НАЦІОНАЛЬНИЙ ІНСТИТУТ СТРАТЕГІЧНИХ ДОСЛІДЖЕНЬ

ПРОТИДІЯ ТЕРОРИЗМУ, НЕРОЗПОВСЮДЖЕННЯ ЗБРОЇ ТА МАТЕРІАЛІВ МАСОВОГО ЗНИЩЕННЯ Й ЗАХИСТ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Збірник матеріалів засідань
Міжвідомчої експертної робочої групи,
створеної при НІСД

Київ 2013

УДК 323.285:623:454.8:502
П 78

За редакцією заслуженого юриста України *О. Д. Маркєєвої*, доктора медичних наук, професора *Ю. М. Скалецького*

Електронна версія: http://www.niss.gov.ua

Протидія тероризму, нерозповсюдження зброї та матеріалів
П 78 масового знищення й захист критичної інфраструктури : зб. матеріалів Міжвідомчої експертної робочої групи, створеної при НІСД / за ред. О. Д. Маркєєвої, Ю. М. Скалецького – К. : НІСД, 2013. – 104 с.

ISBN 978-966-554-194-3

У збірнику представлені інформаційні та аналітичні матеріали, що висвітлюють діяльність створеної у березні 2011 р. при Національному інституті стратегічних досліджень Міжвідомчої експертної робочої групи (МЕРГ) з питань протидії загрозам розповсюдження зброї та матеріалів масового знищення, а також пов'язаних із ними терористичних загроз, і захисту критично важливої для забезпечення життєдіяльності держави інфраструктури.

До частини І видання увійшли матеріали, що стосуються створення групи, а також окремі доповіді та повідомлення членів МЕРГ з актуальних проблем, віднесених до компетенції групи.

У ІІ частині видання представлена аналітична доповідь, присвячена актуальним проблемам протидії незаконному обігу ядерних та інших радіоактивних матеріалів, а також ядерному та радіаційному тероризму, презентація якої відбулася на одному із засідань МЕРГ.

Збірник розрахований на представників органів державної влади, співробітників правоохоронних органів та спецслужб, промисловців, науковців, експертів, а також на широке коло читачів, які цікавляться відповідною проблематикою.

ISBN 978-966-554-194-3

ПЕРЕДМОВА

Національний інститут стратегічних досліджень (*далі* – НІСД) визначено базовою науково-дослідною установою аналітико-прогнозного супроводження діяльності Президента України. Згідно зі статутом НІСД для виконання поставлених перед ним завдань Інститут може використовувати, зокрема, такі форми діяльності, як *«круглі столи», конференції, семінари, до роботи в яких запрошуються провідні науковці, політики, представники органів державної влади, аналітики, незалежні експерти*». Крім того, «*фахівці Інституту залучаються до складу дорадчих органів, що утворюються при Президентові України, офіційних делегацій України, міжвідомчих і відомчих, урядових та інших комісій і робочих груп*».

У результаті здійснення реформ, спрямованих на оптимізацію президентської гілки влади, НІСД залишився єдиною науково-дослідною установою у системі підтримки діяльності Президента України. Така ситуація передбачала подальший розвиток форм та інструментів діяльності Інституту на найважливіших напрямах забезпечення національної безпеки держави, передусім пов'язаних із новими викликами та загрозами. Зважаючи на це, відділом екологічної та техногенної безпеки було підготовлено концепцію створення міжвідомчої експертної групи, яка розглядала би проблеми, пов'язані із загрозами розповсюдження зброї масового знищення (ЗМУ) й тероризму, а також із захистом критично важливої для життєдіяльності держави інфраструктури. Відповідна пропозиція була надана на розгляд керівництва НІСД.

Ця ініціатива була підтримана, і наказом директора Інституту від 15.03.2011 р. № 17 було створено Міжвідомчу експертну робочу групу (МЕРГ) з питань протидії загрозам розповсюдження зброї та матеріалів масового знищення, а також пов'язаних з ними терористичних загроз, і захисту критично важливої для забезпечення життєдіяльності держави інфраструктури. Для участі у роботі групи були запрошені представники державних органів (у т.ч. правоохоронних органів і спецслужб), науково-дослідних установ, державних і приватних компаній тощо. Засідання групи сприяли налагодженню та зміцненню міжвідомчих контактів та обміну відкритою інформацією між державними органами та іншими організаціями, установами та компа-

ніями, діяльність яких пов'язана із забезпеченням національної безпеки у зазначених сферах.

Протягом 2011–2012 рр. МЕРГ регулярно проводила свої засідання, на яких було розглянуто широке коло проблем, віднесених до компетенції групи. За результатами засідань було підготовлено низку аналітичних матеріалів та інформаційних листів до Адміністрації Президента України.

Дане видання складається із двох частин: частина І включає концепцію створення МЕРГ, а також окремі виступи та повідомлення членів МЕРГ, а у частині ІІ представлена аналітична доповідь з актуальних проблем протидії незаконному обігу ядерних та інших радіоактивних матеріалів, а також ядерному та радіаційному тероризму.

КОНЦЕПЦІЯ СТВОРЕННЯ ПРИ НІСД МІЖВІДОМЧОЇ ЕКСПЕРТНОЇ РОБОЧОЇ ГРУПИ З ПИТАНЬ ПРОТИДІЇ ЗАГРОЗАМ РОЗПОВСЮДЖЕННЯ ЗБРОЇ ТА МАТЕРІАЛІВ МАСОВОГО ЗНИЩЕННЯ, А ТАКОЖ ПОВ'ЯЗАНИХ З НИМИ ТЕРОРИСТИЧНИХ ЗАГРОЗ, І ЗАХИСТУ КРИТИЧНО ВАЖЛИВОЇ ДЛЯ ЗАБЕЗПЕЧЕННЯ ЖИТТЄДІЯЛЬНОСТІ ДЕРЖАВИ ІНФРАСТРУКТУРИ

Для виконання завдань, поставлених перед НІСД, використовуються, зокрема, такі форми діяльності, як *«круглі столи», конференції, семінари, до роботи в яких запрошуються провідні науковці, політики, представники органів державної влади, аналітики, незалежні експерти*». Крім того, «*фахівці Інституту залучаються до складу дорадчих органів, що утворюються при Президентові України, офіційних делегацій України, міжвідомчих і відомчих, урядових та інших комісій і робочих груп*».

Ці важливі й, без сумніву, достатньо ефективні інструменти діяльності НІСД у разі роботи на напрямах, особливо пов'язаних із новими викликами та загрозами, на наш погляд, можуть бути доповнені діяльністю міжвідомчих експертних груп, утворених при Інституті. У такому випадку НІСД відіграватиме активнішу роль в експертному середовищі, матиме ширші можливості для акумулювання нової інформації та ідей щодо протистояння найнебезпечнішим загрозам, сприятиме обміну інформацією між суб'єктами забезпечення національної безпеки, що створює можливості для більш ефективного інформаційно-аналітичного супроводження процесу прийняття рішень стосовно викликів та загроз, які потребують негайних дій або дій на випередження.

З точки зору глобальної безпеки загрози розповсюдження зброї масового знищення та загрози тероризму, особливо з використанням зброї та матеріалів масового знищення, мають особливе значення. Подальше зростання цих загроз ставить під питання саме існування цивілізованого людства. Про зростання уваги міжнародної спільноти до цих загроз свідчать, наприклад, такі непересічні події 2010 року, як Вашингтонський саміт з (фізичної) ядерної безпеки та прийняття нової Стратегічної концепції НАТО на саміті Альянсу в Лісабоні.

Україна завдяки своїй послідовній миролюбній політиці, невід'ємною частиною якої стали як історична відмова від ядерної зброї

невдовзі після набуття незалежності, так і прийняття у цьому році зобов'язання відмовитися до 2012 р. від використання високозбагаченого урану на своїй території, проголошене під час цьогорічного Вашингтонського саміту, зробила значний внесок у міжнародні зусилля у цій сфері, що є суттєвим чинником формування високого авторитету нашої держави на світовій арені. Про це свідчить, зокрема, і Указ Президента України «Про Національний план з реалізації Робочого плану Вашингтонського саміту з ядерної безпеки на 2010–2012 роки». Крім того, Україною ратифіковано низку міжнародних конвенцій, вона є учасницею ряду глобальних ініціатив з питань протидії розповсюдженню ЗМУ (у першу чергу ядерної) та тероризму. Виконання взятих Україною на себе міжнародних зобов'язань, у т.ч. у рамках прийнятих національних планів і програм, потребує ефективної взаємодії суб'єктів відповідних процесів, а також адекватного рівня обміну інформацією між ними.

З точки зору протидії розповсюдженню ЗМУ й тероризму проблема обміну інформацією є однією з найгостріших, оскільки, поміж іншого, пов'язана із традиційною «закритістю» безпекового сектору в кожній державі. Проілюструвати це можна, зокрема, тим, що одним із восьми основоположних принципів *Глобальної ініціативи щодо боротьби з актами ядерного тероризму* (ГІБЯТ), до якої Україна приєдналася у 2007 р., є саме «*сприяння обміну інформацією для запобігання актам ядерного тероризму*». Кілька пунктів Робочого плану Вашингтонського саміту з (фізичної) ядерної безпеки також присвячені цьому важливому елементу зусиль держав-учасниць. Відзначимо також, що ця проблема є актуальною не тільки на міжнародному, а й на національному рівнях.

Справді, якщо, наприклад, хтось спробує визначити пріоритетні напрями діяльності у цій сфері на національному рівні, а також сегменти, в яких найбільш динамічно розвивається міжнародне співробітництво України, і оцінити обсяги міжнародної технічної допомоги, то при цьому доведеться зіткнутися з відсутністю узагальненої інформації, оскільки відповідні дані розпорошені по багатьох державних органах, із браком аналітичних матеріалів, недостатньою кількістю досліджень і публікацій із цієї пріоритетної для міжнародного співтовариства тематики тощо. Крім того, у той час, як відповідні міжнародні організації, зарубіжні партнери нашої країни намагаються забезпечити представництво України на найважливіших міжнародних форумах у цій сфері, на національному рівні гостро бракує інформації від представників українських делегацій та окремих осіб, які брали участь у міжнародних заходах. Усе це створює в Україні певний інформаційний вакуум щодо

гострих проблем, якими переймається світове співтовариство у цьому сегменті глобальної безпеки, сприяє певній «відстороненості» українських експертів від світових процесів і тенденцій.

У зв'язку з викладеним, а також спираючись на деякий досвід створення та функціонування міжвідомчої експертно-консультативної ради з питань протидії загрозам ядерного розповсюдження та ядерного тероризму при Інституті проблем національної безпеки РНБОУ, у роботі якої активну роль відігравали теперішні співробітники відділу техногенної та екологічної безпеки, пропонуємо створити при НІСД **міжвідомчу експертну робочу групу (МЕРГ)** з питань протидії загрозам розповсюдження зброї та матеріалів масового знищення, а також пов'язаних із ними терористичних загроз, і захисту критично важливої для забезпечення життєдіяльності держави інфраструктури.

На наш погляд, МЕРГ може певною мірою не тільки задовольнити запит **щодо обміну відкритою інформацією** між міністерствами, відомствами, неурядовими експертними організаціями тощо, які працюють у цій сфері, а й сприяти набуттю НІСД лідируючої ролі при визначенні стратегічних підходів до проблем у цій сфері, а також формуванні національного експертного співтовариства. Все це має позитивно вплинути на виконання Україною взятих на себе міжнародних зобов'язань.

Підсумовуючи зазначене, пропонуємо створити робочу групу, діяльність якої має базуватися на таких принципах:

• регулярність засідань (оптимальним було б затвердження річного робочого плану з чіткою періодичністю і заздалегідь визначеними датами проведення засідань МЕРГ);

• значна увага з боку керівництва НІСД (пропонується, щоб МЕРГ очолив заступник директора Інституту за відповідним напрямом);

• участь у роботі представників усіх зацікавлених відомств і установ на основі дійсно існуючої потреби в обміні відкритою інформацією та у професійному спілкуванні;

• реагування на поточні події у сфері протидії розповсюдженню зброї та матеріалів масового знищення та пов'язаної з ними терористичної діяльності;

• сприяння міжвідомчим контактам, міжвідомчій координації дій та обміну інформацією, розробці узгоджених пропозицій щодо актуальних проблем протидії розповсюдженню зброї та матеріалів масового знищення та пов'язаної з ними терористичної діяльності;

• вивчення передового світового досвіду, сприяння участі представників МЕРГ та інших суб'єктів забезпечення національної безпеки у цій сфері у заходах на міжнародному та національному рівнях;

• підготовка і розповсюдження на регулярній основі звітів щодо діяльності МЕРГ керівництву НІСД, інших заінтересованих державних органів;

• гнучкий формат засідань і відкритість до обговорення пропозицій щодо організації засідань з боку членів групи.

Рекомендації (рішення) МЕРГ можуть оформлюватися у вигляді доповідних записок керівництву НІСД, які супроводжуються, за необхідності, інформаційно-аналітичними матеріалами та довідками.

Типовий порядок денний засідання групи, на наш погляд, має включати: обговорення заздалегідь визначеної проблеми; огляд поточних подій за інформацією спеціалізованих веб-ресурсів; окремі повідомлення та запити членів групи щодо заходів на міжнародному та національному рівнях тощо; підготовка рекомендацій (рішень); різне. На основі попереднього досвіду можна рекомендувати, щоб тривалість типового засідання групи не була довшою за дві–дві з половиною години. На 2011 р. пропонується розробити план роботи МЕРГ на основі регулярних засідань (раз на 2 місяці) з можливістю скликання групи позачергово для обговорення невідкладних проблем і подій.

Діяльність групи не потребуватиме суттєвих витрат – для матеріально-технічного забезпечення роботи групи необхідно буде лише передбачити деякі додаткові кошти на витратні матеріали (папір, картриджі для принтерів і копіювальної техніки).

Відділ техногенної та екологічної безпеки
Національного інституту стратегічних досліджень[1]

[1]Тут і далі назви державних органів, наукових установ та їхніх підрозділів, а також посади членів МЕРГ та інших залучених осіб вказуються такими, якими вони були під час підготовки того чи іншого матеріалу.

ВСТУПНА ПРОМОВА

ЛИТВИНЕНКО Олександр Валерійович,
заступник директора НІСД, керівник МЕРГ

Міжвідомча експертна робоча група з питань протидії загрозам розповсюдження зброї та матеріалів масового знищення, а також пов'язаних з ними терористичних загроз, і захисту критично важливої для забезпечення життєдіяльності держави інфраструктури при Національному інституті стратегічних досліджень була утворена відповідно до наказу директора Інституту від 15 березня 2011 р. № 17 з метою підвищення рівня інформаційно-аналітичної підтримки діяльності Президента України у сфері протидії розповсюдженню зброї масового знищення й тероризму.

Згідно із цим наказом керівником групи призначено мене, Литвиненка Олександра Валерійовича, заступника директора Інституту, а заступниками керівника – завідувача відділу стратегій реформування сектору безпеки Маркєєву Оксану Дмитрівну та завідувача відділу техногенної та екологічної безпеки Скалецького Юрія Миколайовича, секретарем – наукового співробітника відділу техногенної та екологічної безпеки Кондратова Сергія Івановича.

Під час підготовчої роботи до створення МЕРГ Інститутом було розіслано інформацію про плани створення такого міжвідомчого органу 29 адресатам, включаючи міністерства, відомства, інші державні органи, а також науково-дослідні установи, науково-виробничі компанії, неурядові організації, які діють у цій сфері.

Від початку ми чітко визначили, що основним завданням створюваної групи є сприяння обміну відкритою інформацією, а також створення умов для регулярного спілкування на експертному рівні. Діяльність групи має забезпечити можливість для професійних контактів і, можливо, стане в нагоді при створенні інших міжвідомчих структур, які будуть призначені для відповідних зусиль, але вже в іншому форматі.

Згоду на участь своїх представників у роботі групи дали 20 міністерств, відомств, наукових установ, неурядових організацій. Такі відомства, як Державна прикордонна[2] та Державна митна служби відповіли

[2]Пізніше представники Адміністрації Державної прикордонної служби все ж приєдналися до роботи МЕРГ і брали активну участь у більшості її засідань.

відмовою, оскільки вони не бачать сенсу в обміні відкритою інформацією, зазначивши при цьому, що не відмовляються співробітничати з Інститутом з окремих питань. При цьому слід зважити, що підготовка до першого засідання групи відбувалася у період здійснення адміністративної реформи, і це не могло не позначитися на відповідях на нашу інформацію про створення МЕРГ. Ми це враховуємо й надалі будемо сповідувати гнучкий підхід, спираючись на уявлення про створену структуру як про «живий організм», який має розвиватися. Тож група й надалі буде відкрита до змін, включаючи набуття членства в ній, на основі відповідних звернень з боку державних органів, організацій та інших установ.

Загалом первинний список членів групи наразі налічує 45 осіб. Він буде розповсюджений між членами групи. Крім того, ми маємо певну контактну інформацію, надану нам в офіційних відповідях. Ми хотіли б, щоб члени групи чітко визначилися щодо можливості надання своєї контактної інформації іншим членам групи. Про це сказано у запропонованому вам *опитувальному листі*. Крім того, цей лист містить інші запитання щодо організації та формату наступних засідань групи. Просимо уважно поставитися до цього пункту нашого порядку денного, адже ми прагнемо таким чином організувати нашу спільну роботу, щоб вона була і корисною, і цікавою для максимально можливої кількості членів МЕРГ.

Вам також розданий попередній план-графік засідань до кінця 2011 р., у якому вже визначені деякі теми основних доповідей. Але ми сподіваємося на вашу активну участь, і в структурі наступних засідань передбачені теми доповідей, які будуть визначені й підготовлені відповідно до ваших пропозицій. Сподіваємося, що встановлення графіку засідань заздалегідь сприятиме плануванню робочого часу і робочих планів членів МЕРГ, а для організаторів буде додатковим стимулом для ритмічної та енергійної діяльності. Але запропонована вам річна програма з графіком не означає, що внесення змін неможливе. Ми будемо орієнтуватися за ситуацією, але цю програму з графіком засідань пропоную розглядати як основу нашої подальшої роботи.

Крім створення можливостей для обміну інформації та експертного спілкування, наша робота буде спрямована на підготовку аналітичних матеріалів з окремих найбільш важливих проблем, що стосуються компетенції групи. Наш Інститут сприятиме підготовці таких матеріалів для їх подальшого подання до Адміністрації Президента відповідно до встановлених процедур.

Бажаю усім успіхів у нашій подальшій спільній роботі!

ВИСТУПИ УЧАСНИКІВ

ГУЦАЛО Марія Григорівна,
головний консультант відділу стратегій реформування сектору безпеки НІСД

СОЦІАЛЬНО-ПОЛІТИЧНІ АСПЕКТИ ПРОТИДІЇ ТЕРОРИЗМУ НА СУЧАСНОМУ ЕТАПІ[3]

1. Тероризм є одним із найбільш небезпечних злочинів проти основ конституційного ладу та безпеки держави. У країнах з високим рівнем терористичної активності сформувалася тенденція щодо здійснення терактів суїцидного характеру. Черговим свідченням цього став теракт 24 січня 2011 р. у московському аеропорту Домодєдово.

Відповідно до Закону України «Про засади внутрішньої та зовнішньої політики» основними завданнями внутрішньої політики держави у сфері національної безпеки та оборони є своєчасне виявлення, запобігання та нейтралізація реальних і потенційних загроз національним інтересам. Останніми роками суверенітет України випробовувався на міцність під тиском зовнішніх політичних впливів та через уразливість національної економіки від кон'юнктури світового ринку. Накопичилися проблемні питання у сфері соціально-економічних відносин. Окреслилися тенденції радикалізації настроїв у суспільстві. Окремі кримінальні прояви резонансного характеру свідчать про високу ймовірність інтенсифікації протестних настроїв, проявів екстремізму й тероризму. За даними Служби безпеки України, у 2010 р. розкрито 135 проявів з ознаками терористичного характеру.

Нині Україна не розглядається лідерами міжнародних терористичних організацій як об'єкт терористичної активності. Тому можна говорити лише про реальні та потенційні чинники загроз міжнародного тероризму.

Високий рівень терористичних загроз у світі позначається на Україні насамперед через факти загибелі українських громадян при здійсненні терористичних актів на території інших країн. Основними каталізаторами активності міжнародного тероризму залишаються не-

[3]Кілька тематично пов'язаних виступів М. Г. Гуцало на засіданнях МЕРГ за бажанням автора представлені в збірнику у вигляді єдиної статті.

врегульованість ситуації в Іраку, Палестині, Афганістані, на Північному Кавказі РФ, збройний конфлікт між Ізраїлем та ліванською «Хезболла», «ядерне питання Ірану». Продовжують оцінюватись як високі ризики терористичних та екстремістських проявів в Індії, Пакистані, Лівані, Ємені, Сомалі, а також у Туреччині, Російській Федерації, Ізраїлі. Тому участь України у міжнародній антитерористичній коаліції, розвиток співробітництва із США та Ізраїлем, утримання на території держави інфраструктури Чорноморського флоту РФ можуть надати терористам мотивів для віднесення України до об'єктів своїх спрямувань. Не можна залишити поза увагою і загострення ситуації у країнах Близького Сходу. Сформований протестний потенціал у Єгипті, Ємені та деяких інших країнах може викликати інтенсифікацію ісламістської небезпеки.

Підвищений рівень терористичних загроз існує для установ і громадян України за кордоном. Це обумовлено збільшенням чисельності українського військового контингенту у складі Міжнародних сил сприяння безпеці в Ісламській Республіці Афганістан, залученням українського військового персоналу до роботи Тренувальної місії НАТО в Іраку, а також чутливими рішеннями України з проблемних питань регіональної безпеки на Близькому Сході. За таких обставин пріоритетним напрямом державної політики протидії тероризму є забезпечення безпеки іноземних представництв в Україні та українських дипломатичних установ і громадян за кордоном. Зазначені проблеми актуалізуються і у зв'язку з необхідністю забезпечення безпеки Євро-2012.

Іншим потенційним чинником, який може стати джерелом зовнішніх терористичних загроз Україні, є значна кількість нелегальних мігрантів, які пересуваються територією держави з кризових регіонів Росії, так званих проблемних країн Південно-Східної Азії, Близького Сходу та Перської Затоки до Західної Європи. Існуючі канали нелегальної міграції можуть бути використані міжнародними терористичними організаціями для переміщення своїх бойовиків до країн Західної Європи чи їх переховування в Україні, створення бізнесових структур для фінансового забезпечення терористичної, іншої злочинної діяльності, у тому числі спроб придбання зброї та інших засобів ураження.

Серед теророгенних чинників слід назвати також перебування на території України прихильників окремих терористичних організацій. Вони використовують канали студентського обміну, місіонерський, бізнесовий, а також нелегальний і намагаються поширювати серед населення радикальну ідеологію. На території держави відмічається

присутність осіб, які можуть бути прибічниками міжнародних радикальних організацій «Хізб-ут Тахрір», «Хамас», «Брати мусульмани» та інших закордонних структур, котрі законодавством окремих країн визнані як терористичні. Їхні осередки функціонують у Києві, Одесі, Харкові, Донецьку, Запоріжжі та формуються за рахунок іноземних студентів і вихідців із країн Близького та Середнього Сходу.

Представники закордонних релігійних екстремістських структур діють шляхом планомірного використання різноманітних форм впливу на мусульманську спільноту України. У травні 2009 р. Служба безпеки України оприлюднила інформацію про попередження створення в Україні первинних терористичних осередків партії «Хізб-ут Тахрір». Як прикриття для своєї діяльності закордонні ісламістські структури використовують недержавні організації, благодійні фонди та просвітницькі об'єднання, головні офіси яких зареєстровані на території країн Близького Сходу та Західної Європи.

Ефективним засобом для пропаганди та поширення екстремістських ідей, залучення нових членів до терористичної діяльності є мережа Інтернет. Серед веб-сайтів, представлених в українському сегменті Інтернету, є інтернет-ресурси руху «Талібан», «Хізб-ут Тахрір», «Джамаат Ісламія», «Брати мусульмани», «Хезболла» та палестинських угруповань.

Нині в Україні відмічається високий рівень насильства серед молоді; за даними Інституту соціології НАН України, у державі зберігається досить високий рівень ксенофобії стосовно окремих етносів та зниження толерантності. Міжнародна організація праці, яка є спеціалізованою установою ООН, внесла Україну до списку країн, у яких через наслідки світової фінансово-економічної кризи присутній високий ризик соціального неспокою. За оцінкою провідних міжнародних організацій, зокрема «Трансперенсі Інтернешнл», Україна у щорічному рейтингу країн за рівнем корумпованості посіла 134 місце серед 178 країн світу. Ці тривожні рейтинги свідчать про необхідність нейтралізації негативних наслідків соціально-економічних, суспільно-політичних, соціально-психологічних процесів у розвитку держави для унеможливлення терористичної активності.

На наш погляд, у системі державного управління має утвердитися розуміння того, що антитерористична діяльність визначених суб'єктів боротьби з тероризмом є лише складником державної політики у даній сфері, яка повинна мати комплексний характер і вирішуватись на засадах системної протидії. Вона повинна передбачати не лише організаційно-адміністративні та спеціальні заходи, а й попереджувальну, профілактичну діяльність, що потребує урегулювання ши-

рокого кола проблем – від подолання бідності та забезпечення прав і свобод людини і громадянина до виховання політичної та правової культури.

Специфіка сучасних проявів міжнародного тероризму актуалізує питання про удосконалення нормативно-правової бази, імплементацію норм міжнародних нормативних актів у національне законодавство. Указом Президента України від 10.12.2010 р. № 1119 визначено необхідність опрацювати з урахуванням нових викликів і загроз національній безпеці України питання про внесення змін до чинних актів законодавства у сфері боротьби з тероризмом. Це стосується уточнення передусім понятійно-категоріального апарату Закону України «Про боротьбу з тероризмом», забезпечення змістовної ідентичності основних понять у Законі «Про боротьбу з тероризмом» і Кримінальному кодексі України.

Хотілося б наголосити, що на рівні Європейського Союзу розпочато роботу з підготовки Всеосяжної стратегії боротьби з тероризмом і злочинністю, концептуальна основа якої будується на розмежуванні тероризму й злочинності. Такий підхід відповідно позначатиметься і на визначенні заходів боротьби, які відображатимуть комплексний характер даної проблеми. Такий підхід є також свідченням того, що на рівні світового співтовариства відбуваються зміни в напрямі комплексного сприйняття тероризму та визначення механізмів протидії на системній основі. Зокрема, активно вживається і вже законодавчо закріплений термін «протидія тероризму», в якому акцентовано увагу на превентивних і регулятивних механізмах запобігання терористичній небезпеці. Цей термін використовується і в Україні. Тому закономірно, що забезпечення відповідності норм права і суспільних реалій потребує коригування на законодавчому рівні.

Постає також питання про необхідність удосконалення нормативно-правової бази у сфері протидії екстремізму. Передусім це стосується правового визначення понять «екстремізм» та «екстремістська діяльність» як правопорушень з їх чіткою кваліфікацією, а також створення правових механізмів визнання конкретної структури терористичною або екстремістською, вироблення правових і процесуальних засад формування національного переліку заборонених терористичних та екстремістських організацій. Проте слід зазначити, що дане питання є дискусійним. У ст. 8 Закону України «Про основи національної безпеки» важливим напрямком державної політики з питань національної безпеки є запобігання проявам екстремізму. Однак дане поняття не визначене у національному законодавстві. Тому для уникнення його довільної кваліфікації існує необхідність

вироблення чітких критеріїв віднесеності того чи іншого суспільно-небезпечного явища до екстремізму. Можливо, тут не обійтися без ґрунтовного науково-експертного обговорення як у практичному, так і в теоретичному аспектах.

Вагомим резервом забезпечення етнорелігійної та соціальної стабільності у державі мають стати заходи з підтримання міжкультурного та міжконфесійного порозуміння. Обов'язковими в ідеологічно-пропагандистському сегменті діяльності Міністерства культури; Міністерства освіти і науки, молоді та спорту; Державного агентства з питань науки, інновацій та інформації України мають бути заходи інформаційно-пропагандистського, освітнього та виховного характеру. У цьому контексті необхідним є посилення координуючої ролі Антитерористичного центру при Службі безпеки України та активізації діяльності Міжрегіональної координаційної комісії з метою об'єднання зусиль міністерств і відомств, громадських організацій, які відповідно до Закону залучаються до протидії тероризму. Особливо важливою є така спільна робота напередодні Чемпіонату Європи з футболу 2012 р., де серед комплексу заходів слід передбачити розробку та впровадження програми інформаційно-психологічної безпеки громадян.

При цьому слід наголосити, що останнім часом в українському суспільстві відмічається тенденція посиленої уваги до тероризму, передусім з боку засобів масової інформації. Тероризмом стали називати хуліганські дії, кримінальні злочини економічного, соціально-побутового характеру. Це лише збурює суспільну думку й не додає розуміння до вкрай небезпечної сутності даного явища, що потребує виважених суджень і неупереджених оцінок.

Для забезпечення єдиного підходу на всіх рівнях держави і суспільства до розуміння сутності тероризму як загрози національній безпеці України необхідно визначити пріоритети держави у підходах до подолання тероризму з урахуванням як кримінологічної специфіки цього виду злочину, так і комплексної соціально-політичної природи даного явища. Йдеться про розробку Концепції протидії тероризму, в якій мають бути визначені основні принципи державної політики, її мета, завдання та напрями подальшої оптимізації у середньостроковій та довгостроковій перспективі.

І наприкінці дозвольте зазначити, що відкритий інформаційний обмін з питань протидії тероризму, експертне обговорення дестабілізуючих чинників соціально-політичного розвитку держави, що можуть призвести до формування терористичного підґрунтя, а також критичне осмислення сучасних шляхів протидії міжнародному те-

роризму мають важливе значення для підвищення ефективності зусиль, які здійснюються в Україні у цій сфері. У зв'язку з цим НІСД запропонував зацікавленим міністерствам та відомствам створити на базі Інституту Міжвідомчу експертну робочу групу з питань протидії загрозам розповсюдження зброї та матеріалів масового знищення, а також пов'язаних із ними терористичних загроз, і захисту критично важливої для забезпечення життєдіяльності держави інфраструктури. Такий формат співпраці, на наш погляд, сприятиме розбудові експертного середовища фахівців-терологів, надасть творчого імпульсу для подальшого удосконалення державної політики протидії тероризму.

2. Складність **проблеми суспільної радикалізації**, що призводить до тероризму, в тому, що її основою є як кризові явища у соціально-економічній, політичній, духовній сферах, так і контекст міжетнічних та міжрелігійних відносин, геополітичних і зовнішньоекономічних впливів. Це проблемне підгрунтя, на якому відбувається трансформація процесів радикалізації у безпосередню загрозу здійснення терористичних актів, стає дедалі відчутнішим в окремих країнах-членах Європейського Союзу.

Базуючись на даних Євробарометру на кінець 2011 р., громадяни Євросоюзу визначають для себе наступні ключові фактори небезпеки: економічну та фінансову кризу (33 %), тероризм (25 %), бідність (24 %), організовану злочинність (22 %), а також корупцію (18 %).

Основні тенденції радикалізації й тероризму для країн ЄС відображають показники Європейського поліцейського бюро. Якщо порівняти з 2008 р., то у 2010 р. у країнах ЄС кількість спроб та здійснених терористичних акцій зменшилася майже удвічі, дещо зменшилася і кількість затриманих за підозрою у вчиненні злочинів терористичного характеру. Проте майже незмінним залишається показник кількості осіб, обвинувачених у терористичній діяльності. У 2008 р. більшість справ була пов'язана з ісламістським тероризмом, у 2009 та 2010 рр. більшість вироків стосується осіб, причетних до сепаратистського тероризму. У 2011 р. для окремих європейських країн набула гостроти проблема радикалізації осіб, які не входять до жодного з терористичних угруповань, не мали приводів у поліцію та не перебувають у полі зору правоохоронних органів.

Новітні тенденції у розвитку тероризму відображають високий адаптивний потенціал тероризму, що загострює існуючі проблеми соціально-політичного, суспільно-психологічного, культурного розвитку.

Світова фінансово-економічна криза, яка значно вплинула на добробут населення, передусім у Греції, Іспанії, Італії, призвела до зрос-

тання кількості терористичних акцій, організованих членами ліворадикальних та анархістських груп. За даними Європолу, відмічається посилення агресивності цих угруповань, для яких пріоритетними цілями стали органи державної влади. При цьому майже удвічі зросла частка терористичних актів з використанням вибухових пристроїв.

За останні два роки особливо гострою проблемою для більшості країн ЄС стало посилення впливу ісламського фактора на суспільно-політичну, культурну, релігійну ситуацію. Вплив на рівень загрози мали події в Північній Африці, наслідком чого стало збільшення потоків нелегальних мігрантів. Водночас частина громадян ЄС, які прийняли іслам, дедалі частіше здійснюють поїздки до Афганістану, Пакистану, Сомалі, Ємену для проходження терористичної підготовки в таборах. Зокрема, чверть усіх бойовиків з іноземних держав, які входять до терористичних угруповань у Сомалі, становлять громадяни Великої Британії. Паралельно із цим ідеї збройного джихаду серед європейських мусульман і громадян ЄС поширюються завдяки практиці радикалізованих проповідників, які пройшли відповідну підготовку. За оцінками європейських експертів, ці процеси не мають тенденції до зменшення.

Незважаючи на загалом лояльне ставлення до мусульман і розуміння миролюбного характеру релігії ісламу, окремим країнам ЄС не вдається уникнути загальноєвропейської проблеми адаптації мусульман-іммігрантів, що зумовлено різницею менталітету, способу життя, ціннісними орієнтирами, пов'язаними з особливостями історичного розвитку. Одним із негативних наслідків цього процесу є перетворення мусульманських діаспор у центри радикалізації населення та джерело поширення ідеології тероризму. Підтвердженням цьому стало здійснення низки терактів проти осіб та установ, причетних до публікації карикатур на Пророка Мохамеда.

Найбільшим викликом для Західної Європи є т.зв. внутрішній тероризм. Зростання майже удвічі кількості саморадикалізованих осіб із числа громадян ЄС становить підвищену небезпеку з огляду на складність їх виявлення. Ефективність діяльності терористів-одинаків, які здійснюють теракт без прямого контакту з терористичними організаціями, була доведена в Німеччині та Норвегії. Внаслідок теракту, який здійснив громадянин Німеччини – за походженням косовський албанець, загинули військовослужбовці США. Теракт у Норвегії, який відзначався високим рівнем організації та масовими жертвами, був розрахований на те, щоб дати поштовх своєрідній ланцюговій реакції серед однодумців в інших країнах ЄС проти подальшої імміграції мусульман. У французькій Тулузі жертвами Моххамеда Мера

стали єврейські діти. Зазначені факти свідчать про те, що у свідомості значної кількості людей як у сучасній Європі, так і на Близькому Сході виявилася подоланою дуже важлива межа, пов'язана із ціною людського життя. Прірва між офіційно задекларованими толерантністю, «діалогом культур і релігій», що повинні торувати шлях до гуманізації людства, та життєвими реаліями з часом поглиблюється дедалі більше.

Проблема тероризму в низці європейських країн усе сильніше переплітається з діяльністю злочинних угруповань, передусім організованих за етнічною ознакою. Зокрема, за даними Євроюсту, більшість кримінальних справ, порушених у Бельгії у зв'язку зі злочинами терористичного характеру, стосується вихідців з Північного Кавказу.

Аналіз відкритих даних стосовно процесів радикалізації в окремих країнах ЄС та окремих державах пострадянського простору дозволяє зробити висновок про поширення даних процесів на пенітенціарну систему. Йдеться про радикалізацію ув'язнених під впливом ісламістської ідеології у виправних установах. Європейські експерти зазначають, що бойовики знаходять потенційних терористів серед ув'язнених, засуджених за релігійний екстремізм, які швидко адаптуються до тюремних умов, поширюють радикальні релігійні настрої, створюють так звані тюремні джамаати. Після звільнення члени організованих злочинних формувань продовжують кримінальну діяльність, проте вже релігійно забарвлену. Ці процеси призводять до того, що злочинний світ почав гуртуватися довкола ісламської релігійної доктрини, наслідком чого стає надзвичайно високий рівень агресії та насильства нової ідентичності членів організованих злочинних угруповань. Під впливом цих процесів відбувається перерозподіл сфер впливу та зміна ієрархії в кримінальному середовищі.

Найефективнішим каналом поширення радикальної ідеології тероризму став нині інформаційний простір. З цією метою використовуються як інтернет-форуми закритого характеру, так і соціальні мережі, які дають змогу вирішувати значно ширший спектр завдань. Сьогодні через інформаційно-пропагандистські ресурси поширюються звернення до мусульман країн Заходу здійснювати теракти в ініціативному порядку, для чого на веб-сайтах розміщуються настанови, інструкції для дотримання як спеціальних заходів безпеки при проведенні операцій, так і загальних правил поведінки для виконавця теракту. Так, внаслідок здійсненої спецслужбами Великої Британії операції «Мазхар» було виявлено 180 веб-сайтів, через які здійснювалася інформаційно-психологічна обробка для рекрутингу потенційних терористів, надання фінансової допомоги. На них розміщувалися також звернення до мусульман країн Заходу здійснювати теракти в

ініціативному порядку із застосуванням не саморобних вибухових пристроїв, а вогнепальної зброї, придбання якої не привертає уваги правоохоронних органів. Особливостями сучасної інформаційно-психологічної кампанії терористів є посилення її насиченості та здатності забезпечити непомітність схилення об'єкта до впливу радикальної ідеології.

Закономірною реакцією на спалах активності радикалізованих осіб, на поступове зростання рівня терористичної загрози стали кроки урядів країн ЄС щодо впровадження превентивних заходів, спрямованих на недопущення переростання загрози радикалізації у безпосередню терористичну загрозу. Основна увага приділяється засобам масової інформації та інтернет-простору; припиненню діяльності мереж та окремих осіб, які втягують людей у терористичну діяльність, передусім молодь та жінок; створено європейську мережу моніторингу радикалізації; упроваджуються механізми раннього виявлення ознак радикалізації та загроз поширення насильства й екстремізму.

У зв'язку з цим слід звернути увагу на Антитерористичну стратегію Великої Британії, в якій у 2011 р. суттєво оновлено один із її складників – Стратегію запобігання. Три ключових завдання цієї стратегії – протидія поширенню терористичної ідеології; захист і підтримка осіб, уразливих для екстремістської й терористичної ідеології; підтримка освітніх, релігійних, культурних і виправних установ, де існує небезпека радикалізації громадян. Ці напрямки розробляються та впроваджуються за рахунок прямого співробітництва та взаємодії між безпековими службами країн-членів ЄС.

Стосовно ситуації в Україні слід зазначити наступне. Згідно з результатами соціологічного дослідження факторами небезпеки для громадян України є бідність (66 %), корупція (53 %), економічні та фінансові кризи (40 %), вулична злочинність (35 %), тероризм (4 %). Серед негативних і гострих виявів сучасного періоду системної трансформації – різка соціальна поляризація населення України на тлі збагачення й демонстративного споживання заможної частини. Для більшості населення стали недоступними звичні раніше стандарти життя, добробут, можливості людського розвитку. Безумовно, не можна говорити про пряму кореляцію між бідністю і радикальними екстремістськими й терористичними проявами. Проте незадоволення населення умовами матеріального існування (як вияв депривації) зумовлює низку супутніх обставин, які можуть спричинити інтенсифікацію соціального протесту і є показником соціальної напруженості. Небезпечним наслідком цих процесів на психологічному рівні є прискорення невротизації населення.

Триваюча соціально-економічна криза здійснює суттєвий вплив на загальний рівень криміногенної ситуації. Злочинність стала однією із загроз національній безпеці. За даними МВС, стійкими є показники щодо незаконного обігу вибухонебезпечних речовин різного типу, а також вогнепальної зброї, в тому числі із сучасними бойовими характеристиками. Потенційними чинниками, що можуть сприяти поширенню на територію України діяльності міжнародних терористичних та екстремістських організацій, є прозорість кордонів, ліберальна візова політика, можливість легалізації бізнесу для отримання коштів, значні обсяги нелегальної міграції, контрабанда зброї, наркотиків.

З 2001 р., із часу уведення в дію 258 ст. КК, в Україні за цією статтею порушено 22 кримінальні справи. За даними Служби безпеки України, у 2010 р. розкрито 135 проявів з ознаками терористичного характеру. Загалом, на даному етапі лідери міжнародних терористичних організацій не розглядають Україну як об'єкт цілеспрямованих посягань. Проте перебування на території держави прихильників міжнародних релігійно-екстремістських угруповань створює додаткові ризики безпеці, особливо у зв'язку з проведенням в Україні Євро-2012.

За останні два десятиліття поміркований іслам став реальним чинником суспільного життя в Україні, водночас його політизовані радикальні версії поширились у середовищі мусульман. Процеси радикалізації частини мусульман Криму зумовлені не тільки зовнішнім впливом ідей хабашизму, ваххабізму та пантюркізму, а й проблемами соціально-економічного характеру, складнощами соціалізації кримсько-татарської молоді, не до кінця вирішеними земельними питаннями. Важливу роль у процесі радикалізації відіграють емісари закордонних ісламських релігійно-екстремістських організацій, одним із профільних видів діяльності яких є підбір та відправка абітурієнтів на навчання до теологічних навчальних закладів світу. Зміст навчальних програм, а також тривале перебування слухачів за кордоном інтенсифікують процес їхньої радикалізації, який виявляється і після повернення на батьківщину.

Пріоритетного значення для протидії терористичним загрозам набуває запобігання терористичним проявам, їх профілактика. Для реалізації цього завдання необхідно відновити інститут профілактики, який існував у державі у сфері попередження злочинності протягом тривалого часу і доводив свою ефективність. Складність організації профілактики злочинів терористичного характеру в тому, що тероризм як нелегітимна форма політичного насилля має соціально-політичний характер та ідеологічне обґрунтування. Виходячи із цього,

пріоритетного значення у профілактичній діяльності набувають соціальні, інформаційні, освітні, гуманітарні аспекти. Вони повинні стати невід'ємним складником загальнодержавної системи заходів профілактики. Обов'язковими в ідеологічно-пропагандистському сегменті діяльності відповідних державних структур мають бути заходи з контрпропаганди тероризму та релігійного екстремізму. Комплекс заходів профілактичної спрямованості має бути відображений у Програмі антитерористичних заходів, яка затверджується Президентом України і формується Антитерористичним центром при СБ України. Одним з основних її завдань є розроблення концептуальних засад і програм боротьби з тероризмом, а також рекомендацій, спрямованих на підвищення ефективності заходів щодо виявлення та усунення причин та умов, які сприяють вчиненню терористичних актів та інших злочинів, здійснюваних із терористичною метою.

3. Запобігання зростанню радикальних настроїв і попередження жорстокості в українському середовищі має важливе значення для національної безпеки й захисту громадян від терористичних проявів. Загалом, ускладнення соціально-економічної ситуації потребує системної регуляції конфліктогенних чинників на загальнонаціональному рівні задля зниження безпекових ризиків, стабілізації соціально-політичної обстановки, збереження територіальної цілісності держави. З метою забезпечення громадського спокою і стабільності в державі, недопущення протиправних проявів, пов'язаних із терористичною діяльністю, 8 червня 2012 р. Указом Президента України № 388 уведено в дію рішення Ради національної безпеки і оборони України від 25.05.2012 р. «Про заходи щодо посилення боротьби з тероризмом в Україні». В ньому передбачено реалізацію нагальних питань організаційно-правового, інформаційно-аналітичного, кадрового забезпечення антитерористичної діяльності.

Важливим кроком для розробки концептуальних основ діяльності держави й суспільства у сфері боротьби з тероризмом є передбачена зазначеним рішенням Ради національної безпеки і оборони України підготовка Концепції боротьби з тероризмом. Вона сприятиме формуванню цілісного комплексу знань про сутність і зміст боротьби з тероризмом та основи організації відповідного механізму протидії; забезпеченню єдності, цілеспрямованості та узгодженості функціонування його складників, передусім основних суб'єктів боротьби з тероризмом. Як важливий політико-програмний документ стратегічного рівня Концепція повинна сформувати єдиний підхід на всіх рівнях держави і суспільства до розуміння тероризму як загрози національній безпеці України, а також системне сприйняття цієї загрози

як багатопланової небезпеки для різних сфер національної безпеки держави, для життєво важливих інтересів особи, суспільства та держави, чітке бачення взаємозв'язку тероризму та існуючих у світі та державі соціальних суперечностей, ролі у цьому комплексі зовнішніх та внутрішніх чинників, їх значення в детермінації сучасного тероризму. Розробка концептуальних основ боротьби з тероризмом матиме важливе значення для виховання антитерористичної свідомості громадян.

4. Десять років, що минули цьогоріч від дня трагедії 11 вересня 2001 р., є вагомим приводом для того, щоб зробити певні проміжні висновки та підбити підсумки т.зв. безкомпромісної війни з тероризмом, яку розпочала міжнародна спільнота. 34 держави – члени антитерористичної коаліції, яка від самого початку мала досить умовний характер, досягли значних успіхів у знешкодженні керівників терористичних угруповань середньої та вищої ланки. Однак при цьому кількість загиблих становить десятки тисяч невинних жертв. 10 років боротьби показали, що тероризм є надзвичайно політизованою проблемою, і досягнення консенсусу щодо прийняття важливих рішень у боротьбі із цим злочином проти людяності щоразу наражається на різницю у поглядах та підходах як щодо поняття тероризму, так і стратегії й тактики боротьби з ним.

Ідеологічно-пропагандистський формат боротьби з тероризмом став для міжнародної спільноти дуже складним завданням, оскільки розгалужена мережа радикальних салафітів, використовуючи релігійну догматику, нині досить успішно поширює радикальну ідеологію насильства. Ці м'які засоби впливу на свідомість людини є надзвичайно небезпечним явищем. І тому, на мій погляд, процеси політизації ісламу, їх вплив на систему міжнародних відносин потребують подальшого ґрунтовного дослідження, що є актуальним також і для Української держави.

Концептуальна різниця у підходах до інтересів безпеки у США, країнах ЄС, наслідки фінансово-економічної кризи зумовили перегляд стратегічної перспективи боротьби з тероризмом та відповідно скоригували антитерористичні заходи в тактичному відношенні.

Дозвольте стисло викласти основні положення нової Контртерористичної стратегії США, прийнятої у 2011 р., та блок антитерористичних заходів Стратегії внутрішньої безпеки Європейського Союзу 2010 р., який пропонується для реалізації на період 2011–2014 рр. Ці документи знаменують початок нового етапу у боротьбі з тероризмом і наочно демонструють концептуальну різницю у підходах у США та країнах ЄС.

Отже, до 11 вересня 2001 р. тероризм не розглядався США в якості головної загрози Західній півкулі. Рубіжними стали події 11 вересня, після яких було прийнято антитерористичний закон *USA PATRIOT ACT*, а згодом сформовано антитерористичну стратегію 2006 р., якими проголошено «глобальну війну з тероризмом». Нова контртерористична стратегія визначає загальні підходи американського уряду до проблеми боротьби з тероризмом і механізми, необхідні для її успішної реалізації. Документ базується на основних засадах попередніх стратегій, але водночас ураховує зміни, які протягом останніх років позначились на розвитку поглядів США на проблему боротьби з тероризмом. На відміну від останньої редакції 2006 р., нова Стратегія є більш конкретизованою щодо визначення загроз і завдань у зазначеній сфері.

Розглянемо далі основні положення цієї Стратегії:

• головна мета контртерористичних зусиль США на сучасному етапі – припинити, зруйнувати і зрештою завдати поразки мережі Аль-Каїда, афілійованим із нею організаціям і прибічникам з метою забезпечення безпеки громадян США та американських національних інтересів;

• головну увагу вперше зосереджено на можливостях Аль-Каїди та її союзників спонукати мешканців США до здійснення терористичних актів на території своєї країни, тобто без прямого зовнішнього втручання. Таким чином, Стратегія – перший документ такого рівня, який визначає національну територію США як головний об'єкт антитерористичних зусиль з боку американського уряду;

• термін «війна» використовується виключно в контексті кампанії, спрямованої проти Аль-Каїди як терористичної мережі. США не вважають себе у стані війни з тероризмом (як тактикою дій) або мусульманською релігією;

• США не планують боротися з усіма терористичними організаціями світу, більшість з яких ніколи не мали ані намірів, ані можливостей для здійснення терористичних актів проти США або американських громадян;

• разом з тим у світі існують певні держави та угруповання, які підтримують тероризм з метою протистояння інтересам США. Головними державами-спонсорами тероризму США визнає Іран та Сирію, найбільш небезпечними організаціями – «Хезболлах» і «Хамас», які становлять загрозу Ізраїлю та інтересам США на Близькому Сході. Сполучені Штати мають намір застосовувати весь спектр інструментів зовнішньої політики для унеможливлення завдання шкоди американським інтересам цими режимами та організаціями.

Стратегія є першим документом концептуального характеру у сфері безпеки, прийнятим у США після дуже важливих із стратегічної точки зору подій на Близькому Сході та в Північній Африці. Зміни, що відбуваються тут, можуть призвести до появи нових викликів уже в найближчій перспективі, про що свідчить розвиток подій у Ємені.

Найбільш небезпечним джерелом теперішніх і майбутніх терористичних загроз є діяльність досить потужної терористичної організації «Аль-Каїда на Аравійському півострові», яка базується в Ємені. Цьому на даному етапі сприяє політична нестабільність у країні, яка перебуває на межі громадянської війни. Дана терористична організація зберігає значний воєнний потенціал, ставлячи за мету створення умов для утворення на підконтрольних Ємену територіях ісламських еміратів. До того ж саме ця організація здійснює потужну інформаційно-пропагандистську діяльність, об'єктом якої є населення країн Заходу.

Головне завдання США союзників та партнерів у цій ситуації – не допустити використання безпекового та владного вакууму в насильницьких цілях. Політика США у сфері контртероризму не є визначальним чинником формування американської зовнішньої політики, натомість її невід'ємним складником, який посилює безпековий компонент цієї політики.

Згідно зі Стратегією основними принципами, на яких будуються контртерористичні зусилля США, є:

• дотримання основоположних американських цінностей;

• розбудова відносин партнерства у сфері безпеки;

• упровадження скоординованих зусиль у загальноурядовому масштабі; баланс довго- та короткострокових підходів;

• дотримання принципу непохитності та стійкості, що має демонструвати готовність США запобігти, а якщо необхідно – швидко ліквідувати наслідки, відновити потенціал і дати гідну відповідь будь-якому теракту, здійсненому проти США.

Стратегія визначає 8 головних цілей, досягнення яких становитиме запоруку успіху глобальної антитерористичної місії США:

• захист американського народу, держави та американських інтересів;

• завдання поразки мережі Аль-Каїда, її союзникам і прибічникам;

• недопущення розробки, отримання та застосування зброї масового ураження із терористичною метою;

• ліквідація «сірих зон», безпечних для переховування, підготовки та розташування баз терористів;

• розбудова постійного антитерористичного партнерства;

• порушення зв'язків між Аль-Каїдою, її регіональними осередками, прибічниками;

• протидія ідеології Аль-Каїди;

• позбавлення терористів засобів для існування та здійснення своєї діяльності.

Сферою та напрямами особливої уваги є:

• безпосередньо територія США;

• Південна Азія: Аль-Каїда, пов'язані з нею організації та прибічники;

• Аравійський півострів: Аль-Каїда та Аль-Каїда на Аравійському півострові (АКАП);

• Східна Африка: Аль-Каїда у Східній Африці та «Аль-Шабаб».

• Територія Європи;

• Ірак: Аль-Каїда в Іраку (АКІ);

• Північна Африка: Аль-Каїда у країнах ісламського Магрибу (АКІМ);

• Південно-Східна Азія: Аль-Каїда та афілійовані з нею організації та прибічники;

• Центральна Азія: Аль-Каїда, її союзники та прибічники;

• інформаційно-пропагандистська сфера: ідеологія та комунікативна стратегія Аль-Каїди.

Як задекларовано Адміністрацією США, Стратегія відображає нову політику президента Б. Обами у сфері боротьби з тероризмом, яка включає такі компоненти:

• зосередження першочергових зусиль на нейтралізації лідерів та найбільш впливових керівників терористичних організацій;

• поглиблення співробітництва з союзниками та партнерами з метою протидії терористичній ідеології та поширенню екстремізму;

• упровадження системних заходів, спрямованих на відновлення світового впливу США.

Можна очікувати, що на найближчу перспективу саме ці три компоненти визначатимуть (багато у чому – пояснюватимуть) подальші практичні кроки США в напрямі боротьби з тероризмом, у т.ч. у сфері міжнародних відносин і розбудови стосунків з партнерами.

Зміна пріоритетів у боротьбі з тероризмом відповідно зумовила корекцію тактики протидії: новий етап полягає не в застосуванні масштабних військових формувань, дислокованих поза межами країни, а в проведенні «хірургічних операцій у конкретному місці». Отже, зміна концептуальних підходів США у боротьбі з тероризмом відповідно зумовить і практичні кроки уряду, в т.ч. у сфері міжнародних

відносин і розбудови стосунків з партнерами, що передбачатиме їх максимальне залучення з подальшим перекладанням на них частини повноважень та відповідальності за цей напрям американської зовнішньої політики. Такі дії зумовлені соціально-економічними проблемами в країні, що не могло не вплинути на значне скорочення обсягу фінансування спецслужб у 2011 р., бюджет яких у 2010 р. становив 80 млрд дол. США.

Форматом практичної реалізації позицій нової контртерористичної стратегії США став Глобальний антитерористичний форум, щойно проведений з ініціативи Вашингтона. Цей форум репрезентовано як новий міжнародний механізм антитерористичного співробітництва 29 держав, у т.ч. Індії, Китаю, РФ та Європейського Союзу. В його складі функціонуватиме координаційний комітет; 5 тематичних і регіональних експертних груп. Одним із важливих рішень цього форуму є, на мій погляд, створення багатостороннього центру підготовки та досліджень у сфері боротьби з тероризмом.

Власне, сама поява такого механізму свідчить про те, що США певною мірою перебирають на себе повноваження у протидії екстремізму й тероризму, що реалізуються загалом через механізм ООН, роботу якої все більше критикують з точки зору неефективності заходів боротьби з тероризмом. Конвенційний механізм ООН, який є основним інструментом у боротьбі з тероризмом, щоразу доводить свою неспроможність охопити регулюючою дією нові форми й методи діяльності терористичних організацій.

Переходячи до короткого аналізу антитерористичних новацій європейської безпекової політики, слід сказати, що у питаннях боротьби з тероризмом вона орієнтована на дотримання основоположних цінностей прав людини, основних свобод і принципу верховенства права. Ці базові положення відображені в конвенції Ради Європи щодо попередження тероризму 2005 р. Особливістю цієї стратегії є установка на криміналізацію тероризму та кримінальне переслідування причетних до терористичної діяльності. Контртерористичні заходи ЄС включають європейський ордер на арешт, посилення візової системи в межах Шенгенської зони, біометричні дані у паспортах, протидію фінансуванню тероризму, попередження радикалізації молоді. Власне, це та система заходів протидії тероризму, яка є актуальною і для України.

Після набуття чинності Лісабонського договору Європейський Союз на початку 2010 р. зробив наступний важливий крок, прийнявши Стратегію внутрішньої безпеки, в якій особливу увагу приділено загрозам безпеки ЄС, пов'язаним із організованою злочинністю, теро-

ризмом, кіберзлочинністю, безпекою кордонів та природними й техногенними катастрофами.

Ситуація й тенденції у сфері боротьби з тероризмом у країнах Європейського Союзу свідчать про те, що на загальний рівень терористичної загрози в Європі продовжує негативно впливати діяльність ісламістських, сепаратистських, ліворадикальних, анархістських і праворадикальних екстремістських і терористичних угруповань. Продовжується зростання кількості так званих саморадикалізованих осіб з числа громадян ЄС, які становлять підвищену небезпеку з огляду на складність їх виявлення. Тому невід'ємними складниками запобігання тероризму є попередження радикалізації та вербування громадян.

Через складну внутрішньополітичну ситуацію у Великій Британії та Франції, пов'язану із зростанням соціальних протестів та масовими погромами, а також насильницькими діями проти іммігрантів, уряди цих країн головну увагу зосередили на запобіганні втягування громадян країн у терористичну діяльність або сприяння такій діяльності. Зокрема, антитерористична стратегія Великої Британії 2007 р. не передбачала боротьбу з екстремістською ідеологією. Нова стратегія 2011 р. найбільшою мірою зосереджена на всіх формах тероризму та екстремізму, включаючи діяльність ультраправих політичних рухів (приклад Норвегії). Три основних завдання Стратегії:

• протидія поширенню ідеології, яка схвалює або пропагує терористичну діяльність;

• захист і підтримка осіб, уразливих для екстремістської або терористичної ідеології;

• підтримка закладів, установ та організацій, у яких існує небезпека радикалізації громадян.

Основними положеннями Стратегії внутрішньої безпеки ЄС у сфері боротьби з тероризмом є:

• попередження радикалізації та вербування громадян для участі в терористичній діяльності шляхом розширення можливостей громадянського суспільства, місцевих органів влади й експертного співтовариства;

• позбавлення терористів доступу до фінансів, відстеження й перекриття фінансових операцій у спосіб заморожування активів та запобігання доступу до вибухових, біологічних, хімічних і ядерних речовин. На рівні Європолу буде розроблено систему раннього попередження інцидентів, пов'язаних із застосуванням ядерних речовин. Ці дії вимагатимуть тісної координації держав-членів та розвитку державно-приватного партнерства;

• останній напрямок Стратегії внутрішньої безпеки з питань запобігання тероризму стосується безпеки на транспорті, передусім авіаційному та морському. Безпека на транспорті забезпечуватиметься з дотриманням балансу необхідного рівня безпеки та прав людини шляхом проведення ефективних інспекційних і режимних заходів, моніторингу вантажних і пасажирських перевезень.

Загалом Стратегія демонструє стійку тенденцію європейської безпекової політики до впровадження заходів м'якої безпеки, яка у складній соціально-політичній ситуації економічної кризи, вибухових процесів у міграційній політиці є найбільш оптимальним варіантом послідовних дій ЄС у боротьбі з тероризмом. Проте дотримання балансу між демократичними цінностями та правами людини на тлі соціально-економічних потрясінь на даному етапі і в подальшому зазнаватиме тиску й коригуватиметься.

Слабким місцем діяльності Європейського Союзу у сфері боротьби з тероризмом є нечітка координація спецслужб держав-членів ЄС і незначна результативність заходів. Найбільш дієвим механізмом, у т.ч. для протидії тероризму, є діяльність Європолу. Уведено пост координатора по боротьбі з тероризмом ЄС, щоправда, його повноваження не мають прямої дії і цій посаді притаманний досить символічний характер.

Найслабкішим місцем сучасної контртерористичної політики є недостатня координація спеціальних служб. Боротьба з тероризмом залишається надто політизованою сферою співробітництва як для США, так і в межах ЄС. Як свідчить ситуація в окремих країнах ЄС (Великій Британії, Франції, Іспанії), де тероризм є гострою проблемою національної безпеки, національний прагматизм при визначенні комплексу антитерористичних заходів превалює над координаційними механізмами ЄС і є відповідно пріоритетним. Це значною мірою створює перешкоди, наприклад при застосуванні ордеру на арешт для видачі терористів не тільки в межах ЄС.

Для України важливими напрямками співробітництва з ЄС є взаємодія під час підготовки законопроектів, навчання фахівців правоохоронних і судових органів, обміну досвідом на міждержавних конференціях та семінарах. Існує також низка перспективних напрямів налагодження двостороннього співробітництва. Одним із таких є обмін досвідом у сфері протидії соціально-політичній радикалізації певної частини мігрантів. У середньостроковій та довгостроковій перспективі Україна може зіткнутися з проблемами інтеграції та радикалізації мігрантів та біженців, які проживають в Україні.

5. Невід'ємними складниками політики боротьби з тероризмом є інформаційно-аналітичний і науковий напрями. Для Української

держави, де нині відсутні прямі ознаки підготовки та вчинення терористичних актів, особливої ваги набуває системна робота наукової спільноти з розробки теоретичних і методологічних основ запобігання тероризму, рекомендацій для вирішення практичних завдань із конкретних напрямів попереджувально-профілактичної діяльності; здійснення науково-прикладних досліджень для прийняття організаційно-правових, управлінських рішень; вивчення міжнародного досвіду.

Національний інститут стратегічних досліджень є базовою науково-дослідною установою аналітико-прогнозного супроводження діяльності Президента України. Інститут здійснює наукові розробки питань внутрішньої і зовнішньої політики, в т.ч. у сфері національної безпеки України. Питання вдосконалення державної політики протидії терористичній загрозі є самостійним напрямом науково-дослідної роботи Інституту. У цьому контексті здійснюються дослідження міжнародного досвіду боротьби з тероризмом, окремих напрямів удосконалення державної політики протидії тероризму, проблемних питань ресурсного забезпечення антитерористичної діяльності. Наукові доробки висвітлюються в науково-аналітичних матеріалах, аналітичних доповідях і наукових статтях.

У 2011 р. в Інституті проведено «круглий стіл» з питань пріоритетів та шляхів реалізації державної політики протидії тероризму, у роботі якого взяли участь представники органів державної влади, наукових інституцій, громадські діячі. За результатами роботи «круглого столу» випущено збірник матеріалів.

У планах роботи на 2012 р. – проведення науково-практичної конференції з питань міжнародного та національного досвіду запобігання радикалізації й тероризму. Такий напрям діяльності Інституту корелюється із пріоритетними напрямами нової антитерористичної програми Ради Європи з удосконалення запобіжних механізмів, спрямованих на усунення причин і умов, що породжують екстремізм і тероризм, дотримання прав людини, основних свобод і принципу верховенства права.

Як уже зазначалося, у 2011 р. Національний інститут стратегічних досліджень запропонував зацікавленим міністерствам і відомствам держави створити на його базі Міжвідомчу експертну робочу групу з питань протидії загрозам розповсюдження зброї та матеріалів масового знищення, а також пов'язаних із ними терористичних загроз, і захисту критично важливої інфраструктури. Протягом року на регулярній основі відбуваються засідання експертної робочої групи, робота якої сприяє налагодженню тісніших міжвідомчих контактів,

обміну інформацією між експертами та науковцями, створює можливості для ефективнішого інформаційно-аналітичного супроводження процесу прийняття управлінських рішень.

Дослідження питань демографічного, соціального, етнополітичного, інформаційного розвитку України, що здійснюються в Інституті, можна розглядати як вагомий науково-інформаційний компонент моніторингу процесів радикалізації, започаткованого Європейським Союзом. У зв'язку із цим хотілося б приділити більшу увагу обміну досвідом із європейськими партнерами з питань протидії соціально-політичній радикалізації певної частини масової міграції, особливо у другому поколінні, який накопичено у Франції та Німеччині.

КОНДРАТОВ Сергій Іванович,
науковий співробітник відділу екологічної та техногенної безпеки НІСД

ПІДТРИМАННЯ ФІЗИЧНОЇ ЯДЕРНОЇ БЕЗПЕКИ ПІД ЧАС КОМПЛЕКСНОЇ КРИЗИ

Світовий інститут з фізичної ядерної безпеки (*World Institute for Nuclear Security, WINS)* оприлюднив спеціальний бюлетень, присвячений урокам і висновкам, які вже зараз можна зробити після аварії на АЕС Фукусіма-1. Назва цієї публікації – «Підтримання фізичної ядерної безпеки під час комплексної кризи» (*Maintaining nuclear security in a complex crisis)*.

Хоча це коротка публікація, але досвідчені експерти з питань фізичної ядерної безпеки «по гарячих слідах» визначили проблемні моменти, пов'язані з підтриманням фізичної ядерної безпеки при стихійних лихах і техногенних аваріях такого масштабу. З повним текстом цієї публікації членам *WINS* можна ознайомитися на сайті інституту[4].

У бюлетені надруковано коротку хронологію подій до моменту публікації матеріалу, на чому нема потреби зупинятися, оскільки, по-перше, ситуація продовжувала змінюватись, і, по-друге, на основну увагу заслуговує точка зору експертів щодо фізичної безпеки аварійної АЕС та їхні попередні висновки з цього приводу. Далі представлені основні висновки та рекомендації публікації в короткому викладі.

[4][Електронний ресурс]. – Режим доступу: http://www.wins.org

На основі аналізу аерофотозйомок і репортажів ЗМІ зроблено висновок, що землетрус і цунамі зруйнували основну частину системи фізичного захисту АЕС, а також зробили неможливим ефективний зв'язок з об'єктом. Пошкоджень зазнали мережі мобільного зв'язку, що ще більше утруднило реагування.

Раптові та неочікувані за масштабами катастрофічні наслідки стали причиною того, що значна частина персоналу з фізичної безпеки на майданчику АЕС, а також члени зовнішніх команд первинного реагування були зненацька захоплені стихійними лихами й виявилися або неспроможними взяти участь у реагуванні, або були задіяні в операціях зі спасіння (гуманітарної допомоги) в інших місцях.

Подальший розвиток кризи, пов'язаний з неможливістю ефективного охолодження реакторів, та виток радіації змусили здійснити часткову евакуацію персоналу об'єкта. Спираючись на повідомлення ЗМІ та офіційні заяви, автори зробили висновок, що внаслідок занепокоєності зростанням рівня радіації, який вельми загрожував здоров'ю людей, на АЕС залишився лише основний інженерний склад, відповідальний за експлуатацію та обслуговування станції. Тривала відсутність електроенергії не тільки на АЕС Фукусіма-1, а й в усьому регіоні, безумовно, суттєво знизила ефективність автоматизованих систем фізичної безпеки, включаючи об'єктові системи телевізійного спостереження (*Closed Circuit Television Systems*), системи сигналізації на периметрі АЕС, а також системи виявлення проникнення порушників (*Intruder Detection System*), які фактично були скомпрометовані.

У бюлетені сказано і про реакцію на цю аварію на міжнародному рівні. Так, проти урядів країн та компаній-власників АЕС у багатьох країнах світу прокотилася хвиля протестів з вимогами заборонити експлуатацію АЕС і скасувати подальші плани розвитку ядерної енергетики.

Криза на японській АЕС Фукусіма-1 здебільшого розглядається виключно як подія, пов'язана лише із забезпеченням технічної ядерної безпеки (*nuclear safety*). У повідомленнях і заявах не згадуються проблеми фізичної безпеки об'єкта попри той факт, що залишок робітників, який бере участь в операціях на АЕС, відноситься лише до оперативного технічного персоналу.

У той час, коли пріоритет у заходах із реагування абсолютно обґрунтовано надано проблемам технічної безпеки з тим, щоб уникнути подальшого розвитку катастрофічних наслідків та ризиків для здоров'я людей, також важливо розглянути ризики щодо фізичної безпеки і зробити правильні висновки. АЕС нині обслуговується скороченим за чисельністю персоналом, і критично важливі для фізич-

ної безпеки об'єкта системи або пошкоджені, або не виконують свої функції внаслідок відсутності електроенергії або пошкодження відповідної інфраструктури. Крім економічних втрат і ризиків, комплексна криза ставить низку питань щодо фізичної безпеки. Хоча деяким із цих питань притаманний локальний характер, однак багато з них матимуть значно ширший вплив, тому всі вони повинні розглядатися міжнародним співтовариством з фізичної ядерної безпеки.

У короткостроковій перспективі японська ядерна криза викличе зростання протестних дій у всіх їхніх проявах. Тиск з боку населення, політичних кіл та регуляторів диктуватиме застосування більш жорстких, ніж уже заплановано, заходів зі зниження ядерних ризиків на існуючих майданчиках, а плани будівництва майбутніх об'єктів дуже прискіпливо переглядатимуться. У середньостроковій перспективі за таких умов імовірно, що обмежені ресурси будуть спрямовані від сфери забезпечення фізичної безпеки на заходи для підвищення технічної безпеки, яка стане домінувати при оцінці ризиків.

Картини лиха й подальшої аварії, що спіткала АЕС Фукусіма-1, стали доступними для спостереження терористами, в т.ч. тими, які представляють їх нове покоління. Вони стали свідками величезного впливу, який спричиняє така подія на людство, довкілля, економіку та політику. У зв'язку із цим експерти *WINS* передбачають, що ядерні та радіоактивні матеріали викликатимуть ще більший інтерес з боку терористів, ніж це було до японської ядерної кризи.

Що ж робити далі? У публікації *WINS* пропонуються такі заходи.

Перегляд планів дій у надзвичайних ситуаціях. *WINS* пропонує переглянути плани дій на випадок надзвичайних ситуацій, включаючи й ті, що вважалися раніше малоймовірними. При цьому необхідно зробити акцент на питанні, що слід вважати ймовірною загрозою для технічної та фізичної безпеки ядерного об'єкта. Слід звернути увагу на оцінку каскадних ефектів, які були недостатньо враховані на АЕС Фукусіма-1.

Перегляд планів управління ризиками у процесі інформування про надзвичайні ситуації. Вплив аварії на АЕС Фукусіма-1 розповсюдився далеко за межі сфери здоров'я персоналу та населення, спричинивши значну дію на фундаментальні проблеми сприйняття ризиків населенням. На думку авторів, за таких умов дезінформація може дуже дорого коштувати, оскільки може сприяти значному зростанню протестних настроїв, чого необхідно уникати, здійснюючи випереджувальні інформаційні кампанії.

Визнання необхідності повного усвідомлення реальної ситуації. Повне усвідомлення всієї складності ситуації вимагає, щоб усі осо-

би, які відповідають за прийняття рішень, мали своєчасний доступ до найбільш надійної інформації про подію. Японська ядерна криза показала наявність проблем, характерних для управління інформацією під час комплексної кризи.

Перегляд загроз. Картини руйнування, страху, масової розгубленості, спричинені ядерною аварією, можуть лише сприяти посиленню бажання терористичних груп досягти своїх цілей через зловмисні дії з використанням таких матеріалів та установок. У зв'язку з цим необхідно переглянути рівні загроз і ризиків, які спричиняє терористична діяльність у світі.

Перегляд оцінок доцільності застосування принципу «Фізична безпека – проектними заходами».

Забезпечення принципу «безперервності фізичної безпеки». Приклад аварії на АЕС Фукусіма-1 показує, що неврахування додаткових факторів ризику може призводити до того, що разом із системами фізичної безпеки можуть повністю вийти з ладу і системи фізичного захисту, для запобігання чому необхідно вживати певних заходів уже на етапі проектування.

СКАЛЕЦЬКИЙ Юрій Миколайович,
завідувач відділу
екологічної та техногенної безпеки НІСД,
заступник керівника МЕРГ;
БІРЮКОВ Дмитро Сергійович,
старший консультант відділу
екологічної та техногенної безпеки НІСД

ПРОБЛЕМИ РЕГУЛЮВАННЯ ПРОТИРАДІАЦІЙНОГО ЗАХИСТУ В АВАРІЙНИХ СИТУАЦІЯХ

На відміну від лімітів доз опромінення персоналу і різних категорій населення в повсякденних умовах використання джерел іонізуючого випромінювання, регламентації опромінення аварійного персоналу приділяється значно менше уваги як у міжнародних і національних документах з радіаційного захисту, так і в наукових публікаціях з протирадіаційного захисту та радіаційної безпеки. Майже відсутні матеріали, що стосуються обмеження опромінення аварійного персоналу, діяльність якого спрямована, наприклад, на врятування життя людей

в умовах радіаційної аварії. Передусім це зумовлено рідкістю аварійних ситуацій на ядерних установках і відсутністю значного практичного досвіду прийняття рішень щодо опромінення персоналу під час аварійних ситуацій.

Водночас в умовах радіаційної аварії необхідно виконувати дії, спрямовані на врятування життя людей, запобігання катастрофічному розвитку ситуації та запобігання отриманню високих доз опромінення значною кількістю людей. В окремих випадках це може бути пов'язано з необхідністю прийняття рішення щодо дій особового складу аварійних бригад у радіаційних умовах, які можуть призвести до переопромінення деяких осіб із цих бригад дозами, вищими за ті, що визначені чинними нормативно-правовими документами для таких випадків для персоналу.

Максимально допустимі рівні опромінення персоналу у випадку аварійного реагування регулюються відповідно до розділу 7 Норм радіаційної безпеки України (НРБУ-97)[5] та розділу 13 Основних санітарних правил забезпечення радіаційної безпеки України (ОСПУ-2005)[6]. Проте положення цих національних документів залишаються неузгодженими з рекомендаціями Міжнародної комісії з радіологічного захисту (МКРЗ) у частині, яка стосується рівнів доз підвищеного опромінення, що планується[7]. Вказана неузгодженість призводить до затримок при прийнятті рішень під час реагування на радіаційні аварії. На це звернули увагу експерти МАГАТЕ при проведенні комплексної перевірки діяльності з регулювання ядерної та радіаційної безпеки в Україні[8].

Таким чином, існує нагальна потреба в обґрунтуванні нормативного затвердження рівнів доз підвищеного опромінення та приведенні національних нормативів у відповідність до рекомендацій МАГАТЕ та МКРЗ.

---

[5]*Норми* радіаційної безпеки України (НРБУ-97) : Державні гігієнічні нормативи. – К. : Відділ поліграфії Українського центру Держсанепіднагляду МОЗ України, 1997. – 121 с.

[6]*Основні* санітарні правила забезпечення радіаційної безпеки України (ОСПУ-2005), затверджені наказом МОЗ України від 02.02.2005 р. № 54 [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/z0552-05

[7]*ICRP* Publication 60. Radiation protection 1990: Recommendations of the International Commission on Radiological Protection. – New York : Pergamon Press, 1991. – 197 p.; *ICRP* Publication 103. The 2007 Recommendations of the International Commission on Radiological Protection // Annals of ICRP. – 2007. – Vol. 37. – Issues 2–4. – P. 1–332.

[8]*Комплексний* огляд регулюючої діяльності (*IRRS*) в Україні : пер. з англ. / Департамент МАГАТЕ з ядерної безпеки та фізичного захисту. – Київ, Україна, 9–20 червня 2008 р. – 199 с.

Рекомендації МКРЗ про дози підвищеного опромінення. У публікації МКРЗ № 26[9] визнається, що під час серйозних аварій може виникнути потреба в таких діях, наслідками яких буде опромінення окремих робітників вище меж, що застосовуються у випадку підвищеного планового опромінення. Однак на той час (1978 р.) МКРЗ не запропонувала конкретну межу такого опромінення, а обмежилась рекомендацією, що «як правило, таке опромінення контролювати повністю неможливо, але разом з тим необхідно зробити все можливе, щоб не перевищити певної крайньої межі для даного ймовірного опромінення». На основі дуже обережних даних про дозові залежності нестохастичних ефектів (Публікації № 41, 1984 р., та № 45, 1985 р.) МКРЗ у 1990 р. таки вийшла на конкретну цифру 0,5 Зв при регламентації доз опромінення аварійних бригад (Публікація № 60). При цьому еквівалентна доза для шкіри не повинна перевищувати приблизно 5,0 Зв.

Необхідно відзначити, що в рекомендаціях МКРЗ (Публікації № 60 та № 103) для випадку врятування життя людей в умовах радіаційної аварії не встановлюються обмеження на отриману рятувальником дозу.

Окрім опромінення, обумовленого безпосередньо аварією, в рекомендаціях МКРЗ передбачається можливість опромінення аварійних бригад під час аварійних ситуацій і відновлювальних робіт[10]. Вважається, що не повинно бути допущено опромінення, яке призводить до отримання ефективних доз, що перевищують 0,5 Зв при контролі аварії та при термінових чи невідкладних роботах, за винятком спасіння життя людей. Не рекомендовано також допускати підвищення еквівалентної дози на шкіру більше 5 Зв (за винятком випадків спасіння людей).

Регулювання протирадіаційного захисту в аварійних ситуаціях (НРБУ-97). Відповідно до НРБУ-97, радіаційна аварія – це будь-яка незапланована подія на будь-якому об'єкті з радіаційною чи радіаційно-ядерною технологією, якщо при виникненні цієї події створюються дві необхідні й достатні умови: втрата контролю над джерелом; реальне (або потенційне) опромінення людей, пов' язане зі втратою контролю над джерелом.

У п. 7.19 НРБУ-97 зазначається: у виняткових випадках, коли роботи виконуються з метою збереження життя людей, мають бути застосовані всі можливі заходи для того, щоб особи з числа аварійного

[9] *ICRP* Publication 26. Recommendations of the International Commission on Radiological Protection // Annals of ICRP. – 1977. – Vol. 1. – Issue 3. – P. 1–53.

[10] *ICRP* Publication 103. The 2007 Recommendations of the International Commission on Radiological Protection // Annals of ICRP. – 2007. – Vol. 37. – Issues 2–4. – P. 1–332.

персоналу, які виконують ці роботи, не могли отримати еквівалентну дозу на будь-який з органів (включаючи рівномірне опромінення всього тіла) більше 500 мЗв. Виконання цієї вимоги забезпечує запобігання детерміністичних ефектів.

Тобто не можна не відзначити, що у національних нормах запроваджено більш жорсткий підхід до опромінення аварійних бригад порівняно з рекомендаціями МКРЗ. Ураховуючи це, доцільно детально проаналізувати дози опромінення осіб, які належали до **різних відомств, але виконували терміново першочергові заходи з мінімізації наслідків аварії.**

Аналіз доз опромінення при ліквідації наслідків аварії на військових і промислових ядерних об'єктах. Під час ліквідації наслідків радіаційних аварій до виконання термінових і першочергових, найбільш радіаційно небезпечних завдань, а також контрзаходів із мінімізації наслідків аварій залучалися як аварійні бригади та пожежники, так і військовослужбовці. Така ситуація мала місце при ліквідації наслідків аварії на Чорнобильській АЕС, а також аварій на військово-технічних ядерних об'єктах колишнього СРСР.

Для оцінки доцільності використання у національних нормативних документах гуманних підходів до визначення доз опромінення членів аварійних бригад було проаналізовано розміри колективних та індивідуальних доз, які отримали пожежники та військовослужбовці при ліквідації аварії на ЧАЕС, а також особовий склад радянських аварійних атомних підводних човнів (табл. 1).

Однозначні висновки можна зробити з досвіду реагування на аварію на Чорнобильській АЕС, якщо проаналізувати отримані дози опромінення і раціональність застосування особового складу.

Працівники зведеного загону Мінвуглепрому СРСР, які виконували роботи з проходження штреку під нижньою плитою реактора і спорудження системи аварійного охолодження розвалу реактора отримали дози від 100 до 500 мЗв. Спеціалістів, здатних виконувати таку роботу, було більш ніж достатньо, а тому були всі можливості отримати дозу в межах 500 Зв.

Значні дози опромінення отримали пожежники, які брали участь у гасінні пожежі на ЧАЕС у перші 3 години аварії. В гасінні пожежі брав участь особовий склад пожежних частин АЕС, м. Прип'яті та м. Чорнобиля – всього 40 осіб. Окремі пожежники, які загинули від радіаційної травми, отримали дози більше 10 Гр. Тобто сумарне дозове навантаження двох пожежників, які отримали смертельне переопромінення, могло бути розподілене на усіх наявних пожежників, і при цьому доза кожного з них не перевищувала би дозової межі.

Таблиця 1

Дози опромінення членів аварійних бригад при ліквідації наслідків аварії на військових і промислових ядерних об'єктах

№ п\п	Контингенти	Колективна доза на все тіло, людино-Гр	Кількість осіб	Середня індивідуальна доза, Гр	Максимально індивідуальна доза, Гр
1	Учасники ліквідації аварії на ЧАЕС				
1.1	Пожежники	93,7	40	2,34	до 10
1.2	Військовослужбовці	523,4	671	0,78	–
2	Учасники ліквідації аварії на військово-технічних ядерних об'єктах				
2.1	Весь особовий склад аварійного атомного підводного човна, 1961 р.	91,25	129	0,71	–
2.2	Особовий склад аварійної партії, 1961 р.	30,88	19	1,63	–
2.3	Весь особовий склад аварійного атомного підводного човна, 1968 р.	87,84	103	0,85	–
2.4	Особовий склад аварійної партії, 1968 р.	47,74	14	3,41	до 6

Усі, хто побував на даху 3-го блока, отримали дози, не менші за 0,7 Гр. Враховуючи, що полум'ям було охоплено дах приміщення машинного залу 3-го блока від 20-ї до 70-ї відмітки, та орієнтуючись на обмеження в 500 мЗв, пожежу гасити було б неможливо. Тобто верхня межа у 500 мЗв лише дозволяла піднятися до вогнища пожежі і, майже нічого не зробивши, повернутися назад. За даними начальника Управління хімічних військ МО СРСР, на 1 травня 1986 р. із 671 військовослужбовців-ліквідаторів були переопроміненні в дозах від 0,2 до 0,5 Зв – 20,4 %, а в дозах більше 0,5 Зв – 11,4 %. Наведені дані та ретельний аналіз обставин опромінення військових ліквідаторів у дозах 500 мЗв і вище (результати опубліковані у збірнику[11]) свідчить про те, що були всі можливості, щоб зазначений дозовий поріг для осіб із цього контингенту ліквідаторів не було перевищено.

Таким чином, можна зробити висновок, що при встановленні лімітів опромінення аварійного персоналу слід орієнтуватися не тільки на

[11] *Скалецький Ю. М.* Випадки переопромінення у значних дозах як критерій оцінки системи протирадіаційного захисту військових ліквідаторів / Ю. М. Скалецький // Гігієнічна наука та практика на рубежі століть : Матеріали XIV з'їзду гігієністів України : у 2 т. / за ред. Ю. І. Кундієва, А. М. Сердюка, Є. Г. Гончарука, О. В. Лапушенко. – Дніпропетровськ : АРТ-ПРЕС, 2004. – Т. 2. – С. 472–475.

медико-біологічні наслідки дії підвищеної радіації, але й ураховувати всі можливості організації аварійно-рятувальних і відновлюваних робіт у межах встановлених лімітів. Після важких радіаційних аварій на корабельних ядерних енергетичних установках у 1961 і 1968 рр. командування Військово-Морського флоту СРСР дійшло висновку, що в аварійній ситуації для збереження життя членів екіпажу та виконання бойових завдань командиру корабля потрібно надати повноваження в окремих випадках дозволяти опромінення деяких членів аварійних партій у будь-яких дозах, виходячи зі всебічного прогнозу розвитку загальної ситуації та радіаційних умов. Цей підхід було відображено в «Инструкции по оценке ближайших вероятных последствий облучения личного состава атомных подводных лодок при авариях на атомных энергетических установках» (1972 р.)

На наш погляд, досвід реалізації термінових і першочергових заходів на ЧАЕС було достатньо ефективно використано спеціалістами США. Так, у керівництві з Медичного забезпечення ліквідації наслідків радіаційних аварій допускається при проведенні пошуку та винесенні уражених або при попередженні подій, наслідком яких може бути переопромінення значної кількості людей, опромінення рятувальників-добровольців або професіоналів у дозах до 1,0 Зв[12]. При цьому додаткова доза на кісті та ступні може досягати 2,0 Зв.

Пожежно-рятувальні підрозділи МНС. Згідно з відомчою інструкцією[13] особовий склад пожежно-рятувальних підрозділів, який залучається до проведення аварійно-рятувальних робіт в умовах радіаційної аварії, прирівнюється на цей період до основного аварійного персоналу (категорії А) і, відповідно, має встановлений максимальний ліміт ефективної дози за рік 50 мЗв (згідно з НРБУ-97) (табл. 2). Цієї граничної межі рекомендується дотримуватись керівникам гасіння пожеж при встановленні доз опромінення особовому складу, що бере участь у гасінні пожежі. Також допускається заплановане підвищення опромінення особового складу. При цьому повинні бути вжиті всі заходи, щоб величина сумарного опромінення не перевищувала 100 мЗв. Особи, які отримали сумарну дозу опромінення більше 100 мЗв, повинні бути негайно виведені з небезпечної зони й направлені на медичне обстеження.

---

[12] *Responding* to a Radiological or Nuclear Terrorism Incident: A Guide for Decision Makers (NCRP Report No.165) / National Council on Radiation Protection and Measurements. – 2010. – 181 p.

[13] *Інструкція* про організацію індивідуального дозиметричного контролю в органах управління та підрозділах МНС, затверджена наказом МНС України від 21.02.2007 р. № 85 [Електронний ресурс]. – Режим доступу: http://www.mns.gov.ua/laws/dcz/49/nakaz.pdf .

Таблиця 2

Порівняння обмежень на дози опромінення, встановлених НРБУ-97 і вказаних у рекомендаціях МКРЗ

Документ / Умови	Рекомендації МКРЗ			НРБУ-97
	Публікація № 26	Публікація № 60	Публікація № 103	
Аварійна ситуація спасіння життя (поінформовані добровольці)	–	Немає обмеження на дози	Немає обмеження на дози, якщо вигода для інших перевищує ризик рятувальників	–
інші термінові операції	1000 мЗв (одноразово)	500 мЗв, 5 Зв (шкіра)	500 мЗв	п. 7.19 еквівалентна доза на будь-який з органів (включаючи рівномірне опромінення всього тіла) менше 500 мЗв
інші операції	менше 100 мЗв (подвоєний річний), але не більше ніж 250 мЗв протягом усього життя	менше 100 мЗв	менше 100 мЗв	п. 7.17 менше 100 мЗв (подвоєне значення максимального ліміту ефективної дози професійного опромінення за один рік)
Повсякденні умови	§103, 104 50 мЗв/рік	20 мЗв у середньому за будь-які послідовні 5 років, але не більше 50 мЗв за окремий рік		

У надзвичайних випадках, коли особовим складом пожежно-рятувальних підрозділів виконуються роботи з рятування життя людей, дози опромінення можуть бути збільшені, але не перевищувати еквівалентної дози в будь-якому органі (включаючи рівномірне опромінення всього організму) у 500 мЗв. Керівник гасіння пожежі є єдиною особою, що має право ухвалювати рішення про підвищення опромінення особового складу пожежно-рятувальних підрозділів. Опромінення осіб з числа особового складу, залученого до ліквідації радіаційної аварії та її наслідків, вище основних дозових меж опромінення допускається лише за їх письмовою згодою, оформленою заздалегідь, у випадках, якщо не можна вжити заходів, які виключають їх перевищення, і може бути виправдане лише рятуванням життя людей та попередженням подальшого небезпечного розвитку аварії та опромінення більшої кількості людей.

Проведений експертами МАГАТЕ у 2008 р. комплексний огляд регулюючої діяльності в Україні виявив недоліки в існуючих нормативах щодо опромінення особового складу аварійних підрозділів, сутність яких викладена далі.

Національні нормативи (розділ 7 НРБУ-97 і розділ 13 ОСПУ-2005) не передбачають надання особливого дозволу на планування опромінення робітників аварійних груп вище лімітів доз (500 мЗв), що в окремих випадках може призвести до затримки виконання термінових захисних заходів, наприклад дій по врятуванню життя людей. Про це свідчать, зокрема, дані, отримані під час аварійних тренувань, що проводилися Держатомрегулюванням, – мінімальний час, необхідний для отримання дозволу на підвищене опромінення робітників аварійних підрозділів від регіонального відділення Міністерства охорони здоров'я або від штабу АЕС (залежно від запланованого рівня опромінення) складав приблизно одну годину[14].

Висновки та пропозиції

1. При регламентуванні дозового навантаження персоналу, який залучається до проведення рятувальних і відновлюваних робіт, слід орієнтуватися не тільки на можливі медико-біологічні ефекти при підвищених дозах, а й на можливість виконання робіт при встановлених дозових обмеженнях.

2. Ліміт дози опромінення аварійних бригад, встановлений НРБУ-97, є необґрунтовано заниженим, що викликає необхідність залучати знач-

[14]*Комплексний* огляд регулюючої діяльності (*IRRS*) в Україні : пер. з англ. / Департамент МАГАТЕ з ядерної безпеки та фізичного захисту. – Київ, Україна, 9–20 червня 2008 р. – 199 с.

ну кількість спеціалістів для виконання аварійних, рятувальних і відновлюваних робіт.

3. Рекомендаціями МКРЗ не встановлюються обмеження на дози опромінення в умовах аварії у випадку спасіння людей або запобігання катастрофічному розвитку ситуації. Натомість прийняті в НРБУ-97 обмеження за аналогічних умов створюють суттєві перешкоди для оперативного прийняття рішень під час реагування.

4. Унаслідок жорстких обмежень на підвищення доз опромінення у випадку аварії особовий склад аварійних бригад забезпечується засобами індивідуального захисту відповідно до занижених, на наш погляд, норм. Такі обмеження створюють перешкоди для запровадження засобів індивідуального захисту для аварійних бригад, які були б розраховані на дози, які може отримати особовий склад бригад у реальних умовах. Підтвердженням цьому є досвід аварійних робіт на ЧАЕС та на об'єктах підводного флоту ВМС СРСР.

ЛЕОНОВ Борис Дмитрович,
старший консультант Штабу
Антитерористичного центру
при Службі безпеки України

ЗАПОБІГАННЯ ТЕРОРИЗМУ – ВАЖЛИВИЙ СКЛАДНИК ПОЛІТИКИ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

У сучасних умовах суттєвою небезпекою для світової спільноти та окремих держав, у тому числі й України, є тероризм. Поширення міжнародного тероризму віднесено до основних реальних і потенційних загроз національній безпеці України (ст. 7 Закону України «Про основи національної безпеки України»). Ця загроза значно посилюється через імовірність використання терористами зброї масового ураження.

Необхідною умовою нейтралізації терористичних загроз на національному ґрунті є формування ефективної державної політики протидії тероризму, що вимагає вироблення чіткої концепції та стратегії, базових принципів, концептуальних засад і визначення шляхів їх практичної реалізації, а також удосконалення правових та організаційних механізмів управління національною безпекою, його відповідного інтелектуально-кадрового і ресурсного забезпечення.

Концепція запобігання тероризму визначається принципами державної політки у сфері національної безпеки, одним із яких є пріоритетність попереджувальних заходів, а необхідність її розробки зумовлена положеннями законів України «Про основи національної безпеки України» (ст. 2), «Про засади внутрішньої і зовнішньої політики» (ч. 3 ст. 2), Стратегії національної безпеки України, затвердженої Указом Президента України від 12.02.2007 р. № 105 (п. 4.1).

Відповідно до п. 4.1 Стратегії національної безпеки України розвиток системи управління національною безпекою України має здійснюватися з урахуванням вдосконалення законодавства з питань національної безпеки, насамперед у спосіб:

• приведення законодавства з питань національної безпеки та оборони у відповідність із Конституцією України, гармонізація його з відповідним європейським законодавством;

• законодавчого уточнення завдань і функцій суб'єктів забезпечення національної безпеки, у т.ч. в умовах особливого періоду та кризових ситуацій, що загрожують національній безпеці України;

• розвитку правових засад управління національною безпекою а саме розробки відповідних законів, концепцій, доктрин, стратегій і програм, зокрема антикорупційного законодавства, національної програми протидії тероризму й екстремізму тощо.

Саме з метою реалізації таких завдань створено Антитерористичний центр при СБ України, який розробляє концептуальні засади та програми боротьби з тероризмом (Положення про Антитерористичний центр та його координаційні групи при регіональних органах Служби безпеки України, затверджене Указом Президента України від 14.04.1999 р. № 379). На жаль, досвід діяльності Антитерористичного центру показує, що на шляху запровадження правових механізмів постає ряд проблем, на вирішення яких мають бути спрямовані зусилля як державних і наукових установ, так і громадськості.

Загалом ця проблематика потребує особливої уваги науковців до опрацювання питань координації діяльності всіх владних структур, до компетенції яких віднесене запобігання терористичним загрозам на національному рівні, створення у суспільстві умов для консолідації громадськості при вирішенні тих проблем сучасного українського суспільства, наявність яких може спричинити прояви тероризму.

Під час науково-практичної конференції «Державна політика у сфері запобігання тероризму: міжнародний досвід і його актуальність для України», яка проводилася 31 жовтня 2008 р. науково-організаційним центром Національної академії СБУ, були запропоновані рекомендації щодо підготовки проекту Концепції запобігання

тероризму в Україні, положення якої повинні бути спрямовані на забезпечення єдиного підходу до розуміння сутності й змісту сучасного тероризму; системне сприйняття цієї загрози як багатопланової небезпеки для різних сфер національної безпеки держави; чітке бачення взаємозв'язку екстремізму, тероризму із соціальними суперечностями та конфліктами.

Аналогічне питання було одним із основних під час «круглого столу» «Державна політика протидії тероризму: пріоритети та шляхи реалізації», який відбувся 24 лютого 2011 р. у приміщенні Національного інституту стратегічних досліджень. За результатами цього заходу було визнано, що для забезпечення єдиного підходу на всіх рівнях держави та суспільства до розуміння сутності тероризму як загрози національній безпеці України необхідно розпочати розроблення Концепції протидії тероризму, зміст якої має визначати пріоритети держави у підходах щодо подолання тероризму з урахуванням як кримінологічної специфіки цього злочину, так і комплексної соціально-політичної природи даного явища.

Але, незважаючи на значний суспільний інтерес, чіткої концепції протидії тероризму, яка розкривала б з точки зору кримінологічної науки суттєві характеристики цієї небезпеки і, тим самим, указала на шляхи її запобігання та створення можливостей такої протидії, поки що не розроблено.

Слід зауважити, що концепція запобігання тероризму має спиратися на Стратегію боротьби із цим явищем, яка повинна бути всеосяжною, не прив'язаною до якої б то не було специфічної загрози, розрахованою на тривалий час і з визначенням необхідних напрямів реформування антитерористичної системи за певними етапами відповідно до їх важливості.

При формуванні та реалізації державної політики у сфері запобігання тероризму потребує врахування позитивний досвід країн-членів ЄС, НАТО і СНД у цій сфері. Зокрема, заслуговує на увагу затверджена указом президента Російської Федерації від 5.10.2009 р. Концепція протидії тероризму, серед положень якої виділяються основні тенденції сучасного тероризму (розділ I), загальнодержавна система протидії тероризму (розділ II), правове, інформаційно-аналітичне, наукове, фінансове й кадрове забезпечення протидії тероризму (розділ III), міжнародне співробітництво у сфері протидії тероризму (розділ IV). На думку фахівців, реалізація державної політики у сфері запобігання тероризму передбачає застосування комплексного підходу, а тому концепція має спиратися не тільки на превентивну, регулятивну та репресивну форми контролю держави, а й ураховувати, як основу,

організацію, координацію та постійну оптимізацію вже існуючих механізмів боротьби з тероризмом залежно від проявів останнього. При цьому, окрім організаційних та ресурсних заходів, слід передбачити структуровану протидію факторам, що сприяють поширенню цього негативного явища.

З метою заповнення цієї прогалини підпунктом «а» підпункту 4 п. 1 рішення Ради національної безпеки і оборони України від 25 травня 2012 року «Про заходи щодо посилення боротьби з тероризмом в Україні» (уведене в дію Указом Президента України від 8.06.2012 р. № 388) передбачено розробку Концепції боротьби з тероризмом.

СБУ як головним органом у загальнодержавній системі боротьби з тероризмом розроблено та внесено на розгляд Кабінету Міністрів України проект цієї концепції[15]. Під час підготовки проекту було враховано думку науковців та громадських діячів, що опікуються цією проблемою.

Вбачається, що реалізація концепції сприятиме забезпеченню захисту конституційних прав і свобод людини і громадянина, конституційного ладу; зменшенню терористичних проявів; оптимізації координації діяльності суб'єктів боротьби з тероризмом, ефективності їх діяльності; підвищенню рівня захищеності громадян від терористичних посягань; зміцненню міжнародної взаємодії у сфері боротьби з тероризмом.

БІРЮКОВ Дмитро Сергійович,
старший консультант відділу екологічної та техногенної безпеки НІСД

ПРО ДОЦІЛЬНІСТЬ ТА ОСОБЛИВОСТІ ВИЗНАЧЕННЯ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УКРАЇНІ

Розвиток цивілізації, що супроводжується економічною глобалізацією, урбанізацією та широким застосуванням інформаційних технологій, спричинив феноменальну залежність як окремої людини, так і суспільства від послуг, які надають енергетичні, телекомунікаційні, транспортні та інші інфраструктурні мережі. Доступність цих послуг нині сприймається як один із показників якості життя і в мегаполісі, і в сільській місцевості. Тільки ті країни, які мають розвинену інфра-

[15]У квітні 2013 року Концепція була схвалена Указом Президента України від 25.04.2013 р. № 230/2013.

структуру, здатні стати сучасними економічними центрами, розвивати та зосереджувати на своїй території фінансові, промислові та інтелектуальні потужності.

Водночас помітною є тенденція до посилення негативних процесів і явищ природного, техногенного та соціально-політичного характеру (у світі збільшуються кількість і масштаб наслідків природних катастроф, тліють та розгораються нові військові конфлікти, постійно здійснюються терористичні акти, надшвидкими темпами зростає кількість кібератак), що зумовлюють прямі та каскадні загрози для стабільного функціонування згаданих інфраструктур, а отже забезпечення їх «абсолютного захисту» стає непосильним завданням навіть для економічно розвинутих держав.

Саме необхідність зосередження ресурсів на захисті найважливіших інфраструктурних об'єктів обумовила розвиток і впровадження концепції критичної інфраструктури (КІ) як складника систем забезпечення національної безпеки низки провідних країн світу. У США до КІ відносять системи, мережі та окремі об'єкти, порушення роботи або руйнування яких може спричинити величезні або навіть незворотні негативні наслідки для економіки, добробуту та здоров'я населення, стабільного перебігу політичних процесів[16]. Подібна дефініція міститься в Директиві Європейської Комісії № 786 2006 р.[17], згідно з якою до загальноєвропейської КІ відносять ті об'єкти національних КІ країн-членів ЄС, вплив яких у разі відмови, інциденту або зловмисного втручання поширюватиметься як на країну, де такий об'єкт розташований, так і на хоча б одну іншу країну-члена ЄС. Концепція захисту КІ реалізована також у таких розвинутих країнах, як Канада, Австралія, Велика Британія.

Зважаючи на процеси поступової модернізації безпекового сектору в Україні та наше прагнення ствердитися як повноправний партнер на європейському та трансатлантичному безпековому просторі, питання впровадження концепції захисту КІ стає все актуальнішим.

Було б невірно стверджувати, що в Україні мало приділяється уваги питанням захисту життєво важливих систем, мереж та об'єктів. Навпаки, в державі паралельно функціонують Єдина система запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків, Єдина державна система запобігання і реагування на над-

[16] *Uniting* and strengthening America by providing appropriate tools required to intercept and obstruct terrorism (PATRIOT ACT) [Електронний ресурс]. – Режим доступу: http://frwebgate.access.gpo.gov

[17] *European* programme for critical infrastructure protection (COM/2006/786 final) [Електронний ресурс]. – Режим доступу: http://eur-lex.europa.eu.

звичайні ситуації техногенного та природного характеру[18], що трансформована у Єдину державну систему цивільного захисту, сутність та особливості якої законодавчо визначені Кодексом цивільного захисту України[19].

В Україні захист об'єктів, які згідно зі світовою практикою належать до категорії «критична інфраструктура», регламентується численними нормативно-правовими актами, що мають переважно внутрішньовідомчий характер. Така ситуація склалася природним чином – кожне окреме відомство розглядало насамперед певний спектр загроз для підпорядкованих об'єктів і володіло певним набором інструментів та ресурсів для забезпечення безпеки цих об'єктів. У результаті в чинному законодавстві визначено низку категорій об'єктів, для яких регламентуються особливі умови забезпечення захисту: підприємства, які мають стратегічне значення для економіки та безпеки держави[20]; об'єкти, які включені до Державного реєстру потенційно небезпечних об'єктів[21]; об'єкти підвищеної небезпеки[22] (у т.ч. Перелік особливо небезпечних підприємств, припинення діяльності яких потребує проведення спеціальних заходів щодо запобігання заподіянню шкоди життю та здоров'ю громадян, майну, спорудам, навколишньому природному середовищу[23]); важливі державні об'єкти, перелік яких визначено спеціальним нормативно-правовим актом; об'єкти, що підлягають обов'язковій охороні підрозділами

---

[18]*Положення* про єдину державну систему запобігання і реагування на надзвичайні ситуації техногенного та природного характеру, затверджене постановою Кабінету Міністрів України від 03.08.1998 р. № 1198 [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/1198-98-п.

[19]*Кодекс* цивільного захисту України [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/5403-17/page.

[20]*Про затвердження* переліку підприємств, які мають стратегічне значення для економіки та безпеки держави : постанова Кабінету Міністрів України від 23.12.2004 р. № 1734 [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/1734-2004-п.

[21]*Про затвердження* Положення про Державний реєстр потенційно небезпечних об'єктів : постанова Кабінету Міністрів України від 29.08.2002 р. № 1288 [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/1288-2002-п.

[22]*Про об'єкти* підвищеної небезпеки : закон України від 18.01.2001 р. № 2245-III [Електронний ресурс].– Режим доступу: http://zakon4.rada.gov.ua/laws/show/2245-14.

[23]Нині відповідний Перелік має назву: «Перелік особливо небезпечних суб'єктів підприємницької діяльності – боржників, припинення діяльності яких потребує здійснення спеціальних заходів із запобігання заподіянню можливої шкоди життю та здоров'ю громадян, майну, спорудам, навколишньому природному середовищу» (затверджений постановою Кабінету Міністрів України від 15 травня 2013 р. № 339).

Державної служби охорони за договорами[24]; об'єкти, які підлягають охороні та обороні в умовах надзвичайних ситуацій і в особливий період; особливо важливі об'єкти електроенергетики[25]; особливо важливі об'єкти нафтогазової галузі[26]; Національна система конфіденційного зв'язку[27]; платіжні системи[28]; Система екстреної допомоги населенню за єдиним номером 112[29]; нерухомі об'єкти культурної спадщини[30].

Проте, попри значну кількість нормативно визначених категорій життєво важливих об'єктів і, відповідно, їх переліків, в Україні не здійснюється комплексна (координована) оцінка ризиків втрати чи ушкодження таких об'єктів. У чинному законодавстві досі не визначено термін «критична інфраструктура», хоча в оновленій Стратегії національної безпеки[31] серед шляхів зміцнення енергетичної безпеки названий «дієвий захист *критичної інфраструктури* паливно-енергетичного комплексу від еколого-техногенних впливів та зловмисних дій» (п. 4.3.4.), а одним із шляхів забезпечення інформаційної безпеки визначається «забезпечення безпеки інформаційно-телекомунікаційних систем, що функціонують в інтересах управлін-

---

[24]*Про заходи* щодо вдосконалення охорони об'єктів державної та інших форм власності : постанова Кабінету Міністрів України від 10.08.1993 р. № 615 [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/615-93-п

[25]*Про затвердження* переліку особливо важливих об'єктів електроенергетики, які підлягають охороні відомчою воєнізованою охороною у взаємодії із спеціалізованими підрозділами інших центральних органів виконавчої влади : постанова Кабінету Міністрів України від 28.07.2003 № 1170 [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/1170-2003-п

[26]*Про затвердження* переліку особливо важливих об'єктів нафтогазової галузі : розпорядження Кабінету Міністрів України від 27.05.2009 р. № 578-р [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/578-2009-р

[27]*Про Національну* систему конфіденційного зв'язку : закон України від 10.01.2002 р. № 2919-III [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/2919-14

[28]*Про платіжні* системи та переказ коштів в Україні : закон України від 05.04.2001 р. №2346-III [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/2346-14.

[29]*Про систему* екстреної допомоги населенню за єдиним телефонним номером 112 : закон України від 13.03.2012 р. №4499-VI [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/laws/show/4499-17

[30]*Про охорону* культурної спадщини : закон України від 08.06.2000 р. № 1805-III [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/1805-14

[31]*Про рішення* Ради національної безпеки і оборони України від 8 червня 2012 року «Про нову редакцію Стратегії національної безпеки України» : указ Президента України від 08.06.2012 р. № 389/2012 [Електронний ресурс]. – Режим доступу: http://zakon0.rada.gov.ua/laws/show/n0002525-12

ня державою, забезпечують потреби оборони та безпеки держави, кредитно-банківської та інших сфер економіки, систем управління *об'єктами критичної інфраструктури*» (п. 4.3.8.)

Очевидно, що введення терміна «критична інфраструктура» в законодавство України само по собі не може бути остаточною ціллю. Концепція критичної інфраструктури має стати підґрунтям дієвого механізму координації зусиль органів влади, спрямованих на недопущення втрати чи завдання невиправної шкоди найважливішим для життєдіяльності держави об'єктам, з урахуванням дії негативних факторів будь-якого походження – техногенного, природного, соціально-політичного або будь-якої комбінації з їх числа.

До того ж, наявність дефініції «критична інфраструктура» в законодавстві не означає автоматичного формування переліку таких об'єктів. Про це свідчить досвід визначення об'єктів КІ у США, де навіть за наявності значних за розмірами матеріальних та організаційних ресурсів при виконанні такого завдання відповідальне відомство зіткнулося з проблемою формування методології, не кажучи вже про необхідність обробки величезної кількості даних про об'єкти (з понад 33 тис. об'єктів-кандидатів до КІ було віднесено 3 тис. об'єктів, що належать до 18 секторів життєдіяльності)[32].

У ЄС спроба визначити КІ була здійснена у 2005 р. під час підготовки «зеленої книги», згідно з положеннями якої до КІ було включено 11 секторів[33]. Згодом Директивою Європейської Комісії № 114 2008 р. лише два сектори були визнані пріоритетними – це енергетика (електромережі та об'єкти з генерування та передачі електроенергії; нафтовидобувна та нафтопереробна промисловість, нафтопроводи та сховища; газовидобувна промисловість, газопроводи, термінали скрапленого газу) і транспорт (автодорожній транспорт; залізничний транспорт; авіаційний транспорт; річковий флот; океанічний і морський флот; порти)[34].

При визначенні елементів КІ будується ієрархія критеріїв, яка охоплює такі основні групи: економічна безпека (значна частка продукції на ринку, велика кількість зайнятих співробітників, великий

---

[32] *Critical* infrastructure and key assets: definition and identification. – Congressional research service, RL32631, October, 2004. – 19 p.

[33] *Green paper* on a European programme for critical infrastructure protection (COM/2005/576 final) [Електронний ресурс]. – Режим доступу: http://eur-lex.europa.eu

[34] *On the identification* and designation of European critical infrastructures and the assessment of the need to improve their protection (Council Directive 2008/114/EC) [Електронний ресурс]. – Режим доступу: http://eur-lex.europa.eu

платник податків); безпека життєдіяльності та здоров'я населення (забезпечення роботи аварійно-рятувальних служб, екстреної допомоги населенню; недопущення техногенних аварій регіонального або національного масштабів); державна безпека та оборона (недопущення порушення керованості державою, зниження боєздатності збройних сил, розголошення таємної інформації); національна самоповага та імідж держави (збереження культурних цінностей, авторитету держави).

Наприклад, згідно з уже згаданою Директивою Європейської Комісії[35] при визначенні потенційних елементів критичної інфраструктури враховують такі фактори та характеристики:

• масштаб (географічне охоплення території, для якої втрата елементу критичної інфраструктури завдає значної шкоди);

• важкість можливих наслідків за такими показниками:

– вплив на населення (число постраждалих, загиблих, осіб, які отримали значні травми, а також чисельність евакуйованого населення);

– економічна шкода (вплив на ВВП, розмір економічних втрат, як прямих, так і непрямих);

– екологічна шкода (вплив на населення та навколишнє природне середовище);

– взаємозв'язок з іншими елементами критичної інфраструктури;

– політичний ефект (втрата впевненості в дієздатності влади);

– тривалість впливу (як саме і коли проявлятимуться наслідки, пов'язані зі втратою чи відмовою об'єктів критичної інфраструктури).

Схожий набір критеріїв використовується в РФ при визначенні критично важливих об'єктів паливно-енергетичного комплексу[36]: критична важливість об'єкта для інфраструктури та життєзабезпечення паливно-енергетичного комплексу; масштаби можливих соціально-економічних наслідків, що виникнуть внаслідок аварії на об'єкті; наявність критичних елементів, потенційно небезпечних ділянок та уразливих місць на об'єкті.

---

[35] *Council* Directive 2008/114/EC «On the identification and designation of European critical infrastructures and the assessment of the need to improve their protection» [Електронний ресурс]. – Режим доступу: http://eur-lex.europa.eu

[36] *О безопасности* объектов топливно-энергетического комплекса ИПС «Закон» : федеральный закон Российской Федерации от 21.07.2011 г. № 256-ФЗ [Електронний ресурс]. – Режим доступу: http://ntc.duma.gov.ru/

В Ізраїлі враховуються такі три ознаки при ідентифікації об'єктів КІ[37]: символічна (ідеологічна, історична або культурна) значимість об'єктів; залежність основних процесів життєзабезпечення суспільства від інфраструктури; наявність складних взаємозв'язків та залежностей між об'єктами інфраструктури. Згідно з таким підходом об'єкти культурної спадщини (музеї, архіви, культові споруди та інші пам'ятки) віднесені до числа об'єктів, які повинні бути захищені в першу чергу. За другою ознакою до критичної інфраструктури відносять ЛЕП, системи водопостачання, каналізаційні мережі, загальні телекомунікаційні мережі, з якими пов'язані процеси управління інфраструктурами. Що стосується третьої ознаки, то спеціалісти вказують на каскадні ефекти у відмовах інфраструктурних елементів.

Загрози для об'єктів КІ оцінюються із застосуванням різноманітних методик і прикладного програмного забезпечення, основою яких є загальна методологія оцінки ризиків, про що свідчить звіт Інституту захисту та безпеки громадян (входить до складу Центру спільних досліджень Європейської Комісії, розташованого у м. Іспра, Італія)[38]. Тобто можна зробити висновок, що, по-перше, загальний підхід до оцінки ризиків об'єктам КІ включає: ідентифікацію та класифікацію загроз, ідентифікацію вразливостей та оцінку наслідків; по-друге, головною особливістю оцінки ризиків для КІ є врахування численних взаємозв'язків та залежностей. Згідно з підходом, прийнятим ЄК, окремі об'єкти КІ є взаємопов'язаними як фізично (наприклад комп'ютерними мережами, забезпеченням електроенергією, транспортними перевезеннями), так і різноманітними регламентуючими нормами[39]. Дослідження, проведені із застосуванням методів математичного моделювання та спеціального програмного забезпечення, дають змогу оцінити ці взаємозв'язки[40].

Для інфраструктурних систем, розрахованих на тривалий період функціонування, також важливо враховувати вплив глобальних при-

---

[37]*Гриняев С.* О взгляде на проблему безопасности критической инфраструктуры в государстве Израиль / С. Гриняев ; Центр стратегических оценок и прогнозов [Електронний ресурс]. – Режим доступу: http://www.csef.ru/

[38]*Risk* assessment methodologies for critical infrastructure protection. Part I: a state of the art / G. Giannopoulos, R. Filippini, M. Schimmer. – Luxembourg : Joint Research Centre of Institute for the Protection and Security of the Citizen, 2012. – 70 p.

[39]*Lewis T. G.* Critical infrastructure protection in homeland security: defending a networked nation / T. G. Lewis. – John Wiley & Sons, Inc., 2006. – 474 p.

[40]*Quantification* of dependencies between electrical and information infrastructures / M. Beccutia, S. Chiaradonnac, F. Di Giandomenicoc, S. Donatellia [etc.] // Int. J. Critical Infrastructure Protection. – 2012. – Vol. 5. – P. 14–27.; *Critical* Infrastructure Interdependency Modeling: A Survey of U.S. and International Research / P. Pederson, D. Dudenhoeffer, S. Hartley, M. Permann. – U.S. Department of Energy : Idaho National Laboratory, 2006. – 116 p.

родних факторів, наприклад кліматичні зміни. Навіть у розвинутих країнах такі дослідження проводяться тільки для найважливіших секторів економіки (зокрема енергетики[41]). Водночас результати подібних досліджень дають можливість ефективніше розподіляти ресурси, виділені на забезпечення стійкого функціонування інфраструктур. Наприклад, проведені у м. Мельбурн (Австралія) дослідження показали, що вплив аномально високих температур був порівняно незначним для функціонування мережі водопостачання, телекомунікації та аеропортів, помірним для залізничного та автомобільного транспорту, тоді як найвразливішою до таких температурних змін виявилася електроенергетика[42].

Своєю чергою елементи КІ також можуть бути впорядковані за значимістю. Наприклад, у Швейцарії найвище значення надано двом підсекторам енергетики (постачання газу та електроенергії), банківським установам, інформаційним технологіям і телекомунікаціям, залізничному транспорту та автомобільним шляхам, а також мережі постачання питної води[43].

Визначення категорій об'єктів КІ дає змогу встановити диференційовані вимоги до забезпечення безпеки цих об'єктів з урахуванням, зокрема, ступеня потенційної небезпеки здійснення акту незаконного втручання або теракту і його можливих наслідків.

Висновки та пропозиції

1. Нині у системах забезпечення національної безпеки провідних країн світу важливу роль відіграє концепція захисту критичної інфраструктури.

Упровадження концепції захисту критичної інфраструктури стане важливим кроком на шляху модернізації системи національної безпеки України, дасть змогу наблизити вітчизняні підходи до загальновизнаних на європейському та трансатлантичному безпековому просторі.

2. Не можна стверджувати, що в Україні не приділяється увага захисту важливих об'єктів, систем і ресурсів, які зазвичай відносять до

---

[41] *Rubbelke D.* Impacts of climate change on European critical infrastructures: The case of the power sector / D. Rubbelke, S. Vogele // Environmental science and policy. – 2011. – Vol. 14, Issue 1. – P. 53–63.

[42] *McEvoy D.* The impact of the 2009 heat wave on Melbourne's critical infrastructure / D. McEvoy, I. Ahmed , J. Mullett // Local Environment: The Int. J. of Justice and Sustainability. – 2012. – 17 (8). – P. 783–796.

[43] *The Federal* Council's Basic Strategy for Critical Infrastructure Protection Federal Administration [Електронний ресурс]. – Режим доступу: http://www.bevoelkerungsschutz.admin.ch

критичної інфраструктури. Навпаки, діє низка законодавчих актів, що визначають особливості забезпечення захисту таких об'єктів.

Проте в державі досі відсутній загальний механізм управління захистом та безпекою цих об'єктів, спостерігаються непоодинокі випадки дублювання функцій та ресурсів, відсутність спільних підходів та узгодженості дій стосовно проблем національного масштабу, а загрози таким об'єктам розглядаються із суто «відомчих» підходів.

3. Процес визначення елементів критичної інфраструктури включає оцінювання ризиків для об'єктів, спричинених факторами різного походження (техногенного, природного та соціально-політичного характеру), а також аналіз взаємозалежностей між цими елементами. Вказане потребує проведення ґрунтовних наукових досліджень, а також розробки та впровадження відповідних інформаційних технологій.

Зважаючи на зроблені висновки, вважаємо за доцільне сформулювати такі **пропозиції**.

1. Ввести термін «об'єкти критичної інфраструктури» в законодавство України, що відповідає загальновизнаним підходам. Наприклад, цей термін можна подати в такій редакції: «системи та об'єкти, фізичні чи віртуальні, настільки важливі для держави, що їх недієздатність або знищення загрожують національній безпеці, економіці, здоров'ю або безпеці життєдіяльності населення».

2. Кабінет Міністрів України повинен визначити перелік об'єктів критичної інфраструктури з урахуванням чинних нормативно-правових актів, якими встановлені певні категорії об'єктів, що потребують особливих умов захисту від загроз техногенного, природного та соціально-політичного характеру. На попередньому етапі перелік об'єктів критичної інфраструктури може бути сформований на основі чинних переліків.

3. Залучити Національну академію наук України до розробки методології визначення переліку об'єктів критичної інфраструктури, проведення досліджень з аналізу ризиків для таких об'єктів і формування науково обґрунтованих підходів до розподілення ресурсів, що виділяються для захисту критичної інфраструктури.

ЧУМАК Дмитро Вікторович,
спеціаліст з міжнародних відносин
Українського ядерного товариства

ПРО ДЕЯКІ ПІДСУМКИ СЕУЛЬСЬКОГО САМІТУ З (ФІЗИЧНОЇ) ЯДЕРНОЇ БЕЗПЕКИ ТА ЗАПРОВАДЖЕННЯ ІНТЕГРОВАНОГО ПІДХОДУ ДО БЕЗПЕКИ ВИКОРИСТАННЯ ЯДЕРНОЇ ЕНЕРГІЇ

Ядерна енергетика нині є високотехнологічною галуззю, яка відіграє важливу роль у формуванні енергобалансу світової економіки. Разом з тим ядерні технології, що використовуються для виробництва електроенергії, є потенційно небезпечними.

Справді, минулорічна ядерна криза на АЕС Фукусіма-1 засвідчила, що використання ядерної енергії у разі недооцінки усіх аспектів забезпечення безпеки функціонування ядерних об'єктів може призводити до катастрофічних наслідків. Події на АЕС Фукусіма-1 ще раз засвідчили, що мирне використання енергії ядра потребує нових підходів, спрямованих на підвищення рівня передусім (експлуатаційної) ядерної безпеки (*nuclear safety*) та (фізичної) ядерної безпеки (*nuclear security*).

Глобальні наслідки важких ядерних аварій, якою би не була їх природа, вимагають тісної співпраці на міжнародній арені з метою розробки *адекватних заходів* щодо зменшення ризиків аварійних ситуацій на ядерних об'єктах і, відповідно, вжиття *максимально ефективних заходів* для ліквідації наслідків таких аварій, якщо їх не вдалося уникнути. При цьому слід ураховувати, що аварійні ситуації можуть бути використані терористами у своїх цілях, або виникнути у результаті вчиненого терористичного акту. Тобто при забезпеченні безпечного функціонування ядерного об'єкта належну увагу слід приділяти *створенню дієвих систем* фізичного захисту ядерних та інших радіаційних матеріалів.

Питання атомної енергетики після підписання Договору про нерозповсюдження ядерної зброї, у якому було визнане, «...невід'ємне право всіх Учасників Договору розвивати дослідження, виробництво та використання ядерної енергії у мирних цілях», посіло провідне місце у системі міжнародних відносин, у результаті чого вирішення ряду проблем, пов'язаних із використанням даного виду енергії, відбувається у дипломатичній площині.

Оскільки «дипломатія – це діяльність щодо ведення переговорів, підписання міжнародних угод, вивчення основних тенденцій та перспектив розвитку як регіональних, так і глобальних міжнародних відносин»[44], то вона може зробити вагомий внесок у підвищення безпеки мирного використання ядерної енергії. Дипломатичні зусилля є невід'ємною частиною застосування міжнародних політичних інструментів, до яких відносяться і саміти на найвищому рівні.

Саме використання механізму самітів на найвищому рівні у політиці президента США Барака Обами щодо протидії загрозам ядерного тероризму стало новим кроком на шляху розвитку політичних інструментів, що свідчить про важливість даної проблематики у зміцненні глобальної системи безпеки.

Програма діяльності адміністрації Барака Обами включала підтримку ідеї світу без ядерної зброї та протидію загрозам ядерного тероризму. У 2009 р. у Празі президент США дав чітко зрозуміти, що для зовнішньої політики США ці цілі є пріоритетними[45]. Першим важливим кроком у сфері протидії ядерному тероризму став Вашингтонський саміт з (фізичної) ядерної безпеки, який відбувся у квітні 2010 р. Головними його здобутками стали практичні заходи як на національному, так і на міжнародному рівнях, спрямовані на досягнення проголошеної Бараком Обамою цілі – убезпечити упродовж наступних 4-х років уразливі ядерні матеріали у глобальному масштабі[46]. У Вашингтоні також було прийнято рішення, що наступний саміт відбудеться у Сеулі у 2012 р., і на ньому буде розглянуто прогрес, досягнутий країнами-учасницями та міжнародними організаціями за два роки.

Про глобальний масштаб Саміту у Сеулі свідчить участь у ньому 53 держав і 4 міжнародних організацій: ООН, МАГАТЕ, ЄС та ІНТЕРПОЛу. Загальна кількість безпосередніх учасників становила 58 чоловік (Європейський Союз представляли президент Ради Європи і президент Європейської Комісії).

Аналізуючи результати даного саміту, передусім слід зауважити, що основні напрями відповідної діяльності були визначені Вашингтонським самітом. Зокрема, результатом виконання взятих на себе у зв'язку із самітом у Вашингтоні зобов'язань стало вивезення близько 480 кг високозбагаченого урану (ВЗУ) з 8 держав, у т.ч. і з України.

---

[44][Електронний ресурс]. – Режим доступу: http://kimo.univ.kiev.ua/DKS/05.htm

[45][Електронний ресурс]. – Режим доступу: http://www.america.gov/st/texttrans-english/2009/April/20090406115740eaifas0.9701763.html

[46][Електронний ресурс]. – Режим доступу: http://www.niss.gov.ua/articles/742/

Даної кількості ядерного матеріалу було б достатньо для виготовлення близько 19 одиниць ядерної зброї.

Іншим основним напрямом діяльності у період між самітами стало переведення (конверсія) реакторів дослідницького призначення з палива на основі ВЗУ на паливо на основі низькозбагаченого урану (НЗУ) в таких країнах, як Чехія, Мексика, В'єтнам, а також рішення низки країн про свої плани щодо подібного переходу в майбутньому. Одним із завдань, сформульованих у Сеульському комюніке щодо цього напряму, стало визначення 2013 р. кінцевим терміном зведення до мінімуму кількості ВЗУ у цивільному секторі.

Важливим є той факт, що Сеульський саміт з (фізичної) ядерної безпеки відбувся фактично у річницю Фукусімської трагедії, що мало відповідний вплив на його порядок денний та ухвалені документи.

У контексті трагедії в Японії обговорювалося дуже важливе питання щодо взаємозв'язку між (експлуатаційною) ядерною безпекою та (фізичною) ядерною безпекою. «Відзначаючи факт аварії на АЕС Фукусіма-1 у березні 2011 р. та взаємозв'язок між (фізичною) ядерною безпекою та (експлуатаційною) ядерною безпекою, ми вважаємо, що необхідні постійні зусилля, з тим щоб проблеми розглядалися на узгодженій основі, що допоможе забезпечити надійне та безпечне мирне використання ядерної енергії»[47].

Кожний із напрямів діяльності щодо забезпечення безпеки робить свій внесок у безпечне використання ядерної енергії упродовж усього ядерного паливного циклу. Разом вони забезпечують належний рівень безпеки ядерних об'єктів, населення та навколишнього середовища.

(Фізична) ядерна безпека. За визначенням МАГАТЕ, *nuclear security* («фізична ядерна безпека») означає «запобігання та виявлення викрадення, саботажу (диверсії), несанкціонованого доступу, незаконної передачі або інших зловмисних дій по відношенню до ядерних матеріалів, інших радіоактивних речовин або пов'язаних з ними установок і реагування на такі дії»[48].

Виходячи з даного визначення, забезпечення фізичної ядерної безпеки включає такі напрями діяльності:

---

[47][Електронний ресурс]. – Режим доступу: http://www.cfr.org/proliferation/seoul-communiqu-2012-nuclear-security-summit/p27735

[48]*Глоссарий* МАГАТЭ по вопросам безопасности. Терминология, используемая в области ядерной безопасности и радиационной защиты [МАГАТЭ]. – изд. 2007 года. – Вена, 2007. – С. 263–264 [Електронний ресурс]. – Режим доступу: http://www-pub.iaea.org/MTCD/publications/PDF/IAEASafetyGlossary2007/Glossary/SafetyGlossary_2007r.pdf

• запобігання – заходи з обліку, контролю та захисту ядерних матеріалів та установок від зловмисних дій;

• виявлення – заходи з розкриття зловмисних дій стосовно ядерних та інших радіоактивних матеріалів, а також пов'язаних з ними установок та іншої інфраструктури;

• реагування – заходи з ефективного реагування у випадку зловмисних дій, розслідування пов'язаних зі зловмисними діями інцидентів, включаючи аналіз та встановлення походження вилучених матеріалів і речовин.

Таким чином, до безпосередніх заходів, спрямованих на забезпечення фізичної ядерної безпеки (ФЯБ), відносяться фізичний захист, який має забезпечувати захищеність ядерних матеріалів та установок з метою створення умов, спрямованих на мінімізацію можливості вчинення несанкціонованих дій, а також облік і контроль ядерних матеріалів, які об'єднують заходи, спрямовані на недопущення переключення ядерного матеріалу на військові цілі та на недопущення потрапляння матеріалу в незаконний обіг.

Від ефективності заходів щодо ФЯБ на національному рівні залежить ступінь ризиків для держави, пов'язаних із незаконним обігом ядерних та інших радіоактивних матеріалів, а також із терористичними актами. Водночас режим ФЯБ на національному рівні є складником забезпечення глобальної безпеки. Відповідають за стан національних систем ФЯБ уряди держав-членів, але МАГАТЕ та країни-донори надають суттєву допомогу окремим країнам для удосконалення їх систем ФЯБ.

У контексті вразливості системи ФЯБ щодо наявних і потенційних загроз важливу роль відіграє захист інформації та інформаційна безпека у зв'язку з широким використанням інформаційних технологій у ядерній галузі. Витікання інформації, наприклад щодо обліку ядерних матеріалів, може призвести до того, що вона може бути використана зловмисниками з метою викрадення таких матеріалів. Зрозуміло також, що, наприклад, чутлива інформація про характеристики систем фізичного захисту ядерного об'єкта може значно полегшити потенційним терористам планування та вчинення акту ядерного тероризму.

(Експлуатаційна) ядерна безпека. У процесі використання ядерної енергії питання (експлуатаційної) ядерної безпеки мають відігравати визначальну роль. Ядерні установки та джерела іонізуючого випромінювання створюють особливі види ризику, пов'язані з дією іонізуючого випромінювання. При цьому основним принципом регулювання безпеки є пріоритет захисту людини та навколишнього се-

редовища від радіаційного впливу та інших видів небезпеки, викликаних функціонуванням АЕС та інших ядерних установок на всіх етапах життєвого циклу.

Слід відзначити, що (експлуатаційна) ядерна безпека стосується як ризиків радіаційного опромінення при нормальних умовах, так і тих, що виникають внаслідок інцидентів або ж внаслідок втрати контролю (над роботою ядерного реактора, ланцюговою реакцією, радіоактивним джерелом), або будь-яким іншим джерелом випромінювання.

Крім того, проблеми забезпечення (експлуатаційної) ядерної безпеки пов'язані з відпрацьованим ядерним паливом і радіоактивними відходами. Дані матеріали також можуть стати об'єктом несанкціонованих дій, що підвищує загрозу ядерного тероризму.

Інтегрований підхід до безпеки використання ядерної енергії. На об'єктах ядерної енергетики існує ряд систем та обладнання, які можуть відігравати важливу роль як для (експлуатаційної) ядерної безпеки, так і для (фізичної) ядерної безпеки. Прикладом цього може слугувати контаймент, тобто герметична залізобетонна попередньо напружена оболонка енергоблоку реакторного відділення, що вкриває реактор та обладнання, примикає до нього і здатна локалізувати радіоактивні речовини при виникненні максимальної проектної аварії. Таким чином, для (експлуатаційної) ядерної безпеки контаймент має значення запобіжного елемента для захисту від значного викиду радіоактивності у навколишнє середовище у разі аварії. Водночас для реактора він слугує захисним бар'єром від терористичних актів та інших несанкціонованих дій, тобто виконує функції елемента ФЯБ.

Серед основних принципів безпеки АЕС особливе значення має принцип глибокоешелонованого захисту (англ. – *defense in depth*). Він використовується для побудови систем як (експлуатаційної) ядерної безпеки, так і систем ФЯБ.

Реалізація цього принципу для забезпечення ФЯБ передбачає створення серії захисних шарів навколо потенційних цілей терористів або інших зловмисників. Тоді як для (експлуатаційної) ядерної безпеки (ЕЯБ) відповідно до цього принципу передбачено створення ряду послідовних рівнів захисту від імовірних відмов технічних засобів і помилок персоналу. В деяких випадках вимоги до систем ФЯБ і ЕЯБ можуть суперечити один одному, тому для оптимізації згаданих систем спеціалісти ЕЯБ і ФЯБ повинні взаємодіяти і спільно визначати компромісні варіанти побудови систем безпеки на основі урахування як проектних аварій, так і проектної загрози, визначеної для даної установки.

Наслідки нехтування вимогами до безпеки використання ядерної енергії не знають кордонів. Таким чином, уся світова спільнота повинна усвідомлювати свою відповідальність за шляхи розвитку ядерної енергетики, розробку нових підходів до її безпеки. Одним із них є забезпечення інтегрованого підходу до питань ФЯБ і ЕЯБ. Про цей підхід йдеться у Сеульському комюніке: «Визнаючи, що заходи у галузі (експлуатаційної) ядерної безпеки та (фізичної) ядерної безпеки мають спільну мету захисту життя і здоров'я людей, а також навколишнього середовища, ми підтверджуємо, що розробка, реалізація й координація заходів щодо забезпечення (експлуатаційної) ядерної безпеки та (фізичної) ядерної безпеки на ядерних установках повинні здійснюватися з дотриманням принципів послідовності та взаємодоповнюваності»[49].

Але на шляху до реалізації цього підходу існує ряд проблем, однією з яких є обробка та обмін інформацією між відомствами, що відповідають за кожний із зазначених напрямів. Інформаційна політика у сфері ФЯБ базується на конфіденційності, що передбачає надання доступу до відповідної інформації лише уповноваженим на це особам. І навпаки, основною метою інформаційної політики у сфері ЕЯБ є прозорість. У т.ч. для інформування населення щодо радіаційної ситуації на об'єкті, у зв'язку з необхідністю обміну досвідом і для того, «...щоб запобігти подібним інцидентам або аваріям на інших об'єктах атомної промисловості у майбутньому»[50].

Тим не менше, проблеми забезпечення ФЯБ та ЕЯБ повинні вирішуватися комплексно. Аналіз наймасштабніших аварій у ядерній галузі – на Чорнобильській АЕС в Україні та АЕС Фукусіма-1 у Японії – підтверджує необхідність саме такого підходу.

Таким чином, для досягнення основної мети, з одного боку, необхідно інтегрувати заходи, що здійснюються в обох напрямах, а з іншого – враховувати особливості кожного з них, тобто існує необхідність в оптимізації процесу інтеграції підходів через їх гармонізацію та взаємоузгодженість. На мій погляд, для цього необхідно:

• розробити нормативно-правове підґрунтя для нормативно-правового забезпечення діяльності у цьому напрямі;

• розробити методичні рекомендації зі впровадження заходів щодо забезпечення інтегрованого підходу до ЕЯБ і ФЯБ на нових об'єктах ядерного паливного циклу;

---

[49][Електронний ресурс]. – Режим доступу: http://www.cfr.org/proliferation/seoul-communiqu-2012-nuclear-security-summit/p27735

[50]*The interface* between safety and security at nuclear power plants: a report by the International Nuclear Safety Group. – Vienna : International Atomic Energy Agency, 2010.

• розробити концепцію та програму щодо впровадження заходів, спрямованих на реалізацію цього підходу на вже існуючих ядерних об'єктах України;

• розробити освітні програми та навчальні курси для фахівців атомної галузі щодо запровадження інтегрованого підходу до ЕЯБ і ФЯБ в Україні.

Виходячи з того, що Державна інспекція ядерного регулювання (Держатомрегулювання) України є національним регулятором як ядерної безпеки, так і фізичного захисту ядерних матеріалів та ядерних установок, то було б доцільно запропонувати створити при Держатомрегулюванні міжвідомчу робочу групу для розробки плану заходів з реалізації одного з основних положень Сеульського комюніке стосовно необхідності запровадження інтегрованого підходу до експлуатаційної ядерної безпеки та фізичної ядерної безпеки.

ЧУМАК Дмитро Вікторович,
спеціаліст з міжнародних відносин Українського ядерного товариства

ПРО СИНЕРГІЮ ФІЗИЧНОЇ ЯДЕРНОЇ БЕЗПЕКИ ТА ГАРАНТІЙ МАГАТЕ З ПИТАНЬ ПРОТИДІЇ ЯДЕРНОМУ ТЕРОРИЗМУ ТА НЕЗАКОННОМУ ОБІГУ ЯДЕРНИХ МАТЕРІАЛІВ

Нині спостерігається значне посилення уваги світової спільноти до проблеми використання ядерної енергії. Ступінь довіри людей до ядерної енергетики визначається тим, наскільки вони вважають мирний атом безпечним. Однак останнім часом сталися події, які негативно вплинули на подальші перспективи ядерної енергетики. З цієї точки зору насамперед слід відзначити, катастрофічні наслідки ядерної кризи на АЕС Фукусіма-1, а також відмову низки європейських країн від розвитку атомної енергетики на своїй території.

Натомість нині приблизно 440 реакторів у світі використовуються для виробництва електроенергії, більш ніж у 15 країнах частка ядерної енергетики в енергобалансі перевищує 25 %[51], а в таких європейських країнах, як Франція, Словаччина та Бельгія – навіть 50 %. До країн,

[51][Електронний ресурс]. – Режим доступу: http://www.world-nuclear.org/why/default.aspx?id=38&terms=Nuclear%20Power%20in%20Belgium

у яких ядерна енергетика відіграє визначальну роль у національній економіці, належить і Україна, де на АЕС виробляється приблизно 50 % електроенергії.

Країни цієї категорії вважають ядерну енергетику найбільш екологічно чистою і такою, яка може задовольнити їх енергетичні потреби, підвищуючи рівень енергетичної незалежності. Природно, що такі країни продовжують свої зусилля, спрямовані на розвиток ядерної енергетики.

Крім того, чимало країн мають довгострокові плани щодо започаткування або відновлення своїх ядерних енергетичних програм. Наведу тільки кілька прикладів. 11 жовтня 2011 р. підписано Контрактну угоду про будівництво енергоблоків № 1 і 2 АЕС на Островецькому майданчику в Гродненській обл. між ЗАТ «Атомстройекспорт» (Російська Федерація) і ГУ «Дирекція будівництва атомної електростанції» (Республіка Білорусь)[52]. Також у жовтні 2011 р. прем'єр-міністр Литви Андрюс Кубілюс заявив, що роботи за проектом Вісагінської АЕС йдуть за планом. Слід відзначити, що будівництво ВАЕС має початися у 2014 р. і завершитися до 2020 р.[53] Польща планує оголосити тендер про відбір реакторної технології для будівництва АЕС у листопаді 2011 р.[54] Україна розглядає питання будівництва 3-го та 4-го енергоблоків на Хмельницькій АЕС[55].

Таким чином, можна зробити висновок, що, незважаючи на ядерну кризу на АЕС Фукусіма-1, у найближчі десятиліття перспективи світової енергетики все ж таки будуть тісно пов'язані з використанням ядерної енергії. Але світова спільнота, безумовно, зробила суттєві висновки після фукусімської трагедії, і питання безпеки визнано найвищим пріоритетом при використанні ядерної енергії. При цьому на всіх рівнях посилюється усвідомлення того, що безпечне використання ядерної енергії можливе лише тоді, коли належна увага приділяється усім загрозам і ризикам, якими супроводжується цей процес.

Слід зазначити, що безпека використання ядерної енергії забезпечується за такими напрямами:

---

[52]Росія і Білорусь вибрали реактор для Гродненської АЕС [Електронний ресурс]. – Режим доступу: http://www.unian.ua/news/461665-rosiya-i-bilorus-vibrali-reaktor-dlya-grodnenskoji-aes.html

[53]Роботи по проекту Вісагінської АЕС йдуть за планом, – прем'єр-міністр Литви [Електронний ресурс]. – Режим доступу: http://www.rbc.ua/ukr/newsline/show/raboty-po-proektu-visaginskoy-aes-idut-po-planu---premer-ministr-06102011072100

[54]На будівництво АЕС у Польщі більшає претендентів [Електронний ресурс]. – Режим доступу: http://www.ua-energy.org/post/11305

[55]Проект «Будівництво енергоблоків ХАЕС – 3, 4» [Електронний ресурс]. – Режим доступу: http://www.energoatom.kiev.ua/ua/arch?_m=pubs&_t=rec&id=29181

• експлуатаційна ядерна безпека (*nuclear safety*) – захист персоналу, населення та довкілля від шкідливого впливу ядерних технологій, ядерних матеріалів та ядерних установок;

• фізична ядерна безпеки (*nuclear security*) – захист ядерних технологій, ядерних матеріалів та ядерних установок від несанкціонованих дій людей;

• гарантії МАГАТЕ (*IAEA Safeguards*) – контроль МАГАТЕ з метою недопущення переключення атомної енергії з мирного застосування на її використання у військових цілях.

Нині одним із найбільш суттєвих викликів, на який ядерна енергетика має дати адекватну відповідь, є ядерний тероризм. Протидії ядерному тероризму було присвячено Вашингтонський саміт з (фізичної) ядерної безпеки *(2010 Washington Nuclear Security Summit*), що відбувся 13–14 квітня 2010 р.[56] Загрози ядерного тероризму тісно пов'язані з рівнем незаконного обігу ядерних матеріалів, які можуть бути використані для вчинення терористичних актів. Заходи, спрямовані на протидію цим загрозам, відносять до фізичної ядерної безпеки (*nuclear security*) та гарантій МАГАТЕ (*IAEA Safeguards*).

Якщо розглядати ці напрями діяльності, то важливо зазначити, що вони охоплюють фактично одну і ту ж сферу – контроль над ядерним матеріалом, але на різних рівнях. Якщо функціонування систем обліку та контролю, а також фізичного захисту матеріалу, які є складниками фізичної ядерної безпеки, забезпечується в основному на національному рівні, то гарантії МАГАТЕ здійснюються на міжнародному рівні. Саме тому взаємодія даних елементів вимагає здійснення заходів щодо оптимізації їх діяльності.

У зв'язку з цим на міжнародній арені поширюється ідея «синергії». Об'єднання зусиль фахівців, які працюють на окремих напрямах забезпечення безпеки, їх взаємодія та співпраця здатні забезпечити ефект позитивної синергії, результатом якого може стати значно вищий рівень захищеності ядерних об'єктів та ядерних матеріалів від загроз ядерного тероризму.

Гарантії МАГАТЕ. Згідно зі ст. III Договору про нерозповсюдження ядерної зброї (ДНЯЗ) кожна «з держав-учасниць Договору, що не володіє ядерною зброєю, зобов'язується прийняти гарантії, як вони викладені в угоді, про яку будуть вестися переговори і яку буде укладено з Міжнародним агентством з атомної енергії відповідно до Статуту Між-

[56] *Коммюнике* участников Вашингтонского саммита по ядерной безопасности [Електронний ресурс]. – Режим доступу: http://www.america.gov/st/peacesec-russian/2010/April/20100415094507eaifas0.7762873.html

народного агентства з атомної енергії та системою гарантій Агентства, виключно з метою перевірки виконання його зобов'язань, прийнятих відповідно до цього Договору з тим, щоб не допустити переключення ядерної енергії з мирного використання на ядерну зброю чи інші ядерні вибухові пристрої».

Відповідно до п. 7 документа МАГАТЕ *IAEA INFCIRC/153* (*corrected*)[57] держава, що підписала угоду з МАГАТЕ, у зв'язку з Договором про нерозповсюдження ядерної зброї повинна створити національну систему обліку та контролю за ядерними матеріалами, причому таким чином, щоб Агентство могло безперешкодно перевіряти її з метою підтвердження, що ядерний матеріал не було переключено на військові цілі.

Таким чином, здійснюється подвійний контроль: суб'єкти державної системи обліку та контролю ядерних матеріалів направляють звіти про свою діяльність до національного регулятора, який, за необхідності, може здійснити інспекцію та перевірити відповідність наданої інформації фактичній ситуації[58]. Після цього регулятор повинен відправити у відповідній (закодованій) формі інформацію до Агентства, яке своєю чергою здійснює інспекції відповідно до угоди з державою[59].

Головною проблемою здійснення заходів у цьому напрямі є неповне охоплення гарантіями всіх держав світу. У цьому контексті передусім слід звернути увагу на те, що система гарантій постійно еволюціонує в напрямі пошуку найефективніших методів виконання поставлених завдань щодо забезпечення контролю над використанням ядерних технологій.

Розширення можливостей і надання додаткового доступу для інспекторів МАГАТЕ відповідно до Додаткового протоколу вимагатиме значних витрат. Разом з тим діяльність МАГАТЕ має реалізовуватися у межах попередньо встановленого бюджету. Ця ситуація вимагала

---

[57][Електронний ресурс]. – Режим доступу: http://www.iaea.org/Publications/Documents/Infcircs/Others/infcirc153.pdf

[58]*Стаття 1.3* наказу Державної інспекції ядерного регулювання України «Про затвердження Правил ведення обліку та контролю ядерних матеріалів» // Про затвердження Правил ведення обліку та контролю ядерних матеріалів : наказ Держ. інспек. ядер. регулювання України від 26.06.2006 р. № 97 [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/laws/show/z0845094420509-06

[59]*Стаття 1.4* наказу Державної інспекції ядерного регулювання України «Про затвердження Правил ведення обліку та контролю ядерних матеріалів» // Про затвердження Правил ведення обліку та контролю ядерних матеріалів : наказ Держ. інспек. ядер. регулювання України від 26.06.2006 р. № 97 [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/laws/show/z0849-06

пошуку оптимального способу вирішення цієї проблеми. У результаті були розроблені підходи до запровадження системи інтегрованих гарантій МАГАТЕ. Це означає, що нові заходи контролю інтегрують у вже імплементовані процедури і завдяки цьому вдається уникати зайвого навантаження на держави, з одного боку, і на Агентство – з іншого, що забезпечує максимальну ефективність діяльності у межах наявних ресурсів.

Але, на жаль, не всі країни підтримують таку еволюцію систем гарантій МАГАТЕ, що має своїм наслідком існування прогалин у режимі нерозповсюдження у вигляді лише часткового, а не всеохопного контролю за ядерною діяльністю країн світової спільноти.

Фізична ядерна безпека. Відповідно до публікацій МАГАТЕ під терміном «фізична ядерна безпека» (англ. – *nuclear security*) розуміється «запобігання та виявлення викрадення, саботажу (диверсії), несанкціонованого доступу, незаконної передачі або інших зловмисних дій по відношенню до ядерних матеріалів, інших радіоактивних речовин або пов'язаних з ними установок і реагування на такі дії»[60].

Заходи, спрямовані на забезпечення ФЯБ, є ключовим складником системи протидії загрозам ядерного тероризму, тому їм приділяється першочергова увага в планах МАГАТЕ з фізичної ядерної безпеки, розробка і виконання яких розпочалися невдовзі після терористичних актів 11 вересня 2001 р.

Перший план з фізичної ядерної безпеки був розрахований на 2002–2005 рр., другий – на 2006–2009 рр. Відповідно до цих планів здійснювалася розробка настанов з фізичної ядерної безпеки, підтримка чинних міжнародних правових інструментів, підвищення рівня захищеності матеріалів та установок, забезпечення безпеки перевезень і кордонів, посилення можливостей виявлення та припинення незаконного обігу ядерних та інших радіоактивних матеріалів[61]. Нині МАГАТЕ виконує свій третій план з фізичної ядерної безпеки, завершення якого заплановане на 2013 р.

На національному рівні зусилля МАГАТЕ та держав-членів спрямовані зокрема на таке:

• протидію незаконному обігу ядерних та інших радіоактивних матеріалів шляхом підсилення національних можливостей щодо запобігання, виявлення та реагування у цій сфері;

---

[60] *Глоссарий* МАГАТЭ по вопросам безопасности. Терминология, используемая в области ядерной безопасности и радиационной защиты [МАГАТЭ]. – Изд. 2007 года. – Вена, 2007. – С. 263–264.

[61] [Електронний ресурс]. – Режим доступу: http://www.iaea.org/Publications/Booklets/NuclearSecurity/nsachievements0312.pdf

• запровадження мультидисциплінарного підходу до підвищення ефективності функціонування інфраструктури фізичної ядерної безпеки;

• синергію експлуатаційної ядерної безпеки, фізичної ядерної безпеки та гарантій;

• культуру фізичної ядерної безпеки[62].

Від ефективності заходів з ФЯБ значною мірою залежить рівень захищеності держави від терористичних загроз. Режим ФЯБ є складником глобальної безпеки.

При оцінці загроз ядерного та радіаційного тероризму, реагуванні на інциденти, пов'язані з незаконним обігом відповідних матеріалів, важливу роль відіграє База даних МАГАТЕ щодо інцидентів, пов'язаних із незаконним обігом ядерних та інших радіоактивних матеріалів (*IAEA's Illicit Trafficking Database, ITDB*)[63].

За даними МАГАТЕ, у програмі Бази даних (БД) нині беруть участь 112 держав-членів, а також держава, яка не є членом Агентства. На 31 грудня 2011 р. БД містила інформацію про 399 підтверджених державою інцидентів (їх загальна кількість – 2164), в яких мали місце несанкціоноване володіння, переміщення, спроби незаконної торгівлі матеріалами або інші злочинні дії. У 16 випадках вони стосувалися матеріалів високозбагаченого урану (ВЗУ) та плутонію. Випадки, зафіксовані у БД, свідчать про те, що в незаконному обігу або поза регулювальним контролем перебуває досить значна кількість ядерного матеріалу, а також радіоактивних джерел, що підвищує загрозу використання даних матеріалів у злочинних цілях.

Для досягнення ефекту синергії при виконанні заходів, спрямованих на безпечне використання ядерної енергії та нерозповсюдження ядерної зброї, існують три основних напрями зусиль, а саме: адекватне планування, ефективний обмін знаннями та оперативною інформацією, поточна координація дій та взаємодія. Необхідної інтеграції зусиль, які докладаються на різних напрямах забезпечення безпеки ядерних об'єктів, можна досягнути лише тоді, якщо існує спільне сприйняття ризиків і загроз ядерним та іншим матеріалам і установкам. Досягненню такого спільного усвідомлення ризиків та загроз управлінцями, спеціалістами та експертами, які забезпечують безпеку ядерних об'єктів,

---

[62]План по физической ядерной безопасности на 2010–2013 годы : доклад Генерального директора МАГАТЭ : GOV/2009/54-GC(53)/18 [Електронний ресурс]. – Режим доступу: http://www.iaea.org/About/Policy/GC/GC53/GC53Documents/Russian/gc53-18_rus.pdf

[63]Бази даних по незаконному обігу (*ITDB*) [Електронний ресурс]. – Режим доступу: http://www-ns.iaea.org/downloads/security/itdb-fact-sheet.pdf

може сприяти підхід, що враховує всі види загроз і небезпек (*англ. – all hazards approach)*.

Таким чином, підбиваючи підсумки, можна сказати, що як фізична ядерна безпека, так і система гарантій МАГАТЕ роблять свій внесок у спільні зусилля з метою протидії ядерному та радіаційному тероризму, а також незаконному обігу ядерних та інших радіоактивних матеріалів. Та якщо об'єднати зусилля на кожному із зазначених напрямів і максимально оптимізувати відповідні заходи за рахунок впровадження насамперед високих стандартів культури безпеки, то це може забезпечити ефект синергії, що позитивно впливатиме на рівень міжнародної безпеки, зміцнення режиму нерозповсюдження ядерної зброї та зниження загроз ядерного тероризму.

Для того, щоб активізувати процеси на цьому напрямі, можна рекомендувати таку послідовність дій:

• розробити нормативно-правове підґрунтя для законодавчого оформлення зусиль, спрямованих на досягнення ефекту синергії при здійсненні заходів із забезпечення експлуатаційної ядерної безпеки, фізичної ядерної безпеки та гарантій;

• розробити методичні рекомендації для вжиття заходів щодо забезпечення ефекту синергії при проектуванні та будівництві нових об'єктів ядерного паливного циклу в Україні;

• розробити концепцію та програму виконання заходів для досягнення синергії ЕЯБ, ФЯБ і гарантій на ядерних об'єктах України, що експлуатуються;

• розробити освітні програми та навчальні курси для фахівців атомної галузі щодо запровадження заходів для досягнення синергії ЕЯБ, ФЯБ і гарантій на ядерних об'єктах України.

БІРЮКОВ Дмитро Сергійович,
старший консультант відділу
екологічної та техногенної безпеки НІСД

ДО ПИТАННЯ ПРО ЗАХИСТ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ВІД КІБЕРАТАК

У сучасних умовах для розвитку національної економіки, вдосконалення роботи органів виконавчої влади, функціонування інформаційного та культурного середовища суттєво зростає значення інформаційних і телекомунікаційних інфраструктур. Уже звичним для

суспільства стала можливість неперервно та повсюдно користуватися численними інформаційними, комунікаційними, фінансовими та іншими видами послуг, що надають такі інфраструктури. Але разом із перевагами, які надають розвиток і широке впровадження інформаційних технологій (ІТ), відмічається і тенденція до зростання кількості спроб несанкціонованого втручання (СНВ) у роботу як корпоративних, так і державних інформаційних систем і мереж[64].

Очевидним є той факт, що найбільша кількість СНВ відмічається у розвинених країнах, причому причини та мотиви їх здійснення переважно мають суто криміналістичне коріння, про що свідчать результати дослідження, опублікованого компанією *PricewaterhouseCoopers*. У ньому, зокрема, зазначається, що проти 23 % респондентів із 4 тис. організацій із 78 країн світу були вчинені кіберзлочини[65].

Разом з тим непоодинокими є випадки кібератак, спрямованих проти інформаційних ресурсів органів влади різних країн. Наприклад, кількість зареєстрованих кібератак на сервери та мережі, що обслуговують федеральні органи влади США, за даними підрозділу Міністерства внутрішньої безпеки (Команди готовності до комп'ютерних надзвичайних ситуацій (*англ.* – *Computer Emergency Readiness Team*, *US-CERT*), уже у 2010 р. становила понад 41 тис. випадків (приріст понад 40 % за рік)[66].

Слід зауважити, що інформаційні ресурси державних установ стають об'єктами атак не тільки у розвинених країнах. Приклад – атака на портал уряду Киргизії[67], яка була здійснена у серпні 2012 р. У результаті атаки на веб-сторінці цього порталу були розміщені гасла та відео ролик, які арабською мовою закликали до безладів.

Впровадження новітніх *IT* та інформаційно-комунікаційних систем (ІКС) у діяльність органів державної влади та органів місцевого самоврядування визначено одним із пріоритетних напрямів державної політики України в інформаційній сфері[68]. Поряд з очевидними

---

[64]*Development* of Policies for Protection of Critical Information Infrastructures // Background Report for OECD Ministerial Meeting on the Future of the Internet Economy. – OECD, 2007. – 101 p.

[65]*Cybercrime:* protecting against the growing threat / Global Economic Crime Survey. – PricewaterhouseCoopers, 2011. – 36 p.

[66]*US* Computer Emergency Readiness Team [Електронний ресурс]. – Режим доступу: http://www.us-cert.gov

[67]*Хакеры* взломали сайт правительства Киргизии. – Комментарии [Електронний ресурс]. – Режим доступу: http://ht.comments.ua/2012/08/28/356974/hakeri-vzlomali-sayt.html

[68]*Про Основні* засади розвитку інформаційного суспільства в Україні на 2007–2015 роки : закон України від 9.01.2007 р. № 537-V // Відомості Верховної Ради України. – 2007. – № 12. – С. 102.

перевагами застосування сучасних ІТ та електронного урядування численні вразливості елементів ІКС утворюють нові неминучі ризики для функціонування системи надання державних послуг.

У нашої держави вже є власний досвід протистояння кібератакам на сайти органів державної влади, що відбулися після закриття за рішенням суду у рамках розслідування кримінальної справи (ч. 2 ст. 176 КК – порушення авторських і суміжних прав) у січні 2012 р. сайту найбільшого сервісу обміну файлами, сервери якого були фізично розміщені в Україні. А під час виборів до Верховної Ради 2012 р. про хакерські атаки на власні сайти повідомляли опозиційні партії[69].

Також слід ураховувати, що в Україні, за експертними оцінками, обсяг безготівкових розрахунків швидко зростає. У 2011 р. він складав приблизно 400 млн дол. США. Водночас відзначається тенденція до зростання числа кіберзлочинів, причому з території України кіберзлочинцями здійснюються атаки на сервери іноземних фінансових установ[70].

Кіберзагрози об'єктам КІ мають такі характерні риси:

• ризики КІ охоплюють сфери відповідальності різних відомств, впливають на різні взаємопов'язані галузі та характеризуються можливістю виникнення каскадного ефекту;

• спостерігається суттєва уразливість об'єктів інформаційної КІ;

• захист об'єктів інформаційної КІ повинен забезпечуватися на всіх об'єктах, незалежно від форми власності.

Розглянувши статистику здійснених кібератак на об'єкти критичної інфраструктури (КІ), можна виділити такі дві групи: атаки, що здійснюються на сервери та мережі, які обслуговують органи влади, фінансові установи, великі компанії та поєднані в ІКС; атаки на автоматизовані системи управління (АСУ) на промислових об'єктах. Остання група атак привертає підвищену увагу, оскільки несанкціоноване втручання у роботу автоматизованих систем управління технологічним процесом (АСУ ТП) на об'єктах КІ може призвести до надзвичайно тяжких наслідків.

Раніше експертами вважалося, що АСУ ТП надійно захищені від зовнішніх СНВ, оскільки, як правило, є ізольованими від зовнішніх комп'ютерних мереж і використовують специфічне апаратне та про-

---

[69] *Оппозиция* заявляет об осуществлении хакерских атак на свои сайты [Електронний ресурс]. – Режим доступу: http://www.rbc.ua/rus/top/show/oppozitsiya-zayavlyaet-ob-osushchestvlenii-hakerskih-atak-na-04112012151800

[70] *Володимир Сивкович*: «Сьогодні кібертероризм – це не віртуальна загроза» [Електронний ресурс]. – Режим доступу: http://www.radioera.com.ua/eranews/?idArticle=44235

грамне забезпечення. Але після виявлення першого факту зараження АСУ ТП вірусом *Stuxnet*[71] у 2010 р. відбулася переоцінка ступеня вразливості промислових об'єктів. Як правило, подібні кібератаки супроводжуються попереднім збором конфіденційної інформації про об'єкт можливого нападу за допомогою вірусів-шпигунів, на зразок *Duqu*[72] та *Flame*[73]. Це підтверджується оприлюдненою у березні 2012 р. інформацією про виявлені спроби втручання у роботу АСУ ТП об'єктів газотранспортних систем у США[74]. Розслідування наслідків спроб втручання показало, що ці кібератаки належать до однієї групи та пов'язані з фішинговою активністю, яка була спрямована проти персоналу компаній-операторів газотранспортних систем, починаючи з грудня 2011 р.

Можливість здійснення кібератак з боку терористичних організацій нині розцінюється як реальна загроза. За даними, оприлюдненими Національним центром захисту інфраструктури Федерального бюро розслідувань США, Аль-Каїда намагалася здійснити хакерську атаку на системи управління об'єктів водопостачання у Сполучених Штатах, а для здійснення цих атак збиралася інформація про технічні характеристики програмного забезпечення[75].

Суттєвим також визнається вплив людського фактора на рівень інформаційної безпеки. Зокрема, у директивах Організації економічного співробітництва та розвитку відзначається, що кожен користувач ІТ повинен мати відповідні знання, бути відповідальним, вжити необхідних заходів для забезпечення безпеки власних інформаційних систем і мереж[76]. Дії користувача ІТ мають бути узгоджені із цінностями демократичного суспільства, такими як необхідність відкритого й вільного обміну інформацією та захист персональних даних.

Узагальнюючи *результати проведених досліджень у галузі інформаційної безпеки АСУ ТП,* потрібно зазначити таке:

---

[71] *Stuxnet* Dossier // Symantec Security Response. – February. – 2011. – 68 p.

[72] *The precursor* to the next Stuxnet // Symantec Security Response. – November. – 2011. – 46 p.

[73] *Joint* security awareness report, May 2012 [Електронний ресурс]. – Режим доступу: http://tinyurl.com/6o2vmvq

[74] *ICS-CERT* Monthly Monitor, April 2012 [Електронний ресурс]. – Режим доступу: http://www.us-cert.gov/control_systems/pdf/ICS-CERT_Monthly_Monitor_Apr2012.pdf

[75] *Grosskruger P.* Analysis of the U.S. Water Infrastructure from a Security Perspective / P. Grosskruger // Strategy Research Project. – U.S. Army War College, 2006. – 24 p.

[76] *OECD* Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security. – Paris : OECD, 2002. – 28 p.

• сучасні програмні засоби у поєднанні із загальнодоступною інформацією дають можливість навіть малодосвідченим зловмисникам здійснювати кібератаку на системи та апаратні засоби таких інфраструктурних мереж, як, наприклад, високовольтні лінії електропередачі[77];

• спостерігається тенденція до стрімкого зростання числа виявлених вразливостей (за перші 3 квартали поточного року у спеціалізованих базах даних та в повідомленнях виробників опубліковано дані про більшу кількість вразливостей, ніж за період часу, починаючи з 2005 р.[78]);

• вразливості виявляються передусім у найпоширеніших моделях устаткування; кожна п'ята вразливість не була закрита протягом місяця, близько 65 % вразливостей належать до високого та критичного ступеня ризику (значно гірше, ніж в інших *IT*-системах, комп'ютерних мережах тощо), а кожна друга вразливість надає зловмиснику можливість виконати довільні команди на атакованій АСУ ТП[79];

• лідерами по кількості АСУ ТП, до яких можливий доступ через Інтернет, є США та країни ЄС, причому вони залишаються найбільш уразливими до такої загрози, зокрема через нехтування вимогами інформаційної безпеки (допущення помилок у конфігурації систем, використання слабких або навіть стандартних паролів, не відмови від оновлень системи)[80].

До *потенційно вразливих складників* інформаційної інфраструктури підприємства, що найчастіше використовуються як об'єкти нападу при здійсненні атаки на АСУ ТП, можна віднести:

• сервер організації, що має вихід у «зовнішній світ» (піддається постійним атакам через Інтернет);

• персональні мобільні комп'ютери (ноутбуки, планшетні комп'ютери, смартфони тощо), які функціонують на основі загальнорозповсюдженої ОС, мають уразливі місця та використовуються спів-

---

[77] *Increasing* Threats to Industrial Controll Systems // ICS-CERT Alert 12-046-01A, October 25, 2012 [Електронний ресурс]. – Режим доступу: http://www.us-cert.gov/control_systems/pdf/ICS-ALERT-12-046-01A.pdf

[78] *Безопасность* промышленных систем в цифрах [Електронний ресурс]. – Режим доступу: http://filearchive.cnews.ru/doc/2012/06/scada.pdf

[79] *An experimental* investigation of malware attacks on SCADA systems / I. N. Fovino, A. Carcano, M. Masera, A. Trombetta // International Journal of Critical Infrastructure Protection. – 2009. – Vol. 2, Issue 4. – P. 139–145.

[80] *Luiijf E.* Assessing and improving SCADA security in the Dutch drinking water sector / *E. Luiijf*, M Ali., A. Zielstra // International Journal of Critical Infrastructure Protection. – 2011. – Vol. 4, Issues 3–4. – P. 124–134.

робітниками й керівництвом підприємства спільно з робочими (захищеними) комп'ютерами (іноді здійснюється передача даних між персональним і робочим комп'ютером);

• апаратне забезпечення (комп'ютери) з підключенням до локальної мережі;

• комп'ютери, які мають порти для приєднання зйомних накопичувачів, дисководи для зчитування інформації з оптичних дисків.

Значну загрозу безпеці об'єктів КІ становлять скоординовані атаки з використанням програмних вірусів. Такий вид атаки поєднує підготовчий етап (дії, що створюють на об'єкті нові уразливі місця) та атакувальні дії (використання уразливих місць). При цьому підготовчі дії можуть бути здійснені далеко заздалегідь, із залученням працівників підприємства (інсайдерів), що є об'єктом нападу, та здійсненням різноманітних відволікальних маневрів.

Основними *контрзаходами*, що використовуються для управління кібербезпекою в АСУ ТП, називають[81]:

• впровадження політики безпеки (політика безпеки повинна бути розроблена для мережі системи управління та її окремих компонентів, вона повинна періодично переглядатися, щоб ураховувати нові загрози та функціональні можливості системи);

• контроль доступу до ресурсів та сервісів (застосовується у мережі шляхом використання таких пристроїв контролю доступу, як брандмауери та проксі-сервери);

• виявлення шкідливої активності (зазвичай реалізується у вигляді регулярного моніторингу лог-файлів досвідченими адміністраторами та застосуванням систем виявлення втручань)[82];

• пом'якшення можливих атак (контроль адміністраторами доступу до вразливості таким чином, щоб уразливість не можна було використати у випадках, коли усунення вразливості може призвести до непрацездатності або неефективності системи);

• виправлення помилок у ядрі системи, що завжди вимагає оновлення програмного забезпечення (мережевого, операційної системи або прикладного програмного забезпечення)[83].

---

[81] *Recommended* Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies. – National cybersecurity division, US DHS, 2009. – 44 p.

[82] *Guide* to Intrusion Detection and Prevention Systems / K. Scarfone, P. Mell. – Recommendations of the National Institute of Standards and Technology. Special Publication 800-94. – 2007. – 127 p.

[83] *Developing* an Industrial Control Systems Cybersecurity Incident Response Capability–CSSP Recommended Practices [Електронний ресурс]. – Режим доступу: http://www.us-cert.gov/control_systems/practices/

Професійно організована комп'ютерна атака складається з декількох етапів, пов'язаних із визначенням цілей, розвідкою, забезпеченням доступу до системи, безпосередньою реалізацією атаки, знищенням доказів про втручання.

Тому загальний *план протидії* кібератакам повинен включати заходи щодо:

• забезпечення можливості своєчасного виявлення та реагування на кібератаки;

• моніторингу та усунення виявлених уразливостей;

• відновлення пошкоджених систем, мереж та устаткування;

• зменшення (мінімізацію) наслідків таких нападів.

Нині проблеми інформаційної безпеки розглядаються на рівні експертів, а кращий досвід у цій галузі узагальнюється у рекомендаціях таких авторитетних організацій, як Всесвітній інститут фізичної ядерної безпеки[84]. Експертами відзначається, зокрема, здійснення компаніями-розробниками АСУ ТП технічного обслуговування та віддаленого налаштування АСУ критично важливих об'єктів у цілому або їх складників, а також телекомунікаційного обладнання, що входить до складу інформаційної КІ, а також прагнення компаній-розробників програмного забезпечення АСУ до зниження витрат і, як наслідок, використання типових рішень і запозиченого програмного забезпечення.

На відміну від США та країн-членів ЄС, в Україні дистанційне управління АСУ технологічних процесів на АЕС, яке забезпечує в тому числі передачу команд пристроям нижнього рівня з використанням мережевих структур або виділених ліній зв'язку, нині не використовує вразливих технологій та апаратного чи програмного забезпечення[85]. У системах життєзабезпечення, енергетики та транспорту часто використовуються АСУ вітчизняного (або ще радянського) виробництва. Але подальша модернізація АСУ на таких інфраструктурних об'єктах з використанням поширених інформаційних технологій та мережевих рішень привнесуть притаманні їм «родинні» вразливості.

Останні тенденції щодо врахування питань кібербезпеки у законодавстві України. На відміну від стрімких темпів розвитку інформаційних технологій, законодавство у цій сфері змінюється значно повільніше.

---

[84] *Security* of IT and IC Systems at Nuclear Facilities. – Vienna : World Institute for Nuclear Security, 2011. – 22 p.

[85] *Дистанционное* дисплейное управление в АСУ ТП атомных электростанций / Е. В. Александров, А. Х. Горелик, И. Д. Розенбаум // Проблемы обеспечения безопасности информационных и управляющих систем АЭС : сб. науч. тр. под ред. М. А. Ястребенецкого. – Одесса : Астропринт, 2010. – С. 84–88.

Термін «інформаційна безпека» було введено в Законі України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» (розділ 3, п. 13)[86]: «Інформаційна безпека – стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації».

Одним із шляхів забезпечення інформаційної безпеки визначається «створення повнофункціональної інформаційної інфраструктури держави та забезпечення захисту її *критичних елементів*» (ІІІ.13[87]). Проте ні самого переліку «критичних елементів» інформаційної інфраструктури, ні методології їх віднесення до такого переліку не було затверджено. Питання щодо необхідності визначення найважливіших (критичних) щодо кіберзагроз об'єктів та інфраструктури в державі порушувалося в Рішенні Ради національної безпеки і оборони України від 17.11.2010 р. «Про виклики та загрози національній безпеці України у 2011 році»[88], в якому (п. 4.б абз. 3) Кабінету Міністрів України доручено «розробити за участю Служби безпеки України та затвердити перелік об'єктів, що мають важливе значення для забезпечення національної безпеки і оборони України та потребують першочергового захисту від кібернетичних атак».

Також потрібно зауважити, що в новій Стратегії національної безпеки[89] у четвертому розділі «Стратегічні цілі та основні завдання політики національної безпеки» одним із шляхів забезпечення інформаційної безпеки (п. 4.3.8.) визначено «забезпечення безпеки інформаційно-телекомунікаційних систем, що функціонують в інтересах управління державою, забезпечують потреби оборони та безпеки держави, кредитно-банківської та інших сфер економіки, систем управління об'єктами критичної інфраструктури».

---

[86]*Про Основні* засади розвитку інформаційного суспільства в Україні на 2007–2015 роки : закон України від 9.01.2007 р. № 537-V // Відомості Верховної Ради України. – 2007. – № 12. – С. 102.

[87]Там само.

[88]Введено в дію Указом Президента України від 10.12.2010 р. № 1119/2010 «Про рішення Ради національної безпеки і оборони України від 17 листопада 2010 року «Про виклики та загрози національній безпеці України у 2011 році».

[89]Введено в дію Указом Президента України від 08.06.2012 р. № 389/2012 «Про рішення Ради національної безпеки і оборони України від 8 червня 2012 року «Про нову редакцію Стратегії національної безпеки України».

Водночас термін «критична інфраструктура» так і не був визначений у законодавстві України, хоча його час від часу використовують в офіційних документах. Уперше він з'явився у 2006 р. у тексті Рекомендацій парламентських слухань з питання розвитку інформаційного суспільства[90]. На жаль, робота зі впровадження цих рекомендацій, у т.ч. стосовно захисту критичної інфраструктури від широкого кола загроз, у подальшому припинилася.

У Проекті закону України «Про внесення змін до деяких законів України щодо забезпечення кібернетичної безпеки України» (зареєстрований під № 11125 від 31.08.2012 р.)[91] передбачалося внесення змін до Закону України «Про основи національної безпеки України», і, зокрема, введення терміна «об'єкти критичної інформаційної інфраструктури» в такій редакції: «Об'єкти критичної інформаційної інфраструктури – це сукупність інформаційно-телекомунікаційних систем державного та приватного сектору, що забезпечують функціонування та безпеку стратегічних інститутів, систем і об'єктів держави (органів центрального та місцевого управління, систем управління енергетикою, транспортом, зв'язком, банківським сектором, підприємств, під час діяльності яких використовуються та/або виробляються небезпечні речовини тощо) і безпеку громадян (системи управління правоохоронних структур й оборонного сектору тощо), несанкціоноване втручання в роботу яких може загрожувати економічній, екологічній, соціальній та іншим видам безпеки або завдати шкоди міжнародному іміджу держави».

Такому визначенню відповідає широкий спектр об'єктів, тому основним питанням нині стає методика віднесення об'єктів до категорії «критична інфраструктура».

Паралельно з названим законопроектом розробляється ще низка нормативно-правових актів у сфері інформаційної безпеки. Відповідно до Рішення Ради національної безпеки і оборони України від 25.05.2012 р. «Про заходи щодо посилення боротьби з тероризмом в Україні»[92] Кабінету Міністрів України доручено розробити Проект закону про кібернетичну безпеку, а Адміністрації Держспецзв'язку

---

[90]*Про Рекомендації* парламентських слухань з питань розвитку інформаційного суспільства в Україні : постанова Верховної Ради України // Відомості Верховної Ради України. – 2006. – № 15. – С. 131.

[91]*Про внесення* змін до деяких законів України щодо забезпечення кібернетичної безпеки України : законопроект [відкликано 12.12.12] [Електронний ресурс]. – Режим доступу: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?id=&pf3511=44208

[92]Введено в дію Указом Президента України від 08.06.2012 р. № 388/2012 [Електронний ресурс]. – Режим доступу: http://www.president.gov.ua/documents/14822.html

разом зі Службою безпеки України проект Програми захисту державних інформаційних ресурсів від протиправного втручання в їх діяльність.

Потрібно зауважити, що становлення нормативно-правової бази у сфері кіберзахисту КІ є тривалим процесом. Наприклад, у США із середини 1990-х рр. були введені в дію: наказ президента «Про роботу з дослідження вразливості захисту критичної інфраструктури від кібернетичних та фізичних загроз» (липень 1996 р.), директива президента № 63 (травень 1998 р.), Національний план захисту інформаційних систем (січень 2000 р.), наказ президента «Організація захисту США від терористичних загроз» і «Про захист національних критичних інформаційних систем» (жовтень 2001 р.), Політика у сфері кіберпростору (2009 р.), а також Стратегія національної безпеки (березень 2010 р.)

Міністерство оборони США є основним ідеологом розвитку інформаційних і телекомунікаційних технологій, а в компетенції «розвідувального співтовариства» – збір інформації щодо усунення загроз і попередження злочинів, спрямованих проти національних інформаційних систем. Для забезпечення безпеки об'єктів КІ *CERT* надає громадськості та приватним компаніям (установам) можливість отримувати оперативну й ефективну допомогу з кібербезпеки. Водночас, на думку експертів Центру стратегічних та міжнародних досліджень (м. Вашингтон, США), поточна політика та законодавчі акти у сфері інформаційної безпеки США потребують перегляду та оновлення. У їх звіті вказується на необхідність впровадження кращих практик «неперервного моніторингу» комп'ютерних мереж в органах влади США.

Необхідність створення дієвої системи захисту критично важливих об'єктів та інфраструктури від кіберзагроз відзначена і в Стратегії національної безпеки Російської Федерації до 2020 р. З метою реалізації основних положень Стратегії, вдосконалення безпеки функціонування інформаційних і телекомунікаційних систем критично важливих об'єктів інфраструктури та об'єктів підвищеної небезпеки Радою безпеки РФ було розроблено Основні напрями державної політики в галузі забезпечення безпеки автоматизованих систем управління виробничими і технологічними процесами критично важливих об'єктів інфраструктури Російської Федерації (липень 2012 р.). У документі йдеться про єдину державну систему виявлення і попередження комп'ютерних атак на критичну інформаційну інфраструктуру та оцінки рівня реальної захищеності її елементів, що включає сили та засоби виявлення і попередження комп'ютерних атак, а також орга-

ни управління різних рівнів, до повноважень яких віднесено питання забезпечення безпеки автоматизованих систем управління критично важливих об'єктів та інших елементів критичної інформаційної інфраструктури.

Висновки та пропозиції

1. Подолання технологічного відставання промисловості та сфери послуг в Україні пов'язане зокрема із впровадженням новітніх інформаційних технологій. Поряд із безсумнівними перевагами та можливостями, що надають такі нововведення, може значно зрости вразливість об'єктів, на яких вони впроваджуються. Про це свідчить статистика здійснених і вдалих спроб несанкціонованого втручання в роботу серверів та мереж, на яких розміщені інформаційні ресурси та системи фінансових установ, великих транснаціональних компаній та органів державної влади розвинених країн світу.

2. Аналіз новітніх досліджень у даній галузі вказує на тенденцію до зростання у розвинених країнах світу кількості спроб несанкціонованого втручання у роботу автоматизованих систем управління технологічним процесом на промислових об'єктах, інтенсивного зростання кількості виявлених вразливостей у таких апаратно-програмних комплексах.

3. В Україні поступово вдосконалюється законодавство у сфері інформаційної безпеки. Водночас у чинному законодавстві досі відсутній термін «критична інфраструктура», тісно пов'язаний із проблематикою кібербезпеки, не впроваджено загального надвідомчого підходу до визначення об'єктів критичної інфраструктури, і, відповідно, не здійснюються координація та оптимізація організаційних і технічних інструментів їх захисту.

Зважаючи на недопустимість відмови інформаційних систем та автоматизованих систем управління на об'єктах критичної інфраструктури та основні тенденції в цій сфері, на нашу думку, в якості першочергових кроків доцільним є таке.

Започаткування експертного діалогу у форматі «регулятор-оператор» (уповноважений орган із питань організації спеціального зв'язку та захисту інформації – суб'єкт господарювання, що належить до критичної інфраструктури) задля поширення обміну передовим досвідом у сфері інформаційної безпеки об'єктів критичної інфраструктури.

Проведення інвентаризації та аналізу вразливості автоматизованих систем управління технологічним процесом, що функціонують в Україні на об'єктах підвищеної небезпеки, підприємствах стратегіч-

ного значення та інших об'єктах, які відносять до критичної інфраструктури.

Удосконалення, розробка та введення в дію національних стандартів у сфері кібербезпеки, зокрема для автоматизованих систем управління, що функціонують на об'єктах критичної інфраструктури.

Упровадження комплексного уніфікованого підходу до управління ризиком і зменшення загроз критичній інфраструктурі, реалізованого у вигляді довгострокових програм управління ризиками, що дають можливість максимізувати ефективність використання ресурсів для захисту, реагування на загрози та відновлення об'єктів критичної інфраструктури.

ТЕНДЕНЦІЇ ТА АКТУАЛЬНІ ПРОБЛЕМИ У СФЕРІ ПРОТИДІЇ НЕЗАКОННОМУ ОБІГУ ЯДЕРНИХ ТА ІНШИХ РАДІОАКТИВНИХ МАТЕРІАЛІВ, А ТАКОЖ ЯДЕРНОМУ ТА РАДІАЦІЙНОМУ ТЕРОРИЗМУ

Аналітична доповідь

КОНДРАТОВ Сергій Іванович,
науковий співробітник відділу техногенної та екологічної безпеки НІСД

ТЕНДЕНЦІЇ ТА АКТУАЛЬНІ ПРОБЛЕМИ У СФЕРІ ПРОТИДІЇ НЕЗАКОННОМУ ОБІГУ ЯДЕРНИХ ТА ІНШИХ РАДІОАКТИВНИХ МАТЕРІАЛІВ, А ТАКОЖ ЯДЕРНОМУ ТА РАДІАЦІЙНОМУ ТЕРОРИЗМУ

(аналітична доповідь)

ВСТУП

Згідно з підходом, застосованим Міжнародним агентством з атомної енергії (МАГАТЕ) при підготовці фундаментального довідника з питань протидії незаконному обігу ядерних та інших радіоактивних матеріалів, під **незаконним обігом розуміють злочинні або несанкціоновані дії по відношенню до ядерних та інших радіоактивних матеріалів, які можуть включати імпорт, експорт, володіння, продаж, постачання, переміщення, використання, зберігання, захоронення або передачу зазначених матеріалів**[93].

Останнім часом міжнародне співтовариство визнає протидію незаконному обігу ядерних та інших радіоактивних матеріалів (*далі* – НО) одним із пріоритетних напрямів у глобальних зусиллях, спрямованих на зниження загроз розповсюдження ядерної зброї, ядерного та радіаційного тероризму. Тож невипадково про це йдеться у Комюніке цьогорічного Сеульського саміту з (фізичної) ядерної безпеки, в якому лідери 53 держав (у т.ч. України), а також керівники таких міжнародних організацій, як ООН, МАГАТЕ, ЄС та ІНТЕРПОЛ, включили протидію НО до числа 13 найважливіших напрямів своєї діяльності[94].

Усвідомлення процесу зростання загроз тероризму, особливо його найнебезпечніших видів – ядерного і радіаційного, обумовлює вине-

---

[93] *IAEA* Nuclear Security, Combating Illicit Trafficking in Nuclear and other Radioactive Material : Reference Manual. – Vienna : IAEA, 2007. – Series No. 6.

[94] [Електронний ресурс]. – Режим доступу: http://thenuclearsecuritysummit.org/userfiles/Seoul%20Communique_FINAL.pdf

сення питань протидії йому на найвищий політичний рівень у глобальному масштабі. Фактори, що сприяють цьому процесу, стають об'єктами підвищеної уваги з боку розвідувальних і правоохоронних органів, спецслужб, а також науковців, експертів та аналітиків, які працюють у цій сфері.

У зв'язку з цим доцільно проаналізувати сучасні тенденції та проблеми, які існують у сфері протидії незаконному обігу ядерних та інших радіоактивних матеріалів, а також пов'язаних із ними видів тероризму. Представлений далі аналіз зроблено на основі матеріалів Другої конференції ІНТЕРПОЛу з аналізу незаконного обігу ядерних і радіоактивних матеріалів, а також ядерного і радіаційного тероризму, що відбулася у Шведському агентстві оборонних досліджень (*FOI*) у м. Умеа (Швеція) у період з 25 по 26 квітня 2012 р.

1. ПРОБЛЕМА НАДІЙНОСТІ ДАНИХ ТА ВІДСУТНОСТІ КРИТЕРІЇВ ОЦІНКИ УСПІШНОСТІ ПРОТИДІЇ НО

Передусім слід зазначити, що, незважаючи на велику увагу, яка приділяється як на національному, так і на міжнародному рівнях проблемам протидії НО, нині спостерігається певна плутанина у статистичних даних, спричинена відсутністю єдиного підходу до визначення самого терміна «незаконний обіг ядерних та інших радіоактивних матеріалів». Правоохоронні та розвідувальні органи, спецслужби та відповідні міжнародні організації, що перебувають на передньому рубежі боротьби із цим небезпечним явищем, поширення якого створює сприятливі умови для зростання загрози ядерного тероризму, відповідно до поставлених перед ними завдань приділяють головну увагу злочинним діям з ядерними та іншими радіоактивними матеріалами, і, таким чином, більш схильні трактувати зміст терміна у сенсі саме зловмисного переміщення, виготовлення та використання таких матеріалів, а також незаконного володіння ними.

Водночас державні органи регулювання у сфері ядерної та радіаційної безпеки, санітарно-епідеміологічні служби та органи реагування на надзвичайні ситуації віддають здебільшого перевагу підходу, згідно з яким будь-яке перебування ядерного та радіоактивного матеріалу поза межами регулюючого контролю вважається випадком незаконного обігу. Оскільки до офісу Бази даних МАГАТЕ щодо інцидентів, пов'язаних із незаконним обігом ядерних та інших радіоактивних матеріалів (*далі* – БДНО МАГАТЕ), рекомендовано звітувати

про усі випадки перебування матеріалів поза контролем державних органів, можна стверджувати, що і МАГАТЕ схильне до більш широкого тлумачення змісту цього терміна. Ця позиція агентства підкріплюється ще й достатньо розповсюдженим судженням про те, що звітування про всі інциденти дає змогу отримати більш повну картину не тільки щодо спроб незаконного та несанкціонованого переміщення матеріалів, а й щодо спроможності національних систем боротьби з НО, включаючи здійснення радіаційного контролю на державних кордонах, ефективно виявляти такі спроби.

Віддаючи належне цим міркуванням, водночас не можна не відзначити, що таке «широке» охоплення може створювати і створює певні труднощі при аналізі та тлумаченні статистичних даних, якщо при цьому не приділяється належної уваги розмежуванню зловмисних і ненавмисних дій щодо ядерних та радіоактивних матеріалів. Справді, в останньому випадку на тлі, наприклад, зниження кількості інцидентів з радіоактивно забрудненим металобрухтом можуть не так чітко вимальовуватися тенденції щодо інцидентів, пов'язаних із злочинними намірами стосовно ядерних та інших радіоактивних матеріалів.

Разом з тим, відзначаючи важливість виділення саме категорії зловмисних дій щодо зазначених матеріалів, не можна не згадати одну принципову річ, притаманну самому процесу кримінального розслідування: до завершення розслідування, яке може тривати достатньо довго, офіційно не можна робити остаточний висновок про наявність або відсутність злочинних намірів, тоді як запроваджені процедури звітування, наприклад до БД НО МАГАТЕ, рекомендують надавати інформацію якнайшвидше.

Крім того, при оцінці діяльності національних органів, які відповідають за протидію НО у тій чи іншій державі, досі не були встановлені загальновизнані чіткі критерії. Зокрема, це стосується статистичних даних щодо НО. У зв'язку з цим уже протягом тривалого часу раз по раз, у т.ч. і на міжнародних заходах, ставиться питання: про що саме свідчить велика кількість зареєстрованих випадків НО? Про незадовільний стан національної системи забезпечення захищеності (фізичної безпеки) матеріалів, або, навпаки, про її ефективність, щонайменше, з точки зору виявлення матеріалів у НО? Це питання було піднято і на згаданій конференції ІНТЕРПОЛу, що було відображено в її підсумковому документі.

Незважаючи на певні застереження, слід усе ж наголосити, що БД НО МАГАТЕ нині є одним із найбільш надійних джерел інформації про НО на міжнародному рівні.

Довідково. *База даних МАГАТЕ щодо інцидентів, пов'язаних із незаконним обігом ядерних та інших радіоактивних матеріалів, є інформаційною системою, яка створена у 1995 р. з метою сприяння МАГАТЕ, державам-членам Агентства та окремим міжнародним організаціям у їх діяльності з підвищення рівня фізичної ядерної безпеки. Інформація, яку збирає та аналізує персонал офісу БД НО МАГАТЕ, надсилається до держав-членів Агентства та до відповідних міжнародних організацій. Участь у програмі БД НО МАГАТЕ є добровільною. Станом на 31 грудня 2011 р. 113 держав (у т.ч. Україна) беруть у ній участь. Зв'язок із державами-учасницями БД НО МАГАТЕ відбувається через національні контактні пункти, визначені тією чи іншою державою. У нашій державі таким пунктом зв'язку визначена Державна інспекція ядерного регулювання України.*

2. ОГЛЯД ПРЕДСТАВЛЕНИХ НА КОНФЕРЕНЦІЇ ДОПОВІДЕЙ ТА РОЗГЛЯНУТИХ У НИХ ПРОБЛЕМ

Переходячи безпосередньо до самої конференції ІНТЕРПОЛу, слід звернути увагу на обмежену кількість аналітиків та експертів (до 30 осіб), залучених до участі в ній у межах проекту «Гейгер». Крім України та Естонії, на конференції не була представлена жодна інша колишня радянська республіка або держава-учасниця Організації Варшавського договору. У зв'язку з цим виникають певні питання щодо ретельності підготовки таких важливих заходів, оскільки вже традиційно (з початку 1990-х рр.) частина західних експертів та аналітиків вважає, що значний вплив на процеси і тенденції у цій сфері, щонайменше у Європі, має стан фізичної безпеки ядерних та інших радіоактивних матеріалів саме у зазначених державах.

На конференції було зроблено ряд доповідей, присвячених огляду тенденцій та методів аналізу у сфері протидії НО у глобальному, регіональному та національному вимірах. Зрозуміло, що найбільший інтерес з точки зору визначення загальносвітових тенденцій викликає інформація, оприлюднена представником офісу МАГАТЕ з питань фізичної ядерної безпеки **Д. Муром** *(G. M. Moore)*[95]. На (рис. 1) пока-

[95] *George M. Moore* (Office of Nuclear Security, IAEA), IAEA's Illicit Trafficking Database System (ITDB) Data and Trends, Interpol Radiological and Nuclear Trafficking and Terrorism: Analysis Conference / M. George. – Umeä, Sweden, 25–26 April 2012.

зано розподіл загальної кількості інцидентів, зафіксованих у БД НО МАГАТЕ по роках, у період з 2001 по 2011 рр. Діаграма відображає «широкий» підхід до тлумачення терміна «незаконний обіг», оскільки в ній враховані усі інциденти, пов'язані з виявленням ядерних і радіоактивних матеріалів поза межами регулюючого контролю.

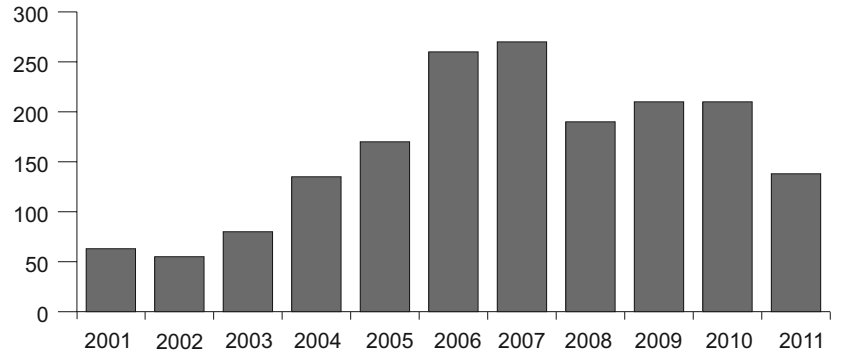

Рис. 1. Кількість інцидентів, зареєстрованих у БД МАГАТЕ

На графіку спостерігається очевидна тенденція значного зростання зареєстрованих інцидентів у період з 2002 по 2007 рр. з піком у 2006–2007 рр. Експерти у цій сфері приписують вказану тенденцію тому, що після терактів 11 вересня 2001 р., які сприяли усвідомленню масштабів загрози ядерного та радіаційного тероризму, у багатьох країнах світу значно активізувалися заходи, спрямовані на протидію НО, в т.ч. шляхом створення систем радіаційного контролю на державних кордонах, об'єктах і системах критичної інфраструктури тощо. Зокрема, саме на початку 2002 р. розпочалася підготовка до співпраці нашої держави зі США у цій сфері у рамках програми «Друга лінія захисту», яка передбачала обладнання всіх пунктів пропуску на державному кордоні України приладами та системами радіаційного контролю з метою подальшого їх об'єднання в єдину систему на національному рівні.

Як показує графік, найбільша кількість інцидентів у БД НО МАГАТЕ зареєстрована у 2006–2007 рр., але, відповідно до роз'яснення, наданих МАГАТЕ у своїх публікаціях, цей пік спричинений не стільки реальним зростанням кількості виявлених випадків НО, скільки змінами у процедурах звітування до БД НО МАГАТЕ, причому лише в

одній державі-учасниці цієї бази даних[96]. При цьому слід зауважити, що попри вже висловлену точку зору, що БД НО МАГАТЕ можна віднести до найбільш надійних джерел інформації стосовно НО, тим не менше при вивченні світових тенденцій і формулюванні висновків на цій основі необхідно дуже прискіпливо оцінювати надійність усіх даних, навіть з такого джерела, адже ситуація, коли в результаті внесення змін у процедури звітування лише в одній державі[97] кардинально змінюється глобальна картина процесів, пов'язаних з НО, безумовно, потребує додаткового аналізу і, напевне, вдосконалення процесу збору даних та їх обробки.

Незважаючи на ці застереження, інформація, надана БД НО МАГАТЕ, безумовно, є достатньо важливою. Починаючи від заснування бази даних (1995 р.) на кінець 2011 р. було зареєстровано 2164 підтверджених інциденти з ядерними та радіоактивними матеріалами, з яких 385 було віднесено до Групи I (несанкціоноване володіння та пов'язані з цим злочинні дії), 576 – до Групи II (крадіжки, втрати та пропажі), ще у 16 звітах інциденти були віднесені одночасно до Груп I та II, 1118 інцидентів потрапили до Групи III (несанкціонована діяльність та пов'язані з нею події). У цій загальній статистиці, знову ж таки, привертає увагу той факт, що в **ній зловмисні та несанкціоновані дії не були рознесені по різних групах**, **як це було б логічно зробити з точки зору протидії тероризму,** і тому, наприклад, до Групи II були віднесені як крадіжки, так і втрати (пропажі) матеріалу.

Наводячи ці дані, представник МАГАТЕ звернув увагу на такі особливості процесів, які відбуваються у цій сфері:

• **досі не було зафіксовано жодного випадку застосування пристрою для розпорошення радіоактивності (брудної бомби)**, але радіаційний інцидент у Гоянії (Бразилія) є прикладом можливих наслідків реалізації такої загрози;

• **досі не було жодного випадку здійснення терористичного акту, у результаті якого відбувся б викид радіоактивності на якійсь АЕС або якомусь дослідницькому реакторі**, але Чорнобиль і Фукусіма дають нам приклади масштабу загрози ядерного тероризму;

• **менш ніж 1 % інцидентів пов'язані з матеріалами, які могли би бути використаними для виготовлення ядерної зброї**, а їхня загальна кількість значно менша за т.зв. суттєву кількість (англ. –*significant quantity*).

---

[96][Електронний ресурс]. – Режим доступу: http://www.iaea.org/newscenter/features/radsources/pdf/fact_figures2007.pdf

[97]МАГАТЕ у своїх публікаціях не вказує назву цієї держави.

> ***Довідково.*** *Суттєва кількість (Significant Quantity) – це приблизна кількість ядерного матеріалу, для якої не можна виключати можливість виготовлення ядерного вибухового пристрою. Суттєві кількості враховують неминучі втрати матеріалу у процесі конверсії та виробництва і їх не слід плутати з критичними масами*[98] *[6].*

У презентації МАГАТЕ було слушно привернуто увагу до того факту, що досі, на щастя, відсутні приклади вчинення актів ядерного тероризму, застосування брудної бомби і, додамо, інших пристроїв для зловмисного використання радіоактивних джерел (наприклад пристроїв для прихованого опромінення населення). Але, на жаль, як з боку МАГАТЕ, так і з боку ІНТЕРПОЛу у рамках проекту «Гейгер» не помітно активних зусиль у напрямі поглибленого аналізу цього факту та усвідомлення причин, які стають на заваді планам терористів, без чого заклики до подальшого посилення заходів з протидії НО не виглядають достатньо переконливими.

Справді, якщо виготовлення ядерного вибухового пристрою терористами вважається хоча й можливим, але все ж достатньо складним технічним завданням, то про конструювання пристрою для розпорошення радіоактивності (якщо при цьому використовується звичайна вибухівка, то тоді йдеться про т.зв. брудну бомбу) цього аж ніяк не можна сказати ані з точки зору конструкції, ані з точки зору відносної доступності радіоактивних матеріалів та звичайної вибухівки для терористів.

Що стосується ядерних матеріалів, НО яких викликає найбільші занепокоєння, то загальна кількість інцидентів із високозбагаченим ураном (ВЗУ) та плутонієм, придатними для виготовлення ядерної зброї, складає лише невелику частку від усіх зареєстрованих у БД НО МАГАТЕ випадків. Представник Агентства проілюстрував ситуацію із цими матеріалами на рис. 2 і 3.

При цьому, за інформацією БД НО МАГАТЕ, **майже усі випадки інцидентів із ВЗУ, які мали місце у 2009–2010 рр., були пов'язані з виявленням ядерного матеріалу в партіях металобрухту.**

З точки зору МАГАТЕ, найбільшу занепокоєність викликають дані про наявність покупців на «чорному ринку», факти повторної участі окремих осіб у незаконній торгівлі ядерними матеріалами, а також можливість того, що перехоплені малі кількості ядерних матеріалів

---

[98] [Електронний ресурс]. – Режим доступу: http://nsspi.tamu.edu/nsep/reference-modules/technical-safeguards-terminology/safeguards-approaches,-concepts,-and-measures/significant-quantity

можуть бути лише зразками, які планувалося пред'явити потенційним покупцям для перевірки та ознайомлення з характеристиками великої партії матеріалу.

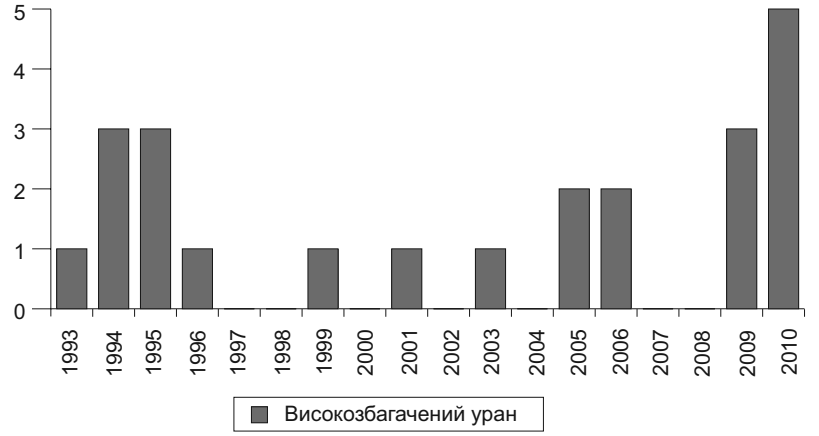

Рис. 2. Кількість інцидентів із ВЗУ

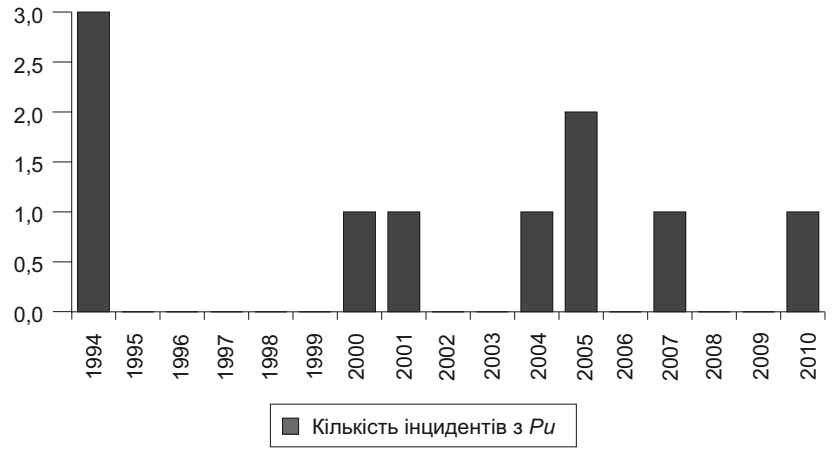

Рис. 3. Кількість інцидентів з *Pu*

Що стосується ситуації з іншими радіоактивними матеріалами, включаючи радіоактивні джерела, то тут найбільший внесок у статистику зловмисних дій дають крадіжки: 345 інцидентів (або 14 % від загальної кількості) за роки функціонування БД НО МАГАТЕ. При цьому саме для цих матеріалів (джерел) залишається суттєвою проблемою забезпечення їх захищеності під час транспортування. На кінець 2011 р. у БД НО МАГАТЕ зафіксовано 140 випадків крадіжки (40 % від загального числа злочинів цієї категорії) матеріалів у процесі їх перевезення. З точки зору попередження та припинення таких випадків заслуговує на увагу той факт, що **приблизно у 50 % інцидентів радіоактивні матеріали викрадалися при крадіжці транспортного засобу**.

Інтерес представляють також статистичні дані, що характеризують привабливість для злочинців тих чи інших джерел за їх сферою застосування. У **38 % випадків викрадалися радіоізотопні вологоміри** (широко використовуються у будівництві), у 17 % – радіографічні джерела, і у 9 % – медичні джерела. У цьому контексті здається доцільним вивчити можливість застосування альтернативних технологій, особливо у вологомірах, крадіжки яких становлять левову частку у загальній статистиці цього виду злочину стосовно радіоактивних матеріалів.

Слід також наголосити, що **МАГАТЕ серед причин, які стають на перешкоді поглибленому аналізу інформації**, що надходить до бази даних із незаконного обігу Агентства, відзначають такі проблеми: значні затримки у **процесі звітування; непослідовність застосування критеріїв при вирішенні питання щодо необхідності звітувати до БД НО МАГАТЕ.** Останнє, ймовірно, може мати безпосередній зв'язок із фактом відсутності загальновизнаних чітких критеріїв оцінки діяльності національних компетентних органів щодо протидії НО, про що вже згадувалося.

Значний інтерес з точки зору глобальних тенденцій, що спостерігаються у боротьбі проти НО, викликала презентація представників **Аргоннської національної лабораторії (АНЛ) Міністерства енергетики США**[99]. Дослідниками лабораторії було зібрано та проаналізовано великий масив історичної інформації щодо зловмисних дій із використанням радіоактивних матеріалів**.** На фактичному матеріалі, який охоплює період з 1960-х рр. по теперішній час, учені з АНЛ до-

[99] *LePoire D.* (U.S. DOE Argonne National Laboratory) Analysis of Historical Malicious Radiological Incidents Interpol Radiological and Nuclear Trafficking and Terrorism: Analysis Conference / Dave LePoire. – Umeä, Sweden, 25–26 April 2012.

слідили, тією чи іншою мірою, фактично всі аспекти зловмисних дій з радіоактивними матеріалами. Застосовані методи аналізу, включаючи математичний апарат, очевидно, заслуговують на окреме обговорення, але у даному форматі аналітичної доповіді доцільно відзначити такі висновки та результати роботи американських дослідників.

За період дослідження були зафіксовані такі типи зловмисного використання ядерних та інших радіоактивних матеріалів:

• *використання пристрою радіаційного опромінення* (англ. – *Radiological Exposure Device, RED*) з метою прихованого опромінення окремих осіб радіоактивним джерелом;

• *використання пристрою для розпорошення радіоактивності* (англ. *Radiological Dispersal Device, RDD)* з метою розпорошення радіоактивного матеріалу в довкіллі. Як уже зазначалося, коли розпорошення здійснюється шляхом підриву звичайної вибухівки, то йдеться про т.зв. брудну бомбу;

• *отруєння* (англ. – *Poisoning*) – навмисне розпорошення радіоактивного матеріалу в продуктах та рідинах із метою поглинання такого матеріалу жертвами;

• *диверсія* (англ. – *Sabotage)* – напад на ядерно- або радіаційно-небезпечний об'єкт з метою викликати викид і розпорошення радіоактивного матеріалу.

Представники АНЛ проілюстрували розподіл інцидентів, пов'язаних зі спробами застосування ядерних і радіоактивних матеріалів у кримінальних і терористичних цілях (рис. 4).

З точки зору аналізу глобальних і регіональних процесів у сфері протидії НО значну увагу привернула також доповідь **представника *FOI* Бьорна Сандстрьома** (*Björn Sandström*)[100], у якій була проаналізована статистика інцидентів з ядерними та іншими радіоактивними матеріалами за період з 2000 по 2011 рр. на території, яка потрапляє в коло, утворене радіусом у 2500 км із центром, розташованим у Швеції. Згідно з таким підходом, інциденти в Туреччині, на Північному Кавказі та на схід від Уралу (Росія) у цьому досліджені до уваги не бралися. При цьому, навіть ураховуючи складнощі, пов'язані великим масивом інформації, яку слід проаналізувати, і необхідність встановлення певних географічних рамок у такій роботі, слід усе ж відзначити, що виключення Туреччини та країн Кавказького регіону можна вважати достатньо суперечливим, ураховуючи їхнє геополітичне положення та

[100] *Sandström B.* (FOI) Illicit Trafficking of RN Materials 2000-2011. A Swedish Perspective, Interpol Radiological and Nuclear Trafficking and Terrorism: Analysis Conference / Björn Sandström. – Umeä, Sweden, 2012. – 25–26 April.

порівняно високий рівень транскордонної злочинності у цьому регіоні. Що стосується ядерних і радіоактивних матеріалів, то у роботі аналізувалися лише випадки зі збагаченими ядерними матеріалами, а радіоактивно забруднені матеріали розглядалися лише у випадку їхнього виявлення на виробничому об'єкті.

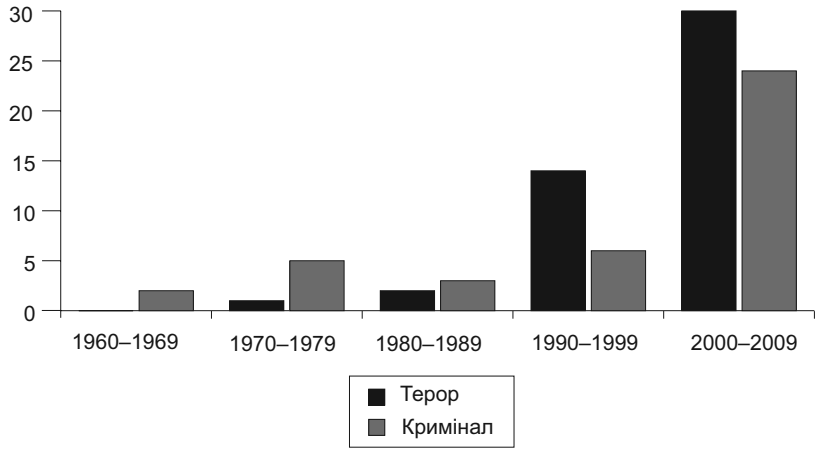

Рис. 4. Кількість інцидентів, пов'язаних зі спробами застосування ядерних і радіоактивних матеріалів у кримінальних і терористичних цілях

На рис. 5, який враховує ці обмеження, також можна побачити чітко виражений пік, який зафіксовано у 2005–2006 рр. При цьому слід відзначити, що порівняно з глобальною статистикою цей пік виявився зсунутим на один рік раніше (для всього світу цей пік припадає на 2006–2007 рр.)

Що стосується регіонального розподілу інцидентів на Європейському субконтиненті, то попри достатньо вкорінену в експертному середовищі точку зору щодо низького рівня фізичної безпеки ядерних та інших радіоактивних матеріалів на території колишніх радянських республік, загальна статистика за 2000–2011 рр. показує, що серед виділених Б. Сандстрьомом регіонів – Північний, Балтійський, Південно-Балтійський, Західна Європа, Східна Європа, **колишні радянські республіки – в останніх (без урахування прибалтійських держав) ситуація зберігалася приблизно на тому ж рівні, що й в**

інших частинах субконтиненту. Лише у період 2004–2007 рр. у республіках колишнього СРСР була зафіксована найбільша кількість інцидентів, тоді як в інші періоди показники або відповідали середньоєвропейському рівню (2000–2003 рр.), або навіть були кращими за нього (2008–2011 рр.)

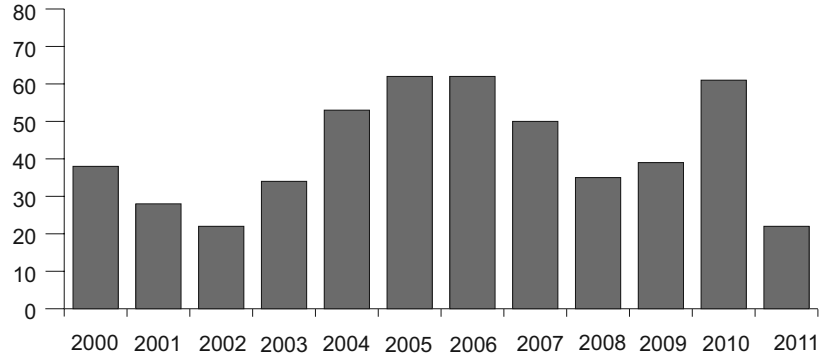

Рис. 5. Європа: загальна кількість інцидентів з ядерними та іншими радіоактивними матеріалами

При аналізі розподілу інцидентів за типами матеріалів у досліджені, проведеному *FOI*, інциденти були розподілені за такими категоріями:

• злочини (за винятком незаконного вивезення матеріалів на звалища);

• значні інциденти (з матеріалами або високої активності (більш ніж 1 *GBq*), або матеріали збройової якості, або матеріали у кілограмових кількостях);

• інциденти, пов'язані з радіоактивно забрудненим металобрухтом;

• комбінації вище зазначеного.

Що стосується інцидентів з ядерними матеріалами, то статистичні дані за період з 2000 по 2011 рр. **не свідчать про якусь явно виражену тенденцію, яка могла би стати підтвердженням того, що найбільший інтерес для терористів, які поставили собі за мету здійснити акт ядерного тероризму, представляє високозбагачений уран**. За період дослідження інцидентів з плутонієм було приблизно у 1,5 раза більше (18). Щоправда, у 2008–2011 рр. кількість інцидентів із ВЗУ дещо зросла, але (про це було сказано у доповіді представника МАГАТЕ) всі вони були пов'язані з виявленням матеріалу в металобрухті

у незначних кількостях і не були враховані у дослідженні, проведеному *FOI*, тому цей факт, очевидно, потребує додаткового аналізу.

Серед інших радіоактивних матеріалів за кількістю пов'язаних із ним значних інцидентів явним лідером залишається радіонуклід *Cs*-137 (близько 30 інцидентів проти 6 із *Co-60*, який «посідає» друге місце у цьому списку). Очевидно, що ця тенденція має глобальний характер і значною мірою зумовлена широким використанням цього радіоактивного ізотопу при вимірюванні характеристик матеріалів у будівництві та промисловості (насамперед у вологомірах), про що вже згадувалося.

Поміж зроблених Б. Сандстрьомом висновків хотілось би звернути увагу на таке:

• із загальної кількості проаналізованих інцидентів (533 за 12 років) 46 % були пов'язані з металобрухтом; 25 % – із злочинними діями; у 28 % випадків за кількістю та/або категорією матеріалів інциденти можна ідентифікувати як суттєві;

• у той час, як загальна кількість інцидентів у регіоні зросла за рахунок повідомлень про інциденти з металобрухтом, кількість інцидентів, пов'язаних зі злочинними діями у період 2008–2011 рр., зменшилася на 60 %;

• найбільше занепокоєння викликали 60 інцидентів (11 %), коли були вилучені значні кількості матеріалів та виявлені злочинні наміри.

Беручи до уваги висновки шведських експертів щодо ситуації з НО в європейському регіоні, який було ними досліджено (Європа за винятком країн Балтії та Кавказу) і до якого потрапляє Україна, а також ураховуючи попередні зауваження щодо надійності статистичних даних БД НО МАГАТЕ, на яку, як виявилося, можуть сильно впливати зміни у процедурі звітування навіть в одній країні, можна зробити висновок, що у даний період **нема вагомих підстав характеризувати ситуацію з протидією НО у колишніх радянських республіках суттєво гіршою, ніж у решті європейських країн.**

З точки зору гармонізації підходу України з підходами ЄС у сфері протидії ядерному тероризму та НО заслуговує на увагу доповідь **представника Директорату внутрішніх справ Європейської Комісії Аве Пума (***Ave Poom***)**[101]**,** присвячена напряму протидії ядерному та радіаційному тероризму у Плані дій ЄС на період з 2010 по 2015 рр.

[101] *Poom A.* (DG Home Affairs European Commission), EU CBRN Action Plan: RN workstream, Second INTERPOL Radiological and Nuclear Trafficking and Terrorism: Analysis Conference / Ave Poom. – Umeä, Sweden, 25–26 April 2012.

щодо загроз тероризму з використанням хімічних, біологічних, ядерних і радіоактивних матеріалів, період виконання якого визначено. У документі відображена прихильність ЄС до передового досвіду в розбудові систем контртерористичного захисту держав-членів на національному та міжнародному рівнях, а саме: запровадження підходу, який враховує усі види загроз (англ. – *all hazard approach*), пов'язаних з хімічними, біологічними, радіоактивними та іншими ядерними матеріалами, які можуть виникнути внаслідок техногенних аварій, стихійних лих, а також зловмисних дій, включаючи акти тероризму. Планом передбачено виконання 124 заходів за основними напрямами діяльності у цій сфері: запобігання інцидентам; виявлення відповідних матеріалів у незаконному обігу; підготовка та тренування до реагування; реагування на інциденти зі згаданими матеріалами.

У доповіді **Пола Міннебо** *(Paul Minnebo*) **(ЄВРОПОЛ)**[102] були коротко представлені підходи та процедури стратегічного звітування та обміну інформацією, запроваджені ЄВРОПОЛом у сфері протидії тероризму. З точки зору трансформування сектору безпеки в Україні та наближення до європейських стандартів взаємовідносин правоохоронних органів та спецслужб у країнах ЄС заслуговує на увагу, зокрема, той факт, що аналітичні підрозділи ЄВРОПОЛу готують різноманітні за форматом доповіді (звіти щодо протидії тероризму) з метою оцінки загрози, оцінки ситуації та трендів, визначення пріоритетів у діяльності тощо. При цьому низка звітів щорічно готується як для обмеженого доступу, так і для широкої громадськості, тобто у відкритій версії. П. Міннебо навів загальні дані за 2011 р. стосовно актів тероризму та екстремізму з використанням насильства у країнах-членах. Такі злочини в Європі здійснювалися особами та групами осіб під впливом релігійних поглядів; етно-націоналістичних і сепаратистських настроїв; лівої та анархістської ідеології; правої ідеології; ідей захисту прав тварин, довкілля тощо. Наведена доповідачем загальна статистика щодо терористичної загрози в ЄС містила такі дані за 2011 р.:

• 174 теракти в державах-членах;

• 484 осіб заарештовано за звинуваченнями, пов'язаними з тероризмом;

• 79 осіб було вбито злочинцями-одинаками у Норвегії та Німеччині;

---

[102]*Minnebo P.* (EUROPOL), Europol Strategic Reporting on Terrorism, Interpol Radiological and Nuclear Trafficking and Terrorism: Analysis Conference / Paul Minnebo. – Umeä, Sweden, 25–26 April 2012.

• 316 осіб отримали вироки за злочини, пов'язані з терористичною діяльністю.

При цьому заслуговує на увагу та аналіз інформація, надана П. Міннебо, щодо засобів, використаних терористами під час вчинення злочинів. Терористи використали:

• саморобні вибухові пристрої (етно-націоналісти та Брейвік);

• саморобні запалювальні пристрої (лівацькі та екстремістські групи);

• стрілецьку зброю (теракти під впливом релігійних поглядів).

З огляду на цю загальну інформацію про терористичну активність, яка включає дані про 174 теракти, вчинені лише у країнах ЄС, **не можна не звернути увагу на факт відсутності актів ядерного та радіаційного тероризму**.

У другій доповіді на конференції, зробленій представниками ЄВРОПОЛу **Х. Гарсія** *(J. Garcia)* **та Ф. Таверна** *(F. Taverna)*[103], йшлося про проект «Резерфорд» (*Project Rutherford*), що виконується контртерористичним підрозділом (підрозділ 04) оперативного департаменту ЄВРОПОЛу, який відповідно до свого мандата діє у чотирьох напрямах:

• боротьба з тероризмом;

• протидія незаконному обігу ядерних та інших радіоактивних матеріалів;

• боротьба із ксенофобією;

• протидія незаконному обігу стрілецької зброї, боєприпасів та вибухівки.

У межах проекту готуються звіти про ситуацію з НО у державах членах. Останній такий звіт, оприлюднений у січні ц. р., охоплює період з 2007 по 2009 рр. З-поміж основних результатів і висновків цього звіту можна виділити таке:

• не було жодного інциденту з плутонієм або ВЗУ;

• не було зареєстровано жодного інциденту з ядерними та радіоактивними матеріалам, які мали б відношення до терористичної діяльності;

• кримінальні дії відзначені лише у 10 % зафіксованих інцидентів, які головно були крадіжками матеріалів;

• інциденти некримінального характеру здебільшого стосувалися виявлення радіоактивних матеріалів портальними моніторами радіоактивності;

---

[103] *Garcia J.* (EUROPOL) Project Rutherford. INTERPOL Radiological and Nuclear Trafficking and Terrorism: Analysis Conference / J. Garcia, F. Taverna. – Umea, Sweden, 25–26 April 2012.

• незважаючи на існуючі розбіжності між державами-членами у даних щодо НО, брак надійних і точних даних про ситуацію на території ЄС, *наявна інформація не свідчить про існування значної загрози ядерного та радіаційного тероризму або про розвиток процесів у напрямі її зростання.*

При цьому представники ЄВРОПОЛу звернули увагу учасників конференції на суттєві недоліки у процедурах звітування та обміну інформацією, відсутність надійних методик аналізу даних, що заважає отримувати більш точну картину щодо НО на території ЄС.

Цікаву інформацію учасникам конференції надали представники **Австралійського центру даних з питань хімічних, біологічних, радіоактивних та ядерних матеріалів** *(The Australian Chemical, Biological, Radiological and Nuclear Data Centre, ACBRNDC*[104]), основним завданням якого є сприяння діяльності правоохоронних та інших органів у сфері забезпечення національної безпеки у спосіб надання їм технічних інформаційних продуктів та послуг для підтримки процесу прийняття рішень. Посилаючись на національну Білу книгу з питань оборони (2009 р.), австралійські експерти схильні вважати, що в найближчі десятиліття **не можна виключати нападу терористів з використанням зброї та матеріалів масового ураження. Разом з тим, на їхню думку, такий напад є менш імовірним порівняно з використанням терористами звичайної вибухівки,** яке, вочевидь, розглядається ними, як достатньо простий, випробуваний та ефективний спосіб здійснення теракту. Заслуговує на увагу правоохоронних органів і спецслужб також інший факт, наведений австралійськими експертами: у кількох не пов'язаних один з одним випадках **у таємних лабораторіях з виробництва наркотиків були виявлені радіоактивні речовини, які використовувалися як каталізатори хімічних процесів.**

Точку зору канадського регулятора з питань ядерної безпеки на конференції представив Б. Маклін *(Barry Mclean)*[105]. Слід відзначити, що тенденції щодо незаконного обігу ядерних та інших радіоактивних матеріалів, а також ядерних технологій, які спостерігаються в Канаді, в основному співпрадають із глобальними процесами. Зокрема із загальної кількості крадіжок (21), що мали місце в країні,

---

[104] *Abbondante S.* (Australian CBRN Data Centre), Australian and South-East Asia CBRN Incidents and Threats, INTERPOL Radiological and Nuclear Trafficking and Terrorism: Analysis Conference / Serena Abbondante, Alan Devlin. – Umea, Sweden, 25–26 April 2012.

[105] *Mclean B.* (Canadian Nuclear Safety Commission), Trafficking and Incident Trends in Canada, INTERPOL Radiological and Nuclear Trafficking and Terrorism: Analysis Conference / Barry Mclean. – Umea, Sweden, 25–26 April 2012.

починаючи з грудня 2007 р., жодна не мала відношення до ядерних матеріалів I та II категорії (найбільш чутливих з точки зору нерозповсюдження ядерної зброї та ядерного тероризму). Серед радіоактивних джерел і матеріалів у 65 % крадіжок ідеться про радіоізотопні вимірювальні прилади (вологоміри та густиноміри), причому, як повідомив Б. Маклін, **здебільшого метою викрадення злочинців були не радіоактивні матеріали, а транспортні засоби**, на яких вони перевозилися.

Достатньо цікавою була інформація представника канадського ядерного регулятора щодо **першого у країні судового вироку за порушення низки законів, включаючи закон про (експлуатаційну) ядерну безпеку та контроль над нею** *(Nuclear Safety and Control Act),* який було винесено у липні 2010 р. канадському громадянину іранського походження Махмуду Ядегарі *(Mahmoud Yadegari)*. Він намагався відправити до Ірану через підставні компанії виготовлені в США перетворювачі тиску (*pressure transducers*), що можуть бути використані у газових центрифугах для збагачення урану. М. Ядегарі було засуджено до позбавлення волі на 4 роки і 3 місяці. Крім того, значний інтерес викликала та частина доповіді Б. Макліна, в якій було коротко представлено процеси оцінки загроз у ядерній сфері.

В Канаді здійснюється аналіз проектної загрози (*Design Basis Threat Analysis*), за основу якого взята оцінка загроз національній безпеці. При цьому беруться до уваги загрози, типові для певного покоління АЕС в усьому світі, включаючи тероризм, екстремізм, кіберзагрози, а також загрози внутрішнього порушника. **Оцінки загроз конкретним установкам і ризиків виконуються щорічно** і розглядаються та затверджуються Комісією з (експлуатаційної) ядерної безпеки Канади (*Canadian Nuclear Safety Commission)*. **Відповідно до поточної оцінки рівень загрози радіоактивним матеріалам у Канаді визнано як низький**. Це достатньо нетривіальний результат, якщо врахувати високий рівень терористичних загроз у сусідніх Сполучених Штатах та відносну прозорість кордону між Канадою та США, щонайменше для громадян цих держав.

Британські дослідники з Науково-технічної лабораторії Міністерства оборони Великої Британії Лоуренс Джонс *(Laurence Jones)* **та Крістофер Хеммонд** *(Christopher Hammond)*[106] зробили достатньо цікаву доповідь про аналітичний інструментарій, який вони пропонують

[106] *Jones L.* (UK DSTL), Analysis of Red CBRN Capability (ARCC) Radiological Vignette Tool, INTERPOL Radiological and Nuclear Trafficking and Terrorism: Analysis Conference / Laurence Jones, Christopher Hammond. – Umea, Sweden, 25–26 April 2012.

використовувати для оцінки можливих сценаріїв застосування хімічних, біологічних, радіоактивних і ядерних матеріалів проти підрозділів Міністерства оборони Великої Британії у різних куточках світу, використовуючи моделювання на основі т.зв. методики він'єток (*англ. – vignettes*).

На завершення конференції відбулося обговорення проекту її підсумкового документа. При цьому стосовно як першої, так і наступної версій документа виник ряд запитань з точки зору основної мети заходу. В огляді зроблених доповідей уже були поставлені деякі запитання у цьому контексті. Далі ці запитання та зауваження зведені в єдиний перелік, у т.ч. у зв'язку з текстом підсумкового документа конференції.

Після терактів 11 вересня 2001 р. у світі на найвищому рівні неодноразово висловлювалися оцінки про велику ймовірність і навіть неминучість вчинення терористами актів ядерного та радіаційного тероризму[107]. Якщо відсутність актів ядерного тероризму можна пояснити, враховуючи глобальні зусилля, спрямовані на убезпечення вразливих ядерних матеріалів і ядерних установок, а також те, що виготовлення ядерної бомби терористами, хоча й можливе, але все ж є достатньо складним технічним завданням, то відсутність актів радіаційного тероризму, зокрема застосування терористами т.зв. брудної бомби при все ще великій кількості випадків втрати, пропажі та викрадень радіоактивних матеріалів потребує усвідомлення та поглибленого аналізу з тим, щоб подальші зусилля у цьому напрямі були осмисленими, базувалися на аналізі реальних мотивів, можливостей і цілей терористів і мали адекватне фінансування.

Запитання: *Чому прогнози та оцінки аналітиків не справдилися і чому відсутність прецедентів використання терористами ядерних і, особливо, інших радіоактивних матеріалів не піддається ґрунтовному аналізу? Чому статистика інцидентів з високозбагаченим ураном і плутонієм не підтверджує широко розповсюджену експертну точку зору про привабливість ВЗУ для терористів?*

Усі учасники конференції відзначали важливість надійних даних для аналізу поточної ситуації та тенденцій щодо НО як на національному, так і на міжнародному рівнях, але досі значна частина інформації надається у змішаному вигляді, оскільки домінує підхід, згідно з

[107] *Allison G.* Nuclear Terrorism: The Ultimate Preventable Catastrophe / Graham Allison, Joanne J. Myers. – New York : Times Books, 2004; *Mowatt-Larssen R.* Islam and the Bomb: Religious Justification For and Against Nuclear Weapons / Rolf Mowatt-Larssen. – Cambridge, Mass.: Harvard Kennedy School. – Jan. 2011. – P. 9, або CIA Chief: Al-Qaida Is Top Nuclear Concern. – Associated Press, 2008. – September 16.

яким до НО відносять усі випадки перебування ядерних та інших радіоактивних матеріалів поза межами регулювального контролю. Зрозуміло, що загальна інформація про стан регулювального контролю, можливості виявлення не тільки незаконного, а й несанкціонованого переміщення матеріалів є корисною у процесі аналізу злочинів щодо ядерних та інших радіоактивних матеріалів, але, враховуючи, що левова частка інцидентів, що реєструються, пов'язана з виявленням радіоактивно забрудненого металобрухту, такий підхід часто приховує масштаби та реальну статистику інцидентів, які можуть мати безпосереднє відношення до тероризму.

Запитання: *Чому досі у багатьох випадках стан справ у сфері НО подається через загальну статистику інцидентів, без виокремлення саме випадків незаконної діяльності по відношенню до ядерних та інших радіоактивних матеріалів?*

Створення та обслуговування бази даних щодо НО можна вважати корисним, якщо зібрані в ній дані та інша інформація активно використовуються для досліджень та аналізу з метою вжиття практичних заходів для зниження ризиків, пов'язаних із зловмисними діями. На жаль, нині БД НО МАГАТЕ, попри всю її унікальність, не повною мірою відіграє таку роль, щонайменше для всіх держав-учасниць, оскільки здебільшого займається фіксацією даних, які надходять у процесі звітування від національних пунктів зв'язку. Процес звітування та обробки інформації бази даних теж, очевидно, потребує удосконалення, оскільки, як виявилося (2006–2007 рр.) на нього можуть суттєво впливати зміни у процедурі звітування навіть однієї держави-учасниці.

Запитання: *Як сталося так, що зміни у процедурі звітування в одній державі призвели до формування піку в глобальній статистиці інцидентів, пов'язаних з НО? Чому цей пік так і залишився на діаграмах, представлених Офісом БД НО МАГАТЕ, якщо процедурні зміни в тій країні, за інформацією МАГАТЕ, були в подальшому скасовані?*

На поставлені запитання, як здається, хоча б частково можна знайти відповідь у роботі відомого американського експерта у сфері безпеки Роджера Джонстона (*Roger G. Johnston*)[108]. Зокрема він звертає увагу на ірраціональну тенденцію до циклічності коливань у фінансуванні заходів із фізичної безпеки (англ. – *security*). Р. Джонстон вважає, що у цій сфері «типовою є ситуація, коли бюджети, що виділяються

[108] *Johnston Roger G.* Effective Vulnerability Assessments for Physical Security Devices, Systems, and Programs, ÖMZ / Roger G. Johnston // Austrian Military Periodical, Nuclear Material Protection, Special Edition, 2003. – P. 51–55.

на цілі фізичної безпеки, з часом скорочуються, причому цей процес триває доти, поки не трапляється серйозний інцидент, пов'язаний із фізичною безпекою. А коли такий інцидент трапляється, то проявляється інша тенденція – виникнення істерії стосовно питань фізичної безпеки. Величезні ресурси одразу ж виділяються на розв'язання відповідної проблеми, значна частина яких врешті-решт витрачається бездумно. Застосовуються драконівські й часто безглузді заходи, деякі з котрих можуть навіть знизити загальний рівень фізичної безпеки, або, щонайменше, відвернути увагу від пошуку більш ефективних заходів. Коли пов'язана з фізичною безпекою криза завершується, увага до неї зазвичай починає спадати аж до наступного серйозного інциденту, який викликає інший сплеск шаленого фінансування та активності».

Якщо поглянути на доповіді та документи згаданої конференції ІНТЕРПОЛу з цієї точки зору, то є деяк і підстави вважати, що на оцінку загроз ядерного та радіаційного тероризму та ризиків, пов'язаних з НО, може впливати процес, описаний Р. Джонстоном.

ЗАКЛЮЧНІ МІРКУВАННЯ ТА ДЕЯКІ ВИСНОВКИ

Друга конференція ІНТЕРПОЛу стала значною подією з точки зору аналізу ситуації та визначення тенденцій щодо незаконного обігу ядерних та інших радіоактивних матеріалів, а також пов'язаних із цими матеріалами видів тероризму, а саме ядерного та радіаційного. Участь представників країн, які дійсно переймаються цією проблематикою і вельми занепокоєні можливими наслідками незаконного переміщення ядерних та інших радіоактивних матеріалів, є, безперечно, корисною і не останньою чергою тому, що дає змогу детальніше відслідковувати процеси у цій сфері, реально уявляти весь комплекс проблем, пов'язаних із протидією загрозам ядерного та радіаційного тероризму, незаконного обігу ядерних та інших радіоактивних матеріалів.

При цьому аналіз доповідей та підсумкових документів таких заходів дає змогу визначати і суперечливі моменти, присутні у роботі експертів, представників міжнародних організацій та національних компетентних органів, що можуть бути, серед іншого, наслідками зацікавленості певних кіл та окремих інституцій у збереженні статускво, тенденції надавати перевагу прогнозам та оцінкам з урахуванням передусім найгірших можливих сценаріїв з метою, наприклад, зберег-

ти рівень фінансування певних проектів, програм і організацій в умовах глобальної фінансової кризи.

Варто наголосити, що наведені міркування жодним чином не мають на меті применшити загрози ядерного та радіаційного тероризму, а також пов'язані з ними ризики незаконного обігу ядерних та інших радіоактивних матеріалів. Ці загрози і ризики потребують адекватної відповіді, отриманої в т.ч. завдяки аналізу дійсних мотивів і дійсних можливостей терористів, а також реальної ситуації, що складається у результаті заходів, які вживаються.

На думку Браєна Дженкінса (*Brian Michael Jenkins*), відомого американського експерта з питань ядерного тероризму, старшого консультанта президента Корпорації РЕНД (*RAND Corporation)*, акцентування уваги людей на проблемі ядерного тероризму може сприяти формуванню ентузіазму у тих, хто є безпосередніми учасниками контртерористичних заходів, а також допомогти в отриманні фінансування від Конгресу США на відповідні проекти і програми. Водночас він же звертає увагу на те, що, перебільшуючи загрозу, спецслужби поширюють серед населення страхи перед ядерним терором і в цьому аспекті фактично грають на руку Аль-Каїді, зробивши з неї терористичну організацію, яка за відсутності інформації про наявність у неї відповідних ядерних можливостей фактично піднялася на рівень віртуальної ядерної держави[109].

Взагалі, із цими твердженнями відомого американського експерта важко не погодитися, але з одним зауваженням стосовно роботи аналітиків. Справді, за самою природою своєї діяльності вони не можуть дозволити собі тривалий час перебувати під впливом поглядів, зумовлених політичною доцільністю, інакше цінність результатів їх роботи буде доволі сумнівна, а виконання заходів, які ґрунтуються на результатах такого аналізу, перебуватиме у зоні значних ризиків.

[109] *The long* shadow of 9/11 : America's response to terrorism / Brian Michael Jenkins, John Paul Godges (ed.)/, RAND Corporation. – 2011.

ЗМІСТ

Наукове видання

ПРОТИДІЯ ТЕРОРИЗМУ, НЕРОЗПОВСЮДЖЕННЯ ЗБРОЇ ТА МАТЕРІАЛІВ МАСОВОГО ЗНИЩЕННЯ Й ЗАХИСТ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Збірник матеріалів засідань Міжвідомчої експертної робочої групи, створеної при НІСД

Літературний редактор: *М. Л. Рубанець*
Коректор: *М. Л. Рубанець*
Комп'ютерне верстання: *Є. Ю. Стрижеус*

Відповідальний за випуск: *В. М. Сизонтов*

Оригінал-макет підготовлено
в Національному інституті стратегічних досліджень:
вул. Пирогова, 7-а, Київ-30, 01030
Тел/факс: (044) 234-50-07
e-mail: info-niss@niss.gov.ua

Формат 60x84/16. Ум. друк. арк. 6,1.
Тираж 200 пр. Зам. №

Віддруковано ПП «Вид-во «ФЕНІКС»
вул. Шутова, 13-Б, м. Київ, 03680
Свідоцтво суб'єкта видавничої справи ДК № 271 від 07.12.2000

ДЛЯ НОТАТОК

ДЛЯ НОТАТОК