Deloitte.

Metodika zajištění ochrany kritické infrastruktury v oblasti výroby, přenosu a distribuce elektrické energie

24. 10. 2012

Obsah

1 Základní ustanovení

1.1 Popis metodiky

Metodika zajištění ochrany kritické infrastruktury (KI) v oblasti výroby, přenosu a distribuce elektrické energie specifikuje postup tvorby a zdokonalování systému řízení ochrany vybrané oblasti kritické infrastruktury. Přínos metodiky je vnímán ve vztahu k potřebě zvyšování bezpečnosti a odolnosti dodávky elektrické energie za účelem udržení funkční kontinuity výroby, přenosu a distribuce elektrické energie.

1.2 Cíle Metodiky

Cílem metodiky je podpora tvorby a zlepšování systému řízení ochrany vybrané oblasti kritické infrastruktury. Metodika je určená subjektům kritické infrastruktury pro využití v praxi. Předmětem systému řízení jsou oblasti bezpečnosti, které reflektují jednak analýzu rizik, která byla v rámci procesu tvorby metodiky realizována, tak i výsledky a výstupy vyplývající z pilotního provozu a ověření systému řízení ochrany na vybrané lokalitě. Součástí metodiky jsou standardy vytvořené a ověřené pro:

- zajištění fyzické bezpečnosti kritické infrastruktury v oblasti, výroby, přenosu a distribuce elektrické energie,
- zajištění bezpečnosti informací v informačních systémech podporujících oblasti výroby, přenosu a distribuce elektrické energie,
- zajištění administrativní a personální bezpečnosti,
- zajištění krizového řízení společnosti subjektu kritické infrastruktury.

Vytvořená metodika zajištění ochrany kritické infrastruktury v oblasti výroby přenosu a distribuce elektrické energie je koncipována jako metodický postup tvorby komplexního systému řízení ochrany v rámci vybrané oblasti kritické infrastruktury, který na základě konzultací s odpovědnými orgány státní správy a subjekty kritické infrastruktury a provedené syntézy rizikovosti, umožnil stanovit konkrétní oblasti bezpečnosti a následně pro tyto oblasti definovat strukturální a kvalitativní požadavky dle všeobecně uznávaných standardů bezpečnosti. Dokument lze vnímat jako základní sadu požadavků na systém řízení ochrany kritické infrastruktury v rámci zvolených oblastí bezpečnosti.

Metodický postup stanovuje obecné strukturální požadavky pro jednotlivé oblasti bezpečnosti (fyzická, informační, administrativní, personální bezpečnost, krizové řízení a plánování) a požadavky na strukturu systému řízení ochrany kritické infrastruktury, které mají zásadní vliv na míru rizika a zranitelnosti v rámci vybrané oblasti kritické infrastruktury.

Zobecnění je použito z důvodu vytvoření manipulačního prostoru pro individualizaci potřeb či filozofie bezpečnosti a řízení ochrany ve vztahu k subjektům kritické infrastruktury. Tak, jak již bylo zmíněno, vytvořený metodický postup je primárně určen pro subjekty kritické infrastruktury. Předpokládá se, že subjekty budou tento dokument považovat za rámec pro podporu procesu tvorby a zdokonalování základní a operativní části plánu krizové připravenosti subjektu kritické infrastruktury, který má umožnit vytvoření komplexního systému řízení ochrany kritické infrastruktury v dané oblasti.

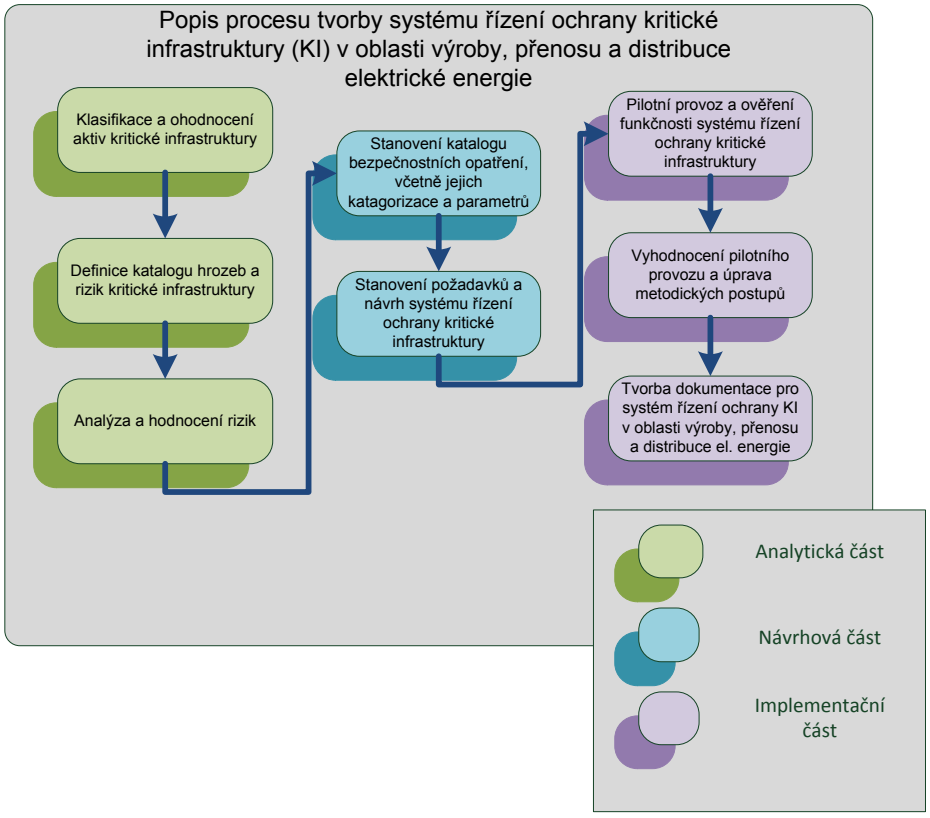
Příklad standardu/best practice pro jednotlivé části a oblasti systému řízení ochrany kritické infrastruktury v oblasti výroby, přenosu a distribuce elektrické energie jako uceleného metodického postupu je součástí přílohové části metodiky.

2 Popis metodického postupu tvorby systému řízení ochrany

Pro optimalizaci procesu a postupu tvorby systému ochrany kritické infrastruktury ve vybrané oblasti je stanoven obecný popis jednotlivých procesních kroků.

1. klasifikace a ohodnocení aktiv kritické infrastruktury z oblasti výroby, přenosu a distribuce elektrické energie,
2. definice katalogu hrozeb a rizik kritické infrastruktury z oblasti výroby, přenosu a distribuce elektrické energie,
3. analýza a hodnocení rizik z oblasti výroby, přenosu a distribuce elektrické energie,
4. stanovení katalogu bezpečnostních opatření, včetně jejich kategorizace a parametrů,
5. stanovení požadavků a návrh systému řízení ochrany kritické infrastruktury z oblasti výroby, přenosu a distribuce elektrické energie,
6. pilotní provoz a ověření funkčnosti systému řízení ochrany kritické infrastruktury na vybrané lokalitě,
7. vyhodnocení pilotního provozu a úprava metodických postupů,
8. tvorba dokumentace pro systém řízení ochrany kritické infrastruktury v oblasti výroby, přenosu a distribuce elektrické energie.

Pro detailnější představu logického členění procesu realizace a tvorby systému řízení kritické infrastruktury v oblasti výroby, přenosu a distribuce elektrické energie byl vytvořen následující diagram (obr. 1).



Obrázek 1 - Popis procesu tvorby systému řízení ochrany

2.1 Seznam zkratek

Tabulka zkratek
BOZP – bezpečnost a ochrana zdraví při práci
BP – bezpečnostní pracovník SBS
BT – bezpečnostní třída
CCTV – uzavřený televizní okruh / kamerový systém (ČSN EN 50132)
DTS – detektor tříštění skla
FO – fyzická ochrana
FOS – fyzická ostraha
CHP – chráněný prostor - prostor s důležitými místy, kde se však nepředpokládá s přítomnosti zařízení ovlivňujícím základní funkci prvku kritické infrastruktury s požadavky na střední úroveň zabezpečení
Incident – je jakákoliv obecná událost, která má za následek ztrátu či poškození aktiv společnosti s dopadem na kontinuitu procesů.
KI – kritická infrastruktura
KP – krizový plán
KPO – krizový plán organizace
KPR - kontrolovaný prostor - představuje prostor mezi důležitými místy (klíčovými místy) objektu s požadavky na nižší úroveň zabezpečení,
KŘ – krizové řízení
KŘO – krizové řízení organizace
LOP – lokalita (areál), objekt (budova) prostor
MK – magnetický kontakt
MS/KS – mimořádný stav/ krizová situace
MZP – mechanické zábranné prostředky
PCO – pult centralizované ochrany
PDS – perimetrický detekční systém
PIR – pasivní infračervený detektor pohybu
PKI – public key infrastructure (infrastruktura veřejných klíčů)
PKP – plán krizové připravenosti
PKPSKI – plán krizové připravenosti subjektu kritické infrastruktury
PPSZ – poplachový přenosový systém (ČSN EN 50136)
PZTS – poplachový zabezpečovací a tísňový systém (ČSN EN 50131)
PZS – poplachový zabezpečovací systém (ČSN EN 50131)
RO – režimová ochrana (opatření)
SBS – soukromá bezpečnostní služba
SKV – systém kontroly vstupů (ČSN EN 50133)
SŘO - systém řízení ochrany ve smyslu tohoto dokumentu (Systém řízení ochrany kritické infrastruktury z oblasti výroby, přenosu a distribuce elektrické energie)
STO – systém technické ochrany
ZCHP – zvláště chráněný prostor - prostor s přítomností klíčových technologických zařízení, popřípadě prostor, v kterém se pracovníky daného objektu vykonávají klíčové pracovní činnosti z pohledu základních funkcí prvku kritické infrastruktury s požadavky na nevyšší úroveň zabezpečení

3 Analytická část postupu tvorby systému řízení ochrany

3.1 Kategorizace a klasifikace aktiv

V souvislosti s procesem realizace analýzy a hodnocení rizik byla definována a kategorizována aktiva pro vybranou oblast kritické infrastruktury a to v rozsahu znění zákona č. 240/2000 Sb. o krizovém řízení a o změně některých zákonů (krizový zákon) a nařízení vlády č. 432/2010 Sb. o kritériích pro určení prvku kritické infrastruktury. Ve vztahu k zmiňovaným legislativním normám lze uvažovat o následujících skupinách aktiv v oblasti výroby, přenosu a distribuce elektrické energie:

Skupiny aktiv v oblasti výroby, přenosu a distribuce el. energie	
Tepelné elektrárny a teplárny	Budova dispečinku
Vodní elektrárny	Vedení
Elektrické stanice	

Tabulka 1 - Skupiny aktiv v oblasti výroby, přenosu a distribuce elektrické energie

3.2 Metodické postupy hodnocení rizik

Návrh a optimalizace systému řízení ochrany vybrané oblasti kritické infrastruktury je podmíněno procesem definice katalogu hrozeb, analýzy a hodnocení rizik a výběrem relevantní metodiky. Vzhledem ke skutečnosti, že je tento proces považován za nezbytný, následující část metodiky popisuje vybrané přístupy k analýze a hodnocení rizik, využitelné a využívané pro oblast výroby, přenosu a distribuce elektrické energie. Příklad katalogu hrozeb pro vybranou oblast kritické infrastruktury je součástí přílohové dokumentace 6.1.

3.2.1 Analýza rizik pro definovanou oblast aktiv

Následující metodika hodnocení rizik je semi-kvantitativním přístupem, který pracuje s třemi složkami rizika (Aktivum, Hrozba, Zranitelnost), kde:

Aktivum	– část hodnoceného systému či jeho dat, která mají pro společnost hodnotu,
Hrozba	– jakákoliv aktivita využívající úmyslně či neúmyslně zranitelnosti s negativním dopadem na důvěrnost, dostupnost a integritu aktiv a která je vyjádřena pravděpodobností výskytu hrozby,
Zranitelnost	– vyjádření slabého místa aktiva nebo skupiny aktiv, které za určitého předpokladu bude využito hrozbou s následkem poškození nebo ztráty aktiv a případných procesů/funkcí, které tyto aktiva podporují.

3.2.1.1 Hodnocení aktiva pro proces analýzy rizik

Důležitým procesním úkonem při analýze rizik je vyjádření hodnoty aktiva, které v kontextu s realizovanou analýzou rizik v předmětné oblasti bude mít semi-kvantitativní charakter.

Bodová hodnota pro vyjádření důležitosti aktiva	
0	Žádná nebo nehodnocena
1	Nízká
2	Málo významná
3	Střední
4	Vysoká
5	Velmi vysoká

Tabulka 2 - Bodová hodnota důležitosti aktiva

3.2.1.2 Hodnocení hrozby pro proces analýzy rizik

Hodnocení významu hrozby je realizováno pomocí vyjádření míry pravděpodobnosti výskytu hrozby v případě konkrétního aktiva či skupiny aktiv.

Bodová hodnota pro vyjádření pravděpodobnosti výskytu hrozby	
0	Nepravděpodobná nebo nehodnocená
1	Velmi málo pravděpodobná
2	Málo pravděpodobná
3	Středně pravděpodobná
4	Značně pravděpodobná
5	Vysoce pravděpodobná až jistá

Tabulka 3 - Bodová hodnota pravděpodobnosti výskytu hrozby

3.2.1.3 Hodnocení zranitelnosti pro proces analýzy rizik

Míra zranitelnosti je podobně jako předešlé složky rizika hodnocena na bodové škále pro vyjádření expertního odhadu míry zranitelnosti vybraného aktiva.

Bodová hodnota míry zranitelnosti aktiva	
0	Žádná
1	Nízká
2	Málo významná
3	Střední
4	Vysoká
5	Velmi vysoká

Tabulka 4 - Bodová hodnota míry zranitelnosti aktiva

Pro názornost uvádíme souhrnnou tabulku škály hodnocení jednotlivých složek rizika:

Bodová hodnota	Hodnota aktiva	Velikost hrozby	Míra zranitelnosti
0	Žádná nebo nehodnocena	Nepravděpodobná nebo nehodnocená	Žádná
1	Nízká	Velmi málo pravděpodobná	Nízká
2	Málo významná	Málo pravděpodobná	Málo významná
3	Střední	Středně pravděpodobná	Střední
4	Vysoká	Značně pravděpodobná	Vysoká
5	Velmi vysoká	Vysoce pravděpodobná až jistá	Velmi vysoká

Tabulka 5 - Hodnocení složek rizika

3.2.1.4 Analýza – hodnocení rizika

Pro finalizaci procesu hodnocení rizika ve vztahu k vybrané oblasti kritické infrastruktury byl definován vztah:

$$R = A \times H \times Z$$

Kde:

R – Riziko
A – Aktivum
H – Hrozba
Z – Zranitelnost

Po stanovení hodnoty jednotlivých složek rizika je možné kvantifikovat riziko a jeho výslednou hodnotu rozdělit do skupin vyjadřujících zvyšující se míru rizika. Pro vyjádření míry rizika jsou stanoveny následující kategorie:

Výsledné riziko	Bodová hodnota
Nízké	1 – 40
Střední	41 – 70
Vysoké	71 – 125

Tabulka 6 - Klasifikace rizika podle celkové bodové hodnoty

Příklad praktického využití této metodiky je součásti přílohy 6.2.

3.2.2 Kvalitativní analýza rizik s využitím jejích souvztažnosti

Pro další proces stanovení závislosti analýzy rizik a struktury systému řízení ochrany vybrané oblasti kritické infrastruktury je potřeba vyjádřit i vzájemnou vazbu mezi identifikovanými riziky. Pro tento účel je použita metodika KARS - kvantitativní analýza rizik s využitím jejich souvztažnosti. Význam této metody je zejména v souvislosti s diverzifikací rizika na základě míry aktivity a pasivity rizika ve vztahu k jiným rizikům (zda vybrané riziko má potenciál způsobit vznik jiného rizika či zda může být způsobeno jinými riziky – domino efekt).

Samotný proces realizace „KARS“ analýzy je vícestupňový, přičemž v prvním kroku se stanoví soupis rizik, který je pro danou oblast (oblast výroby, přenosu a distribuce elektrické energie) specifický. V dalším kroku realizace analýzy je provedeno vyjádření vzájemných vazeb mezi identifikovanými riziky a to pomocí tabulky souvztažností.

	Index	1	2	3	4
Index	**Rizika**	**Vysoká teplota**	**Blesk**	**Pád stromu**	**Provozní chyba pracovníků třetích stran**
1	Vysoká teplota				
2	Blesk				
3	Pád stromu				
4	Provozní chyba pracovníků třetích stran				

Tabulka 7 - Tabulka pro hodnocení souvztažností

Pro vyjádření vzájemných vazeb mezi riziky je tabulka souvztažnosti rizik vyplněna hodnotami kde:

- x – vyjadřuje skutečnost, že riziko samo sebe vyvolat nemůže,
- 1 – vyjadřuje reálnou možnost, že Riziko R_i může vyvolat Riziko R_j,
- 0 – vyjadřuje stav, kdy neexistuje reálná možnost, že Riziko R_i může vyvolat Riziko R_j,

Následujícím krokem je vyjádření již zmiňované aktivity (koeficient aktivity K_AR_i), která vyjadřuje celkový potenciál rizika způsobovat vznik dalších rizik či vyjádření pasivity (koeficient pasivity K_PR_i), která vyjadřuje počet všech rizik, která dané riziko mohou vyvolat. (Celou kvantifikaci je možné zobrazit pomocí grafu - kapitola 6.3)

Pro výpočet daných koeficientů se použijí vztahy:

$$K_A R_i = \frac{\sum R_i}{x-1}$$

$$K_P R_i = \frac{\sum R_i}{x-1}$$

Kde:

$\sum R_i$ je součet rizik (pro koeficient aktivity je to horizontální osa a pro koeficient pasivity vertikální osa),

x je celkový počet rizik

Současně je možné považovat hodnoty horizontální osy za parametry osy x (koeficient aktivity) a hodnoty vertikální osy za parametry osy y (koeficient pasivity)

Pro účely prioritizace rizik je nutné vytvořený graf rozdělit na jednotlivé segmenty, které diverzifikují rizika podle jejich významnosti. Pro rozdělení grafu na 4. segmenty je nutné definovat přímky P1 a P2, které rozdělí samotný graf tak i rizika do segmentů, kde se předpokládá, že v prvním segmentu bude 80% nejvýznamnějších rizik.

Pro vyjádření parametrů pro přímky P1 a P2 použijeme vztah:

$$P_1 = K_{A\max} - \frac{(K_{A\max} - K_{A\min})}{100} * 80$$

$$P_2 = K_{P\max} - \frac{(K_{P\max} - K_{P\min})}{100} * 80$$

Kde:

K_{Amax} a K_{Amin} - jsou minimální a maximální hodnoty z tabulky s koeficienty aktivity

K_{Pmax} a K_{Pmin} - jsou minimální a maximální hodnoty z tabulky s koeficienty pasivity

Praktický příklad použití KARS metodiky je součásti přílohové dokumentace (příloha 6.3.).

4 Návrhová část postupu tvorby systému řízení ochrany

Stanovení požadavků na systém řízení ochrany kritické infrastruktury v oblasti výroby přenosu a distribuce elektrické energie vyplývá z potřeby udržení funkční kontinuity dodávky elektrické energie. V rámci procesu formulace požadavků a parametrů na systém řízení a jeho jednotlivé části byla zohledněna specifika vybrané oblasti kritické infrastruktury, výstupy fáze analytické tak i fáze pilotního provozu a ověření metodiky.

Samotný metodický postup je rozdělený do ucelených, na sobě závislých celků. Výstupem metodiky je konkretizace vybraných oblastí bezpečnosti, a to ve vztahu k optimalizaci procesu řízení ochrany kritické infrastruktury ve vybrané oblasti za účelem zajištění kontinuity dodávky elektrické energie. Oblasti bezpečnosti, které budou v následujícím textu strukturálně popsány, lze rozdělit na tyto celky:

- Fyzická bezpečnost,
- Informační bezpečnost,
- Administrativní bezpečnost,
- Personální bezpečnost,
- Krizové řízení a plánování.

Vymezení těchto oblastí bezpečnosti vyplývá z obecných požadavků subjektů kritické infrastruktury či odpovědných orgánů státní správy.

4.1 Stanovení požadavků na systém řízení ochrany kritické infrastruktury - fyzická bezpečnost

Tato část metodického postupu stanovuje strukturální a kvalitativní požadavky na jednotlivé části systému fyzické ochrany jako prostředku zajištění fyzické bezpečnosti kritické infrastruktury, které do jisté míry reflektují stanovená rizika a jejich potenciál způsobit degradaci funkční kontinuity subjektu a skutečností, vyplývajících z fyzických prověrek vybraných objektů a prvků kritické infrastruktury.

Následující text formuluje strukturální a kvalitativní požadavky na systémy fyzické ochrany pro tyto oblasti:

Prvky systému fyzické ochrany:

- Systémy technické ochrany:
  - PZTS - poplachový zabezpečovací a tísňový systém,
  - CCTV – kamerový systém,
  - SKV/EKV – systém kontroly vstupu,
  - MZP – mechanické zábranné prostředky,
- Fyzická ostraha,
- Režimová opatření,

Prostorové členění:

- Perimetr areálu,
- Vnější prostory,
- Vnitřní prostory a prostory budov.

Klasifikace prostorů podle významu:

- KPR – Kontrolovaný prostor - představuje prostor mezi důležitými místy (klíčovými místy) objektu s požadavky na nižší úroveň zabezpečení,
- CHP – Chráněný prostor - prostor s důležitými místy, kde se však nepředpokládá přítomnost zařízení ovlivňujících základní funkci prvku kritické infrastruktury s požadavky na střední úroveň zabezpečení,
- ZCHP – Zvláště chráněný prostor - prostor s přítomností klíčových technologických zařízení, popřípadě prostor, v kterém se pracovníky daného objektu vykonávají klíčové pracovní činnosti z pohledu základních funkcí prvku kritické infrastruktury s požadavky na nejvyšší úroveň zabezpečení.

Následující tabulka obsahuje základní členění prostor a jejich klasifikaci podle významu, kdy se předpokládá, že konečná struktura bude individuálně přizpůsobená dle individuálních a specifických potřeb subjektů kritické infrastruktury.

	Oblasti využití MZP	Parametry lokality - areálu, objektu - budovy, prostoru (LOP)
Perimetr areálu	KPR	Vnější oplocení
	KPR	Vstupy (vstupní branka)
	KPR	Vjezdy (vjezdová a vlečková brána)
	KPR	Budovy v perimetru
Vnější prostory	KPR	Venkovní stanoviště silového en. zařízení
	KPR	Odstavné plochy uvnitř objektu s uloženým majetkem
	KPR	Vstupy do průchozích kabelových kanálů
Vnitřní prostory a budovy	KPR	Vstupní (venkovní) dveře a vrata v plášti budovy vč. nouzových východů a vstupů z průchozích nebo průlezných kabelových kanálů
	KPR	Prosklené části (dveře, okna) v plášti budovy
	KPR	Prosklené části (sklepní okna) v plášti budovy, které jsou pod úrovní okolního terénu
	KPR	Další technické otvory v plášti budovy
	CHP	Vyústění průchozího nebo průlezného kabelového kanálu (do/z vnitřního prostoru budovy)
	CHP	Vstupní (vnitřní) dveře do prostorů, resp. místností související s provozem objektu
	CHP	Prostor nebo místnost s instalovanou ústřednou PZTS
	ZCHP	Prostory, resp. místnosti související s provozem objektu
	ZCHP	Prostory, resp. místnosti související s provozem (řízením) objektu a nepřetržitou přítomností osob (stálá služba)

Tabulka 8 - Klasifikace prostor podle významu

4.1.1 Mechanické zábranné prostředky

Využití MZP naplňuje základní funkci systému fyzické ochrany „zpomalení“ (delay). Ve vztahu k formulaci strukturálních a kvalitativních parametrů MZP je potřebné vybranou oblast systémů fyzické ochrany popsat a to z pohledu oblastí potenciálního využití zmiňovaných prostředků či z pohledu vybraných parametrů lokality, objektu či prostoru. Je zřejmé, že tabulkové vymezení a členění lze chápat jen jako základní a obecné vymezení oblastí využití, což vytvoří subjektům kritické infrastruktury dostatečný manipulační prostor pro úpravu kvalitativních parametrů (jednostranný bavolet, osazený třemi řadami žiletkového drátu nebo dvoustranný bavolet osazený žiletkovou spirálou, funkční mříž musí splňovat požadavky bezpečnostní třídy 3 podle normy ČSN P ENV 1627) v návaznosti na specifičnost a jedinečnost vybraného objektu, či interní filozofii využívaní MZP v rámci systémů fyzické ochrany ve vztahu k implementaci systému řízení ochrany kritické infrastruktury. Příklad stanovení strukturálních a kvalitativních parametrů a požadavků pro oblast výroby, přenosu a distribuce elektrické energie je součásti příloh 6.4.1 – 6.4.3.

Oblasti využití MZP		Parametry lokality - areálu, objektu - budovy, prostoru (LOP)
Mechanické zábranné prostředky	Perimetr areálu	Vnější oplocení
		Vstupy (vstupní branka)
		Vjezdy (vjezdová a vlečková brána)
		Budovy v perimetru
	Vnější prostory	Venkovní stanoviště silového en. zařízení
		Odstavné plochy uvnitř objektu s uloženým majetkem
		Vstupy do průchozích kabelových kanálů
	Vnitřní prostory a budovy	Vstupní (venkovní) dveře a vrata v plášti budovy vč. nouzových východů a vstupů z průchozích nebo průlezných kabelových kanálů
		Uzamykací systém nebo visací zámek ve vstupních (venkovních) dveřích a vratech do budovy
		Samouzavírací mechanismus na hlavních vstupních (venkovních) dveřích do budovy
		Prosklené části (dveře, okna) v plášti budovy
		Prosklené části (sklepní okna) v plášti budovy, které jsou pod úrovní okolního terénu
		Další technické otvory v plášti budovy
		Pevné žebříky na plášti budovy vyúsťující na střechu

Tabulka 9 - Mechanické zábranné prostředky a jejich základní členění

4.1.2 PZTS, CCTV, SKV, PPSZ

Pro optimální strukturu systému fyzické ochrany či optimální strukturu komplexního systému řízení ochrany kritické infrastruktury je nutné stanovit strukturální a funkční požadavky a vymezit oblasti použití PZTS, CCTV, SKV, PPSZ či formulovat parametry lokality, objektu, budovy pro naplnění další základní funkce systému fyzické ochrany - funkce detekce (detection). Tento proces následně umožní individuální konkretizaci kvalitativních parametrů (monitorovat kamerami venkovního sledovacího systému CCTV s digitálním záznamem obrazového signálu (dle ČSN EN 50 132-7), MK stupně zabezpečení 3 - střední až vysoké riziko dle ČSN EN řady 50 131). Příklad stanovení strukturálních a kvalitativních parametrů a požadavků pro oblast výroby, přenosu a distribuce elektrické energie je součástí přílohové dokumentace 6.4.5 – 6.4.6.

Oblasti využití PZTS, CCTV, SKV, PPSZ		Parametry lokality - areálu, objektu - budovy, prostoru (LOP)
PZTS, CCTV, SKV, PPSZ	Perimetr areálu	Vnější oplocení
		Vstupy (vstupní branka)
		Vjezdy (vjezdová a vlečková brána)
		Budovy v perimetru
		Ostatní prostupy
	Vnější prostory	Venkovní stanoviště silového energetického zařízení
		Odstavné plochy uvnitř objektu s uloženým majetkem
		Vstupy do průchozích kabelových kanálů
		Evidence vstupu ve venkovních prostorách objektu
		Přenos poplachových a jiných funkčních stavů PZS na energetický dispečink
		Přenos poplachových a jiných funkčních stavů PZS na regionální dohledové pracoviště
	Vnitřní prostory a budovy	Vstupní (venkovní) dveře a vrata v plášti budovy vč. nouzových východů a vstupů z průchozích nebo průlezných kabelových kanálů
		Prosklené části (dveře, okna) v plášti budovy
		Prosklené části (dveře, okna) v plášti budovy přístupné z dosažitelných míst (pochůzné římsy a střechy, žebříky, balkony)
		Prosklené části (sklepní okna) v plášti budovy, které jsou pod úrovní okolního terénu
		Další technické otvory v plášti budovy

		Pevné žebříky na plášti budovy vyúsťující na střechu
		Vyústění průchozího nebo průlezného kabelového kanálu (do/z vnitřního prostoru budovy)
		Vstupní (vnitřní) dveře do prostorů, resp. místností související s provozem objektu
		Prostory, resp. místnosti související s provozem objektu
		Prostory, resp. místnosti související s provozem (řízením) objektu a nepřetržitou přítomností osob (stálá služba)
		Vnitřní prostory u vstupních dveří do budovy (zádveří) a další společné prostory (chodby, schodiště)
		Prostor nebo místnost s instalovanou ústřednou PZTS
		Evidence vstupu do budovy a evidence vstupu do vybraných prostor nebo místnosti souvisejících s provozem objektu (v PZTS nebo SKV)
		Přenos poplachových a jiných funkčních stavů PZS na energetický dispečink
		Přenos poplachových a jiných funkčních stavů PZS na regionální dohledové pracoviště

Tabulka 10 - Stanovené oblasti využití PZTS, CCTV, SKV, PPSZ

4.1.3 Režimová opatření a fyzická ostraha

Další relevantní oblastí systému fyzické ochrany subjektu kritické infrastruktury v kontextu implementace komplexního systému řízení ochrany kritické infrastruktury je oblast režimových opatření a fyzické ostrahy, pro které se požaduje a předpokládá detailní formulace vybraných zásad a požadavků pro konkrétní nastavení těchto oblastí za účelem naplnění významné funkce systému fyzické ochrany - odezva resp. reakce na činnost a postup narušitele (response). Následující tabulka popisuje oblasti, s kterými lze uvažovat v oblasti výroby, přenosu a distribuce elektrické energie, kde jejich konkretizace (fyzická kontrola stavu (neporušenosti) vnějšího oplocení, pláště budov v objektu, odvrácení vzniku majetkové újmy) bude realizována na základě individuálních potřeb subjektů kritické infrastruktury. Příklad stanovení strukturálních a kvalitativních parametrů a požadavků pro oblast výroby, přenosu a distribuce elektrické energie je součásti přílohové dokumentace 6.4.7 – 6.4.8.

Rozdělení parametrů		Zásady režimových opatření a fyzické ostrahy
Režimová opatření a fyzická ostraha	Parametry vztahující se k RO	Stanovení určených vstupů pro osoby a vjezdů pro vozidla do objektu
		Stanovení rozsahu oprávnění osob pro vstup a dopravních prostředků pro vjezd do objektu
		Režim pohybu osob, vozidel v objektu
		Režim pohybu materiálu v objektu (vnášení, vynášení majetku)
		Režim manipulace s klíči a STO
		Řešení mimořádných událostí (bezpečnostní incidenty)
	Parametry vztahující se k FOS	Výkon stálé služby na objektu
		Obchůzková činnost na objektu (pravidelná nebo nepravidelná)
		Strážní činnost na objektu bez instalovaného STO (pravidelná nebo nepravidelná)
		Obsluha STO na dohledovém pracovišti (nepřetržitě)
		Vyhodnocování stavů STO a reakce na ně (průběžné)
		Mobilní zásah na objektu (neprodleně)

Tabulka 11 - Režimová opatření a fyzická ostraha

Obecné vymezení základních strukturálních požadavků na jednotlivé části systému fyzické ochrany je významnou vstupní činností v rámci procesu tvorby komplexního systému řízení ochrany kritické infrastruktury ve vybrané oblasti. Lze konstatovat, že stanovené požadavky reflektují výstupy z analýzy rizik a skutečností, které byly zjištěny v rámci procesu fyzické prověrky vybraných objektů a prvků kritické infrastruktury. Předpokládá se, resp. je zde prostor, aby struktura požadavků i jejich konkretizace a individualizace byla přizpůsobená požadavkům a filozofii jednotlivých subjektů kritické infrastruktury v oblasti výroby, přenosu a distribuce elektrické energie.

4.2 Stanovení požadavků na systém řízení ochrany kritické infrastruktury - Informační bezpečnost

4.2.1 Zásady řízení informační bezpečnosti

Nastavení a formulace procesu řízení informační rizik resp. řízení informační bezpečnosti je základním aspektem nastavení jednotných standardů pro zajištění funkčnosti informačních systémů subjektů kritické infrastruktury v oblasti výroby, přenosu a distribuce elektrické energie. Komplexnost informačních systémů a současné trendy ve vývoji ICT zvyšují důraz na budování standardů informační bezpečnosti. Informační (ICT) bezpečnost je jedním ze základních pilířů ochrany kritických aktiv zejména poskytováním ochrany informacím spravovaných uvnitř databází a informačních systémů a procesům, které nad těmito daty pomocí aplikačního vybavení probíhají. Oblast ICT navíc poskytuje komunikační platformu dalším bezpečnostním systémům, jako jsou například systémy fyzické ochrany. V následujícím textu jsou identifikovány standardní oblasti řízení bezpečnosti IS/IT, ve kterých je možné identifikovaná rizika jednotným postupem minimalizovat a jsou relevantní pro potřeby systému řízení ochrany kritické infrastruktury. Příklad stanovení strukturálních a kvalitativních parametrů a požadavků pro oblast výroby, přenosu a distribuce elektrické energie je součástí přílohové dokumentace 6.5.1 – 6.5.18.

Požadovaný parametr systému řízení bezpečnosti		Související procesy
Zásady řízení informační bezpečnosti	Identifikace a autentizace,	Distribuce hesla
		Délka hesla
		Komplexnost hesla
		Použití hesla
		Četnost změny hesla
		Identifikátory uživatelů
		Sdílení účtů
	Řízení logického přístupu,	Zásady řízení přístupu
		Omezení přístupu k informacím
		Časový limit práce pracovní stanice / heslem chráněné spořiče obrazovek
		Blokace defaultních účtů
		Přístup k auditním záznamům
	Evidence událostí a audit,	Záznam událostí
		Doba uchovávání evidenčního deníku
		Monitoring
		Pravidelné kontroly přístupových oprávnění
		Analýza evidence událostí
		Vyšetřování incidentu
		Řízení systémového auditu
	Integrita programového vybavení,	Kontroly integrity programového vybavení
		Aktualizace operačních systémů, databází a síťových komponent
		Aktualizace SW vyvíjeného na klíč
	Zálohování a skartace dat,	Zálohování provozu
		Zálohování dat
		Bezpečná likvidace médií
		Skartace logická
	Odolnost sítě,	Redundance síťových zařízení
		Protokoly a služby
		Šifrovaná spojení
		Firewall; IDS/IPS; Proxy server
		Pravomoci síťových administrátorů
		Zálohování směrovacích tabulek

	Testování systému,	Testování bezpečnosti
		Testování obnovy záloh
		Testování aktualizací
	Ochrana proti škodlivým programům,	Opatření na ochranu proti škodlivým programům
		Odstranění škodlivého programového vybavení
	Kontrola správy systému,	Omezení změn v komerčním balíku aplikací
		Řízení přístupu k účtům správců systému
	Provozní kontroly,	Provozní postupy
		Zálohovací logy
	Infrastruktura veřejných klíčů	Používaní certifikátů pro vybrané IS
	Kontrola změny programového vybavení,	Nouzové opravy programového vybavení
	Autorizace zákazníků,	Autentizační služby
		Služby správy zákazníků
		Zabezpečený vzdálený přístup
	Analýza zranitelností,	Identifikace a hodnocení aktiv
		Identifikace a hodnocení hrozeb a zranitelností
		Identifikace a hodnocení ochranných opatření
	Kontroly dokumentů/médií,	Uložení dokumentů, médií.
	Virtualizace	Řízení komunikace a řízení provozu Klasifikace a řízení aktiv Řízení přístupu
	Organizace bezpečnosti	Infrastruktura bezpečnosti informací
		Bezpečnost přístupu třetích stran
	Plánování kapacit	Plánování kapacit programového vybavení
		Kontrola dostatečné kapacity
		Akceptace systému

Tabulka 12 - Oblasti informační bezpečnosti

Formulace základních požadavků informační bezpečnosti je dalším základním stavebním kamenem řízení ochrany kritické infrastruktury v oblasti výroby, přenosu a distribuce elektrické energie. Obdobně jako v předešlých částech přepokládáme, že základní sada požadavků uvedená v přílohách je považována za sadu standardních parametrů, ze které lze čerpat a přizpůsobit dle individuálních potřeb jednotlivých subjektů kritické infrastruktury.

4.3 Stanovení požadavků na systém řízení ochrany kritické infrastruktury – Administrativní a personální bezpečnost

4.3.1 Administrativní bezpečnost

Mezi další významnou část systému řízení ochrany pro vybranou oblast kritické infrastruktury patří i aspekty administrativní bezpečnosti, která řeší zajištění dostatečné ochrany dokumentů v listinné a elektronické podobě při jejich tvorbě, příjmu, evidenci, zpracování, odesílání, přepravě, přenášení, ukládání, skartaci, archivaci a podobně. Za základní oblasti administrativní bezpečnosti se považují:

Oblasti administrativní bezpečnosti	
Administrativní bezpečnost	Odpovědnosti, povinnosti a pravomoci
	Označování a klasifikace dokumentů
	Manipulace s dokumenty
	Ztráta dokumentů a jejich nosičů - médií
	Administrativní bezpečnosti při personálních změnách

Tabulka 13 - Oblasti administrativní bezpečnosti

Příklad stanovení strukturálních a kvalitativních parametrů a požadavků pro oblast výroby, přenosu a distribuce elektrické energie je součásti přílohové dokumentace 6.6.1.

4.3.2 Personální bezpečnost

Na základě realizované analýzy a konzultací s odpovědnými orgány v předmětné oblasti kritické infrastruktury byla jako další část komplexního systému řízení ochrany definována oblast personální bezpečnosti, která je vnímána jako systém výběru fyzických osob ve vztahu k přístupu a přístupům k informačním aktivům organizace, ověřování podmínek pro jejich přístup k informacím a jejich výchovu a ochranu. Požadavky se soustředí na minimalizaci dopadu lidských chyb, potenciální krádeže, podvodu nebo zneužití informačních prostředků organizace. Ve vztahu k formulaci zásad personální bezpečnosti metodika stanovuje tyto oblasti:

Oblasti personální bezpečnosti	
Personální bezpečnost	Odpovědnosti, povinnosti a pravomoci
	Prověřování zaměstnanců
	Dohody o ochraně informací
	Podmínky výkonu pracovní činnosti
	Školení zaměstnanců
	Reakce na bezpečnostní incidenty a selhání
	Disciplinární proces
	Ukončení pracovního vztahu

Tabulka 14 - Oblasti personální bezpečnosti

Příklad stanovení strukturálních a kvalitativních parametrů a požadavků pro oblast výroby, přenosu a distribuce elektrické energie je součásti přílohové dokumentace 6.6.2.

4.4 Stanovení požadavků na systém řízení ochrany kritické infrastruktury - krizové řízení a plánování

Krizové řízení a plánování je považováno za velmi důležitou část z pohledu řízení ochrany kritické infrastruktury, která by měla identifikovat požadavky a potřeby pro zajištění kontinuity a obnovy funkčnosti kritické infrastruktury v oblasti výroby, přenosu a distribuce elektrické energie. Navržené strukturální a funkční požadavky na jednotlivé oblasti krizového řízení a plánování optimalizují proces řešení vzniklé mimořádné události/situace v systému, za předpokladu zachování základních funkcí vybrané oblasti a jejich obnovu.

4.4.1 Systém krizového řízení a plánování – strukturální požadavky

Následující tabulka stanovuje standardní oblasti odpovědností a činností na jednotlivých úrovních řízení a plánování ve vybrané oblasti kritické infrastruktury.

Personální struktura krizového řízení organizace	
Personální struktura KŘO	Představitel vedení pro krizové řízení organizace / Styčný bezpečnostní zaměstnanec
	Manažer krizového řízení organizace
	Garant krizového řízení organizace za úsek
	Řešitel
	Zaměstnanci

Tabulka 15 - Personální struktura krizového řízení organizace

Další funkční oblastí je personální struktura krizového týmu, jehož povinnosti a odpovědnosti zásadním způsobem ovlivňují funkční kontinuitu a proces krizového řízení v případě vzniku mimořádné události.

Personální struktura krizového týmu organizace	
Personální struktura krizového týmu organizace	Vedoucí krizového týmu organizace
	Zástupce vedoucího krizového týmu organizace
	Koordinátor KPO
	Členové

Tabulka 16 - Personální struktura krizového týmu organizace

V případě řešení mimořádného stavu, krizové situace (dále jen MS/KS) se klade zvýšený důraz na formulaci optimální formy řízení krizového týmu a rozdělení procesu řízení do několika úrovní. V tabulce jsou stanoveny zásadní požadavky procesu řízení krizového týmu na jednotlivých úrovních, a je zřejmé, že pro udržení funkční kontinuity výroby, přenosu a distribuce elektrické energie budou jednotlivé úrovně a popis jednotlivých činností přizpůsobeny reálným požadavkům jednotlivých subjektů.

Úroveň řízení krizového týmu	
Úroveň řízení krizového týmu	Operativní úroveň
	Taktická úroveň
	Strategická úroveň

Tabulka 17 - Úroveň řízení krizového týmu

Důležité je stanovení priorit činností a úrovní řízení krizových týmů a stanovení stupně významu MS/KS ve vztahu k dostupnosti klíčových funkcí systému. Následující tabulka proto formuluje oblasti resp. stupně MS/KS.

Stupně mimořádných stavů/krizových situací	
Stupeň MS/KS	1. STUPEŇ (AKTIVACE KP a KPO)
	2. STUPEŇ
	3. STUPEŇ
	4. STUPEŇ

Tabulka 18 - Stupně mimořádných stavů/ krizových situací

Činnosti krizového týmu organizace	
Stupeň MS/KS	Vznik mimořádné události a vyhlášení MS/KS
	Aktivace krizového týmu organizace
	Řízení mimořádného stavu
	Vyhodnocení a ukončení mimořádného stavu

Tabulka 19 - Činnosti krizového týmu organizace

Příklad konkretizace požadavků na jednotlivé aspekty krizového řízení je předmětem přílohové dokumentace 6.7.1 – 6.7.5.

4.4.2 Krizový plán subjektu KI – strukturální požadavky

Další významnou součástí zachování funkční kontinuity vybrané oblasti KI, v rámci které je potřeba implementovat stanovené požadavky je plánovací dokumentace, která zajišťuje krizovou připravenost subjektu KI. Mezi relevantní dokumentaci, lze v tomto kontextu považovat krizové plány či plány krizové připravenosti subjektu KI, kde v druhém případě by měla být věnována zvýšená pozornost právě operativní části, kde se předpokládá jistá forma propojenosti plánu na jinou a další bezpečnostní dokumentaci.

	Legislativní dokument	Specifikace zaměření vybrané normy
KPO- Vazby na vnější dokumenty	zákon č. 458/2000 Sb.	- o podmínkách podnikání a o výkonu státní správy v energetických odvětvích a o změně některých zákonů (energetický zákon),
	zákon č. 240/2000 Sb.	- o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění zákona č. 320/2002 Sb.
	zákon č. 241/2000 Sb.	- o hospodářských opatřeních pro krizové stavy a o změně některých souvisejících zákonů, ve znění zákona č. 320/2002 Sb.
	zákon č. 222/1999 Sb.	- o zajišťování obrany ČR
	zákon č. 239/2000 Sb.	- o integrovaném záchranném systému
	zákon č. 238/2000 Sb.	- o Hasičském záchranném sboru ČR
	zákon č. 133/1985 Sb.	- o požární ochraně (úplné znění vyhlášeno jako č. 67/2001 Sb.)

	zákon č. 254/2001 Sb.	- o vodách (vodní zákon)
	zákon č. 258/2000 Sb.	- o ochraně veřejného zdraví
	vyhláška Správy státních hmotných rezerv č. 498/2000 Sb.	- o plánování a provádění hospodářských opatření pro krizové stavy, ve znění vyhlášky č.542/2002 Sb.
	vyhláška Ministerstva průmyslu a obchodu č. 219/2001 Sb.	- o postupu v případě hrozícího nebo stávajícího stavu nouze v elektroenergetice

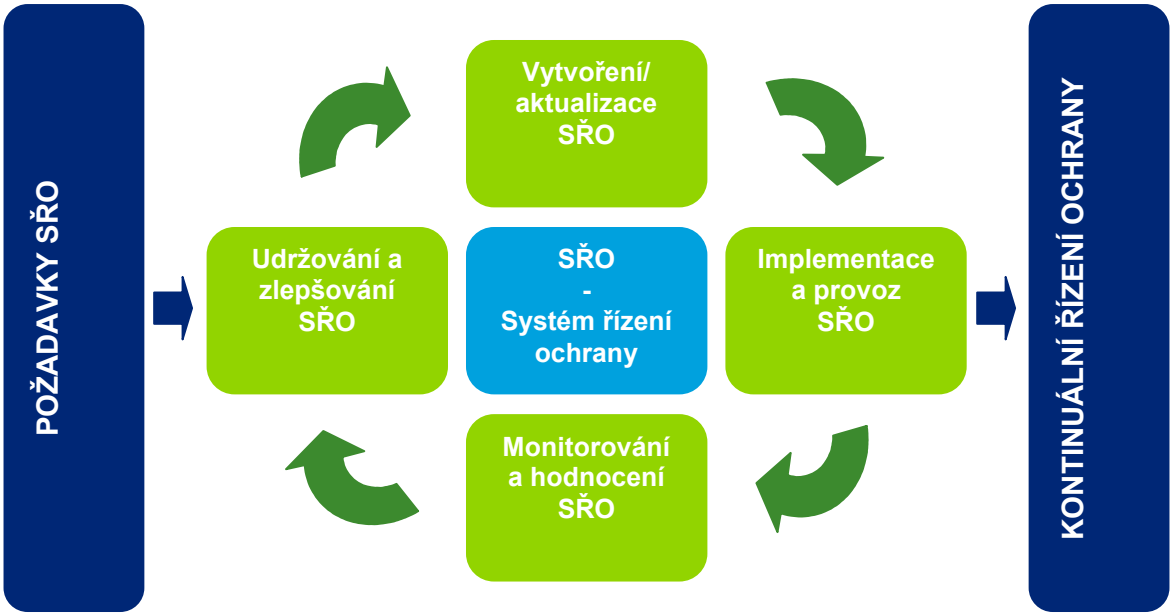
Tabulka 20 - Seznam regulatorních požadavků

5 Implementační část postupu tvorby systému řízení ochrany

5.1 Systém řízení ochrany

Systém řízení ochrany kritické infrastruktury (dále SŘO) jednotlivé oblasti bezpečnosti propojuje do řízeného procesu nasazení a zdokonalování opatření, která se zaměřují na ochranu definovaných aktiv vybrané oblasti kritické infrastruktury. SŘO je navrhován dle kontinuálního procesu PDCA (Plánuj-Udělej-Zkontroluj-Jednej). Vstupem jsou jednotlivé požadavky dle oblastí SŘO, výstupem je kontinuální řízení ochrany ve zvolených oblastech bezpečnosti, případně v dalších oblastech, které budou do systému řízení později zakomponovány

Jednotlivé kroky procesu řízení ochrany kritické infrastruktury je možné znázornit jako kontinuální cyklus:



Obrázek 2 - Grafické znázornění SŘO

Plánuj – Vytvoření SŘO

Navržení/aktualizace SŘO kritické infrastruktury v oblasti výroby, přenosu a distribuce elektrické energie dle požadavků na identifikované oblasti bezpečnosti:

- Fyzická bezpečnost,
- Informační bezpečnost,
- Administrativní a personální bezpečnost,
- Krizové řízení a plánování.

Udělej – Implementace a provoz SŘO

Definování postupu implementace navrženého SŘO a následné řízení vybraných oblastí bezpečnosti. Implementace by měla probíhat dle jasně stanovených kroků a časového harmonogramu (ROAD mapy). Bezpečnostní systémy a prvky, které jsou již implementovány, musí být provozovány dle nastavených standardů s dostatečnou materiální a personální podporou. V průběhu provozu či implementace bude docházet k zajišťování zpětné vazby viz. následující krok procesu.

Zkontroluj – Monitorování a hodnocení SŘO

Řízení ochrany zahrnuje automatické i administrativní (manuální) procesy monitorování, které umožní zachytit incidenty a na jejich základě případně i na základě absence incidentů provádět jejich analýzy a

hodnotit kvalitu provozovaného SŘO. A to buď kontinuálně v návaznosti na konkrétní zjištění anebo formou předem definovaných intervalů, během kterých bude docházet k analýzám a hodnocení. Rovněž stav implementace požadavků by měl být kontinuálně v definovaných intervalech monitorován a vyhodnocován pro každou geografickou lokalitu a její oblasti bezpečnosti. V návaznosti na výstupy monitoringu a hodnocení pak dojde k reflexi v samotném SŘO.

Jednej – Udržování a zlepšování SŘO

Na základě zjištění provedeného monitorování a hodnocení stavu SŘO včetně zohlednění aktuální situace v oblasti legislativních a jiných požadavků na úroveň bezpečnosti a ochrany jsou sepsány aktuální požadavky k úpravě/aktualizaci návrhu SŘO na výše uvedené oblasti bezpečnosti.

Celý cyklus může probíhat kontinuálně v návaznosti na jednotlivá zjištění či požadavky které je třeba reflektovat v praxi (kontinuální ladění) anebo v předem definovaných intervalech při kterých bude docházet nejprve k implementaci, následně provozu, vyhodnocení provozu a reflexi vyhodnocení v návrhu úprav například v ročním cyklu (periodické ladění). Volba periodicity či volba mezi kontinuálním a rozdílovým laděním závisí zejména na požadavcích jednotlivých subjektů kritické infrastruktury, ale také kritičnosti zjištění. Oba přístupy tak mohou existovat vedle sebe a je doporučeno kritická zjištění reflektovat na bázi kontinuálního ladění a zároveň provádět aktualizace v předem definované periodě.

Vzhledem k rozdílným potřebám a podmínkám jednotlivých subjektů je nutné provést upřesnění a následně rozdílovou analýzu stávajícího a navrhovaného stavu stanovených oblastí bezpečnosti. Výsledky rozdílové analýzy jsou vstupem do následného kroku procesu řízení ochrany.

Následující tabulka uvádí aktivity, které by měly být v jednotlivých krocích procesu řízení ochrany prováděny. Cyklus PDCA je vhodné podpořit také pomocí pravidelného fóra pro řízení ochrany vybrané oblasti kritické infrastruktury, na kterém jsou bezpečnostní opatření, jejich efekt či zjištěné bezpečnostní incidenty reportovány a které by mělo přicházet s nápravnými opatřeními. Cyklus PDCA není nutné vnímat pouze jako souhrnné fáze pro všechny oblasti bezpečnosti probíhající v průběhu zvolené periody, ale je možné paralelně sledovat více cyklů dle jednotlivých oblastí bezpečnosti nebo dokonce dle jednotlivých opatření jelikož nasazování opatření zpravidla neprobíhá naráz pro všechna opatření ze všech oblastí ale spíše v průběhu roku dle potřeb a možností jednotlivých subjektů.

	Systém řízení ochrany	Popis kontinuálního cyklu
Fáze systému řízení ochrany	Plánuj – Vytvoření.	Bezpečnostní manažer by měl ve spolupráci s odpovědnými zaměstnanci provádět pravidelné plánování ochranných opatření, jejich implementace, pravidelné interní i nezávislé kontroly a další aktivity v oblasti bezpečnosti. Měl by být vytvořen harmonogram a alokovány kapacity, které umožní plánované aktivity realizovat.
	Udělej – Implementace a provoz.	Ve spolupráci s administrátory systémů, zaměstnanci fyzické ochrany, správci procesů či zástupcem administrativní bezpečnosti a dalšími osobami odpovědnými za zvolené oblasti bezpečnosti nebo jejich části by měly být realizována a provozována opatření bezpečnosti, za která jsou tito správci odpovědní.
	Zkontroluj – Monitorování a hodnocení.	Kontrola opatření by měla probíhat jednak v úrovni vyhodnocování bezpečnostních událostí v daných oblastech, ale také přímo kontrolou nastavení jednotlivých opatření a projekce jejich úspěšnosti v oblasti prevence a zjišťování bezpečnostních událostí.
	Jednej – Udržování a zlepšování.	Na základě zjištění získaných pravidelným monitorováním a hodnocením stavu řízení ochrany včetně zohlednění aktuální situace v oblasti legislativních a jiných požadavků na úroveň bezpečnosti a ochrany jsou připraveny aktuální požadavky k úpravě/aktualizaci opatření řízení ochrany ve všech zvolených oblasti řízení bezpečnosti a ochrany

Tabulka 21 - Stanovení požadavků na systém řízení ochrany

6 Přílohová část

6.1 Příloha 1 - Vymezení katalogu hrozeb kritické infrastruktury z oblasti výroby, přenosu a distribuce elektrické energie

Skupiny hrozeb v oblasti výroby, přenosu a distribuce el. energie	
Přírodní hrozby	Lidský faktor – organizační selhání
Technická selhání	Lidský faktor – ohrožení fyzické povahy
Technická selhání systémů fyzické ochrany	Lidský faktor – terorizmus
Logické hrozby	Chyby
Komunikační hrozby	Fyzické hrozby
Závady zařízení	

Tabulka 22 - Skupiny hrozeb v oblasti výroby, přenosu a distribuce el. energie

Přírodní hrozby	
Povodeň	Vichřice
Přívalový déšť	Blesk
Sesuv půdy	Požár
Kroupy	Pád stromu
Sníh	Znečistěné ovzduší prachem
Námraza	Elektromagnetická radiace
Vysoká teplota	Zemětřesení

Tabulka 23 - Přírodní hrozby

Technická selhání	
Přerušení dodávky elektřiny	Selhání záložních zdrojů napájení
Přerušení dodávky vody	Selhání topení
Únik a výbuch plynu mimo prostor	Selhání klimatizace
Únik ropných látek mimo prostor	Selhání osvětlení v posuzovaném prostoru
Únik ropných látek v prostoru	Zamoření ovzduší nebezpečným plynem
Únik vody z vod. Řadu mimo prostor	Rozsáhlé nehody vně prostoru
Únik vody z vod. Řadu v prostoru	Jaderná havárie
Provozní porucha	

Tabulka 24 - Technická selhání

Technické selhání systémů fyzické ochrany	
Porucha serveru	Porucha prvku PZTS
Porucha pracovní stanice	Porucha prvku CCTV
Porucha kabeláže	Porucha zámkových systémů
Porucha prvku SKV	Selhání software

Tabulka 25 - Technické selhání systémů fyzické ochrany

Lidský faktor – organizační selhání	
Nevhodně stanovené pracovní postupy	Neznalost, nepřipravenost zaměstnanců
Nedodržení pracovních postupů	Nedbalost, ignorance pracovníků
Provozní chyba zaměstnanců	Nedostatek materiálních zdrojů
Provozní chyba pracovníků třetích stran	Nedostatek lidských zdrojů
Chybná manipulace s prvky systému fyzické ochrany	Selhání bezpečnostní služby

Tabulka 26 - Lidský faktor – organizační selhání

Lidský faktor – ohrožení fyzické povahy	
Získání informací o ochraně prostoru	Předstírání fyzické identity cizími osobami
Odezírání při kódování a přihlášení do systému fyzické ochrany	Násilné vniknutí cizí osoby do prostor
Odposlech komunikace prvků systému fyzické ochrany	Vloupání do prostor
Předstírání uživatelské identity	Krádež provedená zaměstnancem
Neoprávněný přístup cizí osoby do prostoru	Krádež provedená pracovníky třetích stran
Neoprávněný přístup k prvkům systému fyzické ochrany	Krádež provedená cizími osobami
Neoprávněná manipulace s prvky systému fyzické ochrany	Zničení bezpečnostních prvků prostor
Úmyslné poškození prostoru zaměstnancem	Zničení chladícího zařízení
Úmyslné poškození prostoru cizí osobou	Zničení vod. řadu
Úmyslné poškození bezpečnostních prvků	Zničení venkovního vedení - lana
Sabotáž zaměstnance	Zničení venkovního vedení - sloupy
Předstírání fyzické identity zaměstnancem	Destrukce prostor nebo jejich části
Předstírání fyzické identity pracovníky třetích stran	Použití zbraně / loupežné přepadení
Demonstrace v blízkosti prostor	

Tabulka 27 - Lidský faktor – ohrožení fyzické povahy

Lidský faktor – terorismus	
Výhrůžky umístnění bomby - telefonicky, e-mailem	Únos zaměstnanců
Výhrůžky umístnění bomby - písemně	Dopisní a balíkové zásilky s nebezpečným obsahem
Výhrůžky napadení Hlavního dispečerského pracoviště	Použití otravných prostředků
Výhrůžky napadení Elektrické stanice a stálé služby	Zničení nebo vyřazení technologických prostorů pro zpracování a přenos dat
Výhrůžky - ostatní	Zničení nebo vyřazení pracoviště stálé služby
Vydírání zaměstnanců	Zničení nebo vyřazení dispečerského pracoviště
Držení rukojmí	

Tabulka 28 - Lidský faktor – terorismus

Logické hrozby	
Falšování uživatelské identity identifikovatelnými osobami	Neoprávněné použití aplikace
Falšování uživatelské identity smluvními poskytovateli služeb	Zavedení destruktivních a škodlivých programů
Falšování uživatelské identity cizími osobami	Zneužití systémových prostředků

Tabulka 29 - Logické hrozby

Komunikační hrozby	
Infiltrace komunikace	Selhání komunikace
Zachycení komunikace	Začlenění škodlivých programů
Manipulace komunikace	Chybné směrování
Odmítnutí odpovědnosti	

Tabulka 30 - Komunikační hrozby

Závady zařízení	
Technická závada počítače	Technická závada síťového rozhraní
Technická závada paměťového zařízení	Technická závada síťové služby
Technická závada tiskového zařízení	Selhání napájení
Technická závada síťového distribučního prvku	Selhání klimatizace
Technická závada síťové brány	Selhání systémového nebo síťového programového vybavení
Technická závada počítače pro řízení / správu sítě	Selhání aplikačního programového vybavení

Tabulka 31 - Závady zařízení

Chyby	
Provozní chyba	Chyba úpravy programového vybavení
Chyba údržby technického vybavení	Chyba uživatele

Tabulka 32 - Chyby

Fyzické hrozby	
Požár	Krádež provedená cizími osobami
Poškození vodou	Úmyslné poškození identifikovatelnými osobami
Přírodní katastrofa	Úmyslné poškození cizími osobami
Nedostatek personálu	Terorismus
Krádež provedená identifikovatelnými osobami	

Tabulka 33 - Fyzické hrozby

6.2 Příloha 2 - Analýza a hodnocení významu rizik pro stanovenou oblast aktiv – praktický příklad,

Analýza rizik realizovaná na základě definovaného katalogu hrozeb specifického pro oblast výroby, přenosu a distribuce elektrické energie dotazníkovým setřením generovala parametry pro jednotlivé složky rizika.

Skupina hrozeb	Hrozby	Bodová hodnota hrozby 0-5	Bodová hodnota aktiva 0-5	Bodová hodnota zranitelnosti 0-5	Celkové riziko
Lidský faktor - terorismus	Zničení nebo vyřazení technologických prostorů pro zpracování a přenos dat	2 x	4 x	4 =	**32**
	Zničení nebo vyřazení dispečerského pracoviště	2 x	5 x	5 =	**50**

Tabulka 34 - Praktický rámec hodnocení rizika

Pro lepší orientaci uvádíme tabulku hodnocení:

Bodová hodnota	Hodnota aktiva	Hodnota hrozby	Hodnota zranitelnosti
0	Žádná nebo nehodnocena	Nepravděpodobná nebo nehodnocená	Žádná
1	Nízká	Velmi málo pravděpodobná	Nízká
2	Málo významná	Málo pravděpodobná	Málo významná
3	Střední	Středně pravděpodobná	Střední
4	Vysoká	Značně pravděpodobná	Vysoká
5	Velmi vysoká	Vysoce pravděpodobná až jistá	Velmi vysoká

Tabulka 35 - Hodnocení složek rizika

Z toho vyplývá:
Bodová hodnota hrozby H (Zničení nebo vyřazení dispečerského pracoviště) byla hodnocená na úrovni „Málo pravděpodobná“ proto H – 2 body
Bodová hodnota aktiva A (Tepelné elektrárny a teplárny) byla hodnocena jako „Velmi vysoká“ proto A – 5 bodů
Bodová hodnota zranitelnosti Z byla hodnocena jako „Velmi vysoká“ proto Z – 5 bodů

Hodnota rizika R se potom = H x A x Z = 2 x 5 x 5 = 50 co je hodnota spadající do žluté škály (tabulka 2.3.2.4) výsledného rizika a pro grafické zobrazení na základě předešlých tabulek je mu přiřazena hodnota 1,5,(tabulka 2.3.2.5) což se projeví v grafickém znázornění rizika.

6.3 Příloha 3 - KARS – praktický příklad

Příklad 1 – výpočet koeficientů aktivity a pasivity

Po doplnění tabulky souvztažnosti pro riziko pád stromu měla horizontální osa následující parametry:

	Ind.	1	2	3	4	5	6	7	8	9	10	
Pád stromu		0	0	x	0	0	0	0	0	1	1	0,22

Tabulka 36 - Vyjádření koeficientu aktivity

Kde v posledním sloupci je vyjádřen koeficient aktivity pomocí vztahu:

$$K_A R_i = \frac{\sum R_i}{x-1} = \frac{2}{10-1} = 0{,}22$$

Tabulka souvztažnosti pro hrozbu pád stromu měla vertikální osa tyto parametry:

Ind.	Pád stromu
1	0
2	1
3	x
4	0
5	0
6	0
7	0
8	0
9	0
10	0
	0,11

Tabulka 37 - Vyjádření koeficientu pasivity

Kde v spodním řádku je vyjádřen koeficient pasivity pomocí vztahu:

$$K_P R_i = \frac{\sum R_i}{x-1} = \frac{1}{10-1} = 0{,}11$$

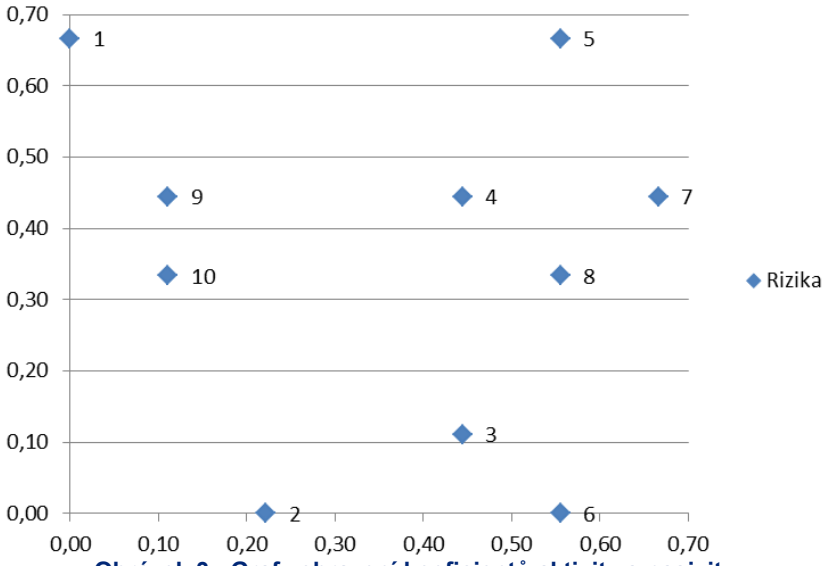
Příklad 2 – vytvoření tabulky koeficientů aktivity a pasivity a jejich zakreslení do grafu

Po vyjádření koeficientů pro všechny hrozby specifické pro skupinu aktiv vedení byla vytvořena tabulka s těmito parametry:

Riziko		1	2	3	4	5	6	7	8	9	10
Koef. Aktivity		0,00	0,22	0,44	0,44	0,56	0,56	0,67	0,56	0,11	0,11
Koef. Pasivity		0,67	0,00	0,11	0,44	0,67	0,00	0,44	0,33	0,44	0,33

Tabulka 38 - Vyjádření a popis koeficientů aktivity a pasivity

Následně byly tyto hodnoty zakresleny do grafu, který v konečném důsledku umožňuje určit nejvýznamnější rizika z pohledu jejích potenciálu (vysoký koeficient aktivity a pasivity).



Obrázek 3 - Graf zobrazení koeficientů aktivity a pasivity

Příklad 3 – rozdělení grafu do segmentů

Máme již definovanou tabulku s koeficienty aktivity a pasivity:

Riziko		1	2	3	4	5	6	7	8	9	10
Koef. Aktivity		0,00	0,22	0,44	0,44	0,56	0,56	0,67	0,56	0,11	0,11
Koef. Pasivity		0,67	0,00	0,11	0,44	0,67	0,00	0,44	0,33	0,44	0,33

Tabulka 39 - Koeficienty aktivity a pasivity

Z této tabulky si vyjádříme maximální a minimální hodnoty pro jednotlivé koeficienty:

K_{Amax} *=0,67*
K_{Amin} *=0,11 – pro větší přesnost se počítají hodnoty mimo 0*

K_{Pmax} *=0,67*
K_{Pmin} *=0,11 – pro větší přesnost se počítají hodnoty mimo 0*

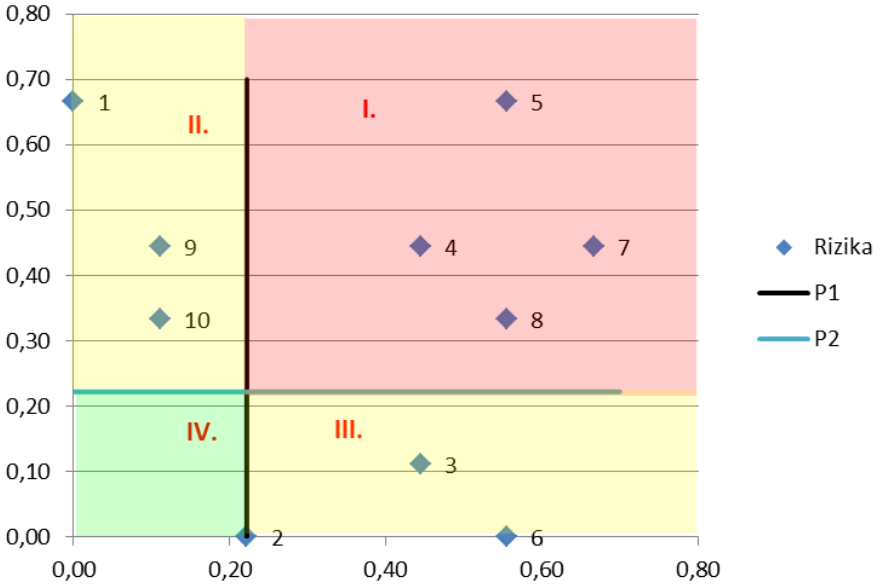
Dosadíme do vztahu pro výpočet P1 a P2:

$$P_1 = K_{A\max} - \frac{(K_{A\max} - K_{A\min})}{100} * 80 = 0{,}67 - \frac{(0{,}67 - 0{,}11)}{100} * 80 = 0{,}22$$

$$P_2 = K_{P\max} - \frac{(K_{P\max} - K_{P\min})}{100} * 80 = 0{,}67 - \frac{(0{,}67 - 0{,}11)}{100} * 80 = 0{,}22$$

Následně jsou přímky implementovány do grafu a rozdělují nám rizika do 4. segmentů, které vyjadřují míru rizikovosti:

1. *I. Segment – Primárně významná rizika - nejvyšší koeficient aktivity a zároveň pasivity*
2. *II. a III. Segment - Sekundárně významná rizika – vysoké koeficienty aktivity nebo pasivity*
3. *IV. Segment – Terciárně významná rizika – nízká úroveň koeficientů aktivity a zároveň pasivity*



Obrázek 4 - Graf souvztažnosti rizik dle koeficientů aktivity a pasivity

Z takto rozděleného grafu následně vyplývá že:

1. *Primárně významná rizika jsou: 4,5,7,8*
2. *Sekundárně významná rizika jsou: 1,2,3,6,9,10*

6.4 Příloha 4 - Stanovení požadavků na systém řízení ochrany kritické infrastruktury - systémy fyzické ochrany

6.4.1 Mechanické zábranné prostředky – perimetr areálu

Parametry FO		Parametry lokality - areálu, objektu - budovy, prostoru (LOP)	Technické, režimové a organizační požadavky na parametry FO v LOP
Perimetr areálu	Vnější oplocení	Konstrukce (mechanická odolnost)	kategorie "A" [1]
		Celková výška (vč. podhrabové přepážky nad terénem a mechanické zábrany na koruně)	min. 230 cm nad terénem
		Podhrabová deska	min. 10 cm nad terén min. 10 cm pod terén
		Mechanická zábrana na koruně	jednostranný nebo dvoustranný bavolet [2]
		Udržované pásmo (odstranění náletu)	min. 120 cm (na obě strany) [3]
	Vstupy (vstupní branka)	Způsob provedení vstupních branek	ručně otvíravá [4]
		Konstrukce (mechanická odolnost)	shodná s kategorií "A" konstrukce oplocení
		Celková výška (vč. mechanické zábrany na koruně)	min. 230 cm nad terénem
		Podhrabová deska - zpevněný povrch	min. 10 cm pod terén [5]
		Mechanická zábrana na koruně	jednostranný bavolet [2]
		Uzamykací systém nebo visací zámek	bezpečnostní třída 3 [6]
	Vjezdy (vjezdová a vlečková brána)	Způsob provedení hlavní vjezdové brány	s elektromotorickým pohonem [7]
		Způsob provedení ostatních vjezdových brán	ručně otvíravá [5]
		Konstrukce (mechanická odolnost)	shodná s kategorií "A" konstrukce oplocení
		Celková výška (vč. mechanické zábrany na koruně)	min. 230 cm nad terénem
		Podhrabová deska - zpevněný povrch	min. 10 cm pod terén [5]
		Mechanická zábrana na koruně	jednostranný bavolet [2]
		Uzamykací systém nebo visací zámek	neinstaluje se u brány s el. Pohonem, bezpečnostní třída 3 u brány ručně otvíravé [7]
	Budovy v perimetru	Pochůznou střechu budovy stejně vysoké nebo nižší než venkovní oplocení	prostředky MZP
	Ostatní prostupy	Funkční mříže	ano [8]
		Uzamykací systém nebo visací zámek	bezpečnostní třída 3 [6]

Tabulka 40 - Požadavky na MZP – perimetr areálu

6.4.1.1 Kvalitativní parametry MZS - perimetr areálu

Číslo požadavku	Popis požadavku
[1]	- oplocení musí být sestaveno z plotových dílců, sloupků, - veškeré kovové díly v pozinkované struktuře, opatřené povrchovou ochranou z PVC (vypalovaný polyester např. fluidní metodou), vyjma žiletkového drátu. Oka budou provařována z důvodu uzemnění oplocení. Systém oplocení bude opatřen přípravkem pro uchycení zemnících pásků, - osová rozteč mezi jednotlivými sloupky nesmí být delší než 255 cm, **- plotové dílce o velikosti oka max. 200 X 55 mm:** - průměr drátu: **Ø horizontálního drátu nesmí být menší než 8 mm,** **Ø vertikálního drátu nesmí být menší než 6 mm,** Nebo **- plotové dílce o velikosti oka max. 100 X 55 mm:** průměr drátu: **Ø horizontálního drátu nesmí být menší než 6 mm,** **Ø vertikálního drátu nesmí být menší než 5 mm,** -sloupky musí být o Ø 60 mm nebo podobný rozměr např. 70X45, stěna sloupku nesmí být menší než 1,5 mm, plus pozinkování a PVC ochrana, -plotové dílce musí být uchyceny přímo do sloupku tak, aby bylo vyloučeno jejich vysunutí nebo jejich demontáž, - sloupky musí být vsazeny do země a spojeny z boku s opěrnými stěnami podhrabové desky min. čtyřmi kotvami nebo jinou obdobnou metodou (stabilizační držáky), aby nebylo možné oplocení demontovat. Základy budou z prefabrikovaných dílců, - životnost oplocení bez údržby, nesmí být nižší než 15 roků a musí být doložena Certifikátem VTÚO Brno nebo jiným akreditovaným ústavem. Nejlépe v ČR, nebo v českém jazyce, - mechanická odolnost musí být dodavatelem stanovena pevností v tahu a to min. odolnost proti tahu 400/550 N/mm², prodloužení max. 15 %, 40 g zinku / m². Doloženo certifikátem.
[2]	- jednostranný bavolet, osazený třemi řadami žiletkového drátu nebo dvoustranný bavolet osazený žiletkovou spirálou.
[3]	- udržované pásmo (odstraňování náletu) 120 cm po obou stranách vnějšího oplocení vybraného objektu, které zabrání v prorůstání vegetace a náletových dřevin oplocením, umožní se tím snadné odhalení poškození oplocení a také se tím znemožní možnost úkrytu případnému narušiteli.
[4]	- mezera mezi spodní hranou vstupní branky a povrchem příjezdové komunikace nesmí umožnit podlezení ani podhrabaní případným narušitelem ani podlezení drobného zvířectva.
[5]	- mezera mezi spodní hranou vstupní branky a vjezdové brány a zpevněným povrchem příjezdové komunikace nesmí umožnit podlezení ani podhrabaní případným narušitelem a nesmí umožnit podlezení drobného zvířectva.
[6]	- dle ČSN EN 12320. **- bezpečnostní uzamykací systém** - je tvořen bezpečnostním (zadlabacím) zámkem, bezpečnostní cylindrickou vložkou a bezpečnostním kováním. Vložka nebo kování musí chránit zámek proti odvrtání. **- bezpečnostní visací zámek** - je tvořen tvrzeným třmenem, cylindrickou vložkou nebo uzamykacím mechanismem odolným proti vyhmatání.
[7]	**- pohon posuvné vjezdové brány** - je navržen tak, aby bylo zamezeno možnému otevření brány (silou) bez použití identifikačního prostředku. - Dle ČSN EN 1627. **- bezpečnostní uzamykací systém** - je tvořen bezpečnostním (zadlabacím) zámkem, bezpečnostní cylindrickou vložkou a bezpečnostním kováním. Vložka nebo kování musí chránit zámek proti odvrtání. **- bezpečnostní visací zámek** - je tvořen tvrzeným třmenem, cylindrickou vložkou nebo uzamykacím mechanismem odolným proto vyhmatání.
[8]	- Funkční mříž musí splňovat požadavky bezpečnostní třídy 3 podle normy ČSN EN 1627.

Tabulka 41 - Kvalitativní požadavky na MZP – perimetr areálu

6.4.2 Mechanické zábranné prostředky – vnější prostory

Parametry FO		Parametry lokality - areálu, objektu - budovy, prostoru (LOP)	Technické, režimové a organizační požadavky na parametry FO v LOP
Vnější prostory	Oblast MZP	Venkovní stanoviště silového en. zařízení	v případě nemožnosti realizovat technické požadavky parametrů vnějšího oplocení perimetru objektu, realizovat tyto u venkovního stanoviště silového en. zařízení.
		Odstavné plochy vně objektu s uloženým majetkem (vozidla nebo materiál)	realizovat dle požadavku vlastníka [1]
		Vstupy do průchozích kabelových kanálů	realizovat dle požadavku vlastníka

Tabulka 42 - Požadavky na MZP – vnější prostory

6.4.2.1 Kvalitativní parametry MZS - vnější prostor

Číslo požadavku	Popis požadavku
[1]	- zabezpečuje se STO ve vazbě na hodnotu uloženého materiálu, resp. hodnoty parkujících dopravních a mechanizačních prostředků

Tabulka 43 - Kvalitativní požadavky na MZP – vnější prostory

6.4.3 Mechanické zábranné prostředky – vnitřní prostory a prostory budov

Parametry FO		Parametry lokality - areálu, objektu - budovy, prostoru (LOP)	Technické, režimové a organizační požadavky na parametry FO v LOP
Vnitřní prostory a budovy	Oblast MZP	Vstupní (venkovní) dveře a vrata v plášti budovy vč. nouzových východů a vstupů (do/z vnitřního prostoru budovy) z průchozích nebo průlezných kabelových kanálů, resp. prostorů v PP budovy (konstrukce - mechanická odolnost)	dveře a vrata podle stanovených požadavků [1]
		Uzamykací systém nebo visací zámek ve vstupních (venkovních) dveřích a vratech do budovy	bezpečnostní třída 3 [2]
		Samouzavírací mechanismus na hlavních vstupních (venkovních) dveřích do budovy	ano [3]
		Prosklené části (dveře, okna) v plášti budovy, které jsou níže než 230 cm nad okolním terénem	funkční mříže nebo bezpečnostní fólie nebo bezpečnostní zasklení [4]/ realizovat dle požadavku vlastníka
		Prosklené části (sklepní okna) v plášti budovy, které jsou pod úrovní okolního terénu, tzv. "anglický dvorek"	funkční mříže nebo bezpečnostní fólie nebo bezpečnostní zasklení [4]/ realizovat dle požadavku vlastníka
		Další technické otvory v plášti budovy (s plochou větší než 600 cm2, které jsou níže než 230 cm nad okolním terénem nebo 120 cm od přístupové trasy)	funkční mříže [4]/ realizovat dle požadavku vlastníka
		Pevné žebříky na plášti budovy vyúsťující na střechu	funkční mříž na úrovni střechy zabezpečená visacím zámkem v BT 3 [5]/ realizovat dle požadavku vlastníka

Tabulka 44 - Požadavky na MZP – vnitřní prostory a prostory budov

6.4.3.1 Kvalitativní parametry MZS - vnitřní prostory a prostory budov

Číslo požadavku	Popis požadavku
[1]	- **plné dveře, vrata**, vjezdy (dále jen dveře) - musí být tuhé a pevné konstrukce, zhotovené z materiálu odolného proti vloupání (dřevo, plast, kov a jejich kombinace) o minimální tloušťce 40 mm.; - je-li výplň dveří kovová, musí být zhotovená z ocelového plechu o min. tloušťce 1 mm. - **prosklené dveře** - musí být, v jejich prosklených částech, zabezpečeny funkční mříží nebo bezpečnostní fólii nebo bezpečnostním zasklením nebo funkčním PZS. - **dvoukřídlé dveře** musí být zajištěny tak, aby obě křídla měla stejnou hodnotu odporu jako dveře jednokřídlé. Musí být zabezpečeny proti vyháčkování (pevné zástrče na neotvíraném křídle dveří, které jsou zajištěny šroubem s maticí nebo visacím zámkem, instalace příčné závory, instalace vzpěry neotvíravého křídla dveří). - **vrata** - musí být dostatečně tuhé a pevné konstrukce, zhotovené z plného plechu o min. tloušťce 3 mm, s rámem z ocelového profilu o min. tloušťce 5 mm, odolná proti vysazení a vyražení, s izolací. - **dvoukřídlé dveře** musí být zajištěny tak, aby obě křídla měla stejnou hodnotu odporu jako dveře jednokřídlé. Musí být zabezpečeny proti vyháčkování (pevné zástrče na neotvíraném křídle dveří, které jsou zajištěny šroubem s maticí nebo visacím zámkem, instalace příčné závory, instalace vzpěry neotvíravého křídla dveří). - **funkční mříž** musí splňovat požadavky bezpečnostní třídy 3 podle normy ČSN EN 1627. - **bezpečnostní zasklení** - vrstvené sklo nebo sklo s drátěnou vložkou musí vykazovat kategorii odolnosti min. třídy P5A podle ČSN EN 356, doloženo certifikátem. - **bezpečnostní fólie** - musí být instalována na skle s min. tloušťkou 4 mm. Po montáži fólie na sklo, musí sklo vykazovat kategorii odolnosti min. třídy P5A podle ČSN EN 356, doloženo certifikátem. Fólie musí být nalepena na vnitřní stranu skla a musí zasahovat až na jeho okraj.
[2]	- dle ČSN EN 1627. - **bezpečnostní uzamykací systém** - je tvořen bezpečnostním (zadlabacím) zámkem, bezpečnostní cylindrickou vložkou a bezpečnostním kováním. - **vložka** nebo kování musí chránit zámek proti odvrtání. - **bezpečnostní visací zámek** - je tvořen tvrzeným třmenem, cylindrickou vložkou nebo uzamykacím mechanismem odolným proto vyhmatání.
[3]	- další vstupy do budovy vybavit samouzavíracím mechanismem dle požadavku vlastníka nebo uživatele objektu
[4]	- **funkční mříž** musí splňovat požadavky bezpečnostní třídy 3 podle normy ČSN EN 1627. - **bezpečnostní zasklení** - vrstvené sklo nebo sklo s drátěnou vložkou musí vykazovat kategorii odolnosti min. třídy P5A podle ČSN EN 356, doloženo certifikátem. - **bezpečnostní fólie** - musí být instalována na skle s min. tloušťkou 4 mm. Po montáži fólie na sklo, musí sklo vykazovat kategorii odolnosti min. třídy P5A podle ČSN EN 356, doloženo certifikátem. Fólie musí být nalepena na vnitřní stranu skla a musí zasahovat až na jeho okraj.
[5]	- **funkční mříž** musí splňovat požadavky bezpečnostní třídy 3 podle normy ČSN EN 1627. - **bezpečnostní uzamykací systém** - je tvořen bezpečnostním (zadlabacím) zámkem, bezpečnostní cylindrickou vložkou a bezpečnostním kováním. - **vložka** nebo kování musí chránit zámek proti odvrtání. - **bezpečnostní visací zámek** - je tvořen tvrzeným třmenem, cylindrickou vložkou nebo uzamykacím mechanismem odolným proti vyhmatání.

Tabulka 45 - Kvalitativní požadavky na MZP – vnitřní prostory a prostory budov

6.4.4 PZTS, CCTV, SKV, PPSZ – Perimetr areálu

Parametry FO		Parametry lokality - areálu, objektu - budovy, prostoru (LOP)	Technické, režimové a organizační požadavky na parametry FO v LOP
Perimetr areálu	Vnější oplocení	PZTS - perimetrická ochrana (PDS v oplocení nebo PDS podél oplocení uvnitř areálu)	ne nadstandard [1]
		Systém CCTV (s digitálním záznamem obrazového signálu)	ne nadstandard [1]
		Bezpečnostní osvětlení	ne nadstandard [1]
	Vstupy (vstupní branka)	Samouzavírací mechanismus (např. BRANO) se signalizací stavu	ano/ realizovat dle požadavku vlastníka
		Signalizace stavu otevření (v PZTS)	ano [2]/ realizovat dle požadavku vlastníka
		Evidence vstupu (v PZTS nebo SKV)	ano [3]
		Monitorování a sledování vstupu (systém CCTV s digitálním záznamem obrazového signálu)	ano [4]
		Přenos stavů PZTS, SKV, CCTV na pracoviště en. dispečinku	ano [5]
		Přenos stavů PZTS, SKV, CCTV na dohledové pracoviště	ano
		Osvětlení vstupních branek	ano [6]
	Vjezdy (vjezdová a vlečková brána)	Světelná signalizace otvírání u hlavní vjezdové brány (MAJÁK - oranžová barva)	ano/ realizovat dle požadavku vlastníka
		Signalizace stavu otevření hlavní vjezdové brány (v PZTS)	ano [2]
		Evidence vstupu / vjezdu u hlavní vjezdové brány (v PZTS nebo SKV)	ano [7]
		Monitorování a sledování vstupu / vjezdu u hlavní vjezdové brány (systém CCTV s digitálním záznamem obrazového signálu)	ano [4]
		Přenos stavů PZTS, SKV, CCTV na pracoviště en. dispečinku	ano [5]
		Přenos stavů PZTS, SKV, CCTV na dohledové pracoviště	ano
		Osvětlení vjezdových brán	ano [6]

Tabulka 46 - Požadavky na PZTS, CCTV, SKV, PPSZ – Perimetr areálu

6.4.4.1 Kvalitativní parametry PZTS, CCTV, SKV, PPSZ – Perimetr areálu

Číslo požadavku	Popis požadavku
[1]	- dle požadavků vlastníka objektu
[2]	- MK stupně zabezpečení 3 - střední až vysoké riziko dle ČSN EN řady 50 131.
[3]	- ovládacím prvkem je oboustranný bezkontaktní snímač identifikačních prostředků. - ovládacím prostředkem je karta. - evidence je součástí PZS.
[4]	- monitorovat kamerami venkovního sledovacího systému CCTV s digitálním záznamem obrazového signálu (dle ČSN EN 50 132-7) a to: - venkovní pevné barevné digitální kamery s vysokým rozlišením a citlivostí a s možností přepnutí do ČB módu v provedení „antivandal“, instalované na exponovaných místech na základě provedených kamerových zkoušek. - přenos videosignálu v digitalizované formě po datové síti LAN realizovat na dohledové pracoviště.

[5]	- přenos pouze stavů PZTS.
[6]	- pochůzkové osvětlení uvnitř perimetru objektu, zaměřené na osvětlení hlavního vstupu a vjezdu a v prostoru kolem budovy společných provozů.
[7]	- ovládacím prvkem jsou bezkontaktní snímače identifikačních prostředků umístěné na vjezdu a výjezdu. - ovládacím prostředkem je karta, dálkový ovládač, mobilní telefon. - evidence je součástí PZTS.

Tabulka 47 - Kvalitativní požadavky na PZTS, CCTV, SKV, PPSZ – Perimetr areálu

6.4.5 PZTS, CCTV, SKV, PPSZ – Vnější prostory

Parametry FO		Parametry lokality - areálu, objektu - budovy, prostoru (LOP)	Technické, režimové a organizační požadavky na parametry FO v LOP
Vnější prostory	Oblast PZTS	Odstavné plochy vně objektu s uloženým majetkem (vozidla nebo materiál)	realizovat dle požadavku vlastníka [1
		Vstupy do průchozích kabelových kanálů uvnitř objektu	nerealizuje se PZS
	Oblast CCTV	Monitorování a sledování venkovního stanoviště silového zařízení uvnitř objektu	ne/ nadstandard [2]
		Monitorování a sledování odstavné plochy vně objektu s uloženým majetkem (vozidla nebo materiál)	realizovat dle požadavků vlastníka
		Monitorování a sledování vstupů do průchozích kabelových kanálů uvnitř objektu	realizovat dle požadavků vlastníka
	Oblast SKV	Evidence vstupu ve venkovních prostorách objektu (v PZS nebo SKV)	nerealizuje se SKV
	Oblast PPSZ	Přenos poplachových a jiných funkčních stavů PZS na energetický dispečink	realizovat dle požadavků vlastníka/ řídicí systém MKD nebo datová síť LAN [3]
		Přenos poplachových a jiných funkčních stavů PZS na regionální dohledové pracoviště	realizovat dle požadavků vlastníka/ datová síť LAN nebo GSM [4]

Tabulka 48 - Požadavky na PZTS, CCTV, SKV, PPSZ – Vnější prostory

6.4.5.1 Kvalitativní parametry PZTS, CCTV, SKV, PPSZ – Vnější prostory

Číslo požadavku	Popis požadavku
[1]	- zabezpečuje se STO ve vazbě na hodnotu uloženého materiálu, resp. hodnoty parkujících dopravních a mechanizačních prostředků
[2]	-dle požadavků vlastníka objektu - monitorovat kamerami venkovního sledovacího systému CCTV s digitálním záznamem obrazového signálu (dle ČSN EN 50 132-7) a to: - venkovní pevné barevné digitální kamery s vysokým rozlišením a citlivostí a s možností přepnutí do ČB módu v provedení antivandal, instalované na exponovaných místech na základě provedených kamerových zkoušek. - přenos videosignálu v digitalizované formě po datové síti LAN realizovat na dohledové pracoviště.
[3]	- na dispečerské pracoviště realizovat přenos stavu PZTS v rozsahu min. signalizace vyhlášení poplachového stavu a informace o aktivním, resp. neaktivním stavu PZTS.
[4]	- optickou a akustickou signalizaci jednotlivých stavů PZTS realizovat prostřednictvím přenosového zařízení na dohledové pracoviště

Tabulka 49 - Kvalitativní požadavky na PZTS, CCTV, SKV, PPSZ – Vnější prostory

6.4.6 PZTS, CCTV, SKV, PPSZ – Vnitřní prostory a prostory budov

Parametry FO		Parametry lokality - areálu, objektu - budovy, prostoru (LOP)	Technické, režimové a organizační požadavky na parametry FO v LOP
Vnitřní prostory a budovy	Oblast PZTS	Vstupní (venkovní) dveře a vrata v plášti budovy vč. nouzových východů a vstupů (do/z vnitřního prostoru budovy) z průchozích nebo průlezných kabelových kanálů, resp. prostorů v PP budovy	realizovat dle požadavků vlastníka /prvky plášťové ochrany stupně zabezpečení 3 [1]
		Prosklené části (dveře, okna) v plášti budovy	realizovat dle požadavků vlastníka /prvky plášťové ochrany stupně zabezpečení 3 do 500 cm nad terén [2]
		Prosklené části (sklepní okna) v plášti budovy, které jsou pod úrovní okolního terénu, tzv. "anglický dvorek"	realizovat dle požadavků vlastníka /prvky plášťové ochrany stupně zabezpečení 3 [3]
		Prosklené části (dveře, okna) v plášti budovy přístupné z dosažitelných míst (pochůzné římsy a střechy, žebříky, balkony)	realizovat dle požadavků vlastníka / prvky plášťové ochrany stupně zabezpečení 3nad 500 cm nad terén [3]
		Další technické otvory v plášti budovy (s plochou větší než 600 cm2, které jsou níže než je stanovená výška nad okolním terénem nebo 120 cm od přístupové trasy)	realizovat dle požadavků vlastníka / prvky plášťové nebo prostorové ochrany stupně zabezpečení 3 do 500 cm nad terén [4]
		Pevné žebříky na plášti budovy vyúsťující na střechu	realizovat dle požadavků vlastníka / prvky venkovní prostorové ochrany stupně zabezpečení 3 [5]
		Vyústění průchozího nebo průlezného kabelového kanálu (do/z vnitřního prostoru budovy)	realizovat dle požadavků vlastníka / prvky prostorové ochrany stupně zabezpečení 3 [6]
		Vyústění nouzového vylezu STOÚ (do/z vnitřního prostoru budovy)	realizovat dle požadavků vlastníka / prvky prostorové ochrany stupně zabezpečení 3 [7]
		Vstupní (vnitřní) dveře do prostorů, resp. místností související s provozem objektu	realizovat dle požadavků vlastníka / prvky plášťové ochrany stupně zabezpečení 3 [1]
		Prostory, resp. místnosti související s provozem objektu	realizovat dle požadavků vlastníka / prvky prostorové ochrany stupně zabezpečení 3 [8]
		Prostory, resp. místnosti související s provozem (řízením) objektu a nepřetržitou přítomností osob (stálá služba)	tísňový systém
		Vnitřní prostory u vstupních dveří do budovy (zádveří) a další společné prostory (chodby, schodiště)	realizovat dle požadavků vlastníka / prvky prostorové ochrany stupně zabezpečení 3 [9]
		Ostatní prostory nebo místnosti v budově na úrovni 1 NP budovy	realizovat dle požadavků vlastníka / prvky prostorové ochrany stupně zabezpečení 3 [9]
		Prostor nebo místnost s instalovanou ústřednou PZTS	realizovat dle požadavků vlastníka / prvky plášťové a prostorové ochrany stupně zabezpečení 3 [10]
	Oblast CCTV	Monitorování a sledování vstupů do budovy, pláště budovy a vybraných vnitřních prostor budovy systémem CCTV (s digitálním záznamem obrazového signálu)	ne nadstandard [11]/ realizovat dle požadavků vlastníka
	Oblast SKV	evidence vstupu do budovy (v PZTS nebo SKV)	realizovat dle požadavků vlastníka / ano [12]
		evidence vstupu do vybraných prostor nebo místnosti souvisejících s provozem objektu (v PZTS nebo SKV)	ano [12]
	Oblast PPSZ	přenos poplachových a jiných funkčních stavů PZTS na energetický dispečink	realizovat dle požadavků vlastníka / řídicí systém MKD nebo datová síť LAN [13]
		přenos poplachových a jiných funkčních stavů PZTS na regionální dohledové pracoviště	realizovat dle požadavků vlastníka / datová síť LAN nebo GSM, [14]

Tabulka 50 - Požadavky na PZTS, CCTV, SKV, PPSZ – Vnitřní prostory a prostory budov

6.4.6.1 Kvalitativní parametry PZTS, CCTV, SKV, PPSZ – Vnitřní prostory a prostory budov

Číslo požadavku	Popis požadavku
[1]	- MK dle ČSN EN řady 50 131 stupně zabezpečení 3 - střední až vysoké riziko. - MK instalovat na všech otvíravých křídlech dveří a vrat.
[2]	- MK dle ČSN EN řady 50 131 stupně zabezpečení 3 - střední až vysoké riziko. - MK instalovat na všech otvíravých křídlech dveří a vrat. - použití prvků PZTS dle konstrukčního řešení prosklených části v plášti budovy.
[3]	- MK a DTS dle ČSN EN řady 50 131 stupně zabezpečení 3 - střední až vysoké riziko - Použití prvků PZTS dle konstrukčního řešení prosklených části v plášti budovy
[4]	- MK nebo DTS nebo PIR dle ČSN EN řady 50 131 stupně zabezpečení 3 - střední až vysoké riziko - použití prvků PZS dle stavebně technického řešení technického otvoru.
[5]	- PIR dle ČSN EN řady 50 131 stupně zabezpečení 3 - střední až vysoké riziko. - instalovat na pochůzné střeše budovy v místě vyústění žebříku.
[6]	- PIR dle ČSN EN řady 50 131 stupně zabezpečení 3 - střední až vysoké riziko. - instalovat před vstupem do vnitřního prostoru budovy (uvnitř kabelového prostoru).
[7]	- PIR dle ČSN EN řady 50 131 stupně zabezpečení 3 - střední až vysoké riziko. - instalovat uvnitř místnosti před vstupem do nouzového vylezu.
[8]	- PIR dle ČSN EN řady 50 131 stupně zabezpečení 3 - střední až vysoké riziko. - instalovat před vstupem do vnitřního prostoru (energetický dispečink, systém kontroly řízení apod.).
[9]	- PIR dle ČSN EN řady 50 131 stupně zabezpečení 3 - střední až vysoké riziko.
[10]	- MK, DTS a PIR dle ČSN EN řady 50 131 stupně zabezpečení 3 - střední až vysoké riziko. - MK instalovat na všech otvíravých křídlech dveří a vrat.
[11]	-dle požadavků vlastníka objektu - monitorovat kamerami venkovního sledovacího systému CCTV s digitálním záznamem obrazového signálu (dle ČSN EN 50 132-7) a to: - venkovní pevné barevné digitální kamery s vysokým rozlišením a citlivostí a s možností přepnutí do ČB módu v provedení antivandal, instalované na exponovaných místech na základě provedených kamerových zkoušek. - přenos videosignálu v digitalizované formě po datové síti LAN realizovat na dohledové pracoviště.
[12]	- ovládacími prostředky prvků plášťové a prostorové ochrany PZTS jsou bezkontaktní identifikační karty typu Mifare, případně karty jiného typu užívané v oblasti výroby, přenosu a distribuce el. energie - ovládacími prvky jsou bezkontaktní snímače identifikačních prostředků, které musí být kompatibilní s technologií používané karty. Instalují se na plášti budovy, zabezpečené PZTS u hlavního vstupu do budovy a dále dle požadavku vlastníka objektu - kódová LCD klávesnice (uživatelská) se instaluje u vstupu do budovy společných provozů a dalších budov dle požadavku vlastníka objektu - evidence je součástí PZTS.
[13]	- na dispečerské pracoviště realizovat přenos stavu PZTS v rozsahu min. signalizace vyhlášení poplachového stavu a informace o aktivním, resp. neaktivním stavu PZTS.
[14]	- optickou a akustickou signalizaci jednotlivých stavů PZTS realizovat prostřednictvím přenosového zařízení na dohledové pracoviště.

Tabulka 51 - Kvalitativní požadavky na PZTS, CCTV, SKV, PPSZ – Vnitřní prostory a prostory budov

6.4.7 Režimová opatření

Parametry RO	Parametry lokality - areálu, objektu - budovy, prostoru (LOP)	Technické, režimové a organizační požadavky na parametry FO v LOP
Parametry vztahující se k RO	Stanovení určených vstupů pro osoby a vjezdů pro vozidla do objektu	Režimová opatření týkajících se objektu zpracovává vlastník objektu interním pracovním dokumentem (Řád fyzické ochrany) tak, aby minimálně všechny zmíněné oblasti byly pokryty.
	Stanovení rozsahu oprávnění osob pro vstup a dopravních prostředků pro vjezd do objektu	
	Režim pohybu osob, vozidel v objektu	
	Režim pohybu materiálu v objektu (vnášení, vynášení majetku)	
	Režim manipulace s klíči	
	Režim manipulace se STO	
	Řešení mimořádných událostí (bezpečnostní incidenty, teroristické výhrůžky)	

Tabulka 52 - Požadavky na režimová opatření

6.4.8 Fyzická ostraha

Parametry FOS	Parametry lokality - areálu, objektu - budovy, prostoru (LOP)	Technické, režimové a organizační požadavky na parametry FO v LOP
Parametry vztahující se k FOS	Výkon stálé služby na objektu	ne / ano [1]
	Obchůzková činnost na objektu (pravidelná nebo nepravidelná)	ne nadstandard [2]
	Strážní činnost na objektu bez instalovaného STO (pravidelná nebo nepravidelná)	realizovat dle požadavků vlastníka / ano [3]
	Obsluha STO na dohledovém pracovišti (nepřetržitě)	ano
	Vyhodnocování stavů STO a reakce na ně (průběžné)	ano [4]
	Mobilní zásah na objektu (neprodleně)	ano [5]

Tabulka 53 - Požadavky na fyzickou ostrahu

6.4.8.1 Kvalitativní parametry požadavků na fyzickou ostrahu

Číslo požadavku	Popis požadavku
[1]	- výkon stálé služby na objektu bude realizován po omezenou dobu v případě, že bude probíhat realizace celkové obnovy, resp. rekonstrukce objektu spojené s rekonstrukcí vnějšího oplocení.
[2]	- lze nadstandardně realizovat a to v případě, že se objekt nachází v bezprostřední blízkosti objektu se stálým stanovištěm fyzické ostrahy a souhlasu vlastníka objektu.
[3]	- fyzická kontrola stavu (neporušenosti) vnějšího oplocení, pláště budov v objektu. - odvrácení vzniku majetkové újmy
[4]	- spolupráce s dispečerem dispečinku, uživatelem a vlastníkem objektu, Policii ČR, HZS, apod.
[5]	- činnost zásahové skupiny na objektu při vyhlášených poplachových stavech STO (výjezdové vozidlo SBS). - odvrácení vzniku majetkové újmy a zadržení narušitele.

Tabulka 54 - Kvalitativní požadavky na fyzickou ostrahu

6.5 Příloha 5 - Stanovení požadavků na systém řízení ochrany kritické infrastruktury - Informační bezpečnost

6.5.1 Identifikace a autentizace

Oblast informační bezpečnosti	Související procesy	Požadavky na související procesy
Identifikace a autentizace	Distribuce hesla	Při distribuci hesel by měla být zajištěna jejich důvěrnost.
		Hesla by neměla být známa ani administrátorům a v případě, že tento požadavek není možné naplnit, musí systém vynutit změnu hesla před prvním přihlášením.
	Délka hesla	Za účelem ztížení dešifrování hesel, by měla hesla mít dostatečnou délku.
		Minimální doporučená délka hesla by měla být nastavena na 8 znaků (12-15 znaků pro administrátorské účty) pokud to daný informační systém umožňuje
	Komplexnost hesla	Heslo by nemělo obsahovat uživatelské jméno, ani křesní jméno/příjmení uživatele a mělo by být zabráněno generování hesla, které bylo použito v posledních 5 případech (15 v případě administrátorských účtů).
		Heslo by se mělo skládat z velkých a malých písmen a dále by mělo obsahovat číslici nebo některý ze speciálních znaků (např. lomítko).
	Použití hesla	Uživatelé by se při výběru a používání hesel měli řídit předepsanými bezpečnostními praktikami.
		Přihlašovací jméno či heslo posledního přihlášeného uživatele či nápovědy k textu přihlašovacího jména, ID či hesla se nesmí zobrazovat v přihlašovacím dialogu.
		Heslo nesmí být sdíleno s ostatními uživateli a ani ukládáno spolu se zařízením.
		Všechny účty by měly být chráněny heslem a hesla by měly být chráněna před neautorizovaným přístupem.
		Hesla by měla být uložena v zašifrované podobě pomocí dostatečně silného šifrovacího algoritmu tak, aby nebylo možné je dešifrovat.
	Četnost změny hesla	Hesla by měla být pravidelně měněna. Maximální stáří hesla by mělo být v rozmezí 30-90 dní (30 dní pro administrátorské účty)
		Minimální stáří hesla by mělo být alespoň 1 den jako prevence obcházení nastavené politiky historie hesel.
		Hesla by měla být v případě podezření na prozrazení změněna
	Identifikátory uživatelů	Všichni uživatelé by měli mít přidělený jednoznačný identifikátor (uživatelské ID) který se bude řídit interní směrnicí pro tvorbu unikátních ID.
	Sdílení účtů	Uživatelské účty musí být přiděleny všem uživatelům tak aby nedocházelo ke sdílení účtů.
		Účty nesmí být sdíleny ani v případě administrátorů.

Tabulka 55 - Požadavky na identifikaci a autentizaci

6.5.2 Řízení logického přístupu

Oblast informační bezpečnosti	Související procesy	Požadavky na související procesy
Řízení logického přístupu	Zásady řízení přístupu	Měly by být definovány požadavky a omezení týkající se řízení přístupu k informacím, které vyplývají z procesů v organizaci, z její struktury a důležitosti informačních aktiv.
		Přístup k informacím je řízen dle schválených přístupových oprávnění vlastníkem dat. Za nastavení přístupových oprávnění je odpovědný administrátor systému.
	Omezení přístupu k informacím	Přístup k datům z aplikací by měl být přidělován v souladu s celkovou politikou řízení přístupu.
	Časový limit práce pracovní stanice / heslem chráněné spořiče obrazovek	Nepoužívané pracovní stanice by měly být chráněny proti neoprávněnému použití – netýká se dispečerských systémů, za účelem kontinuální činnosti řídicích systémů
		Nastavení automatického odhlášení uživatele při nečinnosti 5-10minut - netýká se dispečerských systémů, za účelem kontinuální činnosti řídicích systémů
	Blokace defaultních účtů	Defaultní (instalační) účty by měly být zablokovány nebo přejmenovány. Pokud je systém nastaven tak, že defaultní účty/účet jsou nutné pro provoz a správu systému, doporučujeme okamžitě provést změnu hesla (viz. 6.5.1) a defaultní účty používat zejména v nouzových případech po protokolovaném vyjmutí hesla ze zapečetěné obálky v trezoru.
	Přístup k auditním záznamům	Přístup k auditním záznamům by měl být řízen (přístup musí být omezen, kontrolován a monitorován) a měl by být poskytnut v módu “read-only“.
		Veškerá činnost nad auditními záznamy je logována.

Tabulka 56 - Požadavky na řízení logického přístupu

6.5.3 Evidence událostí a audit

Oblast informační bezpečnosti	Související procesy	Požadavky na související procesy
Evidence událostí	Záznam událostí	Informační systémy, které poskytují funkcionalitu uživatelům, by měly logovat následující události vždy spolu s ID uživatele, který událost spustil: - datum a čas pokusu o přístup do systému a jeho výsledek
		- spuštění služby, funkcionality, modulu, nastavení automatických úkolů a jejich detail
		- přístup k datům a změnu či vytvoření záznamů
		- jako vhodná forma alternativy evidence je použití provozních deníků, kde evidenci provede operátor
	Doba uchovávání evidenčního deníku	Zařízení vytvářející evidenční záznamy a vytvořené záznamy by měly být chráněny proti manipulaci a neoprávněnému přístupu. Přístup musí být umožněn pouze určenému personálu.

		Personál nesmí mít přístup pro zápis anebo musí docházet ke kontinuálnímu zálohování na read-only media/zařízení která zajistí autentičnost záznamu.
Audit	Monitoring	Jedním ze základních vstupů je monitoring, který provádí aktivní záznam a komunikaci/eskalaci aktivit probíhajících na síti.
		Využití vybraných automatických nástrojům pro oblast bezpečnostních incidentů
	Pravidelné kontroly přístupových oprávnění	Přístupová práva musí být revidována vždy, když uživatel opustí organizaci nebo změní roli.
		Přístupová práva uživatelů a uživatelské účty by měly být v pravidelných intervalech kontrolovány a měla by být posuzována správnost přiřazení na základě formálních podkladů ke stavu přiřazení uživatelských účtů a jejich oprávnění (požadavkové formuláře ap.)
		Kontroly by se měly týkat všech uživatelských účtů včetně uživatelských účtů externích zaměstnanců a dodavatelů, testovacích a administrativních účtů, které umožňují přístup k síti, aplikacím a ostatním informačním zdrojům společnosti.
		Perioda provádění kontrol může záviset na důležitosti konkrétního IS, minimálně však jednou za čtvrtletí.
	Analýza evidence událostí	Musí být definovány události, které by měly podléhat revizi. Je nutné vytvořit seznam systémů podléhajících kontrole bezpečnosti (na základě analýzy rizik) a vybrat klíčové bezpečnostní události pro jednotlivé systémy, s detailními popisy řešení událostí, korelací a procesu analýzy činností (tj. centralizace logů, upozornění, stupňování, atd.).
		Administrátoři by měli revidovat tyto logy: - výkonnostní, - kapacitní, - aplikační, - dávkových prací, - stavu sítě, - zálohování.
		V rámci revize logů by měly být uvedeny tyto informace: - revidovaný log - doba provedení revize - výsledek revize (o jakou událost se jednalo a jaká korekční činnosti byly provedeny) - kdo danou revizi provedl
		Měla by být stanovena časová perioda analýzy záznamu o účtu.
		Vzniklé logy a zprávy narušení bezpečnosti na všech úrovních by měly být pravidelně kontrolovány a hodnoceny.
	Vyšetřování incidentu	Na základě revize logů by měly být identifikovány a vyšetřeny všechny systémové/bezpečnostní incidenty a zjištěné pokusy o narušení bezpečnosti.
	Řízení systémového auditu	Požadavky na audit a auditní činnosti by měly být plánovány tak, aby byla zajištěna nezávislá kontrola při minimálním narušení chodu organizace.

Tabulka 57 - Požadavky na audit

6.5.4 Integrita programového vybavení

Oblast informační bezpečnosti	Související procesy	Požadavky na související procesy
Integrita programového vybavení	Kontroly integrity programového vybavení	Mělo by se předcházet narušení integrity programového vybavení a případný výskyt narušení by měl být detekován.
	Aktualizace operačních systémů, databází a síťových komponent	Veškeré operační systémy a databáze by měly být udržovány v nejnovější verzi, která byla dodavatelem označena za stabilní. Pravidelně by mělo docházet k nahrávání bezpečnostních záplat.
		Software a firmware síťových prvků by měl být pravidelně aktualizován bezpečnostními záplatami.
	Aktualizace SW vyvíjeného na klíč	Aktualizace SW by měla probíhat řízeným způsobem na základě změnového řízení, které zahrnuje testování a akceptaci funkcionalit a systémů.

Tabulka 58 - Požadavky na integraci programového vybavení

6.5.5 Zálohování dat

Oblast informační bezpečnosti	Související procesy	Požadavky na související procesy
Zálohování	Zálohování provozu	Systém by měl být odolný proti výpadkům a v případě závady jedné jednotky (disk, databáze, aplikační sever) musí být systém schopný zajistit přechod na další jednotku (Cluster, RAID)
		Pro případ závažné havárie musí být k dispozici náhradní zařízení anebo takové služby, které umožní obnovu provozu v požadované době.
	Zálohování dat	Priorita dat určených k zálohování by měla být určena na základě klasifikace dat ze strany uživatelů systému.
		Pro účely obnovy či pozdějšího využití musí být zálohovací média dostupná v jiné lokalitě než datové centrum a zálohy musí být prováděny v takové periodě, aby v případě obnovy systému bylo možné navázat na předchozí operace a plynule pokračovat v provozu. Zálohy zároveň musí být zabezpečeny nejlépe formou uložení v trezoru s řízeným přístupem. Detailní požadavky se stanoví na základě BCP/DRP.
		Data na zálohovacích médiích musí být šifrována.
Skartace dat	Bezpečná likvidace médií	Měla by být formalizována a implementována procedura pro bezpečné zbavování se zálohovacích pásek, harddisků, USB disků a jiných médií používaných pro ukládání dat.
		Nepotřebná a nefungující média určená ke skartaci musí být vymazána (skartována) takovým způsobem, aby nemohlo dojít ke znovuobnovení dat.
	Skartace logická	Procedura bezpečného smazání dat, která popisuje metody bezpečného výmazu dat (několikanásobné přepsání, degaussing apod.).

Tabulka 59 - Požadavky na zálohování dat

6.5.6 Odolnost sítě

Oblast informační bezpečnosti	Související procesy	Požadavky na související procesy
Odolnost fyzické vrstvy sítě	Redundance síťových zařízení	Počet klíčových bodů možného selhání v návrhu sítě musí být minimalizován.
		Síťová zařízení musí být zálohována redundantními komponentami, které v případě potřeby umožní plynulý přechod na záložní vedení.
Odolnost logické vrstvy sítě	Protokoly a služby	Měla by být použita oddělena DMZ.
		Používaní služeb/komunikačních protokolů by mělo být omezeno na potřebné minimum a řádně zabezpečeno (Telnet, http, smtp FTP, TFTP, NFS, snmp) by měly být zakázány nebo zabezpečeny například pomocí SSH.
		Nepoužívané porty by měl být zablokovány.
	Šifrovaná spojení	Přihlašování k směrovačům a firewallům by mělo probíhat zašifrovaným způsobem.
		Komunikace mezi pobočkami by měla být šifrovaná.
Prevence a detekce neautorizovaných aktivit	Firewall; IDS/IPS; Proxy server	Firewall by měl být použit jako osobitý síťový prvek, ne jako součást nějakého operačního systému.
		Doporučujeme použití IDS/IPS na monitorování provozu za otevřenými porty firewallu/aktivní reagování na případný útok.
		Měl by být používán Proxy server.
	Pravomoci síťových administrátorů	Pravomoci administrátorů na různých síťových úrovních by měly být logicky odděleny.
Bezpečnost směrovacích tabulek	Zálohování směrovacích tabulek	Konfigurační nastavení by měla být pravidelně zálohována.

Tabulka 60 - Požadavky na odolnost sítě

6.5.7 Testování systému

Oblast informační bezpečnosti	Související procesy	Požadavky na související procesy
Testování systému	Testování bezpečnosti	Testování zranitelností a penetrační testování by mělo být pravidelně prováděno na kritickém programovém vybavení.
		Bezpečnostní testy by měly kontrolovat prosazení bezpečnostních požadavků poměřovaných podle daných kritérií vždy při nasazování nových či upravených funkcionalit systému.
	Testování obnovy záloh	Mělo by být prováděno pravidelné testování obnovy dat ze záloh na základě definovaného harmonogramu, které by mělo být formálně zdokumentováno.
	Testování aktualizací	Veškeré aktualizace systémů, které jsou zamýšleny k nahrání do provozu, musí být nejprve otestovány a schváleny.

Tabulka 61 - Požadavky na testování systému

6.5.8 Ochrana proti škodlivým programům

Oblast informační bezpečnosti	Související procesy	Požadavky na související procesy
Ochrana proti škodlivým programům	Opatření na ochranu proti škodlivým programům	Aplikace pro detekci škodlivých programů (antivirové programy) musí být na všech zařízeních pravidelně aktualizovány (on line) a musí mít aktuální knihovnu škodlivých programů.
		Mělo by se zvyšovat odpovídající bezpečnostní povědomí uživatelů.
		Systém by měl být pravidelně/kontinuálně kontrolován, zda v něm nepůsobí škodlivé programy.
		Nastavení antivirových programů musí být pravidelně zálohována.
	Odstranění škodlivého programového vybavení	Veškeré zjištěné škodlivé programy by měly být izolovány a odstraněny pomocí automatizovaných specializovaných nástrojů.

Tabulka 62 - Požadavky na ochranu proti škodlivým programům

6.5.9 Kontrola správy systému

Oblast informační bezpečnosti	Související procesy	Požadavky na související procesy
Kontrola správy systému	Omezení změn v komerčním balíku aplikací	Změny programového vybavení COTS (Commercial off-the-shelf) mohou být provedeny pouze způsobem, který nevyvolá následné problémy v podpoře a provozu.
	Řízení přístupu k účtům správců systému	Použití programových utilit umožňujících obejít systémová a aplikační opatření by mělo být omezeno a přísně kontrolováno.

Tabulka 63 - Požadavky na kontrolu správy systému

6.5.10 Provozní kontroly

Oblast informační bezpečnosti	Související procesy	Požadavky na související procesy
Provozní kontroly	Provozní postupy	Provozní postupy by měly pokrýt všechny činnosti administrátora.
		Veškerá práce administrátorů musí být logována a logy musí být pravidelně vyhodnocovány.
	Zálohovací logy	Zálohovací logy by měly být pravidelně kontrolovány a v případě výskytu chyby při zálohování by mělo být provedeno manuální zálohování.

Tabulka 64 - Požadavky na provozní kontroly

6.5.11 Infrastruktura veřejných klíčů

Oblast informační bezpečnosti	Související procesy	Požadavky na související procesy
Infrastruktura veřejných klíčů	Používaní certifikátů pro vybrané IS	Doporučujeme použití různých certifikátů pro šifrování a pro podepisování. Certifikáty by měly být uchovávány tak, aby nebyly přístupné neautorizovaným subjektům.
		Certifikační autorita archivuje soukromé klíče používané pro šifrování.

Tabulka 65 - Požadavky na infrastrukturu veřejných klíčů

6.5.12 Kontrola změny programového vybavení

Oblast informační bezpečnosti	Související procesy	Požadavky na související procesy
Kontrola změny programového vybavení	Nouzové opravy programového vybavení	Změny programového vybavení, které musí být provedeny bez schválení, by měly podléhat kontrole.
		Změny v systému by se měly nejprve otestovat v prostředí určeném na testování a měly by být použita nesenzitivní testovací data. V případě úspěšného průběhu testování se změna teprve může zavést do produkčního prostředí. Doporučujeme uploadovat změnu v systému mimo rush hours, neboť provádění změny může způsobit zpomalení systému.
		V případě přístupu programátorů do produkčního prostředí jsou vytvořeny přístupové účty pouze pro dobu výkonu opravy a jejich činnost by měla být logována.

Tabulka 66 - Požadavky na kontroly změny programového vybavení

6.5.13 Autorizace vzdáleného přístupu

Oblast informační bezpečnosti	Související procesy	Požadavky na související procesy
Autorizace vzdáleného přístupu mimo objekty 24/7	Autentizační služby	Autentizace uživatelů by měla být založena na platném certifikátu vydaném spolehlivou autoritou.
	Služby správy zákazníků	Aby byla zajištěna úplnost, přesnost a stálá platnost informací o uživateli, měly by být tyto informace ve stanoveném intervalu prověřeny.
	Zabezpečený vzdálený přístup	Měl by být formalizován seznam uživatelů, kteří mají vzdálený přístup do lokální sítě, a měl být omezen pro nevyhnutelné minimum.
		Vzdálený přístup by měl být zabezpečen pomocí sítě VPN s dostatečnou sílou šifry (alespoň SHA-2).

Tabulka 67 - Požadavky na autorizaci zákazníků

6.5.14 Analýza zranitelností

Oblast informační bezpečnosti	Související procesy	Požadavky na související procesy
Analýza rizik	Identifikace a hodnocení aktiv	Měla by proběhnout identifikace informačních aktiv s následným kvalitativním a kvantitativním ohodnocením.
	Identifikace a hodnocení hrozeb a zranitelností	Následné doporučujeme identifikaci druhů událostí a akcí, které mohou negativně ovlivnit hodnotu aktiv; určení slabých míst subjektu, které mohou umožnit působení hrozeb. Pak by se měla určit pravděpodobnost výskytu hrozby a míra zranitelnosti subjektu vůči dané hrozbě.
	Identifikace a hodnocení ochranných opatření	Měla by proběhnout identifikace existujících a plánovaných ochranných opatření a stanovení akceptovatelné míry rizika.

Tabulka 68 - Požadavky na analýzu zranitelností

6.5.15 Kontroly dokumentů/médií

Oblast informační bezpečnosti	Související procesy	Požadavky na související procesy
Kontroly dokumentů/médií	Uložení dokumentů/médií	Média, která nejsou používána, musí být bezpečným způsobem uložena (např. v uzamčené místnosti, zamykatelné skříně, trezory,…). Jejich uložení by mělo být evidováno a pravidelně kontrolováno.
		Mělo by být prosazováno pravidlo prázdného stolu (důvěrné dokumenty/výměnné média nesmí být ponechávány volně na stole) a pravidlo prázdné obrazovky monitoru u prostředků pro zpracovávání informací.

Tabulka 69 - Požadavky na kontrolu dokumentů/médií

6.5.16 Virtualizace

Oblast informační bezpečnosti	Související procesy	Požadavky na související procesy
Virtualizace	Řízení komunikací a řízení provozu	Všechny poskytované služby virtuálního prostředí musí být jasně vymezeny.
		Hypervisor by měl být monitorován jako prevence jeho zneužití.
		Administrátor hypervisoru nemůže mít možnost jakkoli měnit auditní záznamy.
		Všechny služby hypervisoru, jako kopírování a sdílení dat mezi OS, by měly být zakázány.
		Pro zálohování virtuálních disků všech hostů by měly být využity stejné zálohovací politiky, které platí pro nevirtualizovaná řešení.
	Řízení přístupu	Pro přístup k OS každého hosta by měla být využita unikátní autentizace.
		Přístup k nástrojům pro správu virtualizovaného prostředí by měl být řízen a monitorován.
		Pro správu hypervisoru je vyžadována vícefaktorová autentizace.
		Všechna rozhraní virtualizovaného řešení musí být bezpečně nakonfigurována.
		Nástroje pro správu virtualizovaného prostředí by měly administrátorovi umožňovat bezpečný vzdálený přístup, zálohu, obnovu, migraci a rekonfiguraci systému.
	Klasifikace a řízení aktiv	Veškerá nevyužívaná zařízení a služby by měly být odpojeny.
		Měla by existovat kontrola propojení hostujících OS s odpovídajícími fyzickými zařízeními v hostitelském systému.
		Měly by být stanoveny limity pro využívání prostředků virtuálního prostředí.
		Veškeré logy by měly být ukládány v zabezpečeném a fyzicky odděleném úložišti.

Tabulka 70 - Požadavky na virtualizaci systémů

6.5.17 Organizace bezpečnosti

Oblast informační bezpečnosti	Související procesy	Požadavky na související procesy
Organizace bezpečnosti	Infrastruktura bezpečnosti informací	Instalace zařízení pro zpracování informací musí být schválena a autorizována z technického hlediska.
		Specialisté na bezpečnost by měli spolupracovat s dalšími odborníky.
		Mělo by být pravidelně provedeno nezávislé přezkoumání stavu bezpečnosti informací.
		Měly by být jasně vymezeny odpovědnosti za bezpečnost informací.
	Bezpečnost přístupu třetích stran	Musí být důsledně řízen a monitorován přístup třetích stran k ICT aktivům.
		Smlouvy uzavírané se třetí stranou by měla pokrývat požadavky na bezpečnost.

Tabulka 71 - Požadavky na organizaci bezpečnosti

6.5.18 Plánování kapacit

Oblast informační bezpečnosti	Související procesy	Požadavky na související procesy
Plánování kapacit	Plánování kapacit programového vybavení	Z důvodu prevence selhání systému, by měly programové prostředky poskytovat pomoc při monitorování a plánování kapacity a při ověřování její dostatečnosti.
	Kontrola dostatečné kapacity	Měly by být prováděny pravidelné kontroly a monitoring dostupné kapacity.
		Plánování kapacit by mělo zahrnovat také manuální procesy při zpracování informací.
		Plánování kapacit musí být prováděno s ohledem na průměrné hodnoty výpadku systémů.
	Akceptace systému	Měla by být stanovena kritéria pro akceptaci nových informačních systémů, aktualizaci a zavádění nových verzí.

Tabulka 72 - Požadavky na plánování kapacit

6.6 Příloha 6 - Stanovení požadavků na systém řízení ochrany kritické infrastruktury - Administrativní bezpečnost a personální bezpečnost

6.6.1 Administrativní bezpečnost

	Požadavek	Popis požadavku
Administrativní bezpečnost	Odpovědnosti, povinnosti a pravomoci	- definování odpovědností, povinností a pravomocí rolím zapojeným do administrativních činností
	Označování a klasifikace dokumentů	- definování jednotného postupu označování dokumentů v listinné i elektronické podobě dle jejich klasifikace
		- definování automaticky generované značky pro označování a následnou identifikaci dokumentů
		- definování používání a označování číslem jednacím, skartačním znakem, razítkem, aj.
		- definování, kde a jakým způsobem mají být dokumenty označeny
		- definování činností a situací, kdy je možné provést změny v označení dokumentu
	Manipulace s dokumenty	- definování administrativních pomůcek (jednací protokol, manipulační kniha, kniha tisku, kniha administrativních pomůcek, kniha zápůjček aj.)
		- definování jasných požadavků na evidenci dokumentů do příslušných jednacích protokolů
		- definovaní jasných postupů pro tisk dokumentů
		- definování možných kanálů pro doručení dokumentů
		- definování podatelen a datových emailových schránek
		- definování činností pro příjem dokumentů od externích subjektů
		- definování postupů pro vkládání dokumentů do systémů (listinná a elektronická podoba)
		- definování postupů při pořízení opisu, kopie, překladu a výpisu dokumentů v listinné a elektronické podobě
		- definování podepisování dokumentů (včetně elektronických podpisů)
		- definování postupu předávání dokumentů uvnitř organizace
		- definování postupu předávání dokumentů mimo organizaci
		- definování razítek a jejich použití, evidence, likvidace
		- definování postupů pro přepravu zásilek (včetně přípravy zásilky na přepravu)
		- definování pravidel pro ukládání dokumentů (dle jejich označení, skartačních a spisových znaků) v listinné a elektronické podobě do archivu (včetně evidence úložek)
		- definování postupu zapůjčování listinných dokumentů (včetně evidence zápůjček)

		- definování postupu pro skartaci dokumentů v listinné a elektronické podobě (na jakémkoliv nosiči dokumentů - médiu)
		- definování postupu pro likvidaci dokumentů v listinné a elektronické podobě (na jakémkoliv nosiči dokumentů - médiu)
	Ztráta dokumentů a jejich nosičů - médií	- definování postupů při ztrátě dokumentů (jejich nosičů-médií)
		- definování návaznosti na právní řád (pracovněprávní vztah)
	Administrativní bezpečnosti při personálních změnách	- definování postupů a pravidel pro výkon administrativní bezpečnosti při personálních změnách

Tabulka 73 - Požadavky na administrativní bezpečnost

6.6.2 Personální bezpečnost

,

	Požadavek	Popis požadavku
Personální bezpečnost	Odpovědnosti, povinnosti a pravomoci	- definování odpovědností, povinností a pravomocí rolím zapojeným do administrativních činností
	Prověřování zaměstnanců	- definování podmínek prověření (dostupnost dvou dostatečných referencí; kontrola životopisu uchazeče; ověření vzdělání a kvalifikace; nezávislé ověření totožnosti)
		- definování postupu k prověření spolehlivosti zaměstnanců,
		- definování pravidelné kontroly práce všech zaměstnanců
		- definování postupu pro zajištění informací o soukromých poměrech, které mohou vést k chybám nebo jiným dopadům na bezpečnost (častá absence, stres, deprese, osobní a finanční problémy, změny v chování a životním stylu apod.)
	Dohody o ochraně informací	- definování postupu pro zajištění podpisu smlouvy o ochraně informací (např.: Dohody o mlčenlivosti v rámci pracovní smlouvy apod.) v případě, kdy je to nutné
	Podmínky výkonu pracovní činnosti	- definování obsahu ustanovení o ochraně informací, povinnosti oprávněných osob by měla trvat i určitou dobu po skončení pracovního poměru a měly by být popsány kroky při nedodržení podmínek
	Školení zaměstnanců	- definování povinných školení v oblasti bezpečnosti
		- definování obsahu školení – zahrnutí bezpečnostních požadavků, právní odpovědnosti a popis relevantních kontrolních mechanismů
		- evidence proškolených zaměstnanců a pravidelné proškolování
	Reakce na bezpečnostní incidenty a selhání	- definování postupů pro hlášení bezpečnostních incidentů a slabin
	Disciplinární proces	- definování postupů při porušení bezpečnostních opatření nebo nedodržení pracovních postupů organizace
	Ukončení pracovního vztahu	- definování postupů pro navrácení aktiv držených zaměstnancem, zaevidování apod. - definování postupu pro odebrání přístupových oprávnění

Tabulka 74 - Požadavky na personální bezpečnost

6.7 Příloha 7 - Stanovení požadavků na systém řízení ochrany kritické infrastruktury - krizové řízení a plánování

6.7.1 Personální struktura KŘO

Oblast KŘO – strukturální požadavky	Člen krizového týmu	Popis povinností a odpovědností
Personální struktura KŘO	**Představitel vedení pro KŘO/Styčný bezpečnostní zaměstnanec**	Řídí a koordinuje veškeré činnosti a aktivity související s ustavením, zaváděním, realizací a kontinuálním rozvojem efektivního a funkčního systému zajištění funkčnosti.
		Zajišťuje vypracování a schválení, krizových plánů, krizových plánů organizace, plánu krizové připravenosti a plánu krizové připravenosti subjektu KI a jejích aktualizaci.
		Odpovídá za koordinaci a komunikaci pro oblast ochrany kritické infrastruktury ve vztahu k státním orgánům
		Řídí přípravu krizového řízení a plánování ve společnosti.
	Manažer KŘO	Je odpovědný za metodickou podporu KŘ ve společnosti.
		Je odpovědný za vlastní zpracování plánu krizové připravenosti subjektu KI.
		Koordinuje zpracování, revizi a aktualizaci požadované dokumentace procesu KŘ, KŘO
		Shromažďuje zápisy mimořádných událostí od stupně 2 hlášené vedoucím krizového týmu případně garantem.
	Garant KŘO za úsek	Nese hlavní odpovědnost za kontinuitu a obnovu procesů příslušného úseku, které spadají do jeho působnosti.
		Poskytuje aktivní podporu při realizaci činností souvisejících s implementací KŘ, KŘO na úrovni úseku.
		Je odpovědný za vypracování konkrétních plánů (krizové plány, krizové plány organizace, plány krizové připravenosti, plány krizové připravenosti subjektu kritické infrastruktury a jejich části) a jejich pravidelné testování.
		Je odpovědný za určení konkrétního řešitele pro zpracování, pravidelnou revizi a aktualizaci PKP a PKPSKI.
		Odpovídá za pravidelné proškolování podřízených zaměstnanců a za implementaci opatření na pokrytí identifikovaných rizik.

	Řešitel	Je povinen poskytnout vstupy a součinnost při realizaci jednotlivých kroků implementace a provozování systému krizového řízení a krizového řízení organizace – analýza dopadů, hodnocení rizik, příprava a testování plánů, apod.
		Je odpovědný za vlastní zpracování, pravidelnou revizi a aktualizaci konkrétních plánů (krizové plány, krizové plány organizace, plány krizové připravenosti, plány krizové připravenosti subjektu kritické infrastruktury a jejich části) a za správnost poskytnutých údajů.
		Provádí pravidelnou revizi analýzy dopadů a hodnocení rizik.
	Zaměstnanci	Jsou povinni se účastnit pravidelných školení KŘ, testování a cvičení plánů.
		Jsou povinni hlásit mimořádné události svému nadřízenému, výpadky IT systémů hlásí na Helpdesk IT.
		Dle pokynů členů krizových týmů poskytují požadovanou součinnost při řešení a odstraňování následků mimořádných událostí či krizových situací.

Tabulka 75 - Personální struktura krizového řízení – povinnosti a odpovědnosti

6.7.2 Personální struktura krizového týmu organizace

Oblast KŘO – strukturální požadavky	Členové krizového týmu	Popis povinností a odpovědností
Personální struktura krizového týmu organizace	**Vedoucí krizového týmu organizace**	Vyhodnocuje mimořádnou událost či krizovou situaci a na základě vyhodnocení aktivuje příslušnou část relevantního plánu.
		Řídí obnovu procesů a zajišťuje informování a komunikaci na taktickou úroveň krizového týmu organizace. Informuje bez zbytečného odkladu manažera KŘO a svého garanta KŘO za úsek o mimořádných událostech a krizových situacích v propojení na konkrétní plán kontinuity činnosti.
	Zástupce vedoucího krizového týmu organizace	Přebírá veškerou odpovědnost v případě nepřítomnosti vedoucího krizového týmu organizace.
	Koordinátor KPO	Koordinuje činnosti obnovy v souladu s krizovým plánem organizace, v případě menších organizačních jednotek roli zastává vedoucí krizového týmu organizace, popř. jeho zástupce.
	Členové	Vykonávají činnosti obnovy v souladu s krizovým plánem organizace

Tabulka 76 - Personální struktura krizového týmu – povinnosti a odpovědnosti

6.7.3 Úroveň řízení krizového týmu

Oblast KŘ – strukturální požadavky	Typ úrovně	Popis činností v rámci úrovně
Úroveň řízení krizového týmu	**Operativní úroveň**	Zajišťuje první reakci na mimořádnou událost, tj. vyhodnocení a hlášení, v rámci organizační jednotky
		Provede prvotní posouzení mimořádné události, její vyhodnocení a hlášení
		Výpadky systémů hlásí na technický dispečink/dohledové centrum a informuje taktický tým.
		V rámci prvotní reakce, pokud je to pro událost relevantní, v první řadě chrání zdraví a životy zaměstnanců a postupuje v souladu s pravidly požární ochrany, BOZP a dle místního evakuačního plánu.
		Následně vykonává kroky směřující k zajištění kontinuity a obnovy činností organizační jednotky, dle priorit a skutečností stanovených v havarijních plánech, krizových plánech, krizových plánech organizace, plánech krizové připravenosti a plánech krizové připravenosti subjektu kritické infrastruktury.
		Informuje vyšší úrovně řízení o stavu řešení události, případně žádá o součinnost
		Komunikuje a koordinuje své činnosti ve spolupráci s dalšími týmy na operativní úrovni např. při mimořádné události, která postihla stejnou budovu.
		Události menšího rozsahu – stupeň 1. a 2. (např. lokální výpadky systémů, zvýšená absence klíčových zaměstnanců apod.) budou často efektivně řešeny na této úrovni řízení, aniž by bylo potřeba aktivního zapojení dalších dvou úrovní řízení.
	Taktická úroveň	Tato úroveň řízení bude aktivována v případě větších událostí – v případě potřeby stupeň 2., vždy při stupni 3. (např. rozsáhlé výpadky systémů, požár, epidemie), které mají dopad do více organizačních jednotek spadajících pod osobu na to pověřenou.
		Krizové řízení a krizové řízení organizace zajišťuje osoba na to pověřená ve spolupráci s Manažerem KŘO. Osoba pověřená má pravomoc do týmu přizvat zástupce dalších organizačních jednotek (zpravidla IT, správa budov atd.).
		Činnosti obnovy řídí a koordinuje v souladu s postupy stanovenými v havarijních plánech, krizových plánech, krizových plánech organizace, plánech krizové připravenosti a plánech krizové připravenosti subjektu kritické infrastruktury jednotlivých organizačních jednotek (procesů) a jejich důležitosti pro organizaci.
		Vytváří komunikační rozhraní mezi strategickou a operativní úrovní (např. zajistí další požadované zdroje z vyšší úrovně).

		Informuje a komunikuje s vedením organizace.
	Strategická úroveň	Je aktivována v případě těch nejzávažnějších událostí v rámci organizace – stupeň 4. (např. zničení budovy centrály, virové epidemie s dopadem na celou společnost, dlouhodobé výpadky klíčových aplikací, apod.).
		Určuje priority řešení požadavků ze strany týmů na taktické úrovni, v případě kdy je aktivováno více krizových týmů organizace taktické úrovně současně.
		Zajišťuje další potřebné zdroje, nad rámec kompetencí taktické úrovně.

Tabulka 77 - Úroveň řízení krizového týmu – popis činností

6.7.4 Stupně mimořádných stavů/krizových situací

Výše stupně MS/KS		Popis stupně MS/KS
Stupeň MS/KS	**1. STUPEŇ (AKTIVACE KP a KPO)**	Kratší výpadky klíčových systémů (obvykle hodiny až jednotky dnů), omezený provoz budovy / pracoviště (obvykle hodiny až jednotky dnů), absence klíčových zaměstnanců (obvykle okolo 30% klíčových zaměstnanců).
	2. STUPEŇ	Výpadky klíčových systémů (obvykle jednotky dnů), omezený provoz budovy / pracoviště (obvykle jednotky dnů), absence klíčových zaměstnanců (obvykle okolo 60% klíčových zaměstnanců).
	3. STUPEŇ	Výpadky klíčových systémů (obvykle jednotky dnů až týdny), omezený provoz budovy / pracoviště (obvykle týdny), absence klíčových zaměstnanců (obvykle okolo 80%-90% klíčových zaměstnanců).
	4. STUPEŇ	Např. zničení budovy dispečinku, virové epidemie s dopadem na celou společnost, s následkem výpadku celé organizační jednotky, dlouhodobé výpadky klíčových aplikací, apod.

Tabulka 78 - Popis stupňů MU/KS

6.7.5 Činnosti krizového týmu organizace

	Stav procesu řešení a řízení MS/KS	Rozsah činností
Činnosti krizového týmu organizace	**Vznik mimořádné události a vyhlášení MS/KS**	Vznik mimořádné události a vyhlášení MS/KS dle kategorizace mimořádných stavů: - stupně mimořádných stavů 1 – 4.
	Aktivace krizového týmu organizace	Aktivace krizového týmu organizace: - operativní úroveň, zajišťuje první reakci na mimořádnou událost, tj. vyhodnocení a hlášení, - strategická úroveň, je aktivovaný v případě těch nejzávažnějších událostí v rámci organizace – stupeň 4. (např. zničení budovy centrály, virové epidemie s dopadem na celou společnost, dlouhodobé výpadky klíčových aplikací, apod.)
		- taktická úroveň, tato úroveň krizového řízení organizace bude aktivována v případě větších událostí – v případě potřeby stupeň 2., vždy při stupni 3. (např. rozsáhlé výpadky systémů, požár, epidemie), které mají dopad do více organizačních jednotek spadajících pod osobu pověřenou
		- strategická úroveň, je aktivovaná v případě těch nejzávažnějších událostí v rámci organizace – stupeň 4. (např. zničení budovy centrály, virové epidemie s dopadem na celou společnost, dlouhodobé výpadky klíčových aplikací, apod.)
	Řízení mimořádného stavu	Realizace: - preventivních opatření jako příprava na případné prohloubení nebezpeční z aktuální situace a na zrychlenou reakci v takovýchto případech,
		- opatření pro zvýšený monitoring zařízení, objektů, personálu nebo samotných hrozeb
	Vyhodnocení a ukončení mimořádného stavu	- posouzení aktuální situace (postižené zdroje, závažnost): prohlášení o situaci a o reálných nebo pravděpodobných dopadech na společnost.
		- stanovení priorit a cílů
		- stanovení a rozdělení úkolů: Sestavení seznamu úkolů a jejich vazeb, jež povedou k obnově postižených nebo ohrožených zdrojů

Tabulka 79 - Činnosti managementu kontinuity činností v případě vzniku MS/KS

6.8 Příloha 8 - Seznam tabulek a obrázků

6.8.1 Seznam tabulek

6.8.2 Seznam obrázků

Deloitte označuje jednu či více společností Deloitte Touche Tohmatsu Limited, britské privátní společnosti s ručením omezeným zárukou, a jejích členských firem. Každá z těchto firem představuje samostatný a nezávislý právní subjekt. Podrobný popis právní struktury společnosti Deloitte Touche Tohmatsu Limited a jejích členských firem je uveden na adrese www.deloitte.com/cz/onas.

Společnost Deloitte poskytuje služby v oblasti auditu, daní, poradenství a finančního poradenství klientům v celé řadě odvětví veřejného a soukromého sektoru. Díky globálně propojené síti členských firem ve více než 150 zemích má Deloitte světové možnosti i hlubokou znalost místního prostředí, a může tak pomáhat svým klientům k úspěchu na všech místech jejich působnosti. Přibližně 182 000 odborníků usiluje o to, aby se společnost Deloitte stala etalonem nejvyšší kvality.

© 2012 Deloitte Česká republika