**1302.**

Na osnovu člana 163 stav 6 Zakona o zaštiti od jonizujućih zračenja, radijacionoj i nuklearnoj sigurnosti i bezbjednosti („Službeni list CG“, broj 49/24), uz saglasnost Ministarstva unutrašnjih poslova, Ministarstvo ekologije, održivog razvoja i razvoja sjevera donijelo je

# PRAVILNIK
# O NAČINU VRŠENJA NADZORA, DETEKCIJE I PROCJENE NEOVLAŠĆENIH ULAZAKA U BEZBJEDNOSNU ZONU

I. OSNOVNE ODREDBE

## Predmet

Član 1

Ovim pravilnikom propisuje se način vršenja nadzora, detekcije i procjene neovlašćenih ulazaka u bezbjednosnu zonu za radioaktivne izvore kategorije 1, 2 i/ili 3.

## Značenje izraza

Član 2

Izrazi upotrijebljeni u ovom pravilniku imaju sljedeća značenja:

1) **perimetar bezbjednosne zone** je spoljašnja granica bezbjednosne zone, određena fizičkim preprekama i/ili tehničkim sredstvima detekcije, koja razdvaja zaštićeni prostor od spoljnog prostora i predstavlja prvi sloj zaštite;

2) **procjena alarma** je postupak utvrđivanja uzroka aktiviranja alarma;

3) **sistem za detekciju upada** jeste skup tehničkih sredstava (senzora, kontrolnih centrala i dr.) namijenjenih za otkrivanje pokušaja neovlašćenog ulaska u bezbjednosnu zonu, koji. obuhvata detektore pokreta ili druge odgovarajuće senzore na barijerama i pristupnim tačkama, povezane na alarmni sistem radi signalizacije upada;

4) **senzori za detekciju upada** – tehnički uređaji namijenjeni otkrivanju neovlašćenog ulaska ili pokušaja ulaska u bezbjednosnu zonu, odnosno narušavanja fizičke barijere, uključujući detektore pokreta, magnetne kontakte, senzore vibracija, lomljenja ili rezanja, kao i druge tehnologije namijenjene detekciji upada;

5) **tamper indikator** je tehničko sredstvo, odnosno uređaj za detekciju manipulacije (pečat, brava sa indikatorskom plombom, senzor otvaranja i dr.) koji omogućava otkrivanje pokušaja neovlašćene manipulacije ili uklanjanja zaštićenog radioaktivnog izvora;

6) **uređaji za digitalno snimanje video-nadzora** su tehnička sredstva namijenjena za snimanje, pohranu i reprodukciju video zapisa sa sistema video-nadzora, koja mogu biti:

- DVR (Digital Video Recorder) - uređaj koji prima video-signal sa analognih kamera, digitalizuje ga i pohranjuje; i
- NVR (Network Video Recorder) - uređaj koji prima digitalni video-signal sa IP kamera putem mreže i pohranjuje ga.

## Plan bezbjednosti i mjere detekcije

Član 3

Mjere nadzora, detekcije i procjene neovlašćenih ulazaka u bezbjednosnu zonu integrišu se u plan bezbjednosti objekta u kojem se nalaze radioaktivni izvori kategorije 1, 2 i/ili 3.

Planom bezbjednosti se utvrđuju uloge i odgovornosti osoblja u vezi sa kontinuiranim nadzorom bezbjednosne zone, praćenjem i procjenom alarma, kao i postupci za blagovremeno reagovanje na svaki neovlašćeni ulazak.

Mjere nadzora i detekcije organizuju se na način da obezbijede efikasno i pravovremeno otkrivanje neovlašćenog pristupa, uz primjenu principa gradiranog pristupa i dubinske odbrane.

## II. NADZOR I DETEKCIJA NEOVLAŠĆENOG ULASKA

### Kontinuirani nadzor i otkrivanje ulazaka

Član 4

Neprekidni, dvadeset četvoročasovni nadzor bezbjednosne zone radi detekcije svih neovlašćenih ulazaka ili pokušaja ulazaka ostvaruju se primjenom jednog ili više sljedećih sistema i mjera:

1) sistema za detekciju upada povezanog sa alarmnim sistemom;
2) elektronskog sistema za alarmiranje (alarmni uređaji);
3) sistema video-nadzora sa odgovarajućim osvjetljenjem;
4) neposrednog vizuelnog nadzora unutar i oko bezbjednosne zone.

Izbor i kombinacija mjera detekcije iz stava 1 ovog člana vrši se u skladu sa propisom kojim se uređuju bezbjednosni nivoi za radioaktivne izvore kategorije 1, 2 i/ili 3 i njihovi ciljevi, mjere za postizanje bezbjednosnih ciljeva i vrste bezbjednosnih zona, kako bi svako neovlašćeno prisustvo u bezbjednosnoj zoni bilo otkriveno odmah po nastanku.

Uspostavljeni sistem nadzora treba da omogući pravovremeno otkrivanje i signalizaciju svakog pokušaja neovlašćenog ulaska, bez obzira na doba dana, okolnosti ili mjesto nastanka ulaska.

### Sistem za detekciju upada i alarmiranje

Član 5

Tehnički sistem za detekciju upada postavlja se na način da pokriva sve relevantne prilaze i ulazne tačke bezbjednosne zone (kapije, vrata, prozore, ventilacione otvore, ograde i dr.).

Sistem za detekciju upada uključuje odgovarajuće senzore (detektore pokreta, kontakte na vratima, odnosno prozorima, senzore vibracije ili lomljenja stakla, i dr.)) koji obezbjeđuju trenutno otkrivanje pokušaja neovlašćenog prolaza kroz fizičke barijere ili perimetar zone.

Detektori treba da budu instalirani u skladu sa uputstvima proizvođača i tehničkim zahtjevima iz Priloga 1 koji čini sastavni dio ovog pravilnika, tako da se minimiziraju mrtvi uglovi i lažni alarmi usljed uticaja okoline.

Elektronski alarmni sistem povezuje se sa sistemom za detekciju upada tako da svaki signal detekcije odmah aktivira alarm.

Alarmni signal se prosljeđuje u realnom vremenu centralnom mjestu za nadzor (kontrolnoj sobi) u objektu i prate ga obučena lica nosioca rješenja o registraciji i/ili licenci.

Alarmni sistem, po potrebi, šalje alarm ili obavještenje i službi fizičkog obezbjeđenja ili organu državne uprave nadležnost za unutrašnje poslove (u daljem tekstu: snage odgovora), radi hitnog reagovanja.

Alarmni panel i komunikacioni linkovi sistema za detekciju treba da budu zaštićeni od neovlašćene manipulacije i opremljeni senzorskim nadzorom integriteta (npr. detekcija otvaranja kućišta, prekida veze i dr.).

Alarmni uređaji (vizuelni i zvučni) postavljaju se na način da budu jasno uočljivi odgovornom osoblju, uz mogućnost lokalne zvučne signalizacije radi odvraćanja izvršioca.

Primjena sistema za detekciju upada se gradira prema kategoriji radioaktivnih izvora, tako da se za kategorije 1 i 2 primjenjuju stalno aktivni sistemi povezani sa centralnim nadzornim mjestom, a za kategoriju 3 mogu se koristiti sistemi povremenog nadzora ili druge odgovarajuće mjere detekcije, u skladu sa procjenom prijetnje.

**Video-nadzor**

Član 6

Sistem video-nadzora projektuje se i instalira na način da omogući stalno pokrivanje kritičnih zona i tačaka pristupa u bezbjednosnu zonu.

Kamere treba da obezbjeđuju jasan prikaz područja od interesa, uključujući prilazne puteve, ulaze u objekte gdje se nalaze radioaktivni izvori, kao i samu unutrašnju bezbjednosnu zonu u kojoj se izvori čuvaju ili koriste.

Kamere sa mogućnošću snimanja u uslovima smanjene osvijetljenosti (noćne kamere/infracrvene) ili obezbjeđivanje odgovarajućeg osvjetljenja treba da se koriste kako bi nadzor bio efikasan u noćnim uslovima.

Snimci video-nadzora treba da se čuvaju određeno vrijeme, u skladu sa bezbjednosnim planom i propisima kojima se uređuje zaštita lica i imovine (najmanje 30 dana), radi mogućeg naknadnog pregleda incidenata.

Uređaji za snimanje treba da budu zaštićeni od neovlašćenog pristupa i povezani na rezervno napajanje.

Ako se sistem video-nadzora koristi kao primarno sredstvo detekcije ulazaka, treba da bude obezbijeđeno kontinuirano praćenje kamera od strane dežurnog osoblja.

Video-nadzor treba da se koristi u kombinaciji sa elektronskim senzorima za detekciju upada radi pravovremene detekcije i smanjivanja rizika propuštanja.

**Neposredni vizuelni nadzor**

Član 7

Neovlašćeni ulazak u bezbjednosnu zonu može da se otkrije i neposrednim vizuelnim nadzorom od strane ovlašćenog osoblja, kao dopunska ili alternativna mjera tehničkim sistemima.

Nadzor iz stava 1 ovog člana obezbjeđuje se fizičkim prisustvom jednog ili više lica koja vrše poslove zaštite na lokaciji ili redovnim obilascima (patrole) oko i unutar bezbjednosne zone, u skladu sa procjenom rizika.

Režim patroliranja (ruta, učestalost obilazaka) prilagođava se veličini i konfiguraciji objekta na način da se onemogući neopaženi pristup izvršioca.

Van radnog vremena uspostavlja se dežurstvo ili druga forma fizičkog nadzora objekta.

Ovlašćeno osoblje koje vrši vizuelni nadzor treba da bude opremljeno pouzdanim sredstvom komunikacije (radio-veza, mobilni telefon i sl.) kako bi moglo odmah prijaviti uočeni incident ili alarm nadležnim snagama odgovora.

Radi međusobne podrške i osmatranja većeg područja, mogu da se angažuju lica koja vrše poslove zaštite istovremeno, a naročito kod šire kontrolisane zone ili tokom nadzora mobilnih izvora na terenu.

Sva zapažanja i sumnjivi događaji tokom patrola evidentiraju se u dnevnik obilazaka.

Vizuelni nadzor od strane osoblja kombinovan je, kada je to moguće, sa tehničkim sistemima (alarmima, senzorima, kamerama) radi veće pouzdanost detekcije (princip dubinske odbrane).

U bezbjednosnim zonama koje se formiraju radi rada na terenu sa mobilnim izvorima treba da se vrši neposredni vizuelni nadzor.

## III. DETEKCIJA NEOVLAŠĆENOG PREMJEŠTANJA ILI UKLANJANJA RADIOAKTIVNOG IZVORA

**Detekcija neovlašćenog premještanja ili uklanjanja**

Član 8

Mjere za otkrivanje pokušaja neovlašćenog premještanja ili uklanjanja radioaktivnog izvora iz bezbjednosne zone obuhvataju:

1) primjenu mehaničkih, elektronskih ili hemijskih indikatora manipulacije na posudama, uređajima ili prostorijama u kojima se nalazi radioaktivni izvor (pečati ili plombe na vratima, sefovima i transportnim kontejnerima, senzori otvaranja, indikatorske brave i sl);

2) redovne fizičke provjere prisustva radioaktivnih izvora na lokaciji, uključujući vizuelni pregled sigurnosnih plombi, odnosno sefova i provjeru inventara izvora;

3) korišćenje mjernih instrumenata (prenosivih detektora zračenja ili dozimetara ili dr.) ili druge dostupne indikatore za utvrđivanje prisustva radioaktivnog materijala na lokaciji.

**Provjere prisustva izvora**

Član 9

Provjere prisustva izvora na lokaciji i integriteta (neoštećenosti i nekompromitovanosti) tamper indikatora vrše se učestalo, u zavisnosti od bezbjednosnog nivoa tog izvora, a najmanje jednom:

1) dnevno, za izvore bezbjednosnog nivoa A (kategorija 1);

2) sedmično, za bezbjednosni nivo B (kategorija 2);

3) mjesečno, za bezbjednosni nivo C (kategorija 3).

O rezultatima provjere iz stava 1 ovog člana vodi se evidencija.

Ako se prilikom provjere uoči da radioaktivni izvor nije na predviđenoj lokaciji ili da je došlo do narušavanja, odnosno otvaranja zaštitnih barijera i indikatora (prekinut pečat, oštećena brava, neobjašnjivo odsustvo signala senzora, neuobičajeno očitanje zračenja), odgovorno lice procjenjuje prijetnju i obavještava nadležne organe, u skladu sa procedurama odgovora.

IV. PROCJENA ALARMA NEOVLAŠĆENOG ULASKA

**Neposredna procjena alarma**

Član 10

Svaki alarm ili indikacija potencijalnog neovlašćenog ulaska u bezbjednosnu zonu treba da bude procijenjen odmah po detekciji.

Ovlašćeno osoblje, čim primi alarm sa sistema za detekciju upada ili sa video-nadzora, preduzima radnje za utvrđivanje uzroka alarma, bez odlaganja, u roku od nekoliko sekundi do najviše par minuta u skladu sa uspostavljenim procedurama.

Procjena iz stava 1 ovog člana može da se izvrši daljinski, putem pregledanja video kamera koje pokrivaju zonu i/ili upotrebom drugog senzorskog sistema za verifikaciju.

Ako procjena iz stava 3 ovog člana nije moguća ili ne daje pouzdane informacije o uzroku alarma, ovlašćeno osoblje neposredno odlazi na lice mjesta (unutar ili oko bezbjednosne zone) radi utvrđivanja okolnosti.

Prilikom procjene, svaka alarmna situacija se tretira kao stvarna prijetnja dok se ne dokaže suprotno (princip “lažni alarm se smatra stvarnim dok se ne verifikuje”).

Prioritet osoblja je da ostane bezbjedno i, u slučaju potvrđene neovlašćene aktivnostin utvrdi neovlašćena aktivnost ili ozbiljna sumnja na takvu aktivnost, ovlašćeno osoblje treba da odmah obavijesti snage odgovora, u skladu sa planom bezbjednosti.

Procjena iz stava 1 ovog člana uključuje i klasifikaciju događaja (lažni alarm, slučajni ulazak ovlašćenog lica, pokušaj provale i sl.), koja se evidentira u bezbjednosnom dnevniku zajedno sa vremenom nastanka alarma i vremenom završetka procjene.

**Neprekidna komunikacija tokom događaja**

Član 11

Stalna komunikacija između osoblja koje vrši procjenu na licu mjesta i nadležnih snaga odgovora tokom trajanja bezbjednosnog događaja obezbjeđuje se u cilju koordinisanog i bezbjednog odgovora i prilagođavanja mjera reagovanja u realnom vremenu.

Sve relevantne informacije o incidentu (lokacija, broj i opis izvršioca, preduzete radnje i dr.) prenose se odmah nadležnom organu unutrašnjih poslova i/ili drugim odgovorim službama, u skladu sa planom odgovora na bezbjednosne događaje.

## V. TEHNIČKI USLOVI I ODRŽAVANJE SISTEMA

### Pouzdanost sistema i rezervno napajanje

Član 12

Svi elementi sistema za nadzor, detekciju i alarmiranje projektuju se i koriste na način koji obezbjeđuje visok stepen pouzdanosti i raspoloživosti.

Sistem treba da ima otpornost na pojave lažnih alarma i mehanizme za automatsku kontrolu ispravnosti.

Radi obezbjeđenja neprekidnog rada, uspostavlja se rezervno napajanje za ključnu opremu fizičke zaštite.

Centralna alarmna stanica, kontrolne table alarmnog sistema, komunikaciona oprema i kritične kamere i senzori priključuju se na neprekidno napajanje (UPS) i/ili autonomni izvor električne energije (generator) koji se automatski aktivira u slučaju pada primarnog napona.

Baterijske rezerve napajanja dimenzioniraju se tako da mogu održavati funkcionisanje sistema dovoljan vremenski period (nekoliko sati) do uspostavljanja glavnog napajanja ili aktiviranja generatora.

Sistem za detekciju upada i alarmiranje treba da posjeduje funkciju nadzora vlastitog stanja i komunikacije, kao i da generiše signal upozorenja u slučaju kvara, isključenja ili gubitka napajanja kritičnog dijela sistema.

U smislu stava 6 ovog člana, prekid komunikacione linije između senzora i centrale ili nestanak napajanja senzora tretira se kao stanje koje zahtijeva provjeru.

### Održavanje i testiranje sistema

Član 13

Radi održavanja sistema fizičke zaštite uspostavlja se program, koji obuhvata redovne provjere, ispitivanja i servisiranje opreme za nadzor, detekciju i alarmiranje.

Oprema iz stava 1 ovog člana se održava u skladu sa preporukama proizvođača i dobrim inženjerskim praksama, kako bi se očuvao zahtijevani nivo performansi.

Periodični funkcionalni testovi sistema za detekciju upada i alarmnog sistema (provjera ispravnosti senzora, alarmnih sirena, komunikacionih kanala) vrše se u unaprijed definisanim intervalima u planu bezbjednosti, a najmanje jednom godišnje.

Testiranje iz stava 3 ovog člana vrše stručna i ovlašćena lica, što se dokumentuje, a uočeni nedostaci ili degradacija performansi sistema otklanjaju se bez odlaganja.

Svaka izmjena ili servis na opremi evidentira se, a posebno kritične komponente (detektori, kamere, elektronske brave i sl.) podliježu verifikacionom testu nakon intervencije.

Preventivno održavanje (zamjena baterija, test generatora, kalibracija senzora i sl.) planira se u rasporedu, kako bi se smanjila mogućnost otkaza u radu sistema.

Evidencija svih aktivnosti održavanja vodi se i čuva u skladu sa internim procedurama i zahtjevima nadzornog organa.

Tehnički zahtjevi za opremu i sistemi za nadzor, detekciju i alarmiranje dati su u Prilogu 1.

VI. ZAVRŠNA ODREDBA

**Stupanje na snagu**

Član 14

Ovaj pravilnik stupa na snagu osmog dana od dana objavljivanja u „Službenom listu Crne Gore”, a primjenjivaće se od 1. jula 2027. godine.

Broj: 0412-322/26-415/3
Podgorica, 14. maja 2026. godine

Ministar,
**Damjan Ćulafić**, s.r.

PRILOG 1

# TEHNIČKI ZAHTJEVI ZA OPREMU SISTEMA NADZORA, DETEKCIJE I ALARMA

1. **Sistem za detekciju upada**: Senzori za detekciju upada (detektori pokreta, magnetni kontakti, mikro-talasi, infracrveni detektori, kablovi za detekciju vibracija, itd.) moraju imati odgovarajuću osjetljivost i domet kako bi pokrili predviđenu površinu ili barijeru. Senzori se postavljaju u skladu s procjenom rizika – na obodu kontrolisane zone (ograde, zidovi), na svim ulazima u zaštićenu zonu (vrata, prozori) i oko/na samim skladištima ili uređajima sa izvorima (unutrašnja zona). Detektori treba da obezbijede otkrivanje osobe normalnog rasta pri pokušaju prolaska kroz zaštićeni sektor, sa vjerovatnoćom detekcije od najmanje 90% (uz odgovarajuće podešavanje kako bi se minimizirali lažni alarmi zbog životinja, vremenskih prilika i sl.). Svaki detektor integrisan je u sistem tako da njegov alarm prenosi informaciju o lokaciji (zoni) aktivacije, omogućavajući osoblju lakšu procjenu događaja. Detektori i njihove linije za komunikaciju moraju imati **anti-tampering** zaštitu (npr. zaštićeno ožičenje, alarm pri otvaranju kućišta ili gubitku signala).

2. **Alarmni sistem**: Centralna kontrolna jedinica alarmnog sistema mora biti smještena u bezbjednoj prostoriji (kontrolna soba) sa ograničenim pristupom. Alarmni sistem treba da ima mogućnost lokalne aktivacije zvučnih/svjetlosnih signala i istovremeno tihu uzbunu udaljenim snagama odgovora putem telefonske linije, radio veze ili GSM mreže. Sirene treba da budu dovoljno glasne (npr. >100 dB na 1 m) i postavljene na otvorenom i/ili unutar objekta, tako da ih mogu čuti dežurno osoblje i eventualno odvratiti uljezi. Sistem mora imati rezervno napajanje koje omogućava rad najmanje 4 sata bez mrežnog napajanja. Takođe, poželjno je da alarmni sistem ima **dvojnu komunikaciju** za prenos alarma (npr. fiksna telefonska linija i mobilna mreža), radi veće otpornosti na sabotažu komunikacija.

3. **Video-nadzorna oprema**: Kamere koje se koriste u svrhe bezbjednosnog nadzora treba da budu razlučivosti najmanje 1080p (Full HD) ili ekvivalentno, kako bi se omogućila identifikacija lica na kontrolnim tačkama ulaska. Za spoljašnji nadzor preporučuju se kamere otporne na vremenske uslove (IP65/IP66 kućišta) i vandalizam (IK10 standard), opremljene infracrvenim osvjetljenjem za noćni rad ili uz postavljeno pomoćno osvjetljenje. Raspored kamera određuje se tako da kritične zone budu pokrivene iz više uglova gdje je to moguće, čime se izbjegavaju mrtvi uglovi i povećava vjerovatnoća detekcije. Sistemi za snimanje (DVR/NVR) konfigurišu se na način da automatski čuvaju podatke najmanje 30 dana unazad, sa mehanizmom za pravovremeno prepisivanje najstarijih snimaka kako disk ne bi ostao bez prostora. Pristup uživo slikama i snimcima ograničava se na ovlašćeno osoblje, a uređaji za čuvanje snimaka smještaju se u zaključan orman ili prostoriju radi zaštite od sabotaže.

4. **Tamper indikatori i pečati**: Sva mehanička i elektronska sredstva za indikaciju neovlašćenog otvaranja ili pomjeranja moraju biti jasno označena i evidentirana. Pečati i plombe postavljaju se na vrata skladišta, kontejnere sa izvorima, sefove i druge kritične barijere, tako da svaki pokušaj uklanjanja pečata ostavlja vidljiv trag (npr. neponovljivo numerisane plombe koje se uništavaju prilikom otvaranja). Elektronski tamper senzori (npr. akcelerometri na kontejneru, prekidači na vratima) povezuju se na alarmni sistem ili daju lokalni signal koji se kontroliše pri obilascima. Izbor tipa tamper indikatora vrši se u skladu sa okruženjem i vrstom opreme – npr. za transportne kontejnere koristiti robuste mehaničke plombe otporne na atmosferske uticaje, dok se za stacionarne sefove mogu primijeniti elektronski senzori. Periodične provjere integriteta tamper indikatora (vizuelno ili elektronski očitavanjem) moraju biti dio rutinske kontrole (kako je propisano članom 8 ovog pravilnika).

5. **Oprema za komunikaciju**: Za potrebe bezbjednosnog nadzora i odgovora, obezbjeđuju se pouzdana komunikaciona sredstva. Dežurno osoblje mora imati mogućnost brzog obavještavanja drugih članova obezbjeđenja i nadležnih organa – preporučuje se korišćenje radio-uredjaja (stanica) sa posebnom frekvencijom za objekat ili sigurnih mobilnih telefona sa definisanim brojevima za hitne pozive. Komunikaciona oprema se redovno testira (dnevno ili sedmično) kako bi se osigurala ispravnost u slučaju incidenta.

6. **Integracija sistema**: Tehnička sredstva za detekciju, video-nadzor i alarmiranje treba međusobno integrisati u jedinstven sistem gdje god je to moguće. Integracija omogućava da, na primjer, aktiviranje senzora automatski pozicionira odgovarajuću kameru (PTZ funkcija) ka zoni alarma i prikaže snimak u kontrolnoj sobi, što olakšava procjenu. Takođe, integrisani sistem može objediniti konzolu za praćenje svih alarmnih stanja (fizička bezbjednost, protivpožarni alarmi, sl.), čime se ubrzava reakcija operatera. Pri integraciji treba voditi računa o cyber bezbjednosti digitalnih komponenti (zaštita lozinkom, kontrola pristupa mreži, redovni softverski update-i), u skladu sa relevantnim standardima i smjernicama.

**Napomena**: Zahtjevi u ovom prilogu zasnivaju se na preporukama IAEA za fizičku zaštitu radioaktivnih izvora (NSS 11 i NSS 43-T), prilagođenim za potrebe ovog pravilnika. Sva oprema treba da ispunjava minimalne standarde kvaliteta i bezbjednosti, a njena specifikacija i izbor mogu biti predmet provjere od strane nadležnog organa prilikom odobravanja plana fizičke zaštite ili inspekcijskog nadzora.