# ЗАХИСТ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ТА БЕЗПЕКА ПРОВЕДЕННЯ МАСОВИХ ПУБЛІЧНИХ ЗАХОДІВ


## Анотація

В аналітичній записці розглянуто проблеми забезпечення безпеки проведення масових публічних заходів у взаємозв'язку із захистом критичної інфраструктури. Показано, що особливості зазначених заходів зумовлюють жорсткі вимоги до процедур взаємодії, координації дій та обміну інформацією між усіма суб'єктами процесу. У матеріалі представлено стислий огляд найкращих практик у цій сфері та виокремлено першочергові завдання щодо забезпечення безпеки масових публічних заходів в Україні, враховуючи, що Кабінетом міністрів України у грудні 2017 року прийнято постанову про створення державної системи захисту критичної інфраструктури. Сформульовано ряд практичних рекомендацій для міністерств, відомств та інших державних органів.

# ЗАХИСТ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ТА БЕЗПЕКА ПРОВЕДЕННЯ МАСОВИХ ПУБЛІЧНИХ ЗАХОДІВ

## 1. Вступ

У теперішній час на стан глобальної безпеки впливає ряд негативних процесів, які призвели, зокрема, до значного зростання терористичних загроз. При цьому характер низки резонансних терористичних актів, що були вчинені в останні кілька років, дозволяє стверджувати, що до числа найбільш пріоритетних і складних у роботі правоохоронних та розвідувальних органів, спецслужб різних країн, а також відповідних міжнародних організацій висунулося завдання забезпечення безпеки при проведенні масових публічних заходів (МПЗ)[1], яке безпосередньо пов'язане із захистом критичної інфраструктури (КІ), тобто, із захистом тих різноманітних об'єктів,на яких у той чи інший час може знаходитися велика кількість людей з метою відвідування, відпочинку, участі у розвагах, здійснення покупок, проживання тощо. В США, країні-лідері у розробці передових підходів на цьому безпековому напрямі, зазначені об'єкти відносять до так званого *сектору комерційних об'єктів (*СКО*)*[2]КІ.

Саме об'єкти цього сектору КІ останнім часом все частіше стають мішенями для атак терористів. Теракти під час проведення МПЗ мають давню історію. При цьому останніми десятиліттями повідомлення про них найчастіше надходили з близькосхідного регіону і стосувалися, зокрема, вчинення терактів під час проведення масових релігійних заходів.

Що стосується країн Європи, то загострення безпосереднього збройного протистояння з ІДІЛ, пов'язаної з цим сирійської кризи на фоні продовження боротьби з Аль-Каїдою та іншими терористичними організаціями, а також

---

[1]Для цілей даної публікації термінів у національному законодавстві до цієї ж категорії віднесемо заходи, які проводяться на високому політичному рівні (міжнародного та національного рівнів), в яких чисельність безпосередніх учасників може бути порівняно невеликою, тоді як забезпечення проведення таких заходів та їх висвітлення у ЗМІ передбачає багатьох тисяч осіб. Крім того, до місця проведення таких заходів можуть прибувати чисельні протестувальники з багатьох країн світу.

[2]*Commercial Facilities Sector* (див. веб-сайт Міністерства внутрішньої безпеки США: [Електронний ресурс]. – Режим доступу: https://www.dhs.gov/commercial-facilities-sector.

вплив ряду інших збройних конфліктів, призвели до того, що європейські країни, у т.ч. Туреччина, зіткнулася з комплексною проблемою біженців та неконтрольованої міграції, одним із наслідків якої стала інфільтрація як вже діючих членів терористичних організацій, так і потенційних терористів у ці країни. Одночасно з цим у західних країнах, включаючи США, активізувався процес поширення екстремістських поглядів та радикалізації певних груп мусульманського населення, що також зробило свій внесок у збільшення окремих видів терористичних загроз.

У контексті теми даного матеріалу привертає увагу одна з особливостей теперішнього етапу трансформації тероризму, яка полягає у тому, що разом із процесом зростання загроз, пов'язаних із зловмисним використанням високих технологій (насамперед, ІТ), для певної категорії терористів та екстремістів найбільш прийнятними виявляються такі способи нападів, сукупність яких вже отримала у західних ЗМІ досить влучну назву ***лоу-кост тероризму***[3], пов’язану з тим, що витрати терористів на підготовку та здійснення цілої низки резонансних терактів були мінімальними.

Тероризм у всіх його проявах серйозно загрожує і Україні, оскільки на сході нашої країни все ще триває антитерористична операція, яка супроводжується актами тероризму і диверсіями. При цьому внаслідок бойових дій у незаконний обіг потрапляє велика кількість зброї та вибухівки. Протидія тероризму та екстремізму в нашій країні відбувається на фоні складного і часом болісного процесу реформування сектору безпеки. За таких умов деякі політичні сили не залишають планів посилити в українському суспільстві атмосферу ворожнечі, розбрату та нетерпимості для підриву основ державності України, що, безумовно,сприяє зростанню терористичних загроз.

Разом з тим слід відзначити, що навіть у надскладній безпековій ситуації нашій країні вдавалося проводити на достатньо високому рівні МПЗ, серед

[3] Від англ. *low-cost* – дешевий, маловитратний. Маються на увазі такі терористичні акти, як наїзди транспортними засобами на скупчення людей під час святкувань, на ярмарках і концертах, у туристичних зонах, зонах відпочинку і розваг, або напади на мирних громадян із застосуванням холодної або стрілецької зброї на вулицях міст, залізничних та автобусних станціях, кіноконцертних залах, торгових закладах тощо.

яких окремим рядком стоїть пісенний конкурс Євробачення–2017. Але, без сумніву,протидія тероризму вимагає неперервної напруженої роботи у т.ч. за такими напрямами, як моніторинг та аналіз загроз і ризиків, вивчення та аналіз змін у тактиці та стратегії терористів, запровадження нових підходів,у т.ч. технологічних, для зменшення загроз та ризиків тероризму, а також вивчення та аналіз досвіду інших країн.

Це особливо важливо усвідомлювати з огляду на вже заплановані міжнародні заходи, які вже найближчим часом буде проводити Україна. Крім того, ретельного вивчення та аналізу потребують нові тенденції, які останнім часом спостерігаються в діях терористів, зокрема у поширенні терористичної «практики» використання транспортних засобів та звичайних видів зброї (холодної та стрілецької, вибухівки) під час проведення МПЗ та у місцях масового перебування людей (наприклад, туристичних пішохідних зонах).

Безпека СКО[4] КІ, і пов'язана з нею безпека МПЗ охоплюють величезне коло питань і потребують спеціальних поглиблених досліджень. У даній ж аналітичній записці акцент зроблено на першочергових заходах на цьому напрямі, виходячи з того, що на даний момент Україна тільки-но робить перші кроки на шляху до створення державної системи захисту КІ[5], відсутність якої може негативно впливати на безпеку проведення МПЗ. При підготовці публікації, зокрема рекомендацій, було використано передовий зарубіжний досвід,результати проведених у НІСД у 2014-17[6] рр. досліджень щодо захисту КІ, висновки з попереднього аналізу результатів командно-штабного навчання національного рівня *CORE 2017*з питань стійкості критичної енергетичної структури України[7],а також деякі уроки, винесені з аналізу недавніх резонансних терактів.

---

[4] За відсутності національної нормативно-правової бази захисту критичної інфраструктури, в якій мають бути визначені сектори критичної інфраструктури, а також сформульовані критерії віднесення інфраструктурних об'єктів до КІ, у записці використовуються терміни, запозичені (у перекладі) із законодавства США.

[5] Кабінет Міністрів України 6 грудня 2017 року затвердив «Концепцію створення державної системи захисту критичної інфраструктури» http://ua.interfax.com.ua/news/economic/467621.html

[6]Див., наприклад,*Developing the Critical Infrastructure Protection System in Ukraine:* monograph / [S.Kondratov, D. Bobro, V. Horbulin et al.]; general editor O. Sukhodolia. – Kyiv : NISS, 2017.

[7]Детальніше див. повідомлення на сайті НІСД: [Електронний ресурс]. – Режим доступу: http://www.niss.gov.ua/articles/2718/ .

## 2. Особливості забезпечення безпеки при проведенні масових публічних заходів

Слід зазначити, що особливості забезпечення безпеки при проведенні МПЗ мають фундаментальну природу, що зумовлено самим характером таких заходів, які передбачають ***надання великій кількості людей безперешкодного або мінімально контрольованого доступу до об'єктів критичної інфраструктури.*** Як відзначає Дейв Крефтон (*DaveCrafton*) з Офісу захисту інфраструктури Міністерства внутрішньої безпеки США: «*Сектор комерційних об'єктів включає в себе переважним чином об'єкти, **які знаходяться у приватній власності** і де можуть перебувати великі кількості людей, що ставить перед власниками і операторами [цих об'єктів] завдання досягти тонкого, але необхідного балансу між запровадженням принципу відкритого публічного доступу та безпекою*»[8]. На його думку, ***серйозність виклику полягає у тому, що необхідно забезпечувати безпечне і стійке та, водночас, прибуткове функціонування сектору***, в якому ефективні та необструкційні[9] програми управління ризиками повинні формувати позитивне відчуття безпеки у населення та створювати сприятливе для ведення бізнесу середовище, яке здатне приваблювати кадри, орендарів та клієнтів[10].

Запровадження збалансованого підходу до участі сил правопорядку та охоронних служб у МПЗ є доволі складним завданням. В залежності від конкретної ситуації, з одного боку, наявна ***присутність поліцейських і охоронців, особливо озброєних, може негативно впливати на загальну атмосферу проведення МПЗ*** і викликати, щонайменше у частини присутніх

---

[8] Див. *Securing the Commercial Facilities Sector: It Starts With People*, the CIP Report, December 2009.[Електронний ресурс]. – Режим доступу: https://www.hsdl.org/?view&did=791103

[9] Від англ. *non-obstructive*. Маються на увазі ті методи та інструменти управління ризиками, які не заважають і не наносять шкоди функціонуванню об'єкту в такому режимі, що відповідає призначенню цього об'єкту.

[10] Вплив наявності такого середовища на ведення бізнесу підтверджений безпосередніми дослідженнями. Див., наприклад, *Shopping in an Age of Terrorism: Consumers Weigh the Risks Associated with Online Versus In-Store Purchases.* Carolyn E. Predmore, Janet Rovenpor and Alfred R. Manduley (Manhattan College), Tara Radin (Wharton School of Business, University of Pensylvania). TheCIPReport, December 2009. [Електронний ресурс]. – Режим доступу: https://cip.gmu.edu/wp-content/uploads/2013/06/89_The-CIP-Report-December-2009_Commercial-Facilities.pdf

і в суспільстві, тривожні настрої. Передбачаючи це,власники та/або оператори об’єктів, що розраховують на економічні здобутки в результаті проведення МПЗ, можуть не проявляти належної зацікавленості у вжитті безпекових заходів у обсязі, що випливає з оцінки загроз та ризиків,а також у демонстрації присутності на об’єкті поліцейських та представників служб безпеки. З іншого боку, слід ураховувати, що невдовзі після резонансних терористичних актів або, коли в суспільстві циркулює інформація про ймовірні терористичні напади,реакція на додаткові безпекові заходи у глядачів, безпосередніх учасників МПЗ може бути, у цілому, позитивною. Крім того, у режимі підвищеної терористичної загрози ***наочна присутність поліції та сил безпеки й демонстрація їхньої готовності до реагування*** на інциденти можуть ***також спричиняти ефект стримування,*** змушуючи терористів змінювати свої плани або взагалі, відмовлятися від них.

Підготовка і проведення МПЗ, включаючи забезпечення безпеки, потребує, починаючи вже з етапу планування, залучення великої кількості центральних і місцевих органів влади,правоохоронних органів і спецслужб, державних і приватних компаній (у т.ч. власників і операторів об’єктів КІ), а також інших організацій. Відповідно, ***заходи з безпеки повинні бути інтегровані у загальний план проведення МПЗ***. За таких умов питання ***забезпечення координації дій, взаємодії, а також належного обміну інформацією між усіма правоохоронними органами і спецслужбами держави та службами безпеки державних і приватних компаній є критично важливими***.

При цьому, зважаючи на структуру власності, притаманну сектору комерційних об’єктів КІ, ***розвинуте державно-приватне партнерство (ДПП)*** у сфері безпеки, що формується на основі усвідомлення спільних цілей, створення атмосфери взаємної довіри та взаємовигідного обміну інформацією між учасниками процесу, ***є абсолютно необхідною умовою*** як для безпеки КІ загалом, так і для безпеки проведення МПЗ, зокрема.

Безпосередню участь у МПЗ можуть брати до сотень тисяч і, навіть, до кількох мільйонів людей, включаючи глав держав, урядів та міжнародних

організацій, урядовців, політиків, видатних представників культури та спорту тощо (далі – ВІП). Масштаби і важливість МПЗ визначають ***необхідність розповсюдження заходів безпеки далеко за межі офіційного місця/місць проведення МПЗ***, (далі для стислості – офіційне місце). У зв'язку з цим план забезпечення безпеки МПЗ у деяких країнах умовно поділяють на його *антитерористичну і контртерористичну* частини[11], перша з яких виконується, головним чином, на місці проведення МПЗ, а друга, в основному, - за його межами.

У процесі підготовки і проведення МПЗ як правило виникає питання щодо необхідності забезпечення контролю доступу як до самого місця проведення заходу, так і до окремих його зон. Рішення щодо цього мають прийматися, виходячи з оцінки загроз та ризиків. У разі визнання необхідності здійснення контролю доступу при плануванні відповідних процедур важливо забезпечити ***збалансований підхід до визначення рівнів контролю доступу***(у т.ч. у випадку створення на місці проведення МПЗ кількох зон з різними рівнями контролю), враховуючи той факт, що при надмірно високому рівні суттєво збільшується час проходження через організовані пункти контролю, в результаті чого поблизу них ймовірне утворення скупчень людей, що можуть стати для терористів альтернативними мішенями у разі невдалої спроби подолати систему безпеки на місці безпосереднього проведення МПЗ[12]. З іншого боку, зрозуміло, що

[11] Хоча це ще й не стало загальновизнаним, але у протидії тероризму бачається доцільним розрізняти такі терміни, як *антитерористична діяльність* і *контртерористична діяльність*, як це вже робиться у США. У даному контексті під першим терміном розуміють виконання *захисних заходів, спрямованих на зменшення уразливості осіб і власності, запобігання терористичним актам на офіційному місці проведення заходу і обмежені заходи з реагування та стримування, які виконують місцеві озброєні формування*. Тоді як під *контртерористичною діяльністю* розуміють *вжиття заходів державними органами та відомствами, включаючи правоохоронні та інші силові структури, корпораціями тощо, з метою нейтралізації терористичних організацій, попередження вчинення ними терактів*. (див., наприклад, [Електронний ресурс]. – Режим доступу: http://www.ctrrc.org/glossary/ ).

[12] Саме така ситуація, очевидно, трапилася 13 листопада 2015 р. під час скоординованих терористичних атак у Парижі, коли одна з груп терористів у кількості трьох осіб не змогла потратити на стадіон, де проходив товариський матч між футбольними збірними Франції та ФРН, на якому були присутні президент Франції Ф. Оланд та міністри закордонних справ Франції та Німеччини Л. Фабіус та Ф.-В. Штайнмайєр. Три терористи підірвали себе поблизу стадіону, в т.ч. один з них - біля пункту контролю на вході до стадіону (див. [Електронний ресурс]. – Режим доступу: http://www.bbc.com/news/world-europe-34822265 ). У даному випадку завдяки створеній системі безпеки МПЗ один з планів терористів було зірвано, але, тим не менше, ця група терористів обрала альтернативні об'єкти для нападів, в результаті яких, все ж таки, загинули люди.

недостатній рівень контролю збільшує шанси зловмисників реалізувати свої плани.

Особливе місце з точки зору безпеки МПЗ займають такі заходи, які проводяться просто неба, а саме фестивалі, карнавали, паради, відзначення релігійних свят і т.д. Для них достатньо типовою є відсутність зовнішніх кордонів (периметру) проведення та видимих фізичних бар'єрів, коли подія ***відбувається практично у відкритому середовищі та охоплює достатньо велику територію***. На безпеку проведення таких заходів серйозно впливають безпекові умови на прилеглих до місця проведення МПЗ територіях та об'єктах[13].

Під час МПЗ в обмежений проміжок часу на обмеженій території може перебувати велика кількість людей, включаючи ВІП, що накладає особливі вимоги на забезпечення їх перевезення та створює серйозні ***навантаження на транспортну інфраструктуру*** (особливо, на окремі вузлові та пересадочні пункти, і на кінцеві пункти призначення) як перед початком заходу, так і після його завершення[14].

## 3. Проблеми забезпечення безпеки МПЗ на початковому етапі створення системи ЗКІ

В Україні ще тільки розпочато процес створення єдиної системи ЗКІ, яка має забезпечувати захист віднесених до КІ об'єктів і систем, включаючи сектор комерційних об'єктів, від усіх видів загроз та їх комбінацій. Одним із головних напрямів відповідної діяльності вбачається інтегрування існуючих в країні національних/державних систем, призначених у теперішній час для реагування ***лише на певні види загроз та ризиків***, круг яких окреслений чинними нормативно-правовими документами.

Як довгострокову ціль слід розглядати створення єдиної інтегрованої (по вертикалі і горизонталі) системи захисту і забезпечення стійкості КІ. Наразі

[13]Саме недостатність заходів з безпеки у готелі «Мандалай Бей» (м. Лас-Вегас, США) дозволила щоб С. Паддоку (*S.Paddock*) кілька днів безперешкодно проносити до номерустрілецькузброю (загалом 23 одиниці)танабоївчинити 2 жовтня 2017 р. масове вбивство присутніх на пісенному фестивалі, який проходив неподалік від готелю.

ж, в Україні, існують значні прогалини та неузгодженості у планах і процедурах координації дій, взаємодії та обміну інформацією (КДВОІ) між створеними для цілей захисту та кризового реагування національними/державними системами та їх елементами. З іншого боку, найбільш жорсткі вимоги до КДВОІ випливають із забезпечення готовності та стійкості стосовно комплексних загроз та криз та при організації та проведенні МПЗ.

Як показує досвід тренувань і навчань, у т.ч. національного рівня (наприклад, *CORE 2017*) суб'єкти забезпечення функціонування окремих систем, як правило, достатньо добре усвідомлюють свої повноваження, функції та сфери відповідальності щодо реагування на загрози і ризики певного типу (у рамках «своєї системи»), але навіть розгляд гіпотетичних ситуацій, які потребують одночасної активації різних систем (випадок комплексних загроз), часто виявляє неузгодженість підходів до розв'язання проблем КДВОІ у представників різних систем, не кажучи вже про реальні інциденти та кризи.

Це стає зрозумілим, якщо взяти, наприклад, випадок загрози акту ядерного (або радіаційного) тероризму. Реалізація такої загрози вимагає одночасного реагування кількох систем, а саме:*Єдиної державної системи цивільного захисту*[15];*Єдиної системи запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків*[16];*Державної системи фізичного захисту*[17].Натомість, аналіз документів, які врегульовують функціонування кожної з них, показує, що їхні плани і процедури КДВОІ, значною мірою, розраховані на проведення автономних заходів[18], на реагування лише на «власні» загрози та ризики. Цей висновок підтверджується тим, що терміни, а також визначені положеннями процедури і критерії запровадження режимів функціонування вказаних систем жодним чином не узгоджені між собою, що робить неможливою ефективну

[15] Положення затверджене постановою КМУ від 09.01.2014 р. № 11.
[16] Положення затверджене постановою КМУ від 15.08.2007 р. № 1051.
[17] Порядок функціонування затверджений постановою КМУ від 21.12.2011 р. №1337.
[18] У сенсі взаємодії з іншими державними/національними системами.

взаємодію між системами як у процесі забезпечення готовності до реагування на комплексну кризу, такі і під час самої кризи.

Таким чином, нормативно-правові акти, що врегульовують функціонування зазначених систем, поки що відображають переважно відомчі підходи державних органів, на які покладена відповідальність за їх роботу, ще одним із наслідків чого, як правило, є обмеженість функціональності цих систем зверху рівнем відповідального органу влади і неконкретні формулювання тих положень, що мають визначати процедури і механізми КДВОІ на надвідомчому рівні, у т.ч. й ті, що стосуються інформування вищого політичного керівництва держави та інформаційно-аналітичної підтримки процесу прийняття політичних рішень.

Внаслідок своїх масштабів, уразливості до усіх видів загроз і ризиків, резонансу, яким супроводжуються будь-які безпекові інциденти під час таких подій, процедури і механізми КДВОІ є ключовими питаннями, що мають бути вирішені при підготовці до МПЗ та їх проведенні.

З огляду на структуру власності сектору комерційних об'єктів КІ (СКО КІ), вирішальну роль у забезпеченні належного рівня КДВОІ відіграє надійне ДПП, розвиток і зміцнення якого є одним з основоположних принципів створення національних систем захисту і забезпечення стійкості КІ у розвинутих країнах світу[19].Важливість ДПП визнається і на міжнародному рівні, наприклад, в офіційних документів таких організацій, як МАГАТЕ[20] і ФІФА[21].

Що стосується України, то звернення до бази даних національного законодавства ***України показує, що правове регулювання ДПП в Україні обмежене майже виключно економічною сферою***. Дійсно, хоча відповідно

[19] У США забезпечення партнерства, насамперед між державою та приватним сектором, віднесено до семи основоположних принципів виконання чинного *Плану захисту національної інфраструктури 2013* (*NIPP 2013: Partnering for Critical Infrastructure Security and Resilience*)
https://www.dhs.gov/publication/nipp-2013-partnering-critical-infrastructure-security-and-resilience

[20] *Nuclear Security Systems and Measures for Major Public Events*, IAEA. Nuclear Security Series No. 18. Implementing Guide. International Atomich Energy Agency, Vienna, 2012.

[21] *FIFA Stadium Safety and Security Regulations*, Fédération Internationale de Football Association, Zurich, Switzerlandта*Football Stadiums.* Technical recommendations and requirements. 5th edition 2011, Fédération Internationale de Football Association, Zurich, Switzerland, [Електронний ресурс]. – Режим доступу*:* www.FIFA.com

до профільного Закону України «*Про державно-приватне партнерство*»[22] ряд сфер застосування ДПП охоплює деякі види діяльності, які є критично важливими для населення, суспільства і держави, але у законі жодним чином не згадані ті напрями ДПП, що мають пряме відношення до забезпечення національної безпеки, зокрема до захисту КІ, протидії тероризму та організованій злочинності.

Крім того,в Україні не повністю врегульовано питання взаємодії органів державної влади з населенням, неурядовими організаціями, експертним співтовариством і ЗМІ. Якщо розглянути, наприклад, нещодавно прийняту Урядом постанову «*Про затвердження Положення про організацію оповіщення про загрозу виникнення або виникнення надзвичайних ситуацій та зв'язку у сфері цивільного захисту*»[23], то, відзначаючи наявність в ній чітких положень, які встановлюють, серед іншого, процедури і механізми інформування населення на об'єктах та у місцях масового перебування людей, важливо відмітити, що згадане має відношення лише до проблематики цивільного захисту. У документі не розглядаються надзвичайні ситуації, що можуть виникнути внаслідок соціально-політичних заворушень, кібер- та терористичних атак тощо, коли критично важливою стає взаємодія з іншими державними системами. Відповідно, згідно з цією постановою, Єдина державна система цивільного захисту не має жодних завдань і у випадку, наприклад, терористичного акту при проведенні МПЗ.

Крім того, в умовах процесу децентралізації державного управління, становлення громадянського суспільства в Україні, у т.ч. у формі розвитку волонтерських рухів, поки що в нашій країні явно недооцінена роль місцевих громад, неурядових організацій (у т.ч. релігійних), добровільних об'єднань громадян у кризовому реагуванні, забезпеченні стійкості об'єктів, що мають бути віднесені до КІ. Якщо ж звернутися до досвіду західних країн, то саме у

---

[22] Закон України «Про державно-приватне партнерство» http://zakon0.rada.gov.ua/laws/show/2404-17/paran197#n197

[23] Постанова Кабінету Міністрів України "*Про затвердження Положення про організацію оповіщення про загрозу виникнення або виникнення надзвичайних ситуацій та зв'язку у сфері цивільного захисту* " № 733, редакція від 27.09.2017 [Електронний ресурс] – Режим доступу:http://www.kmu.gov.ua/control/ru/cardnpd?docid=250311065

цих питаннях переліченим суб’єктам процесу кризового реагування відведені важливі ролі, особливо у пост-кризовий період.

Підсумовуючи попередні міркування можна сказати, що в Україні наявні системи кризового реагування та забезпечення безпеки (захищеності) певних категорій інфраструктурних об’єктів ***не забезпечують належних умов у таких важливих напрямах діяльності щодо захисту КІ та підвищення її стійкості:***

1. Розвиток ДПП в цій сфері;
2. Планування і перевірка планів кризового реагування на безпекові інциденти і кризи комплексного характеру;
3. Об'єднання зусиль населення, суспільства і держави для забезпечення належного рівня захисту та стійкості КІ.

Згадане вище безпосередньо впливає на здатність забезпечувати безпеку при проведенні МПЗ на об’єктах СКО КІ. У даній записці основну увагу приділено першим двом напрямам, але це зовсім не означає другорядність проблематики об’єднання зусиль з метою підвищення рівня захисту та стійкості КІ.

## 4. Передовий досвід і приклади найкращої практики

Відповідно до перелічених у попередньому розділі проблемних для України напрямів забезпечення безпеки об’єктів, які мають бути віднесені до КІ, нижче йдеться про передовий досвід та найкращу практику в контексті забезпечення безпеки МПЗ і наведено ряд конкретних прикладів.

### 4.1.Розвиток ДПП

Що стосується розвитку і підтримки належного рівня ДПП, у т.ч. у рамках діяльності, спрямованої на захист КІ і забезпечення проведення МПЗ,то, очевидно, що досягнення цієї цілі неможливе без ***створення необхідної нормативно-правової бази***, тобто включення відповідних положень про ДПП у стратегічні та концептуальні документи, законодавчі та нормативні акти України, що мають врегульовувати діяльність у сфері національної

безпеки.

*Приклад 1.*У США ***забезпечення партнерства, насамперед між державою та приватним сектором, включено до семи основоположних принципів виконання чинного Плану захисту національної інфраструктури 2013***[24], прийнятого на виконання Політичної директиви Президента США (*PPD-21*). Ще одним з основоположних принципів діяльності у цій сфері в документі визначене набуття знань про ризики для КІ та взаємозалежності між її елементами. Обмін відповідною інформацією між суб'єктами процесу, в т.ч. у рамках ДПП, є імперативною вимогою для посилення захисту та стійкості КІ, створення атмосфери довіри між усіма залученими сторонами. Що стосується Плану для сектору комерційних об'єктів (*Commercial Facilities Sector-Specific Plan*)[25], то в ньому до найвищого пріоритету (1А) віднесено «*удосконалення офіційних процесів обміну інформацією у рамках ДПП на всіх рівнях; розширення доступу операторів та власників до відповідної розвідувальної інформації; зосередження на питаннях забезпечення двостороннього обміну інформацією щодо загроз*»[26].

Важливість надійного ДПП усвідомлюється не тільки в США, яка започаткувала цей безпековий напрям, але й в інших країнах-членах НАТО і ЄС.

*Приклад 2.*У *Національній стратегії захисту критичної інфраструктури*[27] Німеччини як одне з ключових положень документу[28] зафіксовано ***зобов'язання забезпечувати підхід до захисту КІ на основі співробітництва між державними органами, службами надання допомоги і кризового реагування, приватними операторами та їх асоціаціями,*** науковими і дослідними установами, промисловими компаніями у сфері безпеки, міжнародними та наднаціональними структурами, а також населенням.

Схожі підходи до ДПП з урахуванням національних особливостей застосовуються у більшості країн-членів НАТО та ЄС.

На міжнародному рівні важливість партнерства підкреслена, зокрема, у публікації МАГАТЕ[29], присвяченій забезпеченню фізичної ядерної безпеки під час проведення МПЗ: «У *багатьох випадках важливі публічні заходи*

[24]*NIPP 2013: Partnering for Critical Infrastructure Security and Resilience, Department of Homeland Security*, p.11. [Електронний ресурс]. – Режим доступу: https://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508_0.pdf

[25] Цей секторальний план є додатком до *Плану захисту національної інфраструктури 2013* (див. посилання 24).

[26]*Commercial Facilities Sector-Specific Plan 2015*. An Annex to the NIPP 2013, Ministry of Homeland Security. [Електронний ресурс]. – Режим доступу: https://www.dhs.gov/sites/default/files/publications/nipp-ssp-commercial-facilities-2015-508.pdf

[27]*National Strategy for Critical Infrastructure Protection (*German Federal Ministry of the Interior, 2009*)*

[28]TRENDS IN CRITICAL INFRASTRUCTURE PROTECTION IN GERMANY, Christine EISMANN, German Federal Office of Civil Protection and Disaster Assistance (BBK), Bonn, Germany, [Електронний ресурс]. – Режим доступу: https://www.degruyter.com/downloadpdf/j/tvsbses.2014.9.issue-2/tvsbses-2014-0008/tvsbses-2014-0008.pdf

[29]Див. МАГАТЕ, посилання 20

*проводяться на об'єктах, що перебувають у приватній власності, і організатори заходів залучають власні служби безпеки, які мають працювати разом із державними безпековими органами*». Розроблені МАГАТЕ підходи були апробовані під час проведення наймасштабніших змагань, включаючи Олімпійські ігри.

Про необхідність розвитку партнерства, у т.ч. між державними органами та приватним сектором, йдеться у нормативному документі ФІФА[30], в якому підкреслено, що «*жодне агентство (державне або приватне) невзмозі ефективно зменшити ризики та самостійно забезпечити безпеку проведення спортивних змагань*».

Для розбудови ДПП у передових країнах світу використовують різноманітні інструменти, серед яких важливе місце займають координаційні ради, форуми і платформи, які забезпечують контакти, обмін інформацією, узгодження позицій тощо між усіма заінтересованими сторонами.

Приклад 3: *У США для досягнення належного рівня КДВОІ (в т.ч. рамках ДПП) у сфері захисту та стійкості національної КІ* ***створені секторальні координаційні ради*** *(Sector Coordinating Councils),****урядові координаційні ради*** *(Government Coordinating Councils),****та міжсекторальні ради*** *(cross-sector councils).Зокрема, Урядова координаційна рада здійснює координацію дій залучених до забезпечення безпеки СКО державних органів. Натомість* ***Секторальна координаційна рада здійснює координацію дій операторів і власників об'єктів і систем сектору, які у свою чергу поділені на підсектори****, що мають власні координаційні ради, а також різноманітні робочі групи та професійні об'єднання. При цьому створені робочі групи працюють за конкретними напрямами забезпечення безпеки СКО, у т.ч. такі: кібербезпека, розвідувальна інформація з обмеженим доступом, науково-дослідні дослідження.*

*Приклад 4.У Польщі з метою досягнення необхідного рівня КДВОІ у рамках виконання Національної програми захисту критичної інфраструктури передбачено* ***створення таких форумів: національного рівня, рівня системи (сектору), регіонального рівня***[31]*. При цьому відповідно до державної політики у цій сфері процедури КДВОІ у рамках ДПП не залежать від форми власності об'єкта КІ.*

[30] Див. ФІФА, посилання 21.

[31] The National Critical Infrastructure Protection Programme. [Електронний ресурс]. – Режим доступу: http://rcb.gov.pl/wp-content/uploads/NPOIK-2015_eng-1.pdf (26 March 2013).

Нормативно-правова база розвитку ДПП у сфері безпеки є необхідною, але не достатньою умовою для зрілих партнерських стосунків між державними органами і приватними компаніями при проведенні МПЗ на об'єктах СКО КІ. ***Визнано, що партнерство успішно розвивається, коли партнери поділяють спільні цілі, разом усвідомлюють існуючі загрози та ризики і на цій основі співпрацюють для їх зменшення до прийнятного рівня***. Більш того, згідно з найкращою практикою необхідно розвивати не тільки офіційні, але й особисті стосунки між представниками усіх заінтересованих сторін:

> *Приклад 5.*У США рекомендовано, як найкращу практику, *щоб «ще до того, як станеться природне лихо або інша надзвичайна ситуація,* ***розвивати особисті взаємини з офіційними представниками місцевих безпекових агенцій****… місцевим бізнесом, організаціями місцевих спільнот (релігійними групами, об'єднаннями сусідніх помешкань), а також з державними офіційними особами (мерами, управлінцями міської влади, главами округів, штатів та представниками федеральних органів тощо)».* Визнано, що наявність*«попередньо встановлених стосунків з ключовими особами та обговорення з ними заздалегідь надзвичайних ситуацій і планів буде забезпечувати значно кращі контакти з ними і швидке отримання від них допомоги у разі, якщо надзвичайна ситуація трапиться»*[32].

У вже згаданій настанові МАГАТЕ[33] звернуто увагу на такий важливий напрям у спільній роботі, як ***встановлення чіткого розподілу ролей і відповідальності між державними органами та приватними службами безпеки*** та узгоджене включення дій останніх до загального плану забезпечення безпеки заходу. При цьому має бути забезпечене усвідомлення технічних, операційних та інформаційних можливостей кожного з суб'єктів забезпечення безпеки, а інформація про потенційні загрози та ризики має бути доведена і до організаторів МПЗ та їхніх служб безпеки.

4.2.Плани реагування на кризові ситуації комплексного характеру

У країнах, де запроваджена концепція захисту КІ, відповідні системи призначені для ***забезпечення ефективного реагування на усі види загроз і***

[32]*Managing Major Events: Best Practices from the Field Police Executive Research Forum June 2011, U.S.A.*[Електронний ресурс]. – Режим доступу: www.policeforum.org

[33]Див. посилання 19.

***ризиків, а також на їх можливі комбінації***. Таке комплексне завдання передбачає залучення великої кількості суб'єктів, ефективна взаємодія між якими на усіх стадіях набуває критично важливого значення. При цьому однією із найсерйозніших проблем є ***забезпечення надійної взаємодії на міжвідомчому рівні, у т.ч. між різноманітними системами,*** призначеними для кризового реагування, що ***має відображатися в інтегрованості кризових планів*** як по вертикалі, так і по горизонталі.

В Україні поки що у питаннях кризового реагування та захисту об'єктів, які будуть віднесені до КІ, можна говорити про домінування відомчих підходів, внаслідок чого завдання відповідних державних систем ***обмежуються визначеними національним законодавством наборами загроз та ризиків***. Це неминуче впливає на процес планування взаємодії суб'єктів кризового реагування в нашій країні. При переході на сучасні підходи до кризового реагування та комплексні загрози доцільно враховувати передовий зарубіжний досвід та найкращі практики. Все вищесказане має безпосереднє значення для безпеки СКО КІ та для проведення МПЗ. Нижче кратко викладені деякі приклади найкращої практики з цього питання.

> *Приклад 6*. На даний момент в США існує всеохопна *Національна система планування (НСП)*[34], що забезпечує уніфікований системний підхід ***для усього процесу планування стосовно усіх видів загроз та небезпек***, *а також для усього ланцюга п'яти взаємопов'язаних місій* - ***запобігання, захист, пом'якшення наслідків, реагування та відновлення***[35].

При усій різноманітності МПЗ підготовка до них може бути спланована у т.ч. через***моделювання проведення заходу***.

> *Приклад 7*. У США з 1998 р. використовується так звана ***Модель проведення Особливого з точки зору безпеки національного заходу*** (ОТЗБНЗ)[36], яка передбачає створення ешелонованої системи безпеки, побудованої на основі участі усіх залучених

[34] *National Planning System. FactSheet*,FEMA, U.S. DHS[Електронний ресурс]. – Режим доступу: https://www.fema.gov/media-library-data/1454437367834-69ac2b642e9e34945b903455dcbde679/NPLANS_Fact_Sheet_011916_For508.pdf

[35] Детальніше про Національну систему планування в США див. у публікації С. Кондратов "*Роль планування у забезпеченні захисту та стійкості критичної інфраструктури*".[Електронний ресурс]. – Режим доступу: http://www.niss.gov.ua/articles/2667/

[36] *National Special Security Events: Fact Sheet*.[Електронний ресурс]. – Режим доступу: https://fas.org/sgp/crs/homesec/R43522.pdf

організацій, кожна з яких зацікавлена у виконанні плану забезпечення безпеки. Модель успішно застосовувалася як для проведення масштабних заходів (наприклад, Олімпіада у Солт-Лейк Сіті), так і для малих з точки зору кількості безпосередніх учасників, але складних з точки зору рівня ризиків подій (саміти *G8/20*).

Передовий досвід планування заходів з безпеки МПЗ передбачає розробку та перевірку планів підтримання зв'язку та планів резервування технічних засобів задля забезпечення неперервності зв'язку між агенціями, а також планів забезпечення зв'язку з відомствами та організаціями, що прибувають для надання допомоги. У цьому питанні найкраща практика полягає у *залученні усіх учасників процесу забезпечення безпеки МПЗ до планування відповідних заходів* (див. приклади 8 і 9).

*Приклад 8. МАГАТЕ у своїй настанові*[37] *серед іншого рекомендує:*

- ***призначати одного керівника*** (один орган), який несе відповідальність за загальну фізичну безпеку заходу в рамках виділеного бюджету;
- ***залучати усіх учасників забезпечення безпеки до процесу планування***;
- ***встановлювати графік навчань та тренувальних заходів.***

*Приклад 9.*У настанові з питань правозастосування при плануванні та управлінні безпекою під час проведення МПЗ, підготовленій для Міністерства юстиції США[38], ***стадію попереднього планування рекомендовано розпочинати***, якщо це можливо, ***за 12-18 місяців до дати проведення МПЗ***. На федеральному рівні попереднє планування може починатися, навіть, за 2-3 роки. Як правило, до підготовки, важливих подій національного та регіонального рівнів залучаються численні правоохоронні структури федерального рівня, рівня штатів та місцевого рівня. До інших ключових партнерів відносяться пожежні служби, служби швидкої медичної допомоги, транспортні компанії, організації, відповідальні за суспільні роботи, агенції з охорони здоров'я та інші агенції, а також приватний сектор – підприємства, які зазнають вплив внаслідок проведення МПЗ, а також приватні безпекові компанії.

При плануванні заходів безпеки для МПЗ важливим моментом є чіткий розподіл повноважень і відповідальності, закріплений у відповідних документах національного рівня. Для планомірної підготовки до важливих подій, включаючи ОТЗБНЗ, має бути розроблена процедура та критерії віднесення тих чи інших заходів до зазначених категорій.

[37] Див. посилання 19.

[38] Edward Connors «*Planning And Managing Security For Major Special Events: Guidelines for Law Enforcement»,*March 2007, Institute for Law and Justice Alexandria, *Virginia,* [Електронний ресурс]. – Режим доступу: www.ilj.org

*Приклад 10.*Для забезпечення процесу планування МПЗ урядові структури повинні визначити події, які потребують найвищої уваги з боку компетентних органів. Наприклад, ***у США Міністр внутрішньої безпеки несе відповідальність за визначення переліку ОТЗБНЗ***[39]. Президентською директивою встановлено, що Секретна служба США *(SecretService)*є відомством відповідальним за розробку та виконання оперативного плану безпеки для ОТЗБНЗ. ФБР (*FBI*) є провідним федеральним відомством у питаннях кризового управління, контртерористичних заходів, визволення заручників та розвідки, а Федеральне агентство з питань управління у надзвичайних ситуаціях (*FEMA*) відповідає за управління процесом ліквідації наслідків (операції з реагування та відновлення функціонування).

Безпека МПЗ, крім того, що такі заходи проводяться на об'єктах і територіях, що відносять до КІ, напряму залежить і від виконання життєво важливих функцій і доступу до життєво важливих ресурсів, що здійснюють інші об'єкти і системи КІ. Найкраща практика передбачає урахування відповідних загроз та вжиття заходів при плануванні безпеки проведення МПЗ.

*Приклад 11.*Відповідно до прикладів найкращої практики в США відповідальне за безпеку МПЗ відомство має координувати з партнерами і переглядати плани безпеки об'єктів КІ, пошкодження яких може загрожувати безпеці при проведенні МПЗ (місцеві системи водопостачання, водообробки, системи електропостачання, комунікаційні та комп'ютерні мережі, каналізаційні системи тощо)[40].

Плани забезпечення безпеки МПЗ, у т.ч. плани і процедури реагування на безпекові інциденти повинні постійно удосконалюватися, виходячи з аналізу реальних подій, або за результатами ***тренувань і навчань, які мають проводитися на регулярній основі на усіх рівнях управління.*** Недостатньо розвинута практика тренувань і навчань, особливо високого рівня,робить об'єкти КІ уразливими до безпекових інцидентів і розвитку криз комплексного характеру.

До кращої практики за напрямом підготовки персоналу, особового складу, волонтерів та населення до МПЗ можна віднести насамперед таке:

- використання різноманітних підходів до навчання і тренування – від онлайн курсів до командно-штабних та повномасштабних навчань (у т.ч. моделювань терористичних актів) національного рівня;

[39] Див. посилання 39.
[40] Див. посилання 41.

- участь у відповідних заходах представників від усіх залучених сторін;
- проведення занять для підготовки до конкретного МПЗ, у т.ч. щодо дотримання прав протестувальників, використання спеціального обладнання для боротьби із заворушеннями, командні оперативні дії, безпека місця проведення МПЗ тощо[41];
- тренування за спеціальними напрямами безпеки, а саме тактики управління натовпом, загрози використання небезпечних матеріалів (ХБРЯ-матеріалів[42]), використання захисного оснащення[43];
- проведення навчань із власниками/операторами об'єктів СКО КІ.

Попередня підготовка персоналу та особового складу є критично важливою для забезпечення готовності до МПЗ, оскільки, як правило, для таких заходів мобілізуються значні ресурси у т.ч. шляхом залучення (відрядження) правоохоронців з других відомств та регіонів, що без належного навчання і знайомства з партнерами може значно ускладнювати КДВОІ під час МПЗ. У таких випадках до найкращої практики можна віднести використання ***онлайн курсів для навчання поліції та інших правоохоронних органів***[44]**.**

## 5. Огляд деяких конкретних організаційно-технічних підходів, і рішень, визнаних найкращою практикою

У даному розділі представлений стисле зведення деяких практичних підходів, рішень, тактик і рекомендацій, що стосуються, головним чином, оперативного рівня і випливають із кращих практик зарубіжних правоохоронних органів.

[41] Див. посилання 41.
[42] Хімічних, біологічних, радіоактивних та ядерних матеріалів.
[43] Див. посилання 41.
[44] Такий підхід було використано поліцією Торонто (Канада) при підготовці до Саміту G-20 2010 року. Див. *Managing Major Events: Best Practices from the Field Police Executive Research Forum June 2011, U.S.A.*

*Таблиця1*

## Огляд найкращих практик

| ***Загрози, ризики та обумовлені ними завдання*** | ***Тактики, рішення, підходи*** | ***Країни (місця), інші примітки*** |
|---|---|---|
| Оцінка загроз/ризиків застосування вибухових пристроїв та начинених вибухівкою транспортних засобів | Згідно з результатами дослідження[45] кількість жертв від підриву вибухових пристроїв дуже сильно залежить від щільності скупчень людей та від конкретної ситуації, і у деяких випадках більшу загрозу становитимуть так звані «пояси шахідів», ніж транспортні засоби завантажені вибухівкою. | Висновки були прийняті до уваги при реконструкції міжнародного аеропорту (LAX) в Лос-Анджелесі (США) |
| Загроза підриву транспортних засобів, завантажених вибухівкою | У відповідь на розвідувальні дані майданчик для паркування автофургонів винесено за межі проведення ярмарок | США, округ Сан-Дієго (Каліфорнія). |
| Застосування вибухових пристроїв, насильницькі дії проти правоохоронців | Біля місць проведення МПЗ заварюють каналізаційні люки, видаляють металеві та бетонні урни для сміття або замінюють їх на пересувні пластмасові на колесах, видаляють автомати/пристрої для видачі газет та інших друк. матеріалів, оскільки вони можуть бути використані для розміщення вибухових пристроїв або для нападу на правоохоронців і для пошкодження майна. | США, Канада |
| Критичне навантаження на транспортні хаби (транспортну інфраструктуру) | Створення віддалених парковок, зупинок для транспорту, анонсований графік руху спеціально виділеного транспорту | США |
| Підриви вибухівок на вокзалах, станціях, портах і аеропортах | Рекомендовано приділити серйозну увагу камерам для зберігання речей, які можуть бути «ідеальними місцями» для розміщення вибухових пристроїв | США |
| Використання транспортних засобів для здійснення наїзду на скупчення людей, місця напруженого вело- та пішохідного трафіку | ○ підвищена увага до інцидентів з вантажними автомобілями;<br>○ повна заборона проїзду важкого транспорту або, при логістичній необхідності, прокладення його маршрутів, що виключають швидке прискорення;<br>○ використання спеціальних перепусток;<br>○ встановлення у пішохідних зонах важких автомобілів, а також засобів для запобігання несанкціонованому пересуванню транспорту[46]:<br>– протитаранних пристроїв,<br>– обмежувальних стовпчиків на доріжках,<br>– натягнутих на певній висоті тросів тощо;<br>○ вжиття інших заходів:<br>– при проектуванні нових вело- та пішохідних доріжок використання | США, а також Франція, Німеччина та деякі інші країни ЄС |

[45] Terry L. Schell, Brian G. Chow, and Clifford Grammich, *Designing Airports for Security: An Analysis of Proposed Changes at LAX*. Public Safety and Justice. RAND Co.https://www.rand.org/pubs/issue_papers/IP251.html

[46] David Biello,*Is High-Tech Security at Public Events Counterproductive*? [Електронний ресурс]. – Режим доступу: https://www.scientificamerican.com/article/how-to-better-protect-public-events/

| | | |
|---|---|---|
| | трас«змієподібної» форми;<br>– використання транспортних засобів з автоматичними системами гальмування. | |
| Загроза застосування вибухівки та/або стрілецької зброї | Прохід на місце проведення заходу тільки через контрольовані пункти пропуску (застосування рамок), біля яких передбачити додаткові заходи, оскільки ймовірні черги самі можуть стати мішенями для нападів | США, Німеччина, Франція |
| Загрози, пов'язані із порушенням встановленого зонування на місці проведення МПЗ (загрози для ВІП) | Ретельна перевірка посвідчень та допусків, у т.ч.:<br>○ забезпечення чіткого усвідомлення різниці між «квитком» та «посвідченням особи, що має допуск»;<br>○ запобігання випадкам формальної перевірки повноважень правоохоронців та приватних охоронців[47] | Рекомендація Секретної служби США |
| Загроза масових заворушень[48] | Використання *Ванкуверської моделі*[49] управління натовпом, яка передбачає більш м'які та гнучкі методи, включаючи:<br>○ входження поліцейських в уніформі в контакт з натовпом на ранніх стадіях його формування з метою запобігання зростанню агресивності;<br>○ використання піших правоохоронців, правоохоронців на велосипедах, мотоциклах, гіробордах, на конях тощо у різних місцях проведення МПЗ;<br>○ звернення підготовлених до цього співробітників до натовпу і пояснення ролі правоохоронців, спроби встановити контакт;<br>○ забезпечення «видимості» поліцейських у «легкому» оснащенні та наявність «важкого» оснащення «під руками»;<br>○ вивчення, урахування та попередження застосування тактик збурення натовпу (звуковий вплив, провокування бігу в певному напрямі, інфільтрація груп осіб у натовп з подальшим переодягненням на націпленням масок);<br>○ звернення до підприємців у зонах ймовірного ризику за допомогою та з рекомендаціями закрити заздалегідь заклади та/або припинити продаж алкогольних напоїв | Канада, США |
| ***Втома та нервове перенапруження особового складу*** | Забезпечення логістичної підтримки роботи правоохоронців під час МПЗ, у т.ч.:забезпечення водою, продуктами та місцем для відпочинку. | США, Канада |
| ***Завдання інформування у режимі онлайн особового складу, який працює «на*** | Утворення єдиного центру управління безпекою МПЗ і «відрядження» його представників, старших офіцерів, «на | США, Канада |

[47] 19 грудня 2016 р. вбивця посла РФ Карлова в Анкарі (Туреччина) Мевлют Мерт Алтинташ (тур. *Mevlüt Mert Altıntaş*) пройшов на офіційну презентацію, показавши значок та недійсне посвідчення поліцейського.

[48] Див. посилання 49.

[49] Там же.

| | | |
|---|---|---|
| ***вулиці» про зміни у ситуації*** | вулицю» для оцінки ситуації та забезпечення кращого зв'язку центру та особового складу на тактичному рівні (критично важливо у випадку залучення представників багатьох правоохоронних відомств) | |
| ***Судові розслідування застосування сили*** | Відеофіксація заворушень підготовленими співробітниками правоохоронних органів | США, Канада країни-члени ЄС |
| ***Реагування на масові заворушення, розслідування подій*** | Розширене використання відеоспостереження (камери, дрони, гелікоптери), моніторинг соціальних мереж, *краудсорсинг*[50] | Канада, США, країни ЄС |
| ***Залучення населення до забезпечення безпеки МПЗ та місць масового перебування людей*** | Проведення кампанії «Якщо ти бачиш щось, повідом про це»[51], яка популяризується через ЗМІ у т.ч. за допомогою соціальної реклами | США, кампанія проводиться низкою організацій країни |

## ВИСНОВКИ

Виходячи з наведеного вище, стосовно безпеки сектору комерційних об'єктів (СКО) критичної інфраструктури (КІ) та масових публічних заходів (МПЗ) можна зробити такі висновки:

1. Внаслідок особливостей, притаманних СКО КІ та МПЗ, у світі поки що не знайдено ефективних рішень щодо зниження терористичних та інших загроз і ризиків до прийнятного рівня, але відповідна робота активно ведеться за цілим рядом напрямів, що мають безпосереднє відношення як усіх секторів КІ, так і СКО, а саме:

a. посилення розвідувальної (насамперед, агентурної) контртерористичної діяльності;
b. інтеграція зусиль громадян, суспільства та держави з метою зниження загроз тероризму та екстремізму;
c. удосконалення координації дій, взаємодії та обміну інформацією між

[50] Від англ. «*crowdsourcing*» ( «*crowd*» — «толпа» та «*sourcing*» — «використання ресурсів»). У випадку використання цієї технології для збору відеоматеріалів важливо передбачити, що їх передача до правоохоронних органів може спричинити перевантаження непідготовлених до цього сайтів.

[51] Кампанія з підвищення обізнаності з питань безпеки, яку проводить Транспортне управління Нью-Йорку (*The Metropolitan Transportation Authority, MTA*) для захисту пасажирів та цінного майна шляхом підтримання постійних контактів з населенням щодо постійної загрози тероризму (детальніше див. сайт *MTA*: [Електронний ресурс]. – Режим доступу: http://www.mta.info/mta-security-campaign)

усіма залученими сторонами; відпрацювання і перевірка відповідних планів і процедур під час навчань і тренувань;

d. розвиток державно-приватного партнерства у сфері безпеки, у т.ч. між державними відомствами та приватними (корпоративними) службами безпеки;
e. використання новітніх технологій (перш за все, ІТ) для оцінки загроз, попередження і припинення терористичної діяльності.

2. До більш специфічних напрямів, пов’язаних із СКО КІ та МПЗ, які останнім часом активно розвиваються у провідних країнах світу, можна віднести:

a. розробка методів управління великими скупченнями (натовпами) людей;
b. моніторинг соціальних мереж з метою розкриття планів та намірів щодо терористичних та екстремістських акцій;
c. використання новітніх технологій: відеоспостереження, дрони, краудсорсинг, біометричні методи (у т.ч. технології розпізнавання обличчя тощо) на усіх етапах підготовки до проведення і проведення МПЗ, а також у випадку можливих розслідувань;
d. удосконалення систем контролю доступу до різних зон у місцях проведення МПЗ;
e. забезпечення безпеки у готелях, хостелах і т.д. і на пов’язаних з проведенням МПЗ об’єктах транспортної інфраструктури;
f. запобігання використанню транспортних засобів (насамперед, важких) для здійснення терористичних атак на об’єктах СКО КІ та у місцях масового перебування людей.

3. Враховуючи існуючий стан забезпечення захисту СКО КІ та безпеки МПЗ на теперішньому історичному етапі до першочергових завдань слід віднести:

a. створення профільної нормативно-правової бази[52];
b. виведення координації дій, взаємодії та обміну інформацією у сфері захисту КІ на якісно новий рівень;
c. започаткування і розвиток державно-приватного партнерства у цій сфері;
d. віднесення до числа пріоритетних питань планування діяльності усіх суб'єктів забезпечення захисту КІ та її стійкості на усіх рівнях управління та перевірки цих планів у ході регулярних навчань і тренувань.

## РЕКОМЕНДАЦІЇ

Беручи до уваги приклади найкращої практики та передовий досвід, накопичений на міжнародному та національному рівнях у сфері забезпечення безпеки при проведенні МПЗ на об'єктах КІ, а також наведені вище результати аналізу ситуації в Україні доцільно рекомендувати таке:

1. ***Міністерству економічного розвитку: і торгівлі України:***
   a. провести консультації із заінтересованими центральними органами виконавчої влади, іншими державними органами і установами щодо включення до складу робочої групи з розробки проекту Закону України «Про критичну інфраструктуру та її захист» представників приватного сектору, зокрема, тих, що представляють сектор комерційних об'єктів;
   b. підготувати пропозиції щодо внесення змін до Закону України «Про державно-приватне партнерство», включивши, зокрема, до переліку сфер застосування державно-приватного партнерства (Стаття 4) національну безпеку і оборону, захист критичної інфраструктури.
2. ***Робочій групі, створеній при Міністерстві економічного розвитку і торгівлі України*** для розробки проекту Закону України «Про критичну

[52]Затвердження Урядом «Концепції створення державної системи захисту критичної інфраструктури» (див. посилання 5) дозволяє зробити наступний крок – розробити і прийняти профільний Закон України «Про критичну інфраструктуру України та її захист».

інфраструктуру та її захист» підготувати пропозиції щодо включення до законопроекту положень про:

a. про державно-приватне партнерство у сфері забезпечення захисту та стійкості критичної інфраструктури України;
b. про відповідальність суб'єктів процесу забезпечення безпеки та стійкості критичної інфраструктури України за розробку, узгодження та регулярну перевірку планів і процедур взаємодії з партнерами, насамперед для випадків комплексних загроз (комбінацій загроз різного походження);
c. про залучення населення, неурядових організацій, експертного співтовариства, місцевих органів влади до зусиль, спрямованих на підвищення рівня безпеки та стійкості критичної інфраструктури;
d. про державний орган, відповідальний за координацію дій, взаємодію та обмін інформацією стосовно критичної інфраструктури (далі – відповідальний за критичну інфраструктуру орган);
e. про створення координаційних рад визначених законодавством секторів критичної інфраструктури, зокрема *сектору комерційних об'єктів* (або його еквіваленту, визначеному законопроектом).

**3.** ***Міністерству інформаційної політики України*** разом із Службою безпеки України та Міністерством внутрішніх справ України та їх освітніми та науково-дослідними установами**:**

a. розглянути можливість включення до планів роботи відповідних структурних підрозділів розробку у співпраці з правоохоронними органами настанов з безпеки для населення при проведенні масових публічних заходів, зокрема на випадок загроз підриву вибухівок, «активних стрільців», масових заворушень;
b. забезпечити онлайн доступ населення до відповідних текстових та відеоматеріалів.

4. ***Службі безпеки України, Антитерористичному центру при Службі безпеки України, Міністерству внутрішніх справ України, Національній***

***поліції України, Національній гвардії України,*** іншим компетентним відомствам підготувати концептуальні пропозиції щодо забезпечення безпеки масових публічних заходів, передбачивши запровадження категорування таких заходів та розробку моделей забезпечення безпеки таких заходів у залежності від їх категорій.

5. ***Службі безпеки України, Антитерористичному центру при Службі безпеки України, Національній академії Служби безпеки України:***

провести консультації із суб'єктами здійснення боротьби з тероризмом щодо необхідності змін у термінологічному забезпеченні боротьби з тероризмом, звернувши увагу, між іншим, на співвідношення і точність використання у нормативно-правових актах термінів «диверсія» та «терористичний акт», а також «антитерористичний» і «контртерористичний» та підготувати відповідні пропозиції щодо внесення змін у національне законодавство.

***6. Київській міській державній адміністрації, міським державним адміністраціям обласних центрів України, міст України з високим рівнем туристичного потоку:***

a. розглянути можливість запровадження заходів для запобігання, обмеження і припинення несанкціонованого проїзду транспортних засобів (особливо, важких) до вже існуючих пішохідних/туристичних зон, зон масового відпочинку та розваг населення тощо;
b. при капітальному ремонті або створенні відповідних зон (об'єктів критичної інфраструктури) при проектуванні передбачати запровадження організаційно-технічних засобів, які мінімізують можливість використання транспорту для наїзду на скупчення людей (пункти контролю, протитаранні засоби, спеціально прокладені траси тощо).

Кондратов С.І.
відділу енергетичної та техногенної безпеки

## Резюме

В аналітичній записці проаналізовано проблеми забезпечення безпеки при проведенні масових публічних заходів у взаємозв'язку із захистом критичної інфраструктури, і зокрема її сектору, який в США отримав назву «*сектор комерційних об'єктів*».

У записці зазначено, що поряд із загостренням загроз використання у терористичних та інших злочинних цілях високих технологій (насамперед, у ІТ-сфері) останніми роками різко зросла кількість терактів, в яких терористи для нападів використовують стрілецьку і холодну зброю та, навіть, просто транспортні засоби. Такі теракти відбувалися, здебільшого, при проведенні масових публічних заходів, у місцях масового перебування людей, (у т.ч. пішохідних зонах деяких туристичних центрів) тощо. У розвинутих країнах світу значна частина таких місць віднесена до критичної інфраструктури, об'єкти якої повинні захищатися від нападів терористів та екстремістів.

Спираючись на результати досліджень, проведених у Національному інституті стратегічних досліджень, а також на аналіз проведеного командно-штабного навчання національного рівня *CORE-2017* з питань енергетичної безпеки України, в аналітичній записці визначені основні проблемні напрями з точки зору захисту критичної інфраструктури, взагалі, та забезпечення безпеки її сектору комерційних об'єктів та масових публічних заходів, зокрема.

У матеріалі представлено стислий огляд найкращих практик і передового досвіду, а також конкретні організаційно-технічні підходи і рішення для забезпечення безпеки масових публічних заходів, ураховуючи те, що процес створення системи захисту критичної інфраструктури в Україні знаходиться на початковій стадії.

На основі проведеного аналізу сформульовано ряд висновків та конкретних рекомендацій щодо розв'язання першочергових проблем у цій сфері.