SERIJA "NUKLEARNA BEZBJEDNOST", br. 11, IAEA

BEZBJEDNOST RADIOAKTIVNIH IZVORA

VODIČ ZA IMPLEMENTACIJU

MEĐUNARODNA AGENCIJA ZA ATOMSKU ENERGIJU
BEČ, 2009.

SADRŽAJ

1. UVOD 3
1.1 POZADINA 3
1.2. CILJ 3
1.3. DJELOKRUG 3
2. ODGOVORNOSTI DRŽAVE I OPERATORA 4
2.1. UVOD 4
2.2. DRŽAVA 4
2.3. OPERATORI 5
3. BEZBJEDNOSNI KONCEPTI 5
3.1. UVOD 5
3.2. KULTURA BEZBJEDNOSTI 6
3.3. SVRHA SISTEMA BEZBJEDNOSTI 7
3.4. BEZBJEDNOSNE FUNKCIJE 7
3.5. KREIRANJE I EVALUACIJA SISTEMA BEZBJEDNOSTI 8
3.6. INTEGRACIJA MJERA SIGURNOSTI I BEZBJEDNOSTI 8
3.7. GRADIRANI PRISTUP BEZBJEDNOSTI 9
3.8. RAZUMIJEVANJE I PRISTUP OKRUŽENJU PRIJETNJE 9
3.8.1 Procjena prijetnje državi 9
3.8.2. Prijetnja kao osnova koncepta 10
3.8.3. Prijetnje od počinilaca iznutra 10
3.8.4. Pojačana prijetnja 11
3.9. PROCJENA UGROŽENOSTI 11
4. USPOSTAVLJANJE REGULATORNOG PROGRAMA ZA BEZBJEDNOST RADIOAKTIVNIH IZVORA 11
4.1. KORAK 1: UTVRDITI GRADIRANE BEZBJEDNOSNE NIVOE SA ODGOVARAJUĆIM CILJEVIMA I ZADACIMA 12
4.2. KORAK 2: UTVRDITI BEZBJEDNOSNI NIVO KOJI SE PRIMJENJUJE NA DATI IZVOR 13
4.2.1 Kategorizacija radioaktivnih izvora 14
4.2.2. Dodjeljivanje bezbjednosnih nivoa 17
4.2.3. Dodatni obziri za dodjeljivanje bezbjednosnih nivoa 17
4.3 KORAK 3: ODABRATI I PRIMIJENITI REGULATORNI PRISTUP 19
4.3.1 Preskriptivni pristup 20
4.3.2. Pristup zasnovan na učinku 35
4.3.3. Kombinovani pristup 36
Aneks I 37
Aneks II 40
Aneks III 41
Aneks IV 42
REFERENCE 47
DEFINICIJE 49

1. UVOD

1.1 POZADINA

Ova publikacija nudi smjernice za primjenu bezbjednosnih mjera na radioaktivne izvore. Ona takođe daje savjet o primjeni odredbi koje se odnose na bezbjednost iz "Kodeksa ponašanja u oblasti sigurnosti i bezbjednosti radioaktivnih izvora" [1] (u daljem tekstu: Kodeks ponašanja) (za objašnjenje termina u ovoj publikaciji vidi *Definicije*).

Ovaj vodič za implementaciju, iako zamjenjuje "Bezbjednost radioaktivnih izvora — Privremeni vodič za komentare" (IAEA-TECDOC-1355) [2], uzima u obzir ukupni pristup bezbjednosti utvrđen u toj publikaciji i koji su neke države možda koristile kao referencu u koncipiranju svojih sadašnjih režima bezbjednosti. Ova publikacija je usklađena sa "Kategorizacijom radioaktivnih izvora" [3] IAEA-e i predlaže gradirani pristup bezbjednosti korištenjem skupa nivoa bezbjednosti i bezbjednosnih funkcija odvraćanja, detekcije, zadržavanja, odgovora i upravljanja bezbjednošću.

Ovu publikaciju treba čitati u vezi sa "Kodeksom ponašanja" [1], "Kategorizacijom radioaktivnih izvora" [3], "Sigurnošću uređaja koji proizvode zračenje i zatvorenih radioaktivnih izvora" [4], "Međunarodnim osnovnim sigurnosnim standardima za zaštitu od jonizirajućeg zračenja i za sigurnost izvora zračenja" [5] i "Osnovnim sigurnosnim principima" [6] IAEA-e.

Na kraju, u ovom vodiču se uvažava da treba postojati ravnoteža između bezbjednog upravljanja izvora i istovremenog omogućavanja da ih autorizovani zaposleni sigurno koriste. Pošto su radioaktivni izvori sastavno i ključno sredstvo u svijetu u djelatnostima zdravstva, proizvodnje, istraživanja i kontrole kvaliteta, treba posvetiti pažnju u cilju osiguranja da mnoge korisne upotrebe izvora ne budu pretjerano ometane. Izazov za regulatorno tijelo, korisnike i druge zainteresovane strane jeste da nađu ispravnu tačku ravnoteže.

1.2. CILJ

Ova publikacija je namijenjena državama za korištenje u formulisanju politike bezbjednosti radioaktivnih izvora i regulatornim tijelima u izradi regulatornih zahtjeva koji su u skladu sa "Kodeksom ponašanja". Ona će takođe pomoći državama potpisnicama da ispune određene obaveze u skladu sa "Međunarodnom konvencijom o sprečavanju akata nuklearnog terorizma" [7]. Ona takođe može biti korisna za operatore koji upravljaju radioaktivnim izvorima u izradi njihovih programa bezbjednosti.

1.3. DJELOKRUG

Ova publikacija uključuje smjernice i preporučene mjere za prevenciju, detekciju i odgovor na protivpravne akte koji uključuju radioaktivne izvore. Ona će takođe pomoći u cilju sprečavanja gubitka kontrole nad tim izvorima. Ona se ne odnosi na nuklearni materijal definisan u "Konvenciji o fizičkoj zaštiti nuklearnog materijala" i Amandmanu na Konvenciju [8] osim na izvore koji sadrže plutonijum-239.

Iako ovaj vodič ne obrađuje konkretno bezbjednost otvorenog radioaktivnog materijala, država se može opredijeliti za primjenu koncepata i mjera bezbjednosti navedenih u glavnim crtama u ovom vodiču za takav materijal.

Ova publikacija preporučuje da se mjere bezbjednosti primijene na radioaktivne izvore u proizvodnji, upotrebi ili privremenom skladištenju (vidi *Definicije*).

Ovaj vodič preporučuje da mjere bezbjednosti budu primijenjene na gradiranoj osnovi, uzimajući u obzir trenutnu procjenu prijetnje, relativnu privlačnost izvora i potencijalne posljedice koje su rezultat protivpravne upotrebe. Zahtijevani nivo bezbjednosti se postiže kroz kombinaciju odvraćanja, detekcije, zadržavanja, odgovora i upravljanja bezbjednošću.

Države mogu odlučiti da rizik za sve li neke izvore bude manji ili veći u odnosu na osnovu na kojoj je napisan ovaj vodič. U tim slučajevima će državama trebati

fleksibilnost u variranju mjera bezbjednosti koje zahtijevaju u poređenju sa onima koje se preporučuju ovdje. Pri tome, države će trebati ostati unutar ukupne strukture ovog vodiča što je više moguće.

Ovaj vodič ne uključuje preporuke o pripremljenosti i odgovoru na vanredne situacije, intervencijama ili saniranju kontaminiranih područja. Takve smjernice su dostupne u drugim publikacijama IAEA-e [5, 9, 10]. Smjernice o zaštiti ljudi od zračenja kao posljedice napada je dala Međunarodna komisija za radiološku zaštitu [11].

Konačno, ova publikacija se ne bavi radioaktivnim materijalom, uključujući i radioaktivne izvore, u transportu. Takve smjernice, uključujući i one za pošiljaoce treće strane, date su u referenci [12].

2. ODGOVORNOSTI DRŽAVE I OPERATORA

2.1. UVOD

"Kodeks ponašanja" [1] uvažava da efikasan sistem regulatorne kontrole ojačava sigurnost i bezbjednost radioaktivnih izvora u državi. U ovom dijelu se daju dalje smjernice o odgovornostima države i operatora u pogledu bezbjednosti radioaktivnih izvora.

2.2. DRŽAVA

Svaka država će trebati definisati svoju unutrašnju prijetnju (vidi Dio 3.8.1). Ovaj proces treba započeti sa procjenom prijetnje državi, koja je analiza koja na državnom nivou dokumentuje vjerodostojne motivacije, namjere i mogućnosti potencijalnih počinilaca koji bi mogli uzrokovati štetu putem sabotaže objekta ili neautorizovanog premještanja radioaktivnog izvora u protivpravne svrhe. Smjernice na ovu temu su detaljno obrađene u referenci [13].

Svaka država će trebati poduzeti odgovarajuće mjere kako bi osigurala da radioaktivni izvori unutar njene teritorije ili pod njenom nadležnošću ili kontrolom budu bezbjedno zaštićeni tokom i na kraju njihovog vijeka trajanja. Ovo obuhvata promovisanje kulture bezbjednosti u vezi sa radioaktivnim izvorima i adekvatnu edukaciju i obuku regulatora i operatora.

Države će trebati imati pripremljenu efikasnu državnu zakonodavnu i regulatornu infrastrukturu u cilju regulisanja bezbjednosti radioaktivnih izvora, kojom se:

- propisuju i dodjeljuju nadležnosti vlasti relevantnim tijelima, uključujući i nezavisno regulatorno tijelo u cilju uspostavljanja, provođenja i održavanja režima kojimse osigurava bezbjednost radioaktivnih izvora;
- utvrđuju bezbjednosni zahtjevi za radioaktivne izvore i uključuje i sistem za evaluaciju, licenciranje i izvršenje ili druge procedure za davanje autorizacije;
- primarna odgovornost za bezbjednost radioaktivnih izvora određuje operatorima;
- propisuju mjere za smanjenje vjerovatnoće pokušaja protivpravnih djela;
- propisuju mjere za ublažavanje/smanjenje na minimum posljedica protivpravnih akata koja uključuju radioaktivne izvore;
- utvrđuju kažnjive nezakonite radnje koje obuhvataju i protivpravne akti koji uključuju radioaktivne izvore.

Provođenje i funkcionisanje zakonodavne i regulatorne infrastrukture za bezbjednost radioaktivnih izvora oslanja se na efikasnu saradnju između različitih tijela kojima su dodijeljene nadležnosti vlasti. Obično ta tijela vjerovatno obuhvataju državno regulatorno tijelo, obavještajne službe, ministarstva unutrašnjih poslova, odbrane, saobraćaja i spoljnih poslova; agencije za provođenje zakona, carinsku službu, obalsku stražu i druge agencije koje imaju nadležnosti vezane za bezbjednost.

Države će trebati osigurati da regulatorno tijelo ima adekvatne resurse u smislu zaposlenih i finansiranja da bi ispunjavalo svoje regulatorne funkcije, uključujući i provođenje programa inspekcije u cilju verifikacije da se bezbjednost radioaktivnih izvora efikasno održava. Ovaj program inspekcije trebaju pratiti pisane procedure, a provoditi ga kvalifikovano osoblje. Kod učestalosti inspekcija treba uzeti u obzir bezbjednosni nivo (vidi Dio 4.1) za radioaktivne izvore i može se razmotriti i raniji rad operatora u održavanju poštovanja bezbjednosnih zahtjeva. Inspekcije mjera bezbjednosti koje primjenjuje operator mogu se provoditi zajedno sa inspekcijama čiji je cilj verifikacija poštovanja drugih regulatornih zahtjeva, poput sigurnosti, ili kao samostalne inspekcije.

2.3. OPERATORI

Operatori, kao autorizovani subjekti, trebaju imati primarnu odgovornost za provođenje i održavanje mjera bezbjednosti radioaktivnih izvora u skladu sa državnim zahtjevima. Zavisno od regulatornih zahtjeva države, operatori mogu imenovati ili sklopiti ugovor sa trećom stranom da provodi poslove i zadatke vezane za bezbjednost radioaktivnih izvora, iako bi autorizovani operator trebao zadržati primarnu odgovornost za poštovanje regulatornih zahtjeva i efikasnost poslova i zadataka. Takođe, operatori trebaju osigurati da su njihovi zaposleni i njihovi ugovarači odgovarajuće obučeni i da zadovoljavaju regulatorne zahtjeve, što bi trebalo uključivati povjerljivost.

Operatori trebaju u propisanim intervalima verifikovati da su izvori prisutni na njihovim autorizovanim lokacijama. Svako odsustvo izvora ili neslaganje treba biti odmah istraženo i prijavljeno regulatornom tijelu. Trebaju postojati pripremljeni procesi kojima se osigurava da svi izvori kategorija 1, 2 i 3 (vidi Dio 4.2.1) za koje su operatori autorizovani mogu identifikovati i biti sljedivi.

Ako to regulatorni organi vlasti traže, operatori trebaju provoditi procjenu ugroženosti (vidi *Definicije*) svojih radioaktivnih izvora na osnovu trenutno procijenjene prijetnje.

Operatori trebaju promovisati kulturu bezbjednosti (vidi Dio 3.2) i uspostaviti sistem upravljanja proporcionalan bezbjednosnim nivoima (vidi Dio 4.1), kako bi osigurali da:

- politike i procedure kojima se bezbjednost utvrđuje kao visoki prioritet budu utvrđene;
- problemi koji utiču na bezbjednost budu odmah utvrđeni i riješeni na način proporcionalan njihovoj važnosti;
- odgovornosti svakog pojedinca za bezbjednost budu jasno utvrđene i da je svaki pojedinac odgovarajuće obučen, kvalifikovan i utvrđen kao povjerljiv;
- jasne granice nadležnosti za donošenje odluka o bezbjednosti budu definisane;
- su organizacioni aranžmani i pravci komunikacije utvrđeni tako da rezultiraju odgovarajućim protokom informacija o bezbjednosti unutar cijele organizacije;
- povjerljive informacije budu utvrđene i zaštićene u skladu sa državnim propisima;
- se radioaktivnim izvorima upravlja u skladu sa bezbjednosnim planom (vidi *Definicije*), ako to propisuje regulatorno tijelo.

3. BEZBJEDNOSNI KONCEPTI

3.1. UVOD

U ovom dijelu se predstavljaju osnovni principi koji se odnose na bezbjednost radioaktivnih izvora i utvrđeni u "Kodeksu ponašanja" [1], a zatim se razrađuju koncepti bezbjednosti, uključujući i osnovne bezbjednosne funkcije odvraćanja, detekcije, zadržavanja, odgovora i upravljanja bezbjednošću (tabela 1).

3.2. KULTURA BEZBJEDNOSTI

Dinamična i efikasna kultura bezbjednosti treba postojati na svim nivoima kod zaposlenih i rukovodstva operatora.

TABELA 1. PRINCIPI IZ "KODEKSA PONAŠANJA" ZA BEZBJEDNOST RADIOAKTIVNIH IZVORA

"Kodeks ponašanja" utvrđuje osnovne principe koji se odnose na bezbjednost radioaktivnih izvora, od kojih je nekoliko relevantno za ovu publikaciju. Prema ovim principima, svaka država mora:

- poduzeti odgovarajuće neophodne mjere u cilju osiguranja da su radioaktivni izvori **"bezbjedno zaštićeni tokom njihovog vijeka trajanja i na kraju njihovog vijeka trajanja"** (tačka 7);
- naglasiti "projektantima, proizvođačima (i proizvođačima radioaktivnih izvora i proizvođačima uređaja koji sadrže radioaktivne izvore), dobavljačima, korisnicima i onima koji upravljaju izvorima van upotrebe **njihove odgovornosti za sigurnost i bezbjednost radioaktivnih izvora**" (tačka 15);
- definisati "svoju **unutrašnju prijetnju** i **procijeniti svoju ugroženost** u pogledu te prijetnje za mnoštvo izvora koji se koriste na njenoj teritoriji, na osnovu potencijala za gubitak kontrole i protivpravne akte koji uključuju jedan ili više radioaktivnih izvora" (tačka 16);
- imati pripremljene zakone i propise za "zahtjeve za **mjere bezbjednosti u cilju odvraćanja, detekcije i zadržavanja** neautorizovanog pristupa ili krađe, gubitka, neautorizovane upotrebe ili premještanja radioaktivnih izvora tokom svih faza upravljanja" (tačka 19);
- osigurati da "regulatorno tijelo osnovano zakonodavstvom države ima ovlaštenje da postavi jasne i nedvosmislene uslove u autorizacijama koje izdaje, uključujući i uslove koji se odnose na …(viii) mjere za utvrđivanje, na odgovarajući način, **povjerljivosti** osoba uključenih u upravljanje radioaktivnim izvorima; i (ix) **povjerljivost informacija** koje se odnose na bezbjednost izvora" (tačka 20);
- osigurati da njeno regulatorno tijelo ima ovlaštenje **da zahtijeva bezbjednosni plan ili procjenu, zavisno šta odgovara, i da promoviše uspostavljanje kulture bezbjednosti** među svim pojedincima i u svim tijelima uključenim u upravljanje radioaktivnim izvorima (tačke 20 i 22).

Karakteristike kulture bezbjednosti su vjerovanja, stavovi, ponašanje i sistemi upravljanja, čiji pravilan skup vodi efikasnijoj bezbjednosti.

Temelj kulture bezbjednosti je priznanje – od strane onih koji imaju ulogu u regulisanju, upravljanju ili vođenju objekata i aktivnosti koji uključuju radioaktivne izvore, ili čak onih na koje bi te aktivnosti mogle uticati – da postoji vjerodostojna prijetnja i da je bezbjednost bitna.

Čitaoci ovog vodiča takođe trebaju pročitati "Kulturu nuklearne bezbjednosti" [14], u kojoj se opisuju osnovni koncepti i elementi kulture bezbjednosti.

Kultura bezbjednosti može biti ojačana raznovrsnim sredstvima, uključujući po potrebi:

- dodjelu odgovornosti za bezbjednost radioaktivnih izvora višem rukovodiocu, ali pritom osiguravajući da su zaposleni svjesni da je bezbjednost zajednička odgovornost širom cijele organizacije;
- dokumentovanje pravnih i regulatornih odgovornosti za bezbjednost koje se odnose na operatora i skretanje pažnje na ovo relevantnim rukovodiocima, zaposlenima i, po potrebi, svim povremeno zaposlenima i ugovaračima;
- osiguranje da postoji svijest o prijetnji i obuku rukovodiocima za bezbjednost, timovima za odgovor i svim zaposlenim koji imaju sekundarne odgovornosti za

bezbjednost;
- razmatranje pitanja bezbjednosti kod orijentacionih kurseva za zaposlene i ugovarače;
- davanje bezbjednosnih uputstava i održavanje tekućih brifinga zaposlenih i ugovarača te izvođenje obuke i evaluacije o stečenim iskustvima;
- provođenje redovnog funkcionalnog testiranja i preventivnog održavanja.

3.3. SVRHA SISTEMA BEZBJEDNOSTI

Sistem bezbjednosti trebaju osmisliti profesionalci za bezbjednost zaposleni kod operatora u cilju odvraćanja potencijalnih počinilaca od izvršenja protivpravnog akta ili smanjenja na minimum vjerovatnoće, kroz detekciju, zadržavanje i odgovor, da potencijalni počinilac okonča protivpravni akt. Takav akt bi se sastojao od niza radnji učinjenih od strane jednog ili više potencijalnih počinilaca (prijetnja) u cilju sticanja pristupa izvoru (meta) bilo u namjeri da počine sabotažu ili drugi protivpravni akt, ili da premjeste izvor bez autorizacije.

3.4. BEZBJEDNOSNE FUNKCIJE

Sistem bezbjednosti u cilju zaštite radioaktivnih izvora od namjere potencijalnog počinioca da izvrši protivpravno djelo treba biti koncipiran tako da obavlja osnovne bezbjednosne funkcije: odvraćanje, detekciju, zadržavanje, odgovor i upravljanje bezbjednošću:

- ***Odvraćanje*** se dešava kada potencijalni počinilac, inače motivisan da počini protivpravni akt, bude odvraćen od poduzimanja takvog pokušaja. Mjere odvraćanja imaju učinak ubjeđivanja potencijalnog počinioca da bi bilo previše teško izvesti protivpravni akt, da bi uspjeh bio previše nesiguran ili da bi posljedice takvog djela bile previše neprijatne za potencijalnog počinioca da bi se opravdao poduhvat. Mjere konkretno sačinjene u cilju odvraćanja tako obuhvataju saopštavanje potencijalnim počiniocima da postoje mjere kojima se vrše druge bezbjednosne funkcije. Ako takvo saopštavanje ima željeni učinak, odvraćanje je rezultat.
- ***Detekcija*** je otkriće pokušaja ili stvarnog upada čiji bi cilj mogao biti neautorizovano premještanje ili sabotaža radioaktivnog izvora. Detekcija se može ostvariti pomoću nekoliko sredstava, uključujući vizuelno posmatranje, video nadzor, elektronske senzore, evidenciju obračuna izvora, pečate i druga sredstva koja otkrivaju neautorizovane pokušaje korištenja, sisteme monitoringa procesa i druga sredstva. Svjesnost potencijalnog počinioca o mjerama detekcije takođe može poslužiti kao sredstvo odvraćanja.
- ***Zadržavanje*** otežava pokušaj potencijalnog počinioca da stekne neautorizovan pristup ili da premjesti ili sabotira radioaktivni izvor, generalno putem barijera ili drugih fizičkih sredstava. Jedna od mjera zadržavanja je faktor vremena nakon detekcije koje je potrebno potencijalnom počiniocu da premjesti ili sabotira radioaktivni izvor. Svjesnost potencijalnog počinioca o mjerama zadržavanja takođe može poslužiti kao sredstvo odvraćanja.
- ***Odgovor*** obuhvata radnje poduzete nakon detekcije da se spriječi uspjeh potencijalnog počinioca ili da se ublaže potencijalno teške posljedice. Te radnje, koje obično obavljaju zaštitari ili policija, odnosno druge državne agencije, uključuju prekidanje radnje potencijalnog počinioca i njegovo savladavanje dok je pokušaj neautorizovanog premještanja ili sabotaže u toku, sprečavanje potencijalnog počinioca da upotrijebi radioaktivni izvor u cilju prouzrokovanja štetnih posljedica, povrat radioaktivnog izvora ili ublažavanje težine posljedica na drugi način. Izgledi za uspješan odgovor takođe mogu poslužiti kao sredstvo odvraćanja.

- ***Upravljanje bezbjednošću*** uključuje osiguranje adekvatnih resursa (ljudskih i finansijskih) za bezbjednost izvora. Ono takođe uključuje izradu procedura, politika, evidencija i planova za bezbjednost izvora i generalno u cilju efikasnije kulture bezbjednosti. Ovaj termin takođe obuhvata i izradu procedura za propisno rukovanje povjerljivim informacijama i njihovu zaštitu od neovlaštenog otkrivanja.

3.5. KREIRANJE I EVALUACIJA SISTEMA BEZBJEDNOSTI

Dobro kreiran sistem bezbjednosti treba integrisati mjere u cilju obavljanja svih pet bezbjednosnih funkcija tako da efikasno obezbijedi metu od prijetnje u skladu sa sljedećim konceptima bezbjednosti:

Odvraćanje se ne može mjeriti: Zadatak odvraćanja je da se potencijalni počinilac odgovori od pokušaja protivpravnog akta. Kao rezultat, uticaj mjera odvraćanja se ne može kvantifikovati. Zbog toga koncept sistema bezbjednosti ne treba u potpunosti biti zasnovan na odvraćanju.

Detekcija prije zadržavanja: Funkcija zadržavanja je da se osoblju zaduženom za odgovor omogući dovoljno vremena da se rasporedi i poremeti ili prekine nastojanja potencijalnog počinioca da dovrši protivpravni akt. Zbog toga detekcija mora prethoditi zadržavanju. Ako se potencijalnom počiniocu da prilika da nadvlada barijere i druge prepreke prije nailaska na senzore koji detektuju upad ili na druga sredstva detekcije, potencijalni počinilac će obaviti najteže zadatke prije nego što bude detektovan i odatle sa određenom vjerovatnoćom može uspjeti u premještanju ili sabotiranju radioaktivnog izvora prije nego što stigne osoblje zaduženo na odgovor. U tom slučaju, barijere nisu u funkciji zadržavanja nego su, u najboljem slučaju, sredstvo odvraćanja.

Detekcija zahtijeva procjenu: Većina sredstava detekcije daju indirektnu indikaciju o potencijalnom protivpravnom aktu, kao što je pokušaj neautorizovanog pristupa, premještaj ili sabotaža radioaktivnog izvora. Jedina direktna indikacija je putem direktnog posmatranja od strane ljudi. Zbog toga, kad se alarm ili drugi indirektni indikator oglasi, uvijek postoji određena nesigurnost oko razloga za to. Kao rezultat, detekcija uvijek treba biti dopunjena procjenom da se utvrdi razlog alarma. Procjena alarma zahtijeva ljudsko zapažanje i prosuđivanje kroz raspoređivanje osoblja zaduženog za odgovor da ispita razlog alarma, kroz sisteme televizije zatvorenog kruga (CCTV) ili slična sredstva. Ponekad potencijalni počinioci mogu pokušati da iskoriste bilo kakvo zadržavanje između detekcije i procjene da bi prikrili svoje protivpravne namjere. Zbog toga je trenutna procjena cilj svakog sistema bezbjednosti.

Zadržavanje duže od procjene plus vrijeme za odgovor: Sistem bezbjednosti je uspješan ako detektuje, a ispravna procjena da potencijalni počinilac pokušava protivpravni akt se obavi u vremenom dovoljnom za naknadne mjere zadržavanja koje omogućavaju osoblju zaduženom za odgovor da prekine i zaustavi potencijalnog počinioca prije dovršavanja protivpravnog akta ili da se odmah poduzmu radnje u cilju ublažavanja potencijalno teških posljedica. Ovaj odnos funkcija detekcije, zadržavanja i odgovora je poznat kao *blagovremena detekcija.*

Uravnotežena zaštita: Ovo je koncept ekvivalentnih bezbjednosnih funkcija (odvraćanje, detekcija, zadržavanje, odgovor i upravljanje bezbjednošću) kojim se omogućava adekvatna zaštita protiv svih prijetnji na svim mogućim pravcima. Drugim riječima, vremena zadržavanja na svakom pravcu, mjere detekcije koje prate svaki element detekcije i rezultirajući odgovori omogućavaju zaštitu neophodnu da se spriječi uspješan protivpravni akt.

Odbrana po dubini: Koncept nekoliko slojeva i metoda zaštite (strukturalna, tehnička, ljudska i organizaciona) koje potencijalni počinilac mora nadvladati ili zaobići da bi ostvario svoj cilj.

3.6. INTEGRACIJA MJERA SIGURNOSTI I BEZBJEDNOSTI

Mjere sigurnosti i mjere bezbjednosti imaju zajednički cilj zaštite ljudskih života i zdravlja te okoliša. Mjere sigurnosti i mjere bezbjednosti trebaju biti osmišljene i

implementirane na integrisan način tako da mjere bezbjednosti ne ugrožavaju sigurnost niti da mjere sigurnosti ne ugrožavaju bezbjednost. U implementaciji preporuka iz ovog vodiča, kreatori sistema bezbjednosti se trebaju konsultovati sa kvalifikovanim ekspertima za sigurnost kako bi osigurali da mjere bezbjednosti ne ugrožavaju sigurnost pojedinaca niti zaštitu okoliša.

3.7. GRADIRANI PRISTUP BEZBJEDNOSTI

Zahtjevi za bezbjednost trebaju biti zasnovani na gradiranom pristupu, uzimajući u obzir trenutnu evaluaciju prijetnje, relativnu privlačnost radioaktivnog izvora, njegovu prirodu i potencijalne posljedice povezane sa njegovim neautorizovanim premještanjem ili sabotažom. Ovaj gradirani pristup osigurava da najveće posljedice od izvora dobiju najveći stepen bezbjednosti.

3.8. RAZUMIJEVANJE I PRISTUP OKRUŽENJU PRIJETNJE

Kreiranje i evaluacija sistema bezbjednosti trebaju uzeti u obzir trenutnu procjenu prijetnje državi i mogu uključivati i izradu i primjenu dokumenta o prijetnji kao osnovi koncepta (eng. design basis threat; DBT) (vidi *Definicije*).

3.8.1 Procjena prijetnje državi

Kodeks ponašanja navodi:

"Svaka država treba definisati svoju unutrašnju prijetnju i procijeniti svoju ugroženost u pogledu te prijetnje za mnoštvo izvora koji se koriste unutar njene teritorije, na osnovu potencijala za gubitak kontrole i protivpravne akte koji uključuju jedan ili više radioaktivnih izvora."

Procedura za zadovoljavanje ovog principa treba započeti procjenom prijetnje državi, što je analiza koja na državnom nivou dokumentuje vjerodostojne motivacije, namjere i mogućnosti potencijalnih počinilaca koje bi mogle prouzrokovati štetu putem sabotaže objekta ili neautorizovanog premještanja radioaktivnog izvora u protivpravne svrhe. Takvu procjenu obično obavljaju bezbjednosne službe države, često uz ulazne informacije od institucija poput ministarstava unutrašnjih poslova, odbrane, saobraćaja i vanjskih poslova; agencija za provođenje zakona, carinske služba i obalske straže i drugih tijela koja imaju odgovornosti u vezi sa bezbjednošću, a mogu uključivati i regulatorno tijelo. Ako prethodno nije bilo uključeno u ovu procjenu, regulatorno tijelo treba biti obaviješteno o prijetnji koju relevantne državne institucije trenutno procjenjuju u cilju izrade svog regulatornog programa za bezbjednost radioaktivnih izvora.

Proces procjene je deduktivno zaključivanje. Počevši od onoga što se zna, pravi se procjena o tome kako grupe potencijalnih počinilaca ili pojedinci mogu da se ponašaju u budućnosti. Ovo bi obuhvatalo, naprimjer, ranije događaje i poznate mogućnosti da se napadnu razni tipovi objekata u kojima se radioaktivni izvori skladište ili koriste. Procjena prijetnje treba obuhvatiti najmanje sljedeća svojstva i karakteristike svakog utvrđenog potencijalnog počinioca i izvana i iznutra (insajder):

- Motivacija. Politička, finansijska, ideološka, lična.
- Nivo posvećenosti. Zanemarivanje ličnog zdravlja, sigurnosti, dobrostanja ili preživljavanja.
- Namjere. Sabotaža materijala ili objekta (neautorizovano premještanje), panika javnosti i poremećaji, politička nestabilnost, masovne povrede i žrtve.
- Veličina grupe. Snaga napada, koordinacija, podrška.
- Oružje. Vrsta, broj, dostupnost, improvizovana.
- Sredstva. Mehanička, toplotna, manuelna, strujna, elektronska, elektromagnetna, komunikacijska oprema.
- Načini transporta. Javni, privatni, kopnom, morem, vazduhom, vrsta, broj,

dostupnost.
- Tehničko znanje. Inženjerstvo, upotreba eksploziva i hemikalija, paravojno iskustvo, vještine komunikacije.
- Znanje kompjutera. Korištenje kompjutera i sistema za automatsku kontrolu kao direktne podrške fizičkim napadima u cilju prikupljanja obavještajnih informacija, napada pomoću kompjutera, prikupljanja novca itd.
- Znanje Mete, planovi lokacija i procedure, mjere bezbjednosti, procedure sigurnosti i zaštite od zračenja, operacije, potencijalna upotreba nuklearnog ili drugog radioaktivnog materijala.
- Finansiranje. Izvor, iznos, raspoloživost.
- Pitanje potencijalnih počinilaca iznutra. Dosluh, pasivni/aktivni, nasilni/nenasilni, broj potencijalnih počinilaca iznutra.
- Struktura podrške. Lokalni simpatizeri, organizacija podrške, logistika.
- Taktika. Prikrivena i otvorena.

Kad jednom država napravi procjenu prijetnje uperene protiv sebe, trebaće odlučiti o osnovi za utvrđivanje propisa o bezbjednosti radioaktivnih izvora. Jedan pristup je da se propisi utvrde na osnovu procjene prijetnje državi, a drugi da se napravi regulativa na osnovu dokumenta o prijetnji kao osnovi koncepta (vidi dalje u tekstu), za koji ulazne informacije dolaze iz procjene prijetnje državi. Pri odabiru regulatorne osnove postoji nekoliko faktora koje država treba razmotriti, uključujući i težinu posljedica povezanih sa protivpravnim aktima koji uključuju radioaktivne izvore u državi, utvrđivanje svoje sposobnosti da uspostavi efikasne sisteme zaštite korištenjem svakog pristupa i mogućnost regulatornog tijela da implementira različite pristupe.

Vrijedi napomenuti da ne trebaju sve države koristiti pristup prijetnje kao osnove koncepta za svoj regulatorni sistem. Međutim, ako se ne odabere taj pristup, države će i dalje trebati pripremiti procjenu prijetnje državi i održavati je aktuelnom.

3.8.2. Prijetnja kao osnova koncepta

Dokument o prijetnji kao osnovi koncepta, definisan na državnom nivou, jeste sredstvo korišteno da se utvrde zahtjevi funkcionisanja u projektu sistema fizičke zaštite za specifične vrste objekata. On se takođe koristi da pomogne operatorima i organima vlasti da procijene efikasnost tih sistema za borbu protiv potencijalnih počinilaca putem evaluacije funkcionisanja sistema u odnosu na mogućnosti potencijalnog počinioca navedene u konceptu i putem obavljanja procjena ugroženosti. Dokument o prijetnji kao osnovi koncepta je sveobuhvatan opis motivacija, namjera i mogućnosti potencijalnih počinilaca na osnovu čega se sistemi zaštite projektuju i evaluiraju. Mogućnosti potencijalnih počinilaca, bilo da su iznutra ili spolja, pomažu da se utvrde zahtjevi za detekciju, zadržavanje i odgovor da bi sistem fizičke zaštite bio efikasan u odnosu na dokument o prijetnji kao osnovi koncepta.

Izrada ovog koncepta će biti specifična za svaku državu zbog socijalnih, kulturnih i geopolitičkih razlika. Kao i kod procjene prijetnje državi, izrada ovog koncepta obično zahtijeva kombinovane napore domaćih vlasti, poput obavještajnih i bezbjednosnih agencija, agencija za provođenje zakona, regulatornih tijela i operatora. Možda će biti potrebno da se koncept s vremena na vrijeme razmotri u svjetlu novih informacija iz državnih organizacija. Detaljnije informacije o procesu izrade ovog koncepta se mogu naći u referenci [13].

3.8.3. Prijetnje od počinilaca iznutra

Prijetnjama od počinilaca iznutra (insajdera) se treba posvetiti posebna pažnja pri kreiranju sistema bezbjednosti. Te prijetnje mogu doći od jedne ili više osoba koje imaju legitiman pristup objektu i detaljno znanje o aktivnostima ili lokacijama izvora. Ti pojedinci mogu biti zaposleni ili ugovarači koji bi mogli premjestiti izvor ili iznijeti informacije, sa protivpravnom namjerom, ili izvršiti akte sabotaže prostorija. Štaviše, pojedinci mogu tražiti zaposlenje u objektu sa namjerom izvršenja protivpravnih akata i

takođe mogu pomoći spoljnim potencijalnim počiniocima da premjeste izvor ili izvrše neprijateljski akt. Prijetnje potencijalnih počinilaca iznutra i preporučene odgovarajuće protivmjere se dalje objašnjavaju u referenci [15].

3.8.4. Pojačana prijetnja

Sistem bezbjednosti treba biti efikasan u suzbijanju trenutno procijenjene prijetnje. Međutim, trebaju postojati odredbe kojima se osigurava da se nivo bezbjednosti može privremeno podići tokom perioda povećane prijetnje. Ovo treba obuhvatati uvođenje dodatnih mjera bezbjednosti ili smanjenje pristupa radioaktivnim izvorima.

3.9. PROCJENA UGROŽENOSTI

Procjena ugroženosti (eng. vulnerability assessment; VA), takođe poznata kao ispitivanje sistema ili procjena bezbjednosti, jeste metod evaluacije zaštitnih sistema bezbjednosti. To je sistematska procjena efikasnosti sistema bezbjednosti u cilju zaštite od procijenjene prijetnje (ili prema dokumentu o prijetnji kao osnovi koncepta ako ga ima). Procjena ugroženosti po prirodi može biti specifična ili generalna, može je lokalno obaviti operator ili država/regulatorno tijelo, i može se koristiti kao pomoć državi/regulatornom tijelu u izradi propisa ili u cilju dokazivanja da operator poštuje regulatorne propise. Dodatne informacije o tome kako obaviti procjenu ugroženosti se mogu naći u Aneksu III.

4. USPOSTAVLJANJE REGULATORNOG PROGRAMA ZA BEZBJEDNOST RADIOAKTIVNIH IZVORA

Odredbe u "Kodeksu ponašanja" koje se odnose na bezbjednost radioaktivnih izvora su ojačane da bi se omogućile mjere za smanjenje vjerovatnoće protivpravnih akata. Kodeks takođe konkretno navodi da države trebaju posvetiti odgovarajuću pažnju onim radioaktivnim izvorima za koje smatraju da imaju potencijal prouzrokovanja neprihvatljivih posljedice ako se upotrijebe u protivpravne svrhe. U slučaju takvog događaja, zahtjevi i smjernice za pripremljenost i odgovor na vanredne situacije, intervencije i saniranje kontaminiranih oblasti su na raspolaganju od strane IAEA [5, 9, 10]. Smjernice za zaštitu ljudi od zračenja kao posljedice radiološkog napada je dala Međunarodna komisija za radiološku zaštitu [11].

Takvi protivpravni akti i potencijalne posljedice mogu uključivati:

- Namjerno postavljanje oštećenog ili nezaštićenog izvora na javnom mjestu;
- Namjernu disperziju radioaktivnog materijala u cilju prouzrokovanja štetnih zdravstvenih efekata (korištenjem naprimjer, oružja za radioaktivno raspršivanje);
- Korištenje oružja za radioaktivno raspršivanje u svrhe kontaminiranja tla, zgrada i infrastrukture, što bi vodilo zabrani pristupa u ta područja i može biti zasnovano na kriterijima zaštite od zračenja, ekonomskom uticaju i troškovima čišćenja i obnove.

Mnoge države već imaju pripremljen regulatorni program koji obuhvata aktivnosti poput autorizacije, razmatranja i procjene, inspekcije i izvršenja [16]. U ovom dijelu se daju smjernice regulatornim tijelima o tome kako da sačine ili ojačaju regulatorne programe da bi pristupili bezbjednosti radioaktivnih izvora s ciljem smanjenja vjerovatnoće protivpravnih akata koji uključuju te izvore. Mjere sigurnosti i bezbjednosti trebaju biti koncipirane i provedene na integrisan način tako da se međusobno ne ugrožavaju.

Uspostavljanje jednog takvog regulatornog programa za bezbjednost radioaktivnih izvora uključuje tri osnovna koraka za regulatorno tijelo:

- Korak 1: Utvrditi gradirane bezbjednosne nivoe sa odgovarajućim ciljevima i zadacima za svaki bezbjednosni nivo (vidi Dio 4.1).

- Korak 2: Utvrditi bezbjednosni nivo primjenjiv na dati izvor (vidi Dio 4.2).

- Korak 3: Odabrati i primijeniti regulatorni pristup (preskriptivni, zasnovan na učinku ili kombinovani) radi upućivanja operatora na način izrade koncepta, implementacije i evaluacije mjere bezbjednosti da bi ispunili bezbjednosne zadatke iz tabele 1 (vidi Dio 4.3).

4.1. KORAK 1: UTVRDITI GRADIRANE BEZBJEDNOSNE NIVOE SA ODGOVARAJUĆIM CILJEVIMA I ZADACIMA

Radioaktivni izvori imaju širok raspon karakteristika (poput aktivnosti) koje ih čine u raznim stepenima privlačnim za potencijalne počinioce. Odgovarajući raspon efikasnih mjera bezbjednosti treba biti iskorišten kako bi se osigurala adekvatna zaštita izvora korištenjem gradiranog pristupa. Da bi se osigurale adekvatne bezbjednosne mogućnosti bez nametanja pretjerano restriktivnih mjera, treba koristiti koncept bezbjednosnih nivoa. Tri bezbjednosna nivoa (A, B i C) su osmišljena da se omogući specifikacija funkcionisanja sistema bezbjednosti na gradirani način. Bezbjednosni nivo A zahtijeva najviši stepen bezbjednosti, dok su ostali nivoi progresivno niži.

Svaki bezbjednosni nivo ima odgovarajući cilj. Taj cilj definiše ukupni rezultat za koji bi sistem bezbjednosti trebao biti sposoban da ga omogući za dati bezbjednosni nivo. Sačinjeni su sljedeći ciljevi:

- Bezbjednosni nivo A: Spriječiti neautorizovano premještanje izvora.
- Bezbjednosni nivo B: Smanjiti vjerovatnoću neautorizovanog premještanja izvora na minimum.
- Bezbjednosni nivo C: Smanjiti vjerovatnoću neautorizovanog premještanja izvora.

Protivpravni akti mogu uključivati neautorizovano premještanje izvora ili sabotažu. Iako se bezbjednosni zadaci jedino bave neautorizovanim premještanjem, ostvarenje tih ciljeva će smanjiti i vjerovatnoću uspješnog čina sabotaže. Sistemi bezbjednosti koji ostvaruju gore navedene ciljeve će omogućiti određenu (iako ograničenu) sposobnost da se čin sabotaže detektuje i odgovori na njega.

Da bi se ciljevi ostvarili, potrebno je postići adekvatan nivo učinka za svaku od bezbjednosnih funkcija: odvraćanje, detekcija, zadržavanje, odgovor i upravljanje bezbjednošću. Taj nivo učinka se definiše kao skup zadataka za svaku od funkcija. Ti zadaci navode željeni učinak kombinacije mjera primijenjenih za dati zadatak. Odvraćanje je bezbjednosna funkcija koju je teško kvantifikovati. Kao rezultat, u ovoj publikaciji njoj nije pripisan prateći skup bezbjednosnih ciljeva i mjera.

Bezbjednosni nivoi i prateći bezbjednosni zadaci su rezimirani u tabeli 2.

Ako je zadatak naveden u tabeli 2 isti za dva ili više bezbjednosnih nivoa, namjera je da se taj zadatak ispuni na rigorozniji način za viši bezbjednosni nivo.

TABELA 2. BEZBJEDNOSNI NIVOI I BEZBJEDNOSNI ZADACI

Bezbjednosne funkcije	Bezbjednosni zadaci		
	Bezbjednosni nivo A	Bezbjednosni nivo B	Bezbjednosni nivo C
	Cilj: Spriječiti neautorizovano premještanje[a]	Cilj: Smanjiti vjerovatnoću neautorizovanog premještanja na minimum[a]	Cilj: Smanjiti vjerovatnoću neautorizovanog premještanja[a]
Detekcija	Omogućiti trenutnu detekciju bilo kakvog neautorizovanog pristupa obezbijeđenoj zoni/lokaciji izvora		

	Omogućiti trenutnu detekciju bilo kakvog neautorizovanog uklanjanja izvora, uključujući i od strane počinioca iznutra	Omogućiti detekciju bilo kakvog neautorizovanog uklanjanja izvora	Omogućiti detekciju neautorizovanog uklanjanja izvora
	Omogućiti trenutnu procjenu detekcije		
	Omogućiti trenutnu komunikaciju sa osobljem zaduženim za odgovor		
	Omogućiti sredstva da se detektuje gubitak izvora putem verifikacije		
Zadržavanje	Omogućiti zadržavanje nakon detekcije dovoljno da osoblje zaduženo za odgovor prekine neovlašteno uklanjanje	Omogućiti zadržavanje da se vjerovatnoća neautorizovanog premještanja smanji na minimum	Omogućiti zadržavanje da se smanji vjerovatnoća neautorizovanog premještanja
Odgovoriti	Omogućiti trenutan odgovor na procijenjeni alarm sa dovoljnim resursima da se prekine i spriječi neautorizovano premještanje	Omogućiti trenutno započinjanje odgovora da se prekine neautorizovano premještanje	Izvršiti odgovarajuće radnje u slučaju neautorizovanog premještanja izvora
Upravljanje bezbjednošću	Omogućiti kontrole pristupa lokaciji izvora kojima se efikasno ograničava pristup na samo autorizovana lica		
	Osigurati povjerljivost autorizovanih osoba		
	Utvrditi i zaštititi povjerljive informacije		
	Predvidjeti bezbjednosni plan		
	Osigurati mogućnost da se upravlja bezbjednosnim događajima koje obuhvata plan za bezbjednosne događaje (vidi *Definicije*)		
	Uspostaviti sistem izvještavanja o bezbjednosnim događajima		

[a] Ostvarenje ovih ciljeva će takođe smanjiti vjerovatnoću uspješnog čina sabotaže.

4.2. KORAK 2: UTVRDITI BEZBJEDNOSNI NIVO KOJI SE PRIMJENJUJE NA DATI IZVOR

Da bi se precizirao odgovarajući bezbjednosni nivo za neki izvor, u obzir treba uzeti potencijalnu štetu koju taj izvor može prouzrokovati ako bi se upotrijebio u protivpravnom aktu. Taj potencijal štete zatim dalje rukovodi procesom dodjeljivanja odgovarajućeg bezbjednosnog nivoa tom izvoru. Taj proces se sastoji od sljedećih koraka:

- Kategorizacija izvora na osnovu potencijala da se prouzrokuje šteta ako se taj izvor koristi u protivpravne svrhe (uključujući po potrebi i skup izvora na datoj lokaciji (vidi Dio 4.2.1);
- Dodjeljivanje odgovarajućeg bezbjednosnog nivoa svakoj kategoriji (vidi Dio 4.2.2).

4.2.1 Kategorizacija radioaktivnih izvora

"Kodeks ponašanja" se primjenjuje na radioaktivne izvore koji mogu predstavljati znatan rizik za pojedince, društvo i okoliš, odnosno izvore kategorija 1–3. Odgovarajuće mjere bezbjednosti se trebaju primijeniti u cilju smanjenja vjerovatnoće protivpravnih akata koji uključuju te izvore.

Kategorizacija izvora koja se koristi u "Kodeksu ponašanja" je zasnovana na konceptu "opasnih izvora", koji su kvantifikovani u smislu D vrijednosti [17]. Ovaj koncept se dalje razmatra u "Kategorizaciji radioaktivnih izvora" [3], IAEA. Ova publikacija daje preporučeni sistem kategorizacije, posebno za izvore koji se koriste u industriji, medicini, poljoprivredi, istraživanju i obrazovanju. Ovaj sistem kategorizacije se takođe može primijeniti, ako to odgovara, u državnom kontekstu, na izvore unutar vojnih ili odbrambenih programa. Kategorizacija predstavlja međunarodno usaglašenu osnovu za donošenje odluka na osnovu informacija o riziku i zasnovana je na logičnom i transparentnom metodu koji omogućava fleksibilnost da se može primijeniti u širokom rasponu okolnosti. Odluke na osnovu informacija o riziku se mogu donijeti u gradiranom pristupu regulatornoj kontroli radioaktivnih izvora u svrhe sigurnosti i bezbjednosti.

U znak priznanja činjenice da je ljudsko zdravlje od najviše važnosti, sistem kategorizacije je prvenstveno zasnovan na potencijalu radioaktivnih izvora da prouzrokuju deterministične zdravstvene efekte. D vrijednost je specifična aktivnost radionuklida za izvor koji, ako nije pod kontrolom, može prouzrokovati teške deterministične efekte u nizu scenarija koji uključuju i vanjsku ekspoziciju od nezaštićenog izvora i nenamjernu unutrašnju ekspoziciju nakon disperzije (npr. putem požara ili eksplozije) izvora.

Aktivnost radioaktivnog materijala (A) u izvorima varira zavisno od mnogo redova veličine; D vrijednosti se zbog toga koriste da se normalizuje niz aktivnosti kako bi se dala referenca za poređenje rizika. Ovo treba biti urađeno uzimanjem aktivnosti A za dati izvor (u TBq) i dijeljenjem te aktivnosti sa D vrijednošću za relevantni radionuklid.

Treba napomenuti da postoji mogućnost da količine materijala manje od D vrijednosti budu opasne [17]. Ovo se može desiti u slučaju namjerne primjene nezaštićenog radioaktivnog materijala na pojedincu.

Granične vrijednosti aktivnosti za radionuklide u "Kodeksu ponašanja" za izvore kategorija 1–3 navedene su u tabeli 3. Što se tiče radionuklida koji nisu navedeni u tabeli, molimo pogledajte reference [3, 17].

U nekim situacijama može biti prikladno kategorizovati neki izvor samo na osnovu omjera A/D, odnosno kada nije poznata ili nije potvrđena namjeravana upotreba izvora. Međutim, ako okolnosti upotrebe izvora jesu poznati, regulatorno tijelo može procijeniti da treba modifikovati početnu kategorizaciju koristeći druge informacije o tom izvoru ili njegovoj upotrebi. U nekim okolnostima može biti zgodno dodijeliti kategoriju na osnovu namjeravane upotrebe izvora (vidi tabelu 4).

Sistem kategorizacije ima pet kategorija, prikazanih u tabeli 4. Ovaj broj kategorija bi trebao biti dovoljan da omoguće praktične primjene ove šeme bez bezrazložne preciznosti. Unutar ovog sistema kategorizacije se izvori kategorije 1 smatraju najopasnijim jer mogu predstavljati veoma visok rizik za ljudsko zdravlje ako se njima ne upravlja na siguran i bezbjedan način. Ekspozicija od samo nekoliko minuta nezaštićenom izvoru kategorije 1 može biti smrtonosna. Na donjem kraju sistema kategorizacije su izvori kategorije 5, najmanje opasni; međutim, čak i ti izvori, ako se ne kontrolišu propisno, mogu dati doze koje prelaze granice doza i zbog toga trebaju biti pod odgovarajućom regulatornom kontrolom. Unutar kategorija ne treba postojati potpodjela, pošto bi to impliciralo stepen preciznosti koji se ne zahtijeva i može voditi gubitku međunarodne harmonizacije.

4.2.1.1 Izvori koji nisu navedeni

Što se tiče radioaktivnih izvora koji nisu navedeni u tabeli 4, regulatorno tijelo može dodijeliti kategoriju takvom izvoru na osnovu omjera A/D.

4.2.1.2 Kratkoživeći radionuklidi

Kod nekih djelatnosti, poput nuklearne medicine, radionuklidi sa kratkim vremenom poluraspada se koriste u obliku izvora koji je nezaštićen.

TABELA 3. AKTIVNOSTI KOJE ODGOVARAJU GRANIČNIM VRIJEDNOSTIMA KATEGORIJA

Radionuclide	Category 1 1000 ×D		Category 2 10 ×D		Category 3 D	
	(TBq)	(Ci)[a]	(TBq)	(Ci)[a]	(TBq)	(Ci)[a]
Am-241	6.E+01	2.E+03	6.E-01	2.E+01	6.E-02	2.E+00
Am-241/Be	6.E+01	2.E+03	6.E-01	2.E+01	6.E-02	2.E+00
Cf-252	2.E+01	5.E+02	2.E-01	5.E-00	2.E-02	5.E-01
Cm-244	5.E+01	1.E+03	5.E-01	1.E+01	5.E-02	1.E+00
Co-60	3.E+01	8.E+02	3.E-01	8.E+00	3.E-02	8.E-01
Cs-137	1.E+02	3.E+03	1.E+00	3.E+01	1.E-01	3.E+00
Gd-153	1.E+03	3.E+04	1.E+01	3.E+02	1.E+00	3.E+01
Ir-192	8.E+01	2.E+03	8.E-01	2.E+01	8.E-02	2.E+00
Pm-147	4.E+04	1.E+06	4.E+02	1.E+04	4.E+01	1.E+03
Pu-238	6.E+01	2.E+03	6.E-01	2.E+01	6.E-02	2.E+00
Pu-239[b]/Be	6.E+01	2.E+03	6.E-01	2.E+01	6.E-02	2.E+00
Ra-226	4.E+01	1.E+03	4.E-01	1.E+01	4.E-02	1.E+00
Se-75	2.E+02	5.E+03	2.E+00	5.E+01	2.E-01	5.E+00
Sr-90 (Y-90)	1.E+03	3.E+04	1.E+01	3.E+02	1.E+00	3.E+01
Tm-170	2.E+04	5.E+05	2.E+02	5.E+03	2.E+01	5.E+02
Yb-169	3.E+02	8.E+03	3.E+00	8.E+01	3.E-01	8.E+00
Au-198*	2.E+02	5.E+03	2.E+00	5.E+01	2.E-01	5.E+00
Cd-109*	2.E+04	5.E+05	2.E+02	5.E+03	2.E+01	5.E+02
Co-57*	7.E+02	2.E+04	7.E+00	2.E+02	7.E-01	2.E+01
Fe-55*	8.E+05	2.E+07	8.E+03	2.E+05	8.E+02	2.E+04
Ge-68*	7.E+02	2.E+04	7.E+00	2.E+02	7.E-01	2.E+01
Ni-63*	6.E+04	2.E+06	6.E+02	2.E+04	6.E+01	2.E+03
Pd-103*	9.E+04	2.E+06	9.E+02	2.E+04	9.E+01	2.E+03
Po-210*	6.E+01	2.E+03	6.E-01	2.E+01	6.E-02	2.E+00
Ru-106 (Rh-106)*	3.E+02	8.E+03	3.E+00	8.E+01	3.E-01	8.E+00
Tl-204*	2.E+04	5.E+05	2.E+02	5.E+03	2.E+01	5.E+02

[a] Primarne vrijednosti koje se trebaju koristiti su date u TBq. Vrijednosti u Ci su date u praktične svrhe i zaokružuju se nakon pretvaranja.
[b] Mjere za kritičnost i zaštitne mjere se trebaju razmotriti za umnožak D.
* Veoma je malo vjerovatno da će se ovi radionuklidi koristiti u individualnim radioaktivnim izvorima sa nivoima aktivnosti koji bi ih svrstali u kategorije 1, 2 ili 3 pa zbog toga ne bi podlijegali tačkama Kodeksa koje se odnose na državne registre ili sisteme kontrole uvoza i izvoza.

TABELA 4. KATEGORIJE ZA UOBIČAJENO KORIŠTENE IZVORE

Kategorija	Izvor[a]	A/D[b]
1	Radioizotopni termoelektrični generatori (RTG) Iradijatori Teleterapijski izvori Višestruki teleterapijski izvori (gama nož)	A/D $\geq$ 1000
2	Izvori u industrijskoj gama radiografiji Brahiterapijski izvori – visoka/srednja brzina doze	1000 > A/D $\geq$ 10
3	Fiksni industrijski mjerači koji sadrže izvor visoke aktivnosti[c] Izvori u ispitivanju bušotina	10 > A/D $\geq$ 1
4	Brahiterapijski izvori – niska brzina doze (osim pločica za terapiju oka i trajnih implantata) Industrijski mjerači koji ne sadrže izvor visoke aktivnosti Izvori za koštanu denzitometriju Eliminatori statičkog elektriciteta	1 > A/D $\geq$ 0.01
5	Brahiterapijski izvori – pločice za terapiju oka niske brzine doze i trajni implantati Izvori za XRF analizu Izvori u detektorima elektronskog zahvata Izvori za Mossbauerovu spektrometriju Izvori za provjeru kod PET uređaja (pozitronska emisiona tomografija)	0.01 > A/D i A > izuzet[d]

[a] Faktori pored samog A/D su uzeti u razmatranje pri dodjeljivanju kategorije izvoru (vidi referencu [3], Aneks I).

[b] Ovaj stubac se može koristiti da se utvrdi kategorija izvora čisto na osnovu omjera A/D. Naprimjer, ovo može biti prikladno ako objekti ili aktivnosti nisu poznati ili nisu navedeni, ako izvori imaju kratko vrijeme poluraspada i/ili su otvoreni ili ako su izvori agregirani (vidi referencu [3], tačka 3.5).

[c] Primjeri su dati u referenci [3], Aneks I.

[d] Izuzete količine su date u Dodatku I reference [5].

Primjeri takvih primjena uključuju ^{99m}Tc u radiodijagnostici i ^{131}I u radioterapiji. U takvim situacijama, principi sistema kategorizacije se mogu primijeniti da se utvrdi kategorizacija za određeni izvor. Te situacije treba razmotriti od slučaja do slučaja.

4.2.1.3. Otvoreni radioaktivni izvori

Regulatorno tijelo može dodijeliti određenu kategoriju otvorenim radioaktivnim izvorima na osnovu omjera A/D.

4.2.1.4. Radioaktivni raspad

Ako aktivnost izvora opada na nivo ispod odgovarajuće granične vrijednosti iz tabele 3 ili ispod one koja se obično koristi (prikazano u tabeli 4), regulatorno tijelo može dozvoliti operatoru da prekategoriše izvor na osnovu omjera A/D.

4.2.1.5. Skup izvora

Biće situacija u kojima su radioaktivni izvori vrlo blizu jedan drugog, kao što je u procesima proizvodnje (npr. u istoj prostoriji ili objektu) ili u skladištima (npr. u istom

ograđenom prostoru). U takvim okolnostima, regulatorno tijelo će možda htjeti da agregira aktivnosti više izvora da utvrdi kategorizaciju specifičnu za datu situaciju u svrhu provođenja mjera regulatorne kontrole. U situacijama ove vrste, ukupna aktivnost radionuklida se treba podijeliti sa odgovarajućom D vrijednošću, a izračunati omjer A/D uporediti sa omjerima A/D iz tabele 2, čim se omogućava kategorizacija skupa izvora na osnovu aktivnosti. Ako se koristi skup izvora koji sadrže različite radionuklide, onda zbir omjera A/D treba biti korišten pri utvrđivanju kategorije, u skladu s formulom:

$$\text{Aggregate A/D} = \sum_n \frac{\sum_i A_{i,n}}{D_n}$$

gdje je:

$A_{i,n}$ = aktivnost svakog pojedinog izvora *i*, radionuklida *n.* D_n = D vrijednost za radionuklid *n.*

Dodatne informacije o skupu radioaktivnih izvora mogu se naći u referenci [3].

4.2.2. Dodjeljivanje bezbjednosnih nivoa

Regulatorno tijelo može koristiti gore navedene kategorije kao zadani poredak da bi se datom izvoru dodijelio primjeren bezbjednosni nivo.

Izvori kategorije 1 trebaju imati mjere bezbjednosti koje ispunjavaju bezbjednosne zadatke bezbjednosnog nivoa A. Izvori kategorije 2 trebaju imati mjere bezbjednosti koje ispunjavaju bezbjednosne zadatke bezbjednosnog nivoa B. Izvori kategorije 3 trebaju imati mjere bezbjednosti koje ispunjavaju bezbjednosne zadatke bezbjednosnog nivoa C.

"Međunarodni osnovni sigurnosni standardi za zaštitu od jonizirajućeg zračenja i za sigurnost izvora zračenja" (tačka 2.34 [5]) uključuju opšte zahtjeve za bezbjednost radioaktivnih izvora. U ovom vodiču se smatra da iako te mjere kontrole omogućavaju dovoljan nivo bezbjednosti za radioaktivne izvore kategorija 4 i 5, pojačane mjere navedene u ovom vodiču trebaju biti primijenjene na radioaktivne izvore kategorija 1, 2 i 3 u namjeri da se smanji vjerovatnoća protivpravnog djela koje uključuje te izvore. Dalje, regulatorno tijelo, uzimajući u obzir prijetnju državi, možda će htjeti da pojača bezbjednost izvora kategorija 4 i 5 u odgovarajućim okolnostima. Ovaj pristup je rezimiran u tabeli 5.

Iako se ovaj pristup može posmatrati kao zadana pozicija, ne mora značiti da će protivpravna upotreba radioaktivnih izvora uključivati najviše rangirane izvore u šemi kategorizacije. Naprimjer, većina izvora kategorije 1 će se čuvati u zaštiti i unutar fiksnog uređaja ili objekta. Nastojanja da se takav izvor premjesti bi oduzela vrijeme i mogla izložiti potencijalne počinioce znatno štetnom nivou zračenja. Zbog toga je moguće da će se potencijalni počinioci fokusirati na izvore niže kategorije, manje opasne za rukovanje, lakše pristupačne, manje opasne za rukovanje, prenosive i koji se lakše mogu sakriti.

Svrha kategorisanja radioaktivnih izvora je da se omogući međunarodno prihvaćena osnova za donošenje odluka na osnovu informacija o riziku, uključujući i mjere za smanjenje vjerovatnoće protivpravnih akata. Međutim, društveno-ekonomske posljedice protivpravnih akata su bile isključene iz kriterija za kategorizaciju pošto ne postoji metodologija za kvantifikovanje i poređenje tih posljedica, posebno na međunarodnoj osnovi.

4.2.3. Dodatni obziri za dodjeljivanje bezbjednosnih nivoa

Aneks I "Kodeksa ponašanja" konstatuje da države trebaju posvetiti odgovarajuću pažnju onim radioaktivnim izvorima za koje smatraju da imaju potencijal prouzrokovanja

neprihvatljivih posljedica ako se upotrijebe u protivpravne svrhe.

Iako reference [3, 17] već uzimaju u obzir neke od dole navedenih faktora, regulatorno tijelo treba posvetiti posebnu pažnju tim faktorima i obzirima pri određivanju dodjeli bezbjednosnih nivoa radioaktivnim izvorima.

TABELA 5. PREPORUČENI ZADANI BEZBJEDNOSNI NIVOI ZA UOBIČAJENO KORIŠTENE IZVORE

Kategorija	Izvor	A/D	Bezbjednosni nivo
1	Radioizotopni termoelektrični generatori (RTG) Iradijatori Teleterapijski izvori Višestruki teleterapijski izvori (gama nož)	A/D $\geq$ 1000	A
2	Izvori u industrijskoj gama radiografiji Brahiterapijski izvori – visoka/srednja brzina doze	1000 > A/D $\geq$ 10	B
3	Fiksni industrijski mjerači koji sadrže izvor visoke aktivnosti Izvori u ispitivanju bušotina	10 > A/D $\geq$ 1	C
4	Brahiterapijski izvori – niska brzina doze (osim pločica za terapiju oka i trajnih implantata) Industrijski mjerači koji ne sadrže izvor visoke aktivnosti Izvori za koštanu denzitometriju Eliminatori statičkog elektriciteta	1 > A/D $\geq$ 0.01	Primijeniti mjere na način opisan u Osnovnim sigurnosnim standardima[5]
5	Brahiterapijski izvori – pločice za terapiju oka niske brzine doze i trajni implantati Izvori za XRF analizu Izvori u detektorima elektronskog zahvata Izvori za Mossbauerovu spektrometriju Izvori za provjeru kod PET uređaja (pozitronska emisiona tomografija)	0.01 > A/D i A > izuzet	

Ti faktori predstavljaju varijable koje su specifične za izvor, način i lokaciju na kojoj se on koristi – i mogu uticati na bezbjednosni nivo koji je odgovarajući za dati izvor ili objekt.

4.2.3.1 Privlačnost izvora

Pored aktivnosti izvora, postoje i drugi faktori koji mogu neke izvore učiniti privlačnijim za upotrebu u protivpravnim aktima. Ti faktori uključuju:

- Hemijski i fizički oblik radioaktivnog materijala u izvoru, koji ga može učiniti lako disperzibilnim i time i privlačnijim za potencijalnog počinioca.
- Prirodu radioaktivne emisije. Neki radionuklidi proizvode veće doze po jedinici unosa nego drugi, posebno alfa emiteri. Izvori koji sadrže te radionuklide mogu biti privlačniji za upotrebu u oružju za radiološko raspršivanje.
- Lakoću rukovanja. Izvori kojima se može lako rukovati ili lako pristupiti mogu biti privlačniji pošto potencijalni počinilac manje vjerovatno može dobiti visoku dozu zračenja, a izvor je lakši za premještanje. Primjer jednog takvog izvora je izvor unutar samozaštićenog prenosivog uređaja.
- Međusobnu blizinu. Više izvora ili velike količine radioaktivnog materijala koje su smještene jedna blizu druge mogu biti privlačne za potencijalnog počinioca

pošto uspješno prodiranje kroz sistem bezbjednosti može omogućiti premještanje ili sabotažu dovoljno materijala da se proizvedu veoma ozbiljne posljedice.
- Smatranu ekonomsku vrijednost izvora ili opreme u kojoj se nalazi.

Regulatorno tijelo će možda htjeti da razmotri privlačnost izvora pri utvrđivanju bezbjednosnog nivoa koji će se dodijeliti izvoru i mjere bezbjednosti koje će se primijeniti na taj bezbjednosni nivo.

4.2.3. Izvori u skladištu

Radioaktivni izvori smješteni u skladište trebaju biti zaštićeni u skladu sa mjerama datim u ovoj publikaciji i u skladu sa kategorizacijom i bezbjednosnim nivoom primijenjenim na dati izvor.

4.2.3.3 Nivo ugroženosti i prijetnje

Nivo prijetnje državi i bilo kakvo njegovo povećanje može zahtijevati evaluaciju bezbjednosnog nivoa primijenjenog na neki izvor, uzimajući u obzir sva druga svojstva tog izvora (npr. privlačnost, ugroženost). Alternativa je takođe jačanje specifičnih mjera bezbjednosti za dati bezbjednosni nivo.

4.2.3.4 Mobilni, prenosivi i udaljeni izvori

Izvori korišteni u primjenama na terenu (npr. radiografija i ispitivanje bušotina) se obično nalaze u uređajima koji su konstruisani da budu prenosivi i često se prevoze sa jedne radne lokacije na drugu. Lakoća rukovanja tim uređajima i njihovo prisustvo u vozilima van obezbijeđenih objekata čini ih privlačnim za neautorizovano premještanje.

Uz shvatanje da mjere bezbjednosti za fiksirane izvore možda neće biti praktične kod primjene izvora korištenih na terenu, treba primijeniti alternativne mjere da bi se ostvario dati bezbjednosni zadatak. Molimo vas da se osvrnete na mjere detekcije i zadržavanja za bezbjednosne nivoe B i C (Dio 4.3.1), kao i na ilustrativne mjere bezbjednosti za mobilne izvore u Aneksu IV.

Izvore koji se koriste na udaljenim lokacijama mogu premjestiti neautorizovani zaposleni i prevesti ih van tog područja prije nego što efikasan odgovor bude moguć.

Regulatorno tijelo će možda htjeti da razmotri mobilnost, prenosivost i lokaciju pri dodjeljivanju bezbjednosnog nivoa izvoru ili da razmotri dodatne mjere unutar već dodijeljenog bezbjednosnog nivoa da bi nadoknadilo takve okolnosti.

4.3 KORAK 3: ODABRATI I PRIMIJENITI REGULATORNI PRISTUP

Postoje tri alternativna pristupa koje regulatorno tijelo može koristiti za upućivanje operatora kako da dokažu da su ispunili bezbjednosne zadatke iz tabele 2. Pristup ili pristupi koje odabere regulatorno tijelo trebaju uzeti u obzir vlastite mogućnosti i resurse, mogućnosti i resurse operatora koje reguliše i raspon izvora koji trebaju biti zaštićeni:

- Preskriptivni pristup utvrđuje specifične mjere bezbjednosti koje regulatorno tijelo utvrdi radi ispunjavanja bezbjednosnih zadataka za svaki bezbjednosni nivo. Smjernice u ovom dijelu utvrđuju skup takvih mjera za svaki bezbjednosni nivo, koje regulatorno tijelo može usvojiti kao zahtjeve u nedostatku dokumenta o prijetnji kao osnovi koncepta. Alternativa je da regulatorno tijelo može koristiti mjere bezbjednosti iz ovih smjernica kao polaznu tačku i prilagoditi ih domaćim okolnostima. Korištenje preskriptivnog pristupa je posebno odgovarajuće u slučajevima u kojima je kombinacija prijetnje i potencijalnih posljedica mala ili u kojima obavljanje detaljne procjene prijetnje nije moguće. Preskriptivni pristup ima prednost jednostavnosti u

primjeni i za regulatorno tijelo i za operatore, te također lakoću inspekcije i revizije. Mana ovog pristupa je njegov relativni nedostatak fleksibilnosti da se pozabavi stvarnim okolnostima. Naprimjer, iskustvo je pokazalo da neki operator može poštovati propisane mjere, ali da ipak ne ispuni svrhu sistema bezbjednosti da zaštiti mete od stvarne ili definisane prijetnje. Kao posljedica, tamo gdje se preskriptivni pristup koristi, regulatorno tijelo treba osigurati da se obavljaju inspekcije ili procjene bezbjednosti radi evaluacije ukupne efikasnosti sistema bezbjednosti objekta u ispunjavanju bezbjednosnog cilja i zadataka za važeći bezbjednosni nivo (vidi Dio 4.3.1).

- Pristup zasnovan na uspješnosti je onaj u kojem regulatorno tijelo omogućava fleksibilnost operatoru da predloži konkretnu kombinaciju mjera bezbjednosti koje će se koristiti da se ostvare bezbjednosni zadaci iz tabele 2. Predložene mjere bezbjednosti trebaju biti zasnovane na procjeni ugroženosti, uzimajući u obzir informacije koje dostavi regulatorno tijelo, zasnovane na procjeni prijetnji državi i, gdje to odgovara, dokumentu o prijetnji kao osnovi konceptae. Prednost ovog pristupa je u tome što on prihvata da efikasan sistem bezbjednosti može biti sačinjen od mnogo kombinacija mjera bezbjednosti te da okolnosti svakog operatora mogu biti jedinstvene. Preduslov za ovaj pristup je zahtjev da i operator i regulatorno tijelo imaju relativno visok nivo stručnog znanja o bezbjednosti (vidi Dio 4.3.2).
- Kombinovani pristup uključuje elemente izvučene i iz preskriptivnog pristupa i iz pristupa zasnovanog na uspješnosti. Postoji mnogo mogućih verzija kombinovanog pristupa. Naprimjer, regulatorno tijelo može usvojiti skup mjera bezbjednosti među kojima operator može napraviti izbor, ali uz zahtjev operatorima da demonstriraju da sistem bezbjednosti kao cjelina ispunjava važeće bezbjednosne zadatke. Kao alternativu, regulatorno tijelo može koristiti pristup zasnovan na uspješnosti za radioaktivne izvore koji imaju najveće potencijalne posljedice od protivpravne upotrebe, a preskriptivni pristup za one izvore za koje bi posljedice bile manje. Ili, na skup preskriptivnih zahtjeva se mogu dodati zahtjevi koji su usmjereni na uspješnost i koji se bave određenim pitanjima. Glavna prednost kombinovanog pristupa je fleksibilnost koju on omogućava (vidi Dio 4.3.3).

U ostatku ovog dijela se daju smjernice regulatornim tijelima za korištenje svakog pristupa.

4.3.1 Preskriptivni pristup

Regulatorno tijelo se može opredijeliti da precizira mjere bezbjednosti za koje zahtijeva od operatora da ih imaju pripremljene u cilju ispunjavanja bezbjednosnih zadataka iz tabele 2. Tabele 6, 7 i 8 preciziraju mjere bezbjednosti čija je namjera da ispune bezbjednosne zadatke bezbjednosnih nivoa A, B i C pojedinačno. Ove tabele uključuju mjere bezbjednosti za izvore u upotrebi ili skladištu. Mjere se detaljno razmatraju nakon svake odgovarajuće tabele. One mogu varirati zavisno da li je dati izvor u upotrebi ili skladištu, odnosno da li je mobilan ili prenosiv. Više informacija o nekim od ovih mjera se može naći u Aneksu I. Ilustrativne mjere bezbjednosti koje se mogu primijeniti na odabrane objekte i aktivnosti su date u Aneksu IV.

Uvod za mjere bezbjednosnog nivoa A

Cilj bezbjednosnog nivoa A je **sprečavanje neautorizovanog premještanja** radioaktivnih izvora. Ako bi se desio pokušaj neautorizovanog pristupa ili neautorizovanog premještanja, detekcija i procjena bi se morale desiti dovoljno rano da se osoblju zaduženom za odgovor omogući reakcija sa dovoljno vremena i dovoljno resursa da omete potencijalnog počinioca i spriječi premještanje izvora. Da bi se ovaj cilj ostvario, preporučuju se sljedeće mjere.

Detekcija

Bezbjednosni zadatak: Omogućiti trenutnu detekciju neautorizovanog pristupa obezbijeđenoj zoni/lokaciji izvora.

Mjere bezbjednosti: Elektronski sistemi za detekciju upada i/ili kontinuirani nadzor od strane zaposlenih kod operatora.

Elektronski senzori povezani sa alarmom ili kontinuirani video nadzor od strane zaposlenih kod operatora pokazaće neautorizovan pristup obezbijeđenoj zoni (vidi dalje dio Zadržavanje) ili lokaciji izvora. Treba se obratiti pažnja u cilju osiguranja da se mjere detekcije upada ne mogu zaobići. Za izvore u upotrebi, takve mjere trebaju detektovati neautorizovan pristup obezbijeđenoj zoni u kojoj se izvor koristi. Za izvore u skladištu, takve mjere trebaju detektovati neautorizovan pristup zaključanoj prostoriji ili drugoj lokaciji na kojoj je izvor uskladišten. Za mobilne ili prenosive izvore u upotrebi, kontinuirani vizuelni nadzor bi mogao biti jedino izvodljivo sredstvo trenutne detekcije upada.

TABELA 6. PREPORUČENE MJERE ZA BEZBJEDNOSNI NIVO A
(Cilj: Spriječiti neautorizovano premještanje)

Bezbjednosna funkcija	Bezbjednosni zadatak	Mjere bezbjednosti
Detekcija	Omogućiti trenutnu detekciju neautorizovanog pristupa obezbijeđenoj zoni/lokaciji izvora.	Elektronski sistemi za detekciju upada i/ili kontinuirani nadzor od strane zaposlenih kod operatora.
	Omogućiti trenutnu detekciju pokušaja neautorizovanog premještanja izvora, uključujući i od strane počinioca iznutra.	Elektronska oprema za detekciju pokušaja neautorizovanog korištenja i/ili kontinuirani nadzor od strane zaposlenih kod operatora.
	Omogućiti trenutnu procjenu detekcije.	Monitoring s daljine korištenjem televizije zatvorenog kruga (CCTV) ili procjena od strane operatora/osoblja zaduženog za odgovor.
	Omogućiti trenutnu komunikaciju sa osobljem zaduženim za odgovor.	Brza, pouzdana, raznolika sredstva komunikacije poput telefona, mobilnih telefona, pejdžera, radio-stanica.
	Omogućiti sredstvo za detekciju gubitka putem verifikacije.	Svakodnevne provjere putem fizičkih provjera, CCTV-a, opreme za detekciju pokušaja neautorizovanog korištenja itd.
Zadržavanje	Omogućiti dovoljno zadržavanje nakon detekcije da osoblje zaduženo za odgovor prekine neautorizovano premještanje.	Sistem od najmanje dva sloja barijera (npr. zidovi, struktura s rešetkama) koji zajedno omogućavaju zadržavanje dovoljno da se omogući osoblju zaduženom za odgovor da prekine radnju.
Odgovor	Omogućiti trenutan odgovor na procijenjeni alarm, sa dovoljno resursa da se prekine i spriječi neautorizovano premještanje.	Mogućnost za trenutan odgovor, uz dovoljan broj ljudstva, opremu i obuku da se prekine radnja.
	Omogućiti kontrole pristupa lokaciji izvora kojima se efikasno ograničava pristup samo na autorizovane osobe.	Identifikacija i verifikacija, naprimjer, putem brave koju kontroliše čitač kroz koji se provlače kartice i PIN-om, ili ključa i kontrole ključa.

Upravljanje bezbjednošću	Osigurati povjerljivost autorizovanih osoba.	Bezbjednosne provjere za sve zaposlene koji su autorizovani za pristup lokaciji izvora bez pratnje i za pristup povjerljivim informacijama.
	Utvrditi i zaštititi povjerljive informacije.	Procedure za utvrđivanje povjerljivih informacija i njihovu zaštitu od neovlaštenog otkrivanja.
	Predvidjeti bezbjednosni plan.	Bezbjednosni plan koji je u skladu sa regulatornim zahtjevima i predviđa odgovor na povišene nivoe prijetnje.
	Osigurati sposobnost upravljanja bezbjednosnim događajima obuhvaćenim planom za bezbjednosne događaje.	Procedure za odgovor na scenarije koji se odnose na bezbjednost.
	Uspostaviti sistem izvještavanja o bezbjednosnim događajima.	Procedure za blagovremeno izvještavanje o bezbjednosnim događajima.

Bezbjednosni zadatak: Omogućiti trenutnu detekciju pokušaja neautorizovanog premještanja izvora (npr. od strane počinioca iznutra).

Mjere bezbjednosti: Elektronska oprema za detekciju pokušaja neautorizovanog korištenja ili kontinuirani nadzor od strane zaposlenih kod operatora.

Elektronski senzori povezani sa alarmom ili kontinuirani nadzor od strane zaposlenih kod operatora pokazaće pokušaj neautorizovanog premještanja izvora. Treba se obratiti pažnja u cilju osiguranja da se mjere detekcije neautorizovanog korištenja ne mogu zaobići. Za mobilne izvore u upotrebi, kontinuirani vizuelni nadzor bi mogao biti jedino izvodljivo sredstvo detekcije pokušaja neautorizovanog premještanja. Imajte u vidu da, ako se kontinuirani nadzor odabere kao bezbjednosna mjera, taj nadzor može zahtijevati uvijek najmanje dva pojedinca koji će vršiti nadzor u cilju zaštite od scenarija koji uključuje počinioca iznutra.

Bezbjednosni zadatak: Omogućiti trenutnu procjenu detekcije.

Mjere bezbjednosti: Monitoring s daljine korištenjem televizije zatvorenog kruga sa daljine (CCTV) ili procjena od strane operatora/osoblja zaduženog za odgovor.

Kad se oglasi alarm za detekciju upada ili pokušaja korištenja, treba uslijediti trenutna procjena uzroka alarma. Procjenu mogu obaviti zaposleni kod operatora na lokaciji izvora, putem CCTV-a ili je mogu obaviti osobe odmah raspoređene da ispitaju uzrok alarma. Za mobilne ili prenosive izvore u upotrebi, ili u drugim okolnostima u kojima detekciju upada ili detekciju pokušaja korištenja obavljaju zaposleni kod operatora kontinuiranim vizuelnim nadzorom, zaposleni kod operatora koji drže izvor pod kontinuiranim vizuelnim nadzorom trebaju obaviti procjenu istovremeno sa detekcijom.

Bezbjednosni zadatak: Omogućiti trenutnu komunikaciju sa osobljem zaduženim za odgovor.

Mjere bezbjednosti: Brza, pouzdana, raznolika sredstva komunikacije poput telefona, mobilnih telefona, pejdžera, radio-stanica.

Ako procjena potvrdi da se desio neautorizovani pristup ili pokušaj neautorizovanog premještanja, zaposleni kod operatora trebaju odmah obavijestiti osoblje zaduženo za odgovor korištenjem različitih sredstava komunikacije (najmanje dva), poput fiksnih telefona, uređaja za automatski telefonski poziv, mobilnih telefona, radio-stanica ili pejdžera.

Bezbjednosni zadatak: Omogućiti sredstvo za detekciju gubitka putem verifikacije.

Mjere bezbjednosti: Svakodnevne provjere putem fizičkih provjera, CCTV-a, opreme za detekciju pokušaja neautorizovanog korištenja itd.

Svakodnevne provjere se trebaju sastojati od mjera u cilju osiguranja da su izvori prisutni i da nisu dirani. Takve mjere bi mogle uključivati fizičke provjere da je izvor na svom mjestu, posmatranje preko CCTV-a sa daljine, verifikaciju pečata ili druge uređaje koji otkrivaju pokušaj korištenja, i mjerenja zračenja ili drugih fizikalnih pojava koje bi dale garanciju da je izvor prisutan. Za izvore u upotrebi, verifikovanje da je uređaj u funkciji može biti dovoljno.

Zadržavanje

Bezbjednosni zadatak: Omogućiti zadržavanje nakon detekcije, dovoljno da osoblje zaduženo za odgovor prekine neautorizovano premještanje.

Mjere bezbjednosti: Sistem od najmanje dva sloja barijera (npr. zidovi, struktura s rešetkama) koji zajedno omogućavaju zadržavanje dovoljno da se omogući osoblju zaduženom za odgovor da prekine radnju.

Uravnotežen sistem koji se sastoji od najmanje dvije barijere treba odvojiti izvor od neautorizovanih zaposlenih i omogućiti dovoljno vrijeme zadržavanja nakon detekcije da se omogući reakcija osoblja zaduženog za odgovor prije nego što počinilac premjesti izvor. Za izvore u upotrebi, takve mjere mogu uključivati zaključani uređaj u obezbijeđenoj zoni, time odvajajući uređaj od neautorizovanih zaposlenih. Za izvore u skladištu, takve mjere mogu uključivati zaključani i fiksirani kontejner ili uređaj koji sadrži izvor u zaključanoj skladišnoj prostoriji, time odvajajući kontejner od neautorizovanih zaposlenih. Za mobilne izvore u upotrebi, kontinuirani vizuelni nadzor od strane zaposlenih kod operatora može biti zamjena za jedan ili oba sloja barijera.

Odgovor

Bezbjednosni zadatak: Omogućiti trenutan odgovor na procijenjeni alarm, sa dovoljno resursa da se prekine i spriječi neautorizovano premještanje.

Mjere bezbjednosti: Mogućnost za trenutan odgovor, uz dovoljan broj ljudstva, opremu i obuku da se prekine radnja.

Operator treba uspostaviti protokole u cilju osiguranja raspoređivanja osoblja zaduženog za odgovor kao reakcije na alarm i bez zadržavanja. Odgovor treba biti i trenutan i adekvatan. *Trenutan* znači da osoblje zaduženo za odgovor, nakon što je obaviješteno, treba stići u vremenu kraćem od onog koje je potrebno da se prodre kroz barijere i obave radnje neophodne da se izvor premjesti. *Adekvatan* znači da tim za odgovor ima dovoljnu brojnost i osposobljenost da savlada potencijalnog počinioca. Odgovor mogu provesti direktno zaposleni radnici na obezbjeđenju, tim za bezbjednost zaposlen kod treće strane, lokalna policija ili državna žandarmerija.

Upravljanje bezbjednošću

Bezbjednosni zadatak: Omogućiti kontrole pristupa lokaciji izvora kojima se efikasno ograničava pristup samo na autorizovane osobe.

Mjere bezbjednosti: Identifikacija i verifikacija, naprimjer, putem brave koju kontroliše čitač kroz koji se provlače kartice i PIN-om, ili ključa i kontrole ključa.

Namjera kontrole pristupa je da se ograniči pristup lokaciji izvora na autorizovane osobe, generalno omogućavanjem tim osobama da privremeno onesposobe fizičke barijere poput zaključanih vrata (mjere zadržavanja) nakon verifikacije identiteta osobe i autorizacije pristupa. (U kontekstu medicinske ekspozicije, pacijenti ne trebaju biti "autorizovani" pošto imaju pratnju do izvora i pod stalnim su nadzorom medicinskog osoblja.)

Identitet i autorizacija osobe koja želi pristup može se verifikovati mjerama poput:

- ličnog identifikacionog broja (PIN) kojim se aktivira čitač za kontrolu vrata;
- sistema bedževa kojim je takođe moguće aktivirati elektronski čitač;
- procedura promjene bedževa na tački kontrole ulaza;
- biometrijskih karakteristika kojima se aktivira uređaj za kontrolu vrata.

Nakon verifikacije autorizacije pristupa za određenu osobu, sistem omogućava toj osobi da uđe u obezbijeđenu zonu ili na lokaciju izvora, npr. otvaranjem brave. Treba zahtijevati kombinaciju dvije ili više mjera verifikacije, npr. korištenje kartice koja se provlači kroz čitač i PIN; ili korištenje spomenute kartice i kontrolisanog ključa; ili PIN i kompjutersku lozinku, ili kontrolisani ključ i vizuelnu verifikaciju identiteta od strane drugih autorizovanih osoba. Za izvore u upotrebi, takve mjere trebaju kontrolisati pristup zoni u kojoj se izvor koristi. Za izvore u skladištu, takve mjere trebaju kontrolisati pristup zaključanoj prostoriji ili drugoj lokaciji na kojoj je izvor uskladišten. Za mobilne izvore u upotrebi, kontinuirani vizuelni nadzor od strane više zaposlenih kod operatora bi mogao biti zamjena za kontrolu pristupa.

Bezbjednosni zadatak: Osigurati povjerljivost autorizovanih osoba.

Mjere bezbjednosti: Bezbjednosne provjere za sve zaposlene koji su autorizovani za pristup lokaciji izvora bez pratnje i za pristup povjerljivim informacijama.

Povjerljivost osobe treba biti procijenjena kroz zadovoljavajuću bezbjednosnu provjeru prije nego što toj osobi bude dozvoljeno da bez pratnje pristupi radioaktivnim izvorima, lokacijama na kojima se izvori koriste ili skladište ili povjerljivim informacijama u vezi s tim. Priroda i obim bezbjednosnih provjera trebaju biti proporcionalni bezbjednosnom nivou za date radioaktivne izvore i u skladu sa propisima države ili na način koji odredi regulatorno tijelo. Kao minimum, bezbjednosne provjere trebaju uključivati potvrdu identiteta i verifikaciju referenci u cilju utvrđivanja integriteta, karaktera i pouzdanosti svake osobe. Taj proces se treba periodično razmatrati i biti podržan tekućom pažnjom nižih i viših rukovodilaca kako bi se osiguralo da zaposleni na svim nivoima nastavljaju da se ponašaju odgovorno i pouzdano, a da sva pitanja u ovom kontekstu budu iznesena pred relevantno tijelo.

Bezbjednosni zadatak: Utvrditi i zaštititi povjerljive informacije.

Mjere bezbjednosti: Procedure za utvrđivanje povjerljivih informacija i njihovu zaštitu od neovlaštenog otkrivanja.

Kao što je neophodno omogućiti bezbjednost radioaktivnih izvora, tako je neophodno i zaštititi prateće informacije, koje mogu obuhvatati dokumente, podatke o kompjuterskim sistemima i druge medije koji se mogu upotrijebiti da se saznaju detalji o:

- specifičnoj lokaciji i inventurnom spisku izvora;
- relevantnom bezbjednosnom planu i detaljnim bezbjednosnim modalitetima;
- sistemima bezbjednosti (npr. alarmi za detekciju upada), uključujući planove funkcionisanja i instalacije;
- privremenim ili dužim slabostima u programu bezbjednosti;
- rasporedu zaposlenih na obezbjeđenju i sredstvima odgovora na događaje ili alarme;
- planiranim datumima, rutama kretanja i načinima slanja ili transfera izvora;
- planovima za bezbjednosne vanredne situacije i bezbjednosnim mjerama odgovora.

Regulatorne smjernice takođe trebaju predvidjeti:

- kontrolu, skladištenje, pripremu, identifikaciju, označavanje i prenos dokumenata ili korespondencije koji sadrže povjerljive informacije;
- preporučene metode za uništavanje dokumenata koji sadrže povjerljive informacije;
- mehanizme koji obuhvataju skidanje oznake tajnosti i upravljanja dokumentima kada zastare ili više nisu povjerljivi.

Bezbjednosni zadatak: Predvidjeti bezbjednosni plan.

Mjere bezbjednosti: Bezbjednosni plan koji je u skladu sa regulatornim zahtjevima i predviđa odgovor na povišene nivoe prijetnje.

Bezbjednosni plan treba biti pripremljen za svaki objekt od strane njegovog operatora. Što se tiče primjera sadržaja bezbjednosnog plana, vidi Aneks II. Bezbjednosne planove može odobravati regulatorno tijelo i razmatrati ih u propisanim intervalima tokom procesa inspekcije kako bi se uvjerilo da oni odražavaju trenutni sistem bezbjednosti. Bezbjednosni planovi mogu biti različiti za mobilne i prenosive izvore u upotrebi ili za izvore u skladištu između perioda upotrebe. Vjerovatno će većina planova sadržavati povjerljive informacije o zaštitnim bezbjednosnim modalitetima i zbog toga planom treba upravljati u skladu s tim. Bezbjednosni plan takođe treba omogućiti efikasnu i trenutnu tranziciju na povišeni nivo bezbjednosti u slučaju povećanja prijetnje bezbjednosti.

Bezbjednosni zadatak: Osigurati sposobnost upravljanja bezbjednosnim događajima obuhvaćenim planom za bezbjednosne događaje.

Mjere bezbjednosti: Procedure za odgovor na scenarije koji se odnose na bezbjednost.

Planovi za bezbjednosne događaje trebaju biti sačinjeni u svakom objektu za niz događaja, uključujući:

- Sumnju na ili zaprijećeni protivpravni akt;
- Javne demonstracije koje imaju potencijal da budu prijetnja bezbjednosti izvora;
- Upad u obezbijeđenu zonu od strane jedne ili više neautorizovanih osoba. Ovo se može kretati od jednostavnog protivpravnog ulaska do odlučnog napada od strane onih koji žele premjestiti ili uticati na radioaktivne izvore.

Operatori trebaju sačiniti razumno predvidljive scenarije koji uključuju takve događaje i procedure za odgovor na njih. Planovi za bezbjednosne događaje trebaju biti dostavljeni odgovarajućim organima vlasti i uvježbavani u redovnim intervalima.

Bezbjednosni zadatak: Uspostaviti sistem izvještavanja o bezbjednosnim događajima.

Mjere bezbjednosti: Procedure za blagovremeno izvještavanje o bezbjednosnim događajima.

Operator treba sačiniti procedure za izvještavanje o bezbjednosnim događajima regulatornom tijelu, timovima koji prvi pružaju odgovor i, po potrebi, drugima, u vremenskom okviru koje propisuje regulatorno tijelo proporcionalno bezbjednosnom značaju događaja. Događaji o kojima se izvještava mogu uključivati:

- neslaganje u podacima o obračunu izvora;
- sumnju na krađu ili stvarna krađa radioaktivnog izvora;
- neautorizovani upad u objekt ili zonu u kojoj se izvori skladište;
- otkriće sumnjivog ili stvarnog eksplozivnog sredstva u ili blizu objekta ili skladišta;
- gubitak kontrole nad radioaktivnim izvorom;
- neautorizovan pristup ili neautorizovana upotreba izvora;
- druge protivpravne akte koji su prijetnja autorizovanim aktivnostima;
- sumnjive događaji ili zapažanja koja mogu ukazivati na planiranje napada sabotažom, upadom ili premještanjem izvora;
- kvar ili gubitak sistema bezbjednosti koji su suštinski za zaštitu radioaktivnih izvora.

TABELA 7. PREPORUČENE MJERE ZA BEZBJEDNOSNI NIVO B
(Cilj: Smanjenje vjerovatnoće neovlaštenog premještanja na minimum)

Bezbjednosna funkcija	Bezbjednosni zadatak	Mjere bezbjednosti
Detekcija	Omogućiti trenutnu detekciju neautorizovanog pristupa obezbijeđenoj zoni/lokaciji izvora.	Elektronski sistemi za detekciju upada i/ili kontinuirani nadzor od strane zaposlenih kod operatora.
	Omogućiti detekciju pokušaja neautorizovanog premještanja izvora	Oprema za detekciju pokušaja neautorizovanog korištenja i/ili periodične provjere od strane zaposlenih kod operatora.
	Omogućiti trenutnu procjenu detekcije.	Monitoring s daljine korištenjem televizije zatvorenog kruga (CCTV) ili procjena od strane operatora/osoblja zaduženog za odgovor.
	Omogućiti trenutnu komunikaciju sa osobljem zaduženim za odgovor.	Brza, pouzdana, raznolika sredstva komunikacije poput telefona, mobilnih telefona, pejdžera, radio-stanica.
	Omogućiti sredstvo za detekciju gubitka putem verifikacije.	Sedmične provjere putem fizičkih provjera, opreme za detekciju pokušaja neautorizovanog korištenja itd.
Zadržavanje	Omogućiti zadržavanje da se vjerovatnoća neautorizovanog premještanja smanji na minimum.	Sistem sa najmanje dva sloja barijera (npr. zidovi, struktura s rešetkama)

Odgovor	Omogućiti trenutno započinjanje odgovora da se prekine neautorizovano premještanje.	Oprema i procedure za započinjanje trenutnog odgovora.
Upravljanje bezbjednošću	Omogućiti kontrole pristupa lokaciji izvora kojima se efikasno ograničava pristup samo na autorizovane osobe.	Jedna mjera identifikacije.
	Osigurati povjerljivost autorizovanih osoba.	Bezbjednosne provjere za sve zaposlene koji su autorizovani za pristup lokaciji izvora bez pratnje i za pristup povjerljivim informacijama.
	Utvrditi i zaštititi povjerljive informacije.	Procedure za utvrđivanje povjerljviih informacija i njihovu zaštitu od neovlaštenog otkrivanja.
	Predvidjeti bezbjednosni plan.	Bezbjednosni plan koji je u skladu sa regulatornim zahtjevima i predviđa odgovor na povišene nivoe prijetnje.
	Osigurati sposobnost upravljanja bezbjednosnim događajima obuhvaćenim planom za bezbjednosne događaje.	Procedure za odgovor na scenarije koji se odnose na bezbjednost.
	Uspostaviti sistem izvještavanja o bezbjednosnim događajima.	Procedure za blagovremeno izvještavanje o bezbjednosnim događajima.

Uvod za mjere bezbjednosnog nivoa B

Cilj bezbjednosnog nivoa B je **smanjenje vjerovatnoće neovlaštenog premještanja** radioaktivnih izvora **na minimum**. Ako bi se desio pokušaj neautorizovanog pristupa ili neautorizovanog premještanja, odgovor mora biti započet odmah nakon detekcije i procjene upada, ali ne zahtijeva se pravovremen odgovor da se spriječi premještanje izvora. Da bi se ostvario ovaj cilj, preporučuju se mjere u nastavku.

Detekcija

Bezbjednosni zadatak: Omogućiti trenutnu detekciju neautorizovanog pristupa obezbijeđenoj zoni/lokaciji izvora.

Mjere bezbjednosti: Elektronska oprema za detekciju pokušaja neautorizovanog korištenja i/ili kontinuirani nadzor od strane zaposlenih kod operatora.

Elektronski senzori povezani sa alarmom ili kontinuirani vizuelni nadzor od strane zaposlenih kod operatora pokazaće pokušaj neautorizovanog pristupa obezbijeđenoj zoni (vidi dio "Zadržavanje" ispod) ili lokaciji izvora. Treba se obratiti pažnja u cilju osiguranja da se mjere detekcije upada ne mogu zaobići. Za izvore u upotrebi, takve mjere trebaju detektovati neautorizovani pristup obezbijeđenoj zoni u kojoj se izvor koristi. Za izvore u skladištu, takve mjere trebaju detektovati neautorizovani pristup zaključanoj prostoriji ili drugoj lokaciji na kojoj je izvor uskladišten. Za mobilne izvore ili prenosive izvore u upotrebi, kontinuirani vizuelni nadzor bi mogao biti jedino izvodljivo sredstvo detekcije upada.

Bezbjednosni zadatak: Omogućiti detekciju pokušaja neautorizovanog premještanja izvora.

Mjere bezbjednosti: Oprema za detekciju pokušaja neautorizovanog korištenja i/ili periodične provjere od strane zaposlenih kod operatora.

Oprema za detekciju pokušaja neautorizovanog korištenja ili vizuelni nadzor od strane zaposlenih kod operatora proveden tokom periodičnih provjera pokazaće pokušaj neautorizovanog premještanja izvora. Treba se obratiti pažnja u cilju osiguranja da se mjere detekcije pokušaja neautorizovanog korištenja ne mogu zaobići. Ovo se može omogućiti korištenjem elektronske opreme za detekciju pokušaja neautorizovanog korištenja. Za mobilne izvore ili prenosive izvore u upotrebi, kontinuirani vizuelni nadzor bi mogao biti jedino izvodljivo sredstvo detekcije pokušaja neautorizovanog premještanja.

Bezbjednosni zadatak: Omogućiti trenutnu procjenu detekcije.

Mjere bezbjednosti: Monitoring s daljine korištenjem televizije zatvorenog kruga s daljine (CCTV) ili procjena od strane operatora/osoblja zaduženog za odgovor.

Kad se oglasi alarm za detekciju upada, treba uslijediti trenutna procjena uzroka alarma. Procjenu mogu obaviti zaposleni kod operatora na lokaciji izvora, putem CCTV-a ili je mogu obaviti osobe odmah raspoređene odmah da ispitaju uzrok alarma. Za mobilne ili prenosive izvore u upotrebi, ili u drugim okolnostima u kojima detekciju upada ili detekciju pokušaja korištenja obavljaju zaposleni kod operatora kontinuiranim vizuelnim nadzorom, zaposleni kod operatora koji drže izvor pod kontinuiranim vizuelnim nadzorom trebaju obaviti procjenu istovremeno sa detekcijom.

Bezbjednosni zadatak: Omogućiti trenutnu komunikaciju sa osobljem zaduženim za odgovor.

Mjere bezbjednosti: Brza, pouzdana, raznolika sredstva komunikacije poput telefona, mobilnih telefona, pejdžera, radio-stanica.

Ako procjena potvrdi da se desio neautorizovani pristup ili pokušaj neautorizovanog premještanja, zaposleni kod operatora trebaju odmah obavijestiti osoblje zaduženo za odgovor korištenjem pouzdanih sredstava komunikacije, poput fiksnih telefona, uređaja za automatski telefonski poziv, mobilnih telefona, radio-stanica ili pejdžera.

Bezbjednosni zadatak: Omogućiti sredstvo za detekciju gubitka putem verifikacije.

Mjere bezbjednosti: Sedmične provjere putem fizičkih provjera, opreme za detekciju pokušaja neautorizovanog korištenja itd.

Sedmične provjere se sastoje od mjera u cilju osiguranja da su izvori prisutni i da nije pokušano neautorizovano korištenje. Takve mjere bi mogle uključivati fizičke provjere da je izvor na svom mjestu, verifikaciju pečata ili druge uređaje koji otkrivaju pokušaj korištenja, i mjerenja zračenja ili drugih fizikalnih pojava koje bi dale garanciju da je izvor prisutan. Za izvore u upotrebi, verifikovanje da je uređaj u funkciji može biti dovoljno.

Zadržavanje

Bezbjednosni zadatak: Omogućiti zadržavanje da se vjerovatnoća neautorizovanog premještanja smanji na minimum.

Mjere bezbjednosti: Sistem sa dva sloja barijera (npr. zidovi, struktura s rešetkama).

Uravnotežen sistem sa dvije barijere treba odvojiti izvor od neautorizovanih zaposlenih. Za izvore u upotrebi, takve mjere mogu uključivati zaključani uređaj u obezbijeđenoj zoni, time odvajajući uređaj od neautorizovanih zaposlenih. Za izvore u skladištu, takve mjere mogu uključivati zaključani i fiksirani kontejner ili uređaj koji sadrži izvor u zaključanoj skladišnoj prostoriji, time odvajajući kontejner od neautorizovanih zaposlenih. Za mobilne ili prenosive izvore u upotrebi, kontinuirani vizuelni nadzor od strane zaposlenih kod operatora može biti zamjena za barijere.

Odgovor

Bezbjednosni zadatak: Omogućiti trenutno započinjanje odgovora da se prekine neautorizovano premještanje.

Mjere bezbjednosti: Oprema i procedure za započinjanje trenutnog odgovora.

Operator treba uspostaviti protokole u cilju osiguranja trenutnog raspoređivanja osoblja zaduženog za odgovor kao reakcije na alarm i bez zadržavanja da bi prekinuo radnju potencijalnog počinioca. Odgovor mogu provesti direktno zaposleni radnici na obezbjeđenju, tim za bezbjednost zaposlen kod treće strane, lokalna policija ili državna žandarmerija. Odgovor treba biti koordiniran sa lokalnim vlastima da se ublaže potencijalne posljedice.

Upravljanje bezbjednošću

Bezbjednosni zadatak: Omogućiti kontrole pristupa lokaciji izvora kojima se efikasno ograničava pristup samo na autorizovane osobe.

Mjere bezbjednosti: Jedna mjera identifikacije.

Svrha kontrole pristupa je da se ograniči pristup lokaciji izvora na autorizovane osobe, generalno omogućavanjem tim osobama da privremeno onesposobe fizičke barijere poput zaključanih vrata (mjere zadržavanja) nakon verifikacije identiteta osobe i autorizacije pristupa (u kontekstu medicinske ekspozicije, pacijenti ne trebaju biti "autorizovani").

Identitet i autorizacija osobe koja želi pristup može se verifikovati mjerama poput:

- ličnog identifikacionog broja (PIN) kojim se aktivira čitač za kontrolu vrata;
- sistema bedževa kojim je takođe moguće aktivirati elektronski čitač;
- procedura promjene bedževa na tački kontrole ulaza;
- biometrijskih karakteristika kojima se aktivira uređaj za kontrolu vrata.

Nakon verifikacije autorizacije pristupa za određenu osobu, sistem omogućava toj osobi da uđe u obezbijeđenu zonu ili na lokaciju izvora, npr. otvaranjem brave. Treba zahtijevati najmanje jednu mjeru identifikacije, npr. korištenje kartice koja se provlači kroz čitač, PIN, kompjutersku lozinku, kontrolisani ključ ili vizuelnu verifikaciju identiteta od strane drugih autorizovanih osoba. Za izvore u upotrebi, takve mjere trebaju kontrolisati pristup zoni u kojoj se izvor koristi. Za izvore u skladištu, takve mjere trebaju kontrolisati pristup zaključanoj prostoriji ili drugoj lokaciji na kojoj je izvor uskladišten. Za mobilne ili prenosive izvore u upotrebi, kontinuirani vizuelni nadzor od strane zaposlenih kod operatora bi mogao biti zamjena za kontrolu pristupa.

Bezbjednosni zadatak: Osigurati povjerljivost autorizovanih osoba.

Mjere bezbjednosti: Bezbjednosne provjere za sve zaposlene koji su autorizovani za pristup lokaciji izvora bez pratnje i za pristup povjerljivim informacijama.

Povjerljivost osobe treba biti procijenjena kroz zadovoljavajuću bezbjednosnu provjeru prije nego što toj osobi bude dozvoljen pristup radioaktivnim izvorima bez pratnje, lokacijama na kojima se izvori koriste ili skladište ili povjerljivim informacijama u vezi s tim. Priroda i obim bezbjednosnih provjera trebaju biti proporcionalni bezbjednosnom nivou za date radioaktivne izvore i u skladu sa propisima države ili na način koji odredi regulatorno tijelo. Kao minimum, bezbjednosne provjere trebaju uključivati potvrdu identiteta i verifikaciju referenci u cilju utvrđivanja integriteta, karaktera i pouzdanosti svake osobe. Taj proces se treba periodično razmatrati i biti podržan tekućom pažnjom nižih i viših rukovodilaca kako bi se osiguralo da zaposleni na svim nivoima nastavljaju da se ponašaju odgovorno i pouzdano, a da sva pitanja u ovom kontekstu budu iznesena pred relevantno tijelo.

Bezbjednosni zadatak: Utvrditi i zaštititi povjerljive informacije.

Mjere bezbjednosti: Procedure za utvrđivanje povjerljviih informacija i njihovu zaštitu od neovlaštenog otkrivanja.

Kao što omogućava bezbjednost radioaktivnih izvora, sistem bezbjednosti tako treba zaštititi i prateće informacije, koje mogu obuhvatati dokumente, podatke o kompjuterskim sistemima i druge medije koji se mogu upotrijebiti da se saznaju detalji o:

- specifičnoj lokaciji i inventurnom spisku izvora;
- relevantnom bezbjednosnom planu i detaljnim bezbjednosnim modalitetima;
- sistemima bezbjednosti (npr. alarmi za detekciju upada), uključujući planove funkcionisanja i instalacije;
- privremenim ili dužim slabostima u programu bezbjednosti;
- rasporedu zaposlenih na obezbjeđenju i sredstvima odgovora na događaje ili alarme;
- planiranim datumima, rutama kretanja i načinim slanja ili transfera izvora;
- planovima za bezbjednosne vanredne situacije i bezbjednosnim mjerama odgovora.

Regulatorne smjernice takođe trebaju predvidjeti:

- kontrolu, skladištenje, pripremu, identifikaciju, označavanje i prenos dokumenata ili korespondencije koji sadrže povjerljive informacije;
- preporučene metode za uništavanje dokumenata koji sadrže povjerljive informacije;
- mehanizme koji obuhvataju skidanje oznake povjerljivosti i upravljanja dokumentima kada zastare ili više nisu povjerljivi.

Bezbjednosni zadatak: Predvidjeti bezbjednosni plan.

Mjere bezbjednosti: Bezbjednosni plan koji je u skladu sa regulatornim zahtjevima i predviđa odgovor na povišene nivoe prijetnje.

Bezbjednosni plan treba biti pripremljen za svaki objekt od strane njegovog operatora. Što se tiče primjera sadržaja bezbjednosnog plana, vidi Aneks II. Bezbjednosne planove može odobravati regulatorno tijelo i razmatrati ih u propisanim intervalima tokom procesa inspekcije kako bi se uvjerilo da oni odražavaju trenutni

sistem bezbjednosti. Bezbjednosni planovi mogu biti različiti za mobilne i prenosive izvore u upotrebi ili za izvore u skladištu između perioda upotrebe. Vjerovatno će većina planova sadržavati povjerljive informacije o zaštitnim bezbjednosnim modalitetima i zbog toga planom treba upravljati u skladu s tim. Bezbjednosni plan takođe treba omogućiti efikasnu i trenutnu tranziciju na povišeni nivo bezbjednosti u slučaju povećanja prijetnje bezbjednosti.

Bezbjednosni zadatak: Osigurati sposobnost upravljanja bezbjednosnim događajima obuhvaćenim planom za bezbjednosne događaje.

Mjere bezbjednosti: Procedure za odgovor na scenarije koji se odnose na bezbjednost.

Planovi za bezbjednosne događaje trebaju biti sačinjeni u svakom objektu za niz događaja, uključujući:

- Sumnju na ili zaprijećeni protivpravni akt;
- Javne demonstracije koje imaju potencijal da budu prijetnja bezbjednosti izvora;
- Upad u obezbijeđenu zonu od strane jedne ili više neautorizovanih osoba. Ovo se može kretati od jednostavnog protivpravnog ulaska do odlučnog napada od strane onih koji žele premjestiti ili uticati na radioaktivne izvore.

Operatori trebaju sačiniti razumno predvidljive scenarije koji uključuju takve događaje i procedure za odgovor na njih. Planovi za bezbjednosne događaje trebaju biti dostavljeni odgovarajućim organima vlasti i uvježbavani u redovnim intervalima.

Bezbjednosni zadatak: Uspostaviti sistem izvještavanja o bezbjednosnim događajima.

Mjere bezbjednosti: Procedure za blagovremeno izvještavanje o bezbjednosnim događajima.

Operator treba sačiniti procedure za izvještavanje o bezbjednosnim događajima regulatornom tijelu, timovima koji prvi pružaju odgovor i, po potrebi, drugima, u vremenskom okviru koje propisuje regulatorno tijelo proporcionalno bezbjednosnom značaju događaja. Događaji o kojima se izvještava mogu uključivati:

- neslaganje u podacima o obračunu izvora;
- sumnju na krađu ili stvarna krađa radioaktivnog izvora;
- neautorizovani upad u objekt ili zonu u kojoj se izvori skladište;
- otkriće sumnjivog ili stvarnog eksplozivnog sredstva u ili blizu objekta ili skladišta;
- gubitak kontrole nad radioaktivnim izvorom;
- neautorizovan pristup ili neautorizovana upotreba izvora;
- druge protivpravne akte koji su prijetnja autorizovanim aktivnostima;
- sumnjive događaje ili zapažanja koja mogu ukazivati na planiranje napada sabotažom, upadom ili premještanjem izvora;
- kvar ili gubitak sistema bezbjednosti koji su suštinski za zaštitu radioaktivnih izvora.

TABELA 8. PREPORUČENE MJERE ZA BEZBJEDNOSNI NIVO C
(Cilj: Smanjenje vjerovatnoće neautorizovanog premještanja)

Bezbjednosna funkcija	Bezbjednosni zadatak	Mjere bezbjednosti
Detekcija	Omogućiti detekciju neautorizovanog premještanja izvora.	Oprema za detekciju pokušaja neautorizovanog korištenja i/li periodične provjere od strane zaposlenih kod operatora.
	Omogućiti trenutnu procjenu detekcije.	Procjena od strane zaposlenih kod operatora ili osoblja zaduženog za odgovor.
	Omogućiti sredstvo za detekciju gubitka putem verifikacije.	Mjesečne provjere putem fizičkih provjera, opreme za detekciju pokušaja neautorizovanog korištenja ili druge vrste provjera u cilju potvrđivanja prisustva izvora.
Zadržavanje	Omogućiti zadržavanje da se smanji vjerovatnoća neautorizovanog premještanja izvora.	Jedna barijera (npr. struktura s rešetkama, kućište izvora) ili posmatranje od strane zaposlenih kod operatora.
Odgovor	Poduzeti odgovarajuće radnje u slučaju neautorizovanog premještanja izvora.	Procedure za utvrđivanje neophodnih radnji u skladu sa planovima za bezbjednosne događaje.
Upravljanje bezbjednošću	Omogućiti kontrole pristupa lokaciji izvora kojima se efikasno ograničava pristup samo na autorizovane osobe.	Jedna mjera identifikacije.
	Osigurati povjerljivost autorizovanih osoba.	Odgovarajuće metode za utvrđivanje povjerljivosti autorizovanih zaposlenih koji imaju pristup radioaktivnim izvorima bez pratnje i pristup povjerljivim informacijama.
	Utvrditi i zaštititi povjerljive informacije.	Procedure za utvrđivanje povjerljviih informacija i njihovu zaštitu od neovlaštenog otkrivanja.
	Predvidjeti bezbjednosni plan.	Dokumentacija o bezbjednosnim mehanizmima i referentnim procedurama.
	Osigurati sposobnost upravljanja bezbjednosnim događajima obuhvaćenim planom za bezbjednosne događaje.	Procedure za odgovor na scenarije koji se odnose na bezbjednost.
	Uspostaviti sistem izvještavanja o bezbjednosnim događajima.	Procedure za blagovremeno izvještavanje o bezbjednosnim događajima.

Uvod za mjere bezbjednosnog nivoa C

Cilj bezbjednosnog nivoa C je **smanjenje vjerovatnoće neautorizovanog premještanja** radioaktivnih izvora. Da bi se taj cilj ostvario, preporučuju se sljedeće mjere.

Detekcija

Bezbjednosni zadatak: Omogućiti detekciju neautorizovanog premještanja izvora.

Mjere bezbjednosti: Oprema za detekciju pokušaja neautorizovanog korištenja i/li periodične provjere od strane zaposlenih kod operatora.

Operatori trebaju verifikovati da su izvori prisutni. Mjere bi mogle obuhvatati fizičke provjere da je izvor na svom mjestu, verifikaciju pečata ili druge uređaje koji otkrivaju pokušaj korištenja, i mjerenja zračenja ili drugih fizikalnih pojava koje bi dale garanciju da je izvor prisutan. Za izvore u upotrebi, verifikovanje da je uređaj u funkciji može biti dovoljno.

Bezbjednosni zadatak: Omogućiti trenutnu procjenu detekcije.

Mjere bezbjednosti: Procjena od strane zaposlenih kod operatora ili osoblja zaduženog za odgovor.

Kada detekcija putem uređaja koji otkrivaju pokušaj korištenja ili fizičke provjere ukaže na to da je izvor možda nestao, treba uslijediti trenutna procjena situacije da se utvrdi da li se zaista desilo neautorizovano premještanje.

Bezbjednosni zadatak: Omogućiti sredstvo za detekciju gubitka putem verifikacije.

Mjere bezbjednosti: Mjesečne provjere putem fizičkih provjera, opreme za detekciju pokušaja neautorizovanog korištenja itd.

Mjesečne provjere se sastoje od mjera u cilju osiguranja da su izvori prisutni i da nije pokušano neautorizovano korištenje. Takve mjere bi mogle uključivati fizičke provjere da je izvor na svom mjestu, verifikaciju pečata ili druge uređaje koji otkrivaju pokušaj korištenja, i mjerenja zračenja ili drugih fizikalnih pojava koje bi dale garanciju da je izvor prisutan. Za izvore u upotrebi, verifikovanje da je uređaj u funkciji može biti dovoljno.

Zadržavanje

Bezbjednosni zadatak: Omogućiti zadržavanje da se smanji vjerovatnoća neautorizovanog premještanja izvora.

Mjere bezbjednosti: Jedna barijera (npr. struktura s rešetkama, kućište izvora) ili posmatranje od strane zaposlenih kod operatora

Najmanje jedna fizička barijera treba odvojiti izvor od neautorizovanih zaposlenih. Za izvore u upotrebi, takve mjere mogu uključivati kućište izvora ili upotrebu izvora u obezbijeđenoj zoni. Za izvore u skladištu, takve mjere mogu uključivati zaključani i fiksirani kontejner, uređaj koji sadrži izvor ili zaključanu skladišnu prostoriju da se odvoji kontejner od neautorizovanih zaposlenih. Za mobilne ili prenosive izvore u upotrebi, kontinuirani vizuelni nadzor od strane zaposlenih kod operatora može biti zamjena za barijeru.

Odgovor

Bezbjednosni zadatak: Poduzeti odgovarajuće radnje u slučaju neautorizovanog premještanja izvora.

Mjere bezbjednosti: Procedure za utvrđivanje neophodnih radnji u skladu sa planovima za bezbjednosne događaje.

Regulatorne procedure trebaju osigurati da sumnja na neautorizovano premještanje ili gubitak izvora bude procijenjena i, ako se potvrdi, prijavljena nadležnima bez odgađanja. Zatim treba nastojati da se izvor locira i vrati i ispitaju okolnosti koje su dovele do tog događaja.

Upravljanje bezbjednošću

Bezbjednosni zadatak: Omogućiti kontrole pristupa lokaciji izvora kojima se efikasno ograničava pristup samo na autorizovane osobe.

Mjere bezbjednosti: Jedna mjera identifikacije.

Namjera kontrole pristupa je da se ograniči pristup lokaciji izvora na autorizovane osobe, generalno omogućavanjem tim osobama da privremeno onesposobe fizičke barijere poput zaključanih vrata (mjere zadržavanja) nakon verifikacije identiteta osobe i autorizacije pristupa (u kontekstu medicinske ekspozicije, pacijenti ne trebaju biti "autorizovani").

Identitet i autorizacija osobe koja želi pristup može se verifikovati mjerama poput:

- ličnog identifikacionog broja (PIN) kojim se aktivira čitač za kontrolu vrata;
- sistema bedževa kojim je takođe moguće aktivirati elektronski čitač;
- procedura promjene bedževa na tački kontrole ulaza;
- biometrijskih karakteristika kojima se aktivira uređaj za kontrolu vrata.

Nakon verifikacije autorizacije pristupa za određenu osobu, sistem omogućava toj osobi da uđe u obezbijeđenu zonu ili na lokaciju izvora, npr. otvaranjem brave. Treba zahtijevati najmanje jednu mjeru identifikacije, npr. korištenje kartice koja se provlači kroz čitač, PIN, kompjutersku lozinku, kontrolisani ključ ili vizuelnu verifikaciju identiteta od strane drugih autorizovanih osoba. Za izvore u upotrebi, takve mjere trebaju kontrolisati pristup zoni u kojoj se izvor koristi. Za izvore u skladištu, takve mjere trebaju kontrolisati pristup zaključanoj prostoriji ili drugoj lokaciji na kojoj je izvor uskladišten. Za mobilne ili prenosive izvore u upotrebi, kontinuirani vizuelni nadzor od strane zaposlenih kod operatora bi mogao biti zamjena za kontrolu pristupa.

Bezbjednosni zadatak: Osigurati povjerljivost autorizovanih osoba.

Mjere bezbjednosti: Odgovarajuće metode za utvrđivanje povjerljivosti autorizovanih zaposlenih koji imaju pristup radioaktivnim izvorima bez pratnje i pristup povjerljivim informacijama.

Povjerljivost osobe treba biti procijenjena kroz zadovoljavajuću bezbjednosnu provjeru prije nego što toj osobi bude dozvoljen pristup radioaktivnim izvorima bez pratnje, lokacijama na kojima se izvori koriste ili skladište ili povjerljivim informacijama u vezi s tim. Priroda i obim bezbjednosnih provjera trebaju biti proporcionalni bezbjednosnom nivou za date radioaktivne izvore i u skladu sa propisima države ili na način koji odredi regulatorno tijelo.

Bezbjednosni zadatak: Utvrditi i zaštititi povjerljive informacije.

Mjere bezbjednosti: Procedure za utvrđivanje povjerljviih informacija i njihovu zaštitu od neovlaštenog otkrivanja.

Regulatorne odredbe trebaju osigurati da operator procijeni da li su pojedinci koji imaju pristup bezbjednosnim informacijama ili radioaktivnim izvorima pouzdani. Osim ako se utvrdi da su pouzdani, ne bi im trebao biti dat pristup bez pratnje.

Bezbjednosni zadatak: Predvidjeti bezbjednosni plan.

Mjere bezbjednosti: Dokumentacija o bezbjednosnim mehanizmima i referentnim procedurama.

Bezbjednosni mehanizmi i referentne procedure trebaju biti usvojeni u formi bezbjednosnog plana. Što se tiče primjera sadržaja bezbjednosnog plana, vidi Aneks II.

Bezbjednosni zadatak: Osigurati sposobnost upravljanja bezbjednosnim događajima obuhvaćenim planom za bezbjednosne događaje.

Mjere bezbjednosti: Procedure za odgovor na scenarije koji se odnose na bezbjednost.

Dokument o prikazu bezbjednosti treba obuhvatati procedure istrage i prijavljivanja neautorizovanog pristupa ili premještanja izvora.

Bezbjednosni zadatak: Uspostaviti sistem izvještavanja o bezbjednosnim događajima.

Mjere bezbjednosti: Procedure za blagovremeno izvještavanje o bezbjednosnim događajima.

Operator treba sačiniti procedure za izvještavanje o bezbjednosnim događajima regulatornom tijelu, timovima koji prvi pružaju odgovor i, po potrebi, drugima, u vremenskom okviru koje propisuje regulatorno tijelo proporcionalno bezbjednosnom značaju događaja. Događaji o kojima se izvještava mogu uključivati:

- neslaganje u podacima o obračunu izvora;
- sumnju na krađu ili stvarna krađa radioaktivnog izvora;
- neautorizovani upad u objekt ili zonu u kojoj se izvori skladište;
- otkriće sumnjivog ili stvarnog eksplozivnog sredstva u ili blizu objekta ili skladišta;
- gubitak kontrole nad radioaktivnim izvorom;
- neautorizovan pristup ili neautorizovano korištenje izvora;
- druge protivpravne akte koji su prijetnja autorizovanim aktivnostima;
- sumnjive događaje ili zapažanja koja mogu ukazivati na planiranje napada sabotažom, upadom ili premještanjem izvora;
- kvar ili gubitak sistema bezbjednosti koji su suštinski za zaštitu radioaktivnih izvora.

4.3.2. Pristup zasnovan na učinku

Regulatorno tijelo se može opredijeliti da precizira upotrebu pristupa zasnovanog na učinku kojim operatori ispunjavaju važeće bezbjednosne zadatke. Generalno, izbor pristupa države će zavisiti od stručnog znanja o bezbjednosti koje je na raspolaganju regulatornom tijelu i operatorima. Pristup zasnivan na učinku bi najefikasnije funkcionisao tamo gdje operatori imaju stručne savjetnike i stručno znanje za kreiranje i implementaciju neophodnih mjera i gdje su pokazali trajniju istoriju dosljednosti i poštovanja regulatornih zahtjeva. Regulatorno tijelo treba osigurati da su odobrene mjere jasno dokumentovane, npr. u okviru bezbjednosnog plana, i procjenjivane u odgovarajućim intervalima.

Što se tiče pristupa zasnovanog na učinku, država će trebati koristiti procjenu prijetnje državi i može se takođe opredijeliti da, po potrebi, sačini i dokument o prijetnji kao osnovi koncepta. Regulatorno tijelo treba dalje precizirati bezbjednosne zadatke za kategorije izvora na koje se odnosi pristup zasnovan na učinku. Generalno, ti bezbjednosni zadaci trebaju biti navedeni u smislu zahtijevane efikasnosti sistema, kao što je opisano u Dijelu 3.

Sistem bezbjednosti kojim se ispunjavaju važeći bezbjednosni zadaci zatim treba biti napravljen putem obavljanja procjene ugroženosti u odnosu na važeći dokument o prijetnji kao osnovi koncepta ili procijenjenu prijetnju. Zavisno od okolnosti, tu procjenu može obaviti regulatorno tijelo ili operator korištenjem pristupa navedenog u Dijelu 3 ili drugom metodologijom, na način koji odredi regulatorno tijelo. Rezultati procjene ugroženosti ili druge metodologije bi se takođe iskoristili da se dokaže da rezultirajući sistem bezbjednosti zaista ispunjava važeće bezbjednosne zadatke.

Ne mora značiti da bi skup mjera bezbjednosti razrađen primjenom pristupa zasnovanog na učinku odgovarao mjerama bezbjednosti za konkretni izvor koje se preporučuju korištenjem preskriptivnog pristupa i navedenih u tabelama 6–8. Iako bi mjere koje obuhvataju bezbjednosne funkcije *detekcije*, *zadržavanja* i *odgovora* iz tabele 2 bile uključene, konkretna kombinacija mjera može varirati u svjetlu analize specifične situacije obavljene putem procjene ugroženosti. Primjena pristupa zasnovanog na učinku generalno vodi ka prilagođenijem i rentabilnijem skupu mjera bezbjednosti nego što je to moguće korištenjem preskriptivnog pristupa. Pristup zasnovan na učinku nije pogodan za statističke analize *odvraćanja* ili *upravljanja bezbjednošću*, iako su te funkcije sastavni dio programa. U skladu s tim, pristup zasnovan na učinku takođe treba uključivati i zahtjev za mjerama odvraćanja i upravljanja bezbjednošću koje se odnose na bezbjednosni nivo za dati izvor, na način opisan u materijalu o preskriptivnom pristupu. U pristupu zasnovanom na učinku treba razmotriti sistematsku interakciju detekcije, zadržavanja i odgovora u utvrđivanju ukupne efikasnosti sistema naspram procijenjene prijetnje.

Efikasnost sistema je ključna mjera pristupa zasnovanog na učinku. Da bi se kreirao sistem bezbjednosti korištenjem tog pristupa, polazi se od pretpostavke da nijedna mjera odvraćanja neće uspjeti i da je protivpravni akt pokušan. Sistem bezbjednosti zato treba biti kreiran tako da ostvari zahtijevani nivo svoje efikasnosti u sprečavanju protivpravnog akta za koji se pretpostavlja da će se desiti u svjetlu procijenjene prijetnje.

4.3.3. Kombinovani pristup

Mnoge države žele kombinovati aspekte i preskriptivnog pristupa i pristupa zasnovanog na učinku da bi primijenile mjere bezbjednosti kojima se ispunjavaju gore navedeni bezbjednosni zadaci. Naprimjer, država može koristiti preskriptivni pristup za radioaktivne izvore za koje protivpravna upotreba rezultira manjim potencijalnim posljedicama, ali primijeniti pristup zasnovan na učinku na najopasnije izvore. Za najopasnije izvore bi se obavila procjena prijetnje državi i sačinio dokument o prijetnji kao osnovi koncepta. Dalje bi operator bio odgovoran za primjenu odgovarajućih mjera bezbjednosti da bi ispunio skup bezbjednosnih zadataka definisanih u smislu bezbjednosnih funkcija *odvraćanja*, *detekcije*, *zadržavanje*, *odgovora* i *upravljanja bezbjednošću*.

Aneks I

OPIS MJERA BEZBJEDNOSTI

Preporučene mjere bezbjednosti, od kojih su neke spomenute u Dijelu 4, navode se dalje u tekstu.

Pošto standardi variraju po državama, ova publikacija ne daje detaljne savjete o specifikacijama ili fizičkim karakteristikama bezbjednosne opreme. Međutim, globalna smjernica je da koncept i pouzdanost mjera bezbjednosti trebaju biti primjereni prijetnji koja je utvrđena procjenom prijetnje ili definisana u dokumentu o prijetnji kao osnovi koncepta. Generalno, to znači korištenje visokokvalitetne, dokazane opreme i tehnologije koja zadovoljava domaće ili međunarodne standarde kvaliteta.

I.1. KONTROLA PRISTUPA

Kontrola pristupa se može provoditi kroz kontrolne tačke na ulazu koje kontroliše osoblje zaduženo za odgovor, upotrebom elektronskih čitača ili mjerama kontrole ključa. Tehnologija u obliku automatskih sistema za kontrolu pristupa (AACS) dostupna je u raznim oblicima, od jednostavnih mehaničkih uređaja na dugme do sofisticiranijih čitača koji reaguju na daljinski modul ili individualne biometrijske karakteristike. U kombinaciji sa mehanizmom sa tri kraka koji se okreću jedan po jedan, AACS takođe može uključivati i kontrole sprečavanja praksi zaobilaženja redoslijeda kontrole i da jedna osoba stane neposredno iza druge koja ima pristup. U većini slučajeva, korištenje kartice treba biti verifikovano PIN-om koji se ukucava u čitač, a u povišenim bezbjednosnim stanjima tačku ulaska koja sadrži AACS treba nadgledati obezbjeđenje koje je vidljivo. Suštinski faktor za potencijalne operatore je da preciziraju izvodljiv AACS koji je primjeren zahtjevima i za kojeg proizvođač ili instalater može dati lokalnu podršku. Takođe je važno ograničiti pristup kompjuterima i softveru za upravljanje AACS-om da se spriječi neautorizovano narušavanje baze podataka sistema. Ako se konvencionalni sistem brave i ključa koristi kao sredstvo kontrole, onda brave trebaju biti dobrog kvaliteta, a treba sačiniti procedure rukovanja ključevima da se spriječi neautorizovan pristup ili ugrožavanje.

I.2. STRUKTURE S REŠETKAMA

Metalne strukture s rešetkama ili kontejneri se takođe mogu koristiti da se izvori odvoje i obezbijede dodavanjem dodatnog sloja zaštite, npr. privremenog zadržavanja unutar zone prijema i slanja izvora. Na drugim mjestima, strukture s rešetkama mogu biti dio modaliteta skladištenja unutar uspostavljene zone koja je ograđena i pod kontrolom i nadzorom.

I.3. NADZOR TELEVIZIJOM ZATVORENOG KRUGA (CCTV)

CCTV je korisno pomagalo koje omogućava zaposlenima na obezbjeđenju da nadgledaju prilaze ljudi spolja i zone u kojima su radioaktivni izvori uskladišteni. Kamere se mogu kombinovati sa sistemima za detekciju upada da se obezbijedi prikaz na kameri aktiviran događajem. Međutim, da bi bilo u potpunosti efikasno, funkcionisanje CCTV kamera i monitora treba biti redovno procjenjivano kako bi se osiguralo da one nastavljaju davati slike dobrog kvaliteta. Ovi sistemi takođe trebaju biti potpomognuti odgovorom, tako da se alarmi prouzrokovani događajem i indikatori koje aktivira tehnologija mogu ispitati.

I.4. KOMUNIKACIJA

Zaposlenima na obezbjeđenju na svim nivoima treba dati efikasna i pouzdana sredstva komunikacije. Ovo obuhvata i komunikaciju između patrola, fiksnih čuvarskih

mjesta i lokalnog centra za izvještavanje ili kontrolu te komunikaciju sa vanjskim agencijama koje su nadležne za davanje brzog odgovora na bezbjednosne događaje.

I.5. OGRADE I KAPIJE

Vrsta ograde korištene na vanjskom rubu objekta treba biti u skladu s prijetnjom, prirodom izvora koji se štite i ukupnom kategorijom lokacije. Postoje razne vrste ograda, od onih koji su malo više od oznake razdvajanja do onih koje su više robusne i mogu se kombinovati sa sistemima za detekciju i procjenu upada postavljenim na ogradu ili sa elektrificiranim pločama. Liniju ograde treba provjeravati redovno u cilju osiguranja da je struktura u dobrom stanju i da nije bilo narušavanja ili štete. Kapije unutar ograde trebaju biti konstruisane u skladu sa standardom ograde i obezbijeđene bravama dobrog kvaliteta.

I.6. SISTEMI ZA DETEKCIJU UPADA

Ovi sistemi su korisno sredstvo za nadzor nad bezbjednošću nekorištenog prostora. Ako je to prikladno, ova tehnologija se može proširiti i na vanjsku zonu objekta korištenjem sistema za detekciju i procjenu povrede vanjskog ruba zone. Svi sistemi detekcije upada trebaju biti potpomognuti odgovorom radi istrage o događaju ili uslovima koji su prouzrokovali alarm. Alarmi se mogu oglasiti daljinski na bezbjednosnoj kontrolnoj tački ili lokalno, putem zvučnika velike jačine. CCTV može biti korisno pomagalo u omogućavanju početne verifikacije događaja unutar zone u kojoj se oglasio alarm, ali obično tu treba podrška patrola koja vrši vizuelne provjere ili istragu.

I.7. PROCEDURE KONTROLE KLJUČA

Ključevi koji omogućavaju pristup radioaktivnim izvorima trebaju biti kontrolisani i obezbijeđeni. To mogu biti ključevi za strukturu s rešetkama, vrata, skladišne kontejnere ili zaštićene jedinice unutar kojih se koriste izvori. Slični nivoi kontrole trebaju biti primijenjeni na duplikate i rezervne ključeve.

I.8. BRAVE, ŠARKE I MEĐUZAVISNA VRATA

Brave koje se koriste za zaštitu radioaktivnih izvora trebaju biti dobrog kvaliteta, sadržavajući karakteristike koje će značiti određen otpor nasilnom ulasku. Isto važi za šarke na vratima. Ključevi trebaju biti čuvani na gore navedeni način u skladu sa proceduralnim mjerama. Unutar prostorija, međuzavisna vrata (*nap. prev.* interlocking; jedna vrata se ne mogu otvoriti dok se neka druga ne zatvore) koja ispunjavaju sigurnosne uslove mogu biti u službi interesa bezbjednosti putem kontrolisanja kretanja zaposlenih i omogućavanjem zaposlenima na obezbjeđenju da nadziru pristup objektu.

I.9. ZAKLJUČANI, ZAŠTIĆENI KONTEJNERI

Zaštita i fiksirane jedinice koje sadrže radioaktivne izvore mogu omogućiti zaštitu i mogu zadržati svaki pokušaj uticanja na izvor. Međutim, kada zaposleni nisu prisutni, takva zona treba biti pokrivena alarmnim sistemom za detekciju upada da bi se upozorilo osoblje zaduženo za odgovor ili zaposleni na obezbjeđenju na potrebu da ispitaju okolnosti upada.

I.10. ODRŽAVANJE I TESTIRANJE BEZBJEDNOSNE TEHNOLOGIJE

Znatan oslonac treba biti dat na bezbjednosnu tehnologiju da bi se omogućilo rano upozorenje ulaska potencijalnog počinioca na širu lokaciju ili u obezbijeđenu zonu. Sistemi za detekciju upada koji se koriste za zaštitu radioaktivnih izvora zato ne trebaju biti samo pravilno specificirani nego i takođe funkcionalno testirani nakon instalacije, održavani u redovnim intervalima od strane kompetentnih osoba, i testirani u intervalima

koje odredi regulatorno tijelo.

I.11. SISTEMI PROPUSNICA

Sistem propusnica je efikasno i rentabilno sredstvo omogućavanja prve indikacije da li pojedinac ima ovlaštenje da bude unutar date prostorije ili obezbijeđene zone. Ipak, propusnice treba provjeriti na ulazu u objekt, a nosilac propusnice je treba vidljivo nositi kao potvrdu ovlaštenja i pomoći u identifikaciji. Tehnologija ugradnje (embedded technology) takođe može omogućiti da propusnice budu kombinovane i za korištenje u sistemima kontrole pristupa.

I.12. OSIGURANJE KVALITETA

Bezbjednosni mehanizmi i procedure trebaju biti pripremljeni, dokumentovani i održavani u skladu sa preporučenim standardima osiguranja kvaliteta, kao što su: evidentiranje službenog odobrenja, kontrola verzije procedura, periodični i planirani uvid, testiranje modaliteta i procedura, i uključivanje stečenih iskustava u procedure.

I.13. BEZBJEDNOST I OSVIJETLJENOST PROSTORA

Efikasno osvjetljivanje prostora može dati važan doprinos fizičkoj zaštiti. U situacijama visoke bezbjednosti može biti potrebna specijalna konfiguracija osvjetljenja. Međutim, osvjetljenje područja i ulice koje je možda već u funkciji za druge svrhe često može dati osvjetljenje u cilju odvraćanja uljeza i pomoći patrolama osoblja zaduženog za odgovor.

I.14. SPECIJALNA BEZBJEDNOSNA VRATA I PRATEĆE KOMPONENTE (OKVIR ITD.)

Unutar određenih objekata koji imaju radioaktivne izvore može biti prikladno da se skladišne prostorije opreme specijalnim bezbjednosnim vratima i okvirom oko njih koji daje otpor nasilnom ulasku. Ovo bi bilo relevantno za zone koje se redovno ostavljaju bez nadzora.

I.15. REZERVNO NAPAJANJE

Prostorije iz kojih se kontroliše bezbjednost i sistemi bezbjednosti trebaju imati mogućnost da se izbore sa padom napona ili direktnim gubitkom glavnog napajanja strujom. Ovo se može osigurati putem neprekinutog snabdijevanja strujom (UPS) i rezervnim generatorom koji se automatski pali kad napon oscilira. Baterije kao rezerva imaju kratak vijek trajanja i zbog toga ih treba posmatrati kao kratkotrajni izvor rezervnog napajanja.

I.16. ZIDOVI

Osim ako već postoje, zidovi su skup način da se napravi granica vanjskog ruba lokacije. Zidovi takođe imaju manu što sprečavaju osoblje zaduženo za odgovor da posmatra područje van zaštićene zone.

Aneks II

PRIMJERI SADRŽAJA BEZBJEDNOSNOG PLANA

Bezbjednosni plan treba uključiti sve informacije koje su neophodne da se opiše pristup bezbjednosti i sistem koji se koristi za zaštitu izvora. Nivo detalja i širina sadržaja trebaju biti proporcionalni bezbjednosnom nivou izvora obuhvaćenih planom. Obično trebaju biti uključene sljedeće teme:

- Opis izvora, njihova kategorizacija i njihova upotreba.
- Opis okoline, objekta i/ili kompleksa u kojem se izvori koriste ili skladište, a po potrebi i plan kompleksa i sistema bezbjednosti.
- Lokaciju objekta ili kompleksa u odnosu na zone dostupne javnosti.
- Lokalne bezbjednosne procedure.
- Zadatke bezbjednosnog plana za dati objekt ili kompleks, uključujući:

    - specifična pitanja koja će se razmatrati: neautorizovano premještanje, uništenje ili zlonamjerna upotreba;
    - vrstu kontrole koja je neophodna da se spriječe neželjene posljedice, uključujući i pomoćnu opremu koja bi možda mogla biti potrebna;
    - opremu ili prostorije koje će biti obezbijeđene.

- Mjere bezbjednosti koje će se koristiti, uključujući:

    - mjere u cilju obezbjeđenja, omogućavanja nadzora, omogućavanja kontrole pristupa, detekcije, zadržavanja, odgovora i komunikacije;
    - karakteristike koncepta mjera u cilju procjene njihovog kvaliteta u odnosu na pretpostavljenu prijetnju.

- Administrativne mjere koje će se koristiti, uključujući:

    - bezbjednosne uloge i odgovornosti rukovodstva, zaposlenih i drugih;
    - rutinske i nerutinske operacije, uključujući i obračun izvora;
    - održavanje i testiranje opreme;
    - utvrđivanje povjerljivosti zaposlenih;
    - primjenu bezbjednosti informacija;
    - metode za autorizaciju pristupa;
    - bezbjednosne aspekte plana za nuklearno bezbjednosne događaje, uključujući i izvještavanje o događajima;
    - obuku;
    - procedure kontrole ključa.

- Procedure za rješavanje povišenog nivoa prijetnje.
- Proces periodične evaluacije efikasnosti plana i njegovog ažuriranja u skladu s tim.
- Eventualne kompenzacijske mjere koje će se možda morati koristiti.
- Reference na postojeće propise ili standarde.

Aneks III

OPIS PROCJENE UGROŽENOSTI

Procjena ugroženosti, takođe poznata kao ispitivanje bezbjednosti ili procjena bezbjednosti, jeste metod za evaluaciju zaštitnih sistema bezbjednosti. To je sistematsko procjenjivanje efikasnosti sistema bezbjednosti naspram procijenjene prijetnje (odnosno dokumenta o prijetnji kao osnovi koncepta ako on postoji). Procjena može biti po prirodi specifična ili opšta, mogu je obaviti operator lokalno ili država/regulatorno tijelo i može se koristiti kao pomoć u izradi propisa od strane države/regulatornog tijela ili za dokazivanje operatorovog poštovanja regulatornih propisa. Procjene treba obavljati obučeno osoblje. Suštinski elementi procjene ugroženosti su:

- Uspostavljanje inventarnog spiska radioaktivnih izvora i pratećih informacija, uz obraćanje pažnje na kategorizaciju, formu, lokaciju i fizičko okruženje. Ovaj proces takođe treba uključiti i izvore van upotrebe;
- Procjena potencijalnih posljedica povezanih sa neautorizovanim premještanjem izvora i njegovom protivpravnom upotrebom ili sa sabotažom u objektu;
- Uzimanje u obzir procjene prijetnje državi (ili dokumenta o prijetnji kao osnovi koncepta ako on postoji) i takođe bilo kojih lokalnih razmatranja;
- Utvrđivanje postojećih mjera bezbjednosti i procjenjivanje očekivane efikasnosti sistema bezbjednosti u odnosu na napade koji proizlaze iz hipotetičkih prijetnji (i/ili dokument o prijetnji kao osnovi koncepta ako on postoji); i
- Utvrđivanje koje su dodatne mjere bezbjednosti potrebne, ako ima takvih, da se osigura prihvatljiv i proporcionalan nivo zaštite.

Oni koji obavljaju procjenu ugroženosti trebaju biti tehnički eksperti upoznati sa datim objektom, posebno njegovim tehničkim i komercijalnim nužnostima, postojećim bezbjednosnim nivoima i sigurnosnim aspektima koji mogu pojačati stepen ukupne zaštite.

Aneks IV

ILUSTRATIVNE MJERE BEZBJEDNOSTI KOJE SE MOGU PRIMIJENITI NA ODABRANE OBJEKTE I AKTIVNOSTI

Namjera ovog aneksa je da za regulatorno tijelo potkrijepi Dio 4 ilustriranjem praktične primjene mjera bezbjednosti za niz relevantnih objekata i aktivnosti, uključujući mobilne operacije u kojima mjere koje važe za stacionarni objekt nisu izvodljive. Procjene prijetnji državi će varirati, pa će tako i mjere bezbjednosti trebati prilagoditi u skladu s tim.

Bezbjedn osna funkcija	Veliki stacionarni objekt Bezbjednosni nivo A (npr. industrijski ozračivač)	Manji stacionarni objekt Bezbjednosni nivo B (npr. malo preduzeće za radiografiju)	Manji stacionarni objekt Bezbjednosni nivo C (mala linija za preradu)	Prilagođavanja za mobilnu upotrebu Bezbjednosni nivo B (poseban slučaj) (npr. mobilna radiografija)
DETEKCIJA	Trenutna detekcija neautorizovanog pristupa obezbijeđenoj zoni/lokaciji izvora. *Sistem za detekciju i procjenu povrede vanjskog ruba zone i lokalni sistem za zaštitu od upada ili kontinuirani nadzor od strane zaposlenih kod operatora*	Trenutna detekcija neautorizovanog pristupa obezbijeđenoj zoni/lokaciji izvora. *Sistem za detekciju i procjenu povrede vanjskog ruba zone ili lokalni sistem za zaštitu od upada ili kontinuirani nadzor od strane zaposlenih kod operatora*		Trenutna detekcija neautorizovanog pristupa obezbijeđenoj zoni/lokaciji izvora. *Kontinuirani nadzor od strane zaposlenih kod operatora.* *Alarm na vozilu kad je izvor u skladištu.*
	Trenutna detekcija pokušaja neautorizovanog premještanja izvora, uključujući i od strane počinioca iznutra (insajdera). *Verifikacija putem podataka o kontroli procesa i međuzavisna vrata kad je izvor u upotrebi* *(lokalni alarm za detekciju upada kad je izvor u bazenu)*	Detekcija pokušaja neautorizovanog premještanja izvora. *Oprema za detekciju pokušaja neautorizovanog korištenja ili vizuelna inspekcija*	Detekcija neautorizovanog premještanja izvora. *Detekcija putem podataka o kontroli procesa i rutinskog održavanja*	Detekcija pokušaja neautorizovanog premještanja izvora. *Oprema za detekciju pokušaja neautorizovanog korištenja ili alarm na vozilu ili vizuelna inspekcija*
	Trenutna procjena detekcije *Monitoring alarma sa daljine ili putem CCTV-a (od strane zaposlenih kod operatora ili*	Trenutna procjena detekcije *Monitoring alarma sa daljine ili putem CCTV-a (od strane zaposlenih kod operatora ili*	Trenutna procjena detekcije *Vizuelna inspekcija*	Trenutna procjena detekcije *Zaposleni kod operatora (Zaposleni kod klijenta ako je rad na terenu)*

	lokalne policije) *Zaštitarska patrola*	*lokalne policije)*		
	Trenutna komunikacija sa osobljem zaduženim za odgovor *Fiksni telefon i jedno od sljedećeg:* *mobilna radio-stanica s privatnom linijom,* *mobilni telefon,* *pejdžer.*	Trenutna komunikacija sa osobljem zaduženim za odgovor *Fiksni telefon* *Mobilni telefon*		Trenutna komunikacija sa osobljem zaduženim za odgovor *Mobilni telefon i/ili mobilna radio-stanica s privatnom linijom* *Fiksni telefon ako je rad na terenu*
	Sredstvo za detekciju gubitka izvora putem verifikacije *Verifikacija putem podataka o kontroli procesa i međuzavisna vrata kad je izvor u upotrebi* *(lokalni alarm za detekciju upada kad je izvor u bazenu)*	Sredstvo za detekciju gubitka izvora putem verifikacije *Verifikacija putem korištenja sigurnosne instrumentacije*	Sredstvo za detekciju gubitka izvora putem verifikacije *Verifikacija putem podataka o kontroli procesa i korištenjem sigurnosne instrumentacije za izvor u skladištu*	Sredstvo za detekciju gubitka izvora putem verifikacije *Verifikacija putem korištenja sigurnosne instrumentacije i vizuelne inspekcije*
ZADRŽAVANJE	Zadržavanje nakon detekcije dovoljno da osoblje zaduženo za odgovor prekine neautorizovano premještanje *Vanjski zid.* *Brave na kontrolnoj tabli procesa/međuzavisna vrata.* *Zaključano skladište alata*	Zadržavanje da se smanji vjerovatnoća neautorizovanog premještanja na minimum *Vanjski zid.* *Brave na radiografskoj ćeliji/međuzavisna vrata.* *Zaključano skladište alata*	Zadržavanje da se smanji vjerovatnoća neautorizovanog premještanja *Jedna barijera poput strukture s rešetkama ili kućišta i obezbijeđene pričvršćenosti*	Zadržavanje da se smanji vjerovatnoća neautorizovanog premještanja na minimum *Kontinuirani nadzor od strane zaposlenih kod operatora.* *Brave na kontejneru izvora.*

	koji se koriste za proces. Bezbjednosna[1] vrata i prateće komponente (okvir itd.)	*koji se koriste za proces. Bezbjednosna vrata i prateće komponente (okvir itd.).* *Van radnog vremena: obezbijeđeno skladište izvora ili bunker*		*Zaključano skladište alata koji se koriste za proces.* *Van radnog vremena: vozilo zaključano i opremljeno alarmom.*
ODGOVOR	Trenutni odgovor na procijenjeni alarm sa dovoljno resursa da se prekine i spriječi neautorizovano premještanje *Zaposleni kod operatora. Policijski odgovor.*	Trenutno započinjanje odgovora u cilju prekida radnje *Zaposleni kod operatora. Policijski odgovor.*	Odgovarajuća radnja u slučaju neautorizovanog premještanja izvora *Zaposleni kod operatora. Policijski odgovor.*	Trenutno započinjanje odgovora u cilju prekida radnje *Zaposleni kod operatora. Policijski odgovor*
UPRAVLJANJE BEZBJEDNOŠĆU	Kontrole pristupa lokaciji izvora kojima se pristup efikasno ograničava samo na autorizovano osoblje. *Sistem propusnica ili identifikacija i verifikacija prepoznavanjem od strane zaposlenih kod operatora*	Kontrole pristupa lokaciji izvora kojima se pristup efikasno ograničava samo na autorizovano osoblje. *Prepoznavanje od strane zaposlenih kod operatora. Brave odgovarajuće specifikacije.* *Upravljanje ključevima (sef, procedure itd.)*	Kontrole pristupa lokaciji izvora kojima se pristup efikasno ograničava samo na autorizovano osoblje. *Jedna barijera poput strukture s rešetkama ili kućišta i obezbijeđene pričvršćenosti.*	Kontrole pristupa lokaciji izvora kojima se pristup efikasno ograničava samo na autorizovano osoblje. *Prepoznavanje od strane zaposlenih kod operatora. Brave na vozilu odgovarajuće specifikacije.* *Ključevi čuvani kod autorizovanog osoblja.*

[1] Nap. prev.: *U originalu je "security final door", ali nisam uspio naći značenje za "final" u ovom kontekstu.*

	Povjerljivost autorizovanih osoba. *Periodične bezbjednosne provjere zaposlenih kod operatora u skladu sa politikom države.*	Povjerljivost autorizovanih osoba. *Periodične bezbjednosne provjere zaposlenih kod operatora u skladu sa politikom države.*	Povjerljivost autorizovanih osoba. *Periodične bezbjednosne provjere zaposlenih koji su uključeni u upravljanje izvorima kod operatora u skladu sa politikom države.*	Povjerljivost autorizovanih osoba. *Periodične bezbjednosne provjere zaposlenih kod operatora u skladu sa politikom države.*
	Utvrditi i zaštititi povjerljive informacije *Promovisanje kulture bezbjednosti.* *Relevantna obuka zaposlenih.* *Uloge i odgovornosti.* *Zaštita inventurne liste.* *Bezbjednosni plan.* *Procedure upravljanja bezbjednošću.* *Bezbjednosni kontejneri.*	Utvrditi i zaštititi povjerljive informacije *Promovisanje kulture bezbjednosti.* *Relevantna obuka zaposlenih.* *Uloge i odgovornosti.* *Zaštita inventurne liste.* *Bezbjednosni plan.* *Procedure upravljanja bezbjednošću.* *Bezbjednosni kontejneri.*	Utvrditi i zaštititi povjerljive informacije *Promovisanje kulture bezbjednosti.* *Relevantna obuka zaposlenih.* *Uloge i odgovornosti.* *Zaštita inventurne liste.* *Bezbjednosni plan.* *Procedure upravljanja bezbjednošću.* *Bezbjednosni kontejneri (zaključan ormar).*	Utvrditi i zaštititi povjerljive informacije *Promovisanje kulture bezbjednosti.* *Relevantna obuka zaposlenih.* *Uloge i odgovornosti.* *Zaštita inventurne liste (u sjedištu firme).* *Bezbjednosni plan.* *Procedure upravljanja bezbjednošću.* *Bezbjednosni kontejneri (u sjedištu firme).*
	Bezbjednosni plan. *Bezbjednosni plan u skladu sa Aneksom II.*	Bezbjednosni plan. *Bezbjednosni plan u skladu sa Aneksom II.*	Bezbjednosni plan. *Dokument o prikazu bezbjednosti u skladu sa Aneksom II.*	Bezbjednosni plan. *Bezbjednosni plan u skladu sa Aneksom II.*

REFERENCE

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Code of Conduct on the Safety and Security of Radioactive Sources, IAEA/CODEOC/2004, IAEA, Vienna (2004).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Radioactive Sources (Interim Guidance for Comment), IAEA-TECDOC-1355, IAEA, Vienna (2003).

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Categorization of Radioactive Sources, IAEA Safety Standards Series No. RS-G-1.9, IAEA, Vienna (2005).

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Radiation Generators, IAEA Safety Standards Series No. RS-G-1.10, IAEA, Vienna (2007).

[5] FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL LABOUR ORGANIZATION, OECD NUCLEAR ENERGY AGENCY, PAN AMERICAN HEALTH ORGANIZATION, WORLD HEALTH ORGANIZATION, International Basic Safety Standards for Protection against Ionizing Radiation and for the Safety of Radiation Sources, Safety Series No. 115, IAEA, Vienna (1996).

[6] EUROPEAN ATOMIC ENERGY COMMUNITY, FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL LABOUR ORGANIZATION, INTERNATIONAL MARITIME ORGANIZATION, OECD NUCLEAR ENERGY AGENCY, PAN AMERICAN HEALTH ORGANIZATION, UNITED NATIONS ENVIRONMENT PROGRAMME, WORLD HEALTH ORGANIZATION, Fundamental Safety Principles IAEA Safety Standards Series No SF-1, IAEA, Vienna (2006).

[7] International Convention for the Suppression of Acts of Nuclear Terrorism, United Nations, New York (2005).

[8] Convention on the Physical Protection of Nuclear Material, INFCIRC/274/Rev.1, IAEA, Vienna (1980); CPPNM Amendment, GOV/INF/2005/10–GC(49)/INF/6, IAEA, Vienna (2005).

[9] INTERNATIONAL ATOMIC ENERGY AGENCY, Preparedness and Response for a Nuclear or Radiological Emergency IAEA Safety Standards Series No. GS-R-2, IAEA, Vienna (2002).

[10] INTERNATIONAL ATOMIC ENERGY AGENCY, Remediation of Areas Contaminated by Past Activities and Accidents Safety Requirement, IAEA Safety Standards Series No. WS-R-3, IAEA, Vienna (2003).

[11] INTERNATIONAL COMMISION ON RADIOLOGICAL PROTECTION, Protecting People against Radiation Exposure in the Event of A Radiological Attack Publication 96, Pergamon Press, Oxford (2005).

[12] INTERNATIONAL ATOMIC ENERGY AGENCY, Security in the Transport of Radioactive Material, IAEA Nuclear Security Series No. 9, IAEA, Vienna (2008).

[13] INTERNATIONAL ATOMIC ENERGY AGENCY, Development, Use and Maintenance of the Design Basis Threat, IAEA Nuclear Security Series No. 10, IAEA, Vienna (2009).

[14] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Culture, IAEA Nuclear Security Series No. 7, IAEA, Vienna (2008).

[15] INTERNATIONAL ATOMIC ENERGY AGENCY Preventive and Protective Measures against Insider Threats, IAEA Nuclear Security Series No. 8, IAEA, Vienna (2008).

[16] INTERNATIONAL ATOMIC ENERGY AGENCY, Legal and Governmental Infrastructure for Nuclear, Radiation, Radioactive Waste and Transport, IAEA Safety Standards Series No. GS-R-1, IAEA, Vienna (2000).

[17] INTERNATIONAL ATOMIC ENERGY AGENCY, Dangerous Quantities of Radioactive Material (EPR-D-Values), IAEA, Vienna (2006).

[18] INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Safety Glossary: Terminology Used in Nuclear Safety and Radiation Protection, IAEA, Vienna (2007), http://www-ns.iaea.org/standards/safety-glossary.html.

[19] The Physical Protection of Nuclear Material and Nuclear Facilities, INFCIRC/225/Rev.4 (Corrected), IAEA, Vienna (1999).

DEFINICIJE

Autorizacija. Dozvola data u dokumentu od strane regulatornog tijela licu koje je podnijelo zahtjev za upravljanje radioaktivnim izvorom. Autorizacija može imati oblik registracije, licence ili alternativnih efikasnih mjera zakonske kontrole kojima se ostvaruju zadaci iz "Kodeksa ponašanja" (preuzeto iz reference [1]).

Dokument o prijetnji kao osnovi koncepta. Sveobuhvatni opis motivacija, namjera i mogućnosti potencijalnih počinilaca na osnovu čega se sistemi zaštite kreiraju i evaluiraju (prilagođeno iz reference [13]).

Izvor van upotrebe. Radioaktivni izvor koji se više ne koristi i za koji ne postoji namjera da se koristi u objektima i aktivnostima za koje je izdata autorizacija (preuzeto iz reference [18]).

Protivpravni akt. Nezakonita radnja ili aktivnost namjerno izvršena ili u kojoj se učestvuje bez zakonskog opravdanja ili razloga (npr. krijumčarenje), ili radnja ili aktivnost sa namjerom da se prouzrokuje smrt ili fizička povreda osobe, materijalna šteta osobi (npr. krađa) ili šteta imovini ili okolišu (preuzeto iz GOV/2002/10).

Operator. Pravno ili fizičko lice koje podnosi zahtjev za autorizaciju ili je autorizovano i/ili odgovorno za nuklearnu sigurnost, radijacijsku sigurnost, sigurnost radioaktivnog otpada ili sigurnost transporta pri obavljanju aktivnosti ili u vezi sa nuklearnim objektima ili izvorima jonizirajućeg zračenja. Ovo uključuje fizička lica, organe vlasti, pošiljaoce ili prevoznike, vlasnike licence, bolnice, osobe koje obavljaju samostalnu djelatnost itd. (preuzeto iz reference [18]).

Radioaktivni izvor. Radioaktivni materijal koji je trajno zapečaćen u kapsuli ili čvrsto uvezan, u čvrstom obliku i koji nije izuzet od regulatorne kontrole. On takođe označava svaki ispušteni radioaktivni materijal ako radioaktivni izvor curi ili je u kvaru, ali ne označava materijal stavljen u kapsulu u svrhu odlaganja, niti nuklearni materijal u okviru ciklusa nuklearnog goriva istraživačkih i energetskih reaktora (preuzeto iz reference [1]).

Regulatorno tijelo. Pravni subjekt ili organizacija ili sistem pravnih subjekata ili organizacija kojem vlada države odredi zakonsko ovlaštenje za vršenje regulatorne kontrole u pogledu radioaktivnih izvora, uključujući izdavanje autorizacija i time i regulisanja jednog ili više aspekata sigurnosti ili bezbjednosti radioaktivnih izvora (preuzeto iz reference [1]).

Sabotaža. Namjerna šteta; sabotaža u ovom kontekstu znači namjernu štetu radioaktivnom izvoru u upotrebi, skladištu ili transportu ili štetu pratećem objektu. Namjerna radnja uperena protiv radioaktivnog izvora u upotrebi, skladištu ili transportu bi mogla direktno ili indirektno dovesti u opasnost zdravlje i sigurnost zaposlenih, stanovništvo ili okoliš ekspozicijom zračenju ili oslobađanjem radioaktivnog materijala (prilagođeno iz reference [19]).

(Nuklearna) bezbjednost. Prevencija, detekcija i odgovor na krađu, sabotažu, neautorizovani pristup, nezakoniti transfer ili druga protivpravnih djela koja uključuju nuklearni materijal, druge radioaktivne supstance ili njihove prateće objekte (preuzeto iz reference [12]).

Kultura bezbjednosti. Karakteristike i stavovi u organizacijama i među osobama kojima se utvrđuje da pitanja bezbjednosti dobijaju pažnju koju njihov značaj zahtijeva (preuzeto iz reference [1]).

Plan za bezbjednosne događaje. Dio bezbjednosnog plana ili samostalni dokument kojim se utvrđuju razumno predvidljivi bezbjednosni događaji, predviđaju početne

planirane radnje (uključujući upozoravanje odgovarajućih organa vlasti) i dodjeljuju odgovornosti odgovarajućim zaposlenim kod operatora i osoblju zaduženom za odgovor.

Bezbjednosni plan. Dokument – kojeg priprema operator uz mogući uslov da ga regulatorno tijelo razmotri – koji predstavlja detaljan opis bezbjednosnih modaliteta u funkciji u određenom objektu.

Skladištenje. Držanje radioaktivnih izvora u objektu kojim se omogućava njihovo ograničavanje sa namjerom povrata (preuzeto iz reference [1]).

Procjena prijetnje. Analiza kojom se dokumentuju vjerodostojne motivacije, namjere i mogućnosti potencijalnih počinilaca koji bi mogli uzrokovati neželjene posljedice u vezi sa radioaktivnim materijalom u upotrebi ili skladištu i njegovim pratećim objektima (preuzeto iz reference [12]).

Neovlašteno premještanje. Krađa ili drugo nezakonito uzimanje radioaktivnih izvora (prilagođeno iz reference [19]).

Procjena ugroženosti. Proces kojim se procjenjuju i dokumentuju karakteristike i efikasnost ukupnog sistema bezbjednosti u određenom objektu.