PAŃSTWOWA
AGENCJA
ATOMISTYKI

PROJEKT

Zabezpieczenie Źródeł Promieniotwórczych

Zalecenia organizacyjno-techniczne Prezesa Państwowej Agencji Atomistyki

Warszawa 2017

Państwowa Agencja Atomistyki

ul. Krucza 36

00-522 Warszawa

SPIS TREŚCI

ABSTRAKT 5
1. WSTĘP 6
1.1 Informacje wstępne 6
1.2 Cel 8
1.3 Zakres 8
1.4 Definicje 8
2. FUNKCJE ZABEZPIECZENIA 9
3. POZIOMY ZABEZPIECZENIA 10
4. KATEGORYZACJA ŹRÓDEŁ PROMIENIOTWÓRCZYCH 11
5. USTALANIE POZIOMÓW ZABEZPIECZENIA 13
6. PROJEKTOWANIE SYSTEMU ZABEZPIECZENIA 15
6.1 Środki zabezpieczenia dla poziomu zabezpieczenia A 17
6.2 Środki zabezpieczenia dla poziomu zabezpieczenia B 21
6.3 Środki zabezpieczenia dla poziomu zabezpieczenia C 25

ZAŁĄCZNIK I:
GRANICZNE WARTOŚCI AKTYWNOŚCI IZOTOPÓW PROMIENIOTWÓRCZYCH STANOWIĄCE KRYTERIUM KATEGORYZACJI ŹRODEŁ PROMIENIOTWÓRCZYCH

ZAŁĄCZNIK II:
OPIS ŚRODKÓW ORGANIZACYJNO – TECHNICZNYCH ZABEZPIECZENIA ŹRÓDEŁ PROMIENIOTWÓRCZYCH

ZAŁĄCZNIK III:
PRZYKŁADOWA ZAWARTOŚĆ PLANU ZABEZPIECZENIA

Niniejszy dokument został opracowany w Państwowej Agencji Atomistyki na podstawie i z wykorzystaniem następujących materiałów:

1 Security of Radioactive Sources. Implementing Guide. IAEA Nuclear Security Series No. 11, Vienna 2009
2 Security of radioactive sources. Interim guidance for comment, IAEA-TECDOC-1355, Vienna June 2003
3 Code of Conduct on the Safety and Security of Radioactive Sources, IAEA/CODEOC/2004, Vienna 2004
4 Categorization of Radioactive Sources, IAEA Safety Standards Series No. RS-G-1.9, Vienna 2005
5 Dyrektywy Rady 2013/59/Euratom z dnia 5 grudnia 2013 r. ustanawiającej podstawowe normy bezpieczeństwa w celu ochrony przed zagrożeniami wynikającymi z narażenia na działanie promieniowania jonizującego oraz uchylającej dyrektywy 89/618/Euratom, 90/641/Euratom, 96/29/Euratom, 97/43/Euratom i 2003/122/Euratom

ABSTRAKT

Zgodnie z art. 110 pkt 3 ustawy z dnia 29 listopada 2000 r. – Prawo atomowe (Dz.U. z 2017 poz. 576 do zakresu działania Prezesa Państwowej Agencji Atomistyki (PAA) należy wykonywanie zadań związanych z zapewnieniem bezpieczeństwa jądrowego i ochrony radiologicznej kraju, a w szczególności wydawanie zaleceń technicznych i organizacyjnych w sprawach bezpieczeństwa jądrowego i ochrony radiologicznej. Zalecenia Prezesa PAA nie należą do katalogu źródeł powszechnie obowiązującego prawa w Polsce, dlatego też nie mogą przyznawać uprawnień ani nałożyć obowiązków jednostkom organizacyjnym, czy też osobom fizycznym.

Niniejszy dokument ma na celu wskazanie podejścia dozorowego PAA do kwestii zapewnienia źródłom promieniotwórczym (w dalszej części niniejszych zaleceń użyto zamiennie określenia źródło lub źródło promieniotwórcze) odpowiedniego poziomu ochrony fizycznej skorelowanego z zagrożeniem stwarzanym przez te źródła w przypadku działania szkodzącego skierowanego przeciwko nim.

Należy podkreślić, że bezpieczeństwo źródeł promieniotwórczych jest pojęciem złożonym obejmującym zarówno bezpieczne postępowanie z tymi źródłami, zgodnie z odpowiednimi przepisami (z uwzględnieniem zasad ochrony radiologicznej), w celach do jakich te źródła zostały przewidziane, jak również ochronę fizyczną tych źródeł.

Ze względu na fakt używania w polskich przepisach dotyczących bezpieczeństwa jądrowego i ochrony radiologicznej terminu ochrona fizyczna w powiązaniu z materiałami i obiektami jądrowymi w dalszej części niniejszych zaleceń stosuje się termin „zabezpieczenie" w odniesieniu do źródeł promieniotwórczych w znaczeniu zabezpieczenia fizycznego (ochrony fizycznej).

W niektórych przypadkach w niniejszym dokumencie zdecydowano się użyć terminu „bezpieczeństwo" (np. stopniowe podejście do bezpieczeństwa) w odniesieniu do źródeł, ale zawsze w znaczeniu tej części bezpieczeństwa, która związana jest z zabezpieczeniem.

Powyższa terminologia jest zgodna z określeniami zastosowanymi w opracowywanym obecnie projekcie ustawy nowelizującej ustawę Prawo atomowe.

Zalecenia niniejsze uzupełniają wymagania prawne w dziedzinie bezpieczeństwa jądrowego i ochrony radiologicznej związane z postępowaniem ze źródłami promieniotwórczymi i w żadnym miejscu nie stoją w sprzeczności z tymi wymaganiami.

Zgodnie z art. 7 ust.1 ustawy Prawo atomowe za przestrzeganie wymagań bezpieczeństwa jądrowego i ochrony radiologicznej odpowiada kierownik jednostki organizacyjnej wykonującej działalność związaną z narażeniem.

Zgodnie z Art. 43 ust. 3. ustawy Prawo atomowe kierownik jednostki organizacyjnej wykonującej działalność związaną ze źródłami promieniotwórczymi ma obowiązek zabezpieczyć je przed uszkodzeniem, kradzieżą lub dostaniem się w ręce osób nieuprawnionych.

Kierownik jednostki organizacyjnej może wyznaczać lub zlecać osobom trzecim przeprowadzanie działań związanych z zabezpieczeniem źródeł, jednak nie zmienia to faktu, że to kierownik tej jednostki organizacyjnej ponosi odpowiedzialność za zgodność z prawem i skuteczność tych działań.

Niniejsze zalecenia mają na celu ułatwienie kierownikowi jednostki organizacyjnej właściwe wywiązanie się z powyższego obowiązku.

1. WSTĘP

1.1 Informacje wstępne

Odpowiedni poziom zabezpieczeń źródeł promieniotwórczych uzyskuje się poprzez stosowanie działań organizacyjnych i technicznych.

W celu właściwego zabezpieczenia źródeł promieniotwórczych Prezes Państwowej Agencji Atomistyki zaleca kierownikom jednostek organizacyjnych wdrożenie opisanych w niniejszym dokumencie przedsięwzięć (działań) organizacyjnych i technicznych.

Do **przedsięwzięć organizacyjnych** służących zabezpieczeniu źródeł promieniotwórczych zalicza się w szczególności:

1) określenie ograniczeń i systemu kontroli dostępu do obszaru, obiektu lub innych miejsc, w których znajdują się źródła promieniotwórcze;

2) określenie sposobu:

a) zabezpieczenia źródeł promieniotwórczych w czasie ich wytwarzania, przetwarzania, przechowywania, stosowania i obrotu nimi oraz składowania,

b) rozmieszczenia środków i urządzeń zabezpieczających, sposobu ich funkcjonowania i współdziałania oraz sposobu rozmieszczenia służby zabezpieczającej, tam gdzie jest ona wymagana,

c) postępowania na wypadek zagrożenia lub zdarzenia radiacyjnego. Sposób postępowania wynika z zakładowego planu postępowania awaryjnego opracowanego zgodnie z rozporządzeniem Rady Ministrów z dnia 18 stycznia 2005 r. w sprawie planów postępowania awaryjnego w przypadku zdarzeń radiacyjnych,

d) postępowania w przypadku zagrożenia aktami kradzieży, terroru, dywersji lub sabotażu albo ich wystąpienia,

e) postępowania w przypadku prób wejścia lub przebywania osób nieupoważnionych na obszarach, w obiektach lub w innych miejscach zabezpieczanych.

Do **przedsięwzięć technicznych** służących zabezpieczeniu źródeł promieniotwórczych zalicza się w szczególności stosowanie:

1) środków zabezpieczających obszary, obiekty lub inne miejsca, w których znajdują się źródła promieniotwórcze, przed dostępem osób nieupoważnionych, a w szczególności środków mechanicznych, w tym ogrodzeń, ścian, stropów, drzwi, bram, zabezpieczeń otworów okiennych, dachowych i wentylacyjnych, atestowanych szaf pancernych, kaset stalowych, specjalnych zamków i kłódek;

2) systemów alarmowych sygnalizujących zagrożenie oraz systemów służących do obserwacji i rejestracji, a także łączności.

Pod pojęciem **działań organizacyjnych** służących zabezpieczeniu źródeł promieniotwórczych rozumie się także promowanie przez kierownika jednostki organizacyjnej kultury bezpieczeństwa (w części dotyczącej zabezpieczenia źródeł promieniowania jonizującego) i ustanowienie systemu zarządzania zabezpieczeniami zapewniającego, że:

- ustanowiony zostanie wysoki priorytet bezpieczeństwa;
- problemy bezpieczeństwa są niezwłocznie identyfikowane i korygowane w sposób współmierny do ich wagi;
- obowiązki każdej osoby związane z bezpieczeństwem są jasno określone i każda osoba jest odpowiednio przeszkolona, wykwalifikowana i uznana za wiarygodną;
- określono wyraźne uprawnienia do podejmowania decyzji dotyczących bezpieczeństwa;

— wprowadzono ustalenia organizacyjne i linie komunikacji, które gwarantują odpowiedni przepływ informacji dotyczących bezpieczeństwa w ramach całej jednostki organizacyjnej;
— dane zawierające informacje niejawne są określone i chronione zgodnie z ustawą z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych[1];
— źródła promieniotwórcze są zarządzane zgodnie z Planem zabezpieczenia (patrz definicje).

Kultura bezpieczeństwa może być wzmocniona różnymi środkami, na przykład:

— przypisywaniem odpowiedzialności za bezpieczeństwo źródeł promieniotwórczych doświadczonym pracownikom, zapewniając przy tym, że są oni świadomi tego, iż bezpieczeństwo to wspólny obowiązek;
— dokumentowaniem prawnie regulowanych obowiązków związanych z bezpieczeństwem, nakładanych na kierownika jednostki organizacyjnej i skupienie na tym uwagi odpowiednich osób zarządzających oraz pracowników i wykonawców;
— uświadamianiem o zagrożeniu, szkoleniem kierowników do spraw bezpieczeństwa, personelu reagowania i pozostałych pracowników z drugorzędnymi obowiązkami w zakresie bezpieczeństwa;
— poruszaniem spraw dotyczących bezpieczeństwa podczas kursów dla pracowników i wykonawców;
— dostarczaniem instrukcji bezpieczeństwa i przeprowadzaniem na bieżąco instruktaży na temat bezpieczeństwa dla pracowników i wykonawców, organizowaniem szkoleń i ocenianiem uzyskanej wiedzy;
— przeprowadzaniem konserwacji i okresowych prób sprawności systemów i urządzeń służących bezpieczeństwu.

Podkreśla się, że elementami kultury bezpieczeństwa są systemy zarządzania, jak również przekonania, nastawienia i zachowania, które dzięki odpowiedniej kombinacji prowadzą do skuteczniejszego zabezpieczenia źródeł promieniotwórczych.

Podstawą kultury bezpieczeństwa jest uznanie – przez wszystkie podmioty biorące udział w procesach związanych ze źródłami promieniotwórczymi oraz organy sprawujące nadzór nad bezpieczeństwem jądrowym i ochroną radiologiczną – że występuje realne zagrożenie i bezpieczeństwo jest istotne.

Do **działań organizacyjnych** służących zabezpieczeniu źródeł promieniotwórczych zalicza się też przygotowanie w jednostce organizacyjnej Planu zabezpieczenia (patrz definicja); przykładową zawartość Planu zabezpieczenia przedstawiono w Załączniku III.

Istotnym elementem **działań technicznych** służących zabezpieczeniu źródeł promieniotwórczych są: identyfikacja i wdrażanie środków zabezpieczających źródła promieniotwórcze. Zalecane do stosowania środki zabezpieczające (środki techniczne) przedstawiono w Załączniku II do niniejszego dokumentu.

W niniejszym dokumencie zastosowano tzw. stopniowe podejście do bezpieczeństwa (w części bezpieczeństwa związanej z zabezpieczeniem), które bierze pod uwagę ocenę zagrożenia, atrakcyjność źródła oraz możliwe konsekwencje wynikające z działania szkodzącego. W zależności od wielkości zagrożenia stwarzanego działaniem szkodzącym, zgodnie ze stopniowym podejściem, określane są niezbędne środki do zabezpieczenia tego źródła. To podejście zapewnia źródłom mogącym teoretycznie powodować największe zagrożenie najwyższy stopień ochrony.

[1] W niniejszym dokumencie użyto także określenia „informacje wrażliwe” w celu zwrócenia uwagi na konieczność chronienia tego rodzaju informacji zgodnie z zasadami obowiązującymi w danej jednostce organizacyjnej.

Wymagany poziom zabezpieczenia uzyskuje się za pomocą połączenia odstraszania, wykrywania, opóźniania, reagowania i zarządzania zabezpieczeniem.

Zastosowane środki organizacyjne i techniczne służące zabezpieczeniu źródeł promieniotwórczych stanowią system zabezpieczenia.

Niniejszy dokument zaleca, aby stopniowe podejście do bezpieczeństwa realizowano poprzez zastosowanie zbioru funkcji zabezpieczeń (punkt 2.) oraz poziomów zabezpieczeń (punkt 3. i 5.) z uwzględnieniem kategoryzacji źródeł (punkt 4.) i poprzez wykorzystanie systemu zabezpieczenia (punkt 6.).

1.2 Cel

Celem niniejszych zaleceń jest dostarczenie osobom odpowiedzialnym za bezpieczeństwo źródeł promieniotwórczych prostych narzędzi do zastosowania właściwych środków zabezpieczenia źródeł promieniotwórczych.

1.3 Zakres

Niniejszy dokument ma zastosowanie do kwestii zabezpieczenia źródeł promieniotwórczych ze szczególnym uwzględnieniem zamkniętych źródeł promieniotwórczych, z wyłączeniem transportu. Jednakże zawarte w nim zalecenia mogą też znaleźć zastosowanie w przypadku zabezpieczenia innych substancji promieniotwórczych z wyjątkiem materiałów jądrowych, w rozumieniu ustawy, przy czym wyłączenie powyższe nie dotyczy źródeł promieniotwórczych zawierających izotop promieniotwórczy Pu-239 (Pluton-239).

Zawarte w dokumencie zalecania mogą być wykorzystane przez podmioty, uczestniczące w procesach związanych ze źródłami promieniotwórczymi, takie jak: projektanci, producenci (zarówno źródeł promieniotwórczych, jak i urządzeń zawierających źródła promieniotwórcze), dostawcy, użytkownicy oraz zarządzający źródłami wycofanymi z eksploatacji.

1.4 Definicje

W rozumieniu niniejszego dokumentu użyte określenia oznaczają:

- **Działanie szkodzące:** działanie dotyczące źródła lub źródeł promieniotwórczych, dokonane umyślnie bez prawnego uzasadnienia lub działanie dotyczące źródła lub źródeł promieniotwórczych dokonane umyślnie, którego celem jest spowodowanie śmierci lub uszkodzenia ciała człowieka lub spowodowanie szkody w mieniu lub środowisku. Określenie to obejmuje także nieuprawnione usunięcie.
- **Kultura bezpieczeństwa:** zespół podstawowych wartości, postaw i zachowań, zarówno grupowych jak i indywidualnych, nadających priorytet zagadnieniom ochrony i bezpieczeństwa przed innymi celami.
- **Nieuprawnione usunięcie:** kradzież lub inne bezprawne przejęcie źródła promieniotwórczego lub źródeł promieniotwórczych.
- **Zabezpieczenie:** zapobieganie działaniom szkodzącym związanym ze źródłami promieniotwórczymi lub obszarami, obiektami bądź innymi miejscami, w których się znajdują, wykrywanie tych działań i reagowanie, czego wynikiem jest ochrona ludności i środowiska przed zagrożeniami wynikającymi z promieniowania jonizującego.
- **Plan zabezpieczenia**: dokument zatwierdzony przez kierownika jednostki organizacyjnej, szczegółowo opisujący system zabezpieczenia źródła/eł.
- **System alarmowy**: grupa urządzeń, tworzących instalację do wykrywania i sygnalizacji zagrożeń związanych z wtargnięciem na obszar lub do obiektu lub innych miejsc, w których znajdują się źródła promieniotwórcze.

Inne określenia użyte w niniejszym dokumencie takie jak na przykład: jednostka organizacyjna, narażenie, ochrona radiologiczna mają znaczenie zdefiniowane w ustawie z 29 listopada 2000 r. Prawo atomowe (Dz. U. z 2014 r. poz. 1512), dalej zwaną ustawą.

2. FUNKCJE ZABEZPIECZENIA

System zabezpieczenia źródła promieniotwórczego przed osobami nieuprawnionymi mającymi zamiar podjęcia działania szkodzącego, powinien zostać opracowany tak, by spełniał podstawowe funkcje zabezpieczenia: odstraszanie, wykrywanie, opóźnianie, reagowanie i zarządzanie zabezpieczeniem.

— ***Odstraszanie***

Celem odstraszania jest zniechęcenie osób nieuprawnionych do podjęcia próby działania szkodzącego. Odstraszanie jest skuteczne, gdy osoba nieuprawniona, która ma zamiar dokonania działania szkodzącego odstępuje od jego wykonania. Skutkiem odstraszania jest przekonanie osoby nieuprawnionej, że działanie szkodzące będzie zbyt trudne do wykonania, odniesienie sukcesu jest zbyt niepewne, a konsekwencje działania szkodzącego dla osoby nieuprawnionej będą zbyt poważne, by uzasadnić podjęcie działania. Środki odstraszające powinny służyć także przekazaniu informacji o obecności środków spełniających inne funkcje zabezpieczenia. Ponieważ skutki środków odstraszających są niemierzalne, opracowanie systemu zabezpieczenia nie powinno bazować wyłącznie na odstraszaniu.

— ***Wykrywanie (wykrycie)***

Wykrywanie, to zaobserwowanie próby wtargnięcia lub rzeczywistego wtargnięcia na teren objęty systemem zabezpieczenia. Wykrywanie realizuje się poprzez: obserwację wzrokową, system alarmowy (obydwa ww. sposoby można nazwać monitoringiem), prowadzenie ewidencji itp. Nie każde jednak wykrycie próby wtargnięcia lub rzeczywistego wtargnięcia oznacza działanie, którego celem jest działanie szkodzące. Wykrycie próby wtargnięcia lub wtargnięcia wymaga weryfikacji polegającej na dokonaniu „oceny wykrycia". Jedyną pewną metodą „oceny wykrycia" jest bezpośrednia obserwacja wykonywana przez człowieka. Dlatego, gdy alarm lub inne wskazanie pośrednie zostanie aktywowane, zawsze istnieje pewien stopień niepewności co do jego przyczyny. Sprawdzenie przyczyny alarmu wymaga od pracowników jednostki organizacyjnej lub zewnętrznej firmy, której zlecono część działań związanych z zabezpieczeniem źródeł promieniotwórczych (dalej nazywanych „personelem reagowania") poczynienia natychmiastowej obserwacji i oceny ewentualnego zagrożenia. Im krótszy czas pomiędzy wykryciem a dokonaniem „oceny wykrycia", tym system zabezpieczenia jest bardziej efektywny.

Należy też zwrócić uwagę na fakt, że wykrywanie może dotyczyć stanu po nieuprawnionym usunięciu lub celowym uszkodzeniu źródła, to znaczy takiego przypadku, kiedy w wyniku prowadzonej inwentaryzacji lub okresowej kontroli (nawet codziennej) w celu sprawdzenia, czy źródła są wciąż na miejscu i nie uległy naruszeniu, wykryty zostanie brak źródła. Stosuje wtedy się określenie „wykrycia utraty". Powyższe jest istotne dla właściwego zrozumienia i zastosowania zaleceń, o których mowa w tabelach 4 – 6 w pozycji „wykrywanie utraty za pomocą weryfikacji".

— ***Opóźnienie***

Celem opóźniania jest zapewnienie personelowi reagowania odpowiedniego czasu na zlokalizowanie zagrożenia i przerwanie działań osoby nieuprawnionej w związku z zamiarem dokonania działania szkodzącego. Opóźnienie zakłóca próbę dokonania działania szkodzącego podjętą przez osobę nieuprawnioną. Opóźnienie realizowane jest przeważnie za pomocą barier lub innych środków fizycznych. Miarą opóźnienia jest czas mierzony od dokonania wykrycia do momentu, w którym osoba nieuprawniona ma nieutrudniony dostęp do źródła promieniotwórczego. Świadomość

osoby nieuprawnionej o barierach opóźniających, może również pełnić funkcję odstraszania.

— ***Reagowanie***
Reagowanie obejmuje czynności podjęte po wykryciu, powstrzymujące przed skutecznym działaniem osoby nieuprawnionej, przeciwdziałające możliwym poważnym skutkom tego działania lub odzyskanie źródła. Reagowanie można podzielić na dwa etapy; w pierwszym główną rolę odgrywa personel reagowania, etap ten kończy się z chwilą uniemożliwienia nieuprawnionego usunięcia źródła promieniotwórczego lub stwierdzenia, że nastąpiło nieuprawnione usunięcie źródła; w drugim etapie, który ma miejsce w przypadku stwierdzenia nieuprawnionego usunięcia źródła, główną rolę odgrywają organy ścigania. Reagowanie może także obejmować zatrzymanie osoby dokonującej próby nieuprawnionego usunięcia lub rzeczywistego usunięcia źródła promieniotwórczego, ale ta część reagowania nie wchodzi w zakres niniejszych zaleceń. Skuteczne reagowanie sprzyja lepszej realizacji funkcji odstraszania.

— ***Zarządzanie zabezpieczeniem***
Zarządzanie zabezpieczeniem obejmuje zapewnianie odpowiednich środków organizacyjnych i technicznych do zabezpieczenia źródeł promieniotwórczych. Termin ten obejmuje również opracowanie procedur właściwego postępowania z informacjami niejawnymi/wrażliwymi i ochrony przed ich bezprawnym ujawnieniem.

3. POZIOMY ZABEZPIECZENIA

Ze względu na zróżnicowane zagrożenie od źródeł promieniotwórczych, jako efekt zainteresowania się nimi osób podejmujących działania szkodzące, należy zastosować właściwy zakres skutecznych środków zabezpieczenia. W celu zapewnienia odpowiedniego zabezpieczenia, bez nakładania nazbyt restrykcyjnych środków, wprowadza się pojęcie poziomów zabezpieczenia A, B oraz C. Poziom zabezpieczenia A oznacza najwyższy stopień zabezpieczenia, a B i C – odpowiednio niższe.

Każdy poziom zabezpieczenia wiąże się z konkretnym celem. Cele te określają ogólny efekt, który system zabezpieczenia powinien zapewnić w ramach danego poziomu:

— **Poziom zabezpieczenia A**: Cel - *zapobieganie* nieuprawnionemu usunięciu źródła.
— **Poziom zabezpieczenia B**: Cel - *zminimalizowanie prawdopodobieństwa* nieuprawnionego usunięcia źródła.
— **Poziom zabezpieczenia C**: Cel - *zmniejszanie prawdopodobieństwa* nieuprawnionego usunięcia źródła.

Aby zapewnić właściwe zabezpieczenie źródeł promieniotwórczych, należy wdrożyć odpowiedni poziom dla każdej funkcji zabezpieczenia: odstraszania, wykrywania, opóźniania, reagowania i zarządzania zabezpieczeniem.

4. KATEGORYZACJA ŹRÓDEŁ PROMIENIOTWÓRCZYCH

Zaleca się zastosowanie pięciu kategorii źródeł promieniotwórczych uwzględniających potencjalne deterministyczne skutki zdrowotne wywoływane przez te źródła w przypadku wykorzystania ich niezgodnego z przeznaczeniem.

Zaleca się przypisanie poszczególnym źródłom promieniotwórczym odpowiedniej kategorii w zależności od urządzenia, w którym te źródła zostały umieszczone - patrz kolumna 2. Tabeli 1.

W szczególnych przypadkach (patrz odnośnik „b" do kolumny 3. w Tabeli 1.) do kategoryzacji źródeł można zastosować wielkość stosunku A/D, gdzie:

- „A" jest aktywnością izotopów promieniotwórczych zawartych w źródłach,
- „D" to taka aktywność izotopów promieniotwórczych zawartych w źródłach, która może spowodować poważne skutki deterministyczne w przypadku utraty kontroli nad tymi źródłami. Wartość D została wyznaczona przy uwzględnieniu scenariuszy obejmujących narażenie zewnętrzne od nieosłoniętego źródła promieniotwórczego i przypadkowe narażenie wewnętrzne w następstwie rozproszenia źródła (np. na skutek pożaru lub eksplozji). Wartości D dla poszczególnych izotopów promieniotwórczych, zostały ujęte w tabeli stanowiącej Załącznik I do niniejszego dokumentu. Warto zauważyć, że wartości „D" (wykorzystane w niniejszym dokumencie) dla poszczególnych izotopów są tożsame z wartościami także oznaczonymi jako „D" w Załączniku III do Dyrektywy Rady 2013/59/Euratom z dnia 5 grudnia 2013 r. ustanawiającej podstawowe normy bezpieczeństwa w celu ochrony przed zagrożeniami wynikającymi z narażenia na działanie promieniowania jonizującego oraz uchylającej dyrektywy 89/618/Euratom, 90/641/Euratom, 96/29/Euratom, 97/43/Euratom i 2003/122/Euratom.
  Wartości „D" określone w Dyrektywie 2013/59/Euratom określają wartości progowe źródeł promieniotwórczych kwalifikowanych jako źródła wysokoaktywne.
  Z kolei wartość P_1 wykorzystana poniżej w Tabeli 1. jest tożsama z wartościami oznaczonymi także jako P_1 zawartymi w załączniku II do ustawy określającymi poziomy progowe aktywności, poniżej których zamknięte źródło promieniotwórcze przestaje być źródłem wysokoaktywnym.

W powyższym, zalecanym systemie kategoryzacji, źródła z kategorii 1. uważa się za najbardziej „niebezpieczne", ponieważ jeśli nie są zarządzane w sposób bezpieczny, stanowią poważne zagrożenie dla zdrowia. Kilkuminutowe narażenie na nieosłonięte źródło kategorii 1. wystarczy, by spowodować zgon. Na końcu systemu kategoryzacji, w kategorii 5., znajdują się źródła najmniej niebezpieczne.

TABELA 1. KATEGORIE ŹRÓDEŁ PROMIENIOTWÓRCZYCH DLA POWSZECHNYCH ZASTOSOWAŃ

Kategoria	Źródło[a]	A/D[b]
1	**2**	**3**
1	Generatory termoelektryczne Urządzenia radiacyjne Urządzenia do telegammaterapii (bomby kobaltowe) Urządzenia do telegammaterapii (noże gamma)	A/D ≥ 1000

2	Aparaty do radiografii przemysłowej (Defektoskopy) Urządzenia do brachyterapii HDR	1000 > A/D ≥ 10
3	Stacjonarne mierniki przemysłowe, które zawierają źródła wysokoaktywne Sondy geofizyczne	10 > A/D > 1
4	Urządzenia do brachyterapii LDR (z wyjątkiem aplikatorów ocznych i źródeł aplikowanych na stałe) Mierniki przemysłowe, które nie wykorzystują źródeł wysokoaktywnych Densytometry izotopowe kości Eliminatory ładunków elektrostatycznych	1 > A/D ≥ 0,01 i A > P_1[c]
5	Aplikatory oczne i źródła aplikowane na stałe Spektrometry izotopowe Detektory wychwytu elektronów Źródła do spektrometrii Mössbauera Źródła kontrolne do pozytonowej tomografii emisyjnej (PET)	0,01 > A/D i A > P_1[c]

[a] Podczas przypisywania źródła do kategorii, wzięto pod uwagę inne czynniki niż A/D.

[b] Kolumnę tą można zastosować do określenia kategorii źródła wyłącznie w przypadku, gdy nie jest znane zastosowanie danego źródła lub zastosowanie to nie jest wyszczególnione w kolumnie drugiej tabeli, gdy źródła mają krótki okres półtrwania, są to źródła otwarte, lub w przypadku dużego nagromadzenia źródeł w jednym miejscu.

[c] Wartości aktywności P_1 podano w Tabeli stanowiącej Załącznik I.

W przypadkach, kiedy nie jest możliwe ustalenie kategorii źródeł w oparciu o kolumnę 2. Tabeli 1., np. gdy źródła promieniotwórcze znajdują się w dużych ilościach blisko siebie, podczas produkcji (w tym samym pomieszczeniu lub budynku) lub podczas przechowywania (na tym samym terenie), należy zsumować aktywności źródeł w celu określenia kategoryzacji dla tego przypadku. W podobnych przypadkach zsumowaną aktywność izotopów promieniotwórczych należy podzielić przez odpowiednią wartość D, a obliczony stosunek A/D należy porównać z wartościami A/D podanymi w Tabeli 1. W ten sposób zbiór źródeł można skategoryzować na podstawie aktywności. Jeśli zgromadzono źródła różnych izotopów promieniotwórczych, należy wykorzystać sumę stosunków A/D do określenia kategorii zgodnie ze wzorem:

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

gdzie:

$A_{i,n}$ = aktywność każdego pojedynczego źródła i izotopu promieniotwórczego n.
D_n = wartość D dla izotopu promieniotwórczego n.

5. USTALANIE POZIOMÓW ZABEZPIECZENIA

Zaleca się, aby źródła kategorii 1. były zabezpieczone środkami spełniającymi cele poziomu zabezpieczeń A; źródła kategorii 2. były zabezpieczone środkami spełniającymi cele poziomu zabezpieczeń B; źródła kategorii 3. były zabezpieczone środkami, które spełniają cele poziomu zabezpieczeń C (patrz Tabela 2.).

Należy pamiętać, że źródła zaliczone do kategorii 4. i 5., mogą wymagać poważniejszych zabezpieczeń, niż by wynikało to z ich aktywności. Powyższe wynika z faktu, że większość źródeł kategorii 1. jest osłonięta lub umieszczona na stałe w urządzeniach; próby usunięcia takich źródeł zajęłyby dużo czasu i mogłyby narazić osoby podejmujące działania szkodzące na duże dawki promieniowania jonizującego. Dlatego takie osoby mogą skupić się na źródłach niższej kategorii, które są łatwiej dostępne, mniej niebezpieczne dla zdrowia, łatwiejsze do transportu i ukrycia (patrz poniżej *Atrakcyjność źródła)*.

TABELA 2. ZALECANE DOMYŚLNE POZIOMY ZABEZPIECZEŃ DLA POWSZECHNIE STOSOWANYCH ŹRÓDEŁ

Kategoria	Źródło	A/D	Poziom zabezpieczenia
1	Generatory termoelektryczne Urządzenia radiacyjne Urządzenia do telegammaterapii (bomby kobaltowe) Urządzenia do telegammaterapii (noże gamma)	$A/D \geq 1000$	A
2	Aparaty do radiografii przemysłowej (Defektoskopy) Urządzenia do brachyterapii HDR	$1000 > A/D \geq 10$	B
3	Stacjonarne mierniki przemysłowe, które zawierają źródła wysokoaktywne (*high activity sealed sources* - HASS) Sondy geofizyczne	$10 > A/D \geq 1$	C
4	Urządzenia do brachyterapii LDR (z wyjątkiem aplikatorów ocznych i źródeł aplikowanych na stałe) Mierniki przemysłowe, które nie wykorzystują źródeł wysokoaktywnych Densytometry izotopowe kości Eliminatory ładunków elektrostatycznych	$1 > A/D \geq 0{,}01$ i $A > P_1$	Zastosowanie rozwiązań odpowiednich do stopnia zagrożenia
5	Aplikatory oczne i źródła aplikowane na stałe Spektrometry izotopowe Detektory wychwytu elektronów Źródła do spektrometrii Mössbauera Źródła kontrolne do pozytonowej tomografii emisyjnej (PET)	$0{,}01 > A/D$ i $A > P_1$	

Ustalając poziom zabezpieczenia dla poszczególnych, indywidualnych przypadków należy wziąć pod uwagę także następujące elementy:

- *Atrakcyjność źródeł*

Oprócz aktywności źródła występują inne czynniki, które mogą sprawić, że niektóre z nich są bardziej atrakcyjne pod względem wykorzystania w celu dokonania działań szkodzących. Czynniki te obejmują:

— postać chemiczną i fizyczną materiału promieniotwórczego występującego w źródle, które sprawiają, że łatwo go rozproszyć;
— rodzaj promieniowania jonizującego. Niektóre izotopy promieniotwórcze (np. emitery promieniowania α) powodują otrzymanie wyższej dawki przy jednostkowym wchłonięciu,
w porównaniu z innymi izotopami. Źródła zawierające te izotopy mogą być atrakcyjniejsze do zastosowania ich w tzw. „brudnej bombie”;
— łatwość zastosowania. Źródła, które są łatwe w użyciu lub łatwo dostępne, mogą być atrakcyjniejsze, gdyż jest mniejsze prawdopodobieństwo otrzymania wysokiej dawki promieniowania i źródła są łatwiejsze w transporcie. Przykładem są źródła znajdujące się w osłonnym urządzeniu przenośnym/osłonnych urządzeniach przenośnych;
— wspólne umieszczenie. Źródła umieszczone razem mogą być atrakcyjne dla osoby podejmującej próbę dokonania działań szkodzących, gdyż skuteczne sforsowanie systemu zabezpieczenia umożliwia usunięcie wystarczającej ich liczby do dokonania działań szkodzących;
— postrzegana wartość ekonomiczna źródła lub urządzenia zawierającego źródła promieniotwórcze.

- *Przechowywanie źródła*

Przechowywane źródła promieniotwórcze należy zabezpieczyć zgodnie ze środkami przedstawionymi w niniejszych zaleceniach i zgodnie z kategoriami oraz poziomami zabezpieczenia, do których przypisano źródła.

- *Podatność i poziom zagrożenia*

Poziom zagrożenia krajowego oraz jego wzrost może wymagać ponownej oceny poziomu zabezpieczenia danego źródła, biorąc pod uwagę wszystkie inne jego cechy (np. atrakcyjność lub podatność na działania szkodzące). Ewentualnie, należy wzmocnić niektóre lub wszystkie środki organizacyjne i techniczne danego poziomu zabezpieczenia.

- *Źródła mobilne, przenośne i w oddalonych lokalizacjach*

Źródła wykorzystywane w terenie (np. w radiografii i geofizyce) są najczęściej umieszczane w urządzeniach specjalnie do tego zaprojektowanych i często są transportowane pomiędzy miejscami zastosowania. Łatwość obchodzenia się z nimi i ich przechowywanie w pojazdach poza zabezpieczonymi obiektami sprawia, że są one atrakcyjnym celem dla osób działających w zamiarze dokonania działań szkodzących.

Biorąc pod uwagę, że środki zabezpieczenia stosowane w przypadku źródeł stacjonarnych mogą być niepraktyczne w przypadku źródeł stosowanych w terenie, aby spełnić cele zabezpieczenia należy zastosować środki alternatywne, równoważne ze środkami stosowanymi do źródeł stacjonarnych.

Źródła, w przypadku których reagowanie jest utrudnione powinny zostać zabezpieczone na wypadek próby dokonania działania szkodzącego, z zastosowaniem wyższych poziomów zabezpieczeń.

6. PROJEKTOWANIE SYSTEMU ZABEZPIECZENIA

Po dokonaniu identyfikacji odpowiedniego poziomu zabezpieczenia, należy przystąpić do projektowania systemu zabezpieczenia, który spełni wymagania danego poziomu.

W procesie projektowania systemu zabezpieczenia należy poświęcić szczególną uwagę zagrożeniom wewnętrznym. Zagrożenia takie mogą powstawać na skutek działań jednej lub więcej osób, które posiadają upoważnienie do dostępu do obszaru, obiektu lub innego miejsca, w którym znajdują się źródła oraz posiadają szczegółową wiedzę na temat wykonywanej działalności ze źródłami lub lokalizacji źródeł. Osoby te mogą być pracownikami (lub wykonawcami z firmy zewnętrznej), które mogą dokonać działania szkodzącego. Ponadto osoby takie, mogą szukać zatrudnienia w danej jednostce w celu przeprowadzenia działania szkodzącego, jak również, mogą pomagać osobom zewnętrznym w usunięciu źródeł lub przeprowadzeniu wrogich działań.

Różnice pomiędzy poziomami zabezpieczenia A, B i C w odniesieniu do celów i funkcji zabezpieczenia zaprezentowano w poniższej Tabeli 3. W tabeli tej zestawiono funkcje zabezpieczenia (wykrywanie, opóźnianie, reagowanie i zarządzanie zabezpieczeniem) oraz wszystkie cele zabezpieczenia i zaznaczono, które z nich powinny być osiągnięte w poszczególnych poziomach zabezpieczenia (A, B i C).

TABELA 3. FUNKCJE I CELE ZABEZPIECZENIA DLA POZIOMÓW ZABEZPIECZENIA A, B i C

Funkcja zabezpieczenia		Cel zabezpieczenia	Poziom Zabezpieczenia			Uwagi
			A ***Cel**: zabezpieczyć przed nieuprawnionym usunięciem*	**B** ***Cel**: zminimalizować prawdopodobieństwo nieuprawnionego usunięcia*	**C** ***Cel**: zmniejszyć prawdopodobieństwo nieuprawnionego usunięcia*	
1.	WYKRYWANIE	natychmiastowe wykrycie **próby nieupoważnionego dostępu** do chronionej lokalizacji źródła, w tym dostępu przez pracownika wewnętrznego	●			
2.		natychmiastowe wykrycie **nieupoważnionego dostępu** do chronionej lokalizacji źródła	●	●		
3.		wykrycie **próby nieuprawnionego usunięcia** źródła		●		W przypadku poziomu A do działań w p.3 i 4 nie może dojść
4.		Wykrycie **nieuprawnionego usunięcia** źródła			●	
5.		natychmiastowa ocena wykrycia (dokonywana zarówno w przypadku wykrycia próby nieupoważnionego dostępu jak	●	●	●	

		i nieupoważnionego dostępu)				
6.		natychmiastowa ocena wykrycia **nieuprawnionego usunięcia** źródła			●	A i B - do działania w p. 6 nie może dojść
7.		natychmiastowa informacja dla personelu reagowania	●	●		
8.		wykrywanie utraty źródła za pomocą weryfikacji	●	●	●	Działanie 8 w przyp. A i B ma miejsce, gdy cele określone dla tych poziomów nie zostaną osiągnięte.
9.	OPÓŹNIANIE	opóźnienie po wykryciu próby usunięcia pozwalające na niedopuszczenie przez personel reagowania do nieuprawnionego usunięcia	●			W przyp. B – nie jest wymagany czas dla personelu reagowania w celu przerwania usunięcia źródła
10.		opóźnienie minimalizujące prawdopodobieństwo nieuprawnionego usunięcia		●		W przyp. A ze względu na osiągnięcie celu zabezpieczenia 9, p. 10 i 11 nie mają zastosowania
11.		opóźnienie zmniejszające prawdopodobieństwo nieuprawnionego usunięcia źródła			●	
12.	REAGOWANIE	natychmiastowa reakcja na potwierdzony alarm za pomocą wystarczających środków w celu uniemożliwienia nieuprawnionego usunięcia	●			
13.		natychmiastowa reakcja na potwierdzony alarm za pomocą wystarczających środków do przerwania nieuprawnionego usunięcia		●		W przyp. A jeśli cel zabezpieczenia 12. został osiągnięty to cel 13 nie ma zastosowania; w przypadku A i B cel 14 nie ma zastosowania.
14.		wprowadzenie działań przewidzianych w zakładowym planie postępowania awaryjnego w przypadku nieuprawnionego usunięcia źródła. Zakładowe plany postępowania awaryjnego opracowywane są zgodnie z rozporządzeniem Rady Ministrów z dnia 18 stycznia 2005 r. w sprawie planów postępowania awaryjnego w przypadku zdarzeń radiacyjnych.			●	

15.	ZARZĄDZANIE ZABEZPIECZENIEM	kontrola dostępu do lokalizacji źródła, która skutecznie ogranicza dostęp osób nieupoważnionych	●	●	●	Punkty 15-20 różnią się szczegółowością działań w zależności od poziomu A, B i C
16.		zapewnienie wiarygodności osób upoważnionych	●	●	●	
17.		określanie i ochrona niejawnych informacji	●	●	●	
18.		opracowanie Planu zabezpieczenia	●	●	●	
19.		zapewnienie zdolności do zarządzania zagrożeniami bezpieczeństwa	●	●	●	
20.		ustanowienie systemu zawiadamiania o zagrożeniach bezpieczeństwa	●	●	●	

Poniżej, w tabelach 4-6 podano zalecane przez Prezesa Państwowej Agencji Atomistyki środki zabezpieczenia jakie powinny zostać zastosowane, aby osiągnąć cele dla poziomów zabezpieczenia A, B i C określonych w punkcie 3. niniejszego dokumentu.

Środki te są omówione szczegółowo poniżej każdej tabeli. Mogą one się różnić w zależności od tego, czy dane źródło jest przetwarzane, wytwarzane, stosowane, czy przechowywane lub czy jest mobilne, czy przenośne. Dodatkowe informacje o niektórych spośród tych środków, znajdują się w Załączniku II.

6.1 Środki zabezpieczenia dla poziomu zabezpieczenia A

- Jak już podano w p. 3 niniejszych zaleceń celem *poziomu* zabezpieczenia A jest **zapobieganie nieuprawnionemu usunięciu** źródła promieniotwórczego. W przypadku **próby nieupoważnionego dostępu** lub zaistnienia **nieupoważnionego dostępu**, wykrywanie i ocena wykrycia muszą nastąpić na tyle wcześnie, aby personel reagowania miał wystarczająco dużo czasu i środków, by przerwać usuwanie źródła osobie działającej w zamiarze dokonania działań szkodzących. Aby osiągnąć ten cel, zaleca się środki zabezpieczenia opisane w Tabeli 4.

TABELA 4. ZALECANE ŚRODKI ZABEZPIECZENIA DLA **POZIOMU ZABEZPIECZENIA A**
(cel: zabezpieczyć przed nieuprawnionym usunięciem)

L.p.	Funkcje zabezpieczenia	Cel zabezpieczenia	Środki zabezpieczenia
1.	Wykrywanie	natychmiastowe wykrywanie próby nieupoważnionego dostępu do chronionej lokalizacji źródła, w tym dostępu przez pracownika wewnętrznego	system alarmowy lub ciągła obserwacja wzrokowa przeprowadzana przez pracowników jednostki organizacyjnej lub firmy wynajętej do zabezpieczenia (firma „ochroniarska" dysponująca personelem reagowania)
2.		natychmiastowe wykrycie **nieupoważnionego** dostępu do chronionej lokalizacji źródła	system alarmowy lub ciągła obserwacja wzrokowa przeprowadzana przez pracowników jednostki organizacyjnej lub firmy „ochroniarskiej"

3.		natychmiastowa ocena wykrycia (dokonywana zarówno w przypadku wykrycia próby nieupoważnionego dostępu jak i nieupoważnionego dostępu)	system alarmowy wyposażony w kamery przekazujące obraz pozwalający na ocenę przyczyny uaktywnienia się systemu alarmowego lub dokonanie tej oceny przez pracowników jednostki organizacyjnej lub firmy „ochroniarskiej”
4.		natychmiastowa informacja dla personelu reagowania	szybkie, pewne i różne środki komunikacji, takie jak telefony stacjonarne, komórkowe, radia
5.		wykrywanie utraty źródła za pomocą weryfikacji	codzienna kontrola fizyczna, urządzenia do zdalnej obserwacji, pomiary
6.	Opóźnianie	opóźnienie po wykryciu pozwalające na niedopuszczenie przez personel reagowania do nieuprawnionego usunięcia	system składający się z co najmniej dwóch warstw barier (np. ścian, krat), które razem zapewniają wystarczające opóźnienie, by umożliwić działanie personelu reagowania
7.	Reagowanie	natychmiastowa reakcja na sprawdzony alarm (potwierdzone wykrycie) za pomocą wystarczających środków w celu uniemożliwienia nieuprawnionego usunięcia	możliwość natychmiastowego reagowania przez odpowiednio przeszkolone osoby dysponujące odpowiednim sprzętem
8.	Zarządzanie zabezpiecze-niem	kontrola dostępu do lokalizacji źródła, która skutecznie ogranicza dostęp osób nieupoważnionych	identyfikacja i weryfikacja osób np. przy pomocy zamka obsługiwanego czytnikiem kart magnetycznych i nr PIN
9.		zapewnienie wiarygodności osób upoważnionych	kontrole przeszłości wszystkich pracowników upoważnionych do samodzielnego dostępu do lokalizacji źródła i informacji wrażliwych
10.		dane zawierające informacje niejawne są określone i chronione zgodnie z ustawą z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych	procedury określające rodzaj informacji i środki ich ochrony przed nieupoważnionym wyjawieniem
11.		opracowanie Planu zabezpieczenia	Plan zabezpieczenia, który spełnia zalecenia organizacyjno-techniczne Prezesa PAA i określa reagowanie w różnych przypadkach (sytuacjach) zagrożenia
12.		zapewnienie zdolności do zarządzania zagrożeniami bezpieczeństwa	procedury odpowiedzi na scenariusze związane z zagrożeniami bezpieczeństwa
13.		ustanowienie systemu zawiadamiania o zagrożeniach bezpieczeństwa	procedury opisane w zakładowym planie postępowania awaryjnego opracowanym zgodnie z Rozporządzeniem Rady Ministrów z dnia 18 stycznia 2005 r. w sprawie planów postępowania awaryjnego w przypadku zdarzeń radiacyjnych

Wykrywanie

Ad. L.p. 1. i 2.

System alarmowy lub ciągła obserwacja wzrokowa wskazują na próbę nieupoważnionego dostępu lub nieupoważniony dostęp do chronionej lokalizacji źródła (być może w celu usunięcia źródła). Należy zwrócić szczególną uwagę na to, by środków wykrywania takich działań nie dało się obejść. W przypadku stosowanych (to znaczy będących w użyciu, w odróżnieniu od przechowywanych) mobilnych źródeł, ciągły nadzór wzrokowy może być jedynym rozsądnym sposobem wykrywania próby nieuprawnionego usunięcia. Należy zwrócić jednak uwagę, że jeśli wybrano obserwację wzrokową jako środek zabezpieczenia, to może ona wymagać realizacji przez co najmniej *dwie* osoby przez cały czas.

Ad. L.p. 3. i 4.

W przypadku stwierdzenia, że nastąpiła próba nieupoważnionego dostępu lub nieupoważniony dostęp, należy natychmiast przekazać taką informację personelowi reagowania.

Ad. L.p. 5.

Codzienna kontrola służy sprawdzeniu czy źródła są wciąż na miejscu, nie uległy naruszeniu i czy są spełnione cele zabezpieczenia określone w pozycji 1 i 2. Zastosowane środki do tej kontroli mogą obejmować: oględziny, obserwację zdalną za pomocą odpowiednich urządzeń, weryfikację pieczęci, zabezpieczeń, barier lub innych środków wskazujących naruszenie oraz pomiary promieniowania jonizującego lub innych zjawisk fizycznych, które potwierdzają obecność źródła. W przypadku źródeł stosowanych w urządzeniach, sprawdzenie czy urządzenie działa, może być wystarczające.

Opóźnianie

Ad. L.p. 6.

Zrównoważony system składający się z co najmniej dwóch barier powinien oddzielać źródło od pracowników nieupoważnionych i zapewnić wystarczające opóźnienie po wykryciu, aby umożliwić personelowi reagowania przerwanie próby usunięcia źródła. W przypadku stosowanych, wytwarzanych lub przetwarzanych źródeł, środki te mogą obejmować blokady zamontowane w obszarze (obiekcie, innym miejscu) chronionym, które oddzielają źródło lub urządzenie od pracowników nieupoważnionych.

W przypadku źródeł przechowywanych, środki te mogą obejmować zamykany i nieruchomy pojemnik lub urządzenie zawierające źródło w zamkniętym magazynie, w ten sposób oddzielając pojemnik od pracowników nieupoważnionych. W przypadku stosowanych mobilnych źródeł, ciągły nadzór wzrokowy przez pracowników jednostki organizacyjnej może zastępować jedną lub dwie bariery.

Reagowanie

Ad. L.p. 7.

Reagowanie na wykrycie powinno być natychmiastowe i odpowiednie do zaistniałej sytuacji. *Natychmiastowe* oznacza, że od momentu powiadomienia, personel reagowania powinien przybyć na miejsce w czasie krótszym, od czasu wymaganego do przedostania się przez bariery i dokonania nieuprawnionego usunięcia. *Odpowiednie* oznacza, że personel reagowania jest odpowiednio liczny i odpowiednio przeszkolony do powstrzymania osoby lub osób działających w zamiarze dokonania nieuprawnionego usunięcia.

Zarządzanie zabezpieczeniem

Ad. L.p. 8.

Kontrola dostępu, to weryfikacja prawa dostępu do lokalizacji źródła. Osoby upoważnione mają pozwolenie na tymczasowe wyłączenie barier fizycznych, takich jak zablokowane drzwi (środki opóźnienia). W przypadku medycznych zastosowań źródeł promieniowania jonizującego, pacjenci nie muszą być „upoważnieni", ponieważ są eskortowani do źródła i znajdują się pod stałym nadzorem personelu medycznego.

Tożsamość i upoważnienie osoby starającej się o dostęp można sprawdzać następującymi środkami:

- osobisty numer identyfikacyjny (PIN), który aktywuje czytnik sterujący drzwiami;
- system odznak, które mogą również aktywować czytnik elektroniczny;
- system wymiany odznak w wejściowych punktach kontrolnych;
- czytnik cech biometrycznych do aktywowania urządzenia sterującego drzwiami.

Po weryfikacji upoważnienia dostępu danej osoby, system pozwala jej na wejście do chronionej lokalizacji źródła, np. przez otworzenie zamka. Należy zastosować połączenie dwóch lub więcej środków weryfikacyjnych, np. zastosowanie karty magnetycznej i numeru PIN; lub karty i klucza; lub PIN i hasła komputerowego; lub klucza i weryfikacji wzrokowej tożsamości przez inną osobę upoważnioną. W przypadku źródeł przechowywanych, stosowanych, wytwarzanych lub przetwarzanych środki te powinny umożliwić kontrolowanie dostępu do chronionego obszaru, obiektu lub innego miejsca gdzie znajduje się źródło. W przypadku przechowywanych źródeł, środki te powinny umożliwić kontrolowanie dostępu do zamkniętego pomieszczenia lub innego miejsca, w którym źródło jest przechowywane. W przypadku stosowanych mobilnych źródeł, ciągły nadzór wzrokowy przez kilku pracowników jednostki organizacyjnej może zastępować kontrolę dostępu.

Ad. L.p. 9.

Wiarygodność osoby należy oceniać na podstawie sprawdzenia jej przeszłości, przed pozwoleniem tej osobie na samodzielny dostęp do źródeł promieniotwórczych, lokalizacji ich stosowania, wytwarzania, przetwarzania lub przechowywania, jak również do niejawnych informacji związanych z tymi źródłami. Charakter i stopień dokładności sprawdzenia przeszłości powinien być proporcjonalny do żądanego poziomu zabezpieczenia źródła promieniotwórczego. W wersji podstawowej sprawdzenie powinno obejmować potwierdzenie tożsamości i weryfikację referencji, w celu określenia uczciwości, charakteru i rzetelności każdej osoby. Proces oceny wiarygodności należy okresowo powtarzać i wspomagać ciągłym nadzorem osób zarządzających w celu zapewnienia, że pracownicy wszystkich poziomów wykonują swoje obowiązki w sposób odpowiedzialny i rzetelny.

Ad. L.p. 10.

Oprócz zabezpieczenia źródeł promieniotwórczych konieczna jest ochrona związanych z nimi informacji wrażliwych. Informacje te obejmują dokumenty, dane w systemach komputerowych oraz inne środki wykorzystywane do określania w szczególności:

- dokładnego położenia i wykazu źródeł;
- Planu zabezpieczenia i szczegółowych informacji dotyczących zabezpieczeń;
- systemu zabezpieczenia (np. alarmy), w tym ich działania oraz schematów instalacji;
- tymczasowych lub długotrwałych słabości Planu zabezpieczenia;
- ustaleń dotyczących pracowników zaangażowanych w zadania związane z zabezpieczeniem oraz środków reagowania na zagrożenia lub alarmy;
- planowanych terminów, tras i sposobu wysyłki lub transportu źródeł;
- środków reagowania.

Ad. L.p. 11.

Za przygotowanie Planu zabezpieczenia odpowiedzialny jest kierownik jednostki organizacyjnej. Przykładowa zawartość Planu zabezpieczenia znajduje się w Załączniku III. Zaleca się, aby wymagany przez Rozporządzenie Rady Ministrów z dnia 30 czerwca 2015 r. w sprawie dokumentów wymaganych przy składaniu wniosku o wydanie zezwolenia na wykonywanie działalności związanej z narażeniem na działanie promieniowania jonizującego albo przy zgłoszeniu wykonywania tej działalności, stanowiący część programu zapewnienia jakości, opis sposobu zabezpieczenia źródeł promieniotwórczych przed uszkodzeniem, kradzieżą i dostaniem się w ręce osób nieuprawnionych, miał formę Planu zabezpieczenia źródeł. Mimo, że posiadanie Planu zabezpieczenia jest jedynie zalecane to inspektorzy dozoru jądrowego podczas przeprowadzanych z odpowiednią częstotliwością kontroli będą pytali o te Plany i sprawdzali ich aktualność oraz zgodność z niniejszymi zaleceniami. Plany te mogą różnić się w odniesieniu do źródeł mobilnych i przenośnych, oraz do źródeł przechowywanych pomiędzy okresami użytkowania. Większość Planów zawiera wrażliwe informacje dotyczące zabezpieczenia, dlatego należy obchodzić się z nimi w odpowiedni sposób. Plan zabezpieczenia powinien również pozwalać na szybkie i skuteczne przejście na wyższy poziom zabezpieczenia w przypadku wzrostu zagrożenia.

Ad. L.p. 12.

Przykładowe zdarzenia, zalecane do ujęcia w Planie zabezpieczenia źródeł:

— podejrzenie popełnienia działania szkodzącego;
— zamieszki, które mogą zagrażać bezpieczeństwu źródeł;
— wtargnięcie nieupoważnionych osób na chroniony obszar, do chronionego obiektu lub innego miejsca, w tym także zaplanowany atak w celu podjęcia działania szkodzącego.

Zaleca się opracowanie procedur opisujących działania podejmowane przez pracowników jednostki organizacyjnej w odpowiedzi na scenariusze zdarzeń zagrażających utrzymaniu poziomu zabezpieczenia A zawarte w Planie zabezpieczenia.

Ad. L.p. 13.

W przypadku stwierdzenia utraty źródła lub podejrzenia utraty należy postępować według zakładowego planu postępowania awaryjnego opracowanego zgodnie z rozporządzeniem Rady Ministrów z dnia 18 stycznia 2005 r. w sprawie planów postępowania awaryjnego w przypadku zdarzeń radiacyjnych.

6.2 Środki zabezpieczenia dla poziomu zabezpieczenia B

Celem poziomu zabezpieczenia B jest **zminimalizowanie prawdopodobieństwa nieuprawnionego usunięcia** źródła promieniotwórczego. W przypadku podjęcia próby nieupoważnionego dostępu lub usunięcia źródła, reakcja musi mieć miejsce natychmiast po wykryciu i ocenie wykrycia, ale personel reagowania nie musi posiadać czasu potrzebnego do uniemożliwienia usunięcia źródła. Taki czas, w przypadku poziomu zabezpieczenia A dawała realizacja funkcji zabezpieczenia „opóźnienie”. W przypadku poziomu zabezpieczenia B funkcja zabezpieczenia „opóźnienie” ma zminimalizować prawdopodobieństwo nieuprawnionego usunięcia. Aby osiągnąć ten cel, zaleca się środki opisane w Tabeli 5.

TABELA 5. ZALECANE ŚRODKI ZABEZPIECZENIA DLA **POZIOMU ZABEZPIECZENIA B** *(cel: minimalizacja prawdopodobieństwa nieuprawnionego usunięcia)*

L.p.	Funkcje zabezpieczenia	Cel zabezpieczenia	Środki zabezpieczenia
1.	Wykrywanie	natychmiastowe wykrywanie nieupoważnionego dostępu do chronionej lokalizacji źródła	system alarmowy lub ciągła obserwacja wzrokowa przeprowadzana przez pracowników jednostki organizacyjnej lub firmy wynajętej do zabezpieczenia (firma „ochroniarska” dysponująca personelem reagowania)
2.		wykrywanie próby nieuprawnionego usunięcia źródła	system alarmowy lub okresowy nadzór wzrokowy przeprowadzany przez pracowników jednostki organizacyjnej lub firmy „ochroniarskiej”
3.		natychmiastowa ocena wykrycia	system alarmowy wyposażony w kamery przekazujące obraz pozwalający na ocenę przyczyny uaktywnienia się systemu alarmowego lub dokonanie tej oceny przez pracowników jednostki organizacyjnej lub firmy „ochroniarskiej”
4.		natychmiastowa informacja dla personelu reagowania	szybkie, pewne i różne środki komunikacji, takie jak telefony stacjonarne, komórkowe, radia
5.		wykrywanie utraty za pomocą weryfikacji	cotygodniowa kontrola fizyczna, pomiary

6.	Opóźnianie	opóźnienie minimalizujące prawdopodobieństwo nieuprawnionego usunięcia	system dwóch barier (np. ściany, kraty)
7.	Reagowanie	natychmiastowa reakcja na sprawdzony alarm w celu przerwania nieuprawnionego usunięcia	dysponowanie wyposażeniem oraz zapewnienie procedur natychmiastowego rozpoczęcia reagowania
8.	Zarządzanie zabezpieczeniem	kontrola dostępu do lokalizacji źródła, która skutecznie ogranicza dostęp osób nieupoważnionych	jeden środek identyfikacyjny
9.		zapewnienie wiarygodności osób upoważnionych	kontrole przeszłości każdego z pracowników upoważnionych do samodzielnego dostępu do lokalizacji źródła i niejawnych informacji
10.		dane zawierające informacje niejawne są określone i chronione zgodnie z ustawą z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych	procedury określające rodzaj informacji i środki ich ochrony przed nieupoważnionym wyjawieniem
11.		opracowanie Planu zabezpieczenia	Plan zabezpieczenia, który spełnia zalecenia organizacyjno-techniczne Prezesa PAA i określa reagowanie w różnych przypadkach (sytuacjach) zagrożenia
12.		zapewnienie zdolności do zarządzania zagrożeniami bezpieczeństwa	procedury odpowiedzi na scenariusze związane z zagrożeniami bezpieczeństwa
13.		ustanowienie systemu zawiadamiania o zagrożeniach bezpieczeństwa	procedury opisane w zakładowym planie postępowania awaryjnego opracowanym zgodnie z rozporządzeniem Rady Ministrów z dnia 18 stycznia 2005 r. w sprawie planów postępowania awaryjnego w przypadku zdarzeń radiacyjnych

Wykrywanie

Ad. L.p. 1.

System alarmowy lub ciągła obserwacja wzrokowa mają za zadanie zidentyfikowanie nieupoważnionego dostępu do chronionej lokalizacji źródła (być może w celu usunięcia źródła). Należy zwrócić szczególną uwagę na to, by środków wykrywania takiego działania nie dało się obejść. W przypadku stosowanych (to znaczy będących w użyciu, w odróżnieniu od przechowywanych) mobilnych źródeł, ciągły nadzór wzrokowy może być jedynym rozsądnym sposobem wykrywania próby nieuprawnionego usunięcia. W przypadku przechowywanych źródeł, środki te powinny wykrywać nieupoważniony dostęp do zamkniętego pomieszczenia lub innego miejsca, w którym źródło jest przechowywane.

Ad. L.p. 2.

System alarmowy lub okresowy nadzór wzrokowy przeprowadzany przez pracowników jednostki organizacyjnej (lub firmy ochroniarskiej) podczas okresowych kontroli, wskazują na próbę działania szkodzącego. Oczywiście w przypadku okresowych kontroli jedynie w szczególnych sytuacjach będzie możliwe wykrycie próby działania szkodzącego. Dlatego też zaleca się stosowanie systemów alarmowych, których zadziałanie zostanie zweryfikowane przez personel reagowania. W przypadku stosowanych mobilnych lub przenośnych źródeł, ciągły nadzór wzrokowy może być jedynym rozsądnym środkiem wykrywania próby nieuprawnionego usunięcia.

Ad. L.p. 3. i 4.

W przypadku stwierdzenia, że nastąpił nieupoważniony dostęp lub próba nieuprawnionego usunięcia źródła promieniotwórczego należy natychmiast przekazać taką informację personelowi reagowania.

Ad. L.p. 5.

Cotygodniowa kontrola służy sprawdzeniu czy źródła są wciąż na miejscu, nie uległy naruszeniu i czy spełnione są cele zabezpieczenia określone w pozycji 1 i 2. Kontrola może obejmować oględziny czy źródło jest na swoim miejscu, weryfikację pieczęci, zabezpieczeń, barier lub innych środków wskazujących naruszenie oraz pomiary promieniowania jonizującego lub innych zjawisk fizycznych, które potwierdzają obecność źródła. W przypadku stosowanych źródeł (urządzeń zawierających źródła), sprawdzenie czy urządzenie działa, może być wystarczające.

Opóźnianie

Ad. L.p. 6.

W przypadku poziomu zabezpieczenia B celem funkcji zabezpieczenia jest zminimalizowanie prawdopodobieństwa nieuprawnionego usunięcia. Zrównoważony system dwóch barier powinien oddzielać źródło od pracowników nieupoważnionych. W przypadku stosowanych, wytwarzanych lub przetwarzanych źródeł, środki te mogą obejmować blokady zamontowane w obszarze chronionym, które oddzielają źródło lub urządzenie od pracowników nieupoważnionych. W przypadku źródeł przechowywanych, środki te mogą obejmować zamykany i nieruchomy pojemnik lub urządzenie zawierające źródło, które jest zamknięte w magazynie, w ten sposób oddzielając pojemnik lub urządzenie od pracowników nieupoważnionych. W przypadku stosowanych mobilnych lub przenośnych źródeł, ciągły nadzór wzrokowy przez pracowników jednostki organizacyjnej może zastępować bariery.

Reagowanie

Ad. L.p. 7.

Reagowanie na wykrycie powinno być natychmiastowe. W przypadku poziomu zabezpieczenia B, celem funkcji zabezpieczenia „reagowanie” jest przerwanie nieuprawnionego usunięcia.

Zarządzanie zabezpieczeniem

Ad. L.p. 8.

Kontrola dostępu, to weryfikacja prawa dostępu do lokalizacji źródła. Osoby upoważnione mają pozwolenie na tymczasowe wyłączenie barier fizycznych, takich jak zablokowane drzwi (środki opóźnienia). W przypadku medycznych zastosowań źródeł promieniowania jonizującego, pacjenci nie muszą być „upoważnieni”, ponieważ są eskortowani do źródła i znajdują się pod stałym nadzorem personelu medycznego.

Tożsamość i upoważnienie osoby starającej się o dostęp można sprawdzać następującymi środkami:

— osobisty numer identyfikacyjny (PIN), który aktywuje czytnik sterujący drzwiami;
— system odznak, które mogą również aktywować czytnik elektroniczny;
— system wymiany odznak w wejściowych punktach kontrolnych;
— czytnik cech biometrycznych do aktywowania urządzenia sterującego drzwiami.

Po weryfikacji upoważnienia do dostępu danej osoby system pozwala jej na wejście do chronionej lokalizacji źródła np. przez otworzenie zamka. Wymagany jest co najmniej jeden z następujących środków identyfikacyjnych, np. zastosowanie karty magnetycznej i numeru PIN, hasła komputerowego, klucza lub weryfikacji wzrokowej tożsamości przez inną osobę upoważnioną. W przypadku źródeł stosowanych, wytwarzanych, przetwarzanych lub przechowywanych środki te powinny zapewniać dostęp do chronionego obszaru, obiektu lub innego miejsca, gdzie znajduje się źródło. W przypadku stosowanych mobilnych lub przenośnych źródeł, ciągły nadzór wzrokowy przez pracowników jednostki organizacyjnej może stanowić zastąpienie kontroli dostępu.

Ad. L.p. 9.

Wiarygodność osoby należy oceniać na podstawie sprawdzenia jej przeszłości, przed pozwoleniem tej osobie na samodzielny dostęp do źródeł promieniotwórczych, lokalizacji ich stosowania, wytwarzania, przetwarzania lub przechowywania, jak również do niejawnych informacji związanych z tymi źródłami. Charakter i stopień dokładności sprawdzenia przeszłości powinien być proporcjonalny do żądanego poziomu zabezpieczenia źródła promieniotwórczego. W wersji podstawowej sprawdzenie powinno obejmować potwierdzenie tożsamości i weryfikację referencji, w celu określenia uczciwości, charakteru i rzetelności każdej osoby. Proces oceny wiarygodności należy okresowo powtarzać i wspomagać ciągłym nadzorem osób zarządzających w celu zapewnienia, że pracownicy wszystkich poziomów wykonują swoje obowiązki w sposób odpowiedzialny i rzetelny.

Ad. L.p. 10.

Oprócz zabezpieczenia źródeł promieniotwórczych konieczna jest ochrona związanych z nimi informacji wrażliwych, które obejmują dokumenty, dane w systemach komputerowych oraz inne środki, wykorzystywane w szczególności do określania:

- dokładnego położenia i wykazu źródeł;
- Planu zabezpieczenia i szczegółowych informacji dotyczących zabezpieczeń;
- systemu zabezpieczenia (np. alarmy), w tym ich działania oraz schematów instalacji;
- tymczasowych lub długotrwałych słabości Planu zabezpieczenia;
- ustaleń dotyczących pracowników zaangażowanych w zadania związane z zabezpieczeniem oraz środków reagowania na zagrożenia lub alarmy;
- planowanych terminów, tras i sposobu wysyłki lub transportu źródeł;
- środków reagowania.

Ad. L.p. 11.

Za przygotowanie Planu zabezpieczenia odpowiedzialny jest kierownik jednostki organizacyjnej. Przykładowa zawartość Planu zabezpieczenia znajduje się w Załączniku III. Zaleca się, aby wymagany przez Rozporządzenie Rady Ministrów z dnia 30 czerwca 2015 r. w sprawie dokumentów wymaganych przy składaniu wniosku o wydanie zezwolenia na wykonywanie działalności związanej z narażeniem na działanie promieniowania jonizującego albo przy zgłoszeniu wykonywania tej działalności, stanowiący część programu zapewnienia jakości, opis sposobu zabezpieczenia źródeł promieniotwórczych przed uszkodzeniem, kradzieżą i dostaniem się w ręce osób nieuprawnionych, miał formę Planu zabezpieczenia źródeł. Mimo, że posiadanie Planu zabezpieczenia jest jedynie zalecane to inspektorzy dozoru jądrowego podczas przeprowadzanych z odpowiednią częstotliwością kontroli będą pytali o te Plany i sprawdzali ich aktualność oraz zgodność z niniejszymi zaleceniami. Plany te mogą różnić się w odniesieniu do źródeł mobilnych i przenośnych oraz do źródeł przechowywanych pomiędzy okresami użytkowania. Większość Planów zawiera wrażliwe informacje dotyczące zabezpieczenia, dlatego należy obchodzić się z nimi w odpowiedni sposób. Plan zabezpieczenia powinien również pozwalać na szybkie i skuteczne przejście na wyższy poziom zabezpieczenia w przypadku wzrostu zagrożenia.

Ad. L.p. 12.

Przykładowe zdarzenia, zalecane do ujęcia w Planie zabezpieczenia:

- podejrzenie popełnienia działania szkodzącego;
- zamieszki, które mogą zagrażać bezpieczeństwu źródeł;
- wtargnięcie nieupoważnionych osób na chroniony obszar, do chronionego obiektu lub innego miejsca w tym także zaplanowany atak w celu usunięcia źródeł promieniotwórczych.

Zaleca się opracowanie procedur opisujących działania podejmowane przez pracowników jednostki organizacyjnej w odpowiedzi na scenariusze zdarzeń zagrażających utrzymaniu poziomu zabezpieczenia B zawarte w Planie zabezpieczenia.

Ad. L.p. 13.

W przypadku stwierdzenia utraty źródła lub podejrzenia utraty należy postępować według zakładowego planu postępowania awaryjnego opracowanego zgodnie z rozporządzeniem Rady Ministrów z dnia 18 stycznia 2005 r. w sprawie planów postępowania awaryjnego w przypadku zdarzeń radiacyjnych.

6.3 Środki zabezpieczenia dla poziomu zabezpieczenia C

Celem poziomu zabezpieczenia C **jest zmniejszenie prawdopodobieństwa nieuprawnionego usunięcia** źródła promieniotwórczego. Aby osiągnąć ten cel, zaleca się następujące środki.

TABELA 6. ZALECANE ŚRODKI ZABEZPIECZENIA DLA POZIOMU **ZABEZPIECZENIA C**
(cel: zmniejszanie prawdopodobieństwa nieuprawnionego usunięcia)

L.p.	Funkcje zabezpieczenia	Cel zabezpieczenia	Środki zabezpieczenia
1.	Wykrywanie	wykrywanie nieuprawnionego usunięcia źródła	system alarmowy lub okresowe kontrole przeprowadzane przez pracowników jednostki organizacyjnej
2.		natychmiastowa ocena wykrycia	ocena przez pracowników jednostki organizacyjnej
3.		wykrywanie utraty za pomocą weryfikacji	comiesięczne kontrola fizyczna, pomiary
4.	Opóźnianie	opóźnienie zmniejszające prawdopodobieństwo nieuprawnionego usunięcia źródła	jedna bariera (np. kraty, osłona źródła) lub obserwacja przez pracowników jednostki organizacyjnej
5.	Reagowanie	wprowadzenie działań przewidzianych w zakładowym planie postępowania awaryjnego w przypadku nieuprawnionego usunięcia źródła. Zakładowe plany postępowania awaryjnego opracowane są zgodnie z rozporządzeniem Rady Ministrów z dnia 18 stycznia 2005 r. w sprawie planów postępowania awaryjnego w przypadku zdarzeń radiacyjnych.	procedury określające konieczne działania zgodnie z zakładowym planem postępowania awaryjnego
6.	Zarządzanie zabezpieczeniem	kontrola dostępu do lokalizacji źródła, która skutecznie ogranicza dostęp osób nieupoważnionych	jeden środek identyfikacyjny
7.		zapewnienie wiarygodności osób upoważnionych	metody określania wiarygodności osób upoważnionych do samodzielnego dostępu do źródła promieniotwórczego i informacji wrażliwych
8.		dane zawierające informacje niejawne są określone i chronione zgodnie z ustawą z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych	procedury określające rodzaj informacji i środki ich ochrony przed nieupoważnionym wyjawieniem
9.		opracowanie Planu zabezpieczenia	Plan zabezpieczenia, który spełnia zalecenia organizacyjno-techniczne Prezesa PAA i określa reagowanie w różnych przypadkach (sytuacjach) zagrożenia
10.		zapewnienie zdolności do zarządzania zagrożeniami bezpieczeństwa	procedury odpowiedzi na scenariusze związane z zagrożeniami bezpieczeństwa
11.		ustanowienie systemu zawiadamiania o zagrożeniach bezpieczeństwa	procedury opisane w zakładowym planie postępowania awaryjnego

Wykrywanie

Ad. L.p. 1.

Do wykrycia nieuprawnionego usunięcia źródła może służyć system alarmowy. W przypadku braku takiego systemu wyznaczony pracownik jednostki organizacyjnej powinien okresowo kontrolować, czy źródła znajdują się w stosownych lokalizacjach. Zastosowane do tej kontroli środki mogą obejmować oględziny, obserwację zdalną za pomocą odpowiednich urządzeń, weryfikację pieczęci, zabezpieczeń, barier lub innych środków wskazujących naruszenie oraz pomiary promieniowania jonizującego lub innych zjawisk fizycznych, które potwierdzają obecność źródła. W przypadku źródeł stosowanych w urządzeniach, sprawdzenie czy urządzenie działa, może być wystarczające.

Ad. L.p. 2.

Gdy system alarmowy wykrywający naruszenie lub kontrola fizyczna wskazują brak źródła, należy przeprowadzić natychmiastową ocenę sytuacji w celu określenia, czy doszło do rzeczywistego nieuprawnionego usunięcia.

Ad. L.p. 3.

Comiesięczna kontrola służy sprawdzeniu czy źródła są wciąż na miejscu, nie uległy naruszeniu i czy są spełnione cele zabezpieczenia określone w pozycji 1. Kontrola może obejmować oględziny, czy źródło jest na swoim miejscu, weryfikację pieczęci, zabezpieczeń, barier lub innych środków wskazujących naruszanie oraz pomiary promieniowania jonizującego lub innych zjawisk fizycznych, które potwierdzają obecność źródła. W przypadku stosowanych źródeł (urządzeń zawierających źródła), sprawdzenie, czy urządzenie działa, może być wystarczające.

Opóźnianie

Ad. L.p. 4.

Co najmniej jedna bariera powinna oddzielać źródło od pracowników nieupoważnionych. W przypadku stosowanych źródeł, środki te mogą obejmować osłonę źródła lub stosowanie go na terenie chronionym. W przypadku źródeł przechowywanych środki te mogą obejmować zamykany i nieruchomy pojemnik lub urządzenie zawierające źródło w zamkniętym magazynie, w ten sposób oddzielając pojemnik od pracowników nieupoważnionych. W przypadku stosowanych mobilnych lub przenośnych źródeł, ciągły nadzór wzrokowy przez pracowników jednostki organizacyjnej może zastępować bariery.

Reagowanie

Ad. L.p. 5.

W przypadku stwierdzenia nieuprawnionego usunięcia źródła należy postępować według zakładowego planu postępowania awaryjnego opracowanego zgodnie z rozporządzeniem Rady Ministrów z dnia 18 stycznia 2005 r. w sprawie planów postępowania awaryjnego w przypadku zdarzeń radiacyjnych. Kierownik jednostki organizacyjnej jest odpowiedzialny za przeprowadzenie analizy okoliczności, które doprowadziły do tego wydarzenia.

Zarządzanie zabezpieczeniem

Ad. L.p. 6.

Kontrola dostępu, to weryfikacja prawa dostępu do lokalizacji źródła. Osoby upoważnione mają pozwolenie na tymczasowe wyłączanie barier fizycznych, takich jak zablokowane drzwi (środki opóźnienia). W przypadku medycznych zastosowań źródeł promieniowania jonizującego, pacjenci nie muszą być „upoważnieni”, ponieważ są eskortowani do źródła i znajdują się pod stałym nadzorem personelu medycznego.

Tożsamość i upoważnienie osoby starającej się o dostęp można sprawdzać następującymi środkami:

- osobisty numer identyfikacyjny (PIN), który aktywuje czytnik sterujący drzwiami;
- system odznak, które mogą również aktywować czytnik elektroniczny;
- system wymiany odznak w wejściowych punktach kontrolnych;
- czytnik cech biometrycznych do aktywowania urządzenia sterującego drzwiami.

Po weryfikacji upoważnienia do dostępu danej osoby system pozwala jej na wejście do chronionej lokalizacji źródła np. przez otworzenie zamka. Wymagany jest co najmniej następujący środek identyfikacyjny: zastosowanie karty magnetycznej i numeru PIN, hasła komputerowego, klucza lub weryfikacji wzrokowej tożsamości przez inną osobę upoważnioną. W przypadku źródeł przechowywanych stosowanych, wytwarzanych lub przetwarzanych, środki te powinny kontrolować dostęp do zamkniętego pomieszczenia lub innego miejsca, w których znajdują się źródła. W przypadku stosowanych mobilnych lub przenośnych źródeł, ciągły nadzór wzrokowy przez pracowników jednostki organizacyjnej może zastępować kontrolę dostępu.

Ad. L.p. 7.

Wiarygodność osoby należy oceniać na podstawie sprawdzenia jej przeszłości, przed pozwoleniem tej osobie na samodzielny dostęp do źródeł promieniotwórczych, lokalizacji ich stosowania, wytwarzania, przetwarzania lub przechowywania lub do niejawnych, powiązanych z nimi informacji. Charakter i stopień dokładności kontroli przeszłości powinien być proporcjonalny do poziomu zabezpieczenia źródeł.

Ad. L.p. 8.

Zaleca się, aby kierownik jednostki organizacyjnej ocenił, czy osoby z dostępem do informacji niejawnych dotyczących źródeł promieniotwórczych są dla niego wiarygodne. Osobom uznanym za niewiarygodne, nie należy przyznawać możliwości dostępu.

Ad. L.p. 9.

Za przygotowanie Planu zabezpieczenia odpowiedzialny jest kierownik jednostki organizacyjnej. Przykładowa zawartość Planu zabezpieczenia znajduje się w Załączniku III. Zaleca się, aby wymagany przez Rozporządzenie Rady Ministrów z dnia 30 czerwca 2015 r. w sprawie dokumentów wymaganych przy składaniu wniosku o wydanie zezwolenia na wykonywanie działalności związanej z narażeniem na działanie promieniowania jonizującego albo przy zgłoszeniu wykonywania tej działalności, stanowiący część programu zapewnienia jakości, opis sposobu zabezpieczenia źródeł promieniotwórczych przed uszkodzeniem, kradzieżą i dostaniem się w ręce osób nieuprawnionych, miał formę Planu zabezpieczenia źródeł. Mimo, że posiadanie Planu zabezpieczenia jest jedynie zalecane to inspektorzy dozoru jądrowego podczas przeprowadzanych z odpowiednią częstotliwością kontroli będą pytali o te Plany i sprawdzali ich aktualność oraz zgodność z niniejszymi zaleceniami. Plany te mogą różnić się w odniesieniu do źródeł mobilnych i przenośnych oraz do źródeł przechowywanych pomiędzy okresami ich użytkowania. Większość Planów zawiera wrażliwe informacje dotyczące zabezpieczenia, dlatego należy obchodzić się z nimi w odpowiedni sposób. Plan zabezpieczenia powinien również pozwalać na szybkie i skuteczne przejście na wyższy poziom zabezpieczenia w przypadku wzrostu zagrożenia.

Ad. L.p. 10.

Zaleca się opracowanie procedur opisujących działania podejmowane przez pracowników jednostki organizacyjnej w odpowiedzi na scenariusze zdarzeń zagrażających utrzymaniu poziomu zabezpieczenia C zawarte w Planie zabezpieczenia.

Ad. L.p. 11.

W przypadku stwierdzenia braku źródła należy postępować według zakładowego planu postępowania awaryjnego opracowanego zgodnie z rozporządzeniem Rady Ministrów z dnia 18 stycznia 2005 r. w sprawie planów postępowania awaryjnego w przypadku zdarzeń radiacyjnych.

ZAŁĄCZNIK I
GRANICZNE WARTOŚCI AKTYWNOŚCI IZOTOPÓW PROMIENIOTWÓRCZYCH STANOWIĄCE KRYTERIUM KATEGORYZACJI ŹRODEŁ PROMIENIOTWÓRCZYCH

TABELA

WAROŚĆ AKTYWNOŚCI IZOTOPÓW PROMIENIOTWÓRCZYCH ZAWARTYCH W ŹRÓDŁACH (P_1) STANOWI WARTOŚĆ GRANICZNĄ, PONIŻEJ KTÓREJ ŹRÓDŁA NIE WYMAGAJĄ ZABEZPIECZEŃ PRZEWIDZIANYCH W NINIEJSZYCH ZALECENIACH
WAROŚĆ AKTYWNOŚCI IZOTOPÓW PROMIENIOTWÓRCZYCH ZAWARTYCH W ŹRÓDŁACH (D) STANOWI WARTOŚĆ GRANICZNĄ, POWYŻEJ KTÓREJ ŹRÓDŁA KLASYFIKOWANE SĄ JAKO ŹRÓDŁA WYSOKOAKTYWNE W ROZUMIENIU DYREKTYWY 2003/122/EURATOM W SPRAWIE WYSOCE RADIOAKTYWNYCH ŹRÓDEŁ ZAMKNIĘTYCH I ODPADÓW RADIOAKTYWNYCH.

Izotop promieniotwórczy	Aktywność P_1[2] (Bq)	Aktywność D[3] (Bq)
1	2	3
H-3	1,00E+09	2,00E+15
Be-7	1,00E+07	1,00E+12
Be-10		3,00E+13
C-11		6,00E+10
C-14	1,00E+07	5,00E+13
O-15	1,00E+09	
N-13		6,00E+10
F-18	1,00E+06	6,00E+10
Na-22	1,00E+06	3,00E+10
Na-24	1,00E+05	2,00E+10
Mg-28		2,00E+10
Al-26		3,00E+10
Si-31	1,00E+06	1,00E+13
Si-32		7,00E+12
P-32	1,00E+05	1,00E+13
P-33	1,00E+08	2,00E+14

[2] Brak poziomu progowego aktywności P_1 oznacza, że kategoria źródeł promieniotwórczych z tym izotopem zależy wyłącznie od stosunku A/D.

[3] Brak poziomu progowego aktywności D oznacza, że źródła promieniotwórcze z tym izotopem zalicza się zawsze do kategorii 5.

S-35	1,00E+08	6,00E+13
Cl-36	1,00E+06	2,00E+13
Cl-38	1,00E+05	5,00E+10
Ar-37	1,00E+08	
Ar-39		3,00E+14
Ar-41	1,00E+09	5,00E+10
K-40	1,00E+06	
K-42	1,00E+06	2,00E+11
K-43	1,00E+06	7,00E+10
Ca-45	1,00E+07	1,00E+14
Ca-47	1,00E+06	6,00E+10
Sc-44		3,00E+10
Sc-46	1,00E+06	3,00E+10
Sc-47	1,00E+06	7,00E+11
Sc-48	1,00E+05	2,00E+10
Ti-44		3,00E+10
V-48	1,00E+05	2,00E+10
V-49		2,00E+15
Cr-51	1,00E+07	2,00E+12
Mn-51	1,00E+05	
Mn-52	1,00E+05	2,00E+10
Mn-52m	1,00E+05	
Mn-53	1,00E+09	
Mn-54	1,00E+06	8,00E+10
Mn-56	1,00E+05	4,00E+10
Fe-52	1,00E+06	2,00E+10
Fe-55	1,00E+06	8,00E+14
Fe-59	1,00E+06	6,00E+10
Fe-60		6,00E+10
Co-55	1,00E+06	3,00E+10
Co-56	1,00E+05	2,00E+10
Co-57	1,00E+06	7,00E+11
Co-58	1,00E+06	7,00E+10
Co-58m	1,00E+07	7,00E+10
Co-60	1,00E+05	3,00E+10
Co-60m	1,00E+06	
Co-61	1,00E+06	
Co-62m	1,00E+05	
Ni-59	1,00E+08	1,00E+15
Ni-63	1,00E+08	6,00E+13
Ni-65	1,00E+06	1,00E+11
Cu-64	1,00E+06	3,00E+11
Cu-67		7,00E+11
Zn-65	1,00E+06	1,00E+11
Zn-69	1,00E+06	3,00E+13

Zn-69m	1,00E+06	2,00E+11
Ga-67		5,00E+11
Ga-68		7,00E+10
Ga-72	1,00E+05	3,00E+10
Ge-68		7,00E+10
Ge-71	1,00E+08	1,00E+15
Ge-77		6,00E+10
As-72		4,00E+10
As-73	1,00E+07	4,00E+13
As-74	1,00E+06	9,00E+10
As-76	1,00E+05	2,00E+11
As-77	1,00E+06	8,00E+12
Se-75	1,00E+06	2,00E+11
Se-79		2,00E+14
Br-76		3,00E+10
Br-77		2,00E+11
Br-82	1,00E+06	3,00E+10
Kr-74	1,00E+09	
Kr-76	1,00E+09	
Kr-77	1,00E+09	
Kr-79	1,00E+05	
Kr-81	1,00E+07	3,00E+13
Kr-83m	1,00E+12	
Kr-85	1,00E+04	3,00E+13
Kr-85m	1,00E+10	5,00E+11
Kr-87	1,00E+09	9,00E+10
Kr-88	1,00E+09	
Rb-81		1,00E+11
Rb-83		1,00E+11
Rb-84		7,00E+10
Rb-86	1,00E+05	7,00E+11
Sr-82		6,00E+10
Sr-85	1,00E+06	1,00E+11
Sr-85m	1,00E+07	1,00E+11
Sr-87m	1,00E+06	2,00E+11
Sr-89	1,00E+06	2,00E+13
Sr-90+	1,00E+04	1,00E+12
Sr-91	1,00E+05	6,00E+10
Sr-92	1,00E+06	4,00E+10
Y-87		9,00E+10
Y-88		3,00E+10
Y-90	1,00E+05	5,00E+12
Y-91	1,00E+06	8,00E+12
Y-91m	1,00E+06	1,00E+11
Y-92	1,00E+05	2,00E+11

Y-93	1,00E+05	6,00E+11
Zr-88		2,00E+10
Zr-93+	1,00E+07	
Zr-95	1,00E+06	4,00E+10
Zr-97+	1,00E+05	4,00E+10
Nb-93m	1,00E+07	3,00E+14
Nb-94	1,00E+06	4,00E+10
Nb-95	1,00E+06	9,00E+10
Nb-97	1,00E+06	1,00E+11
Nb-98	1,00E+05	
Mo-90	1,00E+06	
Mo-93	1,00E+08	3,00E+14
Mo-99	1,00E+06	3,00E+11
Mo-101	1,00E+06	
Tc-95		1,00E+11
Tc-96	1,00E+06	3,00E+10
Tc-96m	1,00E+07	3,00E+10
Tc-97	1,00E+08	
Tc-97m	1,00E+07	4,00E+13
Tc-98		5,00E+10
Tc-99	1,00E+07	3,00E+13
Tc-99m	1,00E+07	7,00E+11
Ru-97	1,00E+07	3,00E+11
Ru-103	1,00E+06	1,00E+11
Ru-105	1,00E+06	8,00E+10
Ru-106+	1,00E+05	3,00E+11
Rh-99		1,00E+11
Rh-101		3,00E+11
Rh-102		3,00E+10
Rh-102m		1,00E+11
Rh-103m	1,00E+08	9,00E+14
Rh-105	1,00E+07	9,00E+11
Pd-103	1,00E+08	9,00E+13
Pd-109	1,00E+06	2,00E+13
Ag-105	1,00E+06	1,00E+11
Ag-108m+	1,00E+06	4,00E+10
Ag-110m	1,00E+06	2,00E+10
Ag-111	1,00E+06	2,00E+12
Cd-109	1,00E+06	2,00E+13
Cd-113		4,00E+13
Cd-115	1,00E+06	2,00E+11
Cd-115m	1,00E+06	3,00E+12
In-111	1,00E+06	2,00E+11
In-113m	1,00E+06	3,00E+11
In-114	1,00E+06	8,00E+11

In-115m	1,00E+06	4,00E+11
Sn-113	1,00E+07	3,00E+11
Sn-117		5,00E+11
Sn-119		7,00E+13
Sn-121		7,00E+13
Sn-123		7,00E+12
Sn-125	1,00E+05	1,00E+11
Sn-126		3,00E+10
Sb-122	1,00E+04	1,00E+11
Sb-124	1,00E+06	4,00E+10
Sb-125	1,00E+06	2,00E+11
Sb-126		2,00E+10
Te-121		1,00E+11
Te-121m		1,00E+11
Te-123m	1,00E+07	6,00E+11
Te-125m	1,00E+07	1,00E+13
Te-127	1,00E+06	1,00E+13
Te-127m	1,00E+07	3,00E+12
Te-129	1,00E+06	1,00E+12
Te-129m	1,00E+06	1,00E+12
Te-131	1,00E+05	
Te-131m	1,00E+06	4,00E+10
Te-132	1,00E+07	3,00E+10
Te-133	1,00E+05	
Te-133m	1,00E+05	
Te-134	1,00E+06	
I-123	1,00E+07	5,00E+11
I-124		6,00E+10
I-125	1,00E+06	2,00E+11
I-126	1,00E+06	1,00E+11
I-129	1,00E+05	
I-130	1,00E+06	
I-131	1,00E+06	2,00E+11
I-132	1,00E+05	3,00E+10
I-133	1,00E+06	1,00E+11
I-134	1,00E+05	3,00E+10
I-135	1,00E+06	4,00E+10
Xe-122		6,00E+10
Xe-123		9,00E+10
Xe-127		3,00E+11
Xe-131m	1,00E+04	1,00E+13
Xe-133	1,00E+04	3,00E+12
Xe-135	1,00E+10	3,00E+11
Cs-129	1,00E+05	3,00E+11
Cs-131	1,00E+06	2,00E+13

Cs-132	1,00E+05	1,00E+11
Cs-134	1,00E+04	4,00E+10
Cs-134m	1,00E+05	4,00E+10
Cs-135	1,00E+07	
Cs-136	1,00E+05	3,00E+10
Cs-137+	1,00E+04	1,00E+11
Cs-138	1,00E+04	
Ba-131	1,00E+06	2,00E+11
Ba-133		2,00E+11
Ba-133m		3,00E+11
Ba-140+	1,00E+05	3,00E+10
La-137		2,00E+13
La-140	1,00E+05	3,00E+10
Ce-139	1,00E+06	6,00E+11
Ce-141	1,00E+07	1,00E+12
Ce-143	1,00E+06	3,00E+11
Ce-144+	1,00E+05	9,00E+11
Pr-142	1,00E+05	1,00E+12
Pr-143	1,00E+06	3,00E+13
Nd-147	1,00E+06	6,00E+11
Nd-149	1,00E+06	2,00E+11
Pm-143		2,00E+11
Pm-144		4,00E+10
Pm-145		1,00E+13
Pm-147	1,00E+07	4,00E+13
Pm-148		3,00E+10
Pm-149	1,00E+06	6,00E+12
Pm-151		2,00E+11
Sm-145		4,00E+12
Sm-151	1,00E+08	5,00E+14
Sm-153	1,00E+06	2,00E+12
Eu-147		2,00E+11
Eu-148		3,00E+10
Eu-149		2,00E+12
Eu-150b		2,00E+12
Eu-150a		5,00E+10
Eu-152	1,00E+06	6,00E+10
Eu-152m	1,00E+06	2,00E+11
Eu-154	1,00E+06	6,00E+10
Eu-155	1,00E+07	2,00E+12
Eu-156		5,00E+10
Gd-146		3,00E+10
Gd-148		4,00E+11
Gd-153	1,00E+07	1,00E+12
Gd-159	1,00E+06	2,00E+12

Tb-157		1,00E+14
Tb-158		9,00E+10
Tb-160	1,00E+06	6,00E+10
Dy-159		6,00E+12
Dy-165	1,00E+06	3,00E+12
Dy-166	1,00E+06	1,00E+12
Ho-166	1,00E+05	2,00E+12
Ho-166m	1,00E+07	4,00E+10
Er-169		2,00E+14
Er-171	1,00E+06	2,00E+11
Tm-167		6,00E+11
Tm-170	1,00E+06	2,00E+13
Tm-171	1,00E+08	3,00E+14
Yb-169		3,00E+11
Yb-175	1,00E+07	2,00E+12
Lu-172		4,00E+10
Lu-173		9,00E+11
Lu-174		8,00E+11
Lu-174m		6,00E+11
Lu-177	1,00E+07	2,00E+12
Hf-172		4,00E+10
Hf-175		2,00E+11
Hf-181	1,00E+06	1,00E+11
Hf-182		5,00E+10
Ta-178		7,00E+10
Ta-179		6,00E+12
Ta-182	1,00E+04	6,00E+10
W-178		9,00E+11
W-181	1,00E+07	5,00E+12
W-185	1,00E+07	1,00E+14
W-187	1,00E+06	1,00E+11
W-188		1,00E+12
Re-184		8,00E+10
Re-184m		7,00E+10
Re-186	1,00E+06	4,00E+12
Re-188	1,00E+05	1,00E+12
Re-189		1,00E+12
Os-185	1,00E+06	1,00E+11
Os-191	1,00E+07	2,00E+12
Os-191m	1,00E+07	1,00E+12
Os-193	1,00E+06	1,00E+12
Os-194		7,00E+11
Ir-189		1,00E+12
Ir-190	1,00E+06	5,00E+10
Ir-192	1,00E+04	8,00E+10

Ir-194	1,00E+05	7,00E+11
Pt-188		4,00E+10
Pt-191	1,00E+06	3,00E+11
Pt-193		3,00E+15
Pt-193m	1,00E+07	1,00E+13
Pt-195m		2,00E+12
Pt-197	1,00E+06	4,00E+12
Pt-197m	1,00E+06	9,00E+11
Au-193		6,00E+11
Au-194		7,00E+10
Au-195		2,00E+12
Au-198	1,00E+06	2,00E+11
Au-199	1,00E+06	9,00E+11
Hg-194		7,00E+10
Hg-195m		2,00E+11
Hg-197	1,00E+07	2,00E+12
Hg-197m	1,00E+06	7,00E+11
Hg-203	1,00E+05	3,00E+11
Tl-200	1,00E+06	5,00E+10
Tl-201	1,00E+06	1,00E+12
Tl-202	1,00E+06	2,00E+11
Tl-204	1,00E+04	2,00E+13
Pb-201		9,00E+10
Pb-202		2,00E+11
Pb-203	1,00E+06	2,00E+11
Pb-210+	1,00E+04	3,00E+11
Pb-212+	1,00E+05	5,00E+10
Bi-205		4,00E+10
Bi-206	1,00E+05	2,00E+10
Bi-207	1,00E+06	5,00E+10
Bi-210	1,00E+06	8,00E+12
Bi-210m		3,00E+11
Bi-212+	1,00E+05	5,00E+10
Po-203	1,00E+06	
Po-205	1,00E+06	
Po-207	1,00E+06	
Po-210	1,00E+04	6,00E+10
At-211	1,00E+07	5,00E+11
Rn-220+	1,00E+07	
Rn-222+	1,00E+08	4,00E+10
Ra-223+	1,00E+05	1,00E+11
Ra-224+	1,00E+05	5,00E+10
Ra-225	1,00E+05	1,00E+11
Ra-226+	1,00E+04	4,00E+10
Ra-227	1,00E+06	

Ra-228+	1,00E+05	3,00E+10
Ac-225		9,00E+10
Ac-227		4,00E+10
Ac-228	1,00E+06	3,00E+10
Th-226+	1,00E+07	
Th-227	1,00E+04	8,00E+10
Th-228+	1,00E+04	4,00E+10
Th-229+	1,00E+03	1,00E+10
Th-230	1,00E+04	7,00E+10
Th-231	1,00E+07	1,00E+13
Th-232nat	1,00E+03	
Th-234+	1,00E+05	2,00E+12
Pa-230	1,00E+06	1,00E+11
Pa-231	1,00E+03	6,00E+10
Pa-233	1,00E+07	4,00E+11
U-230+	1,00E+05	4,00E+10
U-231	1,00E+07	
U-232+	1,00E+03	6,00E+10
U-233	1,00E+04	7,00E+10
U-234	1,00E+04	1,00E+11
U-235+	1,00E+04	8,00E+07
U-236	1,00E+04	2,00E+11
U-237	1,00E+06	
U-238+	1,00E+04	
U-238nat	1,00E+03	
U-239	1,00E+06	
U-240	1,00E+07	
U-240+	1,00E+06	
U Wzb. 10-20%		8,00E+08
U Wzb. >20 %		8,00E+07
Np-235		1,00E+14
Np-236		7,00E+09
Np-236		8,00E+11
Np-237+	1,00E+03	7,00E+10
Np-239	1,00E+07	5,00E+11
Np-240	1,00E+06	
Pu-234	1,00E+07	
Pu-235	1,00E+07	
Pu-236	1,00E+04	1,00E+11
Pu-237	1,00E+07	2,00E+12
Pu-238	1,00E+04	6,00E+10
Pu-239	1,00E+04	6,00E+10
Pu-240	1,00E+03	6,00E+10
Pu-241	1,00E+05	3,00E+12
Pu-242	1,00E+04	7,00E+10

Pu-243	1,00E+07	
Pu-244	1,00E+04	3,00E+08
Am-241	1,00E+04	6,00E+10
Am-242	1,00E+06	
Am-242m+	1,00E+04	3,00E+11
Am-243+	1,00E+03	2,00E+11
Am-244		9,00E+10
Cm-240		3,00E+11
Cm-241		1,00E+11
Cm-242	1,00E+05	4,00E+10
Cm-243	1,00E+04	2,00E+11
Cm-244	1,00E+04	5,00E+10
Cm-245	1,00E+03	9,00E+10
Cm-246	1,00E+03	2,00E+11
Cm-247	1,00E+04	1,00E+09
Cm-248	1,00E+03	5,00E+09
Bk-247		8,00E+10
Bk-249	1,00E+06	1,00E+13
Cf-246	1,00E+06	
Cf-248	1,00E+04	1,00E+11
Cf-249	1,00E+03	1,00E+11
Cf-250	1,00E+04	1,00E+11
Cf-251	1,00E+03	1,00E+11
Cf-252	1,00E+04	2,00E+10
Cf-253	1,00E+05	4,00E+11
Cf-254	1,00E+03	3,00E+08
Es-253	1,00E+05	
Es-254	1,00E+04	
Es-254m	1,00E+06	
Fm-254	1,00E+07	
Fm-255	1,00E+06	
Pu-239/Be-9		6,00E+10
Am-241/Be-9		6,00E+10

Załącznik II

OPIS ŚRODKÓW ORGANIZACYJNO – TECHNICZNYCH ZABEZPIECZENIA ŹRÓDEŁ PROMIENIOTWÓRCZYCH

Zalecane środki organizacyjno-techniczne zabezpieczenia, których część opisano w punkcie 6. wyjaśniono poniżej.

1. KONTROLA DOSTĘPU

Kontrolę dostępu przeprowadza się za pomocą wejściowych punktów kontrolnych, obsługiwanych przez pracowników jednostki organizacyjnej lub zewnętrzną firmę (np. ochroniarską), czytników kart magnetycznych lub specjalnych kluczy. Wyróżnia się szereg automatycznych systemów kontroli dostępu (*automatic access control systems*, AACS): od zwykłych urządzeń mechanicznych obsługiwanych przyciskami, do złożonych czytników, które reagują na klucze zbliżeniowe lub osobiste cechy biometryczne. Stosowane wraz z bramkami obrotowymi mogą również obejmować systemy kontroli, które nie pozwalają na takie praktyki jak: przekazywanie klucza osobie następnej lub przechodzenie kilku osób przy jednorazowym użyciu tego samego klucza. W większości przypadków zastosowanie karty powinno być weryfikowane numerem PIN wprowadzonym do czytnika, a w przypadkach wymagających wysokiego poziomu zabezpieczenia wejścia AACS powinny być dozorowane przez strażnika. Kluczowym czynnikiem dla kierowników jednostek organizacyjnych jest określenie AACS, które są odpowiednie do wymagań, i które mogą być wspierane lokalnie przez producenta lub instalatora. Ważną kwestią jest również ograniczenie dostępu do komputerów i oprogramowania zarządzających AACS, aby zapobiec nieupoważnionej ingerencji w bazę danych systemu. W przypadkach, gdy stosuje się zwykły zamek i klucz jako środki kontroli dostępu, zamki powinny być dobrej jakości, a procedury zarządzania kluczami należy opracować tak, aby zapobiec nieupoważnionemu dostępowi.

2. KRATY

Metalowe kraty, klatki lub pojemniki mogą być zastosowane, aby oddzielić i zabezpieczyć źródła.

3. SYSTEM ALARMOWY

Na rynku dostępnych jest wiele systemów alarmowych o różnej funkcjonalności, wyposażonych w różnego rodzaju czujki. System alarmowy pozwala pracownikom (jednostki organizacyjnej lub firmy „ochroniarskiej") zaangażowanym w realizację zadań związanych z zabezpieczeniem na monitorowanie zewnętrznych obszarów, obiektów oraz miejsc, w których źródła promieniotwórcze są przechowywane. System alarmowy może wykorzystywać kamery razem z systemem wykrywania nieautoryzowanego dostępu, szczególnie w celu oceny zdarzenia aktywującego działanie systemu. Należy regularnie sprawdzać działanie kamer oraz monitorów, aby zagwarantować pełną skuteczność systemu, a w szczególności, aby zapewnić dobrą jakość wyświetlanego obrazu.

4. KOMUNIKACJA

Pracownicy wszystkich szczebli, realizujący zadania związane z zabezpieczeniem, powinni być wyposażeni w skuteczne i niezawodne urządzenia komunikacyjne, które zapewniają:

- komunikację pomiędzy patrolami, budkami strażniczymi,
- raportowanie: lokalne i do centrum kontroli,
- komunikację z odpowiedzialnymi za szybkie reagowanie na zagrożenie bezpieczeństwa komórkami zewnętrznymi (jeśli takim zostały powierzone zadania związane z zabezpieczeniem).

5. OGRODZENIA I BRAMY

Stosowany rodzaj ogrodzenia powinien być odpowiedni do zagrożenia, charakteru zabezpieczanego źródła i ogólnej charakterystyki obszaru, obiektu lub innego miejsca, w którym znajdują się źródła promieniotwórcze. Istnieją różnego rodzaju ogrodzenia, począwszy od takich, które tylko oddzielają teren, do takich, które mają mocną konstrukcję i które można połączyć ze środkami wykrywania wtargnięcia oraz systemem kontroli lub panelami pod napięciem. Ogrodzenie należy regularnie sprawdzać pod kątem stanu materiału i uszkodzeń lub prób ingerencji. Bramy w ogrodzeniu należy skonstruować tak, by prezentowały porównywalny standard do ogrodzenia i były zabezpieczone odpowiednimi zamkami dobrej jakości.

6. PROCEDURY ZABEZPIECZANIA KLUCZY

Klucze, które pozwalają na dostęp do źródeł promieniotwórczych, powinny być zabezpieczone i pod stałą kontrolą. Mogą to być klucze do krat lub drzwi do pomieszczeń z pojemnikami, w których znajdują się źródła promieniotwórcze. Podobne poziomy kontroli należy zastosować do kluczy zapasowych i dodatkowych kompletów.

7. ZAMKI, ZAWIASY I BLOKADY DRZWI

Zamki stosowane do zabezpieczenia źródeł promieniotwórczych powinny być dobrej jakości, wyposażone w rozwiązania, które stawiają opór podczas wyważania. To samo dotyczy zawiasów drzwi. Klucze powinny być chronione w sposób określony w punkcie 6. W obrębie obiektu blokady drzwi, które spełniają wymagania bezpieczeństwa (certyfikaty), mogą pełnić odpowiednią funkcję zabezpieczenia, przez kontrolowanie ruchu pracowników, pozwalając obsłudze na monitorowanie dostępu do obiektu.

8. ZAMKNIĘTE I OSŁONIĘTE POJEMNIKI

Stacjonarne pojemniki zawierające źródła promieniotwórcze mogą zapewniać zabezpieczenie i opóźniać próbę nieuprawnionego usunięcia źródeł. Jednakże, gdy członkowie obsługi są nieobecni, obszar, obiekt lub inne miejsce, w którym znajdują się źródła, powinny być objęte systemem alarmowym wykrywającym wtargnięcie, aby informować personel reagowania o potrzebie sprawdzenia okoliczności wtargnięcia.

9. KONSERWACJA I SPRAWDZANIE ŚRODKÓW TECHNICZNYCH ZABEZPIECZEŃ

W środkach technicznych zabezpieczenia pokłada się znaczne zaufanie, gdyż stanowią one wczesne ostrzeżenie o próbie wejścia lub wejściu osoby nieupoważnionej na teren obiektu, do obszaru lub innego zabezpieczanego miejsca. Środki techniczne stosowane w zabezpieczeniu źródeł promieniotwórczych powinny być precyzyjnie określone, a ich działanie po zamontowaniu należycie sprawdzone. Ponadto, należy przeprowadzać regularną konserwację tych środków przy pomocy wykwalifikowanych pracowników.

10. SYSTEMY PRZEPUSTEK

System przepustek jest efektywnym sposobem zabezpieczenia obszaru (jak również obiektu lub innego miejsca) przed przebywaniem na nim osób nieuprawnionych. Przepustki należy sprawdzać w momencie wejścia do obiektu; powinny być noszone w widocznym miejscu, aby potwierdzać upoważnienie i ułatwiać identyfikację. System przepustek może być łączony z innymi systemami kontroli dostępu.

11. ZAPEWNIENIE JAKOŚCI

Procedury zabezpieczeń należy przygotować, udokumentować i utrzymywać w zgodzie z zalecanymi normami zapewnienia jakości. Obowiązek posiadania programów zapewnienia jakości wynika z Rozporządzenia Rady Ministrów z dnia 30 czerwca 2015 r. w sprawie dokumentów wymaganych przy składaniu wniosku o wydanie zezwolenia na wykonywanie działalności związanej z narażeniem na działanie promieniowania jonizującego albo przy zgłoszeniu wykonywania tej działalności.

13. OŚWIETLENIE OBIEKTU, OBSZARU LUB INNEGO MIEJSCA

Skuteczne oświetlenie obiektu, obszaru lub innego miejsca, w którym znajdują się źródła promieniotwórcze może znacznie przyczynić się do jego zabezpieczenia.

14. SPECJALNE DRZWI OCHRONNE I ZESTAWY DRZWI

Niektóre obiekty i pomieszczenia, w których znajdują się źródła promieniotwórcze, mogą być często opuszczane przez pracowników. W takich przypadkach, należy stosować drzwi o specjalnej konstrukcji, celem minimalizacji zagrożenia podczas nieobecności pracowników.

15. ZASILANIE AWARYJNE

Zabezpieczane obiekty, obszary, inne miejsca, w których znajdują się źródła promieniotwórcze, jak również środki techniczne zasilane prądem elektrycznym powinny być chronione przed spadkami napięcia lub całkowitą utratą zasilania elektrycznego. W tym celu, należy zastosować system zasilania bezprzerwowego (akumulatorowego) lub awaryjny agregat prądotwórczy, który uruchamia się automatycznie, gdy zostanie wykryte wahanie się poziomu zasilania. Zabezpieczenie w postaci akumulatorów ma tylko ograniczony czas działania, dlatego stanowi krótkotrwałe źródło zasilania awaryjnego.

16. MURY

Mury stanowią kosztowną metodę otoczenia terenu, jeśli wymagają wybudowania. Wadą istniejących murów jest to, że personel reagowania nie widzi nic poza obszarem chronionym.

Załącznik III

PRZYKŁADOWA ZAWARTOŚĆ PLANU ZABEZPIECZENIA ŹRÓDEŁ

Poziom szczegółowości Planu powinien być współmierny do poziomu zabezpieczenia źródła/eł nim objętych. Najczęściej należy zawrzeć następujące elementy:

— opis źródła, kategoryzację i zastosowanie;
— opis środowiska, obszaru, obiektu lub miejsca, w którym źródło jest stosowane, przetwarzane, wytwarzane lub przechowywane i, jeśli istnieje taka potrzeba, schemat obiektu i systemu zabezpieczenia;
— lokalizację obszaru, obiektu lub innego miejsca gdzie znajdują się źródła promieniotwórcze względem obszarów dostępnych dla ludności;
— opis zdarzeń zagrażających osiągnięciu zaplanowanego poziomu zabezpieczenia;
— procedury opisujące działania podejmowane przez pracowników jednostki organizacyjnej (lub innej, której zlecono zadania związane z zabezpieczeniem) w odpowiedzi na scenariusze zdarzeń zagrażających utrzymaniu danego poziomu zabezpieczenia;
— cele Planu zabezpieczenia dla konkretnego obszaru, obiektu lub innego miejsca, w którym znajdują się źródła promieniotwórcze, w tym:
  • działania mające zapobiec dokonaniu działań szkodzących;
  • rodzaj wymaganej kontroli/atestacji wyposażenia pomocniczego;
  • opis wyposażenia i terenu podlegającego zabezpieczeniu;
— zastosowane środki zabezpieczenia, w tym:
  • środki zabezpieczenia zapewniające nadzór, kontrolę dostępu, wykrywanie, opóźnianie, reagowanie i komunikację;
  • opisy ww. środków umożliwiające dokonanie oceny ich jakości i skuteczności przeciwko potencjalnemu zagrożeniu;
— zastosowane środki administracyjne, w tym:
  • role i obowiązki związane z zabezpieczeniem wyznaczone dla zarządu, pracowników i innych osób;
  • rutynowe i nierutynowe działania, w tym ewidencjonowanie źródeł lub odwołanie do dokumentu zawierającego informacje o tych działaniach i systemie ewidencji;
  • konserwacja i sprawdzanie wyposażenia;
  • określanie wiarygodności pracowników;
  • stosowanie ochrony informacji;
  • metody upoważniania do dostępu;
  • szkolenia;
  • procedury zabezpieczania kluczy.
— procedury odnoszące się do podwyższonego poziomu zagrożenia;
— proces okresowej oceny skuteczności Planu i jego odpowiedniej aktualizacji;
— odniesienia do istniejących przepisów lub norm.