка на следните аспекти:

- Оценка на размера на щетите (телесни повреди, материални щети);
- Оценка на възможността за провеждане на спасителни операции;
- Оценка на възможността за предприемане на самостоятелни спасителни действия;
- Оценка на степента на защита и уязвимост на обекта на КИ;
- Оценка на техническото състояние на съоръженията на КИ и др.

Оценката се определя по скалата от таблица 2 .

Величина на въздействие на риска	Описание		Точки
	Материални щети	Човешки жертви	
Катастрофален	Обектът не може да бъде експлоатиран	над 5 бр. човешки жертви	9
Тежък	Сериозна заплаха за експлоатация на обекта	1-5 бр. човешки жертви	7
Съществен	Увеличават се значително оперативните разходи	тежки травми	5
Пределен (умерен)	Малък ефект върху оперативните разходи	леки телесни наранявания	3
Несъществен	Пренебрежимо малък ефект	без телесни наранявания	1

таблица 2 - Въздействие на събитието

Въз основа на Регистъра на идентифицираните общи рискове, всеки оценител осъществява самостоятелна оценка по фактора „вероятност на събитието” и фактора „влияние на събитието” на всеки риск.

4.3.2. Определяне на стандартното отклонение на риска

На база на резултатите от оценка на риска се определят „рискове под въпрос”, които имат стандартно отклонение повече от „1”. Обикновено се срещат такива случаи, когато амплитудата в оценките на даден риск е прекалено голяма, т.е. има крайно различни мнения на оценителите от комисията относно вероятността да се случи даден риск или степента на влияние, което би оказал.

Стандартното отклонение на риска се изчислява отделно за всеки риск, както за фактора „вероятност”, така и за фактора „влияние” по следните формули:

$$SDL = \sqrt{\frac{(L_1 - AL)^2 + (L_2 - AL)^2 + (L_3 - AL)^2 + \dots + (L_n - AL)^2}{n}}$$

Където: SDL- Стандартно отклонение на риска по фактора „вероятност”;

L- Индивидуална оценка на конкретен риск по фактора „вероятност” на всеки оценител на риска;

AL- Обща вероятност (средноаритметичната стойност от оценките на всички оценители на риска за конкретен риск по фактора „вероятност”)

$$AL = \frac{(L_1 + L_2 + L + \dots + L_n)}{n}$$

n- брой на оценките.

$$SDE = \sqrt{\frac{(E_1 - AE)^2 + (E_2 - AE)^2 + (E_3 - AE)^2 + \dots + (E_n - AE)^2}{n}}$$

Където: SDE- Стандартно отклонение на риска по фактора „влияние”;

E- Индивидуална оценка на конкретен риск по фактора „влияние” на всеки оценител на риска;

AE- Обща вероятност (средноаритметичната стойност от оценките на всички оценители на риска за конкретен риск по фактора „влияние”)

$$AE = \frac{(E_1 + E_2 + E_3 + \dots + E_n)}{n}$$

n- брой на оценките

Рисковете под въпрос се оценяват отново от оценителите, като се следва описаната процедура, която продължава до момента, в който се постигне консенсус.

4.3.3. Оценка на взаимното влияние между обектите от КИ – непреки загуби от присъщия риск.

Непреките загуби са естествен резултат от намалението на производството и доставянето на стоки и услуги – тук се включват загубата на приходи и по-високите разходи за производството. Непреките загуби се оценяват чрез експертен анализ и оценка на чувствителността и взаимното влияние на обектите в системата на инфраструктурата, водещо до нарушаване на тяхното нормално функциониране. В такъв случай инфраструктурата се разглежда като сложна система от взаимодействащи си компоненти.

В настоящата методология се разглежда влиянието, в случай на реализация на всеки идентифициран риск, върху следните категории (групи) жизнени фактори, най-силно засягащи условията на живот:

- доставка на храна;
- доставка на лекарствени материали и медицинско обслужване;
- доставка на енергоизточници – твърди горива, газ, петролни продукти;
- доставка на суровини и материали за промишлеността;
- обществен транспорт;
- международен транспорт.

За оценка на непреките загуби, т.е. нарушаването в осигуряването на тези групи стоки и услуги като основен се възприема критерия „брой засегнати хора”. Използва се скалата за оценка на непреките загуби (Таблица 3).

Оценка	Засегнати хора (брой)	Оценъчна стойност
МАЛКИ	до 500	0 - 3
СРЕДНИ	до 2 000	3 - 5
ГОЛЕМИ	до 7 000	5 - 8
КАТАСТРОФАЛНИ	до 15 000	8 - 9

Таблица 3 - Критерии за класификация на непреките загуби

На основата на характеристиките на обектите и тяхната функционалност, при изчисляването на обобщените оценки за всеки риск на обекта, експертните оценки за отделните категории стоки и услуги се умножават със съответен тегловен коефициент (Таблица 4).

Групи	Тегловен коефициент
доставка на храна	3
доставка на лекарствени материали и медицинско обслужване	2

доставка на енергоизточници – твърди горива, газ, петролни продукти	2
доставка на суровини и материали за промишлеността	1
обществен транспорт и международен транспорт	1

Таблица 4 - Тегловни коефициенти за групите жизнени фактори

Изчисляване на размера на непреките загуби (Таблица 5):

№	Критерий	Тегловен коефициент	Засегнати хора (брой) ¹	Оценка на непреките загуби
1.	К1 - доставка на храна	Тк1 - 3	Н1	Z1
2.	К2 - доставка на лекарствени материали и медицинско обслужване	Тк2 - 2	Н2	Z2
3.	К3 - доставка на енергоизточници – твърди горива, газ, петролни продукти	Тк3 - 2	Н3	Z3
4.	К4 - доставка на суровини и материали за промишлеността	Тк4 - 1	Н4	Z4
5.	К5 обществен транспорт и международен транспорт	Тк5 - 1	Н5	Z5
				Z общо

Таблица 5 - Изчисляване на размера на непреките загуби

$$Тк \times Н = Z$$

$$Z \text{ общо} = Z1 + Z2 + Z3 + Z4 + Z5$$

Където:

К- Критерий;

Тк- Прагове за тежест;

Н- Оценка на предполагаем брой на засегнатите хора;

Z- Оценка на непреките загуби от конкретен риск;

Z общо - Обща оценка на непреките загуби /на един оценител/.

¹ Нанася се оценъчната стойност от таблица 3

4.3.4. Определяне на общата оценка на риска

Общата оценка на всеки риск представлява средното аритметично число от оценките на всички оценители, представени поотделно за фактора „вероятност” и за фактора „влияние” (за преките загуби) и оценката на непреките загуби.

$$P = \frac{P_1 + P_2 + P_3 + \dots + P_n}{n}$$

$$S = \frac{S_1 + S_2 + S_3 + \dots + S_n}{n}$$

$$Nz = \frac{Z_1 + Z_2 + Z_3 + \dots + Z_n}{n}$$

Където: P – обща вероятност от настъпване на събитието;

S – общо влияние (значимост на събитието);

Nz – обща стойност на непреките загуби;

n- брой на оценките

4.3.5. Определяне на Рейтинга на присъщия риск

Рейтингът на риска се изчислява по следната формула:

$$V = \frac{(P * S) + Nz}{2}$$

Където: P – обща вероятност от настъпване на събитието;

S – общо влияние (значимост на събитието);

Nz – обща стойност на непреките загуби;

V – рейтинг на риска (общ резултат на риска /OPP/).

4.3.6. Определяне на ефективността и адекватността на контрола

Като част от процеса по управление на риска се определят съществуващите механизми за контрол, които могат да ограничават идентифицираните рискове. Оценката на ефективността на контрола по същество представлява оценка и на остатъчния риск, който се дефинира като: „рискът, който остава след предприетия първоначален контрол върху него”, т.е. вземат се предвид съществуването или липсата на контроли или други дейности по управлението му.

Оценката на ефективността на контрола се прави чрез следните 2 показателя:

- **Стойност на риска** - стойността на риска се изчислява по следната формула:

$$I = \frac{(P+S) + \sqrt{Nz}}{3}$$

Където: P – вероятност от настъпване на събитието;

S – влияние (значимост на събитието);

Nz – обща стойност на непреките загуби;

I – стойност на риска.

- **Ефективност на контрола** – Ефективността и адекватността на контрола се определя като отговор на въпроса - До каква степен активно контролирате този риск (каква е възприеманата адекватност и ефективност на дейностите / наличните контроли, които упражнявате)? Стойността на остатъчния риск се определя от адекватността и ефективността на контролите. Колкото по-неадекватни и по-неефективни са контролите, толкова е по-висок остатъчният риск.

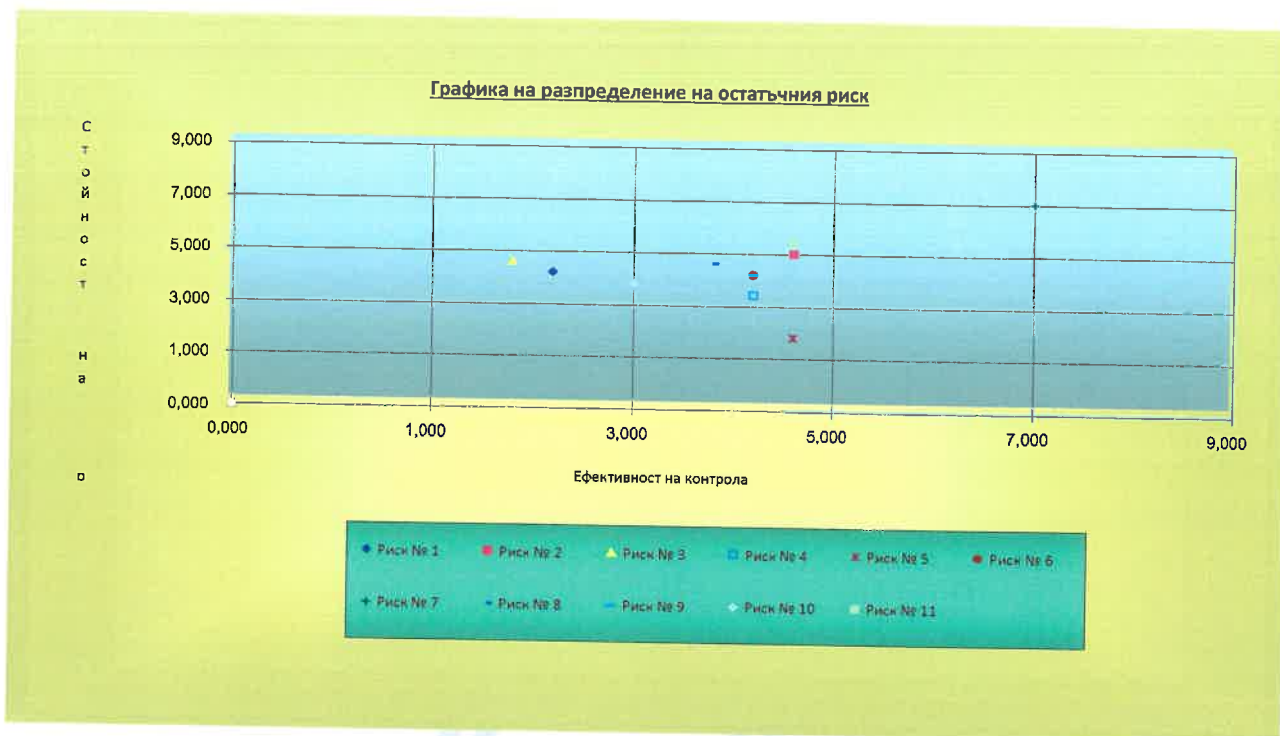
Оценката за Ефективност на контрола се прави според скалата от таблица 6.

Оценка	Описание
1	Трябва да правим много по-малко
3	Трябва да правим по-малко
5	Усилията, които полагаме за този риск, са напълно адекватни
7	Трябва да направим повече
9	Трябва да направим много повече

таблица 6 - Оценка за ефективност на контрола

- Висок риск е този, който се оценява с висока стойност и към който не е приложен адекватен и ефективен контрол.
- Среден риск е този, който е с висока стойност, но са предприети необходимите мерки за ограничаването му чрез въвеждане на адекватни и ефективни контроли или е с ниска стойност, но организацията е изложена на този риск поради липса на ефективни контролни механизми за ограничаването му, като в този случай следва да се анализира общото влияние на всички такива рискове, за да се провери дали те не надвишават риск апетита.
- Нисък риск е този, който има ниска стойност и същевременно са предприети необходимите мерки за ограничаването му чрез въвеждане на ефективни контролни дейности. Следва да се прецени дали да се запази съществуващото ниво на контролни дейности, или да се преразпределят ресурсите, тъй като поради ниска стойност на риска би могъл до голяма степен да се приеме.

Графиката изобразена на фигура 3 по-долу представя резултата от оценката на остатъчния риск по показатели „стойност на риска” и „ефективност на контрола”:



фигура 3 - Графика на разпределение на остатъчния риск

4.3.7. Определяне Рейтинга на остатъчния риск

Рейтингът на остатъчният риск след разглеждането е резултат от умножението на стойността на риска и ефективността на контрола и се нанася в Приложение 6.

$$T = I \cdot C$$

Където: I - стойност на риска;

C – ефективност и адекватност на контрола;

T - Рейтинг (OPR) на остатъчният риск след разглеждането.

4.3.8. Определяне на риск апетит (праг на търпимост)

Определянето на Риск-апетита (прага на търпимост на риска) се извършва чрез поставянето на разграничителна линия между рисковете, които изискват незабавно действие и рискове, които могат да бъдат поставени под наблюдение. Нивото на риск апетита, има директно отношение към реакцията спрямо даден риск, т.е. първо дали организацията ще поеме, прехвърли, избегне или ограничи риска и второ, как и чрез какви дейности ще бъде изразена тази реакция.

Риск-апетитът (праг на търпимост) на ниво остатъчен риск се определя по таблица 7:

ОЦЕНКА (стойност на риска * ефективност на контрола)	РЕЙТИНГ
1-9	ПРИЕМЛИВ
10-54	ИЗИСКВА ВНИМАНИЕ
55-81	НЕПРИЕМЛИВ

таблица 7 - Праг на търпимост на риска

5. Контрол върху риска

5.1. Реакция на риска

След като идентифицираните рискове са оценени и е изчислен техният рейтинг се определя подходящата реакция към всеки от рисковете, която може да бъде:

Ограничаване на риска – Ограничаването на риска представлява намаляване или третиране на риска чрез прилагане на контроли (например чрез законодателството, партньорство и сътрудничество, повишаване на ефикасността на контрола чрез засилване на съществуващите контроли или въвеждането на нови и т.н.) с цел да се намали остатъчният риск. Решението да се ограничи даден риск изисква: адекватен подбор на действията в съответствие с оценката на риска; 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. Рисковете, обект на тази реакция, трябва да се наблюдават периодично.

Прехвърляне на риска - Прехвърляне или споделянето на риска по същество означава да се влезе в партньорство с трета страна, така че той да бъде управляван съвместно. Типични примери за прехвърляне на риска са застраховането, публично-частните партньорства, различни степени на сорсинг споразумения и др. Подобни схеми позволяват достъп до допълнителен ресурс (например контролни дейности или опит и квалификация), като в същото време ограничават възможността от загуба на контрол над дейностите, която е възможна при 100% прехвърляне на трета страна. Председателят на Управителният съвет на АПИ, като цяло, продължава да бъде отговорно лице за управлението на риска в АПИ, независимо от факта, че рискът е прехвърлен или споделен.

Толериране на риска – Приемането или толерирането на даден риск означава, че организацията поема риска без да предприеме конкретни мерки за управлението му. Такова решение означава, че следва периодично да се наблюдава и преоценява риска, за да може при необходимост да бъде избран друг подход за управлението му. Решението да се толерира даден риск трябва да бъде взето имайки предвид оценката на риска, последствията за постигането на целите, риск апетита и правните последици (например решението да не се

предприемат действия може да доведе до по-голям риск). Причините да се толерира даден риск без по-нататъшни действия за управлението му могат да бъдат:

- Действията по ограничаването на риска са свързани със съществени контролни дейности, разходите за които значително надхвърлят ползите;
- Управлението на риска е извън контрола на ръководството и/или неизлагането на риск би могло да означава преустановяване на дейности, които са от ключова важност за организацията.

Прекратяване (избягване) на риска – Избягването на даден риск означава да се прекратят дейностите, свързани с потенциалното му проявление. Подобно решение би могло да означава, че следва да се преразгледат поставените цели и доколкото те са изпълними и съвместими с останалите цели и основни дейности. Трябва да се разгледат и приложимите регулаторни изисквания и ограничения, за да се прецени дали е допустимо дадена дейност да не се извършва или да не се оперира в определена среда. Съществуват 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.

5.1.1. Подбор на действията в съответствие с оценката на преките загуби от риска (фигура 4)



фигура 4 - Класификация на рисковете

Приоритет 1 : Критични рискове- това са рисковете, които притежават и двата фактора, оценени със стойност над или равна на 5. Обикновено това е група рискове, които изискват незабавното внимание и подробно разглеждане на дейностите, свързани с управление на риска. Следва да се предприемат действия за подсилване на дейностите по ограничаване на риска.

Приоритет 2 : Непредвидени рискове- тези рискове трябва да бъдат контролирани преди „системните рискове”, тъй като влиянието им може да бъде значително, въпреки че вероятността да се случат е по-малка отколкото при критичните рискове. За такива рискове обикновено се взимат предпазни мерки (например избухване на пожар). Следва да се изготви план за тестване на съществуващите контроли, за да се постигне увереност, че структурното звено, за което се отнася този риск е добре подготвено за ограничаването му.

Приоритет 3 : Системни рискове- Тези рискове са с голяма вероятност да се случат, но влиянието им е сравнително ниско. За такива рискове обикновено се взимат предпазни мерки. По-скоро трябва да се има предвид ефектът на натрупването (например поредица от малки проблеми с голямо влияние при натрупване или системно нарушение). Следва да се изчисли общото им влияние, за да може при необходимост да се приложат допълнителни мерки за намаляване на остатъчния риск или да се направи план за постоянен мониторинг и периодичен преглед на оценката.

Приоритет 4: Релевантни рискове- Тук се отнасят рисковете, при които и двата фактора са оценени под 5. сновани на нивото рискова допустимост, тези рискове привличат вниманието или не. Това зависи от наличните ресурси и от изискванията на заинтересованите страни. Следва да се анализира възможността за прегрупиране на ресурсите, така че да се пренасочат усилия към по-съществените рискове, без да се компрометира настоящото ниво на управление и контрол.

5.1.2. Разработване на контролни дейности

За рисковете, за които е избрана реакцията „Ограничаване”, т.е. прилагане на контрол, се определя съответната цел на контрола. Целите на контрола могат да бъдат:

Оперативни- насочени към ефективността и ефикасността на оперативните дейности, що се касае до организационната структура, както и до приетите политики и процедури за постигане на планираните резултати и цели.

Съответствие- контроли, които се внедряват, за да осигурят спазване на законите и съответствие с нормативната рамка, спазване на етичните принципи на организацията, съответствие на дейностите с установените правила, спазване на политики и процедури и договори.

Финансови- могат да бъдат свързани с процесите на:

- одобрение;
- осчетоводяване;
- защита на активите;
- съпоставяне на данни.

На базата на избраната реакция на рисковете се определят съответните контролни цели и конкретни контролни дейности, които се вписват в плана за действие (плана за ограничаване въздействието на риска - Приложение 7). Броят и обхватът на контролните

дейности трябва да е достатъчен, за да даде увереност, че съществените рискове са ограничени до приемливи нива.

Контролните дейности могат да бъдат превантивни, отчитащи/откриващи, последващи.

5.1.3. Анализ на разходите и ползите от контрола

За да бъдат разпределени ресурсите и въведени разходно-ефективни контроли, трябва да се предприеме анализ на разходи-ползи за всеки предложен контрол, за да определи кой е задължителен и подходящ при дадените обстоятелства. Анализът разходи-ползи за предложените нови контроли или за подсилени контроли включва както определяне на влиянието от въвеждането на новите или подсилените контроли, така и определяне на влиянието от невъвеждане на контролите.

Анализът на разходите и ползите от контрола има за цел да гарантира, че изразходваните средства за намаляване на риска се изразходват по такъв начин, че да се получи оптимално ниво на безопасност. Ето защо анализът на разходите и ползите от контрола може да помогне да се определят приоритети сред различните мерки за безопасност.

Анализът на ефективността на разходите съдържа следните стъпки:

- Идентификация на всички възможни мерки за безопасност. Този списък трябва да включва всички индивидуални мерки за безопасност, както и комбинации от тях. Причината за това е, че някои комбинации могат да бъдат по-ефективни от сумата на индивидуалната тяхна ефективност. Някои могат да бъдат ефективни само, ако другите са реализирани;
- Оценка на ефективността и разходите на всички мерки за безопасност и смислени комбинации. Ефективността се измерва като намаляване на монетарния риск. Цената включва начални инвестиционни разходи, както и последващите годишни оперативни и разходи за поддръжка;
- Представянето на всички мерки за безопасност и смислени комбинации в риск-разходи диаграма (фигура 5). Всяка мярка за безопасност или комбинацията е представена като една точка, чиято позиция се определя от остатъчната стойност на риска и разхода за контролната мярка;
- Идентифицирането на оптимална крива за намаляване на риска, определена чрез свързване на всички точки, които водят до най-голямото намаляване на риска на всички нива на разходите. Мерките за безопасност, които не са част от оптималната крива за намаляване риска, не са оптимални (или непропорционални), в смисъл, че същото намаление на риска може да се постигне по-ниска цена;
- Оптимална мярка или комбинация от мерки за безопасност е посочена от точката по наклона на кривата, при която съотношението разход / намаление на риска е по-малко от 1. Мерките за безопасност, които се намират от дясната страна на тази точка, изискват разходи (за единица предотвратени щети), които са по-големи от пределния разход.

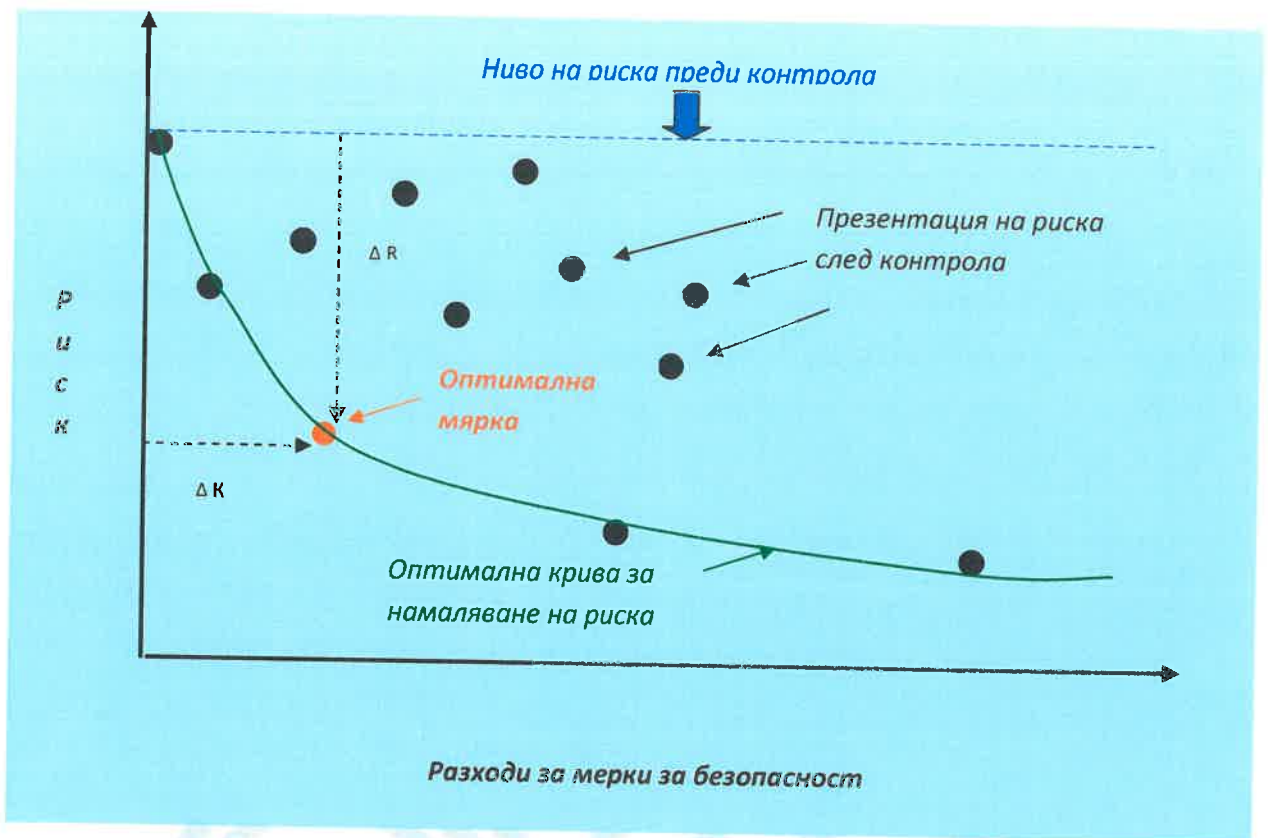
$$OM = \frac{\Delta K}{\Delta R}$$

Където:

OM- Оптимална мярка за безопасност (комбинация от мерки за безопасност)

ΔK - Нарастване на разхода за мярка за безопасност;

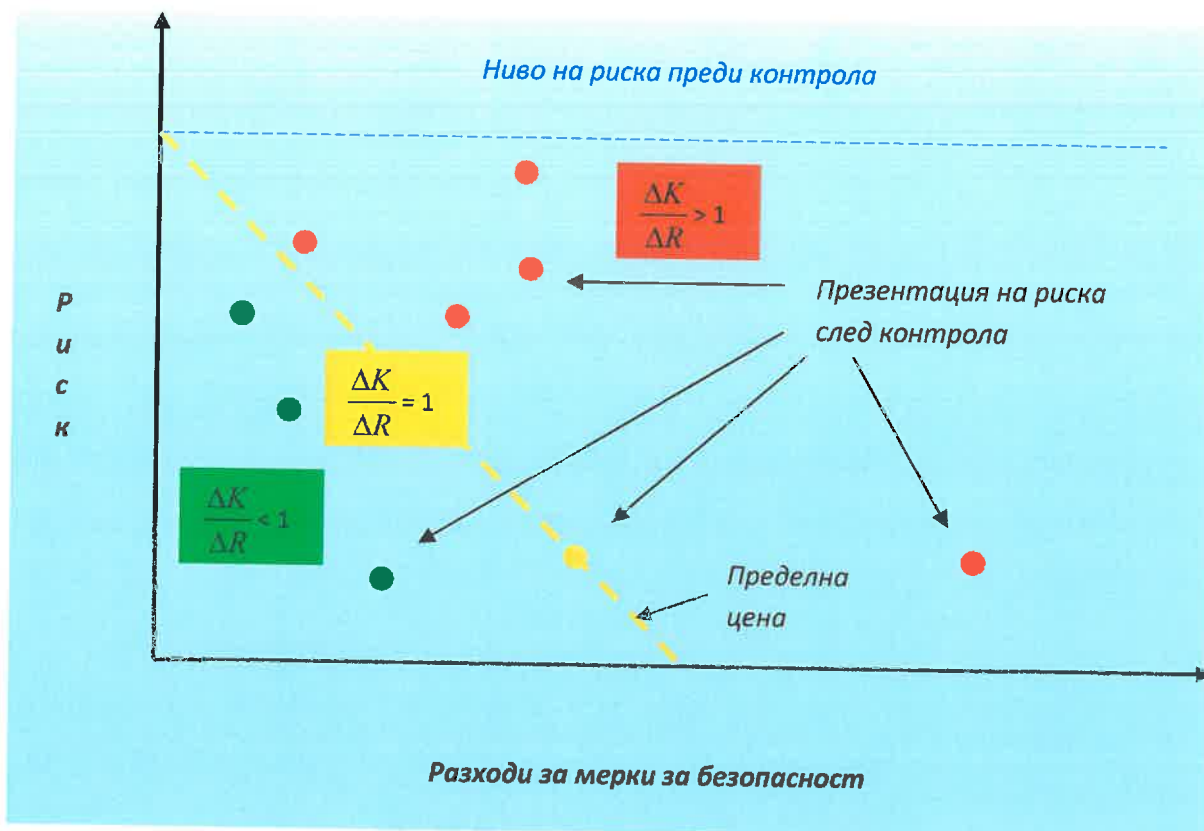
ΔR - Намаление на нивото на риска



фигура 5 - Намаляване на риска и разходите за допълнителни мерки

Пределната цена се изразява в готовността за плащане на определените мерки за намаляване на риска. На база пределната цена се определят какви действия са подходящи или какви мерки вече не са полезни.

Чрез съотношението между стойността на разходите и очакваното намаление на риска се определя рентабилността на мерките за безопасност (фигура 6).



фигура 6 - Диаграма риск-разходи

В зависимост от съотношението риск-разходи мерките за безопасност се класифицират както следва:

- $\frac{\Delta K}{\Delta R} < 1$ - мерките трябва да бъдат изпълнени;
- $1 \leq \frac{\Delta K}{\Delta R} < 2$ - прилагането на мерки трябва да се разглежда за всеки отделен случай;
- $\frac{\Delta K}{\Delta R} > 2$ - изпълнението на мерките не е рентабилно.

5.2. Мониторинг и докладване

След като реакцията за отговор на риска е определена, е необходимо постоянно наблюдение с цел да се гарантира, че тя е въведена и работи успешно. Мониторингът (наблюдението) е може би най-важната стъпка от цялостния процес на управление на риска, тъй като осигурява ранно предупреждение за рисковете, които могат да се сбъднат и материаллизират.

Следните техники трябва да бъдат използвани, с цел да се подпомогне процесът по мониторинг (наблюдение) на рисковете:

- Идентифициране и проследяване на показателите за риска, които могат да действат като системи за ранно предупреждение;

- Преразглеждане статуса на проявление на управляваните рискове в плана за ограничаване влиянието/въздействието на риска.
- Преразглеждат се мерките по ограничаване на риска и при необходимост се въвеждат нови.
- В случай на идентифициране на нов критичен риск или отчитане на проявление на риск, който в Риск-регистъра (Приложение 6) е толериран до този момент, се предприемат действия за ограничаването му в плана за действие.
- Напредъкът по отношение на ограничаването на риска следва да бъде обсъждан на редовни срещи;
- Дирекция АРОК трябва периодично да докладва за прогреса на изпълнение на плана за действие на Председателя на Управителния съвет на Агенция „Пътна инфраструктура”.

Етапът на докладване на резултатите от управлението на риска е от изключителна важност и следва да бъде организиран по начин, по който да се осигури непрекъсваемост на процеса.

Честотата на докладване зависи от оценката на остатъчния риск. Като минимум докладването се прави един път годишно. Нивото, до което се докладват рисковете зависи от естеството на поставената оперативна цел и на рейтинга на риска, пречупен през риск апетита на обектите от КИ.

5.2.1. Форма и съдържание на докладите

Целта на тази методика не е да опише в детайли формата на докладването, а да посочи минималните изисквания по отношение на това какво трябва да се докладва за всеки риск.

Тези минимални изисквания са:

- Ясно описание на риска, включително на контекста на риска;
- Целта, над чието постигане влияе;
- Оценката на влиянието, вероятността, стойността на риска, стойността на непреките загуби, рейтинга и на остатъчния размер на риска;
- Съществуващи контроли за отговор на риска;
- Предложената реакция за намаляване на остатъчния риск с допълнителни действия/контроли;
- Собственик на риска.

6. Документиране на процеса

6.1. Изготвяне на документи по управление на риска

- **Риск- регистър**

Риск-регистърът е документ в установения формат (Приложение 6), който е еднакъв за всеки обект или група обекти с еднакви функции от КИ. Служителите от Дирекция АРОК са ангажирани да попълват риск регистъра за съответния обект/група обекти от КИ.

Идентифицираните рискове се записват и подреждат в низходящ ред по степен на значимост (рейтинг).

В колона „Описание на риска” се попълва индивидуалното разбиране за проявлението на дадения риск в рамките на конкретния обект/група обекти от КИ и евентуални пояснения за причините, които биха могли да предизвикат случването на риска.

След като всеки оценител е оценил, за всеки идентифициран риск, преките загуби по факторите „Влияние” и „Вероятност” (във формуляр по образец Приложение 3) и непреките загуби (във формуляр по образец Приложение 4), индивидуалните оценки се нанасят във Риск-регистъра и Рейтинга на присъщия риск се изчислява автоматично. В случай, че стандартното отклонение на риска е по-малко от 1, се предписват първоначалните контролни мерки за всеки риск чрез съществуващите механизми за контрол, които могат да ограничават идентифицираните рискове. Определят се отговорните лица и срока за изпълнението им. На база предписаните контролни дейности, всички оценители или служители отговорни за управление на риска от Дирекция АРОК /най-малко двама/, оценява ефективността на контрола във формуляр по образец Приложение 5 и оценките се нанасят във Риск-регистъра. Рейтинга на остатъчния риск се изчислява автоматично и предвид величината му, оценителите предписват необходимата реакция на риска в Риск-регистъра.

- **План за действие (план за ограничаване въздействието на риска)**

Целта на плана за действие е да се намали влиянието на рисковете към които АПИ е предприела реакция „Ограничаване на риска”. Рисковете се подреждат в низходящ ред по степен на значимост (рейтинг) и за всеки риск се определя целта на контролната мярка за ограничаването му. За всеки риск се предписват необходимите контролни мерки и се определят отговорните служители и сроковете за докладване и изпълнение.

Служителите отговорни за управлението на риска от Дирекция АРОК разписват план за действие за ограничаване на рисковете за обекта/група обекти от Критичната инфраструктура, като цяло.

Планът за действие има следните характеристики:

- Включва ясно дефинирани индивидуални и групови отговорности;
- Предвижда постижими, реалистични, прецизни и стриктни крайни срокове за изпълнение;
- Мотивира служителите и създава чувство за лична отговорност и „собственост” на риска (т.е. определят се канали за комуникация, дейностите се обсъждат, анализират се мнения, предложения и оценки, за да може всеки включен в процеса да е напълно убеден, че дейностите, включени в плана са най-подходящите и най-добрите);
- Определя и разграничава функциите, свързани с ръководството, изпълнението и надзорна на дейностите, както и линиите на докладване между тях;
- Позволява лесно и обективно проследяване на напредъка, докладване и отчетност, като отбелязва етапи на изпълнение и ключови индикатори за измерване на представянето.

Примерен формат на План за действие (план за ограничаване въздействието на риска) е представен в Приложение 7.

6.2. Поддържане на единна база данни за управление на риска

За да се постигне приемственост в процеса по управление на риска и осведоменост на всички нива служителите отговорни за управление на риска от Дирекция АРОК следва да поддържа единна база данни за управлението на риска, в която да се поддържат следните документи в електронен формат:

- актуалната версия на Методология за оценка на риска на установените критични инфраструктури и обектите им;
- изготвени документи с пряко отношение в процеса по управление на риска (документи, свързани с риск-регистри, планове за действие и др.);
- политики и процедури, свързани с вътрешния контрол;

Директора на Дирекция АРОК следва да определи Администратор на базата данни, както и правила за достъп до информацията, която се поддържа в нея. Базата данни следва да бъде достъпна за служители на АПИ (съгласно определените правила и нива на достъп).

Съгласували:

Инж. Явор Иванов..... 

Директор на Дирекция „Анализ на риска и оперативен контрол”

Изготвили:

инж. Красимир Найденов 

Началник-отдел „Анализ на риска, нередности и предварителен контрол”

и Председател на работна група съгласно Заповед №РД-11-1339/04.11.2019 г.

Илинтин Порязов..... 

*Главен инспектор в отдел „Анализ на риска, нередности и предварителен контрол”,
Дирекция „Анализ на риска и оперативен контрол” и*

Член на работна група съгласно Заповед №РД-11-1339/04.11.2019 г.

05.12.2019 г.