ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ ВЗАЄМОДІЇ ПРИ РЕАГУВАННІ НА ІНЦИДЕНТИ ТА КРИЗИ КОМПЛЕКСНОГО ХАРАКТЕРУ НА ОБ`ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Анотація

У чинній Стратегії національної безпеки України до загроз безпеці критичної інфраструктури віднесені «неефективне управління безпекою критичної інфраструктури» та «недостатній рівень захищеності критичної інфраструктури від терористичних посягань і диверсій». В аналітичній записці проаналізовані проблеми забезпечення взаємодії державних систем безпеки та кризового реагування у випадках інцидентів та криз комплексного характеру, пов’язаних з критичною інфраструктурою. На основі проведеного аналізу зроблено висновок, що існуючі державні (національні) системи безпеки та кризового реагування в Україні у теперішньому своєму стані не забезпечують рівня взаємодії та обміну інформацією між суб’єктами захисту критичної інфраструктури, якого вимагають сучасні безпекові умови. У зв’язку з цим запропоновано ряд рекомендацій для сприяння забезпеченню взаємодії систем безпеки та кризового реагування у рамках державної системи захисту критичної інфраструктури в Україні, створення якої передбачено відповідним рішенням РНБО України, введеним у дію Указом Президента України №8/2017 від 16 січня 2017 року.

ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ ВЗАЄМОДІЇ ПРИ РЕАГУВАННІ НА ІНЦИДЕНТИ ТА КРИЗИ КОМПЛЕКСНОГО ХАРАКТЕРУ НА ОБ`ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Вступ

В стратегії національної безпеки України до загроз безпеці критичної інфраструктури (КІ) віднесені, зокрема, неефективне управління безпекою КІ та недостатній рівень її захищеності від терористичних посягань і диверсій. Нижче представлений аналіз планів, процедур і механізмів координації дій, взаємодії та обміну інформацією (КДВОІ) між державними системами безпеки та кризового реагування з точки зору відповідних положень *Стратегії національної безпеки України.*

Останніми роками у багатьох країнах світу, включаючи Україну, спостерігається зростання загроз тероризму, екстремізму та сепаратизму, постійно збільшується кількість надзвичайних ситуацій техногенного та природного характеру, все більше різноманітних державних установ, компаній, підприємств стають мішенями для кібератак, – і все це відбувається на тлі процесів подальшого ускладнення і розгалуження взаємозв'язків і взаємовпливів при забезпеченні життєдіяльності сучасної держави, її національної безпеки і оборони. Вплив усіх цих чинників значно підвищує уразливість об'єктів і систем, життєво-важливих для забезпечення повсякденного функціонування кожної сучасної держави.

У розвинутих країнах світу, насамперед у країнах-членах НАТО та ЄС, одним із інструментів адекватного реагування на цей безпековий виклик стало запровадження та постійне удосконалення державних систем, спеціально призначених для забезпечення *захисту* (*безпеки*) та *стійкості* КІ[1].

[1] При наявності загальновизнаних підходів до захисту КІ внаслідок національних особливостей застосування термінів *безпека, захист* та *стійкість у* національних законодавствах можуть дещо відрізнятися від країни до країни.

При цьому загальновизнаним є підхід, коли до *національної критичної інфраструктури* або просто *критичної інфраструктури* відносять різноманітні об'єкти, системи і мережі (фізичні та віртуальні), відібрані за основним критерієм – ***надзвичайної важливості для безпечного та сталого повсякденного життя країни***. Тобто таких, знищення або вихід з ладу (повний або частковий) яких може призвести до швидких важких наслідків для населення, суспільства і держави в цілому. Захист саме таких об'єктів має бути забезпечений у першу чергу.

Разом з тим ресурси будь-якої держави є обмеженими, і тому до КІ відносять лише невелику частину усіх інфраструктурних об'єктів, а саме — лише ті, безпекові інциденти на яких можуть спричинити кризову ситуацію національного рівня, завдяки тому, що її негативний вплив при неналежному реагуванні може швидко розповсюдитися далеко за межі того чи іншого сектору економіки та/або безпеки держави.

Масштаб і комплексний характер загроз та наслідків криз, пов'язаних з безпекою КІ, необхідність її захисту від усіх видів фізичних та кіберзагроз, вимагають якісно нового рівня КДВОІ між численними суб'єктами процесу реагування[2]. Зрозуміло, що у випадку реалізації загроз комплексного характеру вимоги до процедур КДВОІ мають бути найжорсткішими.

Актуальність удосконалення процедур і механізмів реагування на комплексні загрози підкреслює і такий «свіжий» факт: у комюніке, яке на початку червня було ухвалене главами держав G7 на саміті у Канаді, зазначено, що «***загрози глобальній безпеці, з якими ми зіштовхуємося, є комплексними і такими, що еволюціонують***, і ми повинні працювати разом для протидії тероризму»[3]. Активну позицію щодо реагування на комплексні

[2] У даному контексті поняття «реагування» включає забезпечення готовності до реагування, безпосередньо дії відповідних суб'єктів процесу під час реагування на інцидент або кризу, пов'язану з безпекою об'єкта КІ, а також ліквідацію та/або пом'якшення наслідків кризи.

[3] [Електронний ресурс]. – Режим доступу: THE CHARLEVOIX G7 SUMMIT COMMUNIQUE https://g7.gc.ca/en/official-documents/charlevoix-g7-summit-communique/

загрози займають НАТО і ЄС, які, наприклад, останнім часом приділяють особливу увагу ХБРЯ-загрозам[4].

Передовий зарубіжний досвід і найкращі практики у цій сфері показують, що задовольнити вимоги до КДВОІ можливо лише на системній основі, тобто у рамках єдиної державної/національної системи захисту КІ.

Натомість, в Україні готовність до реагування на комплексні загрози та ризики до цього часу має забезпечуватися за умов наявності цілої низки державних/національних систем безпеки та кризового реагування, за функціонування яких несуть відповідальність окремі державні органи, що створює умови для ***домінування відомчих підходів, під впливом яких уповноважені державні органи проявляють схильність опікуватися лише певним набором загроз та ризиків.***

Ще однією характерною рисою теперішнього стану речей у цій сфері є те, що в Україні об'єкти, системи і мережі, які у розвинутих країнах відносять до КІ, «розпорошені» по більш ніж 10 різноманітних переліках і списках об'єктів, включаючи «*особливо важливі*»; «*важливі*»; такі, які підлягають «*охороні та обороні*» або «*обов'язковій охороні*»; «*об'єкти підвищеної небезпеки*», «*радіаційно-небезпечні об'єкти*» тощо.

Така ситуація неминуче створює міжвідомчі бар'єри для опрацювання питань, що лежать поза межами конкретних систем, і це, зокрема, перешкоджає урахуванню загроз та ризиків, реалізація яких може викликати так звані ***каскадні ефекти,*** тобто випадки, коли надзвичайні та кризові ситуації, які можуть мати місце в одній галузі (одному секторі КІ) спричиняють швидкий негативний вплив на інші галузі, сектори і сегменти національної економіки, національної безпеки та оборони.

При тому, що необхідність КДВОІ на національному рівні у тому чи іншому вигляді формально визнається у всіх установчих документах щодо функціонування існуючих систем, а також деяких планів взаємодії,

[4] Загрози, пов'язані з хімічними, біологічними, радіоактивними та ядерними матеріалами.

поглиблений аналіз зазначених документів показує, що здебільшого визначені ними процедури та механізми носять здебільшого декларативний характер і важко піддаються перевірці. Опосередкованим підтвердженням цього є той факт, що до осені 2017 року плани взаємодії суб'єктів систем безпеки і кризового реагування перевірялися у ході навчань або тренувань виключно тактичного (об'єктового) рівня[5].

Дійсно, проведенню навчань не може сприяти те, що ***кожна з систем використовує «власну» термінологію***, не узгоджену з іншими системами; що ***для визначення (оцінки) рівнів загроз та ризиків,*** якими опікується кожна з них, ***використовуються різні підходи, а критеріям встановлення режимів функціонування однієї системи важко, а іноді й неможливо, поставити у відповідність критерії іншої системи.*** Далі ці твердження будуть проілюстровані конкретними прикладами.

Нижче коротко проаналізовано теперішній стан захисту об'єктів, систем і мереж, які мають бути віднесені до КІ в Україні, та обґрунтовується необхідність у суттєвому прискоренні виконання у повному обсязі Указу Президента України, яким було введено в дію рішення РНБОУ щодо створення державної системи захисту критичної інфраструктури (ДСЗКІ).

Запровадження концепції захисту КІ вимагає подолання вузьковідомчих підходів

Як згадувалося вище, розвинуті країни світу реалізують свою політику в сфері захисту КІ через створення єдиних державних/національних систем, призначених забезпечувати ефективне реагування ***на усі види фізичних загроз та кіберзагроз, а також на їх можливі комбінації***. При цьому держава визначає або створює спеціальний державний орган[6], який координує діяльність, сприяє взаємодії та обміну інформацією усіх суб'єктів

[5] Лише у 2017 році за сприяння західних країн-партнерів вперше в історії незалежної України були проведені командно-штабні навчання національного рівня, які стосувалися відпрацювання взаємодії державних органів та інших організацій у випадках радіоактивного забруднення (вересень), а також реалізації загроз критичній енергетичній інфраструктурі (жовтень).

[6] У деяких країнах така відповідальність розподіляється між кількома державними органами.

захисту КІ.

В Україні завдяки спільним зусиллям ряду представників державних органів, наукового та експертного співтовариств та за активної технічної та консультативної підтримки з боку відповідних структур НАТО було забезпечене належне інформування вищого політичного керівництва держави щодо актуальності проблематики захисту КІ, внаслідок чого наприкінці 2016 – на початку 2017 років були прийняті важливі для цього безпекового напряму документи.

Головною подією слід вважати те, що Указом Президента України №8/2017 від 16 січня 2017 року було введено в дію рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «*Про удосконалення заходів забезпечення захисту об'єктів критичної інфраструктури*». На виконання Указу Президента Кабінетом міністрів України за участі Національного інституту стратегічних досліджень було розроблено «*Концепцію створення державної системи захисту критичної інфраструктури*» і розпочато роботу над законопроектом «*Про критичну інфраструктуру та її захист*»[7].

Відповідно до президентського указу зазначений законопроект мав би бути переданий на розгляд Верховної Ради України ще у травні минулого року, але доводиться констатувати, що робота над ним суттєво затримується. Розгляд зауважень та пропозицій, отриманих при підготовці перших варіантів законопроекту, показує що до причин гальмування виконання рішення РНБО та Указу Президента можна віднести вплив суто відомчих поглядів на можливі шляхи розв'язання проблем, які мають загальнонаціональний вимір.

Це відображається, наприклад, у недооцінці або ігноруванні найкращого зарубіжного досвіду при визначенні видів загроз та ризиків, для зменшення

[7] На сайті Мінекономрозвитку опубліковано для обговорення текст проекту Закону України «Про критичну інфраструктуру та її захист» [Електронний ресурс]. – Режим доступу: http://www.me.gov.ua/Documents/Detail?lang=uk-UA&id=f6481532-9ec0-4ca5-9832-dcc32e31da3c&title=ProektZakonuUkrainiproKritichnuInfrastrukturuTaYiiZakhist

та протидії яким державна система захисту КІ має бути створена, хоча це питання має фундаментальне значення[8] для усього процесу розбудови системи.

Ще одним із проявів впливу відомчих інтересів можна вважати те, що у низки державних органів сформувалося дуже насторожене відношення до змін, які мають бути внесені у функціонування існуючих систем у зв'язку зі створенням ДСЗКІ, у зв'язку з чим вони намагаються «мінімізувати» наслідки такого кроку для конкретного відомства та відповідної державної системи.

Саме таким чином можна інтерпретувати ряд відповідей відомств, які отримав НІСД у рамках проведеного опитування з цієї проблематики. В них, по суті, стверджується, що основні питання КДВОІ у випадку реалізації комплексних загроз ***або врегульовані чинною нормативно-правовою базою, або не передбачені нею***, і тому, не потребують якихось додаткових зусиль.

Дійсно, наприклад, Держатомрегулювання, загалом підтримуючи ідею створення ДСЗКІ, разом з тим вважає, що включення ДСФЗ[9] до складу ДСЗКІ є нераціональним і недоцільним, оскільки це може «*негативно вплинути на стан ДСФЗ та призвести до її дисбалансу*».

Натомість, ДСНС у своїй відповіді звертає увагу на те, що відомство діє «*лише на підставі, в межах повноважень та у спосіб, що передбачені Конституцією та законами України*», а відповіді на поставлені НІСД питання «*відображені у Кодексі цивільного захисту та відповідних підзаконних актах*».

Аналогічну позицію займає Антитерористичний центр (АТЦ) при Службі

[8] Наприклад, в нормативно-правовій базі США, а саме у *Плані захисту національної інфраструктури США 2013* (*National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilien*ce). [Електронний ресурс]. – Режим доступу: https://www.dhs.gov/publication/nipp-2013-partnering-critical-infrastructure-security-and-resilience та у *Політичній директиві президента 21 Presidential Policy Directive / PPD-21 Critical Infrastructure Security and Resilience.* [Електронний ресурс]. – Режим доступу: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil чітко зазначено, що КІ має бути захищена від ***«фізичних та кібер-загроз».*** При цьому до перших віднесені загрози природного і техногенного походження, а також загрози зловмисних дій (тероризм, злочинність тощо).

[9] Державна система фізичного захисту – система, яка забезпечує захист ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання.

безпеки України, який у своєму листі звертає увагу на відсутність понять «*критична інфраструктура*»[10], «*державна система*» *її захисту* тощо в національному законодавстві. У відповіді АТЦ також зазначено, що «*механізми взаємодії, координації дій та заходи реагування суб'єктів боротьби з тероризмом, залежно від встановлених в державі рівнів терористичних загроз, визначені Положенням про єдину державну систему запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків*»[11].

І лише стосовно кібербезпеки, ми маємо іншу картину, яка відображає суттєвий прогрес, якого Україна досягла на цьому безпековому напрямі: в Україні вже закладені організаційно-правові основи забезпечення кіберзахисту держави. Зокрема, стосовно процедур КДВОІ Державний центр кіберзахисту та протидії кіберзагрозам Держспецзв'язку повідомив, що ним розроблено і передано на погодження проект *Протоколу спільних дій основних суб'єктів кіберзахисту та власників (розпорядників) об'єктів критичної інформаційної інфраструктури під час попередження, виявлення, припинення кібератак, а також при усуненні їх наслідків*.

З іншого боку, слід визнати, що насторожене відношення до реформування, яке проявляють відомства, відповідальні за функціонування державних/національних систем безпеки та кризового реагування, не можна вважати повністю безпідставним. Було б неправильно ігнорувати ризики, пов'язані із нанесенням шкоди існуючим в Україні системам у разі механічного і бездумного перенесення зарубіжного досвіду на українські терени, без урахування національної специфіки і теперішньої безпекової ситуації навколо України.

Усвідомлюючи певну обґрунтованість занепокоєнь, разом з тим слід звернути увагу згаданих відомств на те, що підхід, запропонований у

[10] У відповіді АТЦ при СБУ не враховано того факту, що термін «критична інфраструктура» вже визначено у постанові КМУ (див. посилання 10).

[11] Затверджене постановою Кабінету міністрів України №92 від 18.02.2016 «Про затвердження Положення про єдину державну систему запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків». [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/92-2016-%D0%BF .

схваленій Кабінетом міністрів України *Концепції створення державної системи захисту критичної інфраструктури в Україні,* полягає у ***максимальному використанні існуючих систем безпеки та кризового реагування*** і має на меті оптимальне використання наявних в державі можливостей і ресурсів та забезпечує достатні передумови для запобігання можливим негативним наслідкам створення ДСЗКІ.

Нарешті, аналіз поточної ситуації щодо захисту об'єктів, що мають бути віднесені до КІ, показує, що ***відомчі оцінки стосовно достатньої урегульованості процедур і механізмів КДВОІ між системами у чинній нормативно-правовій базі не зовсім відповідають дійсному стану речей***, і це особливо яскраво проявляється у випадках ситуацій, пов'язаних з проблематикою реагування на реалізацію комплексних загроз. У наступних розділах представлене обґрунтування цього висновку.

Чи здатні існуючі національні/державні системи безпеки та кризового реагування ефективно взаємодіяти?

У розвинутих країнах світу ефективна взаємодія систем реагування на загрози, небезпеки і ризики є важливим елементом забезпечення національної безпеки. Це можна проілюструвати зокрема тим, що у США для характеристики здатності систем взаємодіяти широко використовується спеціальний термін «***interoperability»***[12], а забезпечення оптимальної здатності систем, персоналу та обладнання отримувати та надавати: функціональну підтримку, дані, інформацію та послуги визначено як найбільш важлива вимога для Міністерства внутрішньої безпеки США при реагуванні на інциденти. Натомість, у законодавстві України щодо національної безпеки такий або аналогічний за змістом терміни відсутні.

Більш конкретно розглянемо проблеми міжсистемної взаємодії на прикладі таких державних/національних систем:

[12] Див. публікацію Міністерства внутрішньої безпеки США: DHS Lexicon Terms and Definitions. October 2017. [Електронний ресурс]. – Режим доступу: https://www.dhs.gov/sites/default/files/publications/18_0116_MGMT_DHS-Lexicon.pdf

- *Єдиної державної системи цивільного захисту* (далі – ЄДСЦЗ)[13];
- *Єдиної системи запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків* (далі – ЄСЗРПТА)[14];
- *Державної системи фізичного захисту* (далі – ДСФЗ)[15].

Урегульованість планів, процедур і механізмів координації дій, взаємодії та обміну інформацією, очевидно передбачає узгодженість основних параметрів функціонування відповідних систем. У таблиці, представленій нижче, наведена інформація про функціонування обраних систем в різних безпекових умовах.

Параметри функціонування деяких систем безпеки та кризового реагування

Таблиця 1

ЄДСЦЗ ***режими*** функціонування	**ДСФЗ** ***умови*** функціонування	**ЄСЗРПТА** ***рівні*** терористичних загроз
режим повсякденного функціонування	нормальне функціонування	**сірий** (можлива загроза) за наявності факторів (умов), що сприяють вчиненню терористичного акту
підвищена готовність	підвищена готовність	**синій** (потенційна загроза) за наявності інформації, що потребує підтвердження, про підготовку до вчинення терористичного акту
надзвичайна ситуація	функціонування у кризовій ситуації	**жовтий** (імовірна загроза) за наявності достовірної (підтвердженої) інформації про підготовку до вчинення терористичного акту
надзвичайний стан	відновлення нормального функціонування	**червоний** (реальна загроза) у разі вчинення терористичного акту

[13] Положення затверджене постановою КМУ від 09.01.2014 р. № 11.
[14] Див. посилання 11.
[15] Порядок функціонування затверджений постановою КМУ від 21.12.2011 р. №1337.

При розгляді представленої таблиці звертає на себе увагу, зокрема, таке:

1. Положення про внесені у таблицю системи використовують різні терміни для опису функціонування у різних умовах, а саме – «*режими*», «*умови*» та «*рівні*».

2. Фактично, про майже повний збіг можна говорити лише для двох перших *режимів/умов* для ЄДСЦЗ та ДСФЗ, які, при цьому, можна вважати найпростішими з точки зору планування і організації діяльності та забезпечення готовності до них[16].

3. Для ЄСЗРПТА, на відміну від двох інших систем, відсутній режим, який можна було б поставити у відповідність режимам «*повсякденного*» або «*нормального*» функціонування.

4. З ускладненням режимів невідповідності критеріїв їх запровадження можуть суттєво збільшуватися (це твердження пояснюється нижче на прикладі).

Розглянемо, як мали б функціонувати згадані вище системи у випадку конкретної загрози.

Приклад 1. ***Гіпотетичний випадок надходження підтвердженої інформації про загрозу теракту на одній з українських АЕС.*** У такому випадку настання серйозних наслідків для життя і здоров'я населення, окремих осіб можливе не тільки в результаті застосування терористами стрілецької зброї та вибухівки, але й в результаті пошкодження технологічного обладнання на реакторних та інших небезпечних технологічних установках, тобто з точки зору ядерної, радіаційної, техногенної та екологічної безпеки, впливу на соціально-політичну ситуацію в країні.

[16] Саме тому, що в таблиці для переважної більшості режимів (умов, рівнів) однієї системи не можливо знайти однозначну відповідність режимів (умов, рівнів) інших систем, рядки у таблиці, що відповідають певним станам окремих систем, зміщені один по відношенню до іншого.

При цьому, відповідно до положень про внесені до таблиці системи, при отриманні вказаної інформації вони мали б функціонувати таким чином:

ДСФЗ – функціонування у кризовій ситуації[17];

ЄДСЦЗ – у режимі повсякденного функціонування[18];

ЄСЗРПТА – у режимі, що відповідає передостанньому «*жовтому рівню*» шкали терористичної загрози[19].

З упевненістю можна припускати, що в реальному житті ЄДСЦЗ не залишилася би поза процесом реагування на таку комплексну загрозу, але при цьому неузгодженості могли би призвести до зайвих витрат часу, ресурсів, неминучих збоїв та плутанини в діях, у т.ч. щодо розподілу (передачі) відповідальності на різних етапах реагування, що, у свою чергу, в результаті, могло б стати причиною важких наслідків, включаючи втрати людських життів.

Цей приклад досить переконливо ілюструє те, що національна нормативно-правова база в її теперішньому вигляді не може бути надійною основою для розробки і реалізації планів і процедур КДВОІ існуючих в Україні систем кризового реагування та безпеки.

Дійсно, розробка дієвих планів і процедур КДВОІ потребує, щонайменше, прийняття спільної термінології, визначення співвідношень між режимами, рівнями та умовами функціонування систем, узгодження принципів управління комплексною кризою, яка пов’язана з дією кількох небезпечних факторів (у розглянутому випадку це тероризм і радіація) тощо.

Запровадження загальних підходів, термінології, процедур і форматів КДВОІ на національному рівні має бути враховане при розробці та коригуванні документів оперативного і тактичного рівнів.

---

[17] По суті, це - стан найвищої готовності системи, адже наступний за шкалою режим – «режим відновлення нормального функціонування»

[18] Положення про ЄДСЦЗ стосовно терористичних загроз передбачає її реагування лише у *режимі надзвичайного стану* за умови «***здійснення масових терористичних актів**, що супроводжуються загибеллю людей чи руйнуванням особливо важливих об'єктів життєзабезпечення*».

[19] Для цього конкретного випадку, а також для усієї «кольорової шкали» рівнів терористичних загроз не зовсім зрозуміло, чому найвищий, *«червоний»,* рівень терористичної загрози встановлюється, а загроза терористичного акту вважається «*реальною*» лише тоді, коли терористичний акт вже вчинено?

Нижче представлений аналіз документу, який дозволяє зробити висновки про ступінь урегульованості планів, процедур і механізмів КДВОІ на національному рівні[20].

Приклад 2. ***Державний план взаємодії центральних та місцевих органів виконавчої влади на випадок вчинення диверсій щодо ядерних установок, ядерних матеріалів, інших джерел іонізуючого випромінювання у процесі їх використання, зберігання або перевезення, а також щодо радіоактивних відходів у процесі поводження з ними***[21] *(далі – Державний план)*

Документ було розроблено безпосередньо для визначення процедур та механізмів міжвідомчої взаємодії на випадок вчинення *диверсій щодо ядерних установок, ядерних матеріалів*…, що можна вважати класичним прикладом загрози комплексного характеру.

Перш за все звертає на себе увагу той факт, що *Державний план жодного разу не був перевірений ані під час навчань, ані у ході реального реагування* на безпекові інциденти. Таким чином, твердження про те, що цим документом врегульовані процедури і механізми КДВОІ щодо інцидентів і криз, пов'язаних з ядерними об'єктами не має під собою надійної основи.

Цей висновок можна підкріпити розглядом деяких положень документу.

Дійсно, урегульованість питань КДВОІ, очевидно, передбачає чіткий розподіл відповідальності, який неможливий без спільного бачення проблем, використання спільних підходів та узгодженої на національному рівні термінології. На жаль, вже назва постанови та *Державного плану* викликає певні питання, адже в них вживається термін «*диверсія*», як він визначений у Законі України «*Про фізичний захист...*», у якому до «*диверсії*» віднесені зловмисні дії, які у національних законодавствах розвинутих країн

[20] Для більш детального розгляду документу див. Додаток 1 до аналітичної записки.

[21] Постанова Кабінет Міністрів України від 24.07.2013 за №598 «Про затвердження державного плану взаємодії центральних та місцевих органів виконавчої влади на випадок на випадок вчинення диверсій щодо ядерних установок, ядерних матеріалів, інших джерел іонізуючого випромінювання у процесі їх використання, зберігання або перевезення, а також щодо радіоактивних відходів у процесі поводження з ними». [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/598-2013-%D0%BF

найчастіше кваліфікують, як «ядерний тероризм» або «радіаційний тероризм»[22].

Такий неоднозначний підхід має своїм наслідком певну плутанину в розподілі сфер відповідальності між правоохоронними органами та спецслужбами, що безпосередньо впливає на усіх рівнях управління на процедури реагування та КДВОІ.

За самим визначенням КІ, її значенням для безпечної повсякденної життєдіяльності населення, суспільства і держави у цілому, інформація про серйозні безпекові інциденти і кризи, пов'язані з нею, повинна передаватися на найвищий політичний рівень для підготовки і прийняття, якщо це виявиться потрібним, термінових політичних рішень. ***Хоча згадка про інформування вищого політичного керівництва держави і присутня в документі, але відповідне положення сформульоване не конкретно і фактично вказує на необхідність розробки додаткового документу***[23]. І взагалі, *Державний план* не відносить вище політичне керівництво держави до числа учасників планів взаємодії.

До цього часу до *Державного плану* ***не було внесено жодного положення, що стосується інформаційних та кіберзагроз ядерним установкам та іншим ядерним та радіаційно-небезпечним об'єктам,*** які обов'язково увійдуть до числа об'єктів КІ.

Одним з основоположних елементів державної системи захисту КІ є розвинуте партнерство між державними органами та операторами та/або власниками елементів КІ у т.ч. у рамках так званого державно-приватного партнерства. Значну роль у ліквідації наслідків криз, як правило, відіграють волонтерські рухи та інші неурядові організації. У формуванні правильного сприйняття дій держави в умовах криз відводять інформуванню населення, та

[22] Щоправда, стосовно визначення цих термінів й досі, навіть у міжнародних документах, не існує загальновизнаного на міжнародному рівні підходу.

[23] Дійсно, у Державному плані написано «…міжвідомчий оперативний штаб ***постійно інформує*** Президента України, Кабінет Міністрів України та Раду національної безпеки і оборони України ***в установленому порядку».*** При цьому документ не містить жодних пояснень, щодо того, як розуміти слова «*постійно інформує*» і яким документом визначено «*установлений порядок*».

роботі зі ЗМІ. Усі ці сучасні підходи не знайшли свого відображення у документі. Натомість, у ньому лише визначені *обов'язки ліцензіатів* ядерних установок.

Нижче викладені деякі зауваження до конкретних розділів *Державного плану* з точки зору урегульованості процедур КДВОІ.

У розділі *«Учасники плану взаємодії»* слід суттєво розширити перелік учасників Державного плану, у т.ч. за рахунок включення державних органів вищого політичного рівня та неурядових організацій.

Положення *розділу «Сили та засоби учасників плану взаємодії»* слід доповнити за рахунок розширення умов залучення Міноборони, включивши до них, зокрема, випадки терористичних актів (диверсій).

Розділ. *«Порядок взаємодії учасників плану взаємодії»* слід суттєво переробити з тим, щоб забезпечити конкретність заходів та процедур, у т.ч. шляхом визначення форматів та часових меж їх виконання, чіткого розподілу відповідальності між органами управління в кризовій ситуації.

Підсумовуючи викладене вище, можна зробити висновок, що зазначений *Державний план* навряд чи можна віднести до числа документів, які дійсно врегульовують процедури і механізми КДВОІ на між- та надвідомчому рівнях навіть у цільовій сфері застосування, не кажучи вже про захист КІ.

В результаті зосередженості на «своїх» загрозах і ризиках тема необхідності забезпечення взаємодії не тільки між окремими суб'єктами існуючих систем, але й на міжсистемному рівні часто залишається поза увагою уповноважених міністерств і відомств. Це, зокрема, проявляється при відпрацюванні реагування на певні події, а також при проведенні навчань і тренувань.

При цьому, навіть, якщо загроза, реагування, на яку передбачене сценарієм, і має комплексний характер, то відомство-організатор часто проявляє схильність до обмеження таких заходів, здебільшого, оперативно-

тактичним рівнем[24], що дозволяє залишатися у рамках «своєї» системи.

Прикладом такого заходу може послужити тренування, яке проводила ДСНС у рамках підготовки до фінального матчу Ліги чемпіонів УЕФА у Києві, коли виявлена за сценарієм загроза мала комплексний характер (ХБРЯ-загроза плюс ймовірні зловмисні дії), а відеоматеріал фактично ілюстрував можливості реагування підрозділів ДСНС на надзвичайну ситуацію техногенного характеру[25].

Іншим прикладом недостатнього рівня КДВОІ при реалізації загроз комплексного характеру може слугувати ситуація із хакерською атакою на сайт Міненерговугілля України, яка мала місце наприкінці квітня ц. р.[26] При цьому спікер Національної поліції озвучив у ЗМІ позицію свого відомства щодо цієї кібератаки, заявивши, що воно ***готове надати допомогу міністерству, але лише у випадку офіційного звернення*** останнього. Такий підхід не свідчить про наявність на момент атаки процедур ефективної взаємодії. Щоправда, з точки зору кібербезпеки перспективи щодо процедур взаємодії можна оцінювати, як достатньо оптимістичні, беручи до уваги наведену вище інформацію.

[24] У записці вже згадувалося про те, що в Україні вперше командно-штабні навчання національного рівня стосовно об'єктів, що мають бути віднесені до КІ, були проведені лише у 2017 році (див. посилання 5).

[25] Виявлений на площі перед стадіоном кейс з хімічною речовиною з їдким запахом. Детальніше див. додаток 2 до аналітичної записки.

[26] «Хакери зашифрували сайт Міненерговугілля: вимагають викуп у біткоінах» [Електронний ресурс]. – Режим доступу: http://www.unn.com.ua/uk/news/1727073-khakeri-zashifruvali-sayt-minenergovugillya-vimagayut-vikup-u-bitkoinakh

Висновки і рекомендації

Проведений аналіз положень про державні системи безпеки та кризового реагування та кількох прикладів, в яких було розглянуто, як системи повинні або як готуються реагувати на безпекові інциденти у випадку реалізації загроз комплексного характеру, дозволяє зробити такі **висновки:**

1. Існуючі в Україні державні/національні системи безпеки і кризового реагування не спроможні забезпечити системний інтегрований підхід до захисту критичної інфраструктури від комбінацій фізичних загроз (природних, техногенних та соціально-політичних) і кіберзагроз, а чинна нормативно-правова база та фактори, що діють у рамках цих систем, не створюють достатньої мотивації для запровадження дієвих процедур і механізмів координації дій, взаємодії та обміну інформацією між системами.

2. Передовий зарубіжний досвід, євроатлантичні та європейські прагнення України зумовлюють необхідність створення державної системи захисту критичної інфраструктури, про що йдеться у відповідному рішенні РНБО та в Указі Президента, який увів в дію це рішення; важливим моментом в реалізації рішення РНБО та Указу Президента України є створення або призначення органу, відповідального за координацію усієї діяльності щодо захисту критичної інфраструктури.

3. На сучасному етапі реформування сектору безпеки і оборони держави слід вважати доцільним створення державної системи захисту критичної інфраструктури на основі існуючих державних/національних систем безпеки та кризового реагування за умови досягнення якісно нового рівня координації дій та взаємодії між ними, що передбачає, зокрема, узгодження основних параметрів функціонування зазначених систем у т.ч. через запровадження єдиної термінології.

4. На короткострокову перспективу найважливішим завданням у рамках заходів, спрямованих на створення державної системи захисту критичної інфраструктури, слід вважати розробку і прийняття профільного законодавчого акту про критичну інфраструктуру та її захист у тій редакції,

яка відповідає загальновизнаним в країнах-членах НАТО та ЄС підходам та національним інтересам України.

Спираючись на зроблені за результатами аналізу висновки, доцільно запропонувати такі **рекомендації:**

Апарату Ради національної безпеки і оборони України:

- проаналізувати стан виконання рішення Ради національної безпеки і оборони України «Про удосконалення заходів забезпечення захисту об'єктів критичної інфраструктури» від 29 грудня 2016 року, введеного в дію Указом Президента України від 16 січня 2017 року №8/2017, і вжити заходів щодо прискорення його виконання;
- розглянути можливість включення до перспективного плану роботи Ради національної безпеки і оборони України питання «Про необхідність узгодження основних параметрів функціонування державних (національних) систем, які функціонують у сфері національної безпеки і оборони;

Кабінету Міністрів України:

- вжити заходів для прискорення підготовки та подання до Верховної Ради України законопроекту «Про критичну інфраструктуру та її захист», положення якого мають бути базовані на прийнятих у країнах-членах НАТО та ЄС принципах побудови державних систем захисту критичної інфраструктури, забезпечивши при цьому мінімізацію відомчого впливу на принципи створення державної системи захисту критичної інфраструктури;
- для підготовки пропозицій щодо внесення необхідних змін до чинного законодавства у зв’язку із запланованим прийняттям закону «Про критичну інфраструктуру та її захист» утворити тимчасову міжвідомчу комісію, до участі у роботі якої залучити представників міністерств та відомств, що несуть головну відповідальність за функціонування державних/національних систем безпеки та кризового реагування.

С. І. Кондратов

Відділ енергетичної та техногенної безпеки

Серпень, 2018 р.

Аналіз Постанови Кабінету міністрів України від 24 липня 2013 р. №598 *«Про затвердження державного плану взаємодії центральних та місцевих органів виконавчої влади на випадок вчинення диверсій щодо ядерних установок, ядерних матеріалів, інших джерел іонізуючого випромінювання у процесі їх використання, зберігання або перевезення, а також щодо радіоактивних відходів у процесі поводження з ними»*

Загальні відомості про нормативний акт

Постанову №598 було розроблено на виконання статті 22 ЗУ «Про фізичний захист ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання» 2001 р. із змінами та доповненнями. Останні з них датовані 23 грудня 2015 року.

Затверджений постановою *Державний план взаємодії центральних та місцевих органів виконавчої влади на випадок вчинення диверсій щодо ядерних установок, ядерних матеріалів, інших джерел іонізуючого випромінювання у процесі їх використання, зберігання або перевезення, а також щодо радіоактивних відходів у процесі поводження з ними* (далі – Державний план) визначає процедури та механізми взаємодії державних органів та інших суб'єктів процесу реагування у випадку вчинення диверсій[27] щодо ядерних установок, ядерних та інших радіоактивних матеріалів та джерел іонізуючого випромінювання, а також пов'язаних з ними об'єктів.

За інформацією автора, Державний план жодного разу не проходив практичної перевірки ані під час тренувань/навчань, ані під час реагування на реальні безпекові інциденти або кризи.

[27] На жаль, вже назва постанови та *Державного плану* викликає певні питання, адже в них вживається термін «диверсія», як він визначається у ЗУ «Про фізичний захист...». Відповідно до визначення терміну в законі до «диверсії» віднесені зловмисні дії, які найчастіше відносять до «ядерного тероризму» або до «радіаційного тероризму». Щоправда, стосовно визначення цих термінів й досі, навіть у міжнародних документах, не існує загальновизнаного підходу.

Засади, на яких проведено аналіз документу

Виходячи з факту відсутності інформації про перевірку Державного плану під час реальних подій або навчань (тренувань), подальший аналіз проведено на основі співставлення його положень із сучасними тенденціями та підходами до забезпечення фізичної ядерної безпеки та прикладами найкращої практики, як у сфері фізичної ядерної безпеки, так і у більш загальній сфері захисту критичної інфраструктури. При аналізі документу були враховані й ті вимоги до процедур і планів взаємодії усіх заінтересованих сторін, які випливають із необхідності реагування на безпекові виклики, перед якими стоїть Україна.

Про деякі сучасні тенденції щодо забезпечення фізичної безпеки і реагування на безпекові інциденти, пов'язані з ядерними об'єктами, що належать до КІ

При аналізі ПКМУ №598 від 24 липня 2013 р., виходячи із сучасних підходів, до уваги будуть взяті такі міркування та підходи:

1. Аналіз серйозних аварій на промислових об'єктах, спричинених техногенними та природними факторами (наприклад, ядерна криза на АЕС Фукусіма) чітко показує, що вони викликають серйозні наслідки не тільки для експлуатаційної безпеки (у даному випадку ядерної), але й для фізичної ядерної безпеки. Безумовно, є справедливим і зворотне твердження: без належного рівня фізичної безпеки (фізичного захисту) неможливо забезпечити відповідний сучасним вимогам рівень експлуатаційної безпеки. Звертаючись безпосередньо до теми аналітичної записки, цей висновок можна сформулювати таким чином: у *процедурах та механізмах координації дій, взаємодії та обміну інформацією (КДВОІ) та під час реагування на кризові ситуації потрібно враховувати усі безпекові загрози та ризики*, що передбачає тісну взаємодію відповідних систем безпеки і реагування, а іноді (щонайменше на певних етапах) й їх інтеграцію.

2. У більш широкому контексті з цим пов'язаний підхід, який застосовується у розвинутих країнах, які намагаються вибудувати національні системи захисту критичної інфраструктури, до якої, безумовно, відносяться

ядерні об'єкти. Цей підхід полягає у тому, що *при створенні та модернізації систем захисту мають бути враховані усі види загроз (all hazards approach*[28]*).*

3. На теперішній час у провідних країнах світу склалося чітке усвідомлення необхідності захисту (забезпечення безпеки) та стійкості національної критичної інфраструктури. Виведення з ладу або знищення внаслідок будь-яких причин об'єктів і систем, віднесених до КІ, дуже швидко буде мати важкі багатоаспектні наслідки для населення, суспільства та держави у цілому. З цього слідує висновок про *необхідність участі на певних стадіях реагування на безпекові інциденти політичного керівництва держави* та підготовки для нього інформації (intelligence) для прийняття політичних рішень

4. В епоху бурхливого розвитку інформаційних технологій при реагуванні у кризових ситуаціях з одного боку слід ураховувати можливість використання терористами та іншими злочинцями сучасних ІТ-технологій для досягнення ними своїх цілей (звідси *висновок про необхідність посилення заходів з інформаційної та кібер-безпеки*), а з іншого боку, - картинка та інформація з місця подій можуть дуже швидко опинитися у репортажах ЗМІ, коментарях експертів і впливати на настрої населення, що *вимагає розробки та виконання спеціальних заходів з інформування населення та експертної спільноти.*

5. Під час серйозних безпекових інцидентів на найбільшу загрозу своєму життю та здоров'ю наражаються члени команд первинного реагування, військовослужбовці та особовий склад спецпідрозділів, які мають здійснювати контртерористичні заходи на майданчиках об'єктів і систем, віднесених до КІ. *Їх права та обов'язки, обов'язки держави, операторів (ліцензіатів) щодо забезпечення захисту особового складу команд первинного реагування повинні бути повністю врегульовані.*

[28] Останнім часом формулювання цього підходу уточнено, а саме: маються на увазі ***усі види фізичних загроз та кіберзагрози*** (див. посилання 5). Можна припускати, що у зв'язку з тим, що в сучасних умовах спостерігається тенденція до розповсюдження кола питань, які відносять до проблематики національної безпеки, внаслідок чого активно використовуються такі поняття і терміни, як «фінансова безпека», «продовольча безпека», «психологічна безпека» тощо. За таких умов, конкретизація видів загроз виглядає як необхідний крок.

6. Підрозділи первинного реагування повинні бути добре знайомі з об'єктами КІ, віднесеними до КІ. *На таких об'єктах повинні проводитися спільні навчання різного рівня підрозділів з охорони таких об'єктів та зовнішніх сил збройного реагування, інших учасників механізмів реагування*. Для ефективного проведення таких заходів *необхідно постійно розвивати партнерські стосунки між силами охорони об'єкту, іншими службами об'єкту, з одного боку, та зовнішніми силами реагування,* які приходять на допомогу у випадку серйозної кризової ситуації.

7. Реагування на серйозні безпекові інциденти, пов'язані з КІ, передбачає участь цілої низки державних органів та інших організацій. В таких умовах *ефективне управління кризовою ситуацією неможливе без надійної взаємодії, зокрема чітких процедур передачі управління* на різних її стадіях, ефективного обміну інформацією диверсифікованими каналами та засобами зв'язку.

8. Оскільки у багатьох країнах об'єкти (у т.ч. ядерні), а також ресурси для забезпечення реагування можуть належати приватним компаніям (зокрема, міжнародним), то для ефективних *КДВОІ під час кризи вирішальну роль може зіграти державно-приватне партнерство* (його відсутність або ступінь розвитку).

Аналіз документу по розділах

Розділ. Загальні вимоги

Слід зазначити, що у назві Державного плану та у *Розділі. Загальні вимоги* і далі по тексту документу вживається термін «диверсія», як він визначається у ЗУ «Про фізичний захист...». Відповідно до визначення терміну в законі, до «диверсії» віднесені зловмисні дії, які у національних законодавствах багатьох країн та у міжнародних документах здебільшого прийнято відносити до «ядерного тероризму» або до «радіаційного тероризму». Щоправда, стосовно визначення цих термінів й досі не існує загальновизнаного на міжнародному рівні підходу.

Розділ. Учасники плану взаємодії

Як зазначено у документі, до учасників Державного плану взаємодії віднесені «суб'єкти державної системи фізичного захисту», як вони визначені у ЗУ «Про фізичний захист…». На жаль, у цій частині прийнятий ще у 2000 р. закон дещо застарів, а внесені до нього в останні роки зміни не відобразили процеси і підходи, які спостерігаються у сфері протидії ядерному тероризму (у сфері фізичної ядерної безпеки), в результаті яких на теперішній час фізичний захист визнається як один (хоча й основний) із напрямів (елементів) діяльності щодо забезпечення фізичної ядерної безпеки. Очевидно, що більш широкому колу завдань з протидії ядерному та радіаційному тероризму повинно відповідати й більш широке коло суб'єктів реагування на диверсії (акти) щодо ядерних об'єктів (ЯО) та ядерних матеріалів (ЯМ).

Враховуючи висновки та міркування, сформульовані у пп. 1 – 4, 7, 8 до кола учасників слід додати такі державні органи, інші організації та компанії:

- Міністерство охорони здоров'я України (Український науково-практичний центр екстреної медичної допомоги та медицини катастроф);
- РНБО України (Головний ситуаційний центр України);
- Компанії-оператори стільникового, провідного та супутникового зв'язку;
- Державні та приватні енергокомпанії;
- Державні ЗМІ;
- Установи, які мають технічні можливості щодо проведення аналізів на предмет наявності ХБРЯ-матеріалів на місці подій;
- Волонтерські організації та інші неурядові організації.

У цьому ж розділі зазначено, що у виконанні Державного плану взаємодії у центральних органах виконавчої влади, які здійснюють державне управління у сфері фізичного захисту беруть участь, серед інших, відповідні структурні підрозділи Державного агентства України з управління зоною відчуження та Національної академії наук України. За нашою інформацією, у зазначених організаціях вказані у Державному плані взаємодії підрозділи відсутні.

Розділ. Сили та засоби учасників плану взаємодії

У цьому розділі крім необхідного розширення кола учасників звертає на себе увагу абзац, яким визначаються умови залучення сил і засобів Міноборони, а саме – виняткові випадки «особливо важких надзвичайних ситуацій техногенного або природного характеру». Очевидно, що це положення Державного плану дій має бути переглянуто у бік більш широкого та активного залучення Міноборони на випадки терористичних нападів (диверсій) проти ядерних об'єктів України, а також на випадок негативного розвитку кризової ситуації, важкі наслідки якої можуть поставити під загрозу національну безпеку і територіальну цілісність держави.

Слід також урахувати досвід та велику роль, яку можуть відіграти волонтерські організації у кризових ситуаціях. Найкраща практика у цій сфері вимагає брати до уваги фактор участі добровольців у надзвичайних ситуаціях, з тим, щоб максимально ефективно використати їх потенціал та можливості. Інакше неконтрольована участь волонтерів у деяких випадках може призвести до ускладнення ситуації на місці подій.

Розділ. Порядок взаємодії учасників плану взаємодії

На жаль, цей основний розділ Державного плану не пройшов практичної перевірки, і можна лише припускати, що деякі нечітко і не конкретно сформульовані пункти плану в умовах кризової ситуації буде неможливо виконати.

Зокрема, це стосується абзацу, який має безпосереднє відношення до цілей та завдань проекту. Мається на увазі положення Державного плану взаємодії про обмін інформацією. Учасникам пропонується підтримувати зв'язок і здійснювати обмін інформацією «про наявні та потенційні загрози в обсягах, що дають їм можливість приймати рішення про вжиття відповідних заходів…». Зрозуміло, що в умовах кризи, у часовому цейтноті така рекомендація нічого не дає учасникам реагування. Натомість, доцільно рекомендувати заздалегідь встановити обсяги та формати обміну інформацією та неодноразово перевірити їхню прийнятність під час навчань та тренувань.

В абзаці 3-му цього розділу вказано, що «у разі загрози вчинення диверсії щодо конкретної ядерної установки, ядерних матеріалів…» обов'язково оповіщені керівники учасників Державного плану взаємодії. Знову, дуже неконкретне зазначення «загрози вчинення…» викликає серйозні сумніви щодо можливості та доцільності реалізації цього пункту плану. Дійсно, відповідно до цього пункту, при будь-якій загрозі (потенційній, безпосередній, ймовірній…) одразу ж інформація повідомляється керівникам міністерств і спецслужб.

Згідно з пунктом Державного плану взаємодії, що стосується виконання планів реагування, учасникам пропонується вживати «необхідних заходів для отримання та проведення аналізу додаткової достовірної інформації про ситуацію, …, прогнозування можливого розвитку ситуації». При цьому не зазначено, хто і з використанням якого інструментарію повинен і може виконати таке складне завдання. Насправді, на стадії первинного реагування його учасники мають стабілізувати ситуацію на місці подій і спробувати обмежити її розповсюдження майданчиком АЕС. Навряд чи на цій стадії є реальні можливості для аналітичної роботи і прогнозування.

В абзаці, що описує заходи з метою організації взаємодії та координації дій, пропонується утворити «міжвідомчий оперативний штаб». Насправді, якщо дійсно готуватися до такої роботи, штаб повинен скликатися, а не «утворюватися» під час кризи. Тут слід зазначити, що згідно з постановою, що аналізується, у випадку терористичного акту (диверсії) на АЕС функціонування такого штабу має забезпечуватися Міненерговугілля. *Очевидно, що на сучасному етапі, функції та повноваження, які покладаються на такий міжвідомчий орган, можуть бути забезпечені лише при створенні Ситуаційно-кризового центру Міненерговугілля, оснащеного у відповідності до сучасних вимог*. Крім того, на наш погляд, слід чітко виписати, яким чином формується склад штабу, оскільки у постанові щодо цього спостерігається суттєва невизначеність – запропоновано включати до штабу керівників учасників реагування або уповноважених ними осіб. Виглядає доцільним,

визначити критерії заміщення керівника «уповноваженою особою» та вимоги до такої особи.

В абзаці, що визначає роль міжвідомчого оперативного штабу, сказано, що він утворюється «з метою організації взаємодії та координації дій». Цей штаб, крім того, «постійно інформує Президента України, Кабінет Міністрів України та Раду національної безпеки і оборони України в установленому порядку». Таке формулювання також викликає багато питань щодо процедури, формату, періодичності такого інформування та каналів зв'язку, якими воно має здійснюватися.

Ще більше неясності додає наступний абзац, який вводить до числа учасників процесу реагування – *Спеціальну урядову комісію*, на яку також покладені функції забезпечення взаємодії та координації, а *Міжвідомчий оперативний штаб* визначений її робочим органом. Як при цьому розподіляються функції та повноваження, у документі не визначено. Не зрозуміло також, як після активації Спеціальної урядової комісії має здійснюватися інформування вищого політичного рівня держави – Президента, РНБОУ та КМУ.

Пункт, присвячений мінімізації наслідків диверсії, зосереджено на розгляді тільки радіологічних наслідків, що також не відповідає сучасним підходам, які передбачають створення можливостей для реагування на всі види загроз, а також загрози, які мають комплексний характер.

На позитивну оцінку заслуговує те, що у *Державному плані* взаємодії згадується про необхідність забезпечення засобами колективного та індивідуального захисту персоналу та особового складу підрозділів, що беруть участь у реагуванні. При цьому, за нашою інформацією, в Україні залишається неврегульованим зокрема таке питання: при яких рівнях радіації може виконувати контртерористичні заходи на місці подій особовий склад підрозділів первинного реагування та підрозділів зовнішніх сил збройного реагування на терористичний напад на ядерний об'єкт в Україні.

Розділ. Повноваження учасників Державного плану взаємодії

Загальні зауваження до розділу:

1. З викладеного не зрозуміло, який орган здійснює безпосередню діяльність з нейтралізації дій терористів щодо ядерних об’єктів, ядерних матеріалів. Очевидно, що це пропущено у підпунктах, що стосуються МВС та СБУ.
2. Роботу з населенням зведено до оповіщення (місцеві органи) та інформування про стан радіаційної ситуації у разі диверсії (також місцеві органи).
3. Оповіщення та інформування центральних та місцевих органів виконавчої влади про загрозу або виникнення надзвичайних ситуацій покладені, чомусь, тільки на ДСНС, хоча комплексний характер загрози (кризи у разі реалізації загрози) вимагає, щонайменше участі СБУ.
4. У розділі повністю відсутні положення про взаємодію з вищим політичним рівнем держави, хоча, очевидно, у випадку розвитку кризової ситуації може виникнути необхідність у прийнятті політичних рішень.

Додаток 2

Аналіз відеоматеріалу про підготовку особового складу ДСНС до проведення фінального матчу Ліги чемпіонів УЄФА 2018 у Києві з точки зору реагування на реалізацію комплексних загроз

У рамках підготовки до фінального матчу Ліги чемпіонів УЄФА 2018 в Києві ДСНС України розмістила на своєму сайті відео-сюжет під назвою «*Рятувальники ДСНС України продемонстрували, як захищатимуть вболівальників під час матчів Ліги Чемпіонів*», датований 15 травня цього року[29].

У відео-матеріалі, показано, зокрема, відпрацювання дій особового складу ДСНС у випадку виявлення хімічної загрози. За сценарієм тренування сигнал надходить від правоохоронного органу, а саме: поліцейський передає телефоном інформацію про виявлення підозрілого предмету (на відео показано невеликий кейс), із «запахом їдкої рідини» і просить через «*контрол рум*» направити на місце події працівників ДСНС. На місце прибуває спеціалізований автомобіль з групою реагування, члени якої одягнені у комбінезони хімічного захисту. Вони проходять до квадратного майданчику за розміром, не більше 10×10 м, обмеженого сигнальною стрічкою, обстежують кейс за допомогою спеціального обладнання, обстежують двох поліцейських, забирають на ношах одну особу і залишають місце події.

Проаналізуємо цей відеоматеріал з точки зору реагування на комплексну загрозу.

При його перегляді одразу ж виникає таке питання: якщо запах їдкої рідини розповсюджується від кейсу, а не від якогось спеціального контейнеру, якоїсь спеціальної упаковки з відповідним маркуванням, попереджувальними знаками тощо, то чи не означає це, що перш за все слід перевірити версію зловмисних дій з використанням небезпечної хімічної речовини? Адже кейс виявлено на

[29] Державна служба України з надзвичайних ситуацій, офіційний сайт. [Електронний ресурс]. – Режим доступу: http://www.dsns.gov.ua/ua/Video-DSNS-Ukrayini/

площі перед стадіоном, і під дію небезпечної речовини (а може хімічної зброї?) на місці проведення тренування у реальних умовах могли би потрапити десятки, а може й сотні вболівальників.

Тобто, виявлення потенційно небезпечної хімічної речовини в неналежному місці (місці проведення масових публічних заходів) та у неналежній упаковці насамперед ставить питання про можливу спробу вчинення терористичного акту або про хуліганські дії, що зумовлює необхідність участі (залучення до участі) правоохоронних органів, зокрема СБУ.

До того моменту, поки не буде встановлене інше, реагування має відбуватися у спосіб, який відповідає ХБРЯ-загрозі[30]. Це, у свою чергу, передбачає не тільки обстеження осіб (на відео це двоє поліцейських), які могли зазнати впливу, наприклад, отруйної речовини, але й дії, спрямовані на збір речових доказів, відбитків пальців, відбору проб, опитування очевидців, проведення інших передбачених законом дій на місці інциденту. На жаль, в частині відеоматеріалу, присвяченій тренуванню, ми цього не побачили.

Крім того, розмір невеличкого майданчика, до якого у ході навчання було обмежено доступ, явно не відповідає вимогам реагування на загрозу акту хімічного (або, відповідно до національного законодавства, «технологічного») тероризму. І це при тому, що кілька місяців тому, (у березні ц.р.) у Великій Британії сталося отруєння Скрипалів та поліцейського, який прибув на місце події і надавав їм першу допомогу, і основною версією розслідування було визнано застосування бойової хімічної зброї.

Звичайно, усі згадані заходи виглядають зайвими, а їх виконання значно б «ускладнило» процес реагування та його перевірку під час тренувань, якщо заздалегідь відомо, яка «речовина» знаходиться у кейсі, і що загроза теракту відсутня. Але такий підхід значно зменшує цінність тренування з точки зору готовності до реальних ситуацій, оскільки він них не врахована необхідність взаємодії з іншими системами та суб'єктами реагування.

[30] Див. посилання 4.

РЕЗЮМЕ

В аналітичній записці проаналізовані проблеми забезпечення взаємодії державних систем безпеки та кризового реагування у випадках інцидентів та криз комплексного характеру, пов'язаних з критичною інфраструктурою, у рамках завдання щодо моніторингу основних загроз критичній інфраструктурі, визначених пунктом 3.8 чинної *Стратегії національної безпеки України.*

Актуальність публікації пов'язана із питаннями створення державної системи захисту критичної інфраструктури на виконання відповідного рішення РНБО України, введеного у дію Указом Президента України №8/2017 від 16 січня 2017 року.

На конкретних прикладах показано, що існуючі державні системи безпеки та кризового реагування не здатні у повній мірі забезпечити належний рівень координації дій, взаємодії та обміну інформацією між системами, оскільки опікуються тільки певними наборами загроз та ризиків, а всередині систем відсутні чинники, які б формували достатню мотивацію для ефективної діяльності за вказаними напрямами.

Передовий зарубіжний досвід, який ґрунтується на системному підході до розв'язання відповідних проблем, а також євроатлантичні та європейські прагнення України зумовлюють необхідність створення державної системи захисту критичної інфраструктури в нашій країні. Важливим моментом в реалізації завдань, поставлених у рішенні РНБО України та Указі Президента України, є створення або призначення органу, відповідального за координацію та взаємодію у сфері захисту критичної інфраструктури.

В аналітичній записці показано, що на теперішньому етапі реформування сектору безпеки і оборони держави створення державної системи захисту критичної інфраструктури доцільно здійснювати на основі існуючих державних/національних систем безпеки та кризового реагування за умови досягнення якісно нового рівня координації дій та взаємодії, що передбачає

узгодження основних параметрів функціонування зазначених систем у т.ч. через запровадження єдиної термінології.

У представленій аналітичній записці сформульовано ряд висновків і конкретних рекомендацій, спрямованих на прискорення виконання рішення РНБО України та Указу Президента України, якими передбачене створення державної системи захисту критичної інфраструктури.