ПРО ЗАБЕЗПЕЧЕННЯ КООРДИНАЦІЇ ДІЙ, ВЗАЄМОДІЇ ТА ОБМІНУ ІНФОРМАЦІЄЮ ПРИ СТВОРЕННІ ДЕРЖАВНОЇ СИСТЕМИ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Аналітична доповідь

Київ - 2018

Про забезпечення координації дій, взаємодії та обміну інформацією при створенні державної системи захисту критичної інфраструктури- К.: НІСД, 2018. – 30 с.

Автор:

Кондратов С. І.

ЗМІСТ

Для цілей даної публікації використані у тексті скорочення та акроніми мають значення, наведені у представленому нижче списку.

Список скорочень та акронімів

ДПП	державно-приватне партнерство
ІАЦ	інформаційно-аналітичні центри
КДВОІ	координація дій, взаємодія та обмін інформацією
КІ	критична інфраструктура
НІСД	Національний інститут стратегічних досліджень
НМ СКІАЦ	Національна мережа ситуаційних, кризових та інформаційно-аналітичних центрів
НПБ	нормативно-правова база
ОІ	обмін інформацією
СЗЗС КІ	система забезпечення захисту та стійкості критичної інфраструктури
СКЦ	ситуаційні та кризові центри

ВСТУП

Останніми роками забезпечення захисту (безпеки) та стійкості КІ стало одним із пріоритетних завдань у сфері національної та колективної безпеки для більшості розвинутих країн світу та їх об'єднанньь (найбільший інтерес, звичайно, викликають країни-члени НАТО та ЄС, а також самі ці структури). Результатом усвідомлення уразливості об'єктів КІ по відношенню до різноманітних загроз стало запровадження зафіксованих у національних законодавствах цих країн спільних підходів до забезпечення захисту

(безпеки) КІ[1], на основі яких були створені та функціонують відповідні державні (національні) системи. Крім того, спільність підходів знайшла своє відображення у практичному збігу або близькості ключових для цієї сфери термінів та понять, зокрема, таких, як «критична інфраструктура», «загрози критичній інфраструктурі».

Як показує зарубіжний досвід, ефективне функціонування національних систем захисту КІ можливе лише за умови досягнення якісно нового рівня КДВОІ між усіма залученими сторонами (акторами) процесу. Значно жорсткіші вимоги до рівня КДВОІ, коли об'єктом відповідної діяльності є КІ, обумовлені такими основними чинниками:

a. масштабністю та швидкістю настання негативних наслідків для життєдіяльності населення, суспільства і держави у разі кризи, пов'язаної з КІ;
b. розширеним спектром загроз та небезпек (усі фізичні загрози та кіберзагрози), які необхідно враховувати у такій діяльності, що, серед іншого, потребує участі значно ширшого кола акторів у порівнянні з реагуванням на окремі категорії загроз і небезпек;
c. необхідністю забезпечувати на національному рівні управління ресурсами та можливостями держави, приватного сектору, місцевих громад, населення тощо для зниження ризиків для КІ, реагування на безпекові події на її елементах, ліквідації наслідків таких подій та відновлення у найкоротші строки функціонування КІ.

Як показав проведений в НІСД аналіз ситуації в Україні[2], наявні

---

[1] Проблематика забезпечення захисту (безпеки) КІ є порівняно новою. У теперішній час, її термінологічна та понятійна база знаходится у стані активного розвитку. Якщо ще недавно відповідна діяльність розглядалася з точки зору "захисту критичної інфраструктури", то зараз разом із цим терміном або замість нього часто використовують такі терміни, як "безпека" та "стійкість" критичної інфраструктури або їх комбінацію. У зв'язку з цим далі по тексту можна зустріти різні варіанти використання цих термінів, особливо, коли йдеться про зарубіжний досвід та назви офіційних документів.

[2] «Проблеми забезпечення взаємодії при реагуванні на інциденти та кризи комплексного характеру на об`єктах критичної інфраструктури». Аналітична записка. Національний інститут стратегічних досліджень. [Електронний ресурс]. – Режим доступу: http://www.niss.gov.ua/articles/3124/

механізми та процедури взаємодії за умов, коли окреме міністерство (відомство) має забезпечувати реагування на "свій" набір загроз та небезпек і несе відповідальність за функціонування "своєї" системи безпеки (кризового реагування), не дозволяють досягти рівня КДВОІ, адекватного цілям та завданням захисту національної КІ. Особливо переконливо про це свідчать результати аналізу планів та процедур реагуванн на безпекові події, викликані реалізацією комбінації загроз. З цього випливає доволі очевидний висновок: ***для ефективного управління усім комплексом заходів щодо КІ на національному рівні,*** у т.ч. в частині КДВОІ***, необхідно запроваджувати надвідомчі структури та механізми***.

Незважаючи на національну специфіку та унікальність безпекової ситуації для кожної конкретної країни, аналіз зарубіжного досвіду показує, що при створенні СЗЗС КІ в розвинутих країнах світу було застосовано ряд загальних підходів, на основі яких можна сформулювати основні завдання зі створеннях такої системи в Україні.

1. Основні завдання зі створення систем забезпечення захисту та стійкості критичної інфраструктури

Уроки, винесені з реагування та ліквідації наслідків Чорнобильської катастрофи (1986 р.), терористичних атак у США (11 вересня 2001 р.), урагану Катріна (2005 р.), ядерної кризи на АЕС Фукусіма (2011 р.), ряду інших техногенних аварій та природних катастроф, численні кібератаки на державні установи, фінансові, енергетичні та інші промислові об'єкти призвели до чіткого усвідомлення взаємозв’язку питань експлуатаційної (технічної) безпеки, фізичної безпеки та кібербезпеки. Результати вивчення та аналізу різних аспектів безпеки були узагальнені у національних законодавствах, а також у ряді офіційних публікацій спеціалізованих міжнародних організацій таких, як МАГАТЕ та WINS[3].

[3] WINS (World Institute for Nuclear Security, www.wins.org), Всесвітній інститут з фізичної ядерної безпеки – міжнародна неурядова організація, яка розташована у Відні (Австрія) і

До ключових висновків, зроблених на основі аналізу результатів згаданих зусиль, стало те, що ***КІ слід системно захищати від усіх видів фізичних загроз і небезпек*** (природного і техногенного походження, зловмисних дій) ***та кіберзагроз***, а також те, що відповідну діяльність слід ***здійснювати, спираючись на результати оцінки загроз та ризиків, розвиваючи ДПП і залучаючи до спільних заходів усе суспільство*** – від окремих сімей та місцевих громад і аж до вищого політичного керівництва держави.

Довідково. На даний момент співвідношення між термінами "загроза" і "небезпека" в національному законодавстві у сфері національної безпеки поки що чітко не визначено. У зв'язку з цим для цілей даної публікації використано підхід Міністерства внутрішньої безпеки США, згідно з яким різниця між термінами полягає у тому, що "загроза" характеризується спрямованістю на певні особу (-и), актив (-и), систему (-и), мережу (-і) або географічну (-і) територію (-ї), у той час, як "небезпека" такої спрямованості не має.[4]

Значення КІ для національної безпеки обумовлене тими багатоаспектними швидкими негативними наслідками для життєдіяльності країни та населення, які можуть спричинити збої в функціонуванні її елементів або їх знищення (руйнування). Це може проявлятися у формі так званих *ефектів доміно*[5] та *каскадних ефектів*, коли ***важкі наслідки безпекових криз на одному із елементів КІ в якомусь із її секторів розповсюджуються на інші елементи і сектори КІ.*** Запобігання таким сценаріям і є одним із головних завдань державної СЗЗС КІ, що вимагає суттєвого підняття рівня КДВОІ між акторами.

Ураховуючи викладені вище міркування, можна сформулювати деякі основні завдання та визначити головні напрями побудови національної СЗЗС КІ, а саме:

фінансується урядами західних країн, фондами та корпораціями, зацікавленими у підвищенні рівня фізичної ядерної безпеки.

[4] Див. *DHS Lexicon Terms and Definitions 2017 Edition* – Revision 2 Issue Date – October 16, 2017, [Електронний ресурс]. – Режим доступу: https://www.dhs.gov/sites/default/files/publications/18_0116_MGMT_DHS-Lexicon.pdf

[5] У випадку *ефекту доміно* цей процес відбувається на однорідних елементах системи (мережі) (примітка автора).

1. Розвиток НПБ забезпечення захисту (безпеки) та стійкості національної (державної) системи захисту КІ, яка має стати правовою основою для регулювання відповідних видів діяльності (у т.ч. за представленими далі напрямами);

2. Забезпечення системного підходу до управління безпековими ризиками для КІ через створення національної (державної) СЗЗС КІ;

3. Залучення до відповідної діяльності широкого кола акторів, ефективність зусиль яких потребує переходу на значно вищий рівень КДВОІ між ними**;**

4. Створення (призначення) спеціального органу — національного координатора для забезпечення належного рівня КДВОІ, сприяння встановленню чіткого розподілу функцій, повноважень і сфер відповідальності та подолання міжвідомчих бар'єрів;

5. Розвиток партнерських стосунків між усіма суб'єктами процесу, включаючи приватний сектор і населення; планування взаємодії між ними у кризових ситуаціях і регулярні перевірки відповідних планів і процедур у ході навчань, тренувань, а також в реальних умовах;

6. Створення національної мережі ІАЦ та СКЦ для підвищення рівня КДВОІ, забезпечення інформаційно-аналітичної підтримки рішень (у т.ч. політичних) щодо безпеки КІ;

7. Забезпечення СЗЗС КІ кадрами, кваліфікація та знання яких мають відповідати сучасним вимогам та специфіці цього безпекового напряму.

Як зазначено у п.3 наведеного переліку, досягнення цілей та виконання завдань із забезпечення захисту та стійкості КІ потребує участі цілої низки акторів. До їх числа відносяться державні органи і відомства (у т.ч. правоохоронні та спецслужби), компанії усіх форм власності, неурядові організації, місцеві органи влади та місцеві громади, населення, ЗМІ, експертне співтовариство тощо. Такий широкий спектр заінтересованих сторін обумовлює жорсткі вимоги до механізмів і процедур КДВОІ та

необхідність створення певних систем, мереж і центрів, які мають забезпечувати ОІ, її обробку та представлення у необхідному вигляді для ефективного здійснення акторами своєї діяльності, включаючи прийняття рішень у ході виконання відповідних місій, а саме:

1. запобігання безпековим інцидентам та кризам на об’єктах КІ;
2. реагування на такі інциденти та кризи у випадках, коли вони, все ж таки, трапилися;
3. пом’якшення та ліквідацію наслідків інцидентів та криз;
4. відновлення функціонування об’єктів КІ.

Звичайно, наведені вище переліки не можуть претендувати на вичерпність. До того ж, створення державної СЗЗС КІ, як одного із ключових елементів системи національної безпеки, в очевидний спосіб пов'язане з більш широким колом проблем забезпечення національної безпеки і оборони, національної стійкості.

Зокрема, це стосується пункту про управління ризиками, виконання якого гостро ставить проблему регулярного проведення оцінки різноманітних загроз і ризиків, у т.ч. вчинення терористичних актів, для чого необхідно розробити і запровадити відповідні методики і процедури.

Сюди ж слід віднести і вирішення питань, пов'язаних із розвитком партнерства у цій сфері. Адже ті безпекові умови, в яких зараз перебуває Україна, потребують активного розвитку ДПП і не лише, наприклад, за напрямами кібербезпеки або безпеки КІ, а й у більш загальному контексті, а саме – національної безпеки та оборони.

Аналогічно, функціонування системи інформаційно-аналітичної підтримки процесу прийняття рішень щодо захисту КІ на практиці буде неможливо відокремити від створення національної мережі ситуаційних центрів сектору безпеки і оборони, передбаченого рішенням РНБО та відповідним указом Президента України[6].

[6] Див. Указ Президента України №92/2016 Про рішення Ради національної безпеки і оборони України від 4 березня 2016 року "Про Концепцію розвитку сектору безпеки і оборони

Тим не менше, спираючись на викладене вище, можна стверджувати, що однією з ключових проблем на шляху створення державної СЗЗС КІ буде забезпечення належного рівня КДВОІ між усіма суб'єктами процесу.

У наступних розділах проблема забезпечення КДВОІ при створенні державної СЗЗС КІ в Україні розглянута більш детально з основним акцентом на механізмах і процедурах ОІ.

2. Ситуація в Україні з точки зору забезпечення координації дій, взаємодії та обміну інформацією з метою захисту критичної інфраструктури

Оцінка національних систем безпеки та кризового реагування на надзвичайні ситуації різного походження має декілька основних аспектів. Зокрема, якщо розглядати можливості України щодо реагування на надзвичайні ситуації техногенного і природного походження, то вони формувалися, значною мірою, на основі уроків, винесених з Чорнобильської катастрофи, та у ході діяльності, спрямованої на ліквідацію та пом'якшення її наслідків. При цьому постійна увага світової спільноти до чорнобильських проблем, отримання у зв'язку з цим значної міжнародної допомоги, необхідність вживати заходів у неодноразових випадках (реального або вигаданого) ускладнення умов на майданчику ЧАЕС та у зоні відчуження, сприяли створенню в Україні доволі ефективних систем у цій сфері.

З іншого боку, з оцінкою глобальних загроз і ризиків ядерного і радіаційного тероризму, а також проблем розповсюдження ядерної зброї значною мірою пов'язана серйозна міжнародна допомога Україні задля створення нею державної системи фізичного захисту (ядерних матеріалів і ядерних установок), системи обліку і контролю ядерних матеріалів, державної системи гарантій ядерного нерозповсюдження, а також запровадження системних заходів щодо протидії незаконному обігу ядерних та інших радіоактивних матеріалів, тобто, усього того, що має запобігати

України". [Електронний ресурс]. – Режим доступу: https://www.president.gov.ua/documents/922016-19832

потраплянню ядерної зброї, ядерних та інших радіоактивних матеріалів до неналежних державних і недержавних акторів, включаючи терористів, та посиленню національних можливостей на випадок, якщо перелічені заходи не спрацюють.

Що ж стосується підходів до реагування на терористичні загрози у більш широкому контексті, а також кіберзагрози об'єктам і системам, що мають бути віднесені до КІ, то можна стверджувати, що системна робота за цими напрямами розпочалася лише після 2014 року. Відповідно, більшість питань щодо забезпечення ефективної взаємодії як між суб'єктами державних (національних) систем безпеки і кризового реагування, так і на міжсистемному рівні, ще потребують свого вирішення.

Дійсно, існуючі в Україні окремі системи ОІ й досі є значною мірою фрагментованими, що відображає все ще існуюче у цій сфері домінування застарілих відомчих підходів, закріплених у чинній НПБ. у частині, що стосується загроз та ризиків, якими мають опікуватися системи безпеки та кризового реагування і відповідальні за їх функціонування державні органи. Наразі, зафіксований у НПБ "розподіл" загроз та ризиків по системах національного рівня консервує вузьковідомчий "погляд" на проблеми і створює бар'єри для організації реагування на більш широкий інтервал загроз і ризиків, як цього вимагає захист КІ.

Зокрема, при всій розгалуженості та детальності національної НПБ в чинних документах, особливо тих, що стосуються реагування на надзвичайні ситуації (головна відповідальність на ДСНС України), останні розглядаються майже виключно як наслідки природних і техногенних подій, а терористичні загрози фактично не враховані, або їх врахування зведене до формального згадування про необхідність брати їх до уваги. І навпаки, коли йдеться про терористичні загрози та ризики (головна відповідальність на СБ України), то у чинних документах спостерігається тенденція розглядати їх, так би мовити, у "чистому вигляді", без урахування можливості їх реалізації у вигляді

комбінації загроз (або комплексних загроз), наприклад, разом з техногенною загрозою[7].

При цьому, навіть тоді, коли така система має статус *державної* чи *національної,* її функціональність виявляється обмеженою зверху рівнем відповідального міністерства чи відомства, що не передбачає наявності дієвих процедур взаємодії та ОІ з вищим політичним керівництвом держави.

З іншого боку, на умовно «нижчому», публічному рівні (або ж, у публічному домені), який, відповідно до найкращої зарубіжної практики, має включати таких акторів, як населення, ЗМІ, неурядові організації та експертне співтовариство, в національному законодавстві та в національній практиці у найкращому випадку ОІ зведено до оповіщення населення в умовах надзвичайних ситуацій.

Слабко розвинута практика проведення навчань та тренувань для забезпечення і перевірки готовності до кризових ситуацій, особливо на регіональному та національному рівнях, сприяла консервації суто формального відношення до процедур КДВОІ, зокрема ОІ між існуючими системами безпеки та кризового реагування України та їх суб'єктами, що проявляється, серед іншого, у декларативності та неконкретності положень відповідних документів, які мають врегульовувати такі процедури та запроваджувати необхідні інструменти.

Для повноти картини слід відзначити і позитивні тенденції, які останнім часом намітилися в організаційно-правовому забезпеченні захисту КІ в Україні після того, як на рубежі 2016 – 2017 рр. на політичному рівні були прийняті важливі рішення щодо захисту КІ[8]. Зокрема, у структурі Міністерства внутрішніх справ України, були створені структурні підрозділи, які опікуються проблематикою захисту КІ, у т.ч. відділ з питань захисту КІ.

---

[7] Звичайно, це не відноситься до реагування на загрози та ризики ядерного тероризму, про що йшлося вище. Більш детально про проблеми взаємодії між системами див. Посилання 2.

[8] Див. Указ Президента України від 16 січня 2017 року №8/2017, яким було введено в дію рішення Ради національної безпеки і оборони України "Про удосконалення заходів забезпечення захисту об'єктів критичної інфраструктури" від 29 грудня 2016 року. [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/n0014525-16

Крім того, у рамках процесу реформування Служби безпеки України триває активний пошук місця та ролі структурних підрозділів відомства у реалізації завдань щодо захисту КІ, які були поставлені згаданим вище указом Президента України[9]. У 2017-2018 рр. помітно активізувалася діяльність міністерств та відомств щодо проведення міжвідомчих навчань і тренувань, спрямованих на відпрацювання процедур взаємодії та обміну інформацією при реагуванні на інциденти та кризи різного походження.

Таким чином, підсумовуючи головні моменти, що характеризують ситуацію в Україні, можна стверджувати, що основні проблеми КДВОІ, зокрема ОІ, при створенні державної СЗЗС КІ необхідно буде подолати у площинах міжсистемної (міжвідомчої) взаємодії, а також взаємодії з рівнем політичного керівництва держави та з *публічним рівнем*.

Іншим важливим аспектом проблеми, що розглядається, є необхідність створити систему прийняття рішень щодо КІ. У зв'язку з цим на сучасному етапі, коли в Україні триває процес глибокого реформування сектору безпеки і оборони, у т.ч. за напрямами кібербезпеки та безпеки КІ, слід активізувати обговорення можливих варіантів архітектури системи ОІ та підтримки прийняття рішень на всіх управлінських рівнях.

При цьому необхідно взяти до уваги те, що у теперішній безпековій та фінансово-економічній ситуації, в якій перебуває наша країна, ***слід вважати доцільним створення державної системи захисту КІ на основі існуючих державних/національних систем безпеки та кризового реагування за умови досягнення якісно нового рівня КДВОІ між ними***, що передбачає, серед іншого, узгодження основних параметрів функціонування зазначених систем, у т.ч. узгодження запровадженої у кожній системі термінології.

Такий же самий підхід виглядає найбільш оптимальним і для вибору моделей взаємодії та ОІ для НМ СКІАЦ, що передбачає максимально можливе використання наявної інфраструктури, ресурсів та технічних

[9] Див. посилання 8.

засобів, що знаходяться у розпорядженні державних органів, компаній різних форм власності, інших суб'єктів забезпечення безпеки та стійкості КІ.

Виходячи з цього, у найближчій перспективі основні рекомендації щодо забезпечення взаємодії та ОІ доцільно формулювати, фокусуючись на ***запровадженні дієвих механізмів взаємодії та ОІ між існуючими системами безпеки та кризового реагування, беручи до уваги усі види фізичних загроз та кіберзагрози, а також необхідність забезпечення взаємодії та ОІ з політичним та публічним рівнями.***

3. Основні підходи до формування архітектури національної мереж і ситуаційно-кризових та інформаційно-аналітичних центрів

Згадані вище проблеми можуть бути значною мірою розв'язані завдяки функціонуванню НМ СКІАЦ, яку необхідно створити в Україні для забезпечення інформаційно-аналітичної підтримки процесу прийняття рішень, у т.ч. через усунення названих вище «вузьких місць» та удосконалення існуючих механізмів і процедур ОІ[10].

Слід зазначити, що у цій сфері забезпечення рівня взаємодії та ОІ, адекватного сучасним загрозам, визначено, як пріоритетне завдання багатьма розвиненими країнами світу та міжнародними організаціями. Дійсно, кризові ситуації на об'єктах КІ, спричинені реалізацією загроз і небезпек, передусім комплексного характеру, можуть мати безпосередній вплив не тільки на національну, а й на регіональну і, навіть, глобальну безпеку. Масштаб потенційних наслідків потребує готовності до мобілізації усіх наявних у державі ресурсів а, при необхідності, й до запиту міжнародної допомоги від країн-партнерів, що неможливо без належної інформаційно-аналітичної підтримки процесів прийняття рішень, у т.ч. на політичному рівні.

Сформульовані вище міркування вказують на доцільність розміщення «на

---

[10] Така мережа могла би бути створена як один із основних компонентів національної мережі, створення якої передбачено Указом Президента України №92/2016 "Про рішення Ради національної безпеки і оборони України від 4 березня 2016 року "Про Концепцію розвитку сектору безпеки і оборони України" (див. Посилання 2).

вершині» ієрархічно побудованої піраміди НМ СКІАЦ центру, який би виконував функції *головного ситуаційно-кризового центру держави* та забезпечував безпосередню інформаційно-аналітичну підтримку процесу прийняття рішень вищим політичним керівництвом держави (див. Рис. 3 у Додатку 2).

На момент підготовки матеріалу за своєю приналежністю та призначенням, на думку автора, цій ролі у найбільшій мірі відповідав Головний ситуаційний центр України при Раді національної безпеки і оборони України. Разом з тим, слід зазначити, що у теперішній час відбувається процес комплексного реформування сектору безпеки держави, у ході якого не можна виключати, що відповідні функції буде доручено виконувати іншому СКЦ, створеному, наприклад, при Президентові або при Уряді України. У будь-якому варіанті важливо, щоб вище політичне керівництво держави у кризових ситуаціях мало можливість своєчасно отримувати належним чином підготовлену інформацію для прийняття рішень стосовно національної та державної безпеки, зокрема безпеки та стійкості КІ.

При ієрархічному структуруванні НМ СКІАЦ доцільно використати апробовані у розвинутих країнах світу підходи до організації обробки інформації, призначеної для підтримки процесу прийняття рішень у сфері національної безпеки.

У залежності від функцій, повноважень і сфери відповідальності замовника (отримувача) інформації кількість і назви етапів (стадій) відповідних циклів підготовки інформації та їхні основні завдання можуть дещо відрізнятися один від одного, тим не менше, їхня сутність залишається практично однаковою. На представлених нижче діаграмах (див. Рис.1 та Рис. 2) такий підхід проілюстровано у вигляді певної послідовності стадій циклу. При практичній реалізації підходів до створення системи інформаційно-аналітичної підтримки прийняття рішень на основі НМ СКІАЦ слід брати до уваги той факт, що з підвищенням рівня управління час, відведений для

прийняття рішень, зменшується. Виходячи з цього, можна зробити доволі очевидний, але важливий для подальшого аналізу висновок: ***найбільш жорсткі часові рамки для процесу прийняття рішень існують на вищому політичному рівні, а час, відведений для прийняття таких рішень, є вельми обмеженим ресурсом національного значення***.

Рис. 1. Типовий цикл підготовки інформації для прийняття рішень (Intelligence Information Cycle)[11].

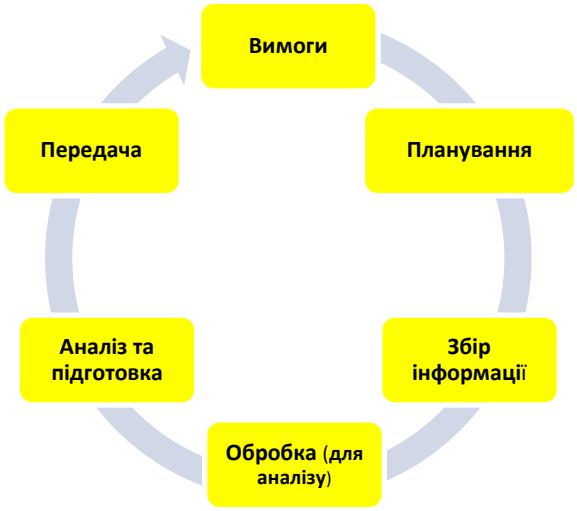

Рис. 2. Адаптований до цілей та завдань НМ СКІАЦ цикл підготовки інформації для підтримки прийняття рішень щодо КІ.

[11] Як й у випадку типового циклу підготовки інформації, запропонований цикл обміну інформацією для НМ СКІАЦ має відображати циклічність процесу, залишаючи переходи між стадіями циклу дещо розмитими. Виявлення відсутності або необхідності уточнення якоїсь інформації може зробити необхідним паралельне виконання деяких завдань або повернення до попередніх завдань з метою уточнення інформації та/або їх доопрацювання.

4. Опис циклу підготовки інформації для прийняття рішень

Нижче описаний цикл підготовки інформації для прийняття рішень за його послідовними стадіями.

Стадія 1. Постановка завдання («формулювання вимог») щодо необхідної інформації;

Стадія 2. Планування заходів та управління ресурсами з метою виконання завдання;

Стадія 3. Збір первинної («необробленої») інформації різноманітними способами і шляхами;

Стадія 4. Обробка та форматування інформації з тим, щоб представити зібрані масиви даних у формі, прийнятній для їх використання аналітиками, включаючи узагальнення інформації, введення даних до відповідних баз тощо;

Стадія 5. Аналіз та підготовка інформації для прийняття рішень (у нашому контексті, - аналіз, оцінку і перевірку даних, об'єднання даних та інформації в єдину взаємоузгоджену картину розвитку кризової ситуації, на основі якої робляться висновки щодо можливих сценаріїв її розвитку та пропонуються варіанти рішень;

Стадія 6. Надання підготовленої інформації (у нашому випадку, її споживачами є ті посадові особи/уповноважені державні органи, які приймають рішення на оперативному, стратегічному та політичному рівнях).

> *Примітка: В результаті прийнятих на Стадії 6 рішень можуть бути сформульовані нові вимоги (запити) щодо отримання певної інформації, що означатиме подальше продовження циклу підготовки інформації.*

Спираючись на представлений вище загальний опис стадій циклу

підготовки інформації, можна передбачати, що функціонування НМ СКІАЦ має забезпечувати виконання завдань, віднесених до стадій 2 – 6 циклу.

Таким чином, у процесі підготовки інформації для її представлення на вищий політичний рівень це обмеження повинно бути враховано, зокрема, у форматі (у т.ч. в обсязі) інформації, що подається.

Співставлення представленого вище циклу підготовки інформації з існуючою в Україні практикою (висновок зроблено на основі відкритої інформації) показує, що на даний момент у процедурах, що передбачені чинною НПБ щодо КДВОІ в нашій країні, недостатньо уваги приділяється стадіям обробки та аналізу інформації. Зокрема, при усій привабливості можливості отримання оперативної інформації безпосередньо з міста тієї чи іншої події (в режимі «он-лайн») забезпечити ефективну підтримку процесу прийняття рішень (особливо, на найвищому політичному рівні) буде не можливо за відсутності стадій, на яких здійснюється серйозна попередня робота з обробки, аналізу та оцінки інформації, прогнозування можливих варіантів розвитку подій, а також формулювання запропонованих у певному форматі варіантів рішень.

Іншими словами, за винятком окремих випадків інформаційного обміну та взаємодії, ***безпосередня передача інформації, яка не пройшла стадії обробки, аналізу, оцінки та підготовки варіантів можливих рішень*** (особливо, на політичному рівні) ***є недоцільною.***

Інший важливий аспект, який має бути відображеними в архітектурі НМ СКІАЦ, полягає у тому, що в Україні існують національні та галузеві системи, сфокусовані на протидії певним видам загроз, включаючи забезпечення готовності до кризового управління у випадку реалізації таких загроз. У рамках функціонування цих систем передбачені механізми ОІ (у т.ч. через спеціально створені з цією метою СКЦ). Прикладами таких систем і підсистем можуть бути:

- Єдина система запобігання, реагування та припинення терористичних

актів і мінімізації їх наслідків;

- Державна система фізичного захисту;
- Єдина державна система цивільного захисту, до якої, серед інших, включений ряд підсистем (наприклад, підсистема безпеки об'єктів ядерної енергетики);
- Єдина державна система запобігання і реагування на надзвичайні ситуації техногенного та природного характеру та деякі інші.

Крім наявності значної кількості важливих систем і підсистем (наприклад, ядерної безпеки), які мають статус національних чи державних, слід також брати до уваги, і те, що за рядом безпекових напрямів Україна має міжнародні зобов'язання, на виконання яких вона повинна надавати інформацію про безпекові інциденти та надзвичайні ситуації, зокрема, до таких міжнародних організацій, як МАГАТЕ, а також до держав-партнерів та їх компетентних органів.

Ураховуючи це, СКЦ та ІАЦ, створені при державних органах, які забезпечують діяльність систем і підсистем національного рівня, а також інформування міжнародних організацій та країн-партнерів, доцільно віднести до наступного за Головним ситуаційним центром України рівня, на якому здійснюються заходи з аналізу інформації та взаємодії, віднесені до стадії 5 інформаційного циклу (див. перелік стадій вище). Виходячи з цього, пропонується, щоб до центрів цього рівня були віднесені СКЦ та ІАЦ таких міністерств/відомств:

- ***ДСНС,*** до компетенції якої належать: надзвичайні ситуації природного та техногенного характеру, цивільний захист, ліквідації наслідків надзвичайних ситуацій, у т.ч. на ядерних об'єктах;
- ***СБУ (АТЦ)***: напрям протидії тероризму, у т.ч. ядерному та радіаційному
- ***Міністерства оборони***: воєнні загрози, боротьба з тероризмом;
- ***МВС (Нацгвардії)***: забезпечення фізичної безпеки ядерних та інших

об′єктів КІ, участь у первинному реагуванні на надзвичайні події різного походження тощо;

- ***Міненерговугілля:*** забезпечення енергетичної безпеки, забезпечення захисту об’єктів критичної енергетичної безпеки, забезпечення технічної ядерної безпеки, забезпечення фізичної ядерної безпеки, міжнародне співробітництво в ядерній галузі тощо;
- ***Держатомрегулювання***: регулювання ядерної безпеки, регулювання забезпечення ядерної захищеності (фізична ядерна безпека), міжнародне співробітництво (у т.ч. інформування МАГАТЕ про інциденти з експлуатаційної та фізичної ядерної безпеки);
- ***Міністерства охорони здоров'я :*** організація екстреної медичної допомоги у кризових ситуаціях, організаційне та методологічне забезпечення діяльності Державної служби медицини катастроф.

До наступного рівня в ієрархічній архітектурі ***системи взаємодії та ОІ*** **доцільно віднести** ***СКЦ та ІАЦ крупних державних і приватних компаній*** (зокрема, в енергетичній галузі – ДП НЕК «Укренерго»; в ядерній – НАЕК «Енергоатом» тощо), ***а також великих підприємств***. На цьому ієрархічному рівні повинні, в основному, виконуватися завдання, віднесені до Стадії. 4, тобто, обробка, форматування і, можливо, первинний аналіз, інформації та даних для їх передачі партнерським організаціям (горизонтальний обмін) та на більш високий ієрархічний рівень (вертикальний обмін). На цьому ж рівні, під час можливого розгортання кризи мають прийматися рішення тактичного та оперативного характеру, інформація про які повинна надходити оперативному персоналу та підрозділам первинного реагування (вертикальний обмін).

Найнижчим у ієрархії, але, ключовим з точки зору збору та отримання первинної інформації, є ***рівень систем моніторингу та контролю різноманітних параметрів безпеки*** (у т.ч. фізичної) ***на об'єктах і системах, віднесених до КІ***, зокрема на ядерних та інших радіаційно-

небезпечних об'єктах, а також систем моніторингу, які контролюють параметри стану довкілля, метеорологічні умови тощо. Саме з цього рівня, як передбачається, будуть надходити основні сигнали, дані та інша безпосередня інформація з місця подій, які у подальшому підлягатимуть обробці та аналізу для забезпечення підтримки процесу прийняття рішень. На цьому ж рівні обмін інформацією між безпосередніми суб'єктами процесу реагування слугує основою для прийняття рішень, в основному, оперативного характеру.

Слід також зазначити, що в Україні у випадку кризових ситуацій існує практика створення міжвідомчих структур (штабів, комісій тощо), які, як правило, очолюють керівники місцевих органів влади відповідного рівня. Серйозні інциденти, які ставлять під загрозу фізичну безпеку ядерних об'єктів, а також інших об'єктів і систем, що відносять до КІ, вимагатимуть прийняття рішень на регіональному і національному рівнях, тому при розробці архітектури НМ СКІАЦ, на погляд автора, доцільно передбачити технічні та організаційно-правові можливості інтегрування ***СКЦ місцевих органів влади*** (у разі їх створення) до національної мережі.

Враховуючи ***безпрецедентний для історії сучасної України рівень воєнних загроз,*** які у теперішній час буває важко відокремити від загроз тероризму, серйозну увагу слід приділити механізмам і процедурам обміну інформацією та даними з СКЦ та ІАЦ ***Міністерства оборони України.***

Як згадувалося вище, на даний момент стратегія розбудови державної СЗЗС КІ на базі існуючих систем безпеки та кризового реагування виглядає найбільш оптимальною. Аналогічний підхід доцільно було б застосувати і до створення НМ СКІАЦ, інтегрувавши ресурси різноманітних кризових, ситуаційних та ІАЦ для цілей захисту КІ, зокрема, та забезпечення національної безпеки, у більш широкому контексті.

Разом з тим, реалізація такого підходу гостро поставить питання архітектури НМ СКІАЦ, адже в такій мережі необхідно буде об'єднати

різноманітні центри, які використовують різне обладнання, програмне забезпечення, протоколи і процедури передачі інформації тощо. Очевидно, що створення НМ СКІАЦ слід розпочинати з активного залучення представників ІТ-сектору до обговорення і розв'язання згаданих проблем.

Для переходу до стадії практичного розв'язання сформульованої проблеми доцільно вже найближчим часом ***розробити концептуальний документ щодо створення національної мережі ситуаційно-кризових центрів для забезпечення національної безпеки і оборони України,*** одним із завдань якої має стати сприяння КДВОІ при забезпеченні безпеки та стійкості КІ**.**

5. Роль обміну інформацією у розбудові державно-приватного партнерства у сфері забезпечення захисту та стійкості критичної інфраструктури

У більшості розвинутих країн світу переважна кількість об'єктів і систем, які віднесені до національної КІ, знаходяться у приватній власності. При цьому саме власники та/або оператори таких об'єктів і систем несуть основну відповідальність за їх безпеку та стійкість по відношенню до усіх видів фізичних загроз і кіберзагроз, роблять інвестиції у побудову, належне функціонування та оновлення відповідних систем захисту. Держава, у свою чергу, має створити необхідну НПБ, а також умови, що сприяють інвестуванню у безпеку КІ, підтримуючи при цьому необхідний рівень конкурентоспроможності національної економіки. Таким чином, викладене вище робить розвиток ДПП у цій сфері безальтернативною умовою створення ефективної державної СЗЗС КІ.

При цьому роль ОІ у розбудові такого партнерства неможливо переоцінити. Дійсно, наприклад, у національному законодавстві таких країн, як США та Німеччина, зафіксовані положення, згідно з якими ***умовою для розвитку ДПП є встановлення атмосфери довіри, фундаментом для чого***

є обмін вчасною, надійною і точною інформацією[12]. У рамках такого обміну компетентні державні органи надають власникам та/або операторам, насамперед, актуальну інформацію про фізичні та кіберзагрози, у свою чергу отримуючи від останніх інформацію про безпекові умови, безпекові інциденти на конкретних об'єктах та системах КІ, виявлення індикаторів підозрілої діяльності навколо об'єктів, про зміни у технологічних процесах тощо. Наявність такої інформації у партнерів дозволяє їм більш ефективно вживати заходів щодо безпеки та стійкості КІ, раціонально розпоряджатися ресурсами, краще планувати взаємодію у разі реальних інцидентів та під час спільних навчань (тренувань) для її відпрацювання.

6. Взаємодія та обмін інформацією з населенням, громадськими організаціями та експертним співтовариством

Для ситуації в Україні особливий акцент слід зробити на ***обміні інформації з населенням, громадськістю та експертним середовищем***. Необхідність розробки та інтегрування до заходів з КДВОІ процедур і механізмів надійного обміну інформацією з населенням, ЗМІ та експертним співтовариством випливає з того, що саме населення та довкілля є основними об'єктами захисту для усіх безпекових систем в державі, а від позиції ЗМІ та експертів буде, серед іншого, у значній мірі залежати усвідомлення населенням безпекових загроз та ризиків, готовність людей до дій у кризових ситуаціях, адекватне сприйняття заходів державних органів та інших акторів у ході реагування та ліквідації наслідків криз тощо. Усе перелічене може мати серйозний вплив на перебіг кризи та її результати.

До основного принципу взаємодії та ОІ з цією категорією учасників процесу слід віднести необхідність своєчасного надання виваженої інформації для запобігання паніці та мобілізації ресурсів місцевих спільнот для ефективного реагування у разі кризи. Тому, як і для випадку

[12] Див. наприклад, *Partnering* for Critical Infrastructure Security and Resilience. National Infrastructure Protection Plan, NIPP 2013 / U.S. DHS / [Електронний ресурс]. – Режим доступу: www.dhs.gov/national-infrastructure-protection-plan

інформування вищого політичного керівництва держави, було б неправильним і недоцільним надавати населенню і широкому колу ЗМІ первинну інформацію без попередньої її перевірки та обробки.

При цьому слід підкреслити, що у розвинутих країнах світу сформувалося усвідомлення того, що забезпечення безпеки та стійкості КІ, а також національної безпеки та національної стійкості потребують мобілізації усіх ресурсів держави, що передбачає залучення населення, місцевих громад і неурядових організацій там, де це можливо і необхідно.

У цьому напрямі проводиться значна робота, яка включає, не тільки, наприклад, участь релігійних і волонтерських організацій у реагуванні на кризові ситуації, у ліквідації наслідків безпекових криз, наданні первинної допомоги постраждалим і т. інш., а й отримання інформації від населення та інших акторів про підозрілу поведінку певних осіб,про безпекову ситуацію на місці подій тощо. Тобто, насправді у таких країнах йдеться саме ***про партнерство, яке включає взаємодію та повноцінний процес ОІ*** між державними органами та населенням, а також іншими акторами, тоді як у національній практиці та у відповідних нормативно-правових документах мова переважно йде про оповіщення та евакуацію населення у випадку надзвичайних ситуацій.

Наведені вище міркування щодо можливих підходів до організації КДВОІ при захисті КІ узагальнені у вигляді таблиці та діаграми у додатках 1 та 2.

7. Про деякі особливості обміну інформації та взаємодії на стадії первинного реагування на безпекові інциденти

Один із важливих висновків, зроблених за результатами аналізу змін у глобальному безпековому середовищі та усвідомлення рівня і характеру загроз та ризиків для КІ, полягає у тому, що з огляду на спектри існуючих в сучасному світі загроз ***визнається за доцільне створювати систему захисту КІ*** держави (включаючи системи реагування) ***з урахуванням усіх видів фізичних загроз і кіберзагроз***.

Виходячи з цього висновку, у випадку коли реалізація загрози викликає безпековий інцидент, пов’язаний з КІ, є підстави передбачати, що ***підрозділи первинного реагування можуть зіткнутися з необхідністю дій у будь-яких умовах, спричинених впливом небезпечних факторів будь-якого походження.*** Це означає, що життю і здоров'ю особового складу таких підрозділів, а також його спроможності виконати поставлене завдання може загрожувати ціла низка чинників – від загрози застосування зброї з боку терористів до, наприклад, високого рівня радіації або високої концентрації шкідливих речовин у повітрі.

Тому залучення до ***виконання професійних обов’язків у шкідливих умовах має бути чітко врегульоване у відповідних нормативно-правових актах***, у т.ч. в частині, що стосується забезпечення підготовки особового складу таких підрозділів до дій у подібних ситуаціях, надання об’єктивної інформації про дію небезпечних факторів, забезпечення необхідними засобами індивідуального захисту тощо.

При цьому на особливу увагу заслуговують процедури та механізми ОІ на ***стадії первинного реагування, на якій за браком часу далеко не завжди буде існувати можливість швидко встановити причини, характер і передбачити можливі наслідки безпекового інциденту.*** Разом з тим, значною мірою від первинного реагування буде залежати використання можливостей запобігти розвитку безпекових інцидентів у кризові ситуації. У багатьох випадках належний рівень взаємодії та ОІ, інформаційна підтримка дій особового складу підрозділів первинного реагування на тактичному рівні можуть мати вирішальне значення.

ВИСНОВКИ ТА РЕКОМЕНДАЦІЇ

Підбиваючи підсумки розгляду проблем забезпечення координації дій, взаємодії та обміну інформацією при створенні державної системи захисту КІ, — завдання, яке поставлене Указом Президента України "Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року "Про

удосконалення заходів забезпечення захисту об'єктів критичної інфраструктури" від 16 січня 2017 року № 8/2017, можна зробити ряд таких висновків:

1. Оскільки важливою умовою для послідовного та сталого процесу розбудови державної системи захисту критичної інфраструктури є нормативно-правове забезпечення відповідних зусиль, на короткострокову перспективу першочерговим завданням у цій сфері залишається прийняття профільного законодавчого акту про критичну інфраструктуру та її захист у тій редакції, яка відповідає національним інтересам України та загальновизнаним в країнах-членах НАТО та ЄС підходам.
2. Захист, забезпечення безпеки та стійкості критичної інфраструктури потребують якісно нового рівня координації дій, взаємодії та обміну інформацією між усіма суб'єктами (акторами) відповідної діяльності, що обумовлене:
   a. комплексним характером і масштабами самого об'єкту захисту – національної критичної інфраструктури;
   b. більш широким спектром загроз, які слід враховувати при забезпеченні захисту (безпеки) та стійкості критичної інфраструктури, який включає усі фізичні загрози та кіберзагрози;
   c. необхідністю залучення на різних рівнях великої кількості суб'єктів відповідної діяльності (акторів) від вищого політичного керівництва держави, що знаходиться на "вершині" умовної піраміди, і до ЗМІ, місцевих громад, суспільних організацій, населення тощо, що складають "фундамент" такої піраміди;
   d. у разі кризи, пов'язаної з безпекою критичної інфраструктури, необхідністю у мобілізації ресурсів у національному масштабі, тобто тих, які є у розпорядженні державних органів, компаній усіх форм власності, місцевих громад, населення тощо;

е. необхідністю інформувати уряди сусідніх країн, уряди країн-партнерів, спеціалізовані міжнародні організації та структури тощо у разі кризи з можливими транскордонними наслідками.

3. Наявні в Україні системи безпеки та кризового реагування та відповідальні за них міністерства/відомства зосереджені на виконанні завдань, визначених чинними нормативно-правовими актами, які не сприяють формуванню достатньої мотивації для запровадження дієвих процедур і механізмів координації дій, взаємодії та обміну інформацією між системами і на практиці не враховують більш широкого безпекового контексту, що відповідає цілям забезпечення захисту (безпеки) та стійкості критичної інфраструктури.
4. На теперішньому етапі реформування сектору національної безпеки і оборони досягти рівня координації дій, взаємодії та обміну інформацією, адекватного цілям створення державної системи захисту критичної інфраструктури, можна лише шляхом запровадження надвідомчих механізмів та інструментів, включаючи створення або призначення спеціального державного органу, на який покладено координувальні функції на національному рівні.
5. Масштабність та рівень завдань щодо забезпечення захисту (безпеки) та стійкості критичної інфраструктури, вимагають прийняття ефективних рішень на усіх рівнях управління: від місцевих громад і до вищого політичного керівництва держави, для чого необхідно створити спеціальну систему (підсистему) інформаційно-аналітичної підтримки процесу прийняття рішень.
6. До числа основних завдань системи (підсистеми) забезпечення інформаційно-аналітичної підтримки процесу прийняття рішень мають увійти завдання щодо підготовки інформації для вищого політичного керівництва держави, а також для населення, причому в обох випадках безпосередня передача первинної інформації

зазначеним користувачам є недоцільною, але внаслідок різних причин.

7. У теперішній ситуації, в якій перебуває Україна, що характеризується складними безпековими, фінансово-економічними та соціально-політичними процесами, оптимальним підходом, як до створення державної системи захисту критичної інфраструктури, так і до створення системи (підсистеми) інформаційно-аналітичної підтримки процесу прийняття рішень щодо критичної інфраструктури, можна вважати підхід, оснований на максимально можливому використанні існуючих систем (підсистем) безпеки та кризового реагування, а також ситуаційних, кризових, інформаційно-аналітичних та інших центрів.
8. У процесі інтегрування наявних в Україні ситуаційних, кризових та інформаційно-аналітичних центрів у єдину мережу з метою удосконалення та підвищення рівня обміну інформацією слід спиратися, серед іншого, на найкращу зарубіжну практику, яка базується на запровадженні апробованих циклів підготовки інформації для прийняття рішень, які обов'язково включають стадію аналітичної обробки інформації.
9. З огляду на значну різноманітність ситуаційних, кризових та інформаційно-аналітичних центрів, яка проявляється, серед іншого, у такому:
    a. приналежності до різних секторів критичної інфраструктури;
    b. різних формах власності;
    c. наявності цілого ряду цільових користувачах інформації, що надається;
    d. різному програмному та апаратному забезпеченні тощо

    для створення зазначеної у попередньому пункті національної мережі центрів вже зараз слід розпочати розробку підходів до визначення

оптимальної архітектури такої системи, яка би забезпечувала, між іншим, масштабованість системи, дозволяла об'єднувати диверсифіковані центри у рамках мережі, для чого необхідно поєднати зусилля фахівців з безпеки та IT-спеціалістів, що потребує максимального використання потенціалу академічної та вузівської науки України.

10. Належний рівень обміну інформацією у сфері забезпечення захисту (безпеки) та стійкості критичної інфраструктури є критично важливим для розбудови державно-приватного партнерства, партнерських стосунків між усіма заінтересованими сторонами, включаючи населення, неурядові організації ЗМІ, експертне співтовариство.
11. Внаслідок можливості реалізації широкого спектру загроз (у т.ч. їх комбінацій) життю та здоров'ю особового складу підрозділів (команд) первинного реагування у випадку інцидентів та криз на об'єктах критичної інфраструктури обмін належною інформацією, як при підготовці до первинного реагування, так і під час нього, є життєво важливим для запобігання людським втратам, для зниження негативного впливу на здоров'я людей і довкілля та недопущення переростання безпекових інцидентів у кризи.

Спираючись на зроблені за результатами аналізу висновки та враховуючи передовий зарубіжний досвід у сфері забезпечення захисту (безпеки) та стійкості критичної інфраструктури, можна сформулювати такі рекомендації та пропозиції:

<u>Апарату Ради національної безпеки і оборони України:</u>

1. Розглянути можливість скликання наради за участі представників державних органів (включаючи правоохоронні органи та спецслужби), інших заінтересованих сторін, представлених у робочій групі з розробки законопроекту "Про критичну інфраструктуру та її захист"

для обговорення стану 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, за результатами якого розробити план заходів щодо прискорення виконання зазначеного указу Президента України;

2. З метою забезпечення необхідних умов для взаємоузгодженого реформування національного сектору безпеки і оборони розглянути можливість включення до перспективного плану роботи Ради національної безпеки і оборони України на 2019 рік питання "Про узгодження основних параметрів функціонування державних (національних) систем у сфері національної безпеки і оборони", за результатами розгляду якого передбачити розробку відповідної концепції, а також ряду концептуальних та стратегічних документів, у т.ч. тих, що пов'язані із захистом (безпекою) та стійкістю критичної інфраструктури, а саме:
   - Концепції розробки та запровадження системи взаємоузгоджених концептуальних і стратегічних документів у сфері національної безпеки і оборони та національної стійкості;
   - Концепції проведення оцінки загроз та ризиків для національної безпеки України;
   - Концепції проведення оцінки терористичних загроз Україні;
   - Концепції створення національної мережі ситуаційних центрів;
   - Стратегії забезпечення науково-технологічної підтримки сектору безпеки і оборони України;
   - Глосарію понять і термінів у сфері національної безпеки і оборони.

<u>Міністерству економічного розвитку і торгівлі України:</u>

3. З метою сприяння завершенню розробки законопроекту "Про критичну інфраструктуру та її захист", до 1 квітня 2019 року підготувати конкретні пропозиції щодо організації подальшої роботи

створеної при міністерстві робочої групи з розробки законопроекту, беручи до уваги необхідність урахування отриманих зауважень щодо першої редакції законопроекту та завершення виконання рішення РНБО та указу Президента України щодо захисту критичної інфраструктури.

4. З метою максимального наближення до підходів щодо захисту критичної інфраструктури, запроваджених в країнах-членах НАТО та ЄС, та відповідно до чинного Положення про Міністерство економічного розвитку і торгівлі України рекомендувати міністерству підготувати пропозицію Кабінету Міністрів України щодо організації відповідної експертизи проекту Закону України «Про критичну інфраструктуру та її захист» до його подання на розгляд Верховної Ради України;

Службі безпеки України та Мінінформполітики

5. З метою інформування населення і суспільства, зарубіжних партнерів, та враховуючи необхідність об’єднання зусиль, формування спільного розуміння і запровадження спільних підходів, єдиної термінології у сфері національної безпеки, взагалі, і захисту критичної інфраструктури, зокрема, а також для удосконалення заходів з цивільного контролю над Воєнною організацією і правоохоронними органами держави, розробити рекомендації щодо підготовки "відкритих версій" концептуальних та стратегічних документів у сфері національної безпеки та у першій половині 2019 року в установленому порядку передати ці рекомендації на розгляд РНБО України.

Сергій Кондратов
Відділ енергетичної та техногенної безпеки НІСД

Додаток 1

Таблиця 1. Підходи щодо формування рівнів та визначення суб'єктів взаємодії та ОІ при реагування на кризові ситуації, пов’язані з КІ

Ієрархічні рівні системи ВОІ	**Структурні елементи/суб'єкти НМ СКІАЦ**	**Роль і функції при взаємодії та ОІ (за стадіями циклу підготовки інформації у кризових ситуаціях)**
Політичний рівень	Президент (РНБОУ), Уряд	*Стадії 1 - 2 інформаційного циклу:* • формування запиту на певну інформацію, стратегічне планування заходів та управління ресурсами з метою виконання завдання; *Стадія 6 інформаційного циклу*: • отримання інформації для прийняття рішення; формування наступного запиту.
1-й рівень НМ СКІАЦ	СКЦ національного рівня (наприклад, Головний ситуаційний центр України при РНБОУ, ін.)	*Стадія 6 інформаційного циклу:* • остаточний аналіз інформації, підготовка, розробка і подання у необхідному форматі альтернативних варіантів стратегічних та політичних рішень щодо кризової ситуації; • обмін інформацією з іншими СКЦ національного рівня (наприклад, з СКЦ КМУ, у разі їх створення) - горизонтальний ОІ; • ОІ з 2-м рівнем НМ СКІАЦ – вертикальний ОІ.
Примітка. Незважаючи на необхідність у проведенні обробки, форматування, перевірки, аналізу інформації перш ніж вона потрапить на *політичний рівень,* керівники держави повинні мати диверсифіковані технічні можливості для отримання безпосередньої інформації з місця інциденту.		
2-й рівень НМ СКІАЦ	СКЦ за основними видами загроз у т.ч. СКЦ та ІАЦ таких суб'єктів процесу: • СБУ (АТЦ при СБУ) • МВС (Нацгвардія) • Міненерговугілля • ДСНС • Держатомрегулювання • Міноборони • МОЗ (Державна служба медицини катастроф, екстрена мед. допомога)	*Стадія 5 інформаційного циклу:* • аналіз, оцінка і перевірка даних та інформації; • об'єднання інформації для отримання взаємоузгодженої (наскільки це можливо) картини розвитку кризової ситуації; • підготовка рекомендацій щодо набору варіантів прийняття рішень для виходу із кризи та зменшення наслідків кризи; • ОІ з 1-м та 3-м рівнями (вертикальний); • ОІ на 2-му рівні (горизонтальний); • брифінги для ЗМІ та експертів, інформування населення.
Примітка. Виходячи з чинної НПБ та національного досвіду, саме до цього умовного рівня слід віднести міжвідомчі органи, які утворюють у випадку кризових ситуацій. Як правило, передбачається, що їх діяльність організовується на базі "профільного" для конкретних умов відомства. У випадку криз, пов'язаних з безпекою КІ, створення таких структур вбачається доцільним, починаючи з регіонального (обласного) рівня.		

Ієрархічні рівні системи ВОІ	**Структурні елементи/суб'єкти НМ СКІАЦ**	**Роль і функції при взаємодії та ОІ (за стадіями циклу підготовки інформації у кризових ситуаціях)**
3-й рівень НМ СКІАЦ	СКЦ та ІАЦ державних і приватних компаній (НАЕК «Енергоатом», «Укренерго», «Укргідроенерго», українських АЕС), інформаційні служби правоохоронних органів та аварійних служб відповідного рівня.	*Стадія 4 інформаційного циклу*: • обробка та форматування первинної інформації з тим, щоб представити її у формі, прийнятній для подальшого використання аналітиками, у т.ч. попереднє узагальнення інформації; • внесення інформації до спеціалізованих баз даних; • ОІ з 2-м, 4-м і публічними рівнями (вертикальний); • ОІ на 3-му рівні (горизонтальний).
4-й рівень НМ СКІАЦ	СКЦ та ІАЦ об'єктів та систем критичної інфраструктури, системи моніторингу безпекових характеристик, інформаційні служби правоохоронних органів та аварійних служб відповідного рівня	*Стадія 3 інформаційного циклу:* • збір первинної інформації та подальша її передача інформації різноманітними способами і шляхами з у т.ч.: o від систем моніторингу; o від персоналу та особового складу, від підрозділів первинного реагування на об'єктах КІ згідно з прийнятими процедурами; o від окремих осіб з числа населення (через загальнонаціональні системи аварійного та надзвичайного зв'язку); o від правоохоронних органів, аварійних служб тощо з місця подій тощо; o ОІ з СКЦ та ІАЦ об'єктів і систем КІ – горизонтальний ОІ; o ОІ з 3-м рівнем НМ СКІАЦ і з публічним рівнем – вертикальний ОІ.
Публічний рівень	Населення, ЗМІ, експертне співтовариство	З одного боку, з цього рівня можуть надходити сигнали та первинна (необроблена) інформація щодо загрози або початку кризової ситуації на об'єкті КІ, а з іншого боку, безпека населення є одним з найвищих пріоритетів реагування на кризові ситуації. ЗМІ та експертне співтовариство повинні сприяти цьому процесу, який має включати, не обмежуючись, таке: o передачу інформації на 3-й і 4-й рівні НМ СКІАЦ – вертикальний ОІ; o ОІ зі ЗМІ та експертами, іншими членами спільноти – горизонтальний ОІ.

Додаток 2

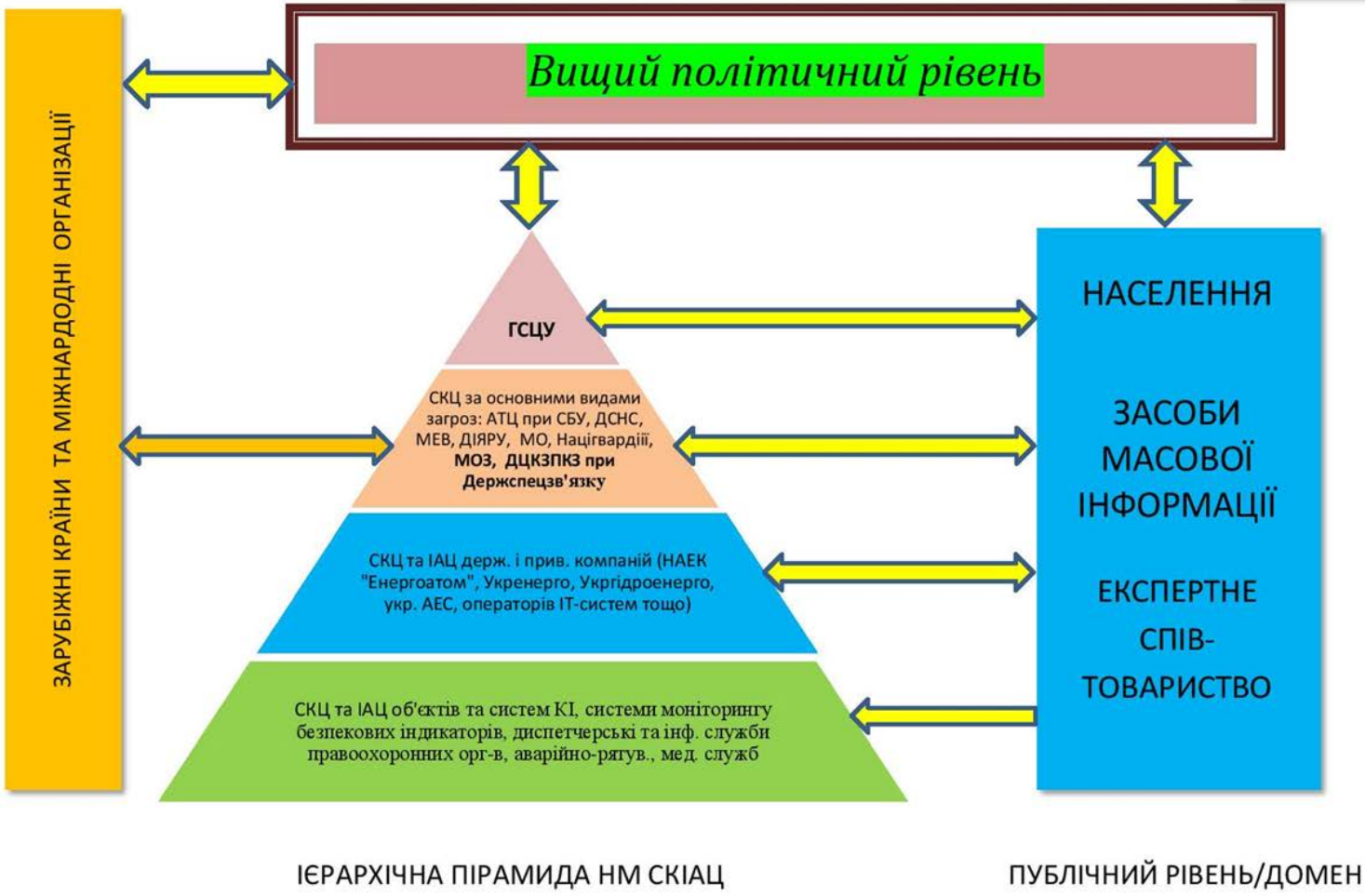

Рис. 3. Загальна картина процесів ОІ у кризових ситуаціях за участі НМ СКІАЦ