

Розробка алгоритму оцінки вразливості джерел іонізуючого випромінювання

■ Сітнікова Ольга Леонідівна

Державне підприємство «Державний науково-технічний центр з ядерної та радіаційної безпеки», м. Київ, Україна
ORCID: <https://orcid.org/0000-0002-0602-9731>

■ Мельник Аліна Ігорівна

Державне підприємство «Державний науково-технічний центр з ядерної та радіаційної безпеки», м. Київ, Україна
ORCID: <https://orcid.org/0000-0003-4053-9716>

Наразі джерела іонізуючого випромінювання розповсюджені та мають широкий спектр застосування. Медицина – одне з перших місць з використання джерел іонізуючого випромінювання, а саме: для лікування онкологічних захворювань, наприклад, брахітерапія, дистанційна променева терапія (за допомогою, зокрема, гамма-ножа). Не менш розповсюджені джерела іонізуючого випромінювання у промисловості: для проведення радіографії (дефектоскопії), калібрування; застосовуються в засобах для вимірювання товщини листового матеріалу, рівня матеріалу в посудинах і трубах, у гамма-детекторах для проведення неруйнівного аналізу зварних швів різних конструкцій та трубопроводів тощо. Рівень небезпеки для людини від джерел іонізуючого випромінювання I та II категорії дуже високий. Такі джерела внаслідок неналежного використання, зберігання чи протиправних дій можуть спричинити в організмі людини стохастичні та детерміновані ефекти у разі контакту з ними без необхідного захисту, як-от за кілька хвилин для джерел іонізуючого випромінювання I категорії та від кількох хвилин до декількох годин для джерел іонізуючого випромінювання II категорії.

До того, у сучасному світі існує велика кількість екстремістських та терористичних угруповань, які можуть бути зацікавлені у заволодінні джерелами іонізуючого випромінювання для вчинення радіологічної диверсії з використанням пристрою розсіювання радіоактивних матеріалів або випромінюючого пристрою. Тому країни, в яких здійснюється діяльність з використанням джерел іонізуючого випромінювання, повинні виконувати оцінку потенційних загроз і вразливості цих джерел та забезпечувати їх захищеність і збереження. Отже, на часі актуальним є питання розробки підходів до оцінки вразливості джерел іонізуючого випромінювання.

У статті наведено загальний алгоритм проведення оцінки вразливості джерел іонізуючого випромінювання медичного і промислового призначення та стисло описано основні його етапи. Запропонований підхід полягає у використанні як кількісних (згідно з нормативно-правовими актами України), так і якісних показників, отриманих під час експертного оцінювання з врахуванням коефіцієнта конкордації (рівень узгодженості думок).

Метою оцінки вразливості є не лише визначення величини ризику вчинення незаконних дій із джерелами іонізуючого випромінювання, а й врахування можливих сценаріїв їх використання, для подальшого ухвалення рішень на основі ризик-орієнтованого підходу щодо розподілу наявних ресурсів для захисту людей та майна від наслідків зовнішньої радіологічної диверсії у різних місцях-цільях: на масовому заході (святкуванні), у столиці, в урядових будівлях, у туристичному місті тощо.

Ключові слова: джерело іонізуючого випромінювання, оцінка вразливості, диверсія, несанкціоноване вилучення, крадіжка, система фізичного захисту.

© Сітнікова О. Л., Мельник А. І., 2022

Радіоактивні матеріали, які використовуються в медичних апаратах, є привабливими для правопорушників через можливість їх викрадення з об'єкта. Несанкціоноване заволодіння джерелами іонізуючого випромінювання

(ДІВ) може призвести до двох основних наслідків: використання в пристрої розсіювання радіоактивних матеріалів (ПРРМ) («брудний бомбі») або випромінюючому пристрої (ВП) («приховане закрите джерело»).

Згідно з публікацією Міжнародного агентства з атомної енергії (МАГАТЕ) [1] в медицині застосовуються різні закриті ДІВ, зокрема: ^{137}Cs , ^{60}Co , ^{192}Ir , ^{226}Ra , ^{125}I , ^{131}I , ^{198}Au , ^{252}Cf , ^{32}P , ^{90}Cr , $^{106}\text{Ru/Rh}$, ^{103}Rd тощо, які належать до I – V категорії.

Категоризація ДІВ в Україні проводиться на основі документа МАГАТЕ [1] відповідно до Технічного регламенту закритих джерел іонізуючого випромінювання [2]. Найбільшу небезпеку становлять ДІВ I-III категорії, для яких повинен бути забезпечений III рівень фізичного захисту [3], згідно з яким вони мають бути розміщені в межах зони контрольованого доступу.

Найпоширенішими ДІВ I-II категорії в медицині та промисловості є ^{60}Co , ^{137}Cs та ^{192}Ir . Досі зустрічаються джерела, які містять хлорид ^{137}Cs у вигляді порошку, який полегшує його використання в ПРРМ та швидкому розповсюдженні радіоактивних матеріалів на великі відстані. Джерела з ^{192}Ir та ^{60}Co використовуються в багатьох стаціонарних і мобільних опромінювачах. Саме ця доступність та мобільність спричиняє занепокоєння.

Вразливість об'єкта визначається як характеристики системи, що відкривають можливість їх використання з злочинною метою; недолік або слаба ланка у системі фізичного захисту (СФЗ) установки [4].

Зазначені характеристики системи або слабкі ланки можуть виникати з багатьох причин, наприклад, як недолік під час проектування СФЗ, планування об'єкта чи установки, а також у разі недотримання персоналом вимог з фізичного захисту та безпеки, розроблених відповідно до характеристик загроз.

Як відомо, засоби виявлення, як будь-яка техніка, мають свій строк експлуатації та свою «сумісність» з іншими елементами СФЗ, час від часу переглядається проєктна загроза [5], тому актуальним є питання аналізу та оцінки стану СФЗ протягом певного періоду. Саме для цього виконується оцінка вразливості.

Для оцінки ефективності розробленої чи існуючої СФЗ необхідно провести оцінку вразливості [4] об'єкта та визначити величину ризику [6]. З огляду на те, що в Україні запроваджена методика оцінки вразливості лише для ядерних об'єктів та ядерних матеріалів [6], актуальним є питання розробки такої методики і для ДІВ.

Існує низка міжнародних підходів з оцінки вразливості, описаних в документах [7]-[8], як-от методологія NUSAM (англ. Nuclear security assessment methodologies) – методологія оцінки ядерної захищеності, методологія VISA (англ. «Vulnerability of Integrated Security Analysis») – методологія вразливості інтегрованого аналізу безпеки, а також методики дерева подій та дерева відмов, ризик-інформований підхід тощо. Порядком проведення оцінки вразливості

ядерних установок та ядерних матеріалів [6] визначено методику розробки сценаріїв дій правопорушника. Однак вимоги цього порядку поширюються лише на ядерні об'єкти та ядерні матеріали.

Отже, пропонуємо розглянути підхід [6], адаптований до проведення оцінки вразливості об'єктів, що здійснюють діяльність з ДІВ. Загальний алгоритм оцінки вразливості ДІВ зображено на рисунку 1 і умовно складається з двох блоків: перший блок – етап проведення оцінки вразливості згідно з документом [6], який адаптовано для об'єктів, що здійснюють діяльність з ДІВ I-III категорії (наприклад, онкологічний диспансер, лікарня, медичний центр тощо) для сценаріїв здійснення внутрішньої радіаційної диверсії [5] та для оцінки ймовірності викрадення ДІВ з об'єкта.

Другий блок – підхід для сценаріїв зовнішньої радіаційної диверсії поза межами об'єкта.

Алгоритм охоплює такі етапи:

розробку дерева подій для сценаріїв зовнішньої радіологічної диверсії з використанням ДІВ;

розробку загальної діаграми послідовності дій правопорушника відповідно до документа [6];

конвертація дерева подій у дерева відмов для визначення ймовірності реалізації сценаріїв зовнішньої радіологічної диверсії;

визначення ймовірності реалізації сценаріїв зовнішньої радіологічної диверсії;

оцінка ризиків.

Приклад розробленого дерева подій наведено на рисунку 2 (на основі методики, описаної в документі [7]).

Для простоти інтерпретації було обрано мінімальну кількість вузлів у дереві подій та мінімум варіацій для кожного вузла.

Відповідно до цієї схеми, якщо розгорнути повністю дерево, то кількість можливих сценаріїв становитиме 48. Утім наступним етапом є аналіз та усунення нереалістичних варіантів, наприклад, ^{192}Ir у вигляді крихтих капсул (розміром з рису зернину) неможливо використати в ПРРМ. Отже, остаточна кількість сценаріїв становить 40.

Наступним кроком є з'ясування ймовірностей для кожного вузла дерева подій.

Для вузла «Набутий матеріал» ймовірності будуть визначатись кількісно з формули:

$$P_k = 1 - P_{N'} \quad (1)$$

де P_N – ймовірність нейтралізації правопорушників під час крадіжки ДІВ, отримана в результаті оцінки вразливості СФЗ об'єкта відповідно до документа [6].

Ймовірності для вузлів «Загроза / Правопорушник», «Пристрій» та «Транспорт / Ціль» повинні бути визначені під час виконання експертної оцінки.

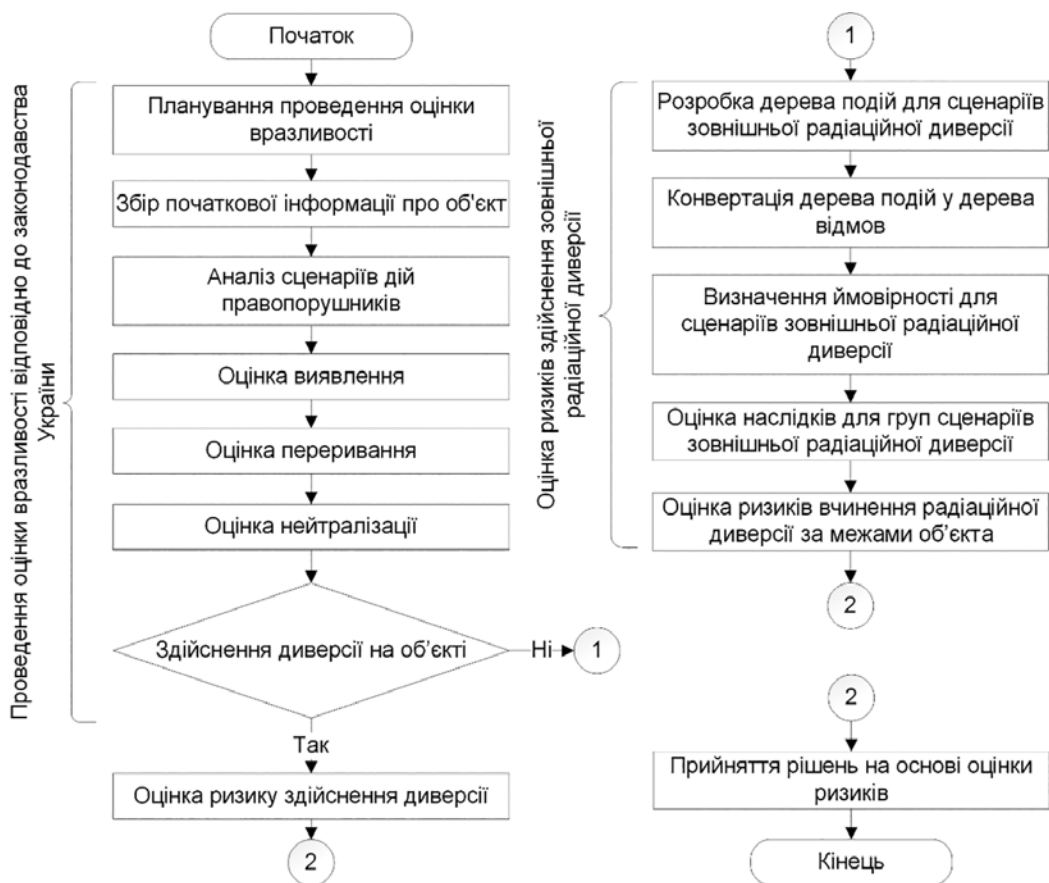


Рисунок 1 – Загальний алгоритм оцінки вразливості ДІВ

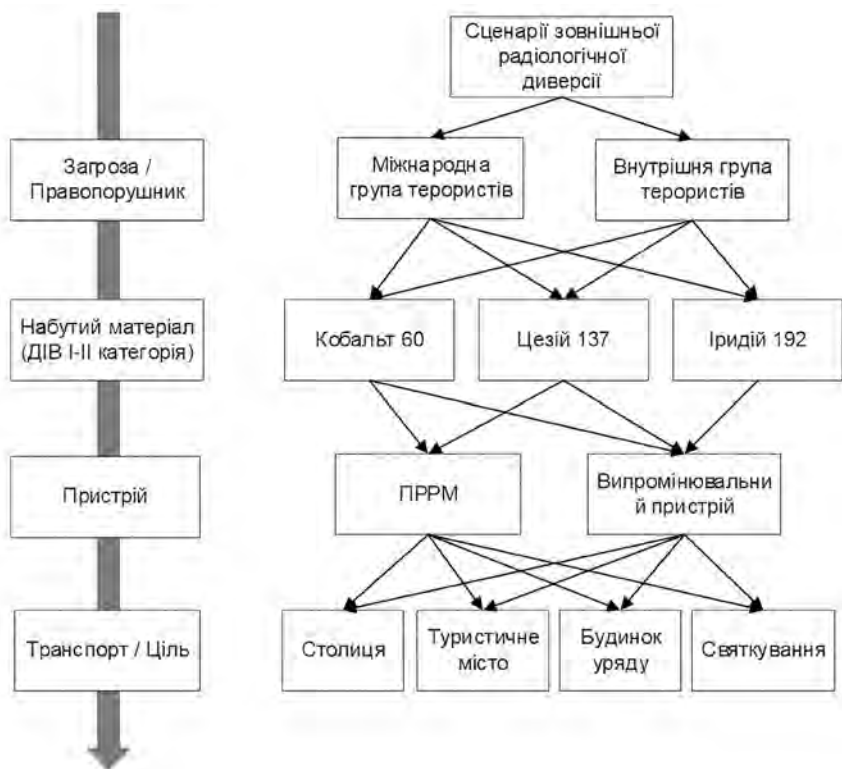


Рисунок 2 – Дерево подій для сценаріїв зовнішньої радіологічної диверсії з використанням ДІВ



Рисунок 3 – Класифікація методів отримання знань від експертів [10]

Методики виконання експертної оцінки розглядались багатьма науковцями, зокрема Грабовецьким [9]. На рисунку 3 наведено класифікацію методів отримання експертних знань.

Процес підготовки і проведення групових методів (наприклад, «мозковий шторм», круглий стіл тощо) є складним. Для проведення групового оцінювання необхідне залучення широкого кола висококваліфікованих спеціалістів, яких важко (а іноді і неможливо) зібрати разом одночасно в одному місці, до того ж в оптимальній кількості і які б відповідали встановленим критеріям.

Усю сукупність спеціалістів необхідної предметної галузі можна «набрати» з авторів статей у відповідній тематиці, Грабовецький у своїй роботі [9] називає це методом «сніжної грудки». Оптимальну кількість експертів у групі можна визначити розрахунковим методом відповідно до встановлення критерію компетентності та критерію Стьюдента, як у джерелі [9].

«Нарівні з розрахунковими методами обчислення розміру експертної групи, рекомендується довільна чисельність опитуваних експертів – у межах від 10 до 20 чоловік, хоча в деяких випадках допускається їх збільшення або зменшення»[9].

Найпоширенішим методом проведення експертного оцінювання є використання «вагових» коефіцієнтів з визначенням узгодженості думок опитаних фахівців за допомогою коефіцієнта конкордації. Алгоритм проведення експертного оцінювання наведено у [10].

Третім етапом методики оцінки вразливості ДІВ медичного та промислового призначення, після оцінки всіх імовірностей, є конвертація отриманого дерева подій у дерево відмов та роз-

рахунок імовірностей здійснення сценаріїв зовнішньої радіологічної диверсії. До прикладу, це можна реалізувати у програмному забезпеченні SAPHIRE, RiskSpectrum, які були використані на АЕС України під час розробки ймовірнісних моделей енергоблоків.

Останнім етапом методики є розрахунок величини ризику здійснення сценаріїв зовнішньої радіологічної диверсії. Відповідно до документа [6] розрахунок ризику здійснюється з урахуванням коефіцієнта потенційних наслідків (рисунок 4).

Пріоритетними є загрози та сценарії здійснення зовнішньої радіологічної диверсії з величиною ризику «дуже високий» та «високий», для яких проводяться всі необхідні заходи для забезпечення безпеки. Другий пріоритет мають сценарії з рівнем ризику «середній», для яких здійснюються заходи за наявності ресурсів. Сценарії з «низьким» та «дуже низьким» ризиком можуть бути відсіяні.



Рисунок 4 – Розподіл ризиків настання відповідних подій (ДВ – дуже високий, В – високий, С – середній, Н – низький, ДН – дуже низький)

Висновки

За результатами оцінки стану використання ДІВ у медицині та промисловості було показано їх розповсюдженість на території України. Країни, в яких здійснюється діяльність з використанням ДІВ, повинні здійснювати оцінку потенційних загроз і вразливості ДІВ по відношенню до них та забезпечувати їх захищеність та збереження. Для цього в державі необхідно створити дієву нормативно-правову базу з фізичного захисту ДІВ. Наразі в Україні відсутній підхід оцінки вразливості ДІВ. З урахуванням активізації за останнє десятиліття терористичних організацій, а також зі зростанням їх можливостей є необхідність проведення оцінки вразливості ДІВ.

Розроблений алгоритм проведення оцінки вразливості ДІВ складається з п'яти етапів та є поєднанням методики дерева подій і розробки сценаріїв дій правопорушника. Запропонований підхід дозволяє оцінити ризики як для сценаріїв безпосередньої диверсії на об'єкті, так і у разі крадіжки для проведення радіологічної диверсії за межами об'єкта. Крім того, алгоритм дозволяє приймати рішення на основі ризик-інформованого підходу для реалізації заходів із виявлення та запобігання радіологічної диверсії.

Список використаної літератури

1. Категоризация радиоактивных источников. Руководство по безопасности № RS-G-1.9. Вена: МАГАТЭ, 2006. 57 с.
2. Технічний регламент закритих джерел іонізуючого випромінювання. Затверджено постановою Кабінету Міністрів України від 05.12.2007 № 1382.
3. Порядок визначення рівня фізичного захисту ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання відповідно до їх категорії. Затверджено постановою Кабінету Міністрів України від 26.04.2003 № 625. *Офіційний вісник України*. 2003. № 18. С. 98.
4. НП 306.7.086-2004. Облік та контроль ядерного матеріалу, фізичний захист ядерного матеріалу і ядерних установок. Тлумачний словник українських термінів. Словники термінів: українсько-англо-російський, русско-украинско-английский, english-russian-ukrainian. Затверджено наказом Держатомрегулювання України від 08.06.2004 № 101.
5. Про фізичний захист ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання. Закон України від 19.10.2000 № 2064-III. Дата оновлення: 28.12.2015. URL: <https://zakon.rada.gov.ua/laws/show/2064-14#Text>.

6. Порядок проведення оцінки вразливості ядерних установок та ядерних матеріалів, затверджений наказом Державного комітету ядерного регулювання України від 30.11.2010 № 169. *Офіційний вісник України*. 2011. № 100. С. 165.

7. Risk Informed Approach for Nuclear Security Measures for Nuclear and Other Radioactive Material out of Regulatory Control. Implementing Guide. IAEA Nuclear Security Series No. 24-G. Vienna, IAEA, 2015. 69 p.

8. Nuclear Security Assessment Methodologies for Regulated Facilities. IAEA-TECDOC-1868. Vienna: IAEA, 2019. 144 p.

9. Грабовецький Б. Є. Методи експертних оцінок: теорія, методологія, напрямки використання : монографія. Вінниця: ВНТУ, 2010. 171 с.

10. Інтелектуальні системи управління: Курс лекцій до теми «Системи експертного оцінювання» розділу «Основи штучного інтелекту» кредитного модуля «Інтелектуальні системи управління» для студ. спец. 151 – «Автоматизація та комп'ютерно-інтегровані технології» / Уклад.: Л. Д. Ярошук. К.: КПІ ім. Ігоря Сікорського, 2017. 40 с.

References

1. Categorization of radioactive sources. Safety guide No. RS-G-1.9. Vienna, IAEA, 2006, 57 p.
2. Technical specifications for sealed radiation sources. Approved by Resolution of the Cabinet of Ministers of Ukraine No. 1382 of 5 December 2007.
3. The procedure for determining the level of physical protection of nuclear facilities, nuclear materials, radioactive waste and other radiation sources according to their category. Approved by Resolution of the Cabinet of Ministers of Ukraine No. 625 of 26 April 2003. Official Gazette of Ukraine, 2003, 18, 98 p.
4. NP 306.7.086-2004. Accounting and control of nuclear materials, physical protection of nuclear materials and nuclear facilities. Glossaries of Ukrainian terms. Glossaries: english-russian-ukrainian. Approved by SNRCU Order No. 101 of 8 June 2004.
5. On the physical protection of nuclear facilities, nuclear materials, radioactive waste, and other radiation sources. Law of Ukraine No. 2064-III dated 19 October 2000. Update date: 28 December 2015. URL: <https://zakon.rada.gov.ua/laws/show/2064-14#Text>.
6. The procedure for assessing vulnerability of nuclear facilities and nuclear materials. Approved by Order of the State Nuclear Regulatory Committee of Ukraine No. 169 dated 30 November 2010. Official Gazette of Ukraine, 2011, 100, 165 p.
7. Risk informed approach for nuclear security measures for nuclear and other radioactive material out of regulatory control. Implementing guide. IAEA Nuclear Security Series No. 24-G. Vienna, IAEA, 2015, 69 p.
8. Nuclear security assessment methodologies for regulated facilities. IAEA-TECDOC-1868. Vienna, IAEA, 2019, 144 p.

9. Hrabovetskyi, B. (2010). Methods of expert assessments: theory, methodology, areas of use: monograph. Vinnytsia, VNTU, 171 p.

10. Intelligent control systems. Course of lectures on expert assessment systems of section "Fundamentals of artificial intelligence" of the credit module "Intelligent control systems" for students in specialty 151 "Automation and computer-integrated technologies". Compiled by Yaroshchuk L., Kyiv, Sikorsky KPI, 2017, 40 p.

Development of the Algorithm to Assess Vulnerability of Radiation Sources

O. Sitnikova, A. Melnyk

State Enterprise «State Scientific and Technical Center for Nuclear and Radiation safety», Kyiv, Ukraine

Currently, radiation sources are widespread and find extensive application. Medicine is one of the first places to use radiation sources, namely: for the treatment of oncological diseases, for example, brachytherapy, remote radiation therapy (using, in particular, a gamma knife). Radiation sources are also widespread in industry: for radiography (flaw detection), calibration; used in means for measuring the thickness of sheet material, level of material in vessels and pipes, in gamma detectors for nondestructive analysis of welds of various structures and piping, etc. The level of hazard for humans from category I and II radiation sources is very high. Due to improper use, storage or illegal actions, such sources can cause stochastic and deterministic effects in the human body during contact

with them without the necessary protection, for example, a few minutes for category I radiation sources and from a few minutes to several hours for category II radiation sources.

In addition, in the today's world, there are many extremist and terrorist groups that may be interested in seizure of radiation sources to commit radiological sabotage using a device to distribute radioactive materials or a radiating unit. Therefore, countries where activities are carried out using radiation sources should assess the potential threats and vulnerability of these sources and ensure their security and integrity. Therefore, the issue of developing approaches to assess vulnerability of radiation sources is topical.

The article presents the general algorithm for assessing vulnerability of medical and industrial radiation sources and briefly describes its main stages. The proposed approach involves both quantitative (according to regulatory documents of Ukraine) and qualitative indexes obtained during an expert assessment, taking into account the concordance coefficient (the level of opinion consistency).

The purpose of the vulnerability assessment is not only to determine the risk magnitude of illegal actions with radiation sources, but also to take into account possible scenarios of their use, for further decision-making based on the risk-based approach to the distribution of available resources to protect the public and property against the consequences of external radiological sabotage in various target places: at a mass event (celebration), in the capital, in government buildings, in a tourist city, etc.

Keywords: radiation source, vulnerability assessment, sabotage, unauthorized seizure, theft, physical protection system.

Отримано 11.01.2022