

**ROZKAZ
MINISTRA OBRANY**

ze dne 6. března 2015

ve znění RMO č. 14/2018 Věstníku (1. *novela*)ve znění RMO č. 27/2019 Věstníku (2. *novela*)ve znění RMO č. 50/2020 Věstníku (3. *novela*)**Řízení rizik v rezortu Ministerstva obrany**

K realizaci § 25 odst. 1 písm. b) a odst. 4 zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole), a k zabezpečení jednotného postupu při řízení rizik v rezortu Ministerstva obrany **s t a n o v u j í :**

**ČÁST PRVNÍ
VŠEOBECNÁ USTANOVENÍ****Čl. 1
Předmět úpravy**

Tento rozkaz:

- a) stanovuje proces řízení rizik v rezortu Ministerstva obrany;
- b) vymezuje základní pojmy, práva a povinnosti subjektů v systému řízení rizik a rozsah dokumentace k němu.

**Čl. 2
Základní pojmy**

Pro účely tohoto rozkazu se rozumí:

- a) aktivem – hmotný nebo nehmotný vstup, výstup nebo zdroj nezbytný pro dosahování cílů pomocí procesního a projektového řízení nebo pro plnění úkolu vycházejícího z působnosti organizačního celku rezortu Ministerstva obrany¹⁾;
- b) analýzou aktiva – postup k získávání informací o aktivu a jeho posouzení z hlediska opravitelnosti/nahraditelnosti a citlivosti/dostupnosti;
- c) zranitelností aktiva – slabá stránka daného aktiva, která může být zneužita hrozbou;
- d) hodnocením aktiva – stanovení hodnoty aktiva na základě jeho potřebnosti pro splnění cíle;
- e) kritičností aktiva – hodnota získaná posouzením opravitelnosti/nahraditelnosti a citlivosti/dostupnosti aktiva;
- f) hrozbou – jev nebo událost, které jsou schopny působit vůči aktivu. Mohou být původu přírodního, fyzikálního a dále mohou vznikat v důsledku organizačního nebo společensko-ekonomického faktoru nebo působením lidského faktoru. Z hlediska jejich působení se rozlišují na vnější hrozby, vnitřní hrozby, náhodné hrozby, úmyslné hrozby a neúmyslné hrozby;
- g) identifikací hrozby – postup k získávání informací o existenci hrozby, její schopnosti a záměru/odhodlání způsobit snížení hodnoty, poškození nebo ztrátu aktiva;
- h) rizikem – možnost naplnění hrozby s následnými nežádoucími provozními, finančními, právními a dalšími dopady na dosažení cíle nebo projektu;
- i) identifikací a analýzou rizika – postup, ve kterém se analyzuje působení hrozby na aktivum (zranitelnost aktiva), na jehož základě se identifikuje riziko, stanovuje pravděpodobnost vzniku rizika a popisuje dopad rizika na cíl (projekt). Identifikované riziko je popsáno rizikovým scénářem;

¹⁾ zrušena

- j) hodnocením rizika – postup, ve kterém se riziko posuzuje z pohledu, zda je možné jej akceptovat nebo je třeba toto riziko postoupit do fáze zvládání;
- k) rizikovým scénářem – popis možného působení hrozby na zranitelnost aktiva;
- l) akceptací rizika – rozhodnutí o přijetí výsledné úrovně rizika;
- m) agregací aktiv a rizik – společné posouzení aktiv a rizik dříve odděleně posuzovaných;
- n) zvládáním rizika – postup směřující k vyhnutí, posunutí, přenesení nebo snížení rizika s konečnou akceptací;
- o) sekundárním rizikem – riziko, které vznikne přijetím určitých opatření ke snížení původního rizika;
- p) zbytkovým rizikem – riziko, které zůstává po přijatých opatřeních ke zvládání rizika. Jedná se o riziko, které lze akceptovat nebo k němu ke zvládání přijmout další opatření;
- q) řízením rizik – nepřetržitý proces, v němž subjekty systému řízení rizik na základě svých pravomocí identifikují rizika, navrhuji řešení a přijímají rozhodnutí, jejichž cílem je snížit dopad rizika na plnění cílů (projektů);
- r) zaměstnancem²⁾ – zaměstnanec ve smyslu čl. 1 odst. 3 písm. g) OŘMO č. 61/2019 Věstníku Ministerstva obrany, Organizační řád Ministerstva obrany;
- s) vedoucím zaměstnancem – vedoucí zaměstnanec a představený ve smyslu čl. 1 odst. 3 písm. h) a i) Organizačního řádu Ministerstva obrany;
- t) organizačním celkem rezortu Ministerstva obrany – organizační celek rezortu Ministerstva obrany ve smyslu čl. 2 odst. 1 RMO č. 22/2017 Věstníku Ministerstva obrany *Zásady tvorby organizační struktury a vnitřní systemizace organizačních celků rezortu Ministerstva obrany*, organizační útvar Ministerstva obrany jako služebního úřadu¹⁰⁾ přímo podřízený ministrovi obrany, organizační útvar Vojenského zpravodajství a Úřad pro obrannou standardizaci, katalogizaci a státní ověřování jakosti.

ČÁST DRUHÁ SYSTÉM ŘÍZENÍ RIZIK

Čl. 3

Charakteristika systému řízení rizik

1. Systém řízení rizik je součástí systému řízení a vnitřní kultury v rezortu Ministerstva obrany a obsahuje činnosti uskutečňované při řízení rizik v rámci procesního a projektového řízení. Rizika se v něm identifikují, analyzují a hodnotí ve všech oblastech činnosti rezortu Ministerstva obrany v souladu se zásadami uvedenými v ČSN ISO 31000 Management rizik – principy a směrnice.

2. Systém řízení rizik zahrnuje:

- a) subjekty v systému řízení rizik;
- b) proces řízení rizik;
- c) programové vybavení k podpoře procesu řízení rizik.

Čl. 4

Subjekty v systému řízení rizik

1. Gestor systému řízení rizik je vedoucí zaměstnanec organizačního útvaru Ministerstva obrany, který nese odpovědnost za systém řízení rizik v rezortu Ministerstva obrany podle čl. 44 odst. 2 písm. o) Organizačního řádu Ministerstva obrany. Gestor systému řízení rizik:

a) řídí koordinátora řízení rizik a odpovídá za chod a monitorování systému řízení rizik, jeho organizaci a technickou podporu;

²⁾ zrušena

¹⁰⁾ Nařízení vlády č. 92/2015 Sb., o pravidlech pro organizaci služebního úřadu

b) na základě vlastního vyhodnocení funkčnosti a výkonnosti systému řízení rizik nebo podnětů kontrolních orgánů řeší opatření ke zlepšení jeho nastavení a nápravě zjištěných nedostatků;

c) odpovídá za zabezpečení technického zhodnocení a správu modulu řízení rizik k podpoře procesu řízení rizik (dále jen „Modul“) v programovém vybavení věcného plánování a určuje jeho správce a redaktora³⁾;

d) odpovídá za předávání souhrnných pololetních informací o funkčnosti a výkonnosti systému řízení rizik a o zvládání rizik Radě ministra obrany pro plánování (souběžně s pololetním vyhodnocením cílů) a realizaci jejích návrhů ke změně nastavení systému řízení rizik a k řízení rizik;

e) předkládá státnímu tajemníkovi v Ministerstvu obrany návrh rozsahu vzdělávání zaměstnanců, kteří působí v rámci systému řízení rizik.

2. Věcný gestor vnitřního předpisu¹¹⁾ odpovídá za zapracování problematiky předcházení vzniku a řízení rizik do vnitřního předpisu upravujícího nastavení příslušného vnitřního procesu v rezortu Ministerstva obrany.

3. Manažer cíle⁴⁾ odpovídá za identifikaci všech rizik souvisejících s plněním cíle, zapracování jejich popisu do dokumentace cíle a jejich zvládání. Po identifikaci rizik na své úrovni se stává jejich vlastníkem. Na základě delegace pravomoci k přijetí opatření ke zvládání rizik odpovídá za monitorování vývoje situace při plnění cíle, za hodnocení rizika podle jím stanovených kritérií a za akceptaci rizika, přijímání a realizaci opatření k jejich zvládání. Je oprávněn iniciovat změny v nastavení systému řízení rizik a zapracování problematiky předcházení vzniku a řízení rizik do vnitřních předpisů, které nespádají do jeho působnosti.

4. Vlastník projektu⁵⁾ odpovídá za identifikaci rizik souvisejících s plněním projektu a je vlastníkem rizik. Odpovídá za monitorování vývoje situace při plnění realizace projektu, za hodnocení rizika podle jím stanovených kritérií a za akceptaci rizika, přijímání a realizaci opatření k jejich zvládání.

5. Gestor aktiva je věcný gestor (např. gestor procesu¹²⁾, gestor schopností, služební orgán odpovídající za vojenský obor nebo odbornost¹³⁾, majetkový hospodář¹⁴⁾, gestor služeb¹⁵⁾, gestor rozvoje komunikačních a informačních systémů¹⁶⁾, gestor provozu komunikačních a informačních systémů¹⁷⁾ nebo gestor stanoveného informačního systému¹⁸⁾, který odpovídá za zvládání rizik posunutých vlastníkem rizik do jeho odpovědnosti podle čl. 7 odst. 3 písm. b).

6. Koordinátor řízení rizik je zaměstnanec organizačního útvaru Ministerstva obrany podřízený gestorovi systému řízení rizik, který:

³⁾ Čl. 2 NVMO č. 94/2014 Věstníku Ministerstva obrany *Intranetové stránky v rezortu Ministerstva obrany*

¹¹⁾ Čl. 2 písm. e) RMO č. 1/2017 Věstníku Ministerstva obrany o přípravě návrhů, posuzování a schvalování vnitřních předpisů a Věstníku Ministerstva obrany (o přípravě vnitřních předpisů)

⁴⁾ Čl. 3 odst. 5 RMO č. 66/2012 Věstníku Ministerstva obrany *Plánování činnosti a rozvoje v rezortu Ministerstva obrany*

⁵⁾ Čl. 4 RMO č. 103/2013 Věstníku Ministerstva obrany *Projektové řízení v rezortu Ministerstva obrany*

¹²⁾ Čl. 2 písm. c) RMO č. 33/2016 Věstníku Ministerstva obrany *Správa a rozvoj Procesního modelu rezortu Ministerstva obrany*

¹³⁾ Čl. 7 RMO č. 64/2015 Věstníku Ministerstva obrany *Působnost služebních orgánů v personální práci*

¹⁴⁾ Čl. 3 odst. 20 a 21 RMO č. 48/2013 Věstníku Ministerstva obrany *Hospodaření a nakládání s majetkem v působnosti Ministerstva obrany*

¹⁵⁾ *zrušena*

¹⁶⁾ Čl. 6 RMO č. 52/2015 Věstníku Ministerstva obrany *Centrální řízení informatizace a využívání služeb mezinárodní počítačové sítě Internet v rezortu Ministerstva obrany*

¹⁷⁾ Čl. 7 RMO č. 52/2015 Věstníku Ministerstva obrany

¹⁸⁾ Čl. 8 RMO č. 52/2015 Věstníku Ministerstva obrany

- a) průběžně vyhodnocuje funkčnost a výkonnost systému řízení rizik a připravuje návrhy ke zlepšení jeho nastavení a nápravě zjištěných nedostatků;
- b) posuzuje zapracování problematiky předcházení vzniku a řízení rizik do návrhů vnitřních předpisů upravujících nastavení vnitřních procesů v rezortu Ministerstva obrany;
- c) soustřeďuje katalogy rizik a mapy rizik v rezortu Ministerstva obrany od všech manažerů cílů (vlastníků projektů), ze kterých vytváří katalog rizik a mapu rizik rezortu Ministerstva obrany;
- d) spravuje Modul a přiděluje uživatelům Štábního informačního systému Armády České republiky přístup do Modulu;
- e) zabezpečuje komunikaci se správcem a hodnotiteli rizik a poskytuje jim konzultace;
- f) připravuje analytické a souhrnné informace o rizicích podle pokynů gestora systému řízení rizik.

7. Vlastník rizika je manažer cíle (vlastník projektu) po identifikaci rizika nebo gestor aktiva u rizika, které bylo posunuto do jeho odpovědnosti.

8. Správce rizik je zaměstnanec určený vlastníkem rizik, který na základě podkladů od vlastníků aktiv a hodnotitelů rizik provádí agregaci aktiv a rizik, zpracovává a průběžně vede katalog rizik a mapu rizik v kompetenci vlastníka rizik, informuje vlastníka rizik o vývoji rizik a účinnosti opatření a úkolů k jejich zvládnutí. Správce rizik je jedním z určených hodnotitelů rizik.

9. Hodnotitel rizik je zaměstnanec určený manažerem cíle (vlastníkem projektu). Identifikuje a analyzuje rizika, hodnotí je a navrhuje opatření k jejich zvládnutí. Poskytuje podklady do katalogu rizik a mapy rizik manažera cíle (vlastníka projektu).

10. Vlastník aktiva je zaměstnanec rezortu Ministerstva obrany, který se jím stává na základě definovaných pravomocí a odpovědností za ochranu jemu svěřeného nebo jím užívaného aktiva, které může rozhodujícím způsobem ovlivnit splnění cíle (projektu).

11. Rada ministra obrany pro plánování a odbor interního auditu a inspekce Ministerstva obrany jsou součástí procesu řízení rizik v souladu s vnitřními předpisy určujícími jejich působnost⁶⁾.

12. Subjekty v systému řízení rizik vykonávají definované činnosti v rámci popisu funkční náplně systemizovaného místa.

ČÁST TŘETÍ PROCES ŘÍZENÍ RIZIK

Čl. 5 Fáze procesu řízení rizik

1. Proces řízení rizik se skládá ze tří vzájemně provázaných fází:
 - a) fáze identifikační, analytická a hodnotící;
 - b) fáze zvládnutí rizik;
 - c) fáze monitorovací, komunikační a vykazovací.
2. Vstupem do procesu řízení rizik jsou opatření a úkoly cílů (projektů) a k nim identifikovaná a analyzovaná aktiva a hrozby, které mají vliv na jejich plnění.

⁶⁾ Čl. 3 odst. 1 RMO č. 66/2012 Věstníku Ministerstva obrany; čl. 4 odst. 3 RMO č. 103/2013 Věstníku Ministerstva obrany; RMO č. 8/2006 Věstníku Ministerstva obrany *Interní audit*

3. Výstupem z procesu řízení rizik je souhrn identifikovaných a hodnocených rizik s opatřeními k jejich zvládnutí a přidělených jednotlivým vlastníkům rizik.

Čl. 6

Fáze identifikační, analytická a hodnoticí

1. Identifikační, analytická a hodnoticí fáze se zahajuje identifikací a analýzou aktiv a hrozeb. Postupy pro tuto fázi řízení rizik jsou uvedeny v příloze.

2. Vlastník aktiva identifikuje potenciálně zranitelná aktiva a v součinnosti s hodnotitelem rizik nebo plánovacím orgánem¹⁹⁾ je bezodkladně zaznamenává do seznamu identifikovaných aktiv. Výstupem je identifikace ohroženého aktiva a souvisejících ohrožených opatření a úkolů cílů (projektů).

3. Hodnotitel rizik:

a) v součinnosti s vlastníky aktiv analyzuje bezodkladně zranitelnost identifikovaného aktiva a zaznamenává ohodnocení jeho zranitelnosti do seznamu identifikovaných aktiv. Výstupem je ohodnocení aktiva z pohledu kritičnosti vůči splnění cíle (projektu);

b) identifikuje hrozby a následně analyzuje jejich možné působení na zranitelnost aktiva. Výstupem je ohodnocení hrozby z pohledu kritičnosti působení na zranitelnost aktiva;

c) identifikuje riziko na základě možnosti působení hrozeb na zranitelnost aktiva. Vznik rizika je vyjádřen v rizikovém scénáři;

d) zavádí kartu rizika, do které identifikované riziko zaznamená;

e) po identifikaci rizika určuje míru pravděpodobnosti vzniku rizika a stanovuje míru dopadu rizika. Výstupem je ohodnocení rizika z pohledu kritičnosti dopadu rizika na aktivum a jeho prostřednictvím na cíl (projekt).

4. Míra kritičnosti rizika se stanovuje, jako „kritická“, „vysoká“, „střední“ a „nízká“.

5. Rizika ohodnocená jako „kritická“ a „vysoká“ jsou vstupem pro fázi zvládnutí rizik procesu řízení rizik a správce rizik je dokumentuje v katalogu rizik vlastníka rizik. Rizika ohodnocená jako „střední“ a „nízká“ se přijímají (akceptují) a jsou vstupem pro fázi monitorovací, komunikační a vykazovací procesu řízení rizik.

Čl. 7

Fáze zvládnutí rizik

1. Vstupem do fáze zvládnutí rizik procesu řízení rizik jsou pouze rizika ohodnocená jako „kritická“ a „vysoká“. K těmto rizikům přijímá, na základě návrhů hodnotitele rizik, vlastník rizika bezodkladně rozhodnutí k jejich zvládnutí, stanovuje metody pro jejich zvládnutí a kritéria pro jejich hodnocení. Rozhodnutí spolu se zdůvodněním, metody zvládnutí a kritéria hodnocení hodnotitel rizik zaznamenává do karty rizika.

2. Účelem zvládnutí rizik je zajištění ochrany aktiv proti působení identifikovaných hrozeb a předcházení vzniku škod a ztrát.

3. Vlastník rizik přijímá ke zvládnutí rizika tato rozhodnutí:

a) vyhnout se riziku vypuštěním plánovaných nebo prováděných opatření a úkolů, u kterých není možné jiným opatřením ke zvládnutí rizika zajistit ochranu jejich aktiv před působením hrozby;

b) posunutí rizika v případě, že nemá dostatečné kompetence k zvládnutí rizika a odpovědnost za zvládnutí rizika, postoupením věcně příslušnému gestorovi aktiva nebo

¹⁹⁾ Čl. 3 odst. 8 RMO č. 66/2012 Věstníku Ministerstva obrany a NVMO č. 50/2016 Věstníku Ministerstva obrany *Zpracování a aktualizace plánů činnosti v rezortu Ministerstva obrany*

nadřazenému manažerovi cíle, který přijme bezodkladně rozhodnutí o převzetí odpovědnosti za posunutí rizika a vlastní rozhodnutí ke zvládnutí tohoto rizika;

c) přenesení rizika předáním rizika třetí straně (mimo rezort Ministerstva obrany), přičemž odpovědnost za jejich řízení mu zůstává;

d) snížení rizika stanovením konkrétních opatření a úkolů (včetně jejich prioritizace a očekávané účinnosti) ke zvládnutí daného rizika, která se mohou realizovat buď v průběhu dosahování cíle (projektu), nebo v případě, že riziko nastane (jedná se o nejběžnější formu zvládnutí rizika);

e) přijetí (akceptace) rizika v případě, že nejsou stanovena opatření ke zvládnutí rizik.

4. Pokud gestor aktiva nesouhlasí s posunutím rizika podle odstavce 3 písm. b) do jeho odpovědnosti, vzniká rozpor. Rozpor bezprostředně vypořádávají vedoucí zaměstnanci přímo podřízení ministrově obrany, kteří jsou nadřizení vlastníkově rizika a gestorovi aktiva. Nedojde-li k vypořádání vzniklého rozporu, předloží rozpor po projednání v Radě ministra obrany pro plánování ke konečnému rozhodnutí ministru obrany gestor systému řízení rizik, který ke vzniklému rozporu vypracuje své stanovisko.

5. Výstupem z této fáze jsou opatření a úkoly ke zvládnutí rizik zapracovaná do ročního plánu rezortu Ministerstva obrany a akceptovaná rizika.

Čl. 8

Fáze monitorovací, komunikační a vykazovací

1. Vstupem do fáze monitorovací, komunikační a vykazovací jsou dokumentovaná aktiva, hrozby a rizika a rozhodnutí přijatá k jejich zvládnutí.

2. Vlastník rizika odpovídá za monitorování rizik. Hodnotitel rizik v součinnosti s vlastníkem aktiva sleduje a analyzuje vývoj aktiv, hrozeb a rizik, realizaci a účinnost opatření a úkolů ke zvládnutí rizik. V průběhu monitorování zjišťuje, analyzuje a ohodnocuje nová a sekundární rizika, která se při plnění cíle (projektu) mohou objevit, aktualizuje stávající a zbytková rizika a navrhuje vlastníkově rizik další opatření k jejich zvládnutí.

3. Subjekty systému řízení rizik jsou povinny navzájem komunikovat a poskytovat si účelné, jednoduché a rychlé informace v elektronické podobě. Vlastník rizik stanovuje správci rizik způsob a četnost informování o vývoji rizik a účinnosti opatření a úkolů k jejich zvládnutí.

4. Vlastník rizika při vykazování odpovídá za hodnocení účinnosti uskutečňovaných opatření a úkolů ke zvládnutí rizik, k tomu provádí opakované shromažďování, třídění, analýzu a vyhodnocování jejich efektivnosti.

5. Výstupem z této fáze je souhrn informací k poskytování údajů pro řízení a hodnocení rizik.

Čl. 9

Agregace aktiv a rizik

1. Agregace aktiv a rizik je specifickou činností procesu řízení rizik, pomocí které se identifikují rizika u manažera cíle, nadřazeného manažera cíle nebo u gestora aktiva (dále jen „odpovědný manažer“).

2. Vstupem k zahájení agregace jsou aktiva, která se mohou vyskytovat u více podřízených vlastníků aktiv nebo kritická aktiva posunutá podle čl. 7 odst. 3 písm. b). Podle společných rysů je správce rizik posuzuje a formuluje jako společné kritické aktivum. Výstupem jsou nově formulovaná agregovaná kritická aktiva.

3. U agregovaných kritických aktiv hodnotitel rizik nově vyhodnotí rizika, jejichž vlastníkem se stává odpovědný manažer.

4. Určení míry kritičnosti rizika agregovaného aktiva probíhá podle postupu uvedeného v příloze.

5. Rizika agregovaného aktiva mírou rizika „kritické“ a „vysoké“ jsou vstupem pro fázi zvládnání rizik procesu řízení rizik realizované odpovědným manažerem. Rizika agregovaného aktiva s mírou rizika „střední“ a „nízká“ se přijímají (akceptují) a jsou vstupem pro fázi monitorovací, komunikační a vykazovací procesu řízení rizik.

Čl. 10 Vyhodnocování rizik

1. Vyhodnocování rizik je součástí jejich monitorování a průběžného hodnocení plnění opatření a úkolů²⁰⁾. Rizika souhrnně vyhodnocují vlastníci rizik v hodnoticích dokumentech rezortu Ministerstva obrany.

2. Souhrnné vyhodnocování rizik se uskutečňuje:

- a) v rámci vyhodnocení ročního plánu rezortu Ministerstva obrany⁷⁾;
- b) v intervalech na základě rozhodnutí vlastníka rizika;
- c) v rámci fáze ukončení projektu⁸⁾.

ČÁST ČTVRTÁ DOKUMENTY SYSTÉMU ŘÍZENÍ RIZIK

Čl. 11 Zpracovávání dokumenty

1. V rámci systému řízení rizik se zpracovávají tyto dokumenty:

- a) seznam identifikovaných aktiv;
- b) seznam kritických aktiv a hrozeb;
- c) karta rizika;
- d) katalog rizik;
- e) mapa rizik.

2. Dokumenty systému řízení rizik se zpracovávají, vedou a ukládají v elektronické podobě v Modulu.

Čl. 12 Seznam identifikovaných aktiv

Hodnotitel rizik vytváří dokument v součinnosti s vlastníky aktiv ve fázi identifikační, analytické a hodnotící procesu řízení rizik. Do dokumentu zaznamenává identifikovaná, analyzovaná a hodnocená aktiva a jejich vlastnosti z pohledu kritičnosti vůči splnění cíle (projektu).

Čl. 13 Seznam kritických aktiv a hrozeb

²⁰⁾ Čl. 6 NVMO č. 49/2016 Věstníku Ministerstva obrany *Vyhodnocení činnosti v rezortu Ministerstva obrany*

⁷⁾ Čl. 18 RMO č. 66/2012 Věstníku Ministerstva obrany a čl. 9 NVMO č. 49/2016 Věstníku Ministerstva obrany

⁸⁾ Čl. 10 NVMO č. 44/2014 Věstníku Ministerstva obrany *Pravidla projektového řízení v rezortu Ministerstva obrany*

Hodnotitel rizik vytváří dokument ve fázi identifikační, analytické a hodnoticí procesu řízení rizik. Do dokumentu zaznamenává identifikovaná kritická aktiva a identifikované hrozby, které mohou působit na tato aktiva, a informace o jejich vlastnostech získaných z analýzy nebo modelování.

Čl. 14 Karta rizika

1. Hodnotitel rizik zpracovává kartu rizika pro každé kritické aktivum samostatně. Do dokumentu zaznamenává údaje o kritickém aktivu, souvisejících hrozbách, riziku a jejich změnách. V procesu plánování je karta rizika součástí dokumentace cíle, v projektu je součástí plánu řízení projektových rizik²¹⁾.

2. Karta rizika obsahuje zejména:

- a) údaje o kritickém aktivu;
- b) seznam ovlivňovaných cílů (projektů), opatření a úkolů;
- c) seznam souvisejících kritických aktiv s parametry hodnocení (v případě agregace);
- d) seznam souvisejících identifikovaných hrozeb s parametry hodnocení;
- e) charakter rizika a rizikový scénář;
- f) ohodnocení rizika;
- g) přístup ke zvládnutí rizika;
- h) seznam opatření ke zvládnutí rizika;
- i) vlastníka kritického aktiva a rizika.

Čl. 15 Katalog rizik

1. Vlastník rizika a koordinátor řízení rizik zpracovává katalog rizik, který je přehledem o „vysokých“ a „kritických“ rizicích. Údaje do katalogu rizik se přenášejí z karty rizika.

2. V katalogu rizik se zobrazují zejména:

- a) číslo a název cíle (projektu);
- b) název kritického aktiva s parametry jeho hodnocení;
- c) charakter a ohodnocení rizika;
- d) přístup ke zvládnutí rizika;
- e) seznam opatření ke zvládnutí rizika;
- f) vlastník kritického aktiva a rizika.

Čl. 16 Mapa rizik

Vlastník rizika a koordinátor řízení rizik vytváří grafickou mapu rizik generovanou z hodnot katalogu rizik jako jeho doplňující informaci.

ČÁST PÁTÁ ZÁVĚREČNÁ USTANOVENÍ

Čl. 17 Řízení rizik u Vojenského zpravodajství

1. Řízení rizik bude prováděno v souladu s tímto rozkazem a upraveno vnitřním předpisem ředitele Vojenského zpravodajství.

²¹⁾ Čl. 8 odst. 12 NVMO č. 44/2014 Věstníku Ministerstva obrany

2. Dokumenty vedené v souladu s tímto rozkazem budou trvale uloženy u ředitele Vojenského zpravodajství a vedeny využívány v souladu s právními předpisy⁹⁾.

Čl. 18

Tento rozkaz nabývá účinnosti **dnem vyhlášení** ve Věstníku Ministerstva obrany.

Čj. 84-4/2015-SPráv MO

Martin S T R O P N I C K Ý

v zastoupení

Ing. Jiří B O R O V Ě C , MBA v. r.

⁹⁾ Např. zákon č. 289/2005 Sb., o Vojenském zpravodajství, ve znění pozdějších předpisů; zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů; příloha č. 18 nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací, ve znění nařízení vlády č. 240/2008 Sb.

IDENTIFIKACE, ANALÝZA A HODNOCENÍ RIZIK

Čl. 1

Analýza aktiv

1. Aktivum se analyzuje z pohledu:
 - a) opravitelnosti – vyjadřuje náročnost opravy aktiva do původního stavu;
 - b) nahraditelnosti – vyjadřuje složitost získání nového aktiva z důvodu jeho nefunkčnosti;
 - c) citlivosti – vyjadřuje, zda se jedná o aktivum veřejné, pro služební potřebu nebo utajované;
 - d) dostupnosti – vyjadřuje vlastnost přístupnosti a použitelnosti aktiva.
2. Kritičnost aktiva pro splnění cíle se stanovuje pomocí číselných hodnot parametrů „opravitelnost/nahraditelnost“ a „citlivost/dostupnost“.
3. Pro parametr „opravitelnost/nahraditelnost“ se kritičnost aktiva hodnotí jako:
 - a) nízká (hodnota 1), je-li možné jej s přiměřeným úsilím nahradit nebo opravit;
 - b) střední (hodnota 2), je-li možné jej velmi obtížně, s vysokým úsilím a na úkor jiných úkolů nahradit nebo opravit;
 - c) vysoká (hodnota 3), je-li téměř nemožné a nerealizovatelné dané aktivum nahradit nebo opravit;
 - d) kritická (hodnota 4), není-li možné a realizovatelné aktivum nahradit nebo opravit.
4. Pro parametr „citlivost/dostupnost“ se kritičnost aktiva hodnotí jako:
 - a) nízká (hodnota 1), je-li aktivum dostupné;
 - b) střední (hodnota 2), je-li dostupnost aktiva částečně omezena;
 - c) vysoká (hodnota 3), je-li dostupnost aktiva omezena ve větším rozsahu;
 - d) kritická (hodnota 4), jedná-li se o nedostupné aktivum.

Čl. 2

Míra kritičnosti aktiva

1. Ke stanovení míry kritičnosti aktiva se využívá součin hodnot parametrů „opravitelnost/nahraditelnost“ a „citlivost/dostupnost“ (čl. 1 odst. 3 a 4 přílohy). Při součinu hodnot parametrů v rozpětí 6 až 16 se jedná o „kritické aktivum“. Při součinu hodnot parametrů v rozpětí 1 až 4 se jedná o „nekritické“ aktivum.
2. Míra kritičnosti aktiva se zaznamenává do seznamu identifikovaných aktiv.
3. V dalších fázích procesu řízení rizik se aktiva s mírou kritičnosti „kritická“ dále hodnotí a aktiva s mírou kritičnosti „nekritická“ se pouze monitorují.

Čl. 3

Identifikace a analýza hrozeb

1. K následné identifikaci rizik se vybírají hrozby, které mohou působit na zranitelnost konkrétního kritického aktiva.
2. Výrazným faktorem k identifikaci hrozeb jsou zkušenosti z předchozích období, průzkumy, předchozí analýzy, výsledky modelování apod.
3. Analýza hrozby se uskutečňuje stanovením číselné hodnoty parametrů „míra intenzity vlivu hrozby“ na zranitelnost aktiva a „míra odhodlání/záměru hrozby“ realizovat svůj vliv na zranitelnost aktiva.

4. Míra intenzity vlivu hrozby na zranitelnost aktiva vyjadřuje schopnost hrozby mít vliv na aktivum. Na základě dostupných informací a zkušeností z dřívějšího výskytu hrozeb se hodnota parametru „míra intenzity vlivu hrozby“ stanovuje jako:

- a) nízká (hodnota 1), jestliže nehrozí poškození aktiva;
- b) střední (hodnota 2), jestliže hrozí poškození aktiva, ale nehrozí narušení rozsahu nebo doby realizace cíle (projektu) v případě nutnosti zpětného získání aktiva;
- c) vysoká (hodnota 3), jestliže hrozí poškození aktiva a narušení rozsahu nebo doby realizace cíle (projektu) v případě nutnosti zpětného získání aktiva;
- d) kritická (hodnota 4), jestliže naplnění hrozby zapříčiní nevratné a neopravitelné poškození aktiva.

5. Míra odhodlání/záměru hrozby vyjadřuje zájem realizovat svůj vliv na aktivum. Na základě dostupných informací a zkušeností z dřívějšího výskytu hrozeb se hodnota parametru „míra odhodlání/záměru hrozby“ stanovuje jako:

- a) nízká (hodnota 1), jestliže se v předchozím období hrozba neobjevila a nejsou indicie jejího výskytu v dalším období;
- b) střední (hodnota 2), jestliže je působení na zranitelnost aktiva předvídatelné a v předchozím období se hrozba objevila;
- c) vysoká (hodnota 3), jestliže lze očekávat časté působení hrozby na aktivum a v předchozím období se hrozba objevila;
- d) kritická (hodnota 4), jestliže lze očekávat velmi častou frekvenci působení hrozby na zranitelnost aktiva.

Čl. 4

Míra kritičnosti hrozby

41. Ke stanovení hodnoty míry kritičnosti hrozby se využívá součin hodnot parametrů hrozby, tj. míry intenzity vlivu hrozby na zranitelnost aktiva a míry odhodlání/záměru hrozby (čl. 3 odst. 4 a 5 přílohy). Při součinu hodnot parametrů v rozpětí 6 až 16 se jedná o „kritickou hrozbu“. Při součinu hodnot parametrů v rozpětí 1 až 4 se jedná o „nekritickou“ hrozbu.

52. Míra kritičnosti hrozby se zaznamenává do seznamu kritických aktiv a hrozeb.

Čl. 5

Míra kritičnosti rizika

1. Ke stanovení hodnoty míry kritičnosti rizika se využívá součin hodnoty míry kritičnosti aktiva (čl. 2 přílohy) a hodnoty míry kritičnosti hrozby (čl. 4 přílohy).

2. Míra kritičnosti rizika je:

- a) „kritická“, je-li hodnota součinu v intervalu větší než 144 a menší nebo rovno 256;
- b) „vysoká“, je-li hodnota součinu v intervalu větší než 36 a menší nebo rovno 144;
- c) „střední“, je-li hodnota součinu v intervalu větší než 16 a menší nebo rovno 36;
- d) „nízká“, je-li hodnota součinu v intervalu menší nebo rovno 16.

3. Míra kritičnosti rizika se zaznamenává do karty rizika.

Čl. 6

Úroveň přijatelného rizika

1. Přijatelným (akceptovatelným) rizikem je riziko, jehož hodnota míry kritičnosti rizika je rovna nebo menší 36, tj. „střední“ a „nízké“ riziko.

2. Nepřijatelným (neakceptovatelným) rizikem je riziko, jehož hodnota míry kritičnosti rizika je větší než 36, tj. „vysoké“ nebo „kritické“ riziko. U těchto rizik se přijímají rozhodnutí o způsobu jejich zvládnutí a opatření k jejich zvládnutí, které se zaznamenávají do karty rizika.