DOPORUČENÍ SÚJB

bezpečné využívání jaderné energie a ionizujícího záření

Zabezpečení radionuklidových zdrojů a jejich kategorizace

radiační ochrana

DR-ZA-1.0

Státní úřad pro jadernou bezpečnost

Revize č.:	Účinnost:	Garant:	Popis či komentář změny:

Radiační ochrana

ZABEZPEČENÍ RADIONUKLIDOVÝCH ZDROJŮ A JEJICH KATEGORIZACE
Doporučení DR – ZA – 1.0

Vydal: Státní úřad pro jadernou bezpečnost, Praha, srpen 2017
Č. j.: SÚJB/RCHK/8648/2017

Účelová publikace bez jazykové úpravy, připomínky směřujte na adresu:
pripominky_doporuceni@sujb.cz

Předmluva

Požadavky na zabezpečení radionuklidových zdrojů byly do nové atomové legislativy zavedeny na základě mezinárodních doporučení, zejména doporučení vydaných Mezinárodní agenturou pro atomovou energii. Jedná se o základní implementaci požadavků k zajištění bezpečnosti zdrojů, která je kompatibilní s přístupem členských států Evropské unie. Nové povinnosti uložené držitelům povolení mají za cíl zvýšit kulturu zabezpečení zdrojů ionizujícího záření v reakci na složitou bezpečnostní situaci v současném světě. Zneužití zdrojů ionizujícího záření není možné zcela vyloučit. Vytvořením kvalitního systému opatření je však možné takové riziko snížit na rozumně dosažitelnou úroveň. Zavedený systém umožní rovněž včas reagovat na změny bezpečnostní situace a vývoj potenciálních rizik.

Cílem předkládaného doporučení je poskytnout držitelům povolení a ohlašovatelům, kteří používají schválený typ drobného zdroje ionizujícího záření, návod, jakým způsobem k novým legislativním požadavkům přistoupit. Je však třeba zdůraznit, že systém zabezpečení musí být vytvořen „na míru“ konkrétnímu zdroji a je kompetencí i odpovědností držitele povolení a ohlašovatele používající schválený typ drobného zdroje ionizujícího záření, jakým způsobem požadavky zákona naplní. Významnou roli v tomto procesu bude mít výběr a ustanovení fyzické osoby povinné zajistit zabezpečení zdroje a koordinovat související činnosti.

Cílem zabezpečení radionuklidových zdrojů je správně identifikovat možná rizika, odhadnout jejich míru, hledat možnosti, jak jim předcházet, a v případě potřeby adekvátně zasáhnout. Podle nastavených požadavků je třeba proces zabezpečení nastartovat, ale samozřejmě ho bude třeba pravidelně hodnotit a případně modifikovat.

Postupy uvedené v Doporučení mají pomoci snížit míru rizika zneužití radionuklidových zdrojů používaných na pracovištích držitelů povolení a ohlašovatelů, kteří používají schválený typ drobného zdroje ionizujícího záření. Pokud bude systém zabezpečení zdroje vycházet z požadavků tohoto doporučení, bude z pohledu Státního úřadu pro jadernou bezpečnost naplňovat požadavky radiační ochrany stanovené platnou legislativou. Zpětná vazba k systému zabezpečení zdrojů i k předkládanému Doporučení je vítána, stejně tak i odborný přínos k uvedené problematice.

Ing. Karla Petrová

ředitelka Sekce radiační ochrany

Obsah

Pojmy

D-hodnota
– aktivita radionuklidu v radionuklidovém zdroji, který může způsobit závažnou tkáňovou reakci, není-li pod dohledem. D-hodnota vybraných radionuklidů je stanovena v příloze č. 1 vyhlášky o radiační ochraně a zabezpečení radionuklidového zdroje č. 422/2016 Sb.

Expoziční situace
– všechny v úvahu připadající okolnosti vedoucí k vystavení fyzické osoby nebo životního prostředí ionizujícímu záření.

Plánovaná expoziční situace
– expozice spojena se záměrným využíváním zdroje ionizujícího záření.

Seznam použitých zkratek

SÚJB - Státní úřad pro jadernou bezpečnost

PZTS - Poplachový zabezpečovací a tísňový systém

EZS - Elektronický zabezpečovací systém

CCTV - Closed Circuit Television (kamerový systém)

EKV - Elektronická kontrola vstupu

PCO - Pult centralizované ochrany

UPC - zdroj nepřerušovaného napájení

PIT - prostorový detektor pohybu

MW - mikrovlnné detektory

1. Úvod

Nové legislativní požadavky uvedené v ustanovení § 164 zákona č. 263/2016 Sb., atomový zákon, ukládají držitelům povolení, kteří vykonávají činnosti v rámci plánované expoziční situace a ohlašovatelům typově schválených drobných zdrojů ionizujícího záření povinnost zabezpečit radionuklidový zdroj před nepovoleným přístupem, jeho zneužitím a neoprávněným přemístěním. Držitelem povolení a ohlašovatelem používající typově schválený drobný zdroj ionizujícího záření by měla být pravidelně posuzována možnost zneužití radionuklidového zdroje. Pokud při tomto posuzování bude zjištěno, že se změnila úroveň rizika možného útoku či jeho zneužití, měl by být celý systém zabezpečení přehodnocen a přizpůsoben novým požadavkům zohledňujícím tyto okolnosti.

Úroveň ochrany a zabezpečení radionuklidových zdrojů by měla být úměrná jejich potenciálnímu nebezpečí. Doporučená bezpečnostní a ochranná opatření jsou zaměřena na prevenci, odvrácení a eliminaci zlovolných činů, zejména vhodnou kombinací prvků zabezpečení. Toto by mělo být provedeno uplatněním odstupňovaného přístupu s ohledem na kategorii zabezpečení radionuklidového zdroje a způsobu nakládání s ním. Ve vyhlášce SÚJB č. 422/2016 Sb. jsou pak uvedeny konkrétní požadavky pro vytvoření odpovídajícího systému zabezpečení radionuklidových zdrojů. Následující kapitoly jsou sestaveny na základě požadavků jednotlivých ustanovení této vyhlášky.

2. Systém zabezpečení radionuklidového zdroje

Systém zabezpečení radionuklidového zdroje je založen na povinnostech, které ukládá atomový zákon držitelům povolení vykonávající činnost v rámci plánované expoziční situace a ohlašovatelům používající schválený typ drobného zdroje ionizujícího záření. Požadavky na zabezpečení radionuklidových zdrojů jsou stanoveny v § 164 odst. 1 a 2 atomového zákona:

1. Držitel povolení vykonávající činnost v rámci plánované expoziční situace a ohlašovatel používající schválený typ drobného zdroje ionizujícího záření jsou povinni:

a) zabezpečit radionuklidový zdroj před nepovoleným přístupem, použitím a přemístěním odstupňovaným přístupem s ohledem na kategorii zabezpečení a způsob nakládání s radionuklidovým zdrojem,

b) poučit pracovníka s přístupem k radionuklidovému zdroji o jeho zabezpečení a ověřit jeho znalosti a

c) provést zabezpečení radionuklidového zdroje 1. až 3. kategorie zabezpečení.

2. Prováděcí právní předpis (vyhláška SÚJB č. 422/2016 Sb.) stanoví požadavky na způsob zabezpečení radionuklidového zdroje, včetně radionuklidového zdroje 1. až 3. kategorie zabezpečení.

2.1. Kategorizace radionuklidových zdrojů pro účely přeshraničního pohybu a zabezpečení

Podle § 61 odst. 2 atomového zákona jsou zdroje ionizujícího záření (radionuklidové zdroje) členěny do pěti kategorií zabezpečení, kdy 1. kategorie zabezpečení je uvažována jako nejrizikovější a 5. kategorie zabezpečení jako kategorie s nejnižším rizikem. Rozdělení do jednotlivých kategorií zabezpečení je dáno výčtem uvedeným v § 17 vyhlášky č. 422/2016 Sb. U otevřených a uzavřených radionuklidových zdrojů je pak kategorie zabezpečení dána poměrem aktivity radionuklidu a tabelované D-hodnoty, která je uvedena v příloze 1 výše citované vyhlášky.

Z praktického pohledu bude tedy nutné, aby každý, kdo žádá o povolení k nakládání s radionuklidovým zdrojem a rovněž tak i ohlašovatel, který se chystá používat drobný typově schválený zdroj ionizujícího záření, provedl stanovení kategorie zabezpečení. Zjištění kategorie zabezpečení bude podkladem pro rozhodnutí, zda musí být vypracován plán zabezpečení.

U uzavřeného radionuklidového zdroje, kde je nutné zjistit poměr aktuální aktivity a D-hodnoty, se stanovení kategorie zabezpečení provede tak, že se vezme v úvahu celkový počet radionuklidů, jejich jednotlivé aktivity se sečtou a celková aktivita se vydělí tabelovanou D-hodnotou. Pokud je používáno více druhů radionuklidů, postupuje se stejným způsobem – vypočítá se poměr A/D pro každý radionuklid a výsledné poměry A/D se sečtou, přičemž je získána celková hodnota poměru A/D, ze které se stanoví kategorie zabezpečení.

U otevřených radionuklidových zdrojů se pro stanovení kategorie zabezpečení vychází z maximálních aktivit všech radionuklidů, které mohou být na pracovišti používány v souladu s příslušným povolením.

Kategorie zabezpečení radionuklidových zdrojů jsou následující:

Radionuklidové zdroje 1. kategorie zabezpečení

- radionuklidové termoelektrické generátory,
- radionuklidové ozařovače, včetně ozařovačů tkání a krve,
- uzavřené radionuklidové zdroje, u kterých je poměr aktuální aktivity a D-hodnoty roven 1000 nebo větší,
- otevřené radionuklidové zdroje, u kterých je poměr nejvýše zpracovávané aktivity na pracovišti a D-hodnoty roven 1000 nebo větší.

Radionuklidové zdroje 2. kategorie zabezpečení

- uzavřené radionuklidové zdroje určené pro defektoskopii,
- uzavřené radionuklidové zdroje určené k brachyterapii s vysokým nebo středním dávkovým příkonem,
- uzavřené radionuklidové zdroje, u kterých je poměr aktuální aktivity a D-hodnoty menší než 1000 a zároveň roven 10 nebo větší,
- otevřené radionuklidové zdroje, u kterých je poměr nejvýše zpracovávané aktivity na pracovišti a D-hodnoty menší než 1000 a zároveň roven 10 nebo větší.

Radionuklidové zdroje 3. kategorie zabezpečení

- uzavřené radionuklidové zdroje pro karotáž,
- uzavřené radionuklidové zdroje v indikačním nebo měřícím zařízení, které jsou vysokoaktivním zdrojem,
- uzavřené radionuklidové zdroje, u kterých je poměr aktuální aktivity a D-hodnoty menší než 10 a zároveň roven 1 nebo větší,
- otevřené radionuklidové zdroje, u kterých je poměr nejvýše zpracovávané aktivity na pracovišti a D-hodnoty menší než 10 a zároveň roven 1 nebo větší,
- kapalná či pevná látka obsahující více než 30 % uranu, jejíž aktivita je větší než 160 MBq.

Radionuklidové zdroje 4. kategorie zabezpečení

- uzavřený radionuklidový zdroj určený k brachyterapii s nízkým dávkovým příkonem s výjimkou očního aplikátoru a permanentního implantátu,
- uzavřený radionuklidový zdroj v indikačním nebo měřícím zařízení, který není vysokoaktivním zdrojem,
- uzavřený radionuklidový zdroj v eliminátoru statické elektřiny,
- uzavřený radionuklidový zdroj, u kterého je poměr aktuální aktivity a D-hodnoty menší než 1 a zároveň roven 0,01 nebo větší,
- otevřený radionuklidový zdroj, u kterého je poměr nejvýše zpracovávané aktivity na pracovišti a D-hodnoty menší než 1 a zároveň roven 0,01 nebo větší.

Radionuklidové zdroje 5. kategorie zabezpečení

- oční aplikátor a permanentní implantát pro radioterapii,
- zdroj ionizujícího záření pro radionuklidovou rentgenofluorescenční analýzu,
- detektor elektronového záchytu,
- radionuklidový zdroj pro Mössbauerovskou spektrometrii,
- kalibrační zdroj ionizujícího záření pro pozitronovou emisní tomografii,
- uzavřený radionuklidový zdroj, u kterého je poměr aktuální aktivity a D-hodnoty menší než 0,01 a zároveň je aktuální aktivita vyšší než zprošťovací úroveň,

- otevřený radionuklidový zdroj, u kterého je poměr nejvýše zpracovávané aktivity na pracovišti a D-hodnoty menší než 0,01 a zároveň je aktuální aktivita vyšší než zprošťovací úroveň.

Pro účely zabezpečení musí být na pracovištích, kde dochází ke shromažďování radionuklidových zdrojů, použita kategorie zabezpečení celého souboru radionuklidových zdrojů na pracovišti nebo v transportním obalovém souboru (§ 18 vyhlášky č. 422/2016 Sb.). Kategorie zabezpečení celého souboru radionuklidových zdrojů musí být stanovena na základě agregovaného poměru A/D, vypočteného následujícím způsobem:

$$Agregovaná \quad A/D = \sum_{n} \frac{\sum_{i} A_{i,n}}{D_n}$$

kde *Ai, n* je aktivita *A* každého jednotlivého zdroje *i* radionuklidu *n* a *Dn* je D-hodnota pro radionuklid *n*.

Jedná se zejména o držitele povolení k výrobě a distribuci radionuklidových zdrojů, k provozování uznaného skladu a držitele povolení či ohlašovatele, kteří hromadně skladují drobné zdroje ionizujícího záření např. likvidované ionizační hlásiče požáru.

3. Základní funkce zabezpečovacího systému

Systém zabezpečení radionuklidových zdrojů by měl být navržen takovým způsobem, aby splňoval základní funkce, kterými jsou - odrazení, detekce, zdržení, zásah a řízení zabezpečení.

Odrazením rozumíme vzdání se úmyslu útočníka od pokusu provést nepovolený přístup či přemístění radionuklidového zdroje. Smyslem odrazovacích prostředků je přesvědčit útočníka o tom, že splnění cíle útoku bude příliš obtížné a výsledek (získaní zdroje či přístup k němu) bude nejistý. Základním prostředkem odrazení je např. evidentní přítomnost jednotlivých prvků systému zabezpečení (oplocení, mříže, kamery, fyzická ostraha).

Detekcí rozumíme zjištění, tj. obdržení informace o nepovoleném přístupu ke zdroji. Zjištění nepovoleného přístupu ke zdroji může být provedeno pracovníky fyzické ostrahy či prostřednictvím varovného akustického signálu, který upozorní na narušení prostor se zdrojem. Vhodnými prostředky jsou např. pohybová čidla, detektory tříštění skla, dveřní či okenní magnetické kontakty. Součástí detekce je i vyhodnocení obdržené informace o narušení prostoru se zdrojem. Vyhodnocení lze provést pomocí kamerového systému či fyzické kontroly v místě jeho uložení.

Zdržením rozumíme záměrné navýšení útočníkova času potřebného k průniku do/z místa, kde je zdroj umístěn. Zdržení přístupu ke zdroji může být zajištěno pomocí mechanických zábranných prostředků – mříží, bezpečnostních zámků, kotevních šroubů a jiných vhodných technických prostředků znesnadňujících přístup a zpomalujících získání zdroje.

Zásahem rozumíme jednání předem určených osob s cílem zabránit pokusu zneužití zdroje či jeho přemístění, a to včetně sabotáže provedené vlastním (vnitřním) pracovníkem. Zásah sestává z přerušení útoku a zabránění ztrátě kontroly nad zdrojem. Přerušením útoku rozumíme nasazení odpovídajících sil pohotovostní ochrany nebo fyzické ostrahy s cílem zabránit útočníkovi v přístupu ke zdroji a zamezit jeho zneužití.

Řízení zabezpečení zahrnuje zajištění dostatečných personálních a finančních zdrojů pro zabezpečení radionuklidových zdrojů, vypracování postupů, plánů a záznamů. S ohledem na zajištění účinnosti systému zabezpečení a zavedení určité kultury zabezpečení je nutné s informacemi o systému zabezpečení nakládat v souladu s § 114 vyhlášky č. 422/2016 Sb.

Stěžejní funkce systému zabezpečení (detekce, zdržení a zásah) jsou v následujícím textu detailně popsány u jednotlivých kategorií zabezpečení radionuklidových zdrojů.

4. Zabezpečení radionuklidových zdrojů

4.1. Požadavky na držitele povolení k nakládání s radionuklidovými zdroji 1. až 3. kategorie zabezpečení

Vyhláška č. 422/2016 Sb. specifikuje požadavky na zabezpečení radionuklidových zdrojů. Doporučení vychází z této vyhlášky a uvádí konkrétní postupy ke splnění stanovených požadavků. Z důvodu lepší přehlednosti jsou jednotlivá ustanovení citované vyhlášky zahrnuta a uspořádána podle jednotlivých kategorií zabezpečení. Rovněž tak jsou v následujícím textu vysvětleny a popsány doporučené postupy k zabezpečení radionuklidových zdrojů s uplatněním odstupňovaného přístupu.

Zde je nutné zdůraznit význam **zavedení odstupňovaného přístupu**. V ustanovení § 5 odst. 8 atomového zákona je uvedeno, že každý, kdo využívá jadernou energii nebo vykoná činnosti v rámci expozičních situací, je povinen při zajišťování jaderné bezpečnosti, radiační ochrany, technické bezpečnosti, monitorování radiační situace, zvládání radiační mimořádné události a zabezpečení využívat přístup odstupňovaný podle velikosti možného ozáření a jeho možných důsledků.

Z výše uvedeného vyplývá, že u radionuklidových zdrojů 1. kategorie zabezpečení bude kladen nejvyšší důraz na jejich ochranu a řízení přístupu do míst jejich uložení. Čím vyšší je riziko jejich zneužití, tím větší akceschopnost se vyžaduje od bezpečnostních a ochranných systémů. Logicky pak u radionuklidových zdrojů 3. kategorie zabezpečení bude použito nižšího důrazu na jejich zabezpečení, omezení přístupu a manipulace s nimi.

V ustanovení § 111 vyhlášky č. 422/2016 Sb. jsou uvedeny postupy, kterými držitel povolení musí provést zabezpečení radionuklidového zdroje 1. až 3. kategorie zabezpečení, a to tak, že:

a) určí informace důležité z hlediska zabezpečení radionuklidového zdroje a zajistí jejich ochranu před zneužitím,

b) přijme opatření k odhalení a zdržení nepovoleného přístupu k radionuklidovému zdroji a odezvě na něj, zejména:

1. zabránění neoprávněnému přemístění, jde-li o radionuklidový zdroj 1. kategorie zabezpečení, a
2. snížení pravděpodobnosti neoprávněného přemístění na nejnižší dosažitelnou míru, jde-li o radionuklidový zdroj 2. nebo 3. kategorie zabezpečení.

V ustanovení § 114 odst. 3 vyhlášky č. 422/2016 Sb. je držitelům povolení stanovena povinnost ustanovit fyzickou osobu povinnou zajistit zabezpečení radionuklidového zdroje a koordinaci činností v rámci zabezpečení radionuklidového zdroje.

Vzhledem k povinnostem této osoby je doporučeno, aby touto osobou nebyla osoba vykonávající soustavný dohled nad radiační ochranou. Jedná se o povinnosti zcela odlišné - vykonávání soustavného dohledu nad radiační ochranou a zajištění zabezpečení radionuklidového zdroje.

Držitel povolení musí dále zajistit, aby fyzická osoba podílející se na zabezpečení radionuklidového zdroje a fyzická osoba samostatně přistupující k radionuklidovému zdroji 1. kategorie zabezpečení byla vybírána a průběžně posuzována s ohledem na riziko z hlediska zabezpečení, které může představovat.

Základním předpokladem k ustanovení této osoby je její posouzení z hlediska důvěryhodnosti (např. pracovní historie zaměstnance, zohlednění rodinných a sociálních podmínek) z pohledu držitele povolení. Možným způsobem ověření důvěryhodnosti zaměstnanců je např. osobní pohovor, doporučení vedoucího pracovníka, eventuálně kontrola výpisu rejstříku trestů v pravidelném intervalu. Předkládání výpisu z rejstříku trestu s pravidelnou četností (např. 1x za 2 roky) je doporučeno zavést u pracovišť se zdrojem 1. kategorie zabezpečení, vždy však před zahájením pracovního poměru zaměstnance na tomto typu pracoviště. U ostatních kategorií je možné tento postup aplikovat obdobným způsobem s ohledem na typ a množství používaných zdrojů.

4.2. Radionuklidové zdroje 1. kategorie zabezpečení

Do této kategorie patří radionuklidové termoelektrické generátory, radionuklidové ozařovače (včetně ozařovačů tkání a krve) a dále pak uzavřené a otevřené radionuklidové zdroje, u kterých je poměr aktuální aktivity radionuklidu a D-hodnoty roven 1000 nebo větší.

4.2.1. Informace důležité z hlediska zabezpečení radionuklidového zdroje

Jedná se o informace o zavedeném bezpečnostním systému a jeho prvcích. V praxi jde o informace uvedené v plánu zabezpečení. Mohou jimi být např. informace o poplachovém a tísňovém systému, kamerovém systému, způsobu vedení zásahů, pravomoci a odpovědnosti oprávněných pracovníků. Dále se může jednat o informace o obsluze elektronického přístupového systému, způsobu předávání a vydávání klíčů od prostor, kde se nachází zdroj. Samotný dokument – plán zabezpečení radionuklidového zdroje, případně jeho související dokumenty či datové soubory, by měly být uchovávány v zabezpečeném prostoru, bez možnosti neautorizovaného přístupu. Pokud se jedná o SW a data uložená v počítači či na datových nosičích, musí být tyto řádně zajištěny proti jejich zneužití.

4.2.2. Opatření k odhalení a zdržení neoprávněného přístupu k radionuklidovému zdroji, odezvě na něj a zabránění jeho přemístění

Tato opatření jsou zaváděna ve snaze zabránit neoprávněnému přemístění radionuklidového zdroje detekčními elektronickými systémy, kamerovými systémy a systémy řízení přístupu. Dalším možným opatřením je zajištění adekvátní ochrany prostoru resp. zdroje, která zabrání neoprávněnému přístupu a přemístění zdroje prostřednictvím zásahové skupiny bezpečnostní služby nebo policejní jednotky. Poplachové a ostatní signály ze zabezpečovacích systémů by měly být přenášeny na místní ostrahu objektu, eventuálně na vzdálený monitoring objektu – Pult Centralizované Ochrany (dále jen PCO), a to včetně zajištění přenosu výstupů kamerových systémů z narušeného či napadeného objektu. Poplachové stavy EZS by měly být přenášeny do kamerového systému jako informace o narušení, kdy následně kamerový systém poskytne obraz z narušeného prostoru.

Zdržení přístupu ke zdroji může být zajištěno pomocí mechanických zábranných prostředků – mříží, bezpečnostních zámků, kotevních šroubů a jiných vhodných technických prostředků znesnadňujících přístup a získání zdroje.

4.2.3. Zabezpečení radionuklidového zdroje 1. kategorie zabezpečení

Detekce nepovoleného přístupu k radionuklidovému zdroji 1. kategorie zabezpečení musí zajistit:

- odhalení každého pokusu o nepovolený přístup k radionuklidovému zdroji musí být zajištěno vhodným zařízením včetně přenosu signálu na PCO. Zajištění této funkcionality musí být provedeno adekvátním umístěním zdroje z hlediska polohy v objektu a stavebního řešení tak, aby vstupy a přístupy ke zdroji byly monitorovány detektory zabezpečovacího systému a řízeny elektronickým přístupovým systémem,
- odhalení pokusu o nepovolený přístup k radionuklidovému zdroji nepovolaným pracovníkem, a to i nepovolaným pracovníkem držitele povolení (insider), by mělo být zajištěno prostřednictvím instalovaných bezpečnostních technologií, zejména systémem PZTS a EKV, kdy je neoprávněný přístup detekován,
- získání informací nezbytných k neprodlenému vyhodnocení nepovoleného přístupu ke zdroji, např. pomocí kamerového systému.

Zdržení dostatečné k zahájení zásahu:

- je propočítáváno od první detekce pokusu o vniknutí do objektu a doby potřebné k překonání mechanických zábran pro vstup do objektu,
- dalším zdržením a navýšením času potřebného k provedení zásahu je zajištění samotného zdroje mechanickým zabezpečením např. připevněním zařízení se zdrojem k pevné části objektu, případně navařením či jiným mechanickým připevněním přípravků bránících v manipulaci se zdrojem (kotvy, ocelové popruhy, ocelové pásy),
- navyšováním a stupňováním těchto opatření získáváme po celkovém sečtení dobu, kdy je nutné provést adekvátní zásah přímo v místě umístění zdroje.

Zásah, **který vede k zabránění neoprávněnému přemístění radionuklidového zdroje:**

- po vyhodnocení první detekce a potvrzení, že došlo k nepovolenému přístupu ke zdroji, musí držitel povolení neprodleně zajistit provedení adekvátního zásahu,
- k tomu je nutné vzít v úvahu proti jakému jednání (útoku či narušení) je zásah veden, a v souvislosti s tím uplatňovat přiměřenost a účinnost zásahu,
- zjištěný nepovolený přístup může mít charakter přímého přijetí poplachové zprávy od zabezpečovacího systému nebo ohlášení takovéto skutečnosti obsluhou zařízení, zaměstnancem, či jinou osobou, která tuto událost zjistí,
- informace o nepovoleném přístupu ke zdroji může být také předána obsluhou pomocí tlačítka stavu nouze, tlačítka nátlaku na klávesnici EZS, či zadáním nátlakového kódu případně zadáním nátlakového otisku prstu u biometrických systémů řízení přístupu,
- samotný zásah by měl být proveden ostrahou objektu, zásahovou skupinou poskytovatele bezpečnostních služeb, případně přímo složkami Policie ČR.

4.3. Radionuklidové zdroje 2. kategorie zabezpečení

V této kategorii jsou zařazené uzavřené radionuklidové zdroje určené pro defektoskopii, brachyterapii s vysokým nebo středním dávkovým příkonem včetně uzavřených a otevřených radionuklidových zdrojů, u kterých je poměr aktuální aktivity a D-hodnoty menší než 1000 a zároveň roven 10 nebo větší.

Vzhledem k typickému způsobu používání radionuklidového zdroje při defektoskopické činnosti je nutné zdůraznit, že při vytváření odpovídajícího a efektivního plánu zabezpečení není možné opomenout zabezpečení zdroje při jeho přepravě na přechodné defektoskopické pracoviště. Držitel povolení musí zvážit možná rizika v souvislosti s převozem zdroje a místem jeho používání. V plánu zabezpečení by měl být uveden způsob zabezpečení během přepravy a postupy pro případ ztráty kontroly nad zdrojem během přepravy a na přechodném pracovišti.

4.3.1. Informace důležité z hlediska zabezpečení radionuklidového zdroje

Jedná se opět o informace uvedené v plánu zabezpečení - o poplachovém a tísňovém systému, kamerovém systému, způsobu vedení zásahu, pravomoci a odpovědnosti oprávněných pracovníků, způsobu zacházení s elektronickým přístupovým systémem (je-li součástí kontroly vstupu ke zdroji), způsob předávání a vydávání klíčů od prostor, kde je zdroj umístěný a jiné.

Plán zabezpečení, případně jeho související dokumenty či datové soubory, by měly být uchovávány v uzamčeném prostoru, řádně uložené bez možnosti neautorizovaného přístupu. Pokud se jedná o SW a data uložená v počítači či na datových nosičích, musí být tyto rovněž řádně zajištěny proti jejich zneužití.

4.3.2. Opatření k odhalení a zdržení nepovoleného přístupu k radionuklidovému zdroji, odezvě na něj a snížení pravděpodobnosti neoprávněného přemístění radionuklidového zdroje na nejnižší dosažitelnou míru.

Rovněž i v tomto případě je třeba zajistit prostor se zdrojem (např. defektoskopické základny). Vhodnou variantou je opět pomocí EZS a zavedení řízení přístupu pomocí EKV. Výstupy narušených prostor by i v tomto případě měly být přenášeny na PCO nebo na stanoviště ostrahy objektu. Takovýmto stanovištěm může být vrátnice objektu, recepce, či jiné stanoviště s nepřetržitou fyzickou ostrahou objektu. Pokud není možné zajistit trvalou fyzickou ostrahu objektu, měly by být signály z bezpečnostních systémů přenášeny na mobilní telefon odpovědné osoby držitele povolení či držitele povolení přímo, a to i v mimopracovní době.

4.3.3. Zabezpečení radionuklidového zdroje 2. kategorie zabezpečení

Detekce nepovoleného přístupu k radionuklidovému zdroji 2. kategorie zabezpečení musí zajistit:

- odhalení každého pokusu o nepovolený přístup k radionuklidovému zdroji, a to i nepovolaným pracovníkem držitele povolení (insider),
- získání informací nezbytných k neprodlenému vyhodnocení zjištěného nepovoleného přístupu, např. pomocí instalovaných bezpečnostních technologií.

Zdržení dostatečné k zahájení zásahu:

- je propočítáváno z času první detekce pokusu o vniknutí do objektu a doby potřebné pro překonání instalovaných mechanických zábran pro vstup do objektu,
- dalším zdržením a navýšením času potřebného pro zásah je zajištění samotného zdroje mechanickým zabezpečením, např. připevněním zařízení se zdrojem k pevné části objektu, případně navařením či jiným mechanickým připevněním přípravků bránících v manipulaci se zdrojem,
- navyšováním těchto opatření a jejich stupňováním získáváme po celkovém sečtení dobu, kdy je nutné provést adekvátní zásah přímo v místě umístění zdroje.

Zásah, **který vede k zabránění neoprávněného přemístění radionuklidového zdroje:**

- po vyhodnocení první detekce a potvrzení, že došlo k neautorizovanému přístupu s cílem přemístit zdroj, musí držitel povolení neprodleně zajistit provedení adekvátního zásahu,
- musí zahrnovat neprodlené přijetí opatření vedoucí ke snížení pravděpodobnosti neoprávněného přemístění radionuklidového zdroje na nejnižší dosažitelnou míru,
- k tomu je nutné vzít v úvahu proti jakému jednání (útoku či narušení) je zásah veden, a v souvislosti s tím uplatňovat přiměřenost a účinnost zásahu,
- samotný zásah by měl být proveden ostrahou objektu, zásahovou skupinou bezpečnostních služeb, případně přímo složkami Policie ČR,
- systémem reakce se rozumí předem zpracovaný plán zásahu a jeho postupy směřující k prověření takovéto krizové události, způsob jakým bude samotný zásah prováděn a kým bude prováděn.

4.4. Radionuklidové zdroje 3. kategorie zabezpečení

V praxi se to týká vysokoaktivních uzavřených radionuklidových zdrojů v indikačních nebo měřících zařízeních a v zařízeních pro karotáž a dále uzavřených či otevřených radionuklidových zdrojů, u kterých je poměr aktuální aktivity a D-hodnoty menší než 10 a zároveň roven 1 nebo větší.

4.4.1. Informace důležité z hlediska zabezpečení radionuklidového zdroje

Stejně jako u předešlých kategorií se jedná se o informace uvedené v plánu zabezpečení – o poplachovém a tísňovém systému (pokud je využíván), kamerovém systému (pokud je nainstalován), pravomoci a odpovědnosti oprávněných pracovníků, způsob předávání a vydávání klíčů od prostor, kde jsou zdroje umístěné a jiné.

Plán zabezpečení a jeho související dokumenty či datové soubory by měly být uchovávány v zabezpečeném prostoru, řádně uložené, bez možnosti neautorizovaného přístupu. Pokud se jedná o SW a data uložená v počítači či na datových nosičích, musí být tyto rovněž řádně zajištěny proti jejich zneužití.

4.4.2. Opatření k odhalení a zdržení nepovoleného přístupu k radionuklidovému zdroji, odezvě na něj a snížení pravděpodobnosti neoprávněného přemístění radionuklidového zdroje na nejnižší dosažitelnou míru

U této kategorie zřejmě nebude nutné vytvářet bezpečnostní režim pomocí EZS. Tyto zdroje jsou nepřímo kontrolovány provozem měřicích a indikačních zařízení (informace o přítomnosti zdroje v zařízení je přenášena na velín či jiné provozní středisko). Tato nepřímá kontrola je ale většinou zajištěna pouze pracovní době. V mimopracovní dobu je nutné zajistit kontrolu nad zdrojem a zavést opatření k odhalení a zdržení neoprávněného přístupu ke zdroji.

4.4.3. Zabezpečení radionuklidového zdroje 3. kategorie zabezpečení

Detekce nepovoleného přístupu k radionuklidovému zdroji 3. kategorie zabezpečení musí zajistit:

- odhalení nepovoleného přístupu a neoprávněné manipulace se zdrojem, včetně předání informace o tom odpovědným osobám.

Zdržení dostatečné k zahájení zásahu:

- je realizováno podle druhu a charakteru objektu,
- vstupy a možné přístupy ke zdroji by měly být osazeny bezpečnostními zámky, bezpečnostními dveřmi, případně mřížemi na prosklených plochách.

Zásah v podobě opatření, **který vede k zabránění neoprávněnému přemístění zdroje:**

- po potvrzení, že došlo k nepovolenému přístupu ke zdroji, musí držitel povolení zajistit opatření k zabránění neoprávněného přemístění radionuklidového zdroje, a to prostřednictvím svého zaměstnance, případně za asistence bezpečnostní služby či Policie ČR,
- k tomu je nutné vzít v úvahu proti jakému jednání (útoku či narušení) je zásah veden a v souvislosti s tím uplatňovat přiměřenost a účinnost zásahu,
- zásahem v podobě opatření se rozumí předem zpracovaný postup zpracovaný v plánu zabezpečení.

5. Plán zabezpečení

V ustanovení § 113 vyhlášky č. 422/2016 Sb. je uveden požadavek na obsah Plánu zabezpečení radionuklidových zdrojů. Plán zabezpečení musí obsahovat informace týkající se zavedeného systému zabezpečení, a to minimálně v rozsahu:

a) popis radionuklidového zdroje, jeho kategorizaci a popis způsobu jeho použití,
b) popis místa používání a uložení radionuklidového zdroje, jeho okolí a jeho umístění v budovách a areálech,
c) umístění budov a areálů vzhledem k veřejně přístupným místům,
d) cíle plánu zabezpečení pro budovy a areály zohledňující
   - zvláštní podmínky a nebezpečí
   - postupy pro zabránění nežádoucím následkům neoprávněného aktu,
e) popis opatření k zabezpečení radionuklidového zdroje, včetně
   - kontroly přístupu k radionuklidovému zdroji,
   - detekce nepovoleného přístupu k radionuklidovému zdroji,
   - zdržení nepovoleného přístupu k radionuklidovému zdroji,
   - zásahu při nepovolaném přístupu k radionuklidovému zdroji,
   - způsobů komunikace mezi osobami, které vyhodnocují výstupy ze zabezpečovacího systému, a zasahujícími osobami,
   - posouzení účinnosti opatření podle bodů výše uvedených,
f) popis administrativních opatření k zabezpečení radionuklidového zdroje, včetně
   - práv a povinností pracovníků,
   - standardních a mimořádných operací s radionuklidovým zdrojem, údržby a oprav technických prostředků ztěžujících přístup k radionuklidovému zdroji a zajišťujících včasné rozpoznání nepovoleného přístupu k radionuklidovému zdroji,
   - způsobu zajištění ochrany informací důležitých z hlediska zabezpečení radionuklidového zdroje,
   - metod kontroly přístupu k radionuklidovému zdroji,
   - způsobu výcviku personálu,
g) popis opatření při zvýšení hrozby.

6. Ochrana informací důležitých z hlediska zabezpečení zdroje

Držitel povolení poskytuje informace důležité z hlediska zabezpečení v souladu s ustanovením § 114 odst. 2 vyhlášky č. 422/2016 Sb. pouze těm osobám, které je potřebují pro výkon činnosti jim svěřené a pouze v takovém rozsahu, který k tomuto výkonu potřebují. Těmito osobami jsou myšleni zejména zaměstnanci držitele povolení případně jiní, např. zaměstnanci servisních organizací či subdodavatelů. Držitel povolení zodpovídá za rozsah podávaných informací – drží se pravidla o poskytnutí minimálního potřebného množství informací druhým či třetím osobám.

Informacemi důležitými z hlediska zabezpečení radionuklidového zdroje jsou:

- údaje o radionuklidových zdrojích a jejich umístění,
- plánované způsoby přepravy a její trasy,
- údaje obsažené v plánu zabezpečení,
- údaje o systému zabezpečení,
- údaje o ostraze,
- údaje o administrativních opatřeních v rámci zabezpečení radionuklidového zdroje,
- údaje o zásahu, který zabrání neoprávněnému přemístění radionuklidového zdroje 1. kategorie zabezpečení.

7. Organizační opatření k zabezpečení zdrojů

7.1. Organizační opatření k zajištění bezpečného přístupu ke zdroji

V souladu s principem odstupňovaného přístupu, typu pracoviště se zdrojem a zohlednění kategorie zabezpečení, musí držitel povolení k zajištění bezpečného přístupu do prostor s radionuklidovým zdrojem zavést organizační opatření, která zajistí:

- kontrolu vstupu a výstupu osob,
- kontrolu vjezdu a výjezdu dopravních prostředků,
- režim pohybu osob, věcí, dopravních prostředků v objektu a jeho jednotlivých částech v pracovní a mimopracovní době,
- režim manipulace s klíči, identifikačními prostředky a médii, které se používají pro účely přístupu ke zdroji,
- způsob evidence a úschovy duplikátů klíčů a způsob jejich použití,
- režim manipulace s technickými prostředky a jejich používání,
- způsoby prověřování důvěryhodnosti osob, kterým jsou předávány informace důležité z hlediska zabezpečení,
- způsob předávání citlivých informací.

Oprávnění osob ke vstupu do prostor s radionuklidovým zdrojem 1. kategorie zabezpečení a seznam dopravních prostředků oprávněných vjíždět do objektu se stanoví v interní dokumentaci, která by měla být součástí plánu zabezpečení. Oprávnění osob ke vstupu a vjezdu dopravních prostředků do objektu by měl vydávat statutární orgán držitele povolení (provozovatele objektu) nebo jím pověřená osoba a měla by být jednoznačně identifikovatelná. Držitel povolení stanoví organizační opatření, která zabrání návštěvám, aby se neoprávněně seznámily s informacemi důležitými z hlediska zabezpečení. Za dodržování stanovených opatření odpovídá určená osoba, která návštěvu doprovází.

V důležitých objektech by měl být návštěvám dovolen pohyb pouze v doprovodu oprávněných osob. Kontrolu oprávněnosti vstupu osob a vjezdu dopravních prostředků do objektu provádí fyzická ostraha objektu nebo osoba pověřená držitelem povolení či provozovatelem objektu způsobem stanoveným v plánu zabezpečení. Na pracovištích se zdroji 1. kategorie zabezpečení by mělo být uplatňováno pravidlo vstupu dvou osob současně. Pro tyto účely lze použít pracovníka ostrahy objektu, eventuálně funkce vzdáleného monitoringu, s jehož pomocí lze případnou verifikaci oprávnění vstupu taktéž provádět.

7.2. Organizační opatření zajišťující odezvu na nepovolaný přístup ke zdroji

Fyzická ostraha a Pulty centralizované ochrany

Držitel povolení je povinen zajistit realizaci zásahu a vyhodnocení poplachových událostí v rámci zavedeného systému zabezpečení. Tímto se rozumí zejména systém reakce na vzniklý alarm z PZTS, vyhodnocení alarmové události prostřednictvím kamerového systému, případně reakce na alarmovou událost ohlášenou jiným způsobem.

Fyzická ostraha objektu

V nejčastějším případě se jedná o pozici strážný/vrátný/recepční. Činnost strážných na jednotlivých objektech je různorodá a vždy reflektuje potřeby daného objektu. Obecně se však dá říci, že se jedná o pravidelné preventivní činnosti směřující k ochraně majetku a osob v objektu. Mezi takovéto činnosti bude patřit zejména kontrola vstupujících osob a návštěv, výstupní kontrola zaměstnanců se zaměřením na vnitřní zaměstnaneckou kriminalitu, kontrola vjíždějících vozidel a jejich evidence, pochůzková činnost, obsluha bezpečnostních technologií a reakce na jejich poplachové výstupy.

Vyhodnocení a rekce na výstupy bezpečnostních technologií

Osoba odpovědná za zabezpečení, ostraha, případně příslušníci Policie ČR provádějí okamžitou reakci na příchozí alarmovou událost, její vyhodnocení a následný adekvátní zásah dle nastavených postupů. Tyto postupy zahrnují nejen systém reakce a kontroly místa narušení, ale taktéž způsob předávání informací o uvedených skutečnostech.

Provádění pochůzkové činnosti

Ostraha provádí pravidelnou případně nepravidelnou pochůzkovou činnost, aby nemohlo dojít k vypozorování a predikování jejího pohybu v rámci objektu. Tato činnost je zaměřena na zjištění přítomnosti neoprávněných osob, narušení plášťové nebo vnitřní ochrany objektu, poškození vybavení objektu a jiného majetku.

Kontrola návštěv a zaměstnanců

Přístupové prostředky (karty, klíče) jsou zaměstnancům vydávány dle platných bezpečnostních směrnic objektu. Databáze je průběžně aktualizována dle nově příchozích a odchozích zaměstnanců. Držitel povolení by měl zajistit provádění těchto opatření. Návštěvy jsou při vstupu do objektu vždy řádně zapsány, totožnost je potvrzena porovnáním s dokladem totožnosti.

Návštěva se po objektu nepohybuje samostatně (pokud není režim objektu určen jako objekt s volným pohybem návštěv), je vždy doprovázena ostrahou nebo oprávněným zaměstnancem držitele povolení.

Dohledová a Poplachová přijímací centra (DPPC)

Tato centra monitorují stav zabezpečení objektu se zdrojem a režim vstupujících osob. Zároveň slouží jako centra pro vyhodnocování alarmových situací. Zde jsou také přijímány informace obecného charakteru, např. stav baterií, výpadek elektrické energie, programování technikem a jiné. Samostatným exekutivním segmentem dohledových a poplachových přijímacích center jsou pak zásahové jednotky.

Jejich činnost spočívá v prověřování vzniklých alarmových událostí ve střežených objektech a realizaci samotných zásahů. V příloze č. 7 je uveden příklad možného harmonogramu a postupu při provádění zásahu v objektu. Obdobné work-flow je vždy tvořeno bezpečnostním manažerem a koordinováno pro jakoukoliv bezpečnostní situaci v objektu.

8. Pravidla pro práci s fyzickými osobami, informacemi a technickými prostředky sloužícími k zabezpečení radionuklidového zdroje

Držitel povolení k nakládání s radionuklidovými zdroji 1. až 3. kategorie zabezpečení musí zajistit vhodný způsob nakládání s informacemi důležitými z hlediska zabezpečení, které poskytuje dalším osobám (zaměstnancům, návštěvám, dodavatelům a osobám servisních organizací). Dále by měl zajistit řádnou evidenci návštěv na pracovišti se zdrojem (zvláště u zdrojů 1. kategorie zabezpečení), provádět ověřování totožnosti a případnou kontrolu zavazadel při vstupu a odchodu. U dodavatelů a pracovníků servisní organizace by měl řádně evidovat práci se zdrojem či zařízením, která byla ohlášena managementem dodavatelského subjektu. Měl by pravidelně aktualizovat seznam oprávněných osob pro vstup do zabezpečených prostor se zdrojem.

Držitel povolení by měl průběžně auditovat své interní procesy, zajišťující bezpečnost informací v souvislosti s ochranou objektu a ochranou radionuklidových zdrojů. V případě potřeby by měl na výstupy těchto interních auditů reagovat změnou nastavených opatření, doplněním a případně rozšířením bezpečnostních opatření.

Jedná se zejména o procesy:
- evidence zdrojů radionuklidového záření,
- změnové řízení,
- politika řízení přístupu,
- popis fyzického zabezpečení,
- postupy pro správu systému,
- likvidace a vyřazení zařízení či zdroje,
- pravidla pro přístup a vyhodnocování služeb třetích stran,
- pravidla pro klasifikaci a označování informací,
- pravidla pro zacházení s informacemi,
- bezpečnost zařízení při převozu.

8.1. Technické prostředky zajišťující včasné rozpoznání nepovoleného přístupu k radionuklidovému zdroji

Jedná se o technické prostředky (viz příloha č. 4 a 5) určené pro detekci vstupu nebo pokusu o vstup narušitele do zabezpečeného prostoru s akustickou či optickou signalizací. Jde tedy o zařízení, které slouží k ochraně osob a majetku. Provedení může být jako drátový elektronický zabezpečovací systém, případně jako bezdrátový elektronický zabezpečovací systém. Pro účely zabezpečení radionuklidových zdrojů je z pohledu bezpečnosti a spolehlivosti zařízení a v neposlední řadě i z důvodů celkových nákladů doporučené využívat drátových systémů s detekcí narušení rozvodů (tamper detekce rozvodů), kdy v případě přerušení rozvodu mezi detekčním prvkem a ústřednou je vyvolán poplach, na který je následně adekvátně reagováno ostrahou objektu. Těmito prostředky je např. poplachový zabezpečovací a tísňový systém (PZTS). V praxi je možné se též setkat se starším termínem - Elektronický zabezpečovací systém (EZS).

Systémy PZTS podle způsobu nasazení:

1. **PZTS pro vnitřní/prostorovou ochranu objektu**, který signalizuje narušení vnitřního prostoru objektu ohraničeného svislými a vodorovnými stavebními konstrukcemi,
2. **PZTS pro ochranu perimetru objektu**, který detekuje narušení obvodu/perimetru objektu – rozumíme tím nejčastěji hranici pozemku, např. plot, obvodová zeď,
3. **PZTS pro plášťovou ochranu objektu**, který signalizuje narušení pláště objektu – svislé či vodorovné stavební konstrukce,
4. **PZTS pro předmětovou ochranu**, který signalizuje bezprostřední přítomnost narušitele v místě střeženého objektu, manipulaci se střeženým zdrojem.

PZTS systém se skládá z jednotlivých prvků:

- **EKV přístupový systém -** přístupový systém slouží jako systém zabezpečení vstupu do budovy. Vstupem jsou vstupní dveře do budovy. Skládá se z kontaktních snímačů docházkových čipů, řídicích dveřních jednotek, napájecích zdrojů a externích zařízení (pohony dveří, elektrické zámky). Nejdůležitějším řídícím faktorem přístupových systémů je přidělování přístupového práva, které se vystavuje konkrétním osobám na základě stupňů oprávnění podle prostorových, časových, personálních a jiných dispozic.

- **Ústředna PZTS -** jedná se o zařízení určené pro příjem a vyhodnocování informací z jednotlivých prvků/periferií systému PZTS. Základními funkcemi jsou např. poplach narušení, přepadení, sabotáže systému – tamper detekce, porucha systému. Dále mohou ústředny zpracovávat signály např. při zatopení, požáru a jiné.

  Zabezpečení a umístění ústředen PZTS - ústředny se umísťují vždy přímo do střežené „zakódované“ oblasti, kdy při takto řešeném umístění, není možné neoprávněně manipulovat se systémem bez předchozího odkódování PZTS. Stejně tak chráníme samotnou ústřednu umístěním do kovového krytu s tamper detektory – spínači, kdy první je umístěn na dvířkách ústředny – detektuje neoprávněné otevření a druhý na zadní straně krytu ústředny a detekuje stržení ústředny ze stěny, na které je připevněna. Ústředna je vybavena AKU baterií pro zajištění minimálně 24 hodinového provozu v případě výpadku hlavního napájení systému – baterie následně zajišťuje napájení jak systému, tak jednotlivých detekčních a ovládacích prvků.

- **Záložní zdroj PZTS -** jedná se o zdroj nepřerušovaného napájení (UPS) s akumulátorem elektrické energie. Primární funkcí UPS je zajistit nepřetržitost střídavého napájení. UPS může také sloužit pro zlepšení jakosti dodávaného výkonu, a to jeho udržováním ve stanovených mezích. V bezpečnostních systémech je UPS aplikována zejména z důvodů udržení funkcionality zařízení i v případě dlouhodobějšího výpadku. Standardně je počítáno a navrhováno UPS na 4 hodiny provozu bez dodávky elektrické energie, a to tak, že UPS zajistí napájení všech komponent (EKV, CCTV i PZTS).

- **Kamerové systémy (CCTV) -** kamerové systémy slouží k monitorování majetku a osob, mají preventivní účinek pro předcházení trestné činnosti a pomáhají při odhalování zločinu. Bezpečnostní kamery snímají obraz monitorovaného prostředí a přenáší obraz do nahrávacího zařízení, které zajišťuje zobrazení na stanovišti obsluhy. Proti poškození a napadení kamerového systému se mohou použít kamery odolávající působením vnějších vlivů.

- **Ovládací prvky PZTS** – jedná se např. o klávesnice, biometrické čtečky a komunikátory.

Klávesnice je nejrozšířenější prvek z pohledu účelu ovládání systému PZTS. Na základě přidělených uživatelských kódů provádí oprávnění uživatelé odkódování či zakódování systému, neboli jeho aktivaci či deaktivaci. Systém PZTS může být ovládán též zcela automaticky – tzn., že ve stanoveném čase provede automatické zakódování či odkódování.

Biometrické čtečky a další systémy řízení přístupu jsou primárně určeny k ovládání a řízení přístupu – tzn., že v případě úspěšné validace uživatele přístupovým systémem může dojít krom otevření dveří i k odkódování systému. Jsou použitelné čtečky oční duhovky, čtečky otisku prstu, skenery krevního řečiště či 3D čtečky obličejů.

Komunikátory - jedná se o GSM komunikátory, GPRS komunikátory, LAN komunikátory, radiové vysílače a telefonní komunikátory. Komunikátory zajišťují přenos zpráv ze zabezpečovací ústředny na PCO, případně na jiné rozhraní uživatele – mobilní telefon, PC či email - prostřednictvím sítí mobilních operátorů (GPRS, SMS), LAN, JTS. V současné době se využívá zejména datových sítí, což umožňuje on-line spojení a přenášení informací v krátkých intervalech, a to včetně krátkých testovacích zpráv, které si systémy mezi sebou posílají v intervalech od 10 s do 90 s. Každá příchozí zpráva, která dorazí na PCO, je zpětně ověřena, aby se vyloučilo zaslání falešné zprávy.

- **Detektory PZTS**
  - *pro vnitřní použití* jsou určeny pro instalaci uvnitř budov a v místech bez vlivu povětrnostních podmínek. Tomuto způsobu použití odpovídá jejich krytí a odolnost proti falešným poplachům, kde se předpokládá výskyt rušivých vlivů,
  - *pro vnější prostředí* mají vyšší stupeň krytí proti vlhkosti a způsob jejich konstrukce a metody vyhodnocování musí počítat s výrazně vyšším výskytem rušení než u detektorů pro prostředí vnitřní (přímý vliv slunce, vítr, déšť, mlha). Další odlišností proti vnitřní detekci je plocha, kterou je potřeba zabezpečit, a ta bývá výrazně větší. Z toho důvodu se u rozsáhlejších instalací volí obvodová ochrana detekující průnik do střeženého prostoru s následnou obrazovou kontrolou pomocí prvků CCTV,
  - *prostorové detektory pohybu (PIR)* detekují pohyb předmětů nebo osob vyzařujících teplo. Zkratka PIR je z anglického názvu „passive infrared detector“ - pasivní infračervený detektor. Čidlo funguje na principu pyroelektrického jevu,
  - *mikrovlnné detektory (MW detekce*) pracují na principu vyhodnocení mikrovlny odražené od předmětu (Dopplerův jev),
  - *duální detektory* pracují na principu kombinace PIR a MW detekce. Tyto detektory se používají do vyloženě problematických prostor s vysokým nárokem na odolnost proti falešným poplachům. PIR detektor snímá teplo**,** MW detektor snímá pohyb**.** Tímto způsobem se velmi účinně eliminuje například vliv teplého vzduchu, který dokáže narušit PIR detektor, ale MW složku neaktivuje,
  - *ultrazvukové detektory* fungují na principu Dopplerova jevu – posun frekvence ultrazvuku, obvyklá frekvence 40 kHz,
  - *pasivní detektory* jsou využívány zejména jako tamper spoje, kdy detekujeme jejich přerušení při neoprávněné manipulaci se zdrojem. Pasivními detektory jsou např. magnetické kontakty sloužící pro detekci otevření oken, dveří a vrat, kde je detekováno samotné otevření a současně je zaznamenán příchodový čas.

- *požární detektory* reagují na změnu teploty ve střeženém prostoru a slouží pro včasnou detekci požáru. Je možné použít autonomní detektory napájené baterií s vlastní sirénou anebo detektory napájené a vyhodnocované ústřednou. Detektory plynu jsou určeny k detekci přítomnosti nebezpečného plynu v zabezpečeném prostoru.

- **Systém generálního klíče**

  Spolehlivým zabezpečením objektu je využití systému generálního klíče. Tímto klíčem je možné bez omezení procházet všemi vstupy v celém systému. Jedná se o systémy uzamykání s jednoduchým ovládáním. Výhodou je možnost uzamknutí celé budovy jediným klíčem. I přesto, že se uzamkne celá budova jediným klíčem, stále se jedná o originál pro každé dveře. V rámci systému umožňuje uzamknout všechny vložky. Tento klíč zpravidla vlastní osoba nejvýše postavená v systému řízení subjektu. A další klíč – záložní, bývá uložen v trezoru.

- **Mechanické zabezpečení objektu**

  Jelikož samotný elektronický zabezpečovací systém, kamerový systém a přístupový systém nezajišťuje bezpečnost objektu, nýbrž jen detekuje a zaznamenává pokusy o napadení, je nutné tyto elektronické systémy doplňovat prvky mechanického zabezpečení. Kombinace mechanického a elektronického zabezpečení společně utváří nejvhodnější ochranu zdrojů.

- **Signalizační prvky**

  Jedná se o vnitřní sirény s blikačem či stroboskopem (akustická signalizace) a tísňové hlásiče sloužící k vyvolání poplachu v případě přímého ohrožení osob**.** Hlásiče je možné instalovat skrytě anebo otevřeně, poplach je vyvolán manuálně stiskem tlačítka. Tísňové hlásiče umístěné na veřejném a viditelném místě je nutné chránit před neúmyslným vyhlášením poplachu (nutno promáčknout ochranné sklíčko).

Seznam příloh:

Příloha č. 1
Modelový plán zabezpečení prostoru s radionuklidovým zdrojem 1. kategorie zabezpečení (např. pracoviště s radioterapeutickým ozařovačem).

Příloha č. 2
Modelový plán zabezpečení prostoru s radionuklidovým zdrojem 2. kategorie zabezpečení (např. defektoskopická základna – uložení krytů s uzavřeným radionuklidovým zdrojem).

Příloha č. 3
Modelový plán zabezpečení prostoru s radionuklidovým zdrojem 3. kategorie zabezpečení (zdroj umístěný v místnosti nebo na pracovišti podobného typu).

Příloha č. 4
Technické prostředky zajišťující včasné rozpoznání nepovoleného přístupu k radionuklidovému zdroji.

Příloha č. 5
Technické prostředky zajišťující včasné rozpoznání nepovoleného přístupu k radionuklidovému zdroji.

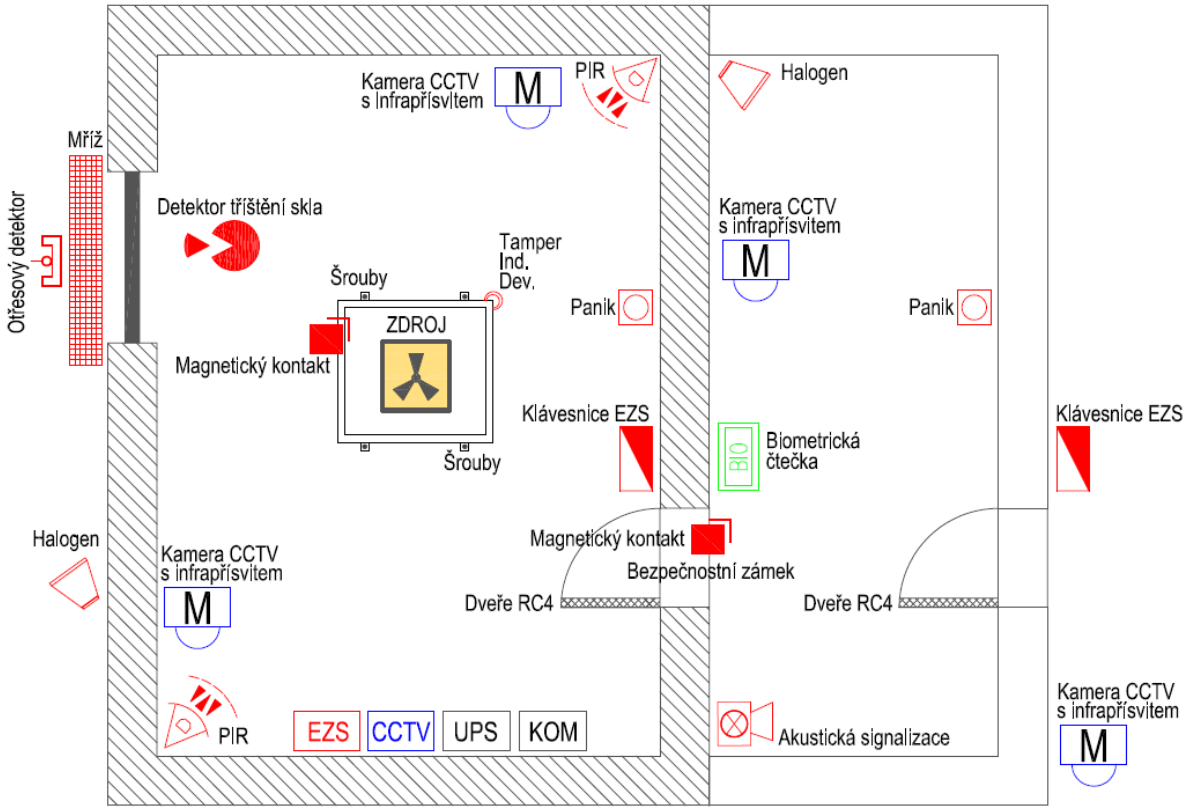
Příloha č. 6
Bezpečnostní prvky.

Příloha č. 7
Harmonogram postupu při provádění zásahu.

Příloha č. 8
Příklad plánu zabezpečení (pracoviště I. kategorie zabezpečení, ozařovač krve).

Příloha č. 1:

Modelový plán zabezpečení prostoru s radionuklidovým zdrojem 1. kategorie zabezpečení (např. pracoviště s radioterapeutickým ozařovačem).



Základní principy:

Plášťová ochrana je zajištěna bezpečnostními mřížemi vybavenými otřesovými detektory, detektorem tříštění skla, 2 x bezpečnostními dveřmi kategorie RC4 oddělujícími prostory, bezpečnostním zámkem a magnetickým kontaktem. Vstup do prostor je dále monitorován CCTV kamerou a řízen systémem EKV (biometrickou čtečkou otisku prstu) případně čtečkou PIN nebo prox karet.

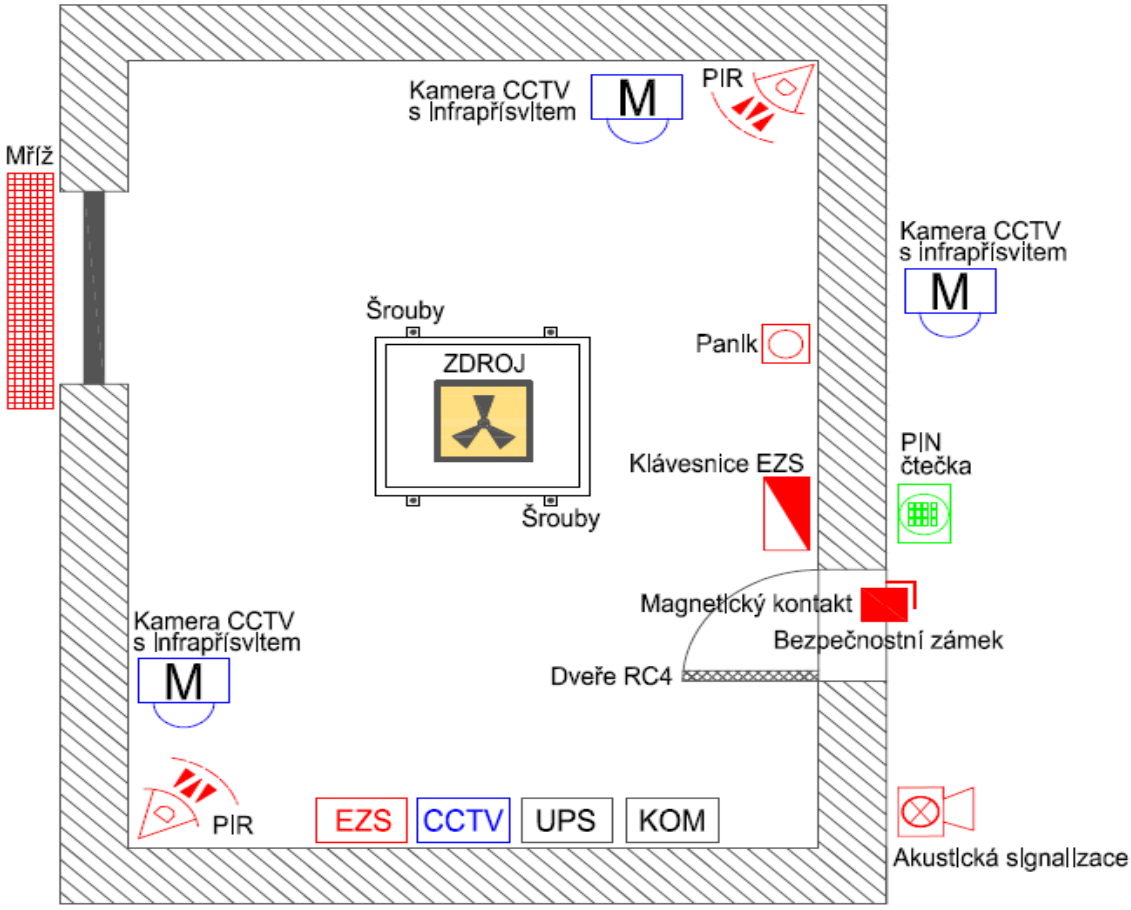
Vnitřní ochrana zajištěna PIR detektory pohybu, kamerovým systémem a panikovými tlačítky.

Ochrana zdroje zajištěna tamper detektorem (např. optická smyčka - aktivní kabel), magnetickým kontaktem (ideálně trojitě polarizovaným), mechanicky je zdroj zajištěn bezpečnostními šrouby k podlaze (s jedinečným typem hlavice).

Pozn. Ústředna PZTS, komunikátor s PCO a GSM komunikátor, UPS, záznamové zařízení CCTV – jsou vždy umístěné uvnitř chráněné oblasti.

Příloha č. 2:

Modelový plán zabezpečení prostoru s radionuklidovým zdrojem 2. kategorie zabezpečení (např. defektoskopická základna – uložení krytů s uzavřeným radionuklidovým zdrojem).



Základní principy:

Plášťová ochrana zajištěna bezpečnostními mřížemi, bezpečnostními dveřmi kategorie RC4 oddělujícími prostory od venkovních a společných prostor, bezpečnostním zámkem a magnetickým kontaktem. Vstup do prostor je dále monitorován CCTV kamerou a řízen systémem EKV – čtečkou PIN nebo prox karet.

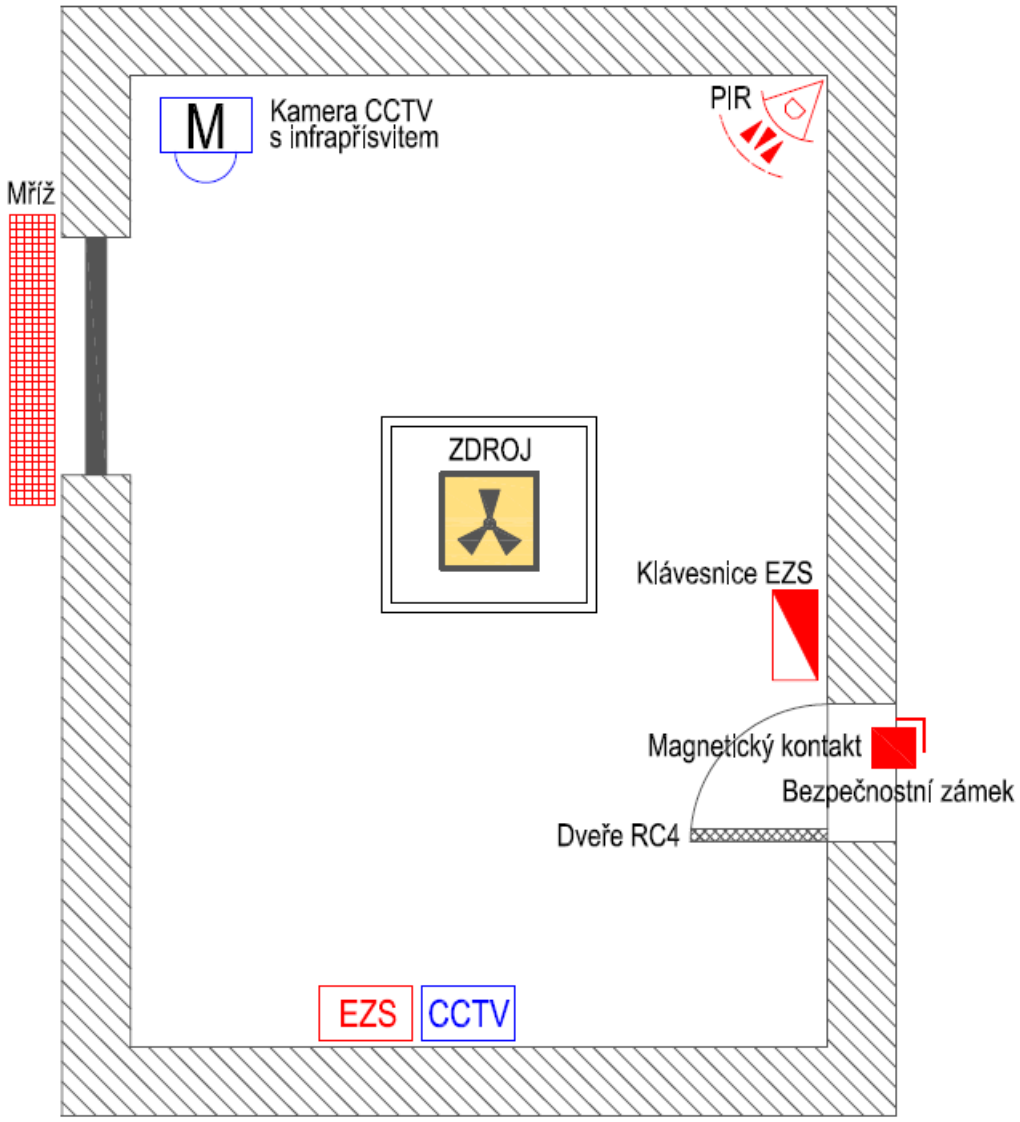
Vnitřní ochrana zajištěna PIR detektory pohybu, kamerovým systémem, panikovými tlačítky.

Ochrana zdroje zajištěna mechanicky - zdroj zajištěn bezpečnostními šrouby (s jedinečným typem hlavice).

Pozn. Ústředna PZTS, komunikátor s PCO a GSM komunikátor, UPS, záznamové zařízení CCTV – jsou vždy umístěné uvnitř chráněné oblasti.

Příloha č. 3:

Modelový plán zabezpečení prostoru s radionuklidovým zdrojem 3. kategorie zabezpečení (zdroj umístěný v místnosti nebo na pracovišti podobného typu).



Základní principy:

Plášťová ochrana zajištěna bezpečnostními mřížemi vybavenými, bezpečnostními dveřmi kategorie RC4 oddělujícími prostory od venkovních a společných prostor, bezpečnostním zámkem, magnetickým kontaktem. Vstup do prostor může být monitorován CCTV kamerou.

Vnitřní ochrana zajištěna PIR detektory pohybu, kamerovým systémem a panikovými tlačítky.

Pozn. Ústředna PZTS, komunikátor s PCO a GSM komunikátor, UPS, záznamové zařízení CCTV – jsou vždy umístěné opět uvnitř chráněné oblasti.

Příloha č. 4:
Technické prostředky zajišťující včasné rozpoznání nepovoleného přístupu k radionuklidovému zdroji (ilustrativní obrázky).

Obr. 1 LCD Ovládací klávesnice PZTS.

Obr. 2 Snímač otisků prstů.

Obr. 3 Bezdotyková kovová čtečka identifikačních karet.

Obr. 4 Analogový detektor pohybu.

Obr. 5 Duální pohybový detektor.

Obr. 6 Stropní detektor pohybu.

Příloha č. 5:

Technické prostředky zajišťující včasné rozpoznání nepovoleného přístupu k radionuklidovému zdroji (ilustrativní obrázky).

Obr. 7 Detektor tříštění skla.

Obr. 8 Panikové tlačítko.

Obr. 9 Magnetický spínací kontakt.

Obr. 10 Tísňový hlásič.

Obr. 11 Externí siréna s blikačem.

Příloha č. 6: Bezpečnostní prvky.

Bezpečnostní prvky jako dveře, mříže, zámky, zámkové vložky, kování apod. mají dle norem ČSN EN 1627 (746001, datum vydání 1. 1. 2012) „Dveře, okna, lehké obvodové pláště, mříže a okenice - Odolnost proti vloupání - Požadavky a klasifikace“ a ČSN EN 1630+A1 (76004, datum vydání 1. 1. 2017) „Dveře, okna, lehké obvodové pláště, mříže a okenice - Odolnost proti vloupání - Zkušební metoda pro stanovení odolnosti proti manuálním pokusům o vloupání“ vždy své označení - tzv. **bezpečnostní třídy**, kterých je celkem **6** (u dveří zpravidla třídy **2, 3, 4**). Dříve se značila zkratkou **BT**, od roku 2012 je to zkratka **RC**. Stupeň bezpečnostní třídy (RC) je dán tím, co musí vydržet bezpečnostní prvek při případné snaze o překonání zlodějem a jeho nářadím.

RC1 – příležitostný zloděj se pokouší o vloupání s použitím malého jednoduchého nářadí a fyzickým násilím, např. kopáním, narážením ramenem, zdviháním, vytrháváním. Zloděj nemá žádné zvláštní znalosti o úrovni odolnosti MZS, má málo času a snaží se nezpůsobit hluk.

RC2 – příležitostný zloděj se navíc pokouší o vloupání s použitím jednoduchého nářadí a fyzickým násilím. Má malé znalosti o úrovni odolnosti MZS, má málo času a snaží se nezpůsobit hluk.

RC3 – zloděj se pokouší překonat MZS při použití páčidla délky 710 mm a dalšího šroubováku, ručního nářadí, jako malé kladívko, důlčíky a mechanická ruční vrtačka. Zloděj má určité povědomí o systému uzávěru a s tímto nářadím je schopen těchto znalostí využít. Při použití páčidla délka 710 mm lze aplikovat zvýšené fyzické násilí.

RC4 – zkušený zloděj používá navíc zámečnické kladivo, sekeru, dláta, sekáče, přenosnou akumulátorovou vrtačku atd. Toto další nářadí umožňuje zloději rozšířit počet způsobů napadení, případně jejich kombinace – vrtání, sekání, páčení, atd. Problém hluku zloděj neřeší.

RC5 – velmi zkušený zloděj používá navíc jednoruční elektrické nářadí např. úhlovou brusku do průměru kotouče 125 mm, přímočarou pilu atd. Neznepokojuje se hlukem.

RC6 – velmi zkušený zloděj používá navíc dvouruční elektrické nářadí např. úhlovou brusku do průměru kotouče 230 mm, přímočarou pilu atd. Neznepokojuje se hlukem.

Pro účely zabezpečení radionuklidových zdrojů, je na pracovištích se zdroji 1. - 3. kategorie zabezpečení doporučeno využívat u mechanických prvků bezpečnostní třídu RC4. Veškeré vstupy a možné přístupy ke zdroji by měly být ideálně osazeny bezpečnostními dveřmi a mřížemi v bezpečnostní třídě RC4. Dle mezinárodních doporučení a standardů, je mechanické zabezpečení zdroje doporučeno řešit prostřednictvím minimálně 2 ks pevných mechanických bariér např. 2 x bezpečnostní ocelové dveře, nebo 1 x bezpečnostní dveře a 1 x mříže dle typu a členění objektu.

Příloha č. 7: Harmonogram postupu při provádění zásahu.

ČAS (min.)	**OPERAČNÍ DŮSTOJNÍK (OPD)**	**ZÁSAHOVÁ JEDNOTKA BEZPEČNOSTNÍ SLUŽBA**	**ZÁKAZNÍK NEBO OSOBA UVEDENÁ ZÁKAZNÍKEM V SEZNAMU KONTAKTNÍCH OSOB**
1	OPD informuje ZJ o přijetí a typu poplachové události na objektu	ZJ vyjíždí ihned po přijetí signálu k prověření poplachové události	
2	V případě, kdy do 1 minuty od přijetí poplachové zprávy na PCO je systém deaktivován platným kódem – je poplach považován za planý		
2	OPD informuje zákazníka na tel. č. dle seznamu o přijetí a typu poplachové události na objektu		Klient v případě přijetí poplachové události je oprávněn odvolat výjezd po uvedení platného komunikačního hesla
3	V případě že OPD obdrží při kontaktu se zákazníkem heslo ke zrušení poplachu, odvolává ZJ	ZJ se ihned po přijetí informace o odvolání poplachové události vrací na základnu	
3+	Pokud se OPD nedovolá, nebo klient poplach potvrdí, nechá OPD ZJ pokračovat v provedení zásahu		
4	Operační důstojník provádí kontrolu stavu EZS a poplachové události s cílem určit místo vniknutí a pohyb pachatele		
5+	OPD informuje ZJ o místě narušení a pohybu pachatele, popřípadě je-li v objektu klient nebo jeho rodinní příslušníci	ZJ ihned po dojezdu rozpečetí klíč (v případě, že jsou klíče k dispozici) a provádí kontrolu pláště dle informací o místě narušení	
6+		ZJ komunikuje s OPD o času příjezdu k narušenému objektu a následné taktice.	
7+	Operační důstojník v případě potvrzení o narušení objektu vyrozumí PČR a informuje ZJ o přivolání policie	ZJ rozpečetí klíč (v případě, že jsou klíče k dispozici) od vstupu do objektu a zahájí fyzickou kontrolu vnitřní části objektu.	

	OPD informuje zákazníka o postupu při kontrole objektu, zjištěném stavu, přivolání policie aj.	ZJ zajišťuje na pokyn OPD objekt střežením do doby příjezdu Policie ČR a majitele (klienta). Pokud nedošlo k informování → 24hod.ostraha	Klient je informován o postupu, stavu objektu a rozhoduje o dalším postupu (střežení do jeho příjezdu atp.)
	OPD Zajistí zapečetění použitých klíčů / vstupních prostředků		
	OPD provede důkladný zápis do KNIHY ZÁZNAMŮ PCO + do SW PCO		

Příloha č. 8:

Příklad plánu zabezpečení (pracoviště I. kategorie zabezpečení, ozařovač krve).

PLÁN ZABEZPEČENÍ

radionuklidového zdroje (ozařovače krve) na pracovišti
Transfúzního oddělení nemocnice XX

Označení: č. XXX/20XX

Platnost od: X. X. 20XX

Autor:

Zodpovídá:

Schválil:

Obsah

1. Úvod

Plán zabezpečení vychází z požadavků ustanovení § 164 odst. 1 a 2 zákona č. 263/2016 Sb., atomový zákon, a požadavků vyhlášky č. 422/2016 Sb., o radiační ochraně a zabezpečení radionuklidového zdroje, při vykonávání činností v rámci plánované expoziční situace – ozařování krevních přípravků před aplikací pacientovi pomocí radionuklidových zdrojů.

Dokument popisuje plán zabezpečení zařízení obsahující radionuklidový zdroj - ozařovač typu Gammacell 3000 ELAN Na Transfuzním oddělení nemocnice. Podle ustanovení § 17 vyhlášky č. 422/2016 Sb. se jedná o pracoviště I. kategorie zabezpečení. Plán zabezpečení je součástí…(např. integrovaného systému managementu vytvořeného podle ČSN EN ISO).

2. Definice a zkratky *(např.)*

ZIZ	-	*zdroj ionizačního záření*
SÚJB	-	*Státní úřad pro jadernou bezpečnost*
RC SÚJB	-	*Regionální centrum SÚJB*
RO	-	*radiační ochrana*
RP	-	*radiační pracovník*
URZ	-	*uzavřený radionuklidový zdroj*
PZTS	-	*Poplachový zabezpečovací a tísňový systém*
PCO	-	*Pult Centralizované Ochrany*
CCTV	-	*Closed Circuit Television (televizní okruh)*
EKV	-	*Elektronická kontrola vstupu*

3. Identifikace společnosti

Název	
Sídlo	
Identifikační číslo	
Pracoviště	
Statutární orgán	
Evidenční číslo SÚJB	

4. Cíle plánu zabezpečení

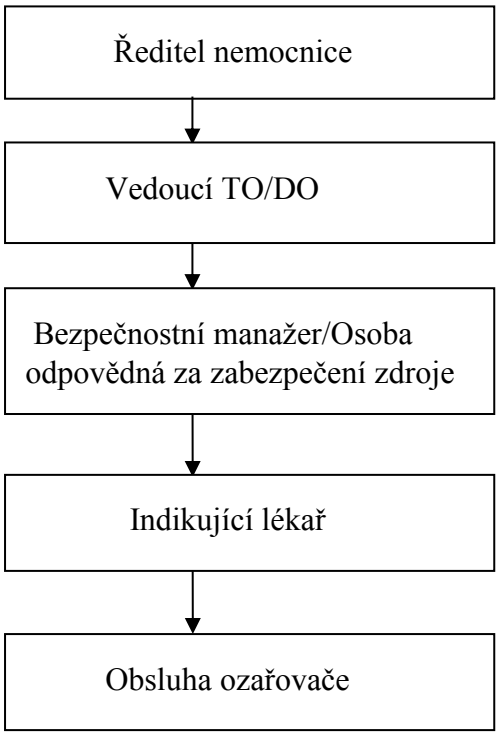
Povinnost zabezpečit radioaktivní zdroje je dána ustanovením § 164 zákona č. 263/2016. Prováděcí právní předpis – vyhláška č. 422/2016 Sb. stanoví požadavky na způsob zabezpečení radionuklidového zdroje 1. kategorie zabezpečení.

Cílem tohoto plánu zabezpečení je:

- zamezit vstupu cizí osoby k ozařovači krve a zabránit manipulaci, zneužití, odcizení a přemístění zdroje,
- rozpoznat nepovolený přístup k radionuklidovému zdroji,
- odhalit každý pokus o nepovolený přístup k radionuklidovému zdroji včetně pokusu o nepovolený přístup zaměstnance nemocnice (insider),
- zajistit opatření k odhalení a zdržení nepovoleného přístupu k radionuklidovému zdroji,
- zajistit systém zábran ke zdržení přemístění radionuklidového zdroje.

Za tímto účelem byla držitelem povolení ustanovena osoba odpovědná za zajištění zabezpečení používaného radionuklidového zdroje (ozařovač krve) na pracovišti transfuzního oddělení nemocnice. Zařízení s radionuklidovým zdrojem mohou obsluhovat pouze určení a zaškolení pracovníci. Seznam oprávněných a zaškolených pracovníků je přílohou tohoto dokumentu.

5. Organizační struktura společnosti (příklad)



6. Odpovědnosti a pravomoci osob

Statutární zástupce (ředitel nemocnice):
Celkovou nedílnou odpovědnost za zabezpečení radionuklidového zdroje nese statutární orgán držitele povolení. Statutární zástupce ustanovuje k provádění činností v oblasti zabezpečení zdroje odpovědnou osobu, která je odpovědná za zajištění zabezpečení používaného radionuklidového zdroje. Statutární zástupce je zodpovědný za organizační, personální a materiálové zajištění provozu oddělení, kterému patří ozařovač.

Vedoucí Transfuzního oddělení:
Je zodpovědný za zajištění provozu zařízení. Ve spolupráci s osobou zodpovědnou za zabezpečení zdroje (bezpečnostní manažer) stanovuje konkrétní postup zabezpečení zdroje na oddělení.

Osoba odpovědná za zabezpečení zdroje:

Společně s vedoucím oddělení stanovuje konkrétní postup zabezpečení zdroje, pravidelně ověřuje funkčnost zavedeného systému zabezpečení, zajišťuje ochranu informací o zabezpečení zdroje a vypracovává zásahové postupy a instrukce pro případ zneužití zdroje či jeho přemístění, ztráty apod.

Tato osoba je odpovědná za proškolení pracovníků o zabezpečení radionuklidového zdroje, vypracovává a aktualizuje plán zabezpečení a kontroluje dodržování stanového postupu pravidelnými a náhodnými kontrolami. Osoba odpovědná za zabezpečení radionuklidového zdroje zajišťuje řízení zásahu při mimořádné události v koordinaci se zásahovými složkami.

Upřesnění: vzhledem k povinnostem vyplývajících z požadavků vyhlášky by tato osoba neměla být osobou vykonávající soustavný dohled nad radiační ochranou. Jedná se o dvě odlišné věci – vykonávání soustavného dohledu nad RO a zajištění zabezpečení zdroje I. kategorie (podle vyhlášky č. 422/2016 Sb. jsou to povinnosti odlišné).

Obsluha ozařovače:

Obsluha ozařovače (lékař, zdravotní sestra, zdravotní laborant) postupuje dle tohoto plánu zabezpečení. Je zodpovědná za provedení požadovaného úkonu ozáření, zaznamenání této činnosti a dodržování stanoveného postupu zabezpečení zdroje na oddělení. Nedodržení postupu je hodnoceno jako porušení pracovních povinností.

7. Identifikace radionuklidových zdroje

7.1 Kategorizace radionuklidového zdroje dle kategorie zabezpečení

Na pracovišti transfuzního oddělení se používá uzavřený radionuklidový zdroj ^{137}Cs, který je součástí zařízení typu Gammacell 3000 ELAN. Dle § 17 odst. 1 písm. b) vyhlášky č. 422/2016, je ozařovač krve zařazen do l. kategorie zabezpečení.

7.2 Způsob použití zdroje a místa používání

Uzavřený radionuklidový zářič ^{137}Cs o certifikované aktivitě XX,X TBq ke dni XX.XX.20XX (výrobní číslo XX) je určen pro ozařování krevních přípravků před aplikací pacientovi. Zdroj je odstíněn, v přístroji je zabudován fixním způsobem. Obsluha vloží ozařované přípravky do kontejneru, který si přístroj po stisknutí tlačítka „START“ sám přesune ke zdroji. Obsluha tedy se zdrojem sama nemanipuluje. Výrobcem je firma XX, USA, výrobní číslo přístroje je XXX. Hmotnost přístroje je XX kg.

7.3 Umístění budov a areálu vzhledem k přístupným místům

Budova Transfuzního oddělení se nachází na jižní straně areálu nemocnice, přístup pro veřejnost do budovy je…Plánek areálu (příloha č. X) je součástí tohoto dokumentu. Areál se nachází v hustě osídlené/neosídlené části města XX. Přístroj je umístěn v místnosti č. XX v suterénu/nadzemním podlaží TO nemocnice, pavilon XX. Plánek suterénu/nadzemního podlaží nemocnice je součástí tohoto dokumentu (příloha č. X).

8. Systém zabezpečení radionuklidového zdroje

Zabezpečení ozařovače krve na Transfuzním oddělení nemocnice je navrženo takovým způsobem, aby splňovalo základní funkce, kterými jsou - odrazení, detekce, zdržení, zásah a řízení zabezpečení. Pro účely odrazení neautorizované osoby od možného pokusu o přemístění či zneužití radionuklidového zdroje je na našem pracovišti zavedeno…. (např. oplocení, kamery, detektory pohybu, fyzická ostraha). Tyto prostředky mají za cíl přesvědčit neautorizovanou osobu o tom, že nebude snadné se dostat ke zdroji a provést svůj záměr.

Řízení zabezpečení radionuklidového zdroje zahrnuje zajištění dostatečných personálních a finančních zdrojů pro zabezpečení radionuklidového zdroje, vypracování postupů a plánů a ochrana informací o systému zabezpečení. S ohledem na zajištění účinnosti systému zabezpečení a kultury zabezpečení je s těmito informacemi zacházeno uvážlivým přístupem. S tímto plánem zabezpečení radionuklidového zdroje jsou seznámeni pouze odpovědní a důvěryhodní pracovníci. Stěžejní funkce systému zabezpečení (detekce, zdržení a zásah) jsou detailně popsány v dalších bodech tohoto plánu zabezpečení.

Upřesnění:
Detekce nepovoleného přístupu k radionuklidovému zdroji 1. kategorie zabezpečení musí zajistit:

- *odhalení každého pokusu o nepovolaný přístup k radionuklidovému zdroji, musí být zajištěno vhodným zařízením a signalizací včetně přenosu do dohledového centra (PCO). Zajištění této funkcionality musí být provedeno adekvátním umístěním zdroje z pohledu polohy v objektu a stavebního řešení, kdy vstupy a přístupy ke zdroji jsou monitorovány detektory zabezpečovacího systému a řízeny elektronickým přístupovým systémem,*
- *odhalení pokusu o nepovolaný přístup k radionuklidovému zdroji nepovolaným pracovníkem držitele povolení (insider) by mělo být zajištěno prostřednictvím instalovaných bezpečnostních technologií, kdy je neoprávněný přístup detekován.*
- *získání informací nezbytných k neprodlenému vyhodnocení zjištěného nepovoleného přístupu, je prováděno výstupy z EZS, EKV, CCTV (kamerový systém) a následně přenášeno na PCO.*

Zdržení dostatečné k zahájení zásahu:

- *je propočítáváno z času první detekce pokusu o vniknutí do objektu, potřebné doby na překonání mechanických zábran pro vstup do objektu (mříže, bezpečnostní dveře, bezpečnostní nerozbitné folie na prosklených plochách, nerozbitné prosklené plochy),*
- *dalším zdržením a navýšením času pro zásah je zajištění samotného zdroje mechanickým zabezpečením např. připevněním zařízení se zdrojem k pevné části objektu, případně navařením či jiným mechanickým připevněním přípravků bránících v manipulaci se zdrojem (kotvy, ocelové popruhy, ocelové pásy),*

- *navyšováním těchto opatření a jejich stupňováním, získáváme po celkovém sečtení dobu, kdy je nutné provést adekvátní zásah přímo na objektu (v místě umístění zdroje).*

Zásah, který vede k zabránění neoprávněnému přemístění radionuklidového zdroje:

- *po vyhodnocení první detekce a potvrzení, že došlo k neautorizovanému přístupu ke zdroji, musí držitel povolení neprodleně zajistit provedení adekvátního zásahu,*
- *k tomu je nutné vzít v úvahu proti jakému jednání (útoku či narušení) je zásah veden a v souvislosti s tím uplatňovat přiměřenost a účinnost zásahu,*
- *zjištěný nepovolaný přístup, může mít charakter přímého přijetí poplachové zprávy od zabezpečovacího systému o narušení místa se zdrojem nebo ohlášením takovéto skutečnosti obsluhou zařízení, zaměstnancem, či jinou osobou, která tuto událost zjistí.*
- *informace o nepovoleném přístupu může být také předána obsluhou např. pomocí tlačítka stavu nouze (panikové tlačítko), tlačítka nátlaku na klávesnici EZS, či zadáním nátlakového kódu, případně zadáním nátlakového otisku prstu u biometrických systémů řízení přístupu,*
- *samotný zásah by měl být proveden ostrahou objektu, zásahovou skupinou externího poskytovatele bezpečnostních služeb, případně přímo složkami Policie ČR,*
- *systémem reakce se rozumí předem zpracovaný plán zásahu a jeho postupy směřující k prověření takovéto krizové události, způsob jakým bude samotný zásah prováděn a kým bude prováděn.*

Možný popis: *přístupové dveře do místnosti s ozařovačem krve jsou vybaveny bezpečnostním/elektronickým zámkem na kartu, z vnější strany jsou vybaveny koulí… Okna místnosti jsou vybavená speciální ochrannou fólií. Přístupové vjezdy do nemocnice jsou zabezpečené monitorovány kamerovým systémem a zajištěny bezpečnostní agenturou. V prostorech ozařovače a chodby je nainstalována kamera s napojením na stálou službu. Ve vnitřním areálu nemocnice jsou prováděny pravidelné pochůzky pracovníky bezpečnostní agentury s četností…. Proti neoprávněnému použití ozařovače je přístroj vybaven bezpečnostním klíčkem pro spuštění alarmu. Dále uveďte popis režimu den/noc (zajištění pracoviště/kódování v mimopracovní době apod.).*

9. Popis opatření k zabezpečení radionuklidového zdroje

9.1 Kontrola přístupu ke zdroji

Navržený režim kontroly přístupu ke zdrojům zajišťuje (pospat v níže uvedeném smyslu):

- *režim pohybu osob v místě umístěné ozařovače krve s radionuklidovým zdrojem v pracovní a mimopracovní době,*
- *režim manipulace s klíči, identifikačními prostředky a médii, které se používají pro systém vstupu (pokud se používají), přidělování a odevzdávání klíčů, jejich úschova a evidence, uložení případných duplikátů a způsob jejich použití,*
- *režim manipulace s technickými prostředky a jejich používání (kamerové, přístupové a zabezpečovací systémy).*

Do míst, kde je umístěn ozařovač krve by měli mít povoleno vstupovat pouze určené osoby, u kterých byla ověřena důvěryhodnost. Přístup k ozařovači by měl být evidován zápisem do deníku případně elektronicky. Klíče od těchto prostor vydávat pouze oprávněným osobám. Pohyb ostatních osob je dovolen pouze v doprovodu oprávněné osoby.

Možný popis:
Přístup do místnosti s ozařovačem krve je možný dvěma vchody z hlavní chodby. Pro zajištění kontroly přístupu k ozařovači je na pracovišti zavedeno režimové opatření za využití organizačních opatření a technických prostředků. Klíč od místnosti s ozařovačem krve je uložen na úseku expedice Transfuzního oddělení. Pracovník, který provádí ozařování vzorků, převezme klíč proti podpisu a přípravky k ozáření. Po ukončení práce klíč vrátí spolu s přípravky na určené místo.

9.2 Detekce nepovoleného přístupu ke zdroji

Pro účely detekce nepovoleného přístupu k ozařovači krve je na našem pracovišti zavedeno…
Dále popište, jakým způsobem bude zajištěna detekce, tzn. zjištění toho, že je něco v nepořádku - např. v pracovní době zjištění obsluhy či někoho dalšího, kdo provádí přímou fyzickou kontrolu zdroje, nebo detekování nepovoleného přístupu ke zdroji pomocí kamerového systému (v mimopracovní době) či pomocí signalizačních a pohybových detektorů, eventuálně dalšími prostředky.

9.3 Zdržení nepovoleného přístupu ke zdroji

Pro účely zdržení nepovoleného přístupu k radionuklidovému zdroji je na našem pracovišti zavedeno, instalováno, např.:

- uzamykatelné dveře, mříže,
- zabezpečení oken proti vniknutí,
- okna místnosti jsou vybavená speciální ochrannou fólií,
- zdroj je pevně zabudován v zařízení,
- zařízení se zdrojem je připevněno do podlahy kotevními šrouby,
- jiné.

Upřesnění: v případě pokusu o neautorizovaný přístup ke zdroji je žádoucí ztížit protivníkovi cestu k zařízení se zdrojem. Jde o navýšení času (zdržení), který neoprávněná osoba potřebuje k tomu, aby se dostala k ozařovači krve a získala nad ním kontrolu. Zdržení přístupu může být provedeno pomocí fyzických barier či mechanických zábranných prostředků. Vytvořením těchto bariér získáváme dobu, kdy je nutné provést adekvátní zásah. Pro účely zabezpečení radionuklidových zdrojů je doporučeno využívat u mechanických prvků vhodnou bezpečnostní třídu.

9.4 Způsob zásahu při nepovolaném přístupu

Při zjištění, že došlo k nepovolenému přístupu k ozařovači krve, personál neprodleně kontaktuje osobu odpovědnou za zabezpečení zdroje a vedení nemocnice. V případě že je odhalena manipulace se zařízením neoprávněnou osobou, je bezprostředně kontaktována zásahová složka (bezpečnostní agentura, příslušné oddělení PČR). Pro účely provedení zásahu na zjištěný a potvrzený nepovolený přístup ke zdroji je na našem pracovišti zaveden následující postup.

Upřesnění: je nutné adekvátním způsobem reagovat a provést předem stanovená opatření, které směřují k realizaci provedení zásahu. Je však potřeba rozlišit pracovní a mimopracovní dobu. Cílem zásahu je zabránění nepovolené činnosti, zajištění neautorizované osoby a získání opětovné kontroly nad zdrojem. Jedná se o akci odpovědných pracovníků, fyzické ostrahy či příslušníků Policie ČR.

9.5 Způsob komunikace mezi odpovědnými osobami

Zde uveďte popis způsobu komunikace mezi odpovědnými osobami, a to jak v pracovní, tak i v mimopracovní době. Kontakty na odpovědné osoby uveďte v příloze plánu zabezpečení.

9.6 Zabezpečení zdroje během jeho přepravy

Zařízení není přenosné, je využíváno na stabilním pracovišti pro účely ozařování krevních přípravků. Přeprava radionuklidového zdroje není prováděna, zdroj je pevně zabudován v přístroji - ozařovači Gammacell, který je upevněn do podlahy kotevními šrouby.

10. Popis administrativních opatření k zabezpečení zdrojů

10.1 Práva a povinnosti pracovníků

Obsluha ozařovače postupuje v souladu s tímto plánem zabezpečení. Je zodpovědná za provedení ozáření vzorků a současně je povinna dodržovat zavedený režim zabezpečení radionuklidového zdroje.

S přístrojem smí manipulovat pouze oprávněná osoba, která prošla školením pro práci na daném přístroji a která byla seznámena s tímto plánem zabezpečení. Při odchodu z místnosti, kde je umístěn ozařovač, je každý pracovník povinen zkontrolovat, že přístupové vchody jsou uzamčené a je zamezeno možnému vstupu nepovolaným osobám.

V případě, že se v prostorách ozařovače nachází jiná osoba než obsluhující personál např. servisní technik, je obsluhující personál povinen být přítomen společně s touto osobou. V případě servisního zásahu je osoba provádějící servisní úkon povinna provést záznam o této činnosti. Osoba, která provedla ozáření vzorků, je rovněž povinna provést záznam.

10.2 Zabezpečení v případě údržby a oprav prvků systému zabezpečení

Během údržby či opravy zavedeného systému zabezpečení, kdy není bezpečnostní systém aktivní, jsou nastavena zvláštní pravidla (opatření), která zajistí, že zdroj bude i nadále pod přímou kontrolou. *Dále uveďte popis způsobu zabezpečení zdroje, pokud systém není funkční (je odstaven)…*

10.3 Zajištění ochrany informací důležitých z hlediska zabezpečení

Výše uvedené informace může držitel povolení poskytnout pouze osobám, které je potřebují pro výkon jim svěřené činnosti a pouze v rozsahu, který k tomuto výkonu potřebují. Držitel povolení pravidelně prověřuje důvěryhodnost osob, kterým jsou předávány informace o zdrojích, jejich zabezpečení a režimových opatření. Každý pracovník je povinen zachovávat mlčenlivost o zabezpečení zdroje a s ním spojených informací.

Upřesnění: je zcela na Vašem rozhodnutí jakou formou bude důvěryhodnost osob ověřena a co bude rozhodující – např. pohovor s pracovníkem, délka jeho praxe v zaměstnání (na pracovišti se zdrojem), názor a doporučení osoby odpovědné za zabezpečení či rozhodnutí vedení.

Držitel povolení musí rovněž zajistit ochranu informací, které se vztahují k zabezpečení radionuklidového zdroje. Mohou jimi být např. informace o poplachovém a tísňovém systému, zavedeném kamerovém okruhu, způsobu provedení zásahu.

Další informace důležité z hlediska zabezpečení radionuklidových zdrojů se týkají organizační struktury zaměstnanců, kteří mají přístup ke zdroji, případně mají oprávnění používat a ovládat zabezpečovací prostředky, informace týkající se ovládání a zacházení s elektronickým přístupovým systémem (pokud je zaveden), klíčového hospodářství a systému generálního klíče.

Podle vyhlášky č. 422/2016 Sb. jsou informacemi důležitými z hlediska zabezpečení radionuklidového zdroje:
- *údaje o radionuklidových zdrojích a jejich*
- *umístění, plánované způsoby přepravy a její trasy,*
- *údaje obsažené v plánu zabezpečení,*
- *údaje o systému zabezpečení,*
- *údaje o ostraze,*
- *údaje o administrativních opatřeních v rámci zabezpečení*
- *radionuklidového zdroje a*
- *údaje o zásahu.*

Dokumenty, SW případně související soubory, musí být uchovávány v uzamčeném a (elektronicky) střeženém prostoru – kanceláři, řádně uložené bez možnosti přímého neautorizovaného přístupu. Pokud se jedná o SW prvky a soubory uložené v počítači, či na datových nosičích, musejí být tyto řádně zabezpečeny.

10.4 Způsob kontroly přístupu ke zdroji

Přístup ke zdroji má oprávněný a proškolený pracovník, který převezme klíč od místnosti, který je uložen na určeném místě (zde konkretizujte způsob kontroly přístupu ke zdroji, předávání klíčů, zaznamenávání vstupu apod.).

10.5 Způsob proškolování a výcviku personálu

Všichni pracovníci jsou odpovědni za dodržování opatření zabezpečení zdroje. S četností jednou za rok jsou seznamováni s požadavky na zabezpečení zdroje. Osoba odpovědná za zabezpečení zdroje provádí namátkovou kontrolu, zda personál dodržuje postupy pro zabezpečení zdroje. Z namátkových kontrol je pořízen záznam, který je uložen u této osoby. Nově zařazení pracovníci jsou proškoleni o bezpečnostních opatřeních a toto proškolení potvrzují svým podpisem.

10.6 Popis opatření při zvýšení hrozby zneužití zdrojů

Pravidelně ve stanoveném termínu je posuzována aktuálnost hrozby zneužití radionuklidového zdroje, a to i posouzením hrozby zneužití zdroje vnitřním pracovníkem. Pokud při tomto posuzování bude zjištěno, že se změnila úroveň rizika možného útoku či zneužití zdroje bude celý systém zabezpečení přehodnocen a přizpůsoben novým požadavkům zohledňujících tyto okolnosti. Transfuzní oddělení a také celá nemocnice budou reagovat na změnu bezpečnostní situace v ČR a zjevně zvýšenou hrozbu zneužití zdroje. Opatření bude konzultováno s ředitelstvím nemocnice, SÚJB a případně s Policií ČR.

Přílohy:

l. Organizační řád nemocnice – jmenný seznam oprávněných pracovníků

2. Plánek areálu nemocnice

3. Plánek nadzemního podlaží TO

4. Kontakty - odpovědné osoby

…… …….

osoba odpovědná za zabezpečení radionuklidového zdroje

vedoucí Transfuzního oddělení

…….

statutární zástupce
(ředitel nemocnice)