

# Jędrzej Łukasiewicz

---

## Rola państwa i operatora w zapewnieniu bezpieczeństwa obiektów, instalacji jądrowych i źródeł radioaktywnych oraz procedura oceny ich zagrożenia w Polsce w świetle zaleceń i rekomendacji Międzynarodowej Agencji Energii Atomowej

---

Przegląd Naukowo-Metodyczny. Edukacja dla Bezpieczeństwa nr 1, 17-32

---

2014

Artykuł został opracowany do udostępnienia w internecie przez Muzeum Historii Polski w ramach prac podejmowanych na rzecz zapewnienia otwartego, powszechnego i trwałego dostępu do polskiego dorobku naukowego i kulturalnego. Artykuł jest umieszczony w kolekcji cyfrowej [bazhum.muzhp.pl](http://bazhum.muzhp.pl), gromadzącej zawartość polskich czasopism humanistycznych i społecznych.

Tekst jest udostępniony do wykorzystania w ramach dozwolonego użytku.

**Jędrzej ŁUKASIEWICZ**  
Politechnika Poznańska

**ROLA PAŃSTWA I OPERATORA W ZAPEWNIENIU BEZPIECZEŃSTWA  
OBIEKTÓW, INSTALACJI JĄDROWYCH I ŹRÓDEŁ RADIOAKTYWNYCH  
ORAZ PROCEDURA OCENY ICH ZAGROŻENIA W POLSCE  
W ŚWIETLE ZALECEŃ I REKOMENDACJI MIĘDZYNARODOWEJ  
AGENCJI ENERGII ATOMOWEJ**

28 stycznia 2014 r. Rada Ministrów podjęła uchwałę o dalszym rozwoju polskiej energetyki jądrowej.<sup>1</sup> Sam program został przygotowany w Ministerstwie Gospodarki RP i przewiduje zbudowanie dwóch elektrowni jądrowych wraz z przygotowaniem całej infrastruktury regulacyjnej i organizacyjnej. Doświadczenia państw posiadających już instalacje jądrowe pokazuje, że na przygotowanie infrastruktury oraz zakończenie budowy elektrowni jądrowej potrzeba około 10 do 15 lat. Okres ten należy wykorzystać nie tylko na przygotowanie infrastruktury regulacyjnej i organizacyjnej ale także na wyszkolenie osób odpowiedzialnych za bezpieczeństwo i ochronę antyterrorystyczną obiektów, urządzeń jądrowych oraz materiałów rozszczepialnych.

W Polsce zbudowano do celów naukowych instalacje jądrowe w Świerku koło Warszawy oraz Krajowe Składowisko Odpadów Promieniotwórczych w miejscowości Różan. Istnieje też wiele laboratoriów i innych operatorów wykorzystujących źródła promieniotwórcze. Niestety, w Polsce nigdy nie uruchomiono elektrowni jądrowej i nie ma kadr z doświadczeniem w ochronie tak dużych obiektów jądrowych. Dlatego bezpieczeństwo obiektów i instalacji jądrowych a także materiałów radioaktywnych musi być zapewnione w oparciu o rekomendacje i zalecenia Międzynarodowej Agencji Energii Atomowej.

Ochrona obiektów, urządzeń i materiałów rozszczepialnych ma dla każdego państwa szczególne znaczenie ze względu na potencjalne skutki dla społeczeństwa i opłacalności ekonomicznej inwestycji jądrowych. Przykładem poniesienia strat materialnych wynikających z ataków terrorystycznych na obiekty jądrowe może być utrata zainwestowanych pieniędzy w skutek wstrzymania w 1983 r. budowy elektrowni jądrowej w hiszpańskim Lemoniz.<sup>2</sup> Elektrownia budowana była przez największy koncern energetyczny w Hiszpanii Iberdrola. Ataki przeprowadzone na ten obiekt prowadzone głównie przez baskijską organizację ETA rozpoczęły się w grudniu 1977 r. kiedy to bojówka ETA raniła strażnika który w skutek poniesionych obrażeń zmarł. W marcu 1978 r. ETA przeprowadziła kolejny zamach bombowy raniąc dwóch pracowników, zabijając dwóch kolejnych i doprowadzając do opóźnienia budowy wskutek zniszczeń już zbudowanych obiektów. W czerwcu 1979 roku bojownicy ETA zdetonowali ładunek wybuchowy niszcząc turbiny parowe elektrowni i powodując śmierć kolejnego pracownika elektrowni. Ostatecznie koncern Iberdrola zdecydował o wstrzymaniu

---

<sup>1</sup> Projekt uchwały Rady Ministrów w sprawie programu wieloletniego po nazwą „Program polskiej energetyki jądrowej”, <http://bip.krpm.gov.pl>, (pobrano 28.01.2014 r.)

<sup>2</sup> L. Mez, M. Schneider and S. Thomas. *International Perspectives of Energy Policy and the Role of Nuclear Power*, Multi-Science Publishing Co. Ltd, p. 371

inwestycji po porwaniu i zabójstwie dyrektora budowy. Obecnie betonowe budynki budowane dla potrzeb energetyki jądrowej stanowią ruinę podobną do ruiny polskiej elektrowni w Żarnowcu.

Do skutków społecznych można zaliczyć zmiany preferencji wyborczych zaatakowanego społeczeństwa, wzrost nieufności do mniejszości religijnych i etnicznych, wzrost aktywności ugrupowań skrajnie prawicowych lub lewicowych i wzrost poparcia dla militarnych prób rozbicia grup terrorystycznych. Jako przykład zmian preferencji politycznych na skutek zamachów terrorystycznych można wskazać upadek hiszpańskiego rządu Jose Marii Aznara po zamachu w dniu 11 marca 2004 na madryckie koleje. Przed zamachem sondaże wskazywały delikatną równowagę między rządzącą partią a partiami opozycyjnymi natomiast po zamachu rządząca partia została obarczona odpowiedzialnością za tragedię i wybory przegrała. Wzrost poparcia dla walki z terrorem można obserwować na przykładzie reakcji obywateli USA na ataki na budynki WTC.

### **Instalacje jądrowe jako cel ataku**

Instalacje, obiekty i materiały rozszczepialne wydają się być dla terrorystów szczególnie atrakcyjnym celem ataku. Przyczyny tego stanu są dobrze znane i opisane w literaturze<sup>3</sup> i można do nich zaliczyć:

- Szczególna pozycja przemysłu jądrowego w państwie. Tylko państwa bogate i dobrze rozwinięte technologicznie są w stanie zbudować i użytkować instalacje jądrowe. Tylko państwa bogate i rozwinięte technologicznie są w stanie zapewnić takim instalacjom bezpieczeństwo i ochronę antyterrorystyczną. Dla terrorysty skuteczny atak wydaje się być zatem szczególnie cennym osiągnięciem ze względu na zachwianie pozycji państwa w Świecie oraz ze względu na podważenie zaufania obywateli do władz państwowych;
- Konsekwencje użycia materiałów radioaktywnych. Użycie materiałów rozszczepialnych przez terrorystów niesie za sobą znaczące konsekwencje dla społeczeństwa oraz środowiska naturalnego. Skutki działania materiałów rozszczepialnych można ocenić na podstawie wypadków w elektrowni Three Mile Island w USA, w elektrowni Czarnobyl w Związku Radzieckim oraz ostatnio w elektrowni Fukushima Dai-Ichi w Japonii. Zanotowano skażenie dużych obszarów dookoła elektrowni, przypadki śmierci w skutek choroby popromiennej, zmiany genetyczne nowo narodzonych dzieci. Podobny wpływ na środowisko naturalne i społeczność zamieszkującą skażony obszar miałby skuteczny atak terrorystyczny na obiekty i instalacje jądrowe lub atak terrorystyczny z użyciem materiałów radioaktywnych;
- Wpływ energetyki jądrowej na kondycję ekonomiczną państwa. Idealnym modelem zasilania energią elektryczną jest model w którym elektrownie jądrowe są tylko jednym z wielu wzajemnie alternatywnych źródeł elektryczności w państwie. Są państwa np. USA w których ten model jest implementowany, ale są też państwa np. Francja w których energetyka

---

<sup>3</sup> On the Need to Strengthen Nuclear Security Culture in View of New Security Risks. (w:) I. Khripunov et al., *Nuclear Security Culture: From National Best Practices to International Standards*. IOS Press 2007, 56-57

jądrowa ma pozycję ściśle dominującą. Atak na elektrownie jądrowe w takich państwach może doprowadzić do przerwania produkcji i dużych strat finansowych (patrz tabela nr 1);

**Tabela nr 1:** Zestawienie procentowego udziału różnych źródeł energii w USA<sup>4</sup> i Francji.<sup>5</sup>

ŹRÓDŁO ENERGII	USA (dane na 2012 r.)	FRANCJA (dane na 2014 r.)
węgiel	37 %	2 %
gaz ziemny	30 %	3 %
energia jądrowa	19 %	76 %
energia wody	7 %	13 %
inne źródła odnawialne	5 %	6 %
paliwa i oleje	1 %	< 1%
inne	< 1%	1 %

**Źródło:** U.S. Energy Information Administration, RTE, le Réseau de la Transition Energetique.

- Militarne znaczenie energetyki jądrowej. Niektóre państwa budują swoje znaczenie polityczne na arenie międzynarodowej w oparciu o posiadaną broń jądrową. Broń jądrową buduje się wykorzystując wzbogacony uran lub pluton. Atak terrorystyczny na zakłady wzbogacania uranu lub miejsca produkcji głowic jądrowych byłaby prestiżową porażką dla państwa i zmuszałaby do zadania pytania o rzeczywisty potencjał takiego państwa.

#### **Zagrożenie dla przemysłu jądrowego na Świecie i w Polsce**

Największą, międzynarodową organizacją zajmującą się zdarzeniami związanymi z obiektami, instalacjami jądrowymi oraz z materiałami rozszczepialnymi w tym z ich nielegalnym pozyskaniem i posiadaniem, a także z nielegalnym transportem i przemytem materiałów rozszczepialnych jest Międzynarodowa Agencja Energii Atomowej (MAEA). Zgodnie ze Statutem MAEA za materiały rozszczepialne uważa się zarówno te występujące naturalnie, jak i uzyskane w wyniku produkcji. W ramach MAEA utworzono w 1995 roku bazę danych (Incident and Trafficking Database) zawierającą informacje zgłoszone przez państwa ją współtworzące.<sup>6</sup> Na dzień 12 grudnia 2012r. państw, członków ITDB było 120, a jednym z państw członkowskich była Polska. Dane zawarte w ITDB są niejawnie i jako takie są udostępniane tylko oficjalnym przedstawicielom państw członkowskich na ich żądanie. Niemniej jednak pewne ogólne dane dotyczące przemytu, nielegalnego transportu, kradzieży, zagubienia lub innych nielegalnych działań z wykorzystaniem materiałów radioaktywnych podaje się do publicznej wiadomości. Jak informuje MAEA do dnia 31 grudnia 2012,

<sup>4</sup> U.S. Energy Information Administration.

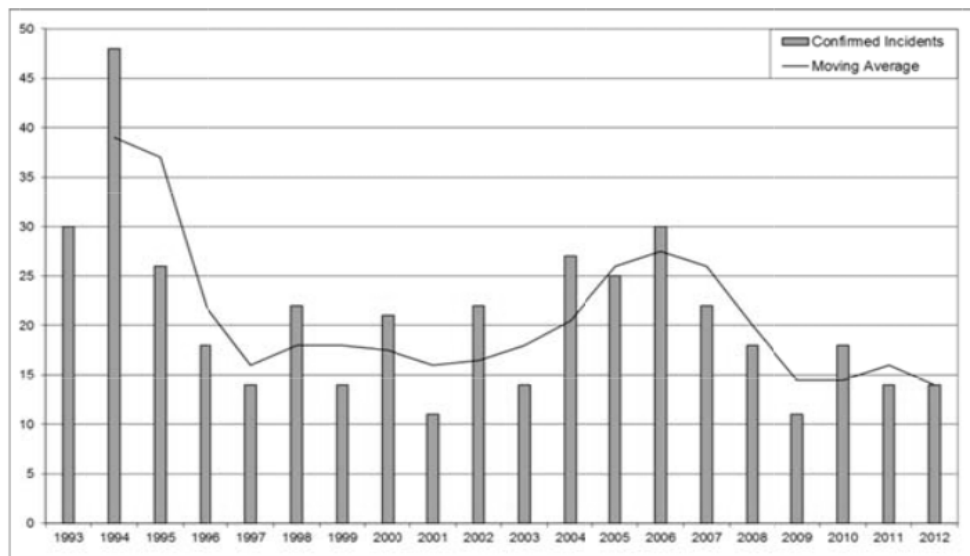
<sup>5</sup> RTE, le Réseau de la Transition Energetique.

<sup>6</sup> <http://www-ns.iaea.org/security/itdb.asp>

zarejestrowano 2331 zdarzeń zgłoszonych przez państwa członkowskie. Wśród wszystkich zgłoszonych zdarzeń można wyróżnić:

- 419 przypadki nielegalnego posiadania materiałów rozszczepialnych i związanej z nimi działalności kryminalnej;
- 615 przypadków kradzieży lub zagubienia materiałów rozszczepialnych;
- 1244 inne przypadki nielegalnej działalności z wykorzystaniem materiałów rozszczepialnych;
- 69 przypadków których ocena nie pozwalała na jednoznaczne określenie kategorii zdarzenia.

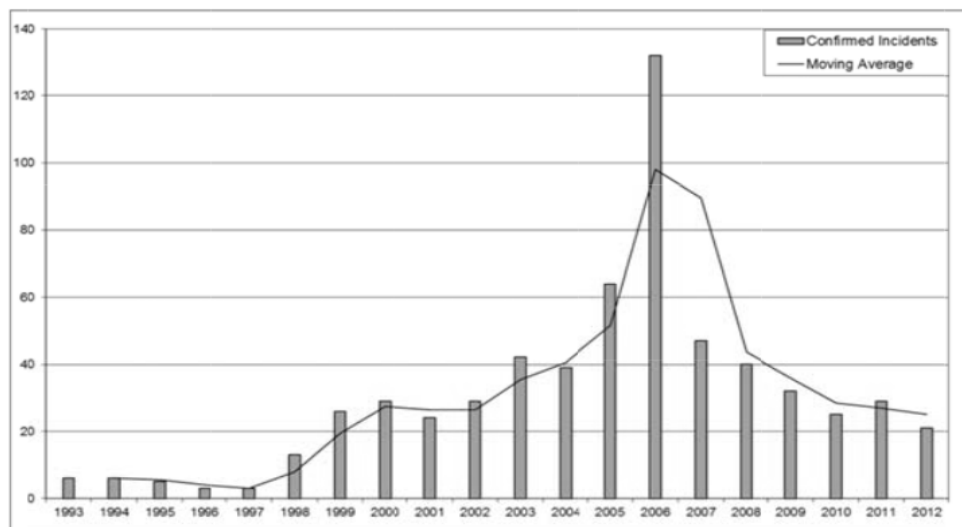
**Rysunek nr 1:** Zestawienie ilości zdarzeń związanych z nielegalnym posiadaniem materiałów radioaktywnych oraz związanych z tymi materiałami działań o charakterze kryminalnym w latach 1993-2012.



**Źródło:** MAEA Incident and Trafficking Database (ITDB), 2013 Fact Sheet.

Rysunek nr 1 pokazuje całkowitą liczbę notowanych zdarzeń związanych z nielegalnym posiadaniem materiałów radioaktywnych oraz związanych z tymi materiałami działań o charakterze kryminalnym zgłoszonych przez państwa, członków ITDB. Maksimum ilości zdarzeń zanotowano w roku 1994. Stosunkowo dużą liczbę zdarzeń z wykorzystaniem materiałów radioaktywnych zanotowano także w roku 2006, ale jak wskazują statystyki od tego momentu średnia liczba notowanych zdarzeń systematycznie spada. Jak informuje MAEA pewna ilość prób nielegalnych sprzedaży i zakupów materiałów radioaktywnych pokazuje, że istnieje zapotrzebowanie na tego typu materiały. Nie jest znana liczba transakcji które doszły do skutku.

**Rysunek nr 2:** Zestawienie ilości zdarzeń związanych z kradzieżą lub zagubieniem materiałów radioaktywnych w latach 1993-2012.



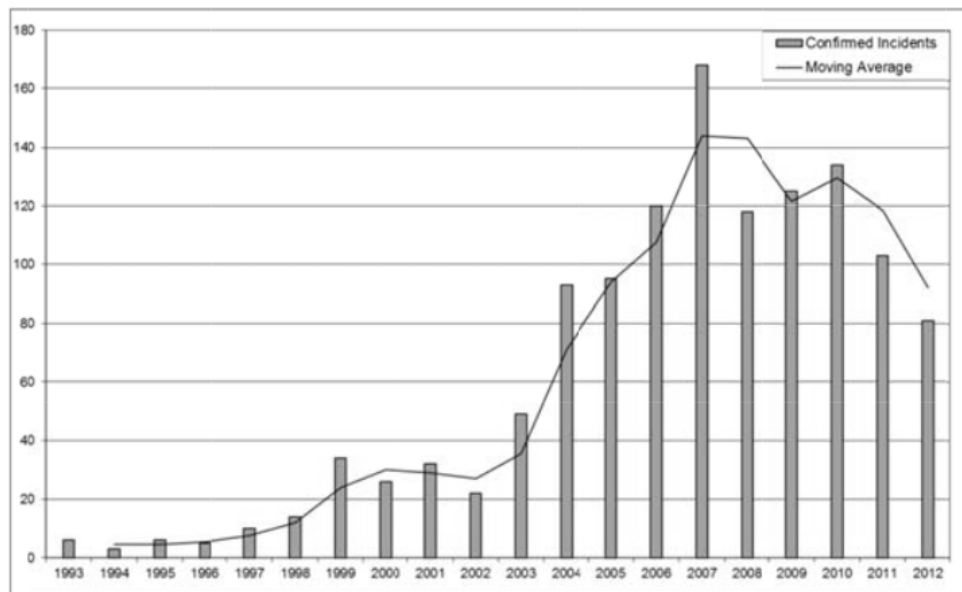
**Źródło:** MAEA Incident and Trafficking Database (ITDB), 2013 Fact Sheet.

Rysunek nr 2 prezentuje całkowitą ilość kradzieży materiałów radioaktywnych w obiektach lub instalacjach jądrowych oraz zagubień materiałów radioaktywnych w czasie transportu. Akt kradzieży można uznać za początek procesu nielegalnego transportu. Prezentowany rysunek wskazuje na rosnącą w latach 1993 do 2006 liczbę kradzieży i zagubień po czym od roku 2006 ilość tego typu zdarzeń systematycznie spada. Zgodnie z informacjami udostępnionymi przez MAEA ww. zdarzenia dotyczą głównie materiałów radioaktywnych wykorzystywanych w przemyśle lub w medycynie. Należy pamiętać, że tego typu źródła należą do grupy materiałów o długim czasie połowicznego rozpadu. Zanieczyszczenie środowiska takim materiałem skutkuje długotrwałym zamknięciem zanieczyszczonego obszaru dla ludzi lub kosztownym procesem dekontaminacji. Analiza ilości zdarzeń związanych ze źródłami radioaktywnymi stosowanymi w przemyśle pozwala na wyciągnięcie wniosków na temat stopnia skuteczności systemów fizycznej ochrony źródeł oraz procedur bezpieczeństwa obowiązujących w danym przedsiębiorstwie. MAEA nie udostępnia danych dotyczących przypadków kradzieży lub nielegalnego transportu materiałów radioaktywnych. Na podstawie informacji prasowych wiadomo, że w Polsce w ciągu ostatnich dwóch lat zanotowano dwa przypadki zaginięcia materiałów radioaktywnych. Pierwsze zaginięcie zauważono 22 listopada 2013 roku w Elektrowni Bełchatów w której zaginęły dwa pojemniki z Kobaltem-60 o aktywności 1,08GBq oraz 2,43 GBq.<sup>7</sup> 15 stycznia 2014 stwierdzono kolejne zaginięcie pojemnika z Kobaltem-60 tym razem w Koniecpolskich Zakładach Płyt Piłśniowych.<sup>8</sup>

<sup>7</sup> <http://www.nuclear.pl/wiadomosci,news,13120101.html>

<sup>8</sup> <http://www.nuclear.pl/wiadomosci,news,14011702.html>

**Rysunek nr 3:** Zestawienie ilości innych przypadków nielegalnej działalności z wykorzystaniem materiałów rozszczepialnych.



Źródło: MAEA Incident and Trafficking Database (ITDB), 2013 Fact Sheet.

Ta kategoria zdarzeń obejmuje np. przypadki przewożenia przez granice państwa skażonych, radioaktywnych odpadów poprodukcyjnych oraz znalezienie radioaktywnych źródeł pozostających bez kontroli. Jak wskazuje wykres liczba zgłaszanych incydentów rosła aż do 2007 roku po czym nastąpił stopniowy spadek zgłoszeń. Materiały radioaktywne pozostające bez kontroli odkrywane są głównie na złomowiskach a ich pochodzenie określa się jako materiały przemysłowe.

#### **Metody wykorzystania materiałów radioaktywnych przez terrorystów**

Istnieją trzy podstawowe sposoby wykorzystania materiałów rozszczepialnych w działaniach terrorystycznych. Najmniej prawdopodobnym scenariuszem jest zbudowanie bomby jądrowej. Budowa bomby wymaga spełnienia kilku warunków w tym:

- posiadania odpowiedniej ilości, wysoko wzbogaconego materiału rozszczepialnego;
- posiadania zaplecza technicznego pozwalającego na wykonanie mechanicznych elementów bomby;
- posiadania wiedzy i doświadczenia pozwalającego na skonstruowanie mechanizmu ściskającego materiał radioaktywny w niezwykle krótkim czasie rzędu  $10^{-8}$ s.<sup>9</sup>

<sup>9</sup> J. Kubowski, *Broń Jądrowa*, WNT. Warszawa 2008, 67-68

Wysoko wzbogaconego materiału nie da się otrzymać metodami chałupniczymi i już sam ten fakt prowadzi do wniosku, że bez pomocy państwa mającego zaplecze technologiczne i wspierającego grupy terrorystyczne budowa bomby nie jest możliwa. Materiały rozszczepialne oraz ich masy krytyczne które potencjalnie można wykorzystać do budowy bomby jądrowej zestawiono w tabelce nr 2.

**Tabela nr 2:** Zestawienie materiałów rozszczepialnych i ich mas krytycznych wymaganych do budowy bomby jądrowej.

Materiał rozszczepialny	Masa krytyczna [kg]
Uran-233	16,5
Uran-235	48,0
Neptun-237	64,4
Pluton-238	9,8
Pluton-239	10,2
Pluton-240	37,6
Pluton-241	13,1
Pluton-242	90,3
Ameryk-241	57,5
Ameryk-243	150,2

**Źródło:** N. N. Ponomarev-Stepnoy, A. N. Romyantsev, A. A. Andrianov. Approaches to and Methods for Quantitive Assessment of Nuclear Proliferation Risk, MEPhI 2011, s. 7-8

Ocenia się, że w państwach atomowych zgromadzone są zapasy wysoko wzbogaconego materiału z którego można zbudować ok. 300 tysięcy bomb.<sup>10</sup>

Drugim sposobem wykorzystania materiałów radioaktywnych jest zbudowanie tzw. brudnej bomby określanej angielskim skrótem RDD (Radiological Dispersal Device). Za brudną bombę uważa się każde urządzenie które w wyniku detonacji konwencjonalnego materiału wybuchowego np. ANFO<sup>11</sup> prowadzi do rozrzucenia i w konsekwencji skażenia terenu materiałem radioaktywnym bez wybuchu jądrowego.

Detonacja brudnej bomby może prowadzić do:

- Skażenie radioaktywnego zaatakowanego obszaru i/lub osób;
- spowodowania urazów mechanicznych i ran w wyniku uderzenia odłamkami konwencjonalnego urządzenia wybuchowego;
- wywołania pożaru;
- spowodowania urazów psychicznych, wywołania strachu i/lub paniki;
- spowodowania strat finansowych.

<sup>10</sup> N. N. Ponomarev-Stepnoy, A. N. Romyantsev, A. A. Andrianov. Approaches to and Methods for Quantitive Assessment of Nuclear Proliferation Risk, MEPhI 2011, 7-8

<sup>11</sup> M. Kurzun, *1000 słów o materiałach wybuchowych i wybuchu*, Wydawnictwo MON. Warszawa 1986, s. 167-168



Trzecim sposobem wykorzystania materiału radioaktywnego w celach terrorystycznych jest umieszczenie takiego materiału w miejscu ukrytym ale takim by znajdujące się w okolicy tego źródła osoby nieświadomie uległy napromieniowaniu. Urządzenie z takim źródłem nazywamy Radiological Exposure Device (RED). Źródło takie może być ukryte w miejscu publicznym np. pod siedzeniem w autobusie, w restauracji, kościele itd., czyli w każdym miejscu, gdzie zbiera się duża grupa ludzi. Tego typu atak może być potencjalnie bardzo groźny, a materiał radioaktywny wykorzystany w ataku będący zazwyczaj emitерem cząstek alfa można łatwo ukryć i przemyścić.<sup>12</sup>

Lista izotopów, które potencjalnie można wykorzystać w budowie brudnej bomby jest dość długa.<sup>13</sup> Wybrane izotopy mogące być użyte w budowie brudnej bomby zestawiono w tabeli nr 3.

**Tabela nr 3:** Zestawienie wybranych izotopów które można wykorzystać w budowie brudnej bomby.<sup>14</sup>

Izotop	Rozpad
Ameryk-241	$\alpha$ $\gamma$
Kaliforn-252	$\alpha$
Cez-137	$\beta$ $\gamma$
Kobalt-60	$\beta$ $\gamma$
Iryd-192	$\beta$ $\gamma$
Pluton-238	$\alpha$ $\gamma$
Polon-210	$\alpha$ $\gamma$
Rad-226	$\alpha$ $\beta$ $\gamma$
Stront-90	$\beta$

**Źródło:** Argonne National Laboratory Environmental Science Division.

Użytkownicy materiałów radioaktywnych w Polsce i posiadane przez nich źródła.<sup>15</sup>

Państwowa Agencja Atomistyki zarejestrowała 3228 (stan na 31 grudnia 2012) jednostek organizacyjnych, których działalność wiąże się z narażeniem na promieniowanie jonizujące. Jednostki te mogą prowadzić jednocześnie kilka różnych działalności stąd liczba zarejestrowanych działalności jest większa i wynosi 4624.

<sup>12</sup> J. M. Acton, M. B. Rogers and P. D. Zimmerman, Beyond the Dirty Bomb: Re-thinking Radiological Terror. Survival, vol. 49 no. 3, Autumn 2007, 151-168

<sup>13</sup> Radiological and Chemical Fact Sheets to Support Health Risk Analyses For Contaminated Areas, Argonne National Laboratory Environmental Science Division, U.S. Department of Energy, 2007

<sup>14</sup> Ibidem.

<sup>15</sup> Raport roczny Prezesa Państwowej Agencji Atomistyki za 2012 rok.

**Tabela nr 4:** Zestawienie jednostek organizacyjnych prowadzących działalność związaną z narażeniem na promieniowanie jonizujące.

Rodzaj działalności jednostki organizacyjnej	Liczba jednostek
Weterynaryjny aparat rentgenowski	660
Urządzenie izotopowe	558
Transport źródeł i odpadów	408
Instalator czujek izotopowych	363
Skaner rentgenowski	345
Inny aparat rentgenowski	339
Chromatograf	218
Defektoskop rentgenowski	184
Instalator urządzeń	137
Pracownia klasy III	114
Aparat gammagraficzny	108
Pracownia klasy Z	89
Pracownia klasy II	83
Akcelerator	57
Obrót źródłami i urządzeniami izotopowymi	51
Prace ze źródłami w terenie	50
Urządzenie radiacyjne	36
Magazyn źródeł izotopowych	33
Aplikatory izotopowe	32
Produkcja urządzeń i źródeł izotopowych	21
Telegammaterapia	3
Pracownia klasy I	1

**Źródło:** Raport roczny Prezesa Państwowej Agencji Atomistyki za 2012 rok.

Państwowa Agencja Atomistyki prowadzi także rejestr zamkniętych źródeł promieniotwórczych. Wybrane izotopy zestawiono w tabeli nr 5.

**Tabela nr 5:** Zestawienie zamkniętych źródeł zawierających wybrane izotopy zarejestrowanych przez PAA.

Izotop	Liczba źródeł		
	Kategoria I	Kategoria II	Kategoria III
Kobalt-60	561	1171	2633
Iryd-192	222	42	1
Cez-137	69	338	2221
Selen-75	169	-	3
Ameryk-241	2	413	973
Plutonu-239	3	122	106
Rad-226	-	80	63
Stront-90	1	19	852
Pluton-238	-	77	19
Krypton-85	-	28	192
Tytan-204	-	-	93
inne	6	119	1339

**Źródło:** Raport roczny Prezesa Państwowej Agencji Atomistyki za 2012 rok.

Źródła kategorii I są to zamknięte źródła stosowane w teleradioterapii, radiografii przemysłowej i w technologiach radiacyjnych. Źródła kategorii II to zamknięte źródła stosowane w brachyterapii, geologii, radiografii przemysłowej. Źródła kategorii III to pozostałe źródła zamknięte stosowane w aparaturze kontrolno-pomiarowej.

Jak wskazują dane PAA w Polsce różne instytucje posiadają materiały rozszczepialne mogące potencjalnie być stosowane w budowie brudnej bomby. Zapewnienie bezpieczeństwa materiałów radioaktywnych należy zarówno do obowiązków państwa jak i do obowiązków operatora tych źródeł.

#### **Obowiązki państwa w zakresie ochrony materiałów radioaktywnych<sup>16</sup>**

Mając świadomość, że zagrożenie atakami terrorystycznymi istnieje zawsze, państwo ma obowiązek zdefiniować źródła potencjalnych zagrożeń. Ocena zagrożeń w państwie jest procesem wieloetapowym, angażującym różne instytucje i służby państwowe. Państwo odpowiada także za upewnienie się, że źródła radioaktywne znajdujące się na obszarze tego państwa znajdują się pod właściwą opieką, że są właściwie chronione i zabezpieczone. Wymienione powyżej czynności państwo realizuje na podstawie prawa. Zgodnie z zaleceniami MAEA:

- Państwo musi ustanowić właściwe ramy prawne które umożliwią bezpieczne użytkowanie materiałów radioaktywnych;

<sup>16</sup> MAEA Nuclear Security Series no. 11 Security of Radioactive Sources.

- prawo powinno umożliwić przekazanie części kompetencji państwa instytucjom i organizacjom rządowym które w imieniu tego państwa prowadzą nadzór nad bezpieczeństwem źródeł radioaktywnych. Do takich instytucji państwowych należy w Polsce np. Państwowa Agencja Atomistyki;
- prawo powinno także określać sposoby oceny, licencjonowania i egzekwowania zaleceń;
- system prawny powinien obarczać podstawową odpowiedzialnością za bezpieczeństwo materiałów radioaktywnych użytkownika tych materiałów;
- państwo określa metody minimalizujące prawdopodobieństwo podjęcia prób nieautoryzowanego użycia materiałów radioaktywnych;
- państwo także określa sposoby ograniczenia skutków nieautoryzowanego użycia materiałów radioaktywnych;
- do jednej z najważniejszych ról państwa w ochronie materiałów radioaktywnych należy ustanowienie prawa w którym nielegalne, agresywne użycie materiałów radioaktywnych będzie skutkowało surową karą.

Jest rzeczą oczywistą, że wprowadzenie reguł prawnych, a następnie ich przestrzeganie i kontrola zależą od współpracy wielu instytucji i służb państwowych. Do państwa należy zapewnienie tym instytucjom i służbom właściwych warunków pracy w tym dostęp do informacji, właściwe finansowanie i co wydaje się bardzo ważne niezależność decyzyjną.

#### **Obowiązki użytkownika w zakresie ochrony materiałów radioaktywnych<sup>17</sup>**

Zgodnie z zaleceniami MAEA Państwo obarcza użytkownika odpowiedzialnością za właściwe zabezpieczenie i zapewnienie bezpieczeństwa materiałów radioaktywnych. Sposób zapewnienia bezpieczeństwa zależy od ram prawnych w których użytkownik działa np. w Wielkiej Brytanii za ochronę miejsc, w których znajdują się duże ilości materiałów rozszczepialnych (elektrownie) odpowiada specjalna jednostka Policji, we Francji jest to służba cywilna której członkowie rekrutują się ze straży pożarnej, policji i wojsk specjalnych. W każdym przypadku użytkownik materiałów radioaktywnych musi upewnić się, że personel bezpośrednio chroniący te materiały jest godny zaufania i spełnia wymagania określone prawem. Do obowiązków użytkownika materiałów radioaktywnych należy także:

- Uznanie faktu, że bezpieczeństwo materiałów radioaktywnych jest priorytetowym zadaniem użytkownika i ustanowienie odpowiednich procedur kontroli tych materiałów;
- ustanowienie procedur identyfikacji potencjalnych zagrożeń, oceny ich wagi i sposobów ich likwidacji odpowiednich do ich znaczenia i wagi;
- określenie zakresu obowiązków każdej osoby odpowiedzialnej za bezpieczeństwo, a następnie przeszkolenia tej osoby w taki sposób by była ona zdolna do właściwego wypełniania obowiązków;
- precyzyjne ustalenie ścieżki decyzyjnej;

---

<sup>17</sup> Ibidem

- zdefiniowanie jasnych i czytelnych sposobów komunikacji umożliwiających szybki przepływ informacji między poszczególnymi jednostkami organizacji lub instytucji;
- określenie które informacje w organizacji są niejawne i muszą być chronione.

### Procedura oceny bezpieczeństwa materiałów radioaktywnych

Ocena zewnętrznego zagrożenia wszelkich obiektów, instalacji oraz miejsc przechowywania lub użytkowania materiałów radioaktywnych odbywa się według dobrze zdefiniowanego schematu postępowania.<sup>18</sup> Oceny dokonuje się przy współpracy odpowiednich służb i instytucji państwowych.

Pierwszym etapem definiowania zagrożenia jest analiza posiadanych informacji i dokumentacji opisujących potencjalne grupy terrorystyczne. Ocenie podlegają przyczyny potencjalnych ataków i motywacje, którymi mogłyby się kierować grupy planujące akt agresji. Do najczęstszych przyczyn ataków terrorystycznych należą: religijne, polityczne i separatystyczne,<sup>19</sup> ale należy także rozważyć przyczyny finansowe i konflikty personalne. Ocenie podlegają również dane historyczne opisujące terrorystyczną działalność badanych grup wraz z celami ich ataków.

Kolejnym czynnikiem podlegającym ocenie jest cel dokonania ataku. Określenie celu ataku należy rozpocząć od przypisania potencjalnym celom wartości liczbowej opisującej konsekwencje osiągnięcia danego celu przez napastników. Wartości te mieszczą się w przedziale liczbowym od 0 do 1.

**Tabela nr 6:** Przykładowe kategorie zdarzeń i przypisane im wartości liczbowe konsekwencji.

Kategoria zdarzenia	Wartość liczbowo konsekwencji
Bardzo znaczący wpływ na środowisko naturalne, przerwanie działania przedsiębiorstwa, śmierć człowieka	Bardzo wysoka 0.75 → 1
Duży wpływ na środowisko naturalne, chwilowe przerwy w pracy przedsiębiorstwa, powodują obrażenia zagrażające życiu, powodują rany lub długotrwałą chorobę	Wysoka 0.50 → 0.75
Średni wpływ na środowisko naturalne, niezbyt poważny wpływ na działalność przedsiębiorstwa, rany nie zagrażające życiu, chwilowe pogorszenie stanu zdrowia	Średnia 0.25 → 0.50
Mały wpływ na środowisko naturalne, minimalny wpływ na działalność przedsiębiorstwa, pomijalny wpływ na zdrowie ludzkie	Niska 0 → 0.25

**Źródło:** Department of Defence per Military Standard 882C, USA.

Dalsza analiza sprowadza się do określenia prawdopodobieństwa, że grupa terrorystyczna dokona ataku. Prawdopodobieństwo to określa się na podstawie analiz grupy terrorystycznej opisanych w innych podpunktach. Prawdopodobieństwo to przybiera wartość liczbową od 0 do 1. Wraz z określeniem

<sup>18</sup> M. L. Garcia, *Design and Evaluation of Physical Protection Systems*, Butterworth-Heinemann 2008.

<sup>19</sup> [economicsandpeace.org](http://economicsandpeace.org)

prawdopodobieństwa ataku określa się też prawdopodobieństwo odniesienia sukcesu przez grupę terrorystyczną. Prawdopodobieństwo to wyznacza się analizując techniczne systemy wykrycia i opóźnienia ataku oraz zbadania możliwości przerwania ataku przez zespół chroniący obiekt przed osiągnięciem celu przez napastników. Mając te dane można wyznaczyć ryzyko.<sup>20</sup>

$$RYZYKO = P_A \times P_S \times C$$

gdzie:

$P_A$  → prawdopodobieństwo ataku na wybrany obiekt, element instalacji lub materiał radioaktywny,

$P_S$  → prawdopodobieństwo, że atak się powiedzie,

$C$  → liczbowa wartość konsekwencji.

Znając ryzyko przypisane każdemu chronionemu obiektowi można teoretycznie określić, który z chronionych obiektów, elementów instalacji lub który z materiałów rozszczepialnych może być celem ataku.

W przypadku materiałów radioaktywnych można brać pod uwagę zarówno próby sabotażu dokonanego na obiektach i instalacjach jądrowych, jak i próby kradzieży materiału jądrowego. Wszelkie tego typu zdarzenia mogą prowadzić do wywołania określonych skutków w sferze politycznej Państwa, do utraty zaufania do instytucji rządowych, do wywołania paniki w społeczeństwie, zapaści ekonomicznej oraz do wywołania bezpośrednich uszkodzeń ciała lub śmierci osób będących obiektem ataku.

Następnym elementem, który należy zbadać jest wielkość grup potencjalnych napastników. Ewaluacji podlega też ich sprawność fizyczna, umiejętności pokonywania przeszkód i koordynacja działań poszczególnych osób w grupie.

Kolejnym etapem oceny zagrożenia jest zebranie informacji na temat potencjalnego dostępu do uzbrojenia i urządzeń technicznych umożliwiających atak. W przypadku broni ocenie podlega typ i ilość broni, którą potencjalni napastnicy mogą się posłużyć. Pożądane także będą informacje na temat umiejętności posługiwania się bronią przez napastników. W przypadku krajów o ograniczonym dostępie do broni należy dokonać oceny możliwości przemytu lub nielegalnego zakupu broni. Jak uczy przykład Brunona K. analizie musi podlegać także problem budowy ładunków wybuchowych z materiałów powszechnie dostępnych w sklepach. Analiza urządzeń technicznych obejmuje rozważania jakimi narzędziami i urządzeniami mogą się posłużyć potencjalni napastnicy. Ocenie podlegają możliwości zasilania tych urządzeń: baterie, zewnętrzne źródła napięcia, paliwo. Przeanalizować należy także zasadę działania urządzeń i narzędzi i sposób ich oddziaływania na atakowany obiekt lub instalację. Celowe wydaje się zbadanie czy istnieją techniczne możliwości sparaliżowania, zablokowania możliwości ich użycia przez stronę broniącą obiektu lub instalacji. Do metod blokujących działanie urządzeń można np. zaliczyć zagłuszanie urządzeń służących do komunikacji.

<sup>20</sup> A Method to Assess the Vulnerability of U.S. Chemical Facilities, U.S. Department of Justice, Office of Justice Programs, USA.

Następnym krokiem oceny zagrożenia jest zbadanie możliwości transportu napastników i ich wyposażenia na miejsce ataku i ewentualnie dróg ucieczki po zakończeniu akcji. Należy określić możliwości użycia transportu morskiego, lądowego lub powietrznego. W każdym z tych przypadków trzeba określić czy transport odbywa się środkami prywatnymi czy może jest to transport publiczny. Zbadanie dróg dostępu do potencjalnego celu ataku i dróg ucieczki z miejsca ataku pozwoli instytucjom i służbom państwowym a także siłom chroniącym atakowany obiekt na znalezienie miejsc blokady dostępu do instalacji zapobieżenie aktowi sabotażu lub miejsc, w których możliwe byłoby odzyskanie skradzionego materiału radioaktywnego w czasie ucieczki napastników z miejsca zdarzenia.

Ważnym elementem podlegającym ocenie są techniczne umiejętności członków grupy terrorystycznej. Ich techniczne umiejętności mogą wynikać z odbytych szkoleń w wojsku, doświadczeń na różnych arenach wojennych, ale także samokształcenia. Jeśli jest to grupa napastników nie będących mieszkańcami danego kraju, ocenie podlega ich możliwość komunikowania się w lokalnym języku w tym umiejętności wypowiedzenia się bez obcego akcentu.

Nie do przecenienia są zagrożenia wynikające z przyłączenia urządzeń i instalacji do globalnej sieci internetowej.<sup>21</sup> Atak na urządzenia odpowiadające za bezpieczeństwo sieci wewnętrznej, za procesy kontroli produkcji materiałów radioaktywnych lub w najgorszym przypadku za sterowanie urządzeniami wykorzystującymi materiał rozszczepialny (reaktory) może prowadzić do gigantycznych strat finansowych lub do zagrożenia utraty zdrowia lub życia ludzkiego. Doskonałym przykładem tego typu ataku jest nie do końca wyjaśniony atak na irańskie instalacje wzbogacania uranu w Natanz przeprowadzone za pomocą wirusa Stuxnet kiedy to wirus został wpuszczony do fizycznie odciętej od świata zewnętrznej sieci wewnętrznej poprzez urządzenia sterujące firmy Simens lub atak na także odcięte od świata zewnętrznego rosyjskie instalacje jądrowe.<sup>22</sup> Cyber ataki pozwalają także na kradzież danych dotyczących procedur i sposobów ochrony obiektów, instalacji i materiałów radioaktywnych. Analiza bezpieczeństwa musi obejmować również ten typ zagrożenia.

Rozpoznanie możliwości grup terrorystycznych należy uzupełnić o wiedzę dotyczącą chronionego obiektu. Przeanalizować należy jego położenie geograficzne w tym odległość do granic państwowych, ukształtowanie terenu, sieć okolicznych dróg oraz bliskość sąsiadujących z chronionymi obiektami osiedli i miast. Dodatkowym rozważaniem podlegają także takie dane jak: zastosowane elektroniczne systemy detekcji potencjalnego ataku. Systemy te charakteryzowane są prawdopodobieństwem detekcji ataku. Prawdopodobieństwo to jest przypisane do każdego detektora i określane jest w przypadku infrastruktury krytycznej eksperymentalnie. Badany detektor badany jest w różnych warunkach pogodowych (dzień, noc, niska temperatura, wysoka temperatura, śnieg, mgła). Oprócz detektorów ocenie podlegają także elektroniczne systemy opóźnienia ataku w tym wszelkie systemy identyfikacji osób mających dostęp do obiektów, instalacji lub materiałów radioaktywnych. Uzupełnieniem systemu ochrony podlegającym analizie jest system biernych przeszkód opóźniających atak. Tego typu elementy to: wszelkiego rodzaju płoty, mury, wzmocnione drzwi i okna, specjalnie

<sup>21</sup> MAEA Nuclear Security Series no. 17 Computer Security at Nuclear Facilities.

<sup>22</sup> Eugene Kaspersky, Australia's National Press Club 2013, Australia.

wzmocnione pomieszczenia i pojemniki z materiałem radioaktywnym. Całość oceny musi być uzupełniona o ewaluację procedur bezpieczeństwa obowiązujących na terenie obiektu oraz o ocenę systemu pracy pracowników obiektu. Ocena stanu bezpieczeństwa analizowanego obiektu wymaga wiedzy na temat godzin, w których pracownicy zaczynają i kończą swoją zmianę, ilości pracowników przypadających na zmianę, wiedzy o tym ilu pracowników i ewentualnie którzy pracownicy mają dostęp do potencjalnego celu ataku. Zebranie wyżej wymienionych informacji umożliwia rozpoznanie możliwych taktyk potencjalnego ataku, a tym samym i sposobów ochrony obiektu, instalacji lub materiałów radioaktywnych.

Do właściwej ewaluacji możliwości potencjalnych napastników wymagana jest ocena ich zaplecza finansowego. Posiadanie środków finansowych pozwala na zakup wymaganego uzbrojenia, opłacenie środków transportowych, zakup fałszywych dokumentów lub opłacenie potencjalnego informatora – insidera.

Osobnym problemem jest ocena zagrożenia wynikającego z działań napastnika tzw. insidera atakującego wewnątrz chronionego obiektu.<sup>23</sup> Insiderem może być osoba, która przeszła postępowanie certyfikujące i może mieć dostęp do potencjalnego celu ataku, w tym do materiałów radioaktywnych. Insider może być także źródłem informacji na temat sposobów zabezpieczania obiektów, instalacji lub materiałów radioaktywnych, może dostarczyć informacji dotyczących rozkładu pomieszczeń. Może też informować o obowiązujących procedurach bezpieczeństwa. Wykrycie osoby, która potencjalnie może być insiderem jest trudne i angażuje różne służby państwowe.

### **Podsumowanie**

Doniesienia prasowe, a także informacje udostępnione przez MAEA dowodzą, że zagrożenie atakami na obiekty, instalacje jądrowe oraz miejsca magazynowania lub użytkowania materiałów rozszczepialnych jest realne. Pamiętając, że taki atak jest każdorazowo szeroko omawiany w środkach masowego przekazu należy brać pod uwagę spadek poparcia społecznego dla energetyki jądrowej oraz dla wszelkich technologii wykorzystujących materiał rozszczepialny. Spadek poparcia może jak dowodzi przykład wstrzymanej budowy elektrowni jądrowej w Hiszpanii doprowadzić do znacznych strat finansowych. Znając skutki dla zdrowia i życia ludzkiego użycia materiału rozszczepialnego potencjalnie wykorzystanego w budowie brudnej bomby należy uznać, że ochrona fizyczna obiektów i instalacji jądrowych oraz miejsc przechowywania materiałów rozszczepialnych musi być priorytetem zarówno dla państwa na terytorium którego wykorzystuje się materiały rozszczepialne, jak i dla operatora tych materiałów. W przypadku dużego przemysłu jądrowego państwo i operatorzy muszą tworzyć procedury i szkolić personel ochrony w oparciu o zalecenia i rekomendacje MAEA.

Moment oddania do użytku pierwszej polskiej elektrowni jądrowej przewidziany jest, na dzień dzisiejszy, na rok 2025 i jest systematycznie oddalany w czasie. Państwo Polskie ma więc jeszcze dużo czasu na to, by w sposób właściwy przygotować się do tak poważnego wyzwania. Stopień przygotowania będzie podlegał ocenie społeczności międzynarodowej i obywateli RP, a ich

---

<sup>23</sup> MAEA Nuclear Security Series no. 8 Preventive and Protective Measures Against Insider Threats.



akceptacja dla nowej technologii pozyskiwania energii zadecyduje o sukcesie komercyjnym przedsięwzięcia. O sukcesie tym decydować także będzie poczucie bezpieczeństwa związanego z materiałami rozszczepialnymi.

### **Streszczenie**

Obiekty i instalacje jądrowe a także materiały rozszczepialne należą do grupy potencjalnie najbardziej atrakcyjnych dla terrorystów celów. Skutki ataku terrorystycznego mogą mieć różne charaktery w tym polityczne, prestiżowe, społeczne, ekonomiczne i militarne. Zagrożenie atakiem na obiekty, instalacje lub na materiały rozszczepialne jest zagrożeniem rzeczywistym na co wskazują statystyki MAEA oraz doniesienia medialne. Zgodnie z decyzją Rządu RP w celu dywersyfikacji źródeł energii i tym samym uniezależnienia się od dostawców zewnętrznych zostaną wybudowane dwie elektrownie jądrowe wraz z całą potrzebną do tego infrastrukturą. Państwowa Agencja Atomistyki zarejestrowała 3228 jednostek organizacyjnych, których działalność wiąże się narażeniem na promieniowanie jonizujące. Brak energetyki jądrowej w Polsce skutkuje brakiem doświadczonego w ochronie tego typu obiektów personelu. Szkolenie personelu ochrony oraz implementacja norm bezpieczeństwa musi być zatem dokonana na podstawie zaleceń i rekomendacji Międzynarodowej Agencji Energii Atomowej.

### **Summary**

Nuclear infrastructure as well as radioactive materials are among the most attractive targets for terrorist groups. Consequences of terrorist attacks maybe of various natures such as political, prestigious, social, economic and military. The threat of a terrorist attack on nuclear infrastructure or radioactive materials is real which can be confirmed by statistical data published by IAEA or massmedia. In order to diversify the energy sources, Polish government has taken the decision to begin the construction of two nuclear power plants as well as associated infrastructure. Polish Atomic Agency has registered 3228 organizational units working under exposure of ionising radiation. The deficiency of experienced security personnel in Poland is the result of the non existing nuclear industry. Training courses for security personnel as well as implementation of nuclear regulations must be done on the basis of International Atomic Energy Agency recommendations.

### **Bibliografia**

1. Kubowski J., Broń jądrowa, WNT. Warszawa 2008
2. Garcia M.L., *Design and Evaluation of Physical Protection Systems*, Butterworth-Heinemann 2008
3. Corera G., *Shopping for Bombs: Nuclear Proliferation, Global Insecurity, and the Rise and Fall of the A.Q. Khan Network*, Oxford University Press 2008
4. Wilson A, Wilson G.D., Olwell D.H., *Statistical Methods in Counterterrorism*, Springer 2006
5. Projekt uchwały Rady Ministrów w sprawie programu wieloletniego po nazwą „Program polskiej energetyki jądrowej”, <http://bip.krpm.gov.pl>, 28 stycznia 2014
6. Raport roczny Prezesa Państwowej Agencji Atomistyki za 2012 r.