



*Зброя знищує
терористів,
освіта переможе
тероризм!*

**Загрози терористичного характеру:
формалізація,
аналіз,
оперативна протидія**

матеріали для самостійної підготовки

Загальна редакція

доктор юридичних наук, професор,
заслужений юрист України *І. М. Рижов*

Київ - 2022

ЗМІСТ

Оглавление

ЗМІСТ.....	2
1. СТРУКТУРА ТА ВИДИ СУЧАСНИХ ВИКЛИКІВ І ЗАГРОЗ НАЦІОНАЛЬНІЙ БЕЗПЕЦІ УКРАЇНИ	4
3. ПОНЯТТЯ РИЗИКУ, НЕБЕЗПЕКИ ТА ЗАГРОЗИ ЯК БАЗОВИХ КАТЕГОРІЙ ІННОВАЦІЙНИХ ТЕХНОЛОГІЙ ПРОТИДІЇ ТЕРОРИЗМУ	26
5. ЕЛЕМЕНТИ РИЗИК-ОРІЄНТОВАНОГО ПІДХОДУ В СУЧАСНИХ КОНЦЕПЦІЯХ ПРОТИДІЇ ТЕРОРИЗМУ.....	49
6. ЗАГРОЗИ ТА НЕБЕЗПЕКИ, МЕТОДИ ЇХ ВИЯВЛЕННЯ І РЕЄСТРАЦІЇ	59
7. КЛАСТЕРИЗАЦІЯ ЗАГРОЗ ТЕРОРИСТИЧНОГО ХАРАКТЕРУ ЗА СФЕРАМИ ТА ВИДАМИ ПРОЯВУ.....	75
8. ПЕРСПЕКТИВИ ФОРМУВАННЯ УНІФІКОВАНОГО ІНФОРМАЦІЙНОГО СЕРЕДОВИЩА У СФЕРІ ПРОТИДІЇ ЗАГРОЗАМ ТЕРОРИСТИЧНОГО ХАРАКТЕРУ.....	85
9. ВИЯВЛЕННЯ ЗАГРОЗ ТЕРОРИСТИЧНОГО ХАРАКТЕРУ ШЛЯХОМ МОНІТОРИНГУ ТА КОНТЕНТНОГО АНАЛІЗУ МЕРЕЖІ ІНТЕРНЕТ	104
10. МОДЕЛЬ ЗВ'ЯЗКІВ МІЖ ЗАГРОЗАМИ ТЕРОРИСТИЧНОГО ХАРАКТЕРУ ТА РЕАКЦІЄЮ СУСПІЛЬСТВА НА ЇХ ВПЛИВИ	115
11. МЕТОДИКА ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ ПРОТИДІЇ ЗАГРОЗАМ ТЕРОРИСТИЧНОГО ХАРАКТЕРУ ОСОБИ АБО МАЛІЙ ГРУПІ ЛЮДЕЙ	124
12. КОНЦЕПТУАЛЬНІ ПІДХОДИ ДО ПОБУДОВИ СИСТЕМИ ПРОТИДІЇ ЗАГРОЗАМ ТЕРОРИСТИЧНОГО ХАРАКТЕРУ	137
13. ФОРМУВАННЯ ВИМОГ АНТИТЕРОРИСТИЧНОГО ЗАХИСТУ ТИПОВИХ КАТЕГОРІЙ ОБ'ЄКТІВ МОЖЛИВИХ ТЕРОРИСТИЧНИХ ПОСЯГАНЬ	145

14. КОМПЕТЕНЦІЯ СУБ'ЄКТІВ БОРОТЬБИ З ПРОТИДІЇ	ТЕРОРИЗМОМ В УКРАЇНІ У ЗАГРОЗАМ ТЕРОРИСТИЧНОГО ХАРАКТЕРУ.....	181
15. ОСОБЛИВОСТІ РЕАЛІЗАЦІЇ ЗАГАЛЬНО- АНТИТЕРОРИСТИЧНОГО ЗАХИСТУ	ПРОФІЛАКТИЧНИХ ЗАХОДІВ 190	
16. СВІТОВИЙ ДОСВІД У ПРОТИДІЇ ЗАГРОЗАМ ТА РЕКОМЕНДАЦІЇ ДЛЯ УКРАЇНИ	ТЕРОРИСТИЧНОГО ХАРАКТЕРУ 203	
17. РЕКОМЕНДОВАНА ЛІТЕРАТУРА.		216

1. СТРУКТУРА ТА ВИДИ СУЧАСНИХ ВИКЛИКІВ І ЗАГРОЗ НАЦІОНАЛЬНІЙ БЕЗПЕЦІ УКРАЇНИ

Геополітичне значення виникнення у Європі нової держави під назвою «Україна» важко переоцінити. Розміри її території, чисельність населення, значний промисловий комплекс, науковий та інтелектуальний потенціали, природні багатства – усе це вже зараз примушує сприймати Україну як значну європейську державу. Крім того, саме її розташування виняткове вигідне, оскільки робить країну ключовим субрегіоном, що з'єднує своїми транспортними артеріями Захід і Схід, Північ і Південь континенту. Незамерзаючі чорноморські порти утворюють сприятливі умови для безпосередніх зв'язків з країнами інших континентів []¹.

Європейська природа Української держави зумовлена її історією та геополітичним розташуванням. Століття існування України у складі євразійської імперської системи виявилися неспроможними винищити природну фундаментальну ознаку української нації. У зв'язку з цим стратегічним напрямом української зовнішньої політики на найближче десятиліття стає активна, цілеспрямована інтеграція України в європейську спільноту. Шлях до Європи є для України також і шляхом зміцнення її незалежності. Проголошена Україною мета – стати міцною, незалежною, демократичною, без'ядерною державою не тільки не суперечить принципам побудови нової Європи, але й навпаки, з урахуванням зазначених її геополітичних характеристик, найкращим чином узгоджуватиметься з ними. Розбудова української державності та формування національної безпеки, включаючи побудову нових Збройних сил, зміцнення кордонів, забезпечення внутрішньої безпеки, здійснюється передусім із врахуванням своїх

¹ *Україна та Росія у системі міжнародних відносин: стратегічна перспектива: Монографія / Рада нац. безпеки і оборони України, Нац. ін-т проблем міжнародної безпеки; За заг. ред. С.І. Пирожкова. – К.: НППМБ, 2001. – 624 с.*

національних інтересів, а також з поєднанням інтересів держав першого та другого порядку – що нас оточують.

Здобуття Україною політичної незалежності є, беззаперечно, позитивним чинником, що істотно покращує геополітичну ситуацію в європейському регіоні, надає їй більшої стабільності та врівноваженості. Зміцнення молодого держави не пов'язане з виникненням загроз для будь-якої із сусідніх країн, а для деяких – стає гарантом незворотності змін на все найкраще у їхній власній долі.

Таким чином, завдяки зусиллям західних науковців та політиків поняття національної безпеки розширило свої рамки, і стало зводиться до здатності держави захистити свої національні цінності та інтереси в конкретних зовнішніх і внутрішніх умовах. У цьому плані важливою є думка президента США Дж.Кеннеді, який вважав, що у США немає окремо взятої політики ні в обороні, ні в дипломатії, ні в роззброєнні – всі вони зведені в єдину політику національної безпеки.

Про сучасні погляди на проблему національної безпеки керівництва цієї країни можна судити з доповіді колишнього міністра оборони США Ф. Карлуччи про бюджет на 1988/89 фінансовий рік. Він, зокрема, відзначав, що інтереси національної безпеки країни впливають з широко розповсюджених цінностей, що включають права людини, свободу, економічне процвітання, які служать для визначення конкретних інтересів і пов'язаних з ними географічних турбот, зокрема територіальної цілісності, союзників, безперешкодного доступу до світових ринків і джерел стратегічних ресурсів. Основний національний інтерес Америки, підкреслив Ф. Карлуччи, – це існування Сполучених Штатів як вільної і незалежної нації при збереженні її фундаментальних цінностей і інститутів безпеки її народу.

У розумінні як американських, так й інших західних дослідників, національна безпека – це здатність країни зберегти цілісність, суверенно вирішувати політичні, економічні, соціальні та інші завдання й виступати як самостійний суб'єкт системи міжнародних відносин.

Слід зазначити що, скажімо у законі Російської Федерації про оборону введено офіційне визначення безпеки як стану захищеності життєво важливих інтересів особи, суспільства і держави від внутрішніх і зовнішніх загроз. За своїм змістом це поняття відповідає прийнятому в світовій практиці терміну «національна безпека».

Варто далі звернути увагу на те, що між виділеними за рівнем інтересів особистою, колективною, національною, регіональною і глобальною безпекою існує тісний зв'язок. Зрештою, вони є елементами єдиної цілісної системи безпеки, в якій глобальна безпека займає верхній структурний рівень.

Глобальна безпека – це певний стан захищеності життєво важливих інтересів земної цивілізації від внутрішніх і зовнішніх загроз в економічній, військовій, екологічній, генетичній і інших галузях, що становлять середовище біологічного і соціального існування людини.

Причому, національна безпека у єдиній системі безпеки виконує ключову роль. Пояснюється це тим, що особистий і колективний інтереси можуть бути гарантовані лише в рамках держави його політичними, юридичними, економічними засобами і інститутами влади. Що ж до регіонального і глобального рівнів інтересів, то тільки держави є суб'єктами відносин відповідних рівнів, оскільки сучасне людство є співтовариством держав. Можливість забезпечити сукупність інтересів всіх рівнів в будь-якій сфері життєдіяльності (політичній, економічній, військовій і інших) визначається перш за все здатністю і готовністю держав виконати це.

Важливими чинниками, що здійснюють вплив на забезпечення національної, регіональної і глобальної безпеки, є, з одного боку, стан військового потенціалу провідних держав, а з іншого – ефективність міжнародних механізмів підтримки стабільності і спокою.

На нашу думку, безпека означає: по-перше, відсутність небезпеки для нормальної життєдіяльності людини (колективу, суспільства, людства); по-друге, надійну захищеність при виникненні загроз; по-третє, здатність

долати і усувати загрози, володіючи адекватними засобами, структурами, силами, тобто володіючи могутністю.

У даному контексті під могутністю розуміється здатність долати всілякі загрози нормальному функціонуванню суспільства і життя його громадян, спираючись на сили, що є в готовності, і засоби, адекватні загрозам, що виникають.

Розгляд проблеми безпеки, як і будь-якої самостійної наукової проблеми, передбачає необхідність розроблення поняття (спеціальних категорій) цього феномена. Думається, що категорія «безпека» може і повинна розроблятися насамперед як загальнонаукова категорія, яка до цього часу ще не ввійшла достатньою мірою в категоріальний апарат науки. З огляду на цю гранично широку за обсягом і глибоку за змістом категорію мають розроблятися також поняття окремих видів безпеки: термоядерної, екологічної, енергетичної, особистої, державної, суспільної, національної, міжнародної, планетарної та ін.

Дуже важливе значення має інтерпретація «безпеки» при опрацюванні проблем суспільствознавства. Практично всі соціальні науки, у тому числі правознавство, філософія, соціологія, політологія та ін., розробляючи проблеми гуманної безпеки або забезпечення безпеки людини, держав, народів, повинні спиратися у своїх дослідженнях на загальнонаукову категорію «безпека». Це поняття, таким чином, виконує методологічну функцію, тому що виступає як концептуальна ідея для пояснення тих чи інших конкретних процесів і явищ соціальної реальності та побудови окремих теоретичних моделей, які описують певні суспільні процеси у сфері безпеки.

Особливу роль ця категорія відіграє у правознавстві. Тут доцільно, на наш погляд, виділити декілька аспектів.

По-перше, категорію «безпека» у правознавстві (правову безпеку) варто тлумачити як суспільну безпеку, безвідносно до того, чи забезпечує безпека публічний або приватний інтерес. Тим самим акцент робиться на

тому, що безпека (як соціально-правове явище) забезпечує захист інтересів усього суспільства, усіх його структурних підрозділів.

По-друге, право загалом має своїм призначенням забезпечити нормальне існування і розвиток особистості, суспільства, держави, що цілком природно передбачає також суспільну безпеку. Отже, право може розглядатися в системі управління як засіб («інструмент») забезпечення безпеки (безпечного існування) особистості, держави, суспільства. Таким чином, застосовується нормативно-інструментальний підхід у тлумаченні співвідношення категорій «суспільна безпека» і «право».

По-третє, правову безпеку потрібно розглядати як фундаментальну категорію, яка має надзвичайно велике методологічне значення в реалізації наукових проблем багатьох галузей права. Це виявляється в такому: категорія «суспільна безпека», інтегруючи найбільш істотні властивості та принципи права, має водночас свій власний зміст; ця категорія дуже важлива для розуміння права і багато в чому визначає його сутність та основні риси; вона значною мірою впливає на зміст і сутність нормотворчості та правозастосування.

По-четверте, правову безпеку варто розглядати як загальну цінність, котра відповідає інтересам суспільства і громадян, тому що вона є однією з постійних потреб, яка детермінована природними умовами життя людини, суспільства, людства. Водночас суспільну безпеку слід розглядати як самостійне благо, котре в свою чергу покликане забезпечити безпечне існування інших благ.

Безпека в аспекті оцінки діяльності є засобом забезпечення інтересів людини, особистості, суспільства, держави. Водночас безпека є метою діяльності національних держав, громадянських співтовариств, людства в цілому. Ця діяльність – об'єктивно існуючий чинник і потреба: чим повноцінніше вони реалізовані, тим більшою мірою захищені, з точки зору безпечного існування, всі інші блага. Звідси випливає, що ефективна діяльність держави і суспільства по створенню безпечних умов існування

забезпечує нормальне «безперешкодне» і природне функціонування та розвиток суспільних відносин.

Отже, під національною безпекою варто розуміти стан країни, при якому відсутні або усунені реальні зовнішні і внутрішні загрози її національним цінностям, інтересам і національному способу життя, тобто забезпечується реалізація життєво важливих інтересів особи, суспільства і держави. Іншими словами, національна безпека – це певний рівень захищеності життєво важливих інтересів окремих громадян, соціальних груп, всього суспільства і держави, а також національних цінностей і способу життя від широкого спектру реальних зовнішніх і внутрішніх загроз. Це такий рівень захищеності, який забезпечує суверенітет і територіальну цілісність держави, стабільність суспільства, благополуччя особи і гарантує можливість прогресивного розвитку нації []².

Проблема формування національної безпеки України має кардинально важливе значення у контексті загального розвитку країни та її інтеграції до євроатлантичних структур та у світове співтовариство. Фактичне геополітичне становище держави дозволяє констатувати неадекватність реального і бажаного стану України в світі, відсутність дійових стратегій, які б зрушили ситуацію з критичної межі. Це зумовлює зосередження значної уваги на проблемі національної безпеки держави особливо тепер в умовах світових трансформацій, поєднавши питання розвитку окремих складових системи національної безпеки із необхідністю забезпечення життєво важливих національних інтересів.

Поняття національної безпеки останнім часом все частіше з'являється на шпальтах інформаційних видань, водночас воно майже (системно) не досліджено вітчизняними науковцями та державними діячами і має вельми широку інтерпретацію, через що формування національної безпеки значно ускладнюється.

² Зогуля І. *Українська нація та її безпека: новий погляд на національну безпеку України // Право України. – 2004. - № 5. – С.141-145.*

Звернемося до конкретних висловлювань сучасних науковців в цій сфері.

Як зазначає в своїй статті колишній директор Інституту проблем національної безпеки при Раді національної безпеки і оборони України В.П. Горбулін, і з чим слід погодитись, головною ознакою нашого часу є невпинне розширення поняття «безпека». Воно вийшло за рамки звичних воєнних і воєнно-політичних відносин. В останні роки з'явилися нові складові, тісно пов'язані з перспективами економічного, технологічного, інформаційного, етнокультурного розвитку держав і народів. Україна є одним з важливих чинників безпеки в Європі. Тому одне з найважливіших питань її державного управління є визнання всіма гілками влади необхідності вироблення своєї власної політики, правового поля та стратегії національної безпеки. Її стратегічною метою повинна стати гарантія незалежності, суверенності, територіальної цілісності, створення сприятливих умов для всебічного і стабільного економічного, етнонаціонального розвитку країни, а також збереження її національної спадщини [3].

Відповідно до окресленого постає проблема у розробленні критеріїв щодо оптимального рівня національної безпеки. На нашу думку, належний рівень національної безпеки досягається здійсненням єдиної державної політики, заснованої в межах правового поля, підкріпленої системою скоординованих заходів підсистем державного і недержавного забезпечення, адекватних внутрішнім та зовнішнім загрозам. Без такої політики система національної безпеки приречена блукати немов би у темряві, визначаючи свій рух лише у моменти безпосереднього зіткнення з об'єктами, що загрожують.

Для створення і підтримки необхідного рівня захищеності об'єктів національної безпеки в Україні варто розробляти систему правових норм, які: регулюють відносини в сфері національної безпеки; сприяють визначенню

³ Горбулін В., Качинський А. *Щодо стратегії національної безпеки України // Політика і час. – 2004. - № 9. – С.40-49.*

основних напрямів діяльності органів державної влади та управління в даній сфері; обумовлюють формування чи в необхідних випадках перебудову (реорганізацію) органів забезпечення національної безпеки і механізму контролю і нагляду за їх діяльністю (будь то державний чи не державний).

Серед засобів нормативно-правового регулювання забезпечення національної безпеки, під якими розуміються прийоми регулювання суспільних відносин в сфері національної безпеки, в залежності від особливостей відповідних правових норм варто виділити, на наш погляд, заборону, зобов'язання та дозвіл.

При розгляді значення правових норм в розрізі державної політики, які регулюють суспільні відносини в сфері національної безпеки, насамперед слід зазначити, що вони повинні забезпечувати: створення і включення в систему забезпечення національної безпеки всіх її суб'єктів; проведення аналізу, узагальнення, отримання, накопичення і обмін інформацією в системі забезпечення національної безпеки; вироблення чіткої взаємодії всіх ланок системи забезпечення національної безпеки у мирний і військовий час; можливість безпосереднього впливу на загрози національній безпеці та їх джерела;

Що ж до безпосереднього правового забезпечення діяльності суб'єктів системи забезпечення національної безпеки, то комплекс правових норм повинен, на наш погляд, визначати: мету, завдання, функції діяльності органів національної безпеки, їх компетенцію; організаційно-правові форми та методи діяльності органів національної безпеки; принципи побудови та функціонування органів національної безпеки; структуру та характер взаємовідносин всередині структури системи, що розглядається; правовий статус та межі оперативної самостійності суб'єктів системи забезпечення національної безпеки; умови, форми, порядок виникнення, зміни та припинення відносин між суб'єктами та об'єктами системи забезпечення національної безпеки.

Таким чином, в процесі нормативно-правового регулювання норми права регулюють відносини, що виникають в процесі забезпечення національної безпеки відповідними суб'єктами, що, в свою чергу, певним чином окреслює межі сфери правового регулювання даної діяльності.

Разом з цим, правові норми в сфері національної безпеки виступають правовою базою діяльності суб'єктів для цілеспрямованого, системного впливу на загрози та виклики національним інтересам країни. Причому попередження виникнення і нейтралізація загроз також здійснюється за допомогою норм права шляхом накладання заборон на діяльність, що провокує чи безпосередньо обумовлює виникнення загрози національній безпеці, шляхом встановлення юридичної відповідальності за діяльність (чи бездіяльність).

Видами такої відповідальності слід назвати: конституційну відповідальність; кримінальну відповідальність; адміністративну відповідальність; цивільно-правову відповідальність; дисциплінарну та матеріальну відповідальність [4].

Отже правове регулювання виступає важливим інструментом в системі забезпечення національної безпеки, оскільки обумовлює найбільш ефективні форми реалізації відповідних функцій суб'єктами системи забезпечення національної безпеки.

Адже країни, які мають розвинену систему національної безпеки за відсутності адекватного механізму правового забезпечення функціонування цієї системи, згодом перетворюються на неправові, тоталітарні держави, де закон стає неправовим. Водночас країни, які мають добру правову базу для забезпечення національної безпеки, але не мають системи національної безпеки, як механізму втілення у життя цієї ідеї, також приречені на провал. Саме тому симбіоз права і системи національної безпеки є іманентною ознакою творення нації – *tertium non datur*.

⁴ *Левіцька М.Б. Теоретико-правові аспекти забезпечення національної безпеки органами внутрішніх справ України: Дис... кандидата юрид. наук: 12.00.01. /Національна академія внутрішніх справ України. – К., 2002. – 206 с.*

Доречною у розглядаємому контексті є історія ставлення до права українського народу, яке характеризувалося розвиненим почуттям відповідальності, правовою культурою. Як приклади можна навести Руську Правду і Литовський статут, Конституцію Пилипа Орлика (1710 р.) та інші.

Ми погоджуємося з точкою зору В. Сіренка і В. Ліпкана, які вказують, що побудова системи національної безпеки має відбуватись паралельно з розробкою пакету нормативно-правових актів, де було б визначено загальні пріоритети розвитку нації, закріплено механізм забезпечення національних інтересів у найбільш важливих сферах суспільного буття. Причому існуюче законодавство має також бути, за необхідності, переглянуто з урахуванням постулату забезпечення національних інтересів []⁵ ⁶.

До цього додамо наступне. Задеклароване у Конституції положення щодо статусу України як правової, соціальної, демократичної держави є ще одним вагомим аргументом на користь необхідності синхронізації процесу побудови національної безпеки та удосконалення системи права в сфері національної безпеки. При цьому слід окреслити можливі підходи до розуміння саме національних інтересів.

Перший – світоглядний. Він полягає у тому, що національні інтереси є свідомим конкретизованим визнанням потреб нації у власному розвитку. За даного підходу їх інституціоналізація не є необхідною. Позитивною у даному випадку вбачається можливість щодо постійної зміни цих інтересів відповідно до реалій часу. Відсутність певної визначеності з даного питання надає творчим представникам як титульного етносу, так і інших етнічних меншин, вкладати у це поняття свій, подеколи значно ширший зміст. З іншого боку, певна аморфність та невизначеність поняття національних інтересів не сприяє згуртованості нації. Крім цього, система національної безпеки, хоч і є за своєю суттю відкритою системою, відтак зазнає впливу

⁵ Сиренко В.Ф. *Аппарат государственного управления: интересы и деятельность / АН Украины. Ин-т государства и права им. В.М. Корецького; Отв.ред. В.Ф. Сиренко. – К.: Наук. думка, 1993.- 165 с.*

⁶ Ліпкан В.А. *Національна безпека України: нормативно-правові аспекти забезпечення. – К.: «Текст», 2003. – 180 с.*

динамічного хаосу, має створюватися на засадах визначеності цілей, принципів, функцій та методів свого функціонування.

Другий підхід – інституційний – передбачає необхідність закріплення у праві не лише механізму забезпечення національних інтересів, а й конкретне визначення останніх. Позитивним моментом тут є визначеність національних інтересів, що сприяє згуртованості різних прошарків українства у монолітний соціум, визначає пріоритети, окреслюючи сьогочасні інтереси нації, впроваджуючи їх прозорість, можливість дискусії і, за необхідності, корекції. Правове закріплення інтересів нації дозволить зробити політику держави більш відкритою, наближеною до кожної людини, а головне – кожному представникові української нації буде відомо, які інтереси нації він має відстоювати, чи сходяться ці інтереси з його інтересами, чи входять його інтереси до інтересів загалу. На наш погляд, правове закріплення поняття та визначення національних інтересів, унеможливуватиме прикриття чиновників різних рівнів категорією «національних інтересів» як трансцендентальною, неосяжною для розуміння, а отже такою, що не підлягає концептуалізації. Негативним моментом будь-якого правового закріплення поняття системного явища є його неповнота. Проте це – апріорі, і навряд чи можна навести приклад ідеального відображення у законі визначення поняття того чи того системного суспільного явища.

Таким чином, правове регулювання системи забезпечення національної безпеки зорієнтоване на практичну координацію всіх видів державних і громадських інститутів (недержавних інститутів) з метою захисту життєво важливих національних інтересів України, запобігання та нейтралізації потенційних і реальних внутрішніх та зовнішніх загроз.

Власне про сучасні виклики і загрози національній безпеці України, їх структуру, види і піде мова у наступному підрозділі, де ми спробуємо, за допомогою синергетичного підходу визначитись із сутністю загроз, дати їх класифікацію та аналіз.

Як вже відзначалося, особливе місце в теорії і практиці національної безпеки, надається такому базовому поняттю як загрози національним інтересам України. Такий підхід базується на наступному теоретичному обґрунтуванні.

По-перше, загрози національним інтересам України виступають невід'ємною складовою сфери національної безпеки України.

По-друге, ґрунтовне наукове вивчення загроз національній безпеці не тільки відповідає меті і завданням цього дослідження, але й складає його суттєву і необхідну ланку, особливо тепер в умовах складних геополітичних трансформацій. Викладене обґрунтування дозволяє не тільки не обмежуватися загальним розглядом згаданої складової щодо значення для побудови ефективної системи забезпечення національної безпеки, але й присвятити його вивченню спеціальний підрозділ.

Отже, проблеми забезпечення національної безпеки в Україні є найбільш актуальними і їх видова різноманітність і складність постійно збільшується, що є закономірним наслідком загрозової ситуації майже в усіх сферах державного і суспільного життя.

При цьому слід звернути на національну специфіку щодо джерел та проявів загроз, їх виникнення, процесів зміни та настання. Зрештою, кожна держава та кожне суспільство мають специфічні «родові» проблеми в галузі безпеки, пов'язані з їхніми власними якостями. Зміст, спрямованість та характер загроз безпосередньо залежить від розвиненості, цивілізованості суспільства та його міжнародних зв'язків. Рівень безпеки врешті визначається здатністю до адекватної оцінки ступеня небезпеки загроз та оптимальної протидії їм. Причому, зміст офіційно виявлених загроз і характер реакції на них є показовими ознаками конкретного суспільства. Загрози, які їх відчуває недемократична держава, цілком відмінні від притаманних демократичній державі. Демократичні ж країни аксіоматично чутливі до небезпек, схильні деталізувати ризики та виклики, але ніколи їх не вигадують. Родовою ознакою авторитарних режимів, як більш примітивних,

є масштабні антагонізми та відповідні загрози. Таким режимам властиве створення реальних та продукування уявних загроз і, як наслідок, ірраціоналізм політики у сфері безпеки. Врешті авторитаризм є загрозою для демократії.

Мета демократичних трансформацій суспільства полягає у зміні уявлень про завдання і засоби гарантування безпеки []⁷.

При проведенні аналізу законів та інших нормативно-правових актів, наукових праць, публікацій автори зіткнулися з різними розуміннями проблеми національної безпеки, в тому числі їх визначеннями і розумінням загроз національній безпеці. Певні дослідники, з висновками яких автор повністю погоджується, (Г. Почепцов, Г. Ситник, М. Левицька, В. Ліпкан, П. Белов, О. Маначинський та інші []⁸ вбачають сутність забезпечення національної безпеки в приділенні належної уваги саме викликам і загрозам національним інтересам, і визначають національну безпеку як відсутність реальних чи потенційних загроз. Так, Е. Любкемейер []⁹ під національною безпекою розуміє ситуацію, коли відсутні загрози, що представляють небезпеку для існування суспільства, держави, особи, чи якщо такі загрози існують, діє ефективний захист проти них. Тому політика національної безпеки розуміється як шлях, що задає напрям роботи держави з актуальними чи потенційними загрозами існуванню своїх громадян. У визначенні національної безпеки він виділяє такі складові:

Класифікація загроз ставить своїм завданням їх поділ за сутнісними ознаками на окремі групи. Якщо ця класифікація виконана правильно, то вона може надати нам точне уявлення про завдання кожної окремо групи

⁷ Дергачов О. *Небезпека як атрибут державності* // *Політична думка*. – 1997. - № 1. – С.89-100.

⁸ Почепцов Г.Г. *Національна безпека країн перехідного періоду: Навч. посібник*. - К., 1996.- 136 с.; Ситник Г. *Методологічні аспекти формування понятійно-категоріального апарату національної безпеки* // *Вісн. Української Академії державного управління*. – 2000.- № 2. – С.19-27.; Левицька М.Б. *Теоретико-правові аспекти забезпечення національної безпеки органами внутрішніх справ України: Дис... кандидата юрид. наук: 12.00.01. /Національна академія внутрішніх справ України. – К., 2002. – 206 с.; Ліпкан В.А. *Теоретичні основи та елементи національної безпеки України: Монографія*. – К.: «Текст», 2003. – 600 с.; Белов П. *Методология национальной и международной безопасности* // *Обозреватель*. – 2000. - № 7. – С. 85.*

⁹ Любкемейер Э. *Безопасность в мире после Берлинской стены: немецкая точка зрения* // *Національна безпека країн перехідного періоду: Навчальний посібник*. - К., 1996.- С.124-126.

загроз та про їх місце у загальній системі дестабілізації. Система безпекогенних чинників потребує правильної логічної класифікації. Лише за її наявності ми можемо говорити про дестабілізацію, як про логічно систематизовану сукупність загроз національній безпеці.

Нині не існує такої класифікації загроз національній безпеці, яка б могла вважатися загальноновизнаною або навіть домінуючою. Завдання правильної класифікації загроз полягає передусім у тому, щоб знайти, які логічні критерії лежать в основі історичного сталого підрозділу загроз національній безпеці і у виправленні цього поділу відповідно до вимог логіки; по-друге, процес поділу загроз ще не завершився. Наукове знання постійно прогресує, не лише розробляючи сучасні системи безпеки, а й створюючи новітні загрози національній безпеці. Класифікація загроз має враховувати і цю обставину, піддаючи логічній перевірці усю систему загроз, відшуковуючи у ній прогалини, вказуючи на ті загрози, яких не вистачає у класифікації для логічної повноти системи, які мають бути знову відтворені, а які вже вичерпали себе з часом.

Отже, класифікація загроз національній безпеці має бути доповнюючою. Вона не має ставити своїм завданням створення абсолютно нової систематики загроз, яка б не мала нічого спільного з тим поділом, який історично склався. Правильна класифікація загроз національній безпеці має вказувати взаємну залежність загроз одна від одної, місце їх у загальній системі дестабілізації і наочно знайти ті принципи, які були утворені історичним розвитком науки і не завжди чітко були сформульовані. На підставі цих знань ми можемо здійснити логічний аналіз існуючих загроз і отримати найбільш наближену до відображення об'єктивної дійсності класифікацію.

В основу даної класифікації нами була покладена певна закономірність, яка полягає не лише у самих елементах, а й у зв'язках між ними.

Отже, до першого типу мають належати такі загрози:

За джерелами походження: природні – передбачають небезпечні геологічні (землетруси, деградація ґрунтів чи надр, лавини та інші літосферні явища), метеорологічні (погоди, повітряні потоки та інші атмосферні явища), гідрологічні (морські хвилювання, режим стоку вод, повені, цунамі, замерзання і скресання акваторії, зміна стану водних ресурсів та інші гідросферні явища), біологічні (врожайність, природні пожежі, масове ураження сільськогосподарських рослин і тварин хворобами чи шкідниками, зміна стану біосфери та інші явища у рослинному і тваринному світі), медико-біологічні (людські хвороби), космологічні (стан і рух небесних тіл, газів, випромінювань, усіх явищ космосфери), фізико-хімічні (зміна стану мікросвіту) загрози. Так, наприклад, для України найбільш актуальною є проблема повенів у Закарпатті, на Одещині, для Вірменії – проблема землетрусів, для західних і центральних штатів Америки – проблема буранів та смерчів (останнім часом 2004-2005 рр – східні узбережжя Америки), а для Японії – землетрусів, тайфунів та цунамі тощо.

До загроз техногенного походження слід відносити транспортні аварії (катастрофи), пожежі, неспровоковані вибухи чи їх загроза, аварії з викидом (загрозою викиду), небезпечні хімічні, радіоактивні, біологічні речовини, рангове руйнування споруд та будівель, аварії на інженерних мережах і спорудах життєзабезпечення, гідродинамічні аварії на греблях, дамбах – усі явища техносфери тощо;

За наслідками, загрози поділяються на: цивілізаційні – реалізовані загрози на певному етапі розвитку суспільства, що призвели до порушення цілісності і сталості суспільства у поступальному історичному розвитку, протікання процесів самоорганізації і саморегуляції, дисбалансу механізму регулювання за допомогою настанов, норм і законів, а також організацій і установ, що забезпечують функціонування суспільства взаємовідносин між соціальними суб'єктами у поступальному його розвитку; глобальні – реалізовані загрози, що охоплюють увесь світ. На відміну від цивілізаційних загроз характеризують здебільшого кількісний бік, обсяг загроз;

транснаціональні – реалізовані загрози, що охоплюють різні нації. Прикладом вияву таких загроз може бути активна діяльність транснаціональної терористської організації Аль Каїда, терористи якої брали участь у вчиненні актів тероризму у різних країнах; регіональні – реалізовані загрози, що охоплюють нації певного регіону; національні – реалізовані загрози, що обмежуються сферою однієї нації; локальні – реалізовані загрози, що обмежуються сферою конкретного об'єкта (району, області, штату, конкретних об'єктів підприємницької діяльності, осіб, групи осіб тощо). Прикладом може слугувати загроза аварії на хімічному заводі, яка може призвести до екологічної катастрофи у певному регіоні.

За рівнем небезпеки: особливо небезпечні – такі, що створюють небезпеку заподіяння шкоди життєво важливим національним інтересам; підвищено небезпечні – такі загрози, що створюють небезпеку заподіяння шкоди важливим національним інтересам; небезпечні – такі загрози, що створюють небезпеку заподіяння шкоди іншим національним інтересам.

Ще на один напрямок хотілось би звернути особливу увагу. З кінця 70-х років ХХ в. у теорії міжнародних відносин з'явилося нове поняття, в англійській транскрипції як «soft security», у вітчизняній літературі – як «м'яка безпека». Основне значення даного терміну у тому, що на відміну від традиційної «жорсткої безпеки», що ґрунтується на двох основних критеріях: військовій силі як основному інструменті, що забезпечує захист від загроз, що виникають, і державі як домінуючому суб'єкті безпеки – м'яка безпека значно розширила межі цього поняття, доповнивши його новими акторами і розширивши предметну галузь цього явища. В результаті цього за останні роки аспект безпеки мігрував з сфери вивчення міжнародних відносин в інші галузі знання – соціологію, психологію, лінгвістику, етнологію і суспільну географію, створивши нові детермінанти безпеки – енергетичну, інформаційну, економічну, демографічну, екологічну і етнічну. У свою чергу, крім держави як основного суб'єкта забезпечення національної безпеки виділилися нові суб'єкти, що постали в певний таксономічний ряд: людина

(окрема особа) і сім'я, співтовариство, держава, міжнародна організація. При цьому держава, що довгий час є монополістом в даній галузі, вимушена передати значний об'єм своїх функцій відповідним субнаціональним і транснаціональним інститутам, а також недержавним організаціям, що ще більш ускладнює вивчення, прогнозування і управління процесами виникнення загроз і захисту від них.

При цьому слід звернути увагу на наступне. В теперішній час існує ряд глобальних проблем, що несуть в собі загрози для всього людства. ООН виділяє дванадцять проблем, для вирішення яких вимагаються зусилля світової спільноти: припинення ядерного конфлікту і роззброєння, демографічна, продовольча, ресурсна, енергетична, екологічна проблеми, підняття економіки відсталих країн, ліквідація небезпечних захворювань, освоєння світового океану і космосу, боротьба із злочинністю і тероризмом, боротьба з наркоманією, нелегальною міграцією та торгівлею людьми.

Загрози діють головним чином у відповідній сфері національних інтересів, але негативний вплив їх розповсюджується на всі інші національні інтереси. Хоча можна виділити загрози, що діють одночасно на значну кількість національних інтересів. Необхідно враховувати, що загрози, як правило, мають декілька стадій розвитку: зародження (початок формування), прояв (знаходження виразних форм), загострення (критична стадія негативного впливу з відповідними наслідками).

Як системне соціальне утворення, національна безпека України покликана, на наш погляд, слугувати, по-перше, запобіганню реально існуючим загрозам та їх відбиттю і, по-друге, вона по суті має бути адекватною цим загрозам і відповідати принципу достатності. В разі ж такої невідповідності система забезпечення національної безпеки України стане економічно марнотратною, а в політичному плані може стати самостійним джерелом загрози для національних інтересів інших держав. Тобто порушення рівноваги між системою гарантій національної безпеки і явними

або потенційними загрозами в одних випадках може призвести до розпаду соціальних структур, а в інших – до необґрунтованих репресій у самій державі і конфліктів у міждержавних відносинах.

Постійний моніторинг загроз і міри їх небезпечності для життєво важливих інтересів України, що повинний здійснюватися на постійних професійних засадах і обіймати всі сфери життя народу України, дозволяє визначити їх якомога раніше й розробити систему заходів впливу, які з найменшими витратами нейтралізують загрози та припиняють деструктивні процеси.

Отже, для своєчасного виявлення та об'єктивної оцінки загроз національним інтересам, вибору та вжиття адекватних засобів їх локалізації, зменшення чи нейтралізації створюється система забезпечення національної безпеки.

У цьому напрямку важливими є дослідження Національного інституту стратегічних досліджень, де за допомогою багатовимірних, системних та інших методів був відстежений і оцінений рівень загроз пріоритетним національним інтересам. Це дає можливість всебічно вивчати і передбачати перебіг процесів у сфері національної безпеки та керувати ними на основі завчасного прийняття необхідних рішень [10].

Аналіз стану національної безпеки України за останні роки свідчить, що до 2014 року внутрішні загрози становили найбільшу небезпеку для розвитку держави. Вони були пов'язані одночасно з декількома національними інтересами й мали тенденцію до зростання. Багато з них є досить небезпечними і відносно тривалими. Їхній сумарний потенціал зосереджено переважно в економічній, соціально-політичній, міжнародній, військовій, інформаційній та екологічній сферах. Сюди слід віднести також сферу регіональних відносин. А така найбільш небезпечна внутрішня загроза як криміналізація суспільства зачіпає практично усі сфери життя.

¹⁰ *Національна безпека України, 1994-1996 рр.: Наук. доповідь НІСД / Гол. ред. колегії Бєлов О.Ф.-К.: Нац. ін-т. стратег. досліджень, 1997.- 200 с.*

Виявлення, запобігання, нейтралізація та ліквідація небезпек, що пов'язані з цією найбільш небезпечною внутрішньою загрозою, значною мірою відносяться до сфери діяльності органів внутрішніх справ, що простежується на основі аналізу таких нормативно-правових актів як, насамперед, Закону України «Про основи національної безпеки України» та Закону України «Про міліцію».

Так, в Законі України «Про основи національної безпеки України» []¹¹ серед загроз національній безпеці у політичній, економічній та соціальній сферах виділяються такі:

1. У зовнішньополітичній сфері: посягання на державний суверенітет України та її територіальну цілісність, територіальні претензії з боку інших держав; спроби втручання у внутрішні справи України з боку інших держав;

Зазначене дає змогу зробити висновок, що структури і підрозділи системи МВС відносяться до суб'єктів системи забезпечення національної безпеки, основним завданням яких є протидія відповідним внутрішнім загрозам національній безпеці України згідно з предметною компетенцією.

Системний аналіз стану національної безпеки, який склався в Україні за останні роки, дає підстави стверджувати, що негативні процеси в Україні мають стійкий характер і комплексно відбиваються на найбільш важливих сферах життєдіяльності суспільства. При цьому особливу увагу привертає те, як вже згадувалося вище, що найважливішою внутрішньою загрозою є криміналізація суспільства, яка практично торкається усіх сфер. Не є новим в Україні і транснаціоналізація злочинності, залучення організованого криміналітету до діяльності злочинних угруповань інших країн, про що більш ґрунтовно піде мова у третьому розділі дослідження. Таким чином, констатується факт політизації, інтелектуалізації та транснаціоналізації високоорганізованої злочинності в Україні.

¹¹ Закон України «Про основи національної безпеки України»: прийм. 19.06.2003 року // Офіційний вісник України. – 2003.-№ 29. – ст.1433; Відомості ВРУ. – 2003. - № 39. – ст. 348.

На цьому фоні зростають такі нові для України і дуже небезпечні форми насильницької злочинності як терористичні акти проти політичних діячів і державних службовців, контрабанда, наркобізнес, вбивства на замовлення, усунення свідків, конкурентна боротьба злочинних угруповань між собою за сфери впливу, нелегальна міграція і торгівля людьми тощо.

За сучасних міжнародних реалій значну зовнішню загрозу для України становить розповсюдження міжнародного тероризму, суб'єктами боротьби з яким є правоохоронні органи та зокрема Служба безпеки України. Обмеженість об'єму дослідження дозволяє нам розглянути лише окремі аспекти цієї проблематики.

Як слушно зазначають В. Антипенко, В. Коваленко, Б. Романюк, тероризм для України перетворюється у конкретну загрозу. За рядом причин та обставин (значне територіальне поширення тероризму і кількісне зростання цього явища в світі та країнах СНД) він стоїть «на порозі» нашої держави, становить реальну небезпеку для суспільства і може суттєво вплинути на демократичні надбання []¹².

Тероризм як явище політичного життя є багатограним і багатоликим. Як відзначають О.В. Змієвський і М. Требін, тероризм – явище надто складне, динамічне і багатоаспектне. Окрім правових, він порушує і цілий ряд інших проблем – психологічні, історичні, технологічні тощо []¹³.

Серед зовнішніх загроз, що виступають за певних умов джерелами вчинення терористичних актів слід, на наш погляд, виділити такі: прагнення деяких держав (наприклад Російська Федерація) до встановлення свого воєнно-політичного впливу в окремих регіонах світу та їх схильність до розв'язання конфліктів силовими методами; сепаратистські тенденції (створення так званих ЛНР та ДНР) у крайніх формах вияву, що дестабілізує

¹² Антипенко В. Визначення поняття «безвинні жертви» у складі тероризму: актуальна проблема // *Право України*. – 2001. - № 6. – С. 75-77.; Коваленко В. Щодо вивчення міжнародного досвіду боротьби з тероризмом // *Стратегічна панорама*. – 2001.- № 3-4. – С. 85-89.; Романюк Б., Коваленко В. Щодо кримінально-правового визначення поняття тероризму // *Право України*. – 2001.- № 6. – С.71-75.

¹³ Требін М. Цивілізація у боротьбі з тероризмом: успіхи, невдачі та перспективи // *Нова політика*. – 2000.- № 4. – С.59-66.

внутріполітичну ситуацію в багатонаціональних державах, якою є Україна; збереження загрози міжнародного шантажу, в тому числі з використанням ядерної та інших видів зброї масового знищення; виникнення збройних конфліктів у сусідніх державах, в які можуть втягнути Україну; інформаційна експансія з боку інших держав.

До внутрішніх загроз, на наш погляд, відносяться: масові порушення прав, свобод та законних інтересів громадян в Україні; відсутність ефективних механізмів забезпечення законності, правопорядку, боротьби із злочинністю, особливо її організованими формами та тероризмом; криміналізація суспільства, діяльність тіньових структур; соціальна напруженість та соціально-політична нестабільність в Україні; створення та функціонування незаконних збройних формувань; низький рівень життя та соціальної захищеності значних верств населення, в т.ч. і етнічних груп, наявність великої кількості громадян працездатного віку, не зайнятих у суспільно-корисній діяльності; неконтрольовані міграційні процеси в суспільстві; загострення міжетнічних та міжконфесійних відносин (наявність відповідних конфліктів).

Загалом тероризм слід віднести до ескалаційної загрози, так як кожна його стадія змінюється новою, більш масштабною. Динаміка терористичних акцій характеризується діями, подібними до концентричних кіл, які розширюються і захоплюють чимраз більший соціальний простір.

Терористичні акти в основному виражені в таких намірах (діях): насильницькій зміні конституційного ладу чи захоплення влади; організації масових безпорядків, диверсій; блокади окремих місцевостей; розпалення міжнаціональних і регіональних конфліктів, що супроводжуються насильством, знищенням або спробою знищення політичних діячів або кримінальних елементів, загрозою життю, безпеці громадян або нормальній діяльності державних інститутів, організацій; вчинення значних аварій,

вибухів, а також захоплення заручників з метою впливу на прийняття органами влади бажаного терористам рішення []¹⁴.

Отже, підсумовуючи вищевикладене, необхідно наголосити, що в сучасних умовах геополітичних трансформацій, Україна стикається з новими викликами та загрозами національній безпеці. І це ще не пік небезпеки. Всередині держави набирають обертів нові злочинні явища, як сепаратистські рухи (ДНР та ЛНР, проект «Новоросія»), які є незаконними військовими формуваннями, анексія російською Федерацією Автономної Республіки Крим тощо, й це все має підпитку зовнішніми факторами. Не є новим в Україні і транснаціоналізація злочинності, залучення організованого криміналітету до діяльності злочинних угруповань інших країн, розгортання такого ганебного явища як торгівля людьми (з її складовими – торгівля і експлуатація жінок, дітей, трансплантація органами тощо) про що більш ґрунтовно піде мова у третьому розділі дослідження.

¹⁴ Глушков В.О., Долженков О.Ф. Організаційно-правові основи боротьби з тероризмом // Актуальні проблеми держави та права: Зб. наук. праць / Одеса. - 2000. – Вип.8. – С. 47-52.

3. ПОНЯТТЯ РИЗИКУ, НЕБЕЗПЕКИ ТА ЗАГРОЗИ ЯК БАЗОВИХ КАТЕГОРІЙ ІННОВАЦІЙНИХ ТЕХНОЛОГІЙ ПРОТИДІІ ТЕРОРИЗМУ

Антитерористична операція на сході України характеризується масштабними бойовими зіткненнями і численними жертвами як серед військових та спецпризначенців, так і серед цивільного населення. Трагізм цих подій свідчить про те, що українське суспільство не було до них готове¹⁵.

В Україні функціонує державна система боротьби з тероризмом, але це не убезпечило громадянське суспільство від проявів масштабної терористичної діяльності, яку ми спостерігаємо сьогодні. Помилки в організації загальнодержавної стратегії протидії тероризму в Україні, на нашу думку, стануть предметом детального розгляду науковців, проте вже очевидно, що глобальною помилкою було те, що головні зусилля антитерористичної діяльності було сконцентровано на формуванні державної системи боротьби з тероризмом, використовуючи лише можливості спеціальних підрозділів суб'єктів боротьби з тероризмом, та ігноруючи потребу постійних інтелектуальних інвестицій, як відповідь на появу нових типів загроз терористичного характеру¹⁶. Недосконалість прогресивних механізмів активної протидії тероризму, ефективних способів викорінювання його джерел указує на певну кризу зовнішніх і внутрішніх політичних стратегій боротьби із цією загрозою. Таким чином, існує нагайна потреба обґрунтовано показати необхідність та особливу актуальність інноваційного розвитку стратегій боротьби з тероризмом в умовах гібридно-інформаційних загроз.

¹⁵ *Війна на сході України* [Електронний ресурс]. – Режим доступу: http://uk.wikipedia.org/wiki/Війна_на_сході_України.

¹⁶ *Закон України «Про боротьбу з тероризмом»* [Електронний ресурс]. – Режим доступу: <http://zakon2.rada.gov.ua/laws/show/638-15>.

Сучасні наукові розробки у сфері боротьби з тероризмом зводяться до кількох напрямів: антологія масового терору й історіографічні нариси вчинених терористичних актів; кримінологічний аналіз злочинів терористичної спрямованості та розроблення оперативно-тактичних прийомів боротьби з терористичною діяльністю на рівні організації та планування антитерористичних операцій. Водночас, недостатньо вивченими є концептуальні та методологічні засади сучасних стратегій національної безпеки в контексті протидії тероризму, теоретичні засади функціонування державної (загальнонаціональної) системи протидії тероризму, здійснення державного контролю в цій сфері. Поза увагою, при формуванні антитерористичних стратегій, залишилися доробки науковців щодо креативних, науково-обґрунтованих рекомендацій розвитку системи боротьби з тероризмом. Про це свідчить той факт, що в державі немає спеціалізованих наукових закладів, які б досліджували проблеми антитерористичної безпеки як комплексної наукової дисципліни. Наслідки такої помилки стали фатальними – як не сумно це констатувати. Прагнення їх виправити зумовлюють необхідність прийняття інноваційних рішень.

Можемо констатувати, що до цього часу не сформовано цілісне наукове вивчення тероризму як явища, не уніфіковано понятійно-категоріальний апарат, теоретично-методологічні засади протидії тероризму. Події останніх місяців в нашій державі свідчать про недосконалість сучасних стратегій протидії тероризму на усіх рівнях їхньої реалізації. Як наслідок, в результаті неопрацьованості тактико-спеціального та військово-технічного аспекту боротьби з тероризмом, недосконалості науково-методологічної основи антитерористичних технологій ми маємо численні жертви терористичних атак. Загалом, вироблення й реалізація ефективної стратегії боротьби зі злочинністю – справа, якою займалися всі держави не одне століття, проте помітних здобутків так і не досягли.

Наслідки терористичної діяльності вражаючі, і це попри те, що в державі понад 15 років функціонує Антитерористичний центр при СБ

України, який діючи в межах відповідного правового поля, очолював, як нам здавалося вельми успішно, державний інституціональний механізм боротьби з тероризмом. Порядок та правові підстави боротьби з тероризмом виписані у низці нормативних актів, зокрема у Концепції боротьби з тероризмом (затвердженої Указом Президента України від 25 квітня 2013 р. № 230 та чинної на цей час), Законі України «Про боротьбу з тероризмом», багатьох імплементованих Україною міжнародних нормах та відомчих документах¹⁷. Незважаючи на це, державна система боротьби з тероризмом, м'яко кажучи, функціонально не спрацювала – це історичний факт, підкріплений чисельними людськими жертвами та матеріальними й моральними збитками. Особливо слід наголосити, що принципи, на яких вона була вироблена, використовуються й в сучасних умовах¹⁸.

З моменту прийняття державної концепції боротьби з тероризмом минуло понад два роки. За цей час багато чого змінилося, причому докорінно. Поодинокі прояви терористичної злочинності, на боротьбу з якими робився акцент раніше, змінилися широкомасштабною терористичною загрозою, район якої за площею та кількістю населення, що проживає в зоні АТО, співвідносні з деякими європейськими державами, а концентрація зброї перевищує потенціали деяких країн НАТО.

Терористична діяльність будується на базі новітніх гібридних соціально-інформаційних технологій маніпулювання людською свідомістю, системними елементами яких вже давно не є захоплення заручників, підпал, убивство, тортури, залякування населення та органів влади. Тероризм у постіндустріальному суспільстві опанував інноваційні механізми вчинення інших злочинних посягань, і, що характерно, не стільки на життя чи здоров'я людей, скільки на їхні думки, мораль та духовність. На додаток до технологій

¹⁷ Розпорядження Кабінету Міністрів України від 11 липня 2013 р. № 547-р «Про затвердження плану заходів з реалізації Концепції боротьби з тероризмом» [Електронний ресурс]. – Режим доступу: <http://zakon2.rada.gov.ua/laws/show/547-2013-p>.

¹⁸ Постанова Кабінету Міністрів України від 15 серпня 2007 р. № 1051 «Про затвердження Положення про єдину державну систему запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків» [Електронний ресурс]. – Режим доступу: <http://zakon2.rada.gov.ua/laws/show/1051-2007-n>.

війн індустріальної епохи, заснованих на фізичному протистоянні сил суперників, у війнах постіндустріального періоду широко використовуються соціально-інформаційні технології провокації соціетальних і соціальних конфліктів, основу яких складають інформаційні та інші нематеріальні активи і інтелектуальний капітал – як значущі компоненти (які впливають на ефективність) у складі потенціалу загроз або системи захисту від них ¹⁹.

Незважаючи на значні зусилля, що вживаються світовим співтовариством, міжнародний тероризм щороку поширюється, стає організованим і витонченим, а українське суспільство вражене вірусом тероризму з усіма трагічними наслідками. Історія подібних протистоянь свідчить про ймовірність переходу, навіть за умови демілітаризації лінії бойового зіткнення, до терористично-диверсійної боротьби на інших територіях України. Тому антитерористична підготовка населення, заходи із упередження та запобігання терористичній діяльності на сьогодні не просто вимога часу, це життєво - необхідна умова подальшого існування суспільства.

Безумовно, такий розвиток подій вимагає від управлінської системи формування й реалізації інноваційних стратегій боротьби з тероризмом та супутніми йому викликами і потребує відповідного рівня інтелектуального забезпечення: розробки, перевірки, впровадження та корегування системи наукових знань щодо можливих, у будь-який спосіб, шляхів вдосконалення протидії терористичній злочинності, інноваційних можливостей антитерористичного захисту об'єктів можливих терористичних посягань та формування антитерористичних компетенцій як суб'єктів боротьби з тероризмом, так і цивільного населення. У зв'язку з сутнісними відмінностями сучасних інтелектуально насичених технологій ведення війн від традиційних, для ефективного функціонування системи антитерористичного захисту необхідно змінювати принципи і моделі

¹⁹ Вовканич С. Соціогуманістична стратегія інтелектуального забезпечення інноваційного розвитку [Текст] / С. Вовканич // Регіональна економіка. – 2004. – № 3. – С. 41-52.

антитерористичної діяльності, формувати інноваційно-креативне мислення, нові концепції, теорії, методи та технології інноваційного розвитку.

Розквіт тероризму хронологічно припадає на період початку процесів світової глобалізації та формування системи політичного і стратегічного менеджменту, вироблення та реалізації найбільш загальних всесвітніх стратегічних рішень. Сучасні центри глобального менеджменту у сфері антитерористичної безпеки інтенсивно й послідовно створюють відповідну інфраструктуру, здатну завдяки застосуванню новітніх технологій, зокрема гуманітарних та соціальних, контролювати свідомість і поведінку людей. Формування інтелектуального потенціалу систем боротьби з тероризмом, супроводження заходів антитерористичної безпеки, координації зусиль і визначення пріоритетів антитерористичних стратегій власних держав, їхніх партнерів і союзників, є пріоритетними напрямками таких всесвітньо відомих організацій, як науково-дослідного інституту Організації Об'єднаних Націй з питань злочинності та правосуддя (UNICRI)²⁰, Національного Контртерористичного центру США (NCTC)²¹, ізраїльської неурядової організації Інформаційний центр вивчення тероризму ім. Меіра Аміта (ICC)²² та інших. До речі, більшість із них повністю або частково фінансується за рахунок добровільних внесків, та випадають із сфери впливу владних структур, а залучення громадських організацій до організації антитерористичного захисту є необхідним атрибутом сучасної демократичної держави²³.

Дієвим механізмом з удосконалення антитерористичних стратегій може стати об'єднання інтелектуальних потенціалів суб'єктів боротьби з

²⁰ Науково-дослідний інститут Організації Об'єднаних Націй з питань злочинності та правосуддя / *United Nations Interregional Crime and Justice Research Institute (UNICRI)*. [Електронний ресурс]. – Режим доступу: <http://www.unicri.it/institute/>

²¹ Національний Контртерористичний центр / *The National Counterterrorism Center (NCTC)*. [Електронний ресурс]. – Режим доступу: <http://www.nctc.gov/overview.html>

²² Інформаційний центр ім. генерала Меіра Аміта по вивченню тероризма / *Meir Amit Intelligence and Terrorism Information Center (ITIC)*. [Електронний ресурс]. – Режим доступу: <http://www.terrorism-info.org.il/ru/index.aspx>

²³ Об'єднаний центр по запобіганню терористичних загроз / *Terrorist Threat Integration Center (TTIC)* – Режим доступу: <http://www.encyclopedia.com/doc/1G2-3403300752.html>

тероризмом та цивільних інституцій, громадянського суспільства. Функції синтезу керуючого інноваційним розвитком антитерористичних стратегій впливу може виконувати спеціальна консультативно-управлінська структура надвідомчої належності, тобто функціональної підпорядкованості системі соціального управління більш високого рівня, створена під егідою РНБО чи МКК, або зі статусом громадської організації, за умови повноправної участі в них представників усіх суб'єктів боротьби з тероризмом, представників громадськості, органів місцевого самоврядування, волонтерських антитерористичних рухів, міжнародних інституцій тощо.

Постіндустріальна, або інформаційна фаза розвитку суспільства, що прийшла на зміну індустріальній в якості основного ресурсу висуває знання, володіння якими визначає конкурентоспроможність не тільки суб'єктів економічної системи, але і технологій управління соціальними системами, у тому числі використовуваними в реалізації агресивно-маніпулятивних технологій і гібридних війн.

На додаток до технологій війн індустріальної епохи, заснованих на фізичному протистоянні протидіючих сторін, у війнах постіндустріального періоду широко використовуються соціально-інформаційні технології провокації соціетальних і соціальних конфліктів, основу яких складають інформаційні та інші нематеріальні активи і інтелектуальний капітал – як значущі компоненти (які впливають на ефективність) у складі потенціалу загроз або системи захисту від них.

Одним з перспективних напрямів формування стратегій протидії гібридним викликам може бути своєрідний композитний стиль (складний, змішаний, що відрізняється поєднанням елементів інших стилів) формування симетричної відповіді. Мова йде не тільки про формування стратегій протидії незаконним збройним формуванням, диверсійно-розвідувальним та терористичним групам і організаціям, а й урахування їх соціального резонансу, вірніше проведення цілеспрямованого, контрольованого, свідомого процесу, у результаті якого з'являються добре продумані стратегії,

які враховують, прогнозують та при необхідності формують за допомогою спеціальних інформаційних операцій реакцію не тільки місцевого населення, а й думку громадськості, геополітичних гравців, блогосферу та інші елементи інформаційного середовища²⁴. Безумовно, формування й реалізації інноваційних стратегій боротьби з тероризмом та супутніми йому викликами потребує відповідного рівня інтелектуального забезпечення: розробки, перевірки, впровадження та корегування системи наукових знань щодо можливих, в будь який спосіб, шляхів вдосконалення протидії терористичній злочинності, інноваційних можливостей та компетенцій суб'єктів боротьби з тероризмом. Інтелектуальне забезпечення антитерористичної діяльності щільно пов'язане з цілим комплексом наук та системою їх трансформації у відповідні компетенції²⁵.

Незважаючи на актуальність питання боротьби з тероризмом – в державі другий рік поспіль проводиться масштабна антитерористична операція, питання інтелектуального забезпечення механізмів протидії та функціонування суб'єктів боротьби з тероризмом як наукова проблема на рівні фундаментальних теоретичних досліджень майже не розглядалася. На думку авторів, такий стан спричиняють, з одного боку, усе ще недостатнє з'ясування сутності самого процесу формування теророгенності соціальних систем та алгоритмів протидії на рівні нейтралізації загроз терористичного характеру, а з іншого – скудність інтелектуального забезпечення інноваційного розвитку системи боротьби з тероризмом та хибність уявлення про дієвість фізичної протидії тероризму як соціальному процесу, на відміну від терористичній діяльності, де антитерористична операція – єдиний дієвий засіб боротьби.

²⁴ *Леонов Б.Д., Рижов І.М. Композитна стратегія протидії мережевим та гібридним викликам сучасного тероризму / Б.Д. Леонов, І.М. Рижов // Правова інформатика. – 2015.– № 1(45).– С.68-74.*

²⁵ *Кудінов С.С., Рижов І.М., Авілова Н.О. Тероризм як об'єкт наукового дослідження: проблеми й перспективи / С.С. Кудінов, І.М. Рижов, Н.О. Авілова // Науковий вісник НА СБ України. – 2015. – № 55. – С.149-158.*

В умовах гібридно-інформаційних загроз, боротьба з тероризмом набуває ознак інтелектуалоемного інструменту соціального маркетингу, який вимагає високого рівня спеціальних знань та компетенцій. У зв'язку з сутнісними відмінностями сучасних інтелектуально насичених технологій ведення війн від традиційних, для ефективного функціонування системи антитерористичного захисту необхідна зміна принципів і моделей антитерористичної діяльності, формування інноваційно-креативного мислення, нових концепцій, теорій, методів та технологій інноваційного розвитку.

Еволюційний перехід в розвитку системи боротьби з тероризмом від стадії пасивного очікування терористичних проявів до інноваційного розвитку вимагає зміни методологічного підходу до дослідження і регулювання цього процесу: від лінійно-рівноважного підходу, який розглядає боротьбу з тероризмом як залежний від навколишнього середовища пасивний процес до синергетичного, що забезпечує його інтерактивну взаємодію з середовищем - соціальною системою.

У таких умовах, безсумнівно, менеджмент знань змінює всі традиційні принципи, підходи та моделі розвитку конкурентоспроможного військового та конспієнтального (гібридного) протистояння протиборчих сторін, за рахунок використання нових видів агресій, в яких основна питома вага починають займати нематеріальні активи (соціально-політичні, технологічні, інформаційні, фінансові і т. п.), які є наслідком ефектного використання інтелектуального капіталу держави (соціальної системи). Отже, зростає роль ефективного управління інтелектуальними ресурсами, їх переважаюче становище в загальній системі забезпечення національної безпеки. Все це обумовлює необхідність інтелектуалізації системи боротьби з тероризмом і, в тому числі її військової складової, що виражається не тільки в тому, що основним продуктом антитерористичної діяльності все частіше виступає інтелектуальний і високотехнологічний продукт (інформаційні, соціально-психологічні, медійні та інші маніпулятивні технології, інформаційне

забезпечення, техніки провокації соціальних конфліктів, гібридних воєн і т. п.), але і в тому, що суспільство стає активним учасником цих процесів використовуючи власний інтелект і можливості віртуальних спільнот та соціальних мереж.

При розробці аналогічних концептуальних положень в Україні доречно використати досвід ФРН з формування Концепції основних заходів антитерористичного захисту, де відправною точкою є організація багатоступінчастого процесу аналізу і планування, який включає в себе виявлення ризиків і подальшу перевірку і, за необхідності, адаптацію технологічних, будівельних, організаційних, інформаційних, кадрових і інших заходів захисту. Вважається, що основою систем ризик-менеджменту є визначення політики щодо ризиків в якості складової підприємницької ділової політики, яка встановлює напрямки щодо запобігання ризиків і реагування в разі їх виникнення. Системи антитерористичного ризик-менеджменту, створюються на основі багатофазовий моделі аналізу ризиків, які спираються на певну для конкретного підприємства політику щодо ризиків²⁶:

1. У рамках здійснення аналізу ризиків слід виявити і проаналізувати всі ризики, що мають значення для конкретного підприємства, включаючи погрози, згадані в концепції основних заходів антитерористичного захисту, дати їм індивідуальну оцінку для кожного окремого підприємства.

2. У рамках здійснення спостереження за ризиками необхідно створити системи раннього попередження та контролінгу та, в разі необхідності, адаптувати політику підприємства відносно ризиків.

3. Велике значення для підприємств має питання фінансування ризиків, причому на перший план повинні висуватися міркування середньо- і

²⁶ *Визначення концепції захисту критичної інфраструктури робочої групи «РГ КРІТІС» у Федеральному міністерстві внутрішніх справ. – Режим доступу: http://www.bmi.bund.de/DE/Themen/Bevoelkerungsschutz/Schutz-Kritischer-Infrastrukturen/schutz-kritischer-infrastrukturen_node.html (дата звернення: 15.03.14). – Назва з екрана.*

довгострокового плану, щоб мати змогу належним чином оцінити переваги інвестиції у безпеку в умовах конкуренції.

4. Введенню системи ризик-менеджменту в організаційному плані може сприяти призначення уповноваженого з питань ризиків , який разом з уповноваженим з безпеки на підприємстві, а також з компетентними державними чи недержавними органами , що не відносяться до підприємства, розробляє концепцію ризик-менеджменту і постійно адаптує її з урахуванням змін у рамкових умовах.

Головне завдання Концепції основних заходів захисту полягає в захисті людського життя шляхом зниження рівня вразливості елементів критичної інфраструктури по відношенню до природних явищ, подій, викликаних технічними збоями або людськими прорахунками, а також до терористичних актів або злочинним діянням. Відповідно, перелік основних заходів захисту повинний враховувати стандартизовані оперативно-технічні, будівельні, організаційні, кадрові та інформаційні заходи безпеки. Адресатом розробок стратегічних концепцій аналізу загроз, систем ризик-менеджменту, а також заходів з мінімізації ризиків має бути, перш за все, керівництво інфраструктурних організацій, яке у разі вчинення порушень має взяти на себе підприємницький ризик, а при необхідності також ризик можливої матеріальної відповідальності. Саме інфраструктурні організації володіють досить детальною інформацією щодо власних елементів інфраструктури і в змозі прийняти ефективні конкретні заходи захисту. Позитивним також є досвід організації антитерористичного ризик-менеджменту та інформаційної взаємодії об'єктів інфраструктури²⁷.

Інноваційна діяльність в сфері боротьби з тероризмом не можлива без створення системи знань, навичок і умінь у сфері протидії тероризму (профілактика тероризму, боротьба з ним, мінімізація і (або) ліквідація наслідків прояви тероризму) з урахуванням масштабу загроз та ризиків.

²⁷ Рижов І.М. Досвід Федеративної Республіки Німеччини з формування концепції антитерористичного захисту критичної інфраструктури / І.М. Рижов, В.Г. Хлань, М.В. Мірошник // Зб. наук. пр. НА СБ України. – 2014. – № 51. – С.134-141

Формування гармонійно розвиненої та підготовленої особистості здатної протистояти гібридним викликам сучасного тероризму, і, що особливо актуально, підготовка висококласного фахівця в галузі боротьби з його проявами, виходить на рівень значущих для національної безпеки проблем та потребує особливої уваги з боку СБ України, як головного суб'єкта боротьби з тероризмом. У такій ситуації, Національна академія СБ України, як єдина структура СБ України, до складу якої входить науковий підрозділ, має відігравати роль ініціатора впровадження новітніх дослідницьких технологій та пошуку оптимальних шляхів і засобів боротьби з тероризмом.

Події, що відбуваються в Україні протягом останніх років, на жаль, свідчать про те, що хвиля тероризму в буквальному значенні накрила Україну. Водночас їх не можна розглядати як випадкові: закономірність подібних трагедій визначається відповідними суспільними процесами. Першопричини таких кризових станів приховані в проблемах соціального управління, коли примусова зміна або корекція його алгоритму відбувається внаслідок соціального конфлікту, обтяженого терористичною діяльністю. Подібні процеси мають властивість повторюватися в процесі еволюційного розвитку людського суспільства, причому з плином часу їхні масштаби збільшуються, якісні характеристики поліпшуються, вбираючи досягнення технічного та технологічного прогресів, породжуючи нові, більш ефективні способи протистояння сторін. Похибки алгоритму соціального управління, насамперед на рівні формування теророгенності соціальних систем, попередження (прогнозування) активізації терористичної діяльності, найчастіше призводять до трагедії.

Основною причиною таких сумних наслідків є недосконалість загальної стратегії боротьби з тероризмом, насамперед у сфері попередження (прогнозування) активізації терористичної діяльності. Відсутність на сучасному етапі розвитку українського суспільства концепції ефективного соціального управління суспільними процесами робить актуальною проблему

формування дієвої соціально-інформаційної політики упереджувального впливу на соціальні процеси, що провокують терористичну діяльність. Складність розробки концепції безконфліктного соціального управління, здатного підтримувати оптимальний стан соціальної організації суспільства та формуючих її суспільних відносин, обумовлена багатофункціональністю системи соціального управління суспільними відносинами, міждисциплінарний характер якої передбачає знання соціології, політичних, економічних, правових, психологічних та інших наук²⁸. Розширення теоретичного арсеналу та практичного управлінського потенціалу систем соціального управління може зробити вагомий вплив у досягнення стабільності та оптимізації безконфліктності суспільних відносин за рахунок розробки та результативного впровадження інноваційних ресурсів, виявлення прихованих резервів інституцій державного управління, насамперед Служби безпеки України.

Відмічаючи повноту аналізу факторів впливу на терористичну злочинність, визначаються лише загальноописові та типологічні категорії, тому їх застосування як теоретичного базису для практичного використання, наприклад побудови моделей або визначення загроз терористичного характеру, вкрай ускладнене. Зазначена проблематика залишається недостатньо охопленою. Ризики та загрози терористичного характеру завжди детерміновані – причиново обумовлені, формуються під впливом інших соціальних процесів та можуть бути визначені за умовними параметрами.

Можна виділити як пріоритетний традиційно-діалектичний підхід до розуміння причиновості тероризму (за аналогами з кримінології) і, відповідно, до аналізу детермінант ризиків та загроз терористичного характеру. У ньому виділяються умови зовнішнього матеріального середовища, що впливає як на громадську свідомість у цілому, так і на конкретну людину, а також безпосередні або найближчі причини ризиків та загроз терористичного характеру, що зв'язуються з характеристиками конкретної особистості. У межах

²⁸ *Анатомія кризисов / [А. Д. Арманд, Д. И. Люри, В. В. Жерихин и др.]. – М. : Наука, 1999. – 238 с.*

цього підходу вплив умов на причини і причин на поведінку є односпрямованим: умови, заломлюючись у свідомості людини, формують причини, які визначають конкретний вчинок. З урахуванням особливостей використання гібридних технологій формування сучасних соціальних кризових станів особливий інтерес становить підхід, що пояснює виникнення ризиків та загроз терористичного характеру зовнішнім провокативно-силовим або інформаційним впливом. Такий вплив розуміється не тільки як фізичне, а й соціально-психологічне явище в різних його варіантах. Визначальним напрямом дослідження детермінації тероризму в контексті його розуміння як глобального соціального процесу має бути розроблення концептуальної соціально-інформаційної моделі ризиків та загроз терористичного характеру, яка в змозі виявити специфіку їхньої детермінації, механізмів функціонування й ефективного використання ресурсів системи державного управління та контролю в умовах реального трансформаційного процесу в Україні, обтяженого проведенням антитерористичної операції та сепаратистсько-екстремістськими настроями. Беручи до уваги базове тлумачення загроз національній безпеці, загрози терористичного характеру – це наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України внаслідок скоєння терористичного акту. Під загрозою терористичного характеру розуміють потенційні дії або події, що прямо чи опосередковано сприяють виникненню терористичної діяльності.

Заходи з прогнозування, виявлення та усунення терористичних загроз передбачені у положеннях п.1 Концепції боротьби з тероризмом, схваленої Указом Президента України від 25.03.2013 року №230 як дійовий напрям запобігання терористичній діяльності.

При розробці пропозицій з віднесення загроз до терористичних враховано досвід Європейської програми по захисту критичних інфраструктур "European Critical Infrastructure Warning Information Network

(CIWIN)"²⁹, в основі якої закладений принцип протистояння всім небезпекам в умовах боротьби з загрозами тероризму. Цей принцип передбачає, що в процесі вироблення критеріїв віднесення загроз та небезпек до терористичних, пріоритетне значення має бути надано загрозі тероризму (диверсії) у відношенні до особи – як головного об'єкта можливих терористичних посягань, з обов'язковим урахуванням ризиків соціально-психологічного впливу на громадськість та суспільство, обумовлених подібними загрозами.

Аналіз загроз терористичного характеру є визначальним у логіко-семантичній конструкції класифікації терористичних загроз та ідентифікації об'єктів можливих терористичних посягань³⁰.

Основною диспозицією при визначенні критеріїв віднесення об'єктів до переліку можливих терористичних посягань, є припущення, що основним об'єктом терористичних посягань є особистість, точніше її центральні диспозиції по відношенню до діючого алгоритму соціального управління (існуючої системи влади), механізмом формуючого впливу є суспільно-політична реакція суспільства на небезпеку, провоковану у будь який спосіб з терористичною метою³¹.

Відповідно, критерії ідентифікації загроз терористичного характеру мають це враховувати.

З метою віднесення об'єктів до можливих терористичних посягань терміни вживаються у такому значенні:

Об'єкт терористичного посягання – під об'єктом терористичного посягання слід розуміти будь-які адміністративні або соціально-економічні

²⁹ *Critical Infrastructure Warning Information Network (CIWIN)* https://ec.europa.eu/home-affairs/what-we-do/networks/critical_infrastructure_warning_information_network_en

³⁰ Рижов І.М., С.С. Кудінов Актуальні питання формалізації об'єктів можливих терористичних посягань *Науковий вісник НА СБ України*. – 2015. – № 56. – С. 93-101.

³¹ Рижов І.М., Кудінов С.С. Цілевизначення та методичні засади ідентифікації об'єктів можливих терористичних посягань/ С.С. Кудінов, І.М., І.М. Рижов / *Збірник наукових праць НА СБ України*. – 2015. – № 55. – С.80-87.

об'єкти, споруди та майнові комплекси (незалежно від форм власності та кількості осіб, які там одночасно перебувають), фізичні особи та їх об'єднання, громадсько-політичні, фінансові, соціально-побутові інститути та процеси, інформаційний простір, місця, ділянки місцевості або території, де відбувається їх діяльність і стосовно яких терористи шляхом скоєння протиправних дій намагаються досягнути мети терористичної діяльності

Терористична загроза (загроза терористичного характеру) – потенційні дії або події, які прямо чи опосередковано сприяють виникненню терористичній діяльності; висловлений (проявлений) в будь-якій формі намір спричинити фізичну, психологічну, матеріальну чи іншу шкоду, що створює небезпеку життєво важливим інтересам людини, суспільства і держави.

Вражаючий фактор терористичної загрози – чинник життєвого середовища, який за умов вчинення (загрози вчинення) терористичної акції та пов'язаною з нею надзвичайною ситуацією сприятиме досягненню мети терористичної діяльності; виступає не в якості мети, а в якості засобу досягнення мети та є початковим у ланцюгу подій (складових ТД), спрямованих на досягнення мети терористичної діяльності.

Соціально-політична реакція суспільства – ризик виникнення соціальних конфліктів (небезпек) з явно вираженими масовими політичними настроями. Масові політичні настрої - це однорідна для досить великої кількості людей суб'єктивна, складна афективно-когнітивна сигнальна реакція, особливі переживання комфорту чи дискомфорту, що відображають задоволеність чи незадоволеність загальними соціально-політичними умовами життя; суб'єктивну оцінку можливості реалізації соціально-політичних домагань за даних умов; а також прагнення до зміни умов заради здійснення бажань. Масові політичні настрої являють собою особливий політико-психологічний феномен, що не зводиться до «громадського настрою», який традиційно фігурує. Вони включають соціально-нормативні (власне «громадські»), а й інші складові, що виникають в результаті переживання відповідності суспільних нормативів в реальному житті. Інколи

масові настрої можуть мати чітко деструктивну у відношенні до пануючої суспільно-політичної системи спрямованість, внаслідок яких відбувається корекція масової свідомості).

Загальноприйняті в ЄС процедури виявлення і встановлення європейських критичних інфраструктур ("ECIs") і проведення оцінки необхідності посилення їхнього захисту, формування критеріїв значущості об'єктів, зокрема, в контексті наслідків можливих терористичних посягань є комплексними та мають враховувати³²:

a) критерій за кількістю жертв (оцінка проводиться з урахуванням кількості потенційних загиблих або поранених);

b) критерій, пов'язаний з економічними наслідками (оцінка проводиться з точки зору значущості економічних втрат та / або ступеня погіршення якості продуктів або послуг; включає можливі наслідки для навколишнього середовища);

c) критерій впливу на населення (оцінка проводиться з точки зору впливу на суспільну довіру, фізичних страждань і порушення у повсякденному житті, включаючи втрату можливості надання важливих послуг).

При визначенні критеріїв віднесення об'єктів до переліку можливих терористичних посягань раціонально виходити з того, що зміст поняття «критерій» (др. - грец. Κριτήριον - здатність розрізнення, засіб судження, мірило) – ознака, підстава, правило прийняття рішення з оцінки будь-чого на відповідність висунутим вимогам (міру).

Критерієм віднесення об'єктів незалежно від форм власності до об'єктів можливих терористичних посягань є можлива соціально-політична реакція суспільства на небезпеку внаслідок сукупного впливу на даний об'єкт вражаючих факторів терористичних загроз.

³² Рижов І.М., Мусієнко І.І., Глуценко Л.Г., Сігарьов С.С. Антитерористична безпека ЄС у нормативно-правових актах і документах : огляд / І.М.Рижов, І.І.Мусієнко, Л.Г.Глуценко, С.С.Сігарьов. – Київ : Нац. акад. СБУ, 2016. – 176 с.

Цей критерій характеризує ефективність терористичного впливу на суспільство, ступінь досягнення мети терористичного акту, надає можливість відрізнати терористичні загрози від інших, наприклад, диверсійних.

Його треба розглядати як комплексний, такий, що включає в себе такі компоненти:

- певна кількість вражаючих факторів та ступінь вірогідності їх настання з урахуванням місця розташування конкретного об'єкту й часу;
- реакція об'єкту та системи забезпечення його безпеки на вражаючі фактори терористичних загроз;
- ступінь суспільної небезпечності наслідків з урахуванням можливих надзвичайних станів (ситуацій), які передують та провокують соціально-політичну реакцію суспільства.

Виходячи із вищевикладеного, можливо прийти до висновку, що існують загальні та спеціальні критерії віднесення об'єктів незалежно від форм власності до можливих терористичних посягань.

З метою врахування та запозичення позитивного досвіду ЄС в контексті визначення критеріїв віднесення об'єктів незалежно від форм власності до можливих терористичних посягань, та, відповідно, загроз терористичного характеру, вважається доцільним вказати на наступні:

- вплив на населення (число постраждалих, загиблих, осіб, які отримали значні травми, а також чисельність евакуйованого населення);
- економічна шкода (розмір економічних втрат, як прямих, так і непрямих);
- екологічна шкода (вплив на населення та навколишнє природне середовище);
- взаємозв'язок з іншими елементами критичної інфраструктури;
- політичний ефект (втрата впевненості у дієздатності влади); тривалість впливу (як саме і коли проявлятимуться наслідки, пов'язані зі втратою або пошкодженням об'єктів критичної інфраструктури).

Останній критерій є найбільш специфічним, зміст якого охоплює такі компоненти:

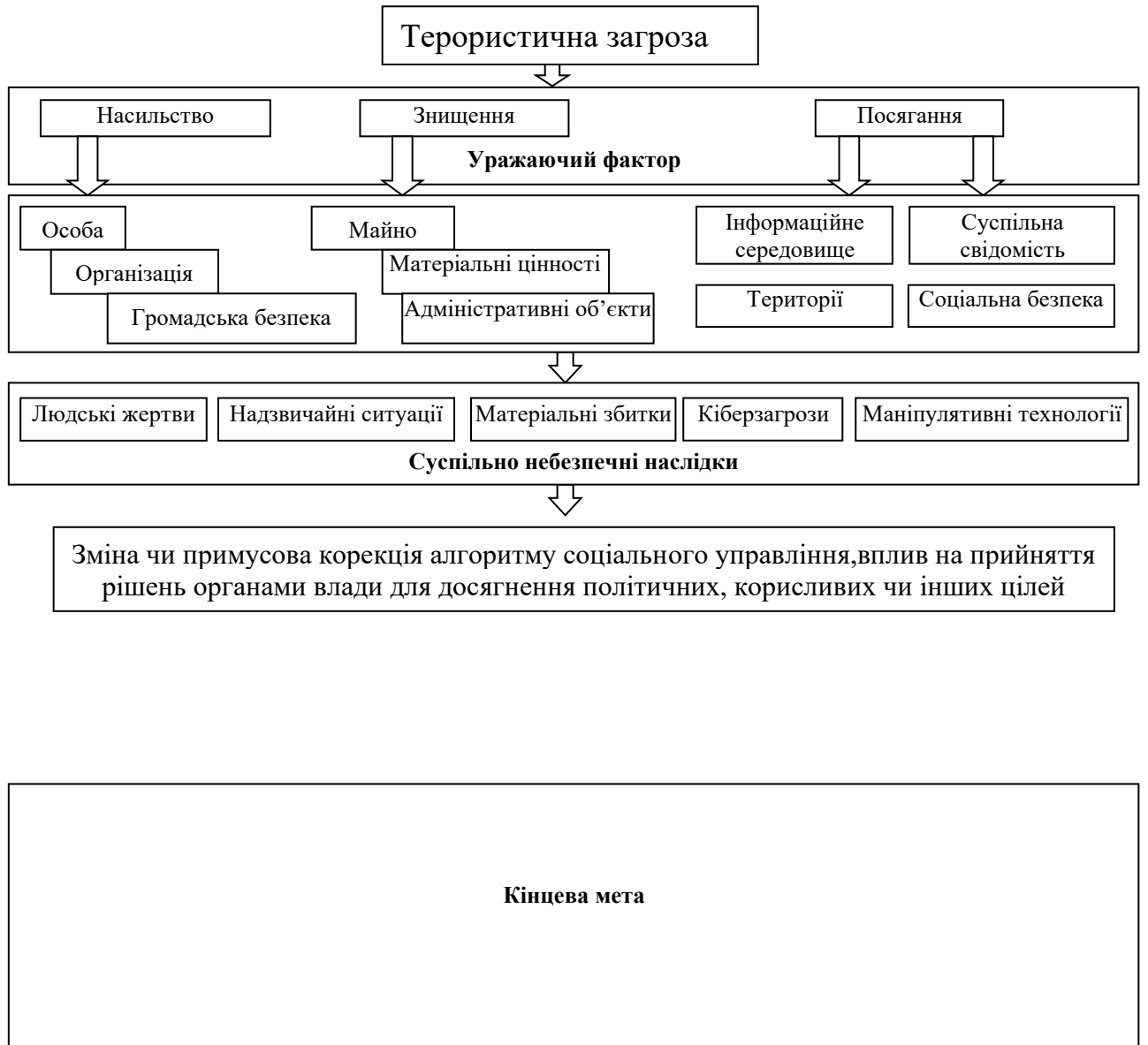
- певна кількість вражаючих факторів та ступінь вірогідності їх настання з урахуванням місця розташування конкретного об'єкту й часу;
- реакція об'єкту та системи забезпечення його безпеки на вражаючі фактори терористичних загроз;
- ступінь суспільної небезпечності наслідків з урахуванням можливих надзвичайних станів (ситуацій), які передують та провокують соціально-політичну реакцію суспільства.

Проблема розпізнавання загроз терористичного характеру із використанням сучасних інформаційних технологій потребує подальшої поглибленої розробки. Найбільш прийнятний з огляду на можливість реалізації в системах моніторингу метод розпізнавання загроз терористичного характеру – метод експертних оцінок. Цей метод прогнозування заснований на припущенні, що на основі думок експертів можна емпірично описати й аксіоматично прогнозувати стан функціональних параметрів, у першому наближенні побудувати адекватну модель майбутнього розвитку об'єкта прогнозування³³. Формалізований набір ознак загроз терористичного характеру може мати визначену їхню кількість, що дозволяє (на думку експерта) із визначеною достовірністю прогнозувати можливу теророгенність наслідків.

Як відомо, за певних умов (у разі неможливості розв'язання сутності протиріччя) соціальний конфлікт може призвести до насильства в суспільстві. Одним із варіантів виходу з такого конфлікту є застосування тактики тероризму. Тому виявлення загроз терористичного характеру для забезпечення функціонування державної системи боротьби з тероризмом є основним етапом організаційно-профілактичної діяльності.

³³ Горбулін В. П. Стратегічне планування: вирішення проблем національної безпеки : монографія / В. П. Горбулін, А. Б. Качинський. – К. : НІСД, 2010. – 288 с.

Схема 1.



Варто зазначити, якщо причини і цілі терористичної діяльності – категорії реальні і конкретні, то її мотивація в повному обсязі не завжди усвідомлюється діючим суб'єктом і значною мірою присутня на несвідомому рівні. Тому при всій важливості психофізіологічного і біологічного аспектів дослідження терористичної діяльності результати, що виявляються в процесі їхнього аналізу, не можуть бути використані як параметри для типологічної класифікації в межах моделювання теророгенності соціальних систем, але мають бути опосередковано враховані в експертному висновку щодо ступеня захищеності від терористичної загрози.

Достовірне оцінювання стану захищеності суспільства від проявів тероризму може проводитися лише на підставі постійного моніторингу загроз терористичного характеру (під загрозою терористичного характеру розуміють потенційні дії або події, що прямо чи опосередковано сприяють виникненню терористичної діяльності).

Загрози можуть бути поділені на внутрішні, зовнішні, комплексні. Слід визначити характер загрози, у яких сферах вона найбільш небезпечна (політична, економічна, воєнна, інформаційна, екологічна, соціальна, демографічна, духовна, етнічна, конфесійна та ін.), якими засобами може бути створена, на які об'єкти спрямовується (загрози особистості, суспільству, державі), якою рушійною силою володіє, чи може бути підсилена, які можуть бути прямі та побічні наслідки тощо.

Існують деякі види загроз, що мають визначені рівні. Наприклад, терористична загроза має п'ять рівнів: дуже високий, високий, підвищений, середній, низький³⁴. Рівень загрози, як правило, визначається здебільшого експертним шляхом. Найбільш розповсюдженим методом виявлення загроз та небезпек є метод зіставлення. Метод передбачає ідентифікацію загрози або небезпеки шляхом зіставлення з відомими загрозами (небезпеками), що заздалегідь занесені в накопичений банк даних варіантів проявів загроз (не

³⁴ Постанова Кабінету Міністрів України “Положення про єдину державну систему запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків” від 15.08.2007 р. № 1051.

будучи до кінця упевненим, що всі варіанти вже перевірені), які вже мали місце. В Україні відомі загрози стосовно основних сфер національної безпеки у систематизованому виді представлені в законі “Про основи національної безпеки України”³⁵. На жаль, цей перелік не є відкритим (тобто його не можна без згоди Верховної Ради України розширювати або скорочувати).

Для прогнозування динаміки небезпек і загроз, як свідчить світовий і вітчизняний досвід, потрібна превентивна діагностика. Щоб точно прогнозувати небезпеки, необхідні відповідні методи, засоби й об’єктивні знання їхніх причиново-наслідкових зв’язків.

У сучасній практиці оцінювання лежать методи, запозичені з різних галузей соціально-наукового знання, насамперед соціології, економіки, політичного аналізу і права. При виборі конкретного методу, якщо є така можливість, то перевагу слід віддавати кількісним методам.

Основна проблема полягає в тому, що майже всі кількісні методи також можуть розглядатися як якісні. Як правило, при оцінюванні використовуються комбінації якісних, кількісних та експертних методів. У кожному окремому випадку вибір методу оцінювання – ключова проблема. Вимірювання результатів та ефектів обумовлюється характером збору даних. Аналітики провідних країн світу використовують багато різних методів діагностики (оцінювання) небезпек та загроз. Розглянемо найбільш вживаний табличний метод³⁶. Цей метод дозволяє оперувати як із кількісними, так і з якісними показниками. Якісні показники оцінюються за допомогою спеціально розроблених для цього бальних шкал. Найбільш уживаною для цього методу вважається восьмибальна шкала від 1 до 8 балів.

Підготовча операція діагностики розпочинається з уточнення бази даних загроз та небезпек станом на визначену дату проведення оцінювання. Залежно від мети оцінювання на цьому етапі визначається коло держав для оцінювання, а з боку кожної держави – перелік небезпек та загроз у

³⁵ Закон України “Про основи національної безпеки України” / Відомості Верховної Ради України. – 2003. – № 39. – Ст. 351.

³⁶ Хохлов Н. В. Управление риском / Н. В. Хохлов. – М. : ЮНИТИ-ДИАНА, 2001. – 239 с.

визначених сферах національної безпеки. Для кожної загрози або небезпеки розробляється відповідний опитувальний лист.

Наступною операцією є заповнення опитувальних листів, у яких по кожному з типів загроз і пов'язаних із ними можливих наслідків оцінюються ймовірність реалізації загроз та їхні рівні, а також рівні вразливості як ступінь легкості, з якою ця загроза здатна спричинити деструктивну дію.

Оцінювання проводиться в якісних шкалах. Наприклад, рівень загроз й уразливостей оцінюється за шкалою “високий–середній–низький”. Необхідну інформацію збирають, опитуючи експертів, які є фахівцями у сфері, де виявлена загроза. У загальному випадку алгоритм розпізнавання загроз терористичного характеру можна умовно звести до двох стадій. Перша, у процесі якої з усієї сукупності факторів, що визначають стан соціального середовища, вибираються найчастіше на інтуїтивній основі такі, що призводять до виникнення конфліктних ситуацій. До кожного класу загроз може бути віднесено певну кількість підкласів або змістовних складових. Для регулювання рівня загроз використовується спеціальний інструментарій, основу формування якого становить класифікація загрозливих факторів та, як результат, визначається оцінка ступеня захищеності конкретного об'єкта від указаної загрози терористичного характеру³⁷.

Друга стадія припускає прогнозування розвитку цих факторів з урахуванням можливих змін ситуації, впливів інших факторів, норм і правил тощо. Якщо в результаті прогнозування можливий такий вихід, що прямо або побічно сприяє виникненню тероризму, ці фактори можна вважати теророгенними, відповідно, можна визначити об'єкт, що підпадає під сферу впливу цього фактора. Прогнозування може здійснюватися будь-яким із відомих методів, при цьому повинні враховуватися необхідні й достатні умови переростання конфлікту в терор.

³⁷ Рижов І. М. Перспективи формування уніфікованого інформаційного середовища у сфері протидії загрозам терористичного характеру / І. М. Рижов // Інформаційна безпека людини, суспільства, держави. – 2014. – № 3(16). – С. 56-62.

Із метою об'єктивного визначення ступеня небезпеки або теророгенного потенціалу тієї чи іншої загрози можуть бути запроваджені формальні критерії, визначення яких і становить основне завдання інформаційно-аналітичної діяльності контртерористичних підрозділів. Комплекс заходів у боротьбі з терористичними проявами варто передбачити в рамках державної системи реагування на терористичні загрози. Передусім мають бути визначені й описані потенційні теророгенно небезпечні об'єкти на території. У зазначеній системі залежно від рівня загроз необхідно визначити відповідний правовий режим, що міститиме адміністративно-режимні, оперативно-розшукові й інші заходи, реалізовані оперативними штабами у взаємодії з антитерористичними комісіями й підрозділами суб'єктів боротьби з тероризмом, а також перелік тимчасових обмежень, спрямованих на недопущення терористичних актів і мінімізацію їхніх наслідків.

Застосовуючи технологію оцінювання ризиків та загроз терористичного характеру, Служба безпеки України (у діалоговому конструкті відносин влади з суспільством) набуває нових функцій – зондування стану соціуму та оперативний контроль над ним. Зазначене вимагає вже нового розуміння відносин між діяльністю правоохоронної системи і соціальною реальністю.

З огляду на власний досвід та наукові рекомендації, удосконалення системи боротьби з тероризмом неможливе без досконалого механізму ризик-менеджменту, моніторингових досліджень його результатів, здатності правоохоронних органів та спеціальних служб прогнозувати терористичні прояви й сповіщати про їхній ризик заздалегідь, до того, як вони стануть очевидними для всього суспільства. Адресатом розробок стратегічних концепцій аналізу загроз та заходів із мінімізації ризиків має бути насамперед об'єкт терористичних посягань.

5. ЕЛЕМЕНТИ РИЗИК-ОРІЄНТОВАНОГО ПІДХОДУ В СУЧАСНИХ КОНЦЕПЦІЯХ ПРОТИДІЇ ТЕРОРИЗМУ

Світова спільнота визнає тероризм однією з найбільш серйозних загроз міжнародному миру і безпеці людству, а подальше поширення терористичних ризиків і загроз зумовлює необхідність удосконалення існуючих та пошуку нових підходів до побудов сучасних концепцій протидії тероризму. Одним із таких є ризик-орієнтований підхід (РОП), який заснований на застосуванні різноманітних методик оцінки ризиків (risk assessment), управління ризиками (risk management) та знайшов своє відображення в стратегіях протидії тероризму провідних західних країн (США, Канада, країни ЄС). Початок застосування європейським співтовариством підходу "антикризового управління" (crisis management) в боротьбі з тероризмом, який являє собою складову частину більше широкого підходу "всіх небезпек" (all hazard) та все більш активно використовується в ЄС для розгляду загроз безпеці, пов'язується з прийняттям у грудні 2005 року нової Контртерористичної стратегії ЄС під назвою "Запобігати, Захищати, Руйнувати, Відповідати" (Prevent, Protect, Disrupt, Respond). Стратегія відображає усвідомлення того, що репресивні заходи по боротьбі з тероризмом необхідно поєднувати з превентивними³⁸.

Ефективні методології оцінки ризиків є основою програм захисту об'єктів критичної інфраструктури зарубіжних країн від широкого спектру природних та техногенних загроз, у тому числі терористичного характеру. РОП необхідний для ідентифікації загроз, оцінки уразливості об'єктів захисту від їх впливу, приймаючи до уваги ймовірність реалізації загроз. Це ключове положення відрізняє РОП від звичайних методик оцінки впливів.

³⁸ Rhinard M. *The European Union and Terrorism [Text]* / M. Rhinard, A. Boin, M. Ekengren ; ed. by D. Spence. – London : John Harper Publishing, 2007. – 265 p. С. 90

Вивченню теоретичних та методологічних аспектів застосування РОП для боротьби з тероризмом присвячена значна кількість праць зарубіжних вчених. Заслужують на увагу публікації таких дослідників як Г. Г. Вілліс, А. Р. Моррал, Т. К. Келли, Дж. Дж. Медбай, Б. Ч. Езел, С. П. Беннет, Д. В. Вінтерфілд, Дж. Соколовски, А. Дж. Коллінс, Г. Гианнопоулс, Р. Філіппіні, М. Шиммер, К. Роббертс, Дж. Хорган, Г. Г. Браун, Л. А. Кокс та інших.

Українськими авторами ґрунтовний аналіз методології оцінки ризиків здійснено переважно в контексті безпеки функціонування екологічних та соціальних систем, промислових виробництв, об'єктів критичної інфраструктури, запобігання виникнення надзвичайних ситуацій. У цьому зв'язку варто виділити роботи А. Б. Качинського, Г. А. Хміля, М. З. Згуровського, Д. Г. Бобра, В. В. Кривошеїна, Ю. П. Стародуба, А. П. Гаврися, Я. І. Федюка, Г. М. Коломійця, Л. Г. Руденко, О. Л. Дронової та багатьох інших.

З урахуванням тривалого проведення антитерористичної операції на сході України, можливості поширення тероризму на інші регіони та для протидії загрозам терористичного характеру, перспектива використання РОП у побудови моделей антитерористичного захисту об'єктів можливих терористичних посягань, насамперед які відносять до критичної інфраструктури потребує додаткового дослідження.

Розгляд сутності РОП необхідно розпочинати з терміну "ризик", відносно якого, як справедливо відмічає А.Б. Качинський, існує значна невизначеність. Різними авторами та засобами масової інформації терміни "ризик" (risk), "небезпека" (hazard), "загроза" (threat) та "невизначеність" (uncertainty) часто вживаються як синоніми. У науковій літературі наводиться 18 визначень терміну "ризик", у чинному законодавстві України - близько 30-ти ³⁹. У більшості науково-технічних публікацій із даної тематики ризиком є

³⁹ Бірюков Д. С. *Захист критичної інфраструктури [Текст] : проблеми та перспективи впровадження в Україні / Д. С. Бірюков, С. І. Кондратов. – К. : НІСД, 2012. – 96 с.*

кількісна міра небезпеки, що дорівнює добутку ймовірності реалізації певної загрози, помноженій на ймовірність величини можливого збитку від неї⁴⁰.

У контексті протидії тероризму заслуговує на увагу визначення терористичного ризику та методологія його оцінювання, запропонована Центром політики управління терористичними ризиками (CTRMP) корпорації RAND (США)⁴¹. Терористичний ризик розглядається як сукупність трьох компонент: 1) загроза цілі (threat); 2) уразливість цілі до загрози (vulnerability); 3) наслідки можливої успішної реалізації терористичної загрози (consequences). У кількісному вираженні загроза цілі може бути виміряна як ймовірність того, що конкретна ціль піддається нападу певним способом протягом певного періоду часу.

Вимір загрози = P (атака відбудеться)

З метою вірного розподілу виділених ресурсів для захисту об'єктів критичної інфраструктури або міст необхідне оцінювання загроз конкретним об'єктам або від певних видів (типів, способів) терористичних атак.

Зрозуміло, що не всі загрози одного типу однаково важливі одночасно. Використовуючи для вчинення терористичного акту, наприклад, машину з вибухівкою, терористам легше завдати збитків звичайному готелю ніж військовій базі, оскільки готель є менш захищеним. Звідси впливає визначення другої складової терористичного ризику - уразливості, яка може бути оцінена як ймовірність того, що збиток буде завданий завдяки реалізації певного виду атаки у певний час стосовно конкретного об'єкта. Збитки можуть бути різних видів: загибель людей, травмування, матеріальні (руйнування будівель), екологічні, політичні тощо.

Вимір уразливості = P (атаки зі збитками / загальна кількість атак)

⁴⁰ Качинський А. Б. *Безпека, загрози і ризик [Текст] : наукові концепції та математичні методи / А. Б. Качинський. — К. : Інст. пробл. нац. без., Нац. акад. Служби безпеки України, 2004 – 472 с.*

⁴¹ *Estimating terrorist risk [Електронний ресурс]. – Режим доступу: https://docviewer.yandex.ua/?url=http%3A%2F%2Fwww.rand.org%2Fcontent%2Fdam%2Frand%2Fpubs%2Fmonographs%2F2005%2FRAND_MG388.pdf&name=RAND_MG388.pdf&lang=en&c=58769bd5be36.*

Зазначені ймовірності вираховуються окремо для кожного виду збитків. У даному випадку оцінюється т.зв. умовна ймовірність атак, які призведуть до завдання збитків (так би мовити "успішних" для терористів атак), але сам розмір збитків до поняття уразливості не відноситься. У більш складних моделях використовується діапазон збитків різного рівня, кожен з яких асоціюється зі своїм показником ймовірності.

Наслідки, як третій компонент ризику, визначаються через розмір та вид збитків від успішних терористичних атак. Вони можуть бути оцінені як умовне математичне очікування збитків (загибель, поранення, руйнування тощо), завданих конкретному об'єкту внаслідок атаки певного виду (типу, способу) у певний час.

Вимір наслідків = E (збитки / загальна кількість атак, що призвели до завдання збитків)

Ризиком є очікувані наслідки після певного періоду часу по відношенню до певної групи цілей внаслідок дії певної групи загроз. Для певної загрози, цілі та виду наслідків ризик може виміряний наступною формулою:

*Вимір ризику = P (атака відбудеться) * P (атаки зі збитками / загальна кількість атак) * E (збитки / загальна кількість атак, що призвели до завдання збитків) = загроза * уразливість * наслідки*

Іншими словами, терористичний ризик являє собою очікувані наслідки атаки, враховуючи вірогідність того, що атаки відбудуться і будуть успішними для терористів. У термінах теорії ймовірності ризик атаки певного типу це безумовне математичне очікування збитків певного виду.

Не вдаючись до детального розгляду недоліків ймовірнісно-статистичного методу розрахунку терористичних ризиків та порівняння його з іншими методами (теоретико-ймовірністними, евристичними), відзначимо лише, що до таке формулювання терористичного ризику має дві переваги. По-перше, воно забезпечує підхід до порівняння ризиків та їх складання (об'єднання). По-друге, дозволяє встановлювати чіткі зв'язки між оцінкою

ризиків (risk assessment), подальшим управлінням ризиками (risk management) та зниженням ризиків (risk reduction). Управляти ризиком можна шляхом впливу на його компоненти: загрози (використання активних заходів розвідки та контррозвідки, профілактична робота), уразливість об'єкта (удосконалення системи антитерористичного захисту) та наслідки (вжиття превентивних заходів з мінімізації можливих збитків, організація захисту населення, створення додаткових запасів продовольства, медикаментів тощо).

Незважаючи на значну кількість джерел невизначеності навколо визначення терористичних ризиків, їх оцінювання необхідне для правильного розподілу (перерозподілу) внутрішніх безпекових ресурсів. Колишній секретар Департаменту внутрішньої безпеки США Мічел Чертофф (2006) справедливо відзначав: "Ми повинні ідентифікувати та визначити за пріоритетами ризику - розуміючи загрозу, вразливість та наслідки. І тоді ми повинні розподіляти наші ресурси економічно ефективним способом"⁴².

На даний час існує значна кількість методик оцінювання ризиків, переважно в інтересах захисту об'єктів критичної інфраструктури, серед яких можна виділити три підходи в залежності від їх мети та сфери застосування: методологія оцінювання ризиків щодо інфраструктурних об'єктів, структурний аналіз та аналіз поведінки⁴³. Основу РОП складають наступні етапи:

1. Ідентифікація факторів ризику. Він полягає у виявленні всіх джерел небезпеки (загроз), подій, що ініціюють виникнення надзвичайних ситуацій, описі об'єкта та існуючих засобів захисту, можливих сценаріїв розвитку подій та їх ранжування.

⁴² *Probabilistic Risk Analysis and Terrorism Risk [Electronic resource] / B. C. Ezell, S. P. Bennett et al. // Risk Analysis. – 2010. – Vol. 30. – № 4. – P. 575 – 589. – Mode of access : <https://docviewer.yandex.ua/?url=https%3A%2F%2Fwww.dhs.gov%2Flibrary%2Fassets%2Frma-risk-assessment-technical-publication.pdf&name=rma-risk-assessment-technical-publication.pdf&lang=en&c=5877677eef51>.*

⁴³ *Giannopoulos G. Risk assessment methodologies for Critical Infrastructure Protection. Part I : A state of the art [Text] / G. Giannopoulos, R. Filippini, M. Schimmer. – Luxembourg : Publications Office of the European Union, 2012. – 44 p.*

2. Оцінка ризику. Це процес визначення ймовірності виникнення негативної події протягом певного періоду і масштабності наслідків для здоров'я людей, майна і навколишнього середовища.

3. Управління ризиком. Воно орієнтоване на мінімізацію соціально-економічних наслідків надзвичайних ситуацій техногенного і природного характеру шляхом впровадження сучасних механізмів регулювання на основі РОП та забезпечення прийняттого рівня безпеки населення і територій⁴⁴.

Наприклад, європейська методологія ризик менеджменту COUNTERACT (Cluster of User Networks in Transport and Energy relating to Anti-terrorist Activities), розроблена у рамках фінансованої Європейською Комісією програми FP6 у сфері досліджень та інновацій, сфокусована на терористичних загрозах у сфері транспортного й енергетичного секторів. Процес оцінки ризиків поділений на 2 частини: аналіз ризиків та оцінка вразливості об'єктів терористичних посягань. Ймовірність реалізації терористичних загроз градується за 5-ма рівнями: значно високий, високий, можливий, низький, малоімовірний. Така класифікація загроз базується на історії подій, що мали місце у минулому для певного типу компаній або групи схожих компаній в інших сферах. Оцінка впливів (наслідків) загроз побудована аналогічним чином і класифікується за 4-ма категоріями: катастрофічний, критичний, маргинальний та некритичний. Комбінація ймовірності реалізації загрози та її впливу утворюють 20 категорій ризику.

Оцінка вразливості здійснюється з метою пошуку додаткових потенційних заходів протидії ризикам, аналіз яких був проведений на попередньому етапі. Зазначені заходи розробляються з урахуванням наступних критеріїв: ефективності, ресурсовитратності, часу для впровадження, необхідності страхування, впливу на повсякденну діяльність.

⁴⁴ *Риски в жизнедеятельности человека [Електронний ресурс]. — Режим доступу : http://studbooks.net/70728/bzhd/riski_zhiznedeyatelnosti_cheloveka.*

Основна ідея побудови Концепції ризик менеджменту Національного плану захисту об'єктів інфраструктури США (Risk Management Framework of the National Infrastructure Protection Plan, далі - NIPP) може бути охарактеризована наступною цитатою: "Ядром NIPP є концепція ризик менеджменту, яка запроваджує процес поєднання інформації про загрози, вразливість та наслідки для того, щоб надавати всебічні, систематичні та раціональні оцінки національному та секторальному ризику"⁴⁵. Теоретичне підґрунтя NIPP становить концепція класичної оцінки ризиків, запроваджена президентською директивою з внутрішньої безпеки № 7 (Homeland Security Presidential Directive-7), яка враховує фізичні, кібер- та людські впливи для подальшого розроблення ефективних програм захисту від проявів тероризму. Концепція охоплює 17 секторів критичної інфраструктури та містить 6 етапів: встановлення мети, ідентифікація загроз, оцінка ризиків та визначення їх пріоритетів, розроблення заходів захисту та вимірювання зниження ризиків.

В системі СБ України для більш якісної класифікації результатів моніторингу і подальшої аналітичної роботи доречно використовувати відповідним чином підготовлений реєстр загроз терористичного характеру⁴⁶. Фахівцями НА СБ України запропонована методика оцінювання ефективності функціонування державної системи протидії виявленим (прогнозованим) загрозам, зокрема при обробці конкретних результатів роботи з формування реєстру загроз терористичного характеру (ЗТХ), розпочатої на підставі розпорядження керівника АТЦ на базі аналітичних підрозділів Штабу АТЦ при СБ України із залученням особового складу НОЦ НА СБ України та помічників начальників регіональних органів СБУ з

⁴⁵ *Probabilistic Risk Analysis and Terrorism Risk [Electronic resource] / B. C. Ezell, S. P. Bennett et al. // Risk Analysis. – 2010. – Vol. 30. – № 4. – P. 575 – 589. – Mode of access : <https://docviewer.yandex.ua/?url=https%3A%2F%2Fwww.dhs.gov%2Flibrary%2Fassets%2Frma-risk-assessment-technical-publication.pdf&name=rma-risk-assessment-technical-publication.pdf&lang=en&c=5877677eef51>.*

⁴⁶ *Рижов І. М. Перспективи формування уніфікованого інформаційного середовища у сфері протидії загрозам терористичного характеру / І. М. Рижов // Інформаційна безпека людини, суспільства, держави. – 2014. – № 3(16) . – С. 56 – 62*

координації антитерористичної діяльності. Вихідна інформація моделі також дає змогу кількісно оцінювати ефективність функціонування державної системи протидії тероризму та визначати межі юридичної відповідальності посадових осіб, що приймають управлінські рішення у системі⁴⁷.

Виходячи з вищевикладеного, формування реєстру ЗТХ у вигляді уніфікованого інформаційного ресурсу сприятиме вивченню ступеня готовності територіальних громад, регіональних підрозділів суб'єктів боротьби з тероризмом й окремих об'єктів до протидії можливим терористичним загрозам. Введення реєстру дозволить здійснювати структурування об'єктів підвищеної небезпеки в регіонах за їх належністю до відповідних суб'єктів боротьби з тероризмом, а також, завдяки методу експертних оцінок, відслідковувати динаміку змін у ступені їхньої захищеності. Фактично, мова йде про можливість впровадження спеціалізованого інформаційно-управлінського процесу у його повному циклі – від отримання даних до відпрацювання управлінських рішень із задіянням всіх елементів інформаційного середовища.

Вже доведено, що аналіз динаміки змін показників реєстру ЗТХ дозволяє своєчасно викривати зовнішній вплив на стан соціальної напруженості і виявляти його джерела, що, у свою чергу, надає можливість здійснювати компенсаційний вплив на інформаційне середовище у регіоні щодо якого здійснюється моніторинг⁴⁸.

Наведений вище аналіз міжнародного та вітчизняного досвіду засвідчив, що РОП є важливим інструментом в організації захисту об'єктів критичної інфраструктури від терористичних загроз і дозволяє забезпечити ефективний перерозподіл захисних ресурсів в залежності від терористичних ризиків в умовах обмеженого бюджетного фінансування. Проте, на жаль, він

⁴⁷ Богданович В. Ю., Ришов І. М., Вареньє Н. М. Методика оцінювання ефективності протидії загрозам терористичного характеру особі або малій групі людей / В. Ю. Богданович, І. М. Ришов, Н. М. Вареньє // Збірник наукових праць НА СБ України. – 2016. – № 59. – С. 109 – 119.

⁴⁸ Ришов І. М. Базові концепти антитерористичної безпеки [Текст] : монографія / І. М. Ришов ; Нац. акад. Служби безпеки України. – Київ : Нац. акад. СБУ, 2016. – 327 с.

не знайшов свого відображення в Концепції боротьби з тероризмом в Україні та функціонуванні Єдиної державної системи запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків. Наразі методологія оцінювання терористичної загрози та встановлення її рівнів залишається невизначеною.

Ризик-орієнтована парадигма забезпечення антитерористичної безпеки не може бути реалізована без елементів системного державного (цивільно-громадського) нагляду, коли традиційні механізми **інспекційного контролю захисту від можливих терористичних посягань доповнюються і модернізуються ризик-орієнтованими моделями.**

Насправді РОП це виявлення, аналіз і прогнозування небезпек терористичної діяльності, оцінка ризиків і можливих масштабів наслідків терористичних актів, визначення найбільш небезпечних (з позицій терористичної загрози) об'єктів для оптимізації необхідних організаційно-технічних заходів попередження терористичних актів, недопущення виникнення загроз терористичного характеру і підвищення ефективності антитерористичного захисту як на окремому небезпечному об'єкті так і в системі піднаглядних об'єктів в цілому.

Основне із завдань РОП полягає в побудові системи моніторингу теророгенності соціальних систем, адекватної сьогоднішньому стану, інноваційно-технологічному та кадровому потенціалу суспільства, розробці та впровадженні відповідного інструментарію та обслуговуючої його державної або громадської (можливо змішаної) виконавчої системи.

Друге завдання сучасного РОП - пошук узгодженого взаємодоповнення сучасних детерміністських та постіндустріальних засобів і методів забезпечення антитерористичної безпеки з їх формалізацією у відповідних нормативно-правових актах та регламентах і правилах (нормах).

І останнє завдання РОП – розробка так званих компенсаційних заходів, що мають запроваджуватися на підставі аналізу вірогідності ЗТХ конкретному об'єкту або системі об'єктів, оцінці наявних і доступних

кадрових, матеріально-енергетичних та науково-технічні ресурсів у формі конкретного алгоритму (регламенту). По суті, мова йде про побудову системи, що дозволяє не тільки прогнозувати ризики, але й бюджетувати управління антитерористичною безпекою на об'єктах можливих терористичних посягань.

Висновки. Вважаємо, що теоретико-правове обґрунтування основ РОП та його подальша імплементація в загальнодержавну систему боротьби з тероризмом в Україні надасть можливість отримати як кількісні так і якісні оцінки терористичних загроз та стану антитерористичної безпеки. Це, в свою чергу, створить підґрунтя для досягнення оптимального балансу між вимогами до антитерористичного захисту об'єктів можливих терористичних посягань та наявними ресурсами, дозволить здійснювати їх розподіл з урахуванням пріоритетності захисту об'єктів, наявності уразливих місць та мінімізації можливих негативних наслідків.

Внаслідок застосування методології ризик-орієнтованого підходу для прогнозування ефективності систем захисту об'єктів можливих терористичних посягань, зокрема елементів критичної інфраструктури від терористичних загроз Служба безпеки України, як головний суб'єкт державної системи боротьби з тероризмом, отримує сучасний інструмент зондування стану соціуму та оперативного контролю над ним в частині аналізу та своєчасного реагування на ЗТХ шляхом запровадження компенсаційних впливів, потенційно знижуючи їх ризики.

6. ЗАГРОЗИ ТА НЕБЕЗПЕКИ, МЕТОДИ ЇХ ВИЯВЛЕННЯ І РЕЄСТРАЦІЇ

При формалізації процесу забезпечення національної безпеки особливе місце відводиться проблемам виявлення, аналізу й оцінювання рівня і характеру загроз та небезпек для реалізації національних інтересів держави.

Класик термінології С.Ожегов поняття “загроза” визначав як “обіцянка заподіяти кому-небудь шкоду, зло”. В.Даль тлумачив загрозу як “дії або наміри загрожувати, лякати, тримати під страхом, під побоюванням, погрожувати”.

У словниках сучасної російської мови “загроза” визначається як “залякування, обіцянка заподіяти кому-небудь неприємність, зло”, “намір завдати фізичну, матеріальну або іншу шкоду, збиток суспільним інтересам, а також окремим особам або їх інтересам”. При цьому під збитком прийнято розуміти “втрату, збиток, утрату”, а шкоду трактувати як “збиток, псування”. Визначення “загроза інтересам безпеки” може бути похідним від дефініції “безпека” – “стан захищеності життєво важливих інтересів держави, суспільства і особи від внутрішніх і зовнішніх загроз”.

Як було вказано вище, для ефективної імплементації національних інтересів держави необхідно уміти своєчасно виявляти загрози й небезпеки, оцінювати їх характер, рівень, масштаби і прогнозувати можливий збиток у разі їх реалізації.

Методи виявлення небезпек і загроз.

Для того, щоб подолати хворобу, потрібно установити точний діагноз. Те ж саме стосується протидії загрозам. Чим більше інформації про загрозу в нас є, тим ефективніша може бути організована протидія.

Очевидним є той факт, що захист національних інтересів повинен мати комплексний характер і базуватися на глибокому аналізі можливих

негативних наслідків. Система забезпечення національної безпеки має бути здатною ефективно реагувати на загрози в різних сферах. До того ж у системі повинні економно витрачатися ресурси, які виділяються на забезпечення національної безпеки. Немає сенсу стріляти з гармати по горобцях і кидатися з пістолетом на танк – необхідно якомога більше знати про характер можливих загроз і небезпек.

Тому дуже важливо уміти виявляти й вивчати загрози на ранніх стадіях їх зародження. Ще В.Белінський відзначав, що “знайти причину зла – майже те саме, що знайти проти нього ліки”.

Теоретично можна будувати захист з орієнтацією на всі можливі загрози, але це економічно недоцільно. Дуже важливо вчитися на чужих помилках. Але краще спочатку уявити собі всі можливі варіанти, а потім відібрати найбільш прийнятні для конкретного випадку.

Найбільш поширеним методом виявлення загроз і небезпек є *зіставлення*. Воно передбачає ідентифікацію загрози або небезпеки шляхом зіставлення з відомими загрозами (небезпеками), які заздалегідь занесені в накопичувальний банк даних варіантів проявів загроз, які вже мали місце. В Україні відомі загрози щодо основних сфер національної безпеки в систематизованому вигляді представлені в Законі “Про основи національної безпеки України”. Цей перелік не є відкритим (тобто його не можна без згоди Верховної Ради розширювати або скорочувати).

Слід зазначити, що на сьогодні відсутні вітчизняні методики виявлення загроз і небезпек. А наявні (на жаль, переважно іноземні) дозволяють отримувати лише якісні оцінки, на які істотно впливають політичні чинники. Наприклад, Законом “Про основи національної безпеки України” визначено, що загрозою національній безпеці України є поява поблизу кордонів держави нових контингентів військ і озброєнь, які порушують співвідношення сил, що склалося. З цього випливає, що переміщення військових баз НАТО до кордонів України, за законом, є загрозою національній безпеці, але попереднє політичне керівництво держави на чолі з В.Ющенком це не

розглядало як загрозу, оскільки проводило політику інтеграції до Альянсу. Такий же підхід спостерігався щодо намірів США розмістити в Польщі, Румунії, Болгарії й Чехії систему протиракетної оборони (ПРО), незважаючи на те, що перехоплення МБР, найбільш ймовірно, буде здійснюватися над територією України.

Схема організації процедури визначення реальних загроз національній безпеці України показана на рис. 1

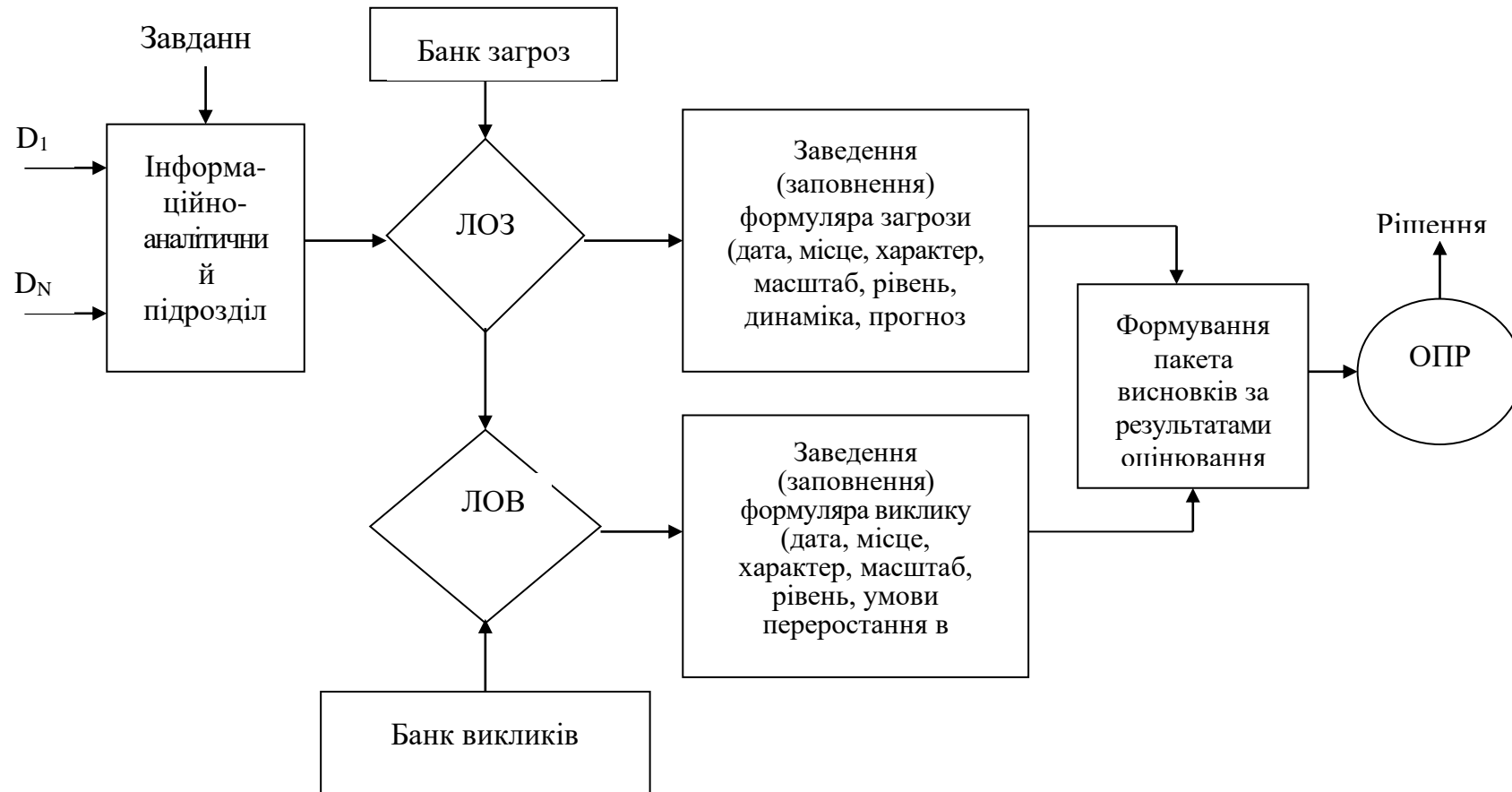


Порядок оцінювання ефективності системи забезпечення
національної безпеки держави

У вітчизняній практиці широко використовується *метод нав'язування загрози*. Нав'язування може бути як зовнішнє (іншою державою), так і внутрішнє (впливовою особою, політичною структурою або організацією). Наприклад, після грузино-осетинського конфлікту і проведення Росією операції з примушування Грузії до миру політичне керівництво України на чолі з В.Ющенком почало нав'язувати суспільству сприйняття загрози військового характеру з боку Росії, що сприяло обґрунтуванню доцільності прискорення інтеграції України до НАТО, незважаючи на спротив більшої частини населення країни.

Провідні держави світу активно застосовують і такий “старий” метод виявлення недружніх намірів інших держав, як агентурний. Зрозуміло, що даним, отриманим агентурною розвідкою, надається відповідний гриф таємності і їх оброблення проводиться спеціальними методами, які не висвітлюються у відкритому друці.

Послідовність виявлення загроз і небезпек *методом зіставлення* показана на рис. 2



. Послідовність проведення моніторингу викликів та загроз національній безпеці

У реєстрах загроз і небезпек зберігається множина відомих загроз і небезпек, які з імовірністю більше нуля можуть бути направлені проти України. Під час моніторингу з використанням логічного оператора загрози (ЛОЗ), виклику (ЛОВ) вхідна інформація зіставляється з множиною загроз, які містяться в реєстрі загроз. Якщо виявлено збіг, то цей факт фіксується у формулярі загрози. Якщо збігу не виявлено, а експерт довів, що це прояв нової загрози або небезпеки, то ця загроза (небезпека) ідентифікується як нова і на неї заводиться свій формуляр, що затверджується особою, яка приймає рішення (ОПР) у цій сфері. Природно, що ОПР цікавить не просто факт виявлення загрози, а передусім її характеристики: джерело, характер, рівень, масштаб, напрям, часовий інтервал зростання, можливі наслідки і тому подібне.

Розглянемо детальніше процедуру опису цих характеристик, які за рішенням ЛПР у подальшому відображатимуться у відповідних розділах паспорта загрози.

У науковій літературі пропонується кілька варіантів класифікації загроз національній безпеці (національним інтересам). Як підстави для класифікації вибираються ознаки, істотні для досліджуваних явищ. Одна з таких підстав – об'єкти безпеки і їхні властивості, по відношенню до яких ті або інші явища, процеси кваліфікуються в координатах виклику, небезпеки і загрози. Закон України “Про основи національної безпеки України” основними об'єктами безпеки визначає особу – її права і свободи; суспільство – його матеріальні й духовні цінності; державу – її конституційний лад, суверенітет і територіальну цілісність. Ми систематизуватимемо загрози так.

Джерело загрози. За джерелами загрози можуть бути розподілені на внутрішні, зовнішні, комплексні.

Характер загрози. Слід визначити, в яких сферах вона становить найбільшу небезпеку (політична, економічна, воєнна, екологічна, інформаційна, соціальна, демографічна, духовна, етнічна, конфесійна й ін.), якими засобами може бути створена, на які об'єкти спрямовується (загроза

особі, суспільству, державі), якою рушійною силою володіє, чи може бути посилена, які можуть бути прямі й побічні наслідки тощо.

Рівень загрози. Деякі види загроз мають певні рівні. Наприклад, терористична загроза має п'ять рівнів: дуже високий, високий, підвищений, середній, низький.

Рівень загрози визначається здебільшого експертним шляхом. Науково-методичний апарат оцінювання рівня воєнної загрози (небезпеки) для держави буде детально розглянутий у наступних параграфах. Загрозам воєнного характеру ми завжди приділяємо більшу увагу, оскільки вони можуть завдати найбільшого збитку всім об'єктам національної безпеки. До того ж воєнні загрози мають комплексний характер, що зумовлено ускладненням процесу протиборства й залежністю від параметрів загроз в інших сферах. Вектори воєнних загроз часто змінюють свій географічний напрямок і об'єкти, на які вони націлені, через зниження рівня оборонного потенціалу, посилення активності сепаратизму, релігійного екстремізму й міжнародного тероризму. Крім того, воєнні загрози можуть змінювати свій пріоритет.

Останнім часом багато дослідників уживають термін “загроза (небезпека) воєнного характеру”, під яким ми будемо розглядати загрозу (небезпеку), реалізація якої супроводжується використанням методів, сил та сучасних засобів ведення контактних та безконтактних війн або іншого впливу, що спричиняє такі ж наслідки (руйнування, каліцтва і загибель людей, порушення штатних режимів функціонування важливих об'єктів інфраструктури і життєзабезпечення адміністративно-промислового центру та ін.).

Масштаб загрози. За масштабом загрози класифікуються як локальні, національні, регіональні й глобальні.

Напрям. Загрози можуть бути направлені проти особи, суспільства, держави. Об'єктами воєнних загроз (загроз воєнного характеру) можуть бути люди, окремі об'єкти й організації, соціально-економічна система країни,

свідомість великих груп людей, культурні цінності, традиції тощо. При цьому об'єкти слід розглядати в такій послідовності: життєво важливі (їх утрата рівнозначна катастрофі), важливі (виведення їх із ладу може привести до серйозних втрат або збоїв у роботі, але в принципі втрати можуть бути поправними) і другорядні (втрата відносно незначна).

Можливі наслідки. Прогнозуються можливі деструктивні наслідки в різних сферах національної безпеки. Ступінь тяжкості наслідків, викликаних реалізацією загрози, може підрозділятися на катастрофічний (руйнівна подія), помірний (наслідки принципово усунені) й легкий (наслідки відносно не істотні).

Усі ці характеристики заносяться в паспорт загрози. Типовий паспорт загрози повинен містити такі дані:

- назва загрози;
- шифр за класифікатором (списком);
- до якої сфери належить;
- дата виявлення;
- напрям дії;
- масштаб;
- характер;
- характеристика загрози;
- характер зміни в часі (динаміка);
- хто (що) може підсилити загрозу;
- хто (що) може ослабити загрозу;
- чинники посилення загрози;
- чинники ослаблення загрози;
- можливі деструктивні прояви в інших сферах;
- додаткові відомості про загрозу.

Складність виявлення і реєстрації загроз не тільки в тому, щоб отримати вичерпний перелік тих явищ і процесів, які створюють негативний фон для

різних об'єктів безпеки. Цей перелік постійно змінюється. Зокрема про такі небезпеки, як СНІД для людини, вестернізація для суспільства або міжнародний тероризм для держави, світ заговорив тільки в останні 5–15 років. У документах провідних країн із зовнішньої політики серед нових викликів і загроз названі міжнародний тероризм, наркотрафік, організована злочинність, небезпека поширення зброї масового знищення і засобів її доставляння, регіональні конфлікти, демографічні проблеми, глобальна бідність, енергетична небезпека, а також нелегальна міграція, зміна клімату, забруднення навколишнього середовища, погіршення якості питної води та ін.

Не менше проблем пов'язано з тим, що забезпечення безпеки одного об'єкта може стати причиною виникнення небезпек для інших. Так, держава покликана бути головним суб'єктом безпеки особи й суспільства. У той же час, здійснюючи функції забезпечення безпеки, вона може перетворитися на загрозу для особи і суспільства. Наприклад, корумпована влада сама становить загрозу національним інтересам. При слабкості Закону і права, відсутності механізмів, що забезпечують безумовне дотримання всіма гілками влади чинних правових норм, держава стає джерелом багатьох небезпек. Свого часу американський фонд “Спадщина” попереджав, що розростання уряду веде “до посилення внутрішньої загрози”. Державні інститути повинні бути структуровані з погляду їхньої безпеки для суспільства. Звідси зрозуміла, наприклад, необхідність розвинутого громадянського суспільства, здатного узяти під контроль державу, її силові структури. В той же час збільшення свободи, посилення самодостатності своїм негативним результатом може мати атомізацію суспільства, зростання соціальної роз'єднаності, що сприяє розвитку тоталітаризму.

Отже, своєрідним джерелом небезпеки національному благополуччю країни є різнорідність об'єктів національної безпеки (особа, група, суспільство, держава) і незбігання (часом зіставлення) їхніх інтересів. Оскільки інтереси особи, суспільства і держави перебувають у складній та суперечливій взаємодії, говорити про їх баланс можна лише з великими

застереженнями й на певному часовому інтервалі (наприклад, у період подолання економічної кризи).

Безумовно, не можна забезпечити безпеку держави і суспільства, не захистивши їх від імовірного збройного нападу, економічної блокади, політичного диктату або зовнішнього інформаційно-психологічного пресингу. Здатність протистояти зовнішній дії формується усередині країни. Тому не можна не бачити взаємозумовленість внутрішніх і зовнішніх викликів.

По-перше, можливості держави із попередження й запобігання зовнішнім загрозам багато в чому визначаються її здатністю вирішувати свої внутрішні проблеми. Виключно важливе, якщо не вирішальне значення в організації діяльності із забезпечення державної безпеки має суб'єктивна сторона сприйняття загроз. Попри об'єктивну природу загроз безпеці, віддзеркалення людиною цього явища часто не відповідає реальному становищу. Оцінка об'єктивно наявної загрози завжди несе в собі елементи суб'єктивізму і вже через це є спотвореним відображенням об'єктивної дійсності. Інколи спотворення в сприйнятті загрози можуть досягати значних масштабів. Більше того, загроза реально існує, формується, а суб'єкти безпеки можуть не знати про це, не усвідомлювати катастрофи, що насувається (наприклад, надмірне захоплення уряду кредитами іноземних банків перетворює країну на вічного боржника зі всіма наслідками). Формування неадекватного суб'єктивного сприйняття загроз може бути наслідком некомпетентності або помилки вищого політичного керівництва чи результатом цілеспрямованої діяльності "агентів впливу", які добиваються цілей їхніх хазяїв [25].

По-друге, в сукупності загроз є чимало таких, у яких виявиться штучною будь-яка спроба розділити їхні внутрішні та зовнішні аспекти. Так, міжнародна злочинність (скажімо, наркобізнес, контрабанда або фальшивомонетництво) нас турбує тому, що порушує нормальний хід внутрішнього життя; в той же час її активність можлива тільки в тій країні із сприятливою соціальною базою.

По-третє, і вихід із внутрішніх труднощів, і попередження, і нейтралізація зовнішніх загроз багато в чому полегшує, а то й повністю забезпечує підтримка світової спільноти, особливо стратегічних партнерів. У сучасній обстановці не можливо забезпечити національну безпеку ізольовано, спираючись лише на індивідуальні зусилля, тим більше – ігноруючи світові проблеми.

По-четверте, у взаємопов'язаному світі, повному глобальних проблем, безпека будь-якої країни не може бути повністю гарантована без усунення регіональних і міжнародних небезпек. Натомість дестабілізація обстановки в одній країні, її внутрішні конфлікти інтернаціоналізуються, що посилює зв'язок внутрішніх і зовнішніх проблем безпеки (наприклад, газове протистояння України й Росії на початку 2009 року і припинення подання газу в країни ЄС). От чому немає сенсу субординувати небезпеки. Скажімо, стверджується, що в нинішніх умовах на безпеку України найбільший вплив мають внутрішні чинники. Серед них найважливіші: відсутність єдності влади, соціально-політична нестабільність, корупція, зниження якості й рівня життя людей, економічна і фінансова кризи, зростання злочинності тощо. Але багато цих небезпек підтримується зовнішніми силами.

Закономірності виникнення й розвитку небезпек і загроз.

Виникнення і розвиток небезпек, загроз та їхня взаємодія підкоряються певним закономірностям. Вони характеризуються таким [65]:

1. *Спонтанність.* Небезпеки для особи, групи, суспільства або держави можуть породжуватися мимоволі, без сторонніх зовнішніх дій, у результаті дії внутрішніх рушійних сил, причин або спонук – землетрус, епідемія (наприклад, “свинячий” грип), економічна криза, національний рух і т. д.). При цьому прогрес в одній сфері нерідко спричиняє появу проблем в іншій. Так, економічний розвиток пов'язаний із несприятливою дією на навколишнє середовище, а зміцнення обороноздатності може викликати утиск соціальних програм.

Спонтанність виникнення небезпек не виключає їх створення цілеспрямованими діями ворожих сил. Зі слів Голови Служби безпеки України, наша країна має серйозні розробки і секрети, отже, є зацікавленість у вербуванні наших громадян з боку іноземних спецслужб. Вони працюють або намагаються працювати на нашій території досить активно, вербуючи українських громадян і полюючи на наші розробки.

2. *Генералізація* (підпорядкування окремих (локальних) явищ загальному принципу), в результаті якої, здавалося б, часткова проблема, тимчасова трудність набуває хворобливого для всього соціального організму характеру, а її подолання стає в центрі уваги суспільства і вимагає загальнодержавних, політичних заходів. Скажімо, злочинність є у всіх країнах. Вона завжди була і в Україні, але тільки в останні роки виросла до масштабів, що загрожують національній безпеці, зокрема за рівнем економічної злочинності до кінця 2009 року Україна вийшла на шосте місце у світовому рейтингу [68]. Злочинний світ, по суті, кинув виклик державі, вступивши з нею у відкриту конкуренцію. Тому боротьба з організованою злочинністю і корупцією повинна мати не тільки правовий, але й політичний характер.

3. *Резонанс*, тобто стрімке зростання небезпеки під впливом зовнішніх чинників, коли одна загроза актуалізується у зв'язку з наявністю іншої. Так, націоналістичні рухи враховують і відображають перемоги й поразки один одного. Фахівці відзначають, що масштаби прояву таких неблагополучних екологічних чинників, як снігопади, досягли нині таких величин, що чинять істотний вплив на рівень соціально-політичної стабільності в країні.

4. *Агрегація або підсумовування*. В цьому випадку збої і неув'язки в різних сферах інтегруються в нову небезпеку. Наприклад, економічні труднощі, соціальна напруженість, руйнування системи охорони здоров'я поставили країну перед небезпекою демографічної катастрофи – фізичного вимирання населення. Іншим проявом агрегації слугує ситуація, коли реалізація однієї загрози створює нові неприємності. Так, збільшення

смертності населення здатне викликати депопуляцію нації, яка може призвести до знелюднення і запусіння території, що таїть у собі небезпеку її іноземної колонізації, а це означатиме повну денаціоналізацію решти населення.

5. *Сублімація*, під якою розуміється перехід небезпеки з одного стану або сфери в інший. Як наслідок цього цілком можливі ситуації, коли факти, відносно безпечні в одній сфері, набувають іншого характеру, виявившись пов'язаними з явищами в інших галузях. Так, природне лихо – засуха і неврожай – або технічні збої в атомній енергетиці можуть стати причиною соціальної напруженості, непродумана економічна політика – викликати порушення екологічної рівноваги в природі, а зниження рівня освіти населення – спричинити зростання технічних аварій.

Або інший приклад. Розвиток науки, що розширює творчі можливості людства, створює багато нових небезпек. Клонування – видатне досягнення біологів – становить проблему генетичної небезпеки для людства.

Тому стратегія безпеки, з одного боку, повинна мати комплексний характер, будуватися не як спосіб протидії окремим загрозам, а становити комплексний підхід, що враховує багатогранність властивостей і різноманітність інтересів України, усі зв'язки й можливі наслідки. Особливу практичну значущість має класифікація загроз державній безпеці за сферами і галузями людської діяльності (політичні, економічні, соціальні й духовні). Такий поділ загроз має велике значення при організації системи забезпечення державної безпеки і визначенні основних напрямів її функціонування. При цьому виділення видів загроз за таким критерієм можна конкретизувати для кожної самостійної сфери людської й суспільної діяльності.

Підсумовуючи сказане, можна назвати явища й тенденції світового розвитку, з якими пов'язана поява і загострення небезпек та загроз: демографічне, сировинне та енергетичне перевантаження планети; руйнування навколишнього середовища; “розповзання” зброї масового ураження; глобалізація життя на тлі посилення самовизначення етнічних,

релігійних і територіальних груп; науково-технічний прогрес; тіньова економіка; наркоманія й організована злочинність; інформаційні технології маніпулювання; тероризм; політична нестабільність у багатьох країнах світу.

З іншого боку, реалізація всесторонньо продуманої стратегії вимагає виділення необхідних сил і засобів. Виступаючи проти марнотратства, не можна досягати економії за рахунок безпеки. Інакше будь-які досягнення виявляються ненадійними, ефемерними, а становище особи, групи, суспільства і держави – хитким. Найбільш економним методом забезпечення національної безпеки слід уважати адаптацію системи до рівня й характеру загроз, про що детальніше йтиметься далі.

7. КЛАСТЕРИЗАЦІЯ ЗАГРОЗ ТЕРОРИСТИЧНОГО ХАРАКТЕРУ ЗА СФЕРАМИ ТА ВИДАМИ ПРОЯВУ

Недосконалість прогресивних механізмів активної протидії тероризму, ефективних способів викорінювання його джерел указує на певну кризу зовнішніх і внутрішніх політичних стратегій боротьби із цією загрозою, її наслідок – українське суспільство вражене вірусом тероризму з усіма трагічними наслідками. Головні зусилля антитерористичної діяльності було сконцентровано на формуванні державної системи боротьби з тероризмом, використовуючи лише можливості спеціальних підрозділів суб'єктів боротьби з тероризмом, та ігноруючи потребу постійних інтелектуальних інвестицій, як відповідь на появу нових типів загроз терористичного характеру.

В липні 2004 року у доповіді Національної Комісії по терористичним нападам на США американськими фахівцями була висунута ініціатива формування «уніфікованого інформаційного середовища в галузі боротьби з тероризмом» та створення єдиної децентралізованої інформаційної мережі сповіщення про терористичні загрози та виклики⁴⁹. Основне завдання подібних інформаційних технологій зводиться до єдиної мети – розпізнавання, формалізація та оцінка загроз терористичного характеру задля прогнозування терористичної активності, а в обов'язки Об'єднаного центру по запобіганню терористичних загроз, який існував в США у 2003-2004 роках, входило складання «щоденної матриці загроз», яка відіграла «важливу роль у рішеннях Президента США у війні з тероризмом»⁵⁰.

⁴⁹ Богданович В.Ю., Свіда І.Ю., Скулиш Є.Д. *Теоретико-методологічні основи забезпечення національної безпеки України: Монографія.* : у 7 т...-Т.1. *Теоретичні основи, методи й технології забезпечення національної безпеки України / В.Ю.Богданович, І.Ю.Свіда, Є.Д.Скулиш; за заг. ред. Є.Д.Скулиша.-К.:Наук.-вид. відділ НА СБ України, 2012.-548с.*

⁵⁰ *Об'єднаний центр по запобіганню терористичних загроз /Terrorist Threat Integration Center (TTIC).* [Електронний ресурс]. – Режим доступу: <http://www.encyclopedia.com/doc/1G2->

Заходи із упередження та запобігання терористичній діяльності на рівні загроз та ризиків на сьогодні не просто вимога часу, це життєво - необхідна умова подальшого існування суспільства, оскільки існує ймовірність переходу, навіть за умови демілітаризації лінії бойового зіткнення на сході, до терористично-диверсійної боротьби на решті території України.

Принципово важливим моментом у забезпеченні як національної безпеки в цілому, так і системи боротьби з тероризмом зокрема, є визначення (уточнення) функцій та завдань їх суб'єктів, розробка можливих сценаріїв (алгоритмів) їх дій у тих чи інших умовах. Науковому супроводженню цих питань, дослідженню та формальному опису загроз у сфері національної безпеки приділяється неабияка увага, зокрема у контексті визначення їх індикаторів та розробки паспортів (матриць) загроз задля можливості подальшого використання механізмів прогнозування адекватності реагування на них соціальних систем. Проте науково-методична база формалізації загроз теоретичного характеру та механізмів їх моделювання потребує розширення та подальшого удосконалення.

Аналіз літературних джерел з цієї тематики дозволяє зробити висновок, що в даний час в Україні не сформована цілісна система протидії тероризму, дуже повільно впроваджуються передові інформаційні технології, які дозволяють прогнозувати та виявляти потенційні джерела загроз терористичного характеру, завчасно виявляти наміри щодо приведення їх в дію, обґрунтовувати та рекомендувати органам (особам), що приймають рішення у цій сфері, найбільш раціональні варіанти рішень, спрямовані на відвернення максимального збитку від цих загроз, що і визначає актуальність даної публікації.

Основні складові та функції системи забезпечення національної безпеки окреслені, але протидія загрозам терористичного характеру розглянута здебільше лише у загальному вигляді, що не дозволяє провести їх

структурну класифікацію, сформувані структуровані бази даних, з використанням яких можна було б здійснювати сценарний аналіз загроз терористичного характеру та організувати протидію цим загрозам з залученням можливостей центрів ситуаційного управління.

На рівні теоретичних розробок залишилися не діставши практичної реалізації спроби структурно-факторного моделювання теророгенності соціальних систем, де системним елементом є теророгенний фактор як умова, першопричина, що провокує тероризм, або визначає його прогрес.

У статті розглянутий методологічний підхід до автоматизації інформаційно-аналітичних процесів безпекового супроводу реалізації національних інтересів, але загрози терористичного характеру розглянуті лише у концептуальному плані⁵¹.

У статті [4] зроблена спроба провести класифікацію загроз терористичного характеру, але запропонована класифікація не є повною, тому потребує суттєвих доповнень⁵².

У наведених публікаціях та у інших наукових працях, з якими змогли ознайомитися автори, відсутня чітка класифікація загроз терористичного характеру, яка б дозволяла побудувати відповідні бази даних, що є необхідною передумовою автоматизації моніторингу загроз, їх оцінювання та обґрунтування управлінських рішень в державній системі протидії тероризму.

Тероризм, як вже з'ясовано, виникає в результаті детермінації (модуляції) умов виникнення і протікання конфлікту зовнішніми впливами (необхідні і достатні умови). У загальному випадку, макросередовище будь-якої соціальної системи можна уявити у вигляді сукупності факторів, що визначають її стан. Отже, теророгенні фактори - це умови та причини що

⁵¹ Богданович В.Ю. *Методологічний підхід до автоматизації інформаційно-аналітичних процесів безпекового супроводу реалізації національних інтересів* / В.Ю.Богданович, А.Л. Висідалко // Київ: ДУТ: Сучасний захист інформації, № 3, 2014, с.4-10

⁵² *Антитерор РГПУ ім. А.І.Герцена [Електронний ресурс]. – Режим доступу: http://www2.bigpi.biysk.ru/antiterror/viewpage.php?page_id=2*

провокують тероризм або визначають його прогрес. Можливість настання наслідків прояву або реалізації теророгенного фактору у вигляді терористичної діяльності становить сутність поняття загрози терористичного характеру.

Беручи до уваги базове тлумачення поняття загрози національній безпеці, поняття загрози терористичного характеру – це наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України унаслідок скоєння терористичного акту. Під загрозою терористичного характеру розуміють потенційні дії або події, які прямо чи опосередковано сприяють виникненню терористичній діяльності. Ризики та загрози терористичного характеру завжди детерміновані – причинново обумовлені, формуються під впливом інших соціальних процесів та можуть бути визначені за умовними параметрами.

Генеральним напрямком дослідження детермінації тероризму в контексті його розуміння як глобального соціального процесу, на наш погляд, має бути розробка концептуальної соціально-інформаційної моделі ризиків та загроз терористичного характеру, яка в змозі виявити специфіку їх детермінації, механізмів функціонування та ефективного використання ресурсів системи державного управління та контролю в умовах реального трансформаційного процесу в Україні, обтяженого проведенням антитерористичної операції та сепаратистсько-екстремістськими настроями.

Соціальна система характеризується наявністю множини теророгенних факторів, які й формують загрози терористичного характеру. Розрізняючи конкретні види терористичної діяльності за різноманітними основами (за формою, засобам здійснення, історичним, національним, релігійним, географічним та іншим особливостям, за окремими елементами структури діяльності, а також і за іншими ознаками), можна виробити практично безкінечний ряд видів загроз терористичного характеру. Це різноманіття має під собою реальну основу – конкретні прояви тероризму на практиці

представляють теоретичний інтерес як специфічна особливість явища. При цьому, ряд теророгенних факторів буде на порядок вищим.

Запобігання загрозам терористичного характеру відіграє значну роль у забезпеченні суспільної та національної безпеки, оскільки сприяє збереженню соціально-політичної стабільності в державі. У реальному житті, через цілий ряд причин система протидії терористичній діяльності в Україні з моменту проголошення незалежності не отримала належного розвитку.

Разом з тим, особливо на початку XXI-го століття, в умовах зростання міжнародної і внутрішньодержавної нестабільності, значення антитерористичної діяльності постійно посилюється зростаючою роллю особи і суспільства в забезпеченні стійкого розвитку держави, що у свою чергу полегшує залучення зарубіжних інвестицій в економіку країни, сприяє формуванню її позитивного іміджу, посиленню конкурентних позицій, стимулює економічне зростання, створює умови для більш успішного вирішення соціальних проблем.

Світові тенденції в посиленні боротьби з тероризмом базуються на високошвидкісній обробці дуже великих масивів різноманітної інформації в обмежений час з використанням сучасних інформаційних технологій. Комп'ютерні технології автоматичного інтелектуального аналізу даних переживають бурхливий розквіт. Це пов'язано головним чином з потоком нових ідей в області комп'ютерних наук, що утворюються на перетині штучного інтелекту, статистики і теорії баз даних. Елементи автоматичної обробки і аналізу даних стають невід'ємною частиною концепції електронних сховищ даних і часто іменуються в цьому контексті data mining (добування знань з даних). У багатьох випадках виникає необхідність якимсь чином класифікувати дані або знайти в них закономірності.

Ухвалення управлінських рішень по нейтралізації виявлених загроз терористичного характеру повинне ґрунтуватися на їх глибокому і всебічному аналізі, врахуванні багатьох теророгенних і інших факторів

обстановки, що складається. Складність проведення такого аналізу пов'язана з багатогранним характером сучасної терористичної діяльності і відсутністю універсальних методичних рекомендацій по виявленню і нейтралізації загроз терористичного характеру. Обмежує ефективність антитерористичної діяльності і відсутність засобів автоматизації пошуку і обробки відповідної інформації, зокрема, автоматизованих систем підтримки ухвалення рішень, автоматизованих робочих місць аналітиків і ін. Першим кроком на шляху вирішення даної проблеми є структуризація загроз терористичного характеру.

Аналіз відомих методів структуризації багатовимірних даних показує, що у зв'язку з великим різноманіттям як сфер прояву погроз, так і їх видів і варіантів реалізації найбільш раціональним є метод кластеризації⁵³. Завдання класифікації є завданням віднесення об'єкту вивчення до однієї з декількох попарно не пересічних множин, які називатимемо кластерами загроз.

Поняття про кластер вперше було введено лауреатом Нобелівської премії Майклом Портером: «кластер або промислова група, - це група взаємозв'язаних компаній, що є сусідами, і пов'язаних з ними організацій, що діють у певній сфері і характеризуються спільністю діяльності і взаємодоповнюванням одна одної». Надалі це поняття було розширене для інших застосувань. У нашому випадку під кластером «кластером загроз» будемо розуміти групу загроз терористичного характеру, що мають ознаки прояву, притаманні конкретній сфері діяльності людини, суспільства та держави.

Характерні особливості кластерів загроз терористичного характеру:

- наявність соціально-орієнтованого виду діяльності, який визначає стратегію кластера в цілому;
- функціональна (територіальна) локалізація основної об'єктів можливих терористичних посягань – учасників кластера;

⁵³ Мандель И. Д. Кластерный анализ: Монография / И.Д.Мандель.- М.: Финансы и статистика, 1988. – 176с.

- стійкість і домінуюче значення господарських зв'язків між об'єктами можливих терористичних посягань;
- довгострокова координація взаємодії учасників системи в рамках
- основних систем управління, соціально-політичних програм, військово-політичних або ідеологічних (партійних, конфесійних та т.п.) блоків.

Проблеми безпеки, а також небезпеки і загрози терористичного характеру, що виникають, можна розглядати на різних ієрархічних рівнях, найбільш високим з яких є глобальний рівень. Для кожної держави пріоритетним завданням є забезпечення державної безпеки, що припускає захист державних інтересів, національних цінностей і способу життя від широкого спектру зовнішніх і внутрішніх загроз.

До державних інтересів відносяться територіальна цілісність; суверенітет країни; політичне самовизначення і самоврядування, відтворення населення, його економічне і соціальне благополуччя; гідне існування майбутніх поколінь. Об'єктами державної безпеки при цьому стають державні інтереси, громадяни, суспільство і держава.

Як суб'єкти, що покликані забезпечити державну безпеку, можна назвати державу в особі її інститутів і організацій, громадські об'єднання громадян; окремих громадян, що мають права і обов'язки в даній сфері відповідно до Конституції і законів держави.

Забезпечення безпеки держави повинне здійснюватися відповідно до базових принципів. Першим з них є пріоритет державних інтересів і безпеки перед інтересами юридичних і фізичних осіб, а також ідеологічними і політичними інтересами. Дуже важливим принципом є законність, тобто дотримання чинного в країні законодавства при здійсненні заходів щодо забезпечення державної безпеки. Третій принцип - відповідальність сил державної безпеки за її забезпечення перед законом. Четвертий принцип полягає в необхідності інформування суспільства про стан державної безпеки

і загрозах у цій сфері при дотриманні державної, службової і комерційної таємниці.

Життя і діяльність держави розгортаються в різних сферах, і в кожній з них можлива дія несприятливих чинників, небезпек і загроз, у тому числі і терористичного характеру, які порушують нормальне життя людини, суспільства і держави.

Виходячи з цього, пропонується кластери структурувати по сферам життєдіяльності держави. Авторами запропонована структура кластерів по 13 сферам життєдіяльності держави. Ця система є відкритою, що означає можливість її розширення у разі появи загроз, які не можуть бути однозначно віднесені до вибраних сфер. Для зручності кластери кодуються двозначними цифрами від 01 до 13.

Виділяють такі кластери (класи) загроз терористичного характеру:

- у зовнішньополітичній сфері (01);
- у сфері державної та громадської безпеки (02);
- у внутрішньополітичній та соціальній сфері (03);
- в етноконфесійній сфері (04);
- в фінансово-економічній сфері (05);
- в екологічній сфері (06);
- у воєнній сфері (07);
- у сфері інформаційної безпеки (08);
- у сфері фінансування тероризму (09);
- у санітарно-епідемологічній та медичній сфері (10);
- у сфері функціонування об'єктів критичної інфраструктури (11);
- у сфері функціонування об'єктів транспорту та зв'язку (12);
- у сфері функціонування об'єктів системи державного управління та місцевого самоврядування (13).

Аналіз практики боротьби з тероризмом показує, що у переважній більшості кожна загроза характеризується властивими тільки їй ознаками і індикаторами, оцінювання і аналіз яких вимагає великих часових і інтелектуальних ресурсів, що негативно позначається на ухваленні своєчасних і адекватних управлінських рішень по їх нейтралізації. Віднесення виявленої загрози терористичного характеру до певного кластера істотно знижує часові витрати на обґрунтування і ухвалення адекватного управлінського рішення, вибір форми, методу, тактики і адекватних загрозі засобів для її нейтралізації. В межах кластеру формується база даних загроз терористичного характеру.

Варто зазначити, якщо причини і цілі терористичної діяльності – категорії реальні і конкретні, то її мотивація в повному обсязі не завжди усвідомлюється діючим суб'єктом і в значній частині присутня на несвідомому рівні. Тому, при усій важливості психофізіологічного і біологічного аспектів дослідження терористичної діяльності, результати, що виявляються в процесі їх аналізу, не можуть бути використані як параметри для типологічної класифікації в межах кластера, але мають бути опосередковано враховані у експертному висновку щодо ступеню небезпеки терористичної загрози.

На мові теорії виявлення «сигналів» віднесення загроз терористичного характеру до певного кластера є багатоканальним стробуванням виявлених загроз (у нашому випадку вибрано 13 «грубих» стробів). Проводячи аналогічну класифікацію загроз в межах вибраного кластера представляється можливим детальніше описувати виявлені загрози і проводити «точне» налаштування системи боротьби з тероризмом на конкретну загрозу.

З метою об'єктивного визначення ступеню небезпеки або теророгенного потенціалу тієї чи іншої загрози, можуть бути запроваджені формальні критерії, визначення яких і становить основне завдання інформаційно-аналітичної діяльності. Це дозволяє в системі протидії тероризму автоматизувати деякі підготовчі процеси (яких фахівців , скільки

залучити, у який спосіб їх задіяти, як захистити тих, хто опинився в зоні дії терористичної загрози й тому подібне).

З огляду на власний досвід та наукові рекомендації, вдосконалення системи боротьби з тероризмом неможливе без досконалого механізму ризик-менеджменту, моніторингових досліджень його результатів, здатності правоохоронних органів та спеціальних служб прогнозувати терористичні прояви й сповіщати про їх ризик заздалегідь, до того, як вони стануть очевидними для всього суспільства. Адресатом розробок стратегічних концепцій аналізу загроз та заходів з мінімізації ризиків має бути, перш за все, об'єкт терористичних посягань.

Таким чином, запропонована кластеризація загроз терористичного характеру дає змогу сформувати бази даних вибраних кластерів загроз, а в кожному кластері сформувати відповідну базу даних конкретних загроз, як таких, що вже мали місце у реальному житті, так і загроз, що прогножуються в державній системі протидії тероризму, що дозволяє впровадити в процес функціонування державної системи протидії тероризму класичні автоматизовані системи підтримки прийняття рішень та забезпечити інформаційну сумісність автоматизованих робочих місць аналітиків, експертів та управлінців, відповідно, суттєво підвищити ефективність протидії загрозам терористичного характеру.

8. ПЕРСПЕКТИВИ ФОРМУВАННЯ УНІФІКОВАНОГО ІНФОРМАЦІЙНОГО СЕРЕДОВИЩА У СФЕРІ ПРОТИДІЇ ЗАГРОЗАМ ТЕРОРИСТИЧНОГО ХАРАКТЕРУ

Впровадження сучасних інформаційних систем і технологій, призначених для поліпшення стану інформаційного забезпечення боротьби з тероризмом – нагальна необхідність і запорука готовності системи боротьби з тероризмом до активізації терористичної діяльності не лише в зоні проведення АТО, а й на решті території держави.

Достовірна оцінка стану захищеності суспільства від проявів тероризму може проводитись лише на підставі моделювання загроз терористичного характеру. У разі виникнення загрози терористичної діяльності, що проявляється у порушенні порогових показників індикаторів стану соціальної напруженості, які виявлені на основі проведення їх моніторингу, зокрема зміни динаміки значень індикаторів стану захищеності, можуть застосовуватись заходи цільового впливу на ситуацію правового та соціально-інформаційного характеру⁵⁴.

Теоретична модель безпеки конструюється на основі класифікації загроз внутрішніх і зовнішніх, сильних і слабких, що діють в різних сферах діяльності суспільства. Вона має враховувати усі чинники в комплексі існуючих загроз – так звані теророгенні фактори. Причому, як правило, приймаються до уваги і обставини, які прямо або побічно сприяли виникненню негативних явищ, конфліктів і криз локального або масштабного характеру⁵⁵.

Базовим науковим підґрунтям дослідження загроз терористичного характеру є теророгенез. Багатостадійний процес зародження, формування і

⁵⁴ Доклад Национальной комиссии по расследованию террористических атак на США 11 сентября 2001 года. – М. : Институт экономических стратегий, 2004. – 833 с.

⁵⁵ Арманд А. Д. Анатомия кризисов / А. Д. Арманд, Д. И. Люри, В. В. Жери- хин [и др.]. – М.: Наука, 1999. – 238 с.

розвитку тероризму, або теророгенез (від лат. терор - страх, від грецької генез – походження) – сукупність історичних, соціальних, юридичних, кримінологічних та інших процесів, що відбуваються в суспільстві, які визначають походження й історико-еволюційне формування тероризму. Базовим у понятійному апараті теророгенезу є поняття теророгенного фактора⁵⁶.

Тероризм, як вже з'ясовано, виникає в результаті детермінації (модуляції) умов виникнення і протікання конфлікту зовнішніми впливами (необхідні і достатні умови). У загальному випадку, макросередовище будь-якої соціальної системи можна уявити у вигляді сукупності факторів, що визначають її стан. Фактор (від лат. *factio*- роблю) - умова, рушійна сила, причина якогось явища. Отже, теророгенні фактори - це умови та причини що провокують тероризм або визначають його прогрес. Можливість настання наслідків прояву або реалізації теророгенного фактору вигляді терористичної діяльності становить сутність поняття загрози терористичного характеру.

Беручі до уваги базове тлумачення поняття загрози національній безпеці, поняття загрози терористичного характеру – це наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України унаслідок скоєння терористичного акту.

Під загрозою терористичного характеру розуміють потенційні дії або події, які прямо чи опосередковано сприяють виникненню терористичній діяльності.

Використання економіко-математичних методів у розробці управлінських рішень передбачає формалізацію взаємозв'язків між певними чинниками, розрахунок відповідних кількісних показників. У випадку дослідження проблеми визначення потенціалу загроз терористичного характеру дуже складно формалізувати взаємозв'язки та об'єктивно

⁵⁶ Рижов І.М. *Основи теророгенності соціальних систем: [монографія]* / І.М.Рижов. – К : Наук.-вид. відділ НА СБ України, 2010. – 232 с.

визначити кількісні показники. Тому на практиці доцільно використовувати евристичні методи, тобто методи неформального аналізу на основі досвіду, інтуїції тощо. Останнє передбачає використання творчого мислення, творчих підходів:

1) порівняння (зіставлення предметів і явищ, знаходження між ними подібності та відмінності);

2) аналіз (поділ предметів і явищ на частини та властивості); 3) синтез (об'єднання частин і властивостей в єдине ціле);

4) узагальнення (об'єднання предметів і властивостей за деякими ознаками);

5) абстрагування (виділення одних ознак і відхилення інших).

Евристичні методи передбачають включення творчого мислення в процес розробки рішення, дозволяють генерувати нові ідеї, використання яких дає можливість підвищувати ефективність виконання управлінських завдань, спираються на досвід, здоровий глузд і аналогії у прийнятті рішень⁵⁷.

Евристичні методи використовують: у визначенні цілей; експертному прогнозі; аналізі сценарію розвитку ситуації; генеруванні та дослідженні альтернатив; під час дослідження рейтингів об'єктів або процесів; для прийняття індивідуальних і колективних рішень тощо. Методи евристичного програмування використовують у складних системах з великою кількістю чинників, для розв'язання слабоструктурованих завдань, не виражених кількісно в явній формі, а описаних декларативно у вигляді дескриптивної моделі.

Важливим засобом об'єднання формального й неформального методів аналізу є метод експертних оцінок, який належить до евристичного програмування. Причини залучення експертів до відповідних оцінок обумовлені багатьма чинниками: неможливістю кількісного вимірювання деяких показників, відсутністю відповідних вимірювальних приладів,

⁵⁷ http://pidruchniki.ws/16520205/menedzhment/ekspertni_metodi_rozrobsi_upravlinskih_rishen#285

складністю досліджуваних явищ, великими витратами коштів або часу при вимірюванні, відсутністю необхідних обсягів вірогідної інформації, суб'єктивністю досліджуваних характеристик тощо.

Методи експертних оцінок – це спосіб прогнозування та оцінки майбутніх результатів дій на основі прогнозів фахівців⁵⁸.

При застосуванні методу експертних оцінок проводиться опитування спеціальної групи експертів (5–7 осіб) з метою визначення певних змінних величин, необхідних для оцінки досліджуваного питання. До складу експертів слід включати людей з різними типами мислення – образне і словесно-логічне, що сприяє успішному розв'язанню проблеми.

Залучені експерти можуть висловити свою думку щодо ступеню загрози, строків досягнення поставлених завдань, критеріїв відбору оптимальних варіантів рішення тощо.

Необхідною умовою ефективного застосування методів експертної оцінки є достатня обізнаність експерта з досліджуваною проблемою, високий рівень ерудиції, здатність його давати чіткі вичерпні відповіді, до того ж експромтом. Крім того, експерт не повинен бути зацікавленим в тому чи іншому варіанті вирішення поставленої перед ним проблеми. Експерти підбираються за ознакою їх формального професійного статусу – посади, наукового ступеня, стажу роботи та ін. Такий підбір сприяє тому, що в число експертів потрапляють високопрофесійні, з великим практичним досвідом у даній галузі спеціалісти.

Метод експертних оцінок – це фактично метод прогнозування, основоположним критерієм якого є досягнення згоди серед усіх членів експертної групи. Організаційно це виглядає так. Експерти, обізнані у взаємопов'язаних сферах діяльності, детально відповідають на питання реєстру, пов'язане з досліджуваною проблемою. Кожен з них фіксує свою думку про проблему, а потім повідомляє про відповідь своїм колегам. У випадку розбіжності його прогнозу з думкою інших, експерт зобов'язаний

⁵⁸ http://pidruchniki.ws/19650323/ekonomika/metodi_ekspertnih_otsinok

пояснити причину такої невідповідності. Далі процедура повторюється до тих пір, поки думки експертів не збіжаться. При цьому потрібно дотримуватися анонімності, що допомагає уникнути можливості групових роздумів над проблемною ситуацією.

Завдяки застосуванню експертних оцінок отримують інформацію, на підставі якої вирішуються завдання різної значимості і на різних етапах формування реєстру:

1. Визначення пріоритету (ранг) конкретної загрози на об'єкті та динаміку зміни пріоритету(рангу) загрози у часі.
2. Інформація про причинно-наслідкові зв'язки в конкретних умовах місця і часу, чинники впливу (посилення, ослаблення), заходи з їх реалізації
3. Інформацію щодо ступеню захищеності конкретного об'єкта від вказаної загрози терористичного характеру. Таку інформацію здатні надати тільки експерти високого класу, професіонали, глибоко обізнані з сутністю та закономірностями прояву вказаних явищ за різних умов оперативної обстановки.

Визначення рівня терористичної безпеки України ґрунтується на індикаторах терористичної загрози, базовим з яких є показник ступеню захищеності. Запропонована методологія та методика визначення та утримання даних індикаторів відповідно до рівня порогових значень характеризує збалансований процес кількісної достатності та якісної повноцінності складових контртерористичної діяльності.

Технологічно виявлення загроз терористичного характеру являє собою процес, при якому на підставі аналізу численних характеристик стану соціального середовища - факторів визначаються ті, що провокують при визначених обставинах вирішення конфліктної ситуації методами тероризму. Тому фактори, що провокують конфлікт, можна вважати потенційно теророгенними. Ступінь їх небезпеки характеризує такий критерій як «теророгенний ефект» - якісна характеристика ступеня впливу того або іншого теророгенного фактора на можливість терористичного прояву.

Теророгенний ефект визначається як ступінь співвідношення теророгенного фактора і норми, що діє в конкретній соціальній системі і є основною інструментальною характеристикою терористичної загрози.

Класи загроз терористичного характеру:

01 – у зовнішньополітичній сфері;

02 – у сфері державної та громадської безпеки;

03 – у внутрішньополітичній (соціальній) сфері;

04 – в етноконфесійній сфері;

05 – в фінансово - економічній сфері;

06 – в екологічній сфері;

07 – у воєнній сфері;

08 – у сфері інформаційної безпеки;

09 – у сфері фінансування тероризму;

10 – у санітарно-епідеміологічній та медичній сфері;

11 – у сфері функціонування об'єктів критичної інфраструктури;

12 – у сфері функціонування об'єктів транспорту та зв'язку;

13 – у сфері функціонування об'єктів системи державного управління та місцевого самоврядування.

До кожного класу загроз може бути віднесено певну кількість підкласів або змістовних складових.

Класифікація загроз терористичного характеру застосовується для систематизації адміністративних даних, характеризуючи існуючі загрози терористичного характеру. Кодування загроз складається з трьох рівнів класифікації: клас, підклас, група. Метод класифікації - ієрархічний, послідовний, шестизначний. Позиція класифікатора має блок ідентифікації та блок назви класифікаційного угруповання. Назва та ознаки загрози формалізовані, наприклад :

Код загрози	Назва та ознаки загрози
1	2
01.	У ЗОВНІШНЬОПОЛІТИЧНІЙ СФЕРІ
01.01.	посягання на життя та здоров'я, викрадення чи незаконне позбавлення волі представника іноземної держави або погроза вчинення таких дій
01.02.	злочини проти осіб та установ, що мають міжнародний захист
01.03.	терористичний акт, про планування такого акту, загрозу його здійснення в іншій країні, в першу чергу у країні, яка межує з нашою державою
01.04.	приїзд або намір приїзду до України осіб, пов'язаних з терористичними і екстремістськими організаціями
01.05	час, місце і тему конференцій, семінарів, зустрічей, які організовуються на території України за участю іноземців, які походять з країн підвищеного ризику
01.06	проникнення терористичних або диверсійно-розвідувальних груп
01.07	перебування на території чи у повітряному просторі України рухомих об'єктів, захоплених терористами за межами нашої держави.
01.08.	інформація стосовно громадян України, які брали участь у збройних конфліктах на території країн підвищеного ризику
01.09.	контакти громадян України та іноземців, які перебувають на території України, з представниками екстремістських та терористичних середовищ
01.10.	незаконне ввезення, вивезення або транзит через територію України воєнної техніки, зброї та її компонентів, боєприпасів, вибухових речовин, засобів масового ураження, ядерних матеріалів та радіоактивних речовин
01.11.	затримання іноземців, які походять з країн підвищеного ризику, під час нелегального перетину кордону.
01.12.	випадки порушення іноземцями, які походять з країн підвищеного ризику, українського законодавства щодо легалізації на території нашої держави або нелегального отримання українських ідентифікуючих документів.

01.13.	ядерної чи радіаційної аварії за межами України із загрозою забруднення її території
02.	У СФЕРІ ДЕРЖАВНОЇ ТА ГРОМАДСЬКОЇ БЕЗПЕКИ
02.01.	посягання на територіальну цілісність України, публічні заклики до зміни меж державного кордону України, сепаратизму, автономізації окремих регіонів України, а також розповсюдження матеріалів із закликами до вчинення таких дій
02.02.	посягання на життя, здоров'я та майно, викрадення або тримання як заручника державного чи громадського діяча, керівника органу державної влади, голови чи депутата місцевої ради або погроза вчинення таких дій
02.03.	терористичний акт або погроза його здійснення
02.04.	угон або захоплення залізничного рухомого складу, повітряного, морського чи річкового судна або погроза вчинення таких дій
02.05.	злочини скоєні загально небезпечним способом (з використанням вогнепальної зброї та вибухівки або погроза їх застосування)
	спрямування терористичних організацій до радикально налаштованих організацій (осіб)
02.06.	зацікавленість сторонніх осіб до об'єктів критичної інфраструктури або важливих об'єктів загального користування (серед іншого, таких, як аеропорти, залізничні та автовокзали, метро).
02.07.	повідомлення про загрозу безпеці громадян (мінування будівель, транспортних засобів, закладення вибухових пристроїв в громадських місцях, погроза застосування хімічної, бактеріологічної зброї тощо).
02.08.	масові заворушення, що супроводжувалися насильством, погромами, підпалами, знищенням майна, захопленням будівель або споруд, насильницьким виселенням громадян, опором представникам влади або наміри щодо вчинення таких дій.
03.	У ВНУТРІШНЬОПОЛІТИЧНІЙ (СОЦІАЛЬНІЙ) СФЕРІ
03.01.	наруга над державними символами
03.02.	порушення виборчого законодавства
03.03.	посягання на захоплення або блокування будівель чи споруд, що забезпечують діяльність органів державної влади, органів місцевого

	самоврядування, об'єднань громадян, з метою перешкоджання їх нормальній роботі або наміри щодо вчинення таких дій
03.04.	передумови до виникнення надзвичайних ситуацій в оточенні об'єктів дипломатичного призначення, можливих протиправних намірів окремих осіб щодо скоєння акцій радикального та терористичного характеру стосовно представників дипломатичного корпусу.
03.05.	громадсько-політичні заходи (збори, мітинги, демонстрації, акції протесту тощо) будь-якої спрямованості та форми або наміри щодо їх проведення.
03.06.	рішення, заяви або звернення органів місцевого самоврядування з приводу проблемних питань суспільно-політичного життя держави чи регіону.
03.07.	руйнування, пошкодження або наруга над пам'ятниками культури та мистецтва, релігійними символами тощо. протиправні прояви, пов'язані з діяльністю правоохоронних органів та державних служб.
03.08.	публічне оголошення радикальних закликів особами, пов'язаними з радикальною або терористичною діяльністю.
03.09.	збройні напади, захоплення й утримування об'єктів державного значення (найважливіших і важливих державних об'єктів) або реальна загроза здійснення таких акцій
03.09.01	збройний напад, захоплення й утримування органу державної влади або реальна загроза здійснення такої акції
03.09.02	збройний напад, захоплення й утримування дипломатичної чи консульської установи або реальна загроза здійснення такої акції
03.09.03	збройний напад, захоплення й утримування установи правоохоронних органів або реальна загроза здійснення такої акції
03.09.04	збройний напад, захоплення й утримування телерадіоцентру чи вузла зв'язку або реальна загроза здійснення такої акції
03.09.05	збройний напад, захоплення й утримування органу військового управління, військової частини, військового навчального закладу, установи та організації збройних сил України або реальна загроза здійснення такої акції
03.09.06	збройний напад, захоплення й утримування державного закладу або реальна загроза здійснення такої акції
03.09.07	збройний напад, захоплення й утримування об'єкта атомної енергетики, хімічної промисловості та об'єкта, на якому виробляють чи зберігають біологічно небезпечні речовини, або реальна загроза

	здійснення такої акції
03.10.	посягання на життя державного чи громадського діяча
03.11.	напад, замах на життя членів екіпажу повітряного або морського (річкового) судна, викрадення (спроба викрадення), знищення (спроба знищення) такого судна, захоплення заручників з-поміж членів екіпажу чи пасажирів
03.12.	установлення вибухового пристрою у багатолюдному місці, установі (організації, підприємстві), житловому секторі, транспорт!
03.13.	зникнення чи викрадення засобів проведення терористичного акту
03.13.01	зникненням чи викраденням технічних одиниць вогнепальної зброї з об'єкта зберігання, використання, переробляння або під час транспортування
03.13.02	зникненням чи викраденням боєприпасів з об'єкта зберігання, використання, переробляння або під час транспортування
03.13.03	зникненням чи викраденням бронетехніки з об'єкта зберігання, використання, переробляння або під час транспортування
03.13.04	зникненням чи викраденням артозброєння з об'єкта зберігання, використання, переробляння або під час транспортування
03.13.05	зникненням чи викраденням вибухових матеріалів з об'єкта зберігання, використання, переробляння або під час транспортування
03.13.06	зникненням чи викраденням радіоактивна речовина (приладів або устаткування, з використанням радіоактивна речовина) з об'єкта зберігання, використання, переробляння та під час транспортування
03.13.07	зникненням чи викраденням небезпечних хімічних речовин (приладів або устаткування, де їх використовують) з об'єкта зберігання, використання, переробляння або під час транспортування
04.	В ЕТНОКОНФЕСІЙНІЙ СФЕРІ
04.01.	конфлікти у сфері міжетнічних, міжнаціональних, міжрелігійних та міжконфесійних відносин, що призвели або можуть призвести до порушення громадського порядку чи інших негативних наслідків.
04.02.	прояви ксенофобії, антисемітизму та релігійної нетерпимості.
04.03.	конфлікти на релігійному ґрунті, пов'язані з майновими претензіями, боротьбою за право володіння культовими спорудами, а також посяганням на свободу совісті та віросповідання.
04.04.	протиправні прояви, пов'язані з діяльністю релігійних сект, культів чи відправленням нетрадиційних релігійних обрядів.

04.05.	поширення через змі та електронні медіа відомостей, що можуть спровокувати міжетнічні, міжконфесійні та релігійні конфлікти, паніку серед великих груп людей або дискредитувати Україну перед світовою спільнотою.
05.	В ФІНАНСОВО- ЕКОНОМІЧНІЙ СФЕРІ
05.01.	надзвичайні події та ситуації на об'єктах промисловості, транспорту та житлово-комунального сектору, що можуть призвести або призвели до порушення їхньої нормальної роботи або людських жертв.
05.02.	надзвичайні події та ситуації на об'єктах фінансово-банківської інфраструктури, що можуть призвести або призвели до порушення їхньої нормальної роботи, паніки або людських жертв.
05.03.	протиправне захоплення (рейдерство) державної власності, банків, кредитних спілок, господарських товариств, кооперативів тощо.
06.	В ЕКОЛОГІЧНІЙ СФЕРІ
06.01.	надзвичайні ситуації природного чи техногенного характеру.
06.02.	масове екологічне збруднення довкілля.
06.03.	викиданням (загрозою викидання), утворенням і розповсюдженням небезпечної хімічної речовини під час їх вироблення, перероблення чи зберігання (захоронення)
06.04.	викиданням (загрозою викидання) біологічно небезпечної речовини на підприємстві промисловості або в науково-дослідній установі
06.05.	наявності у воді шкідливих (забруднювальних) речовин
06.06.	наявності у навколишньому середовищі шкідливих (забруднювальних) і радіоактивних речовин
06.07.	викиданням (загрозою викидання) радіоактивних речовин
07.	У ВОЄННІЙ СФЕРІ
07.01.	катастрофи та аварії, спричинені використанням зброї та воєнної техніки.
07.02.	надзвичайні події військового характеру, які призвели до людських жертв.
07.03.	відключення від електропостачання військових частин, що перебувають на бойовому чергуванні.

07.04.	спроби проникнення на військові об'єкти або спроби крадіжки зброї, боєприпасів, вибухових матеріалів і елементів озброєння з території військових підрозділів, об'єктів або цивільних суб'єктів.
08.	У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ
08.01.	несанкціоноване втручання, блокування роботи державних електронних інформаційних ресурсів, виведення з ладу інфраструктури, яка забезпечує їх функціонування.
08.02.	надзвичайні події на об'єктах зв'язку, що загрожують функціонуванню національної системи зв'язку.
08.03.	підготовки або здійснення акцій кібертероризму (у т.ч. хакерство).
08.04.	установлені факти участі громадян України та іноземців, що тимчасово мешкають в Україні, в міжнародних хакерських угрупованнях, їх деструктивна діяльність на території України.
08.05.	несанкціонованого втручання в автоматизовані чи інформаційно-телекомунікаційні системи об'єктів енергетики, транспорту, зв'язку, житлово-комунальної та медичної сфер, які забезпечують управління технологічними процесами з виробництва основної продукції та послуг, що призвело або може призвести до виникнення надзвичайної ситуації техногенного характеру, масової загибелі громадян, соціального невдоволення, блокування роботи систем життєзабезпечення.
08.06.	створення або використання вже існуючих інтернет-порталів, форумів, блогів тощо для пропагування ксенофобії, радикалізму та тероризму.
08.07.	Спеціальні інформаційні операції ЗМІ провокаційного характеру.
09.	У СФЕРІ ФІНАНСУВАННЯ ТЕРОРИЗМУ
09.01.	щодо фінансових операцій, які здійснюються через суб'єктів, що підозрюються у зв'язках з радикальними чи терористичними угрупованнями.
09.02.	щодо виявлення фінансових операцій які можуть бути пов'язані, мати відношення або призначатися для фінансування тероризму.
09.03.	щодо фінансових операцій з легалізації доходів, одержаних

	злочинним шляхом.
09.04.	щодо фінансової операції учасником або одержувачем якої є особа, включена до переліку осіб, пов'язаних із здійсненням терористичної діяльності.
09.05.	щодо відкриття рахунків особою, яку включено до переліку осіб, пов'язаних із здійсненням терористичної діяльності.
09.06.	щодо підозрілих фінансових операцій, які не характерні специфіці та напрямам діяльності суб'єкта і можуть бути легалізацією доходів отриманих злочинним шляхом, або фінансування тероризму.
09.07.	щодо фінансових операцій пов'язаних із зарахуванням (списанням) коштів на (з) рахунок(у) юридичної особи якщо операції на зазначеному рахунку не проводились з моменту його відкриття.
09.08.	щодо зарахування на рахунок особи коштів у готівковій формі з подальшим переказом усієї суми наступного дня на користь третьої особи.
09.09.	щодо діяльності організованих злочинних груп с точки зору фінансування або фінансової підтримки терористичних угруповань.
10.	У САНІТАРНО-ЕПІДЕМОЛОГІЧНІЙ ТА МЕДИЧНІЙ СФЕРІ
10.01.	перевищення епідемічного порогу захворюваності на інфекційні хвороби, а також випадки масового захворювання особливо небезпечними інфекційними хворобами (холерою, віспою, чумою, тифом, небезпечними штамами грипу тощо).
10.02.	штучна Пандемія - найвищий ступінь поширення інфекційного захворювання (напр., грипу), що охоплює більшість населення
10.03	Штучна Панзоотія - вибухоподібне розповсюдження заразної хвороби тварин, що значно перевищує звичайний рівень захворюваності на цю хворобу на даній території
10.04.	Штучна Панфітотія - вибухоподібне розповсюдження заразної хвороби рослин, що значно перевищує звичайний рівень захворюваності на цю хворобу на даній території. Аналог епізоотії у тварин та епідемії у людей
11.	У СФЕРІ ФУНКЦІОНУВАННЯ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ
11.01.	Об'єктів критичної інфраструктури економіки

11.01.01	збройний напад, захоплення й утримування об'єкта атомної енергетики, хімічної промисловості та об'єкта, на якому виробляють чи зберігають біологічно небезпечні речовини, або реальна загроза здійснення такої акції
11.01.02	пожежі, вибуху на об'єкті розвідування, видобування, переробляння, транспортування чи зберігання легкозаймистих, горючих, а також вибухових речовин
11.02.	Об'єктів соціально-побутової інфраструктури
11.02.01	пожежа, вибух на руйнування будівлі чи споруди житлової призначеності (об'єкті житлового сектору)
11.02.02	пожежа, вибух руйнування будівлі чи споруди виробничої призначеності
	руйнування будівлі чи споруди нежитлової призначеності в жиллому секторі
11.02.03	пожежа, вибух на технологічних об'єктах у житловому секторі
11.02.04	на об'єктах тепло-, газо-, електро- та водопостачання; масове відключення від них споживачів.
11.02.05	збройний напад, захоплення й утримування органу управління житловим господарством, навчального закладу, медичної, дитячої та т.п. установ або реальна загроза здійснення такої акції
11.02.06	збройний напад, захоплення й утримування місць масового скупчення населення, торговельних центрів, дозвілля або спорту або реальна загроза здійснення такої акції
11.02.07	руйнування підземних споруд систем життєзабезпечення
12.	У СФЕРІ ФУНКЦІОНУВАННЯ ОБ'ЄКТІВ ТРАНСПОРТУ ТА ЗВ'ЯЗКУ
12.01	нанесення збитків окремим фізичним елементам інформаційної інфраструктури (руйнування мереж електрозв'язку, теле-, радіомовлення, енергетичних комплексів і споруд, використання біологічних та хімічних засобів руйнування елементної бази тощо).
12.02	аварій чи катастроф на залізничному транспорті
12.03.	аварії в метрополітені
12.04.	аварій на водному транспорті

12.05.	авіаційних аварій і катастроф
12.06.	аварій автомобільного транспорту
12.07.	аварій на трубопроводах
12.08.	аварій на міському транспорті
12.09.	аварії в електричних мережах
13.	У СФЕРІ ФУНКЦІОНУВАННЯ ОБ'ЄКТІВ СИСТЕМИ ДЕРЖАВНОГО УПРАВЛІННЯ ТА МІСЦЕВОГО САМОВРЯДУВАННЯ
13.01	підпал (підрив) об'єктів державного значення (найважливіших і важливих державних об'єктів) або реальна загроза здійснення таких акцій
13.02.	збройний напад, захоплення й утримування державного закладу або реальна загроза здійснення такої акції
13.03.	збройний напад, захоплення й утримування дипломатичної чи консульської установи або реальна загроза здійснення такої акції
13.04.	збройний напад, захоплення й утримування органу військового управління, військової частини, військового навчального закладу, установи та організації збройних сил України або реальна загроза здійснення такої акції
13.05.	збройний напад, захоплення й утримування органу державної влади або реальна загроза здійснення такої акції
13.06.	збройний напад, захоплення й утримування телерадіоцентру чи вузла зв'язку або реальна загроза здійснення такої акції
13.07.	збройний напад, захоплення й утримування установи правоохоронних органів або реальна загроза здійснення такої акції

Друга стадія припускає прогнозування розвитку цих факторів з урахуванням можливих змін ситуації, впливів інших факторів, норм і правил тощо. Якщо в результаті прогнозування можливий такий вихід, що прямо або побічно сприяє виникненню тероризму, ці фактори можна вважати теророгенними, відповідно, можливо визначити об'єкт, який підпадає під сферу впливу цього фактора. Прогнозування може здійснюватися будь-яким

із відомих методів, при цьому повинні враховуватися необхідні і достатні умови переростання конфлікту в терор.

З метою об'єктивного визначення ступеню небезпеки або теророгенного потенціалу тієї чи іншої загрози, можуть бути запроваджені формальні критерії, визначення яких і становить основне завдання інформаційно-аналітичної діяльності контртерористичних підрозділів. Насамперед, мають бути визначені та описані потенційні теророгенно-небезпечні об'єкти на території. На підставі кодифікованих загроз, проводиться обстеження, на підставі результатів якого формується перелік об'єктів, які складають потенційну небезпеку скоєння терористичного акту за даними ознаками. Для кожного з цих об'єктів мають бути вказані певні характеристики, визначені показники небезпеки та чинники впливу на них та визначено ступень захищеності від вказаної загрози терористичного характеру, зокрема:

1. Пріоритет (ранг) загрози на об'єкті, який визначається шляхом експертної оцінки оперативного співробітника за 5-рівневою шкалою (1-не значуща, 2- значуща, потребує особливої уваги, 3- важлива, 4-пріоритетна, 5- критична). Звичайно, один конкретний об'єкт може бути віднесений до кількох загроз, і по кожній з яких він має бути оцінений.

2. Сфера компетенції (відношення до суб'єкту боротьби з тероризмом) – вказується підрозділ СБ України (координати чергового підрозділу та або) відповідального) та суб'єкт боротьби з тероризмом (відомство, підрозділ тощо) у сфері компетенції та підпорядкованості цей об'єкт знаходиться.

3. Динаміка (+/-) – показник визначає динаміку зміни пріоритету (рангу) загрози у часі у порівнянні з моментом попереднього визначення параметру. Позначається «—» коли напруженість з плином часу має тенденцію зменшуватися, «+» коли ранг загрози підвищується. В разі, коли зміна пріоритету у часі не спостерігається, позначається як «+/-».

4. Чинники впливу (посилення, ослаблення), заходи з їх реалізації – вказуються необхідні заходи впливу (посилення, ослаблення), якщо, на думку експерта, такі є, виходячи з реальних можливостей органів місцевої влади та управління, правоохоронних органів або оперативних підрозділів СБУ. При визначенні чинників впливу слід враховувати архітектоніку конкретного об'єкта, яка відображає стан та вектор його організаційного розвитку, що є первинним у діагностуванні рівня як загальної безпеки, так і контртерористичної захищеності. При цьому, слід враховувати впливи, особливо деструктивні, з боку оточуючого соціального середовища, у тому числі й віртуального, на кадровий потенціал об'єкту, як найбільш уразливу його складову.

5. Ступінь захищеності – наводиться експертна оцінка ступеню захищеності конкретного об'єкта від вказаної загрози терористичного характеру. Оцінювання проводиться в якісних шкалах: «високий – середній – низький». Необхідну інформацію збирають, опитуючи експертів, які є фахівцями у сфері, де виявлена загроза. Робота над моделлю такої складної соціальної системи починається зі збору та аналізу фактичного матеріалу з подальшим використанням найбільш прийняттого, із огляду на можливість реалізації в системах моніторингу, методом розпізнавання загроз терористичного характеру – методом експертних оцінок. Цей метод заснований на аналізі експертів, що в подальшому дає можливість спрогнозувати адекватну модель майбутнього розвитку подій на об'єкті реагування. Причини залучення експертів до відповідних оцінок обумовлені багатьма чинниками: неможливістю кількісного вимірювання деяких показників, складністю досліджуваних явищ, відсутністю необхідних обсягів вірогідної інформації, суб'єктивністю досліджуваних характеристик тощо. Необхідною умовою ефективного застосування методів експертної оцінки є достатня обізнаність експерта з досліджуваною проблемою, здатність його давати чіткі вичерпні відповіді, до того ж у обмежений термін. Експерти підбираються за ознакою їх формального професійного статусу – посади.

Оптимальним варіантом є залучення представників громадськості до визначення ступеню захищеності об'єктів, наприклад із використанням можливостей соціальних мереж. Такий підхід сприяє тому, що в число експертів потрапляють високопрофесійні, з великим практичним досвідом у даній галузі спеціалісти.

Визначення рівня терористичної безпеки України ґрунтується на індикаторах терористичної загрози, та передбачає наявність спеціального інформаційного середовища, оскільки пов'язане з поняттям інформаційної роботи в її повному циклі. Запропонована методологія та методика визначення та утримання даних індикаторів відповідно до рівня порогових значень характеризує збалансований процес кількісної достатності та якісної повноцінності складових контртерористичної діяльності⁵⁹.

Виходячи з вищевикладеного, формування реєстру загроз терористичного характеру у вигляді уніфікованого інформаційного ресурсу сприятиме вивчення ступеню готовності територіальних громад, регіональних підрозділів суб'єктів боротьби з тероризмом й окремих об'єктів до протидії можливим терористичним загрозам. Введення реєстру дозволить здійснювати структурування об'єктів підвищеної небезпеки в регіонах за їх належністю до відповідних суб'єктів боротьби з тероризмом, а також, завдяки методу експертних оцінок, відслідковувати динаміку змін у ступені їхньої захищеності. Фактично, мова йде про можливість впровадження спеціалізованого інформаційно-управлінського процесу у його повному циклі, від отримання даних до відпрацювання управлінських рішень із за діянням всіх елементів інформаційного середовища.

З урахуванням викладеного вище, І.М. Рижовим на базі аналітичних підрозділів Штабу АТЦ при СБ України із залученням особового складу НОЦ НА СБ України було розпочато роботу методики формування Реєстру загроз терористичного характеру. На підставі розпорядження керівника АТЦ

⁵⁹ Качинський А.Б. Індикатори національної безпеки: визначення та застосування їх граничних значень: монографія / А.Б. Качинський. – К. : НІСД, 2013. – 104 с.

(ШТ № 45109 від 10.06.14 р.) в усі регіональні підрозділи УСБУ було розіслано проект «Реєстру терористичних загроз». Окремим було визначено питання щодо надання окремим посиленням інформації для ЗМІ, яка стосується формування у населення України та світу позитивного іміджу органів державної влади.

Метою розсилки проекту було надати можливість фахівцям на місцях ознайомитись, проаналізувати та надати свої рекомендації щодо змісту реєстру та його необхідності. Для помічників начальників регіональних органів СБУ з координації антитерористичної діяльності проведено семінар-тренінг, на якому, зокрема, були розглянуті питання щодо організації спільної роботи з цим реєстром. Була проведена робота з його вдосконалення та методичного забезпечення. Загалом ідея запровадження реєстру була позитивно схвалена. Вся інформація, що надходить, вноситься до тимчасової бази даних, яка дає можливість проводити аналіз усієї інформації, що отримана. За допомогою даних, що надходять до реєстру з областей, у тестовому режимі може відслідковуватися динаміка змін у рівні загроз терористичного характеру по регіонам, районам та конкретним об'єктам критичної інфраструктури. Отримані результати враховуються під час складання доповідей щодо оперативної обстановки та плануванні Штабом АТЦ спеціальних інформаційних операцій.

Також було акцентовано увагу керівництва на потребу створення окремого структурного підрозділу Штабу АТЦ з моніторингу інформаційного простору та планування спеціальних інформаційних операцій основними завданнями якого мало б стати відслідковування оперативного стану контртерористичної захищеності на місцях за допомогою реєстру загроз терористичного характеру.

9. ВИЯВЛЕННЯ ЗАГРОЗ ТЕРОРИСТИЧНОГО ХАРАКТЕРУ ШЛЯХОМ МОНІТОРИНГУ ТА КОНТЕНТНОГО АНАЛІЗУ МЕРЕЖІ ІНТЕРНЕТ

Враховуючи зростання популярності глобальної мережі Інтернет серед різного роду терористичних організацій, для своєчасного виявлення і недопущення здійснення терористичних актів, значно збільшилась потреба у створенні нових та модернізації існуючих методів контентного аналізу.

Питання означеної проблеми розглянуті в наукових працях Григор'єва В.Р., Ільїна Е.П., Антоновича І.І. та інших учених. Дослідження методів оцінки зв'язків у соціальних мережах описувались С. Вольффрамом, Д. Ланде, В. Прищепою. Проте, варто зазначити, що моніторинг соціальних мереж в Інтернеті сьогодні став одним з найефективніших, а методи OSINT-аналізу зазнали суттєвих змін. Тому більшість публікацій, пов'язаних з даною тематикою, децю втратили свою актуальність, що стало однією з ключових підстав для написання цієї статті.

Сучасні технології передачі даних стають доступними все більшій кількості людей. Створюються нові та модернізуються існуючі мережеві сервіси, що робить Інтернет дійсно засобом масової комунікації, а виникнення технологій хмарних обчислень (cloud computing) та Web 2.0 дали початок використанню мережевого простору для розподілених обчислень, які, в свою чергу, надають не лише інформаційні, а й ресурсномісткі алгоритмічні послуги.

Хмарні обчислення у комплексі з новітніми розробками у сфері інформаційних технологій із використанням соціальних мереж сприяють майже миттєвому поширенню інформації, проте глобалізація телекомунікаційних мереж створює нові загрози інформаційному середовищу. Глобальна мережа стає новим простором – інформаційним, в

якому здійснюється формування громадської думки, відображаються соціальні процеси, але, разом з тим, проводяться психологічні операції з використанням інформаційних мем-технологій у вигляді пандемій ідей-вірусів⁶⁰.

Через використання новітніх інформаційних технологій на стадії планування терористичних актів, злочинні угруповання нового типу вже самі здатні забезпечувати свою діяльність та майже не орієнтуються на будь-які державні засоби фінансування⁶¹.

Інформаційна війна набуває рис системного протиборства, а інфосфера становиться середовищем, у якому цілком можливою стає реалізація загроз безпеці та стабільності держав, що змушує змінювати підходи до інформаційного протиборства та організації розвідувальної діяльності⁶².

Можливість оперативного обміну будь-якою текстовою, графічною, аудіо- та відео- інформацією почала активно використовуватись різними терористичними організаціями для координації дій та залучення до своїх лав нових прибічників. Поширеність соціальних мереж дозволяє спілкуватись користувачам, які можуть називатись вигаданими іменами і знаходитись у самих різних куточках земної кулі, а обговорення злочинних намірів припинило бути явним. Більшість з учасників терористичних організацій володіють лише невеличкою часткою інформації про загальні наміри самих координаторів зловмисних дій, впевнені у своїй винятковості і часто не сприймають себе єдиним цілим з будь-якою конкретною організацією.

Ільїн Е. П. у своїй статті «Про оцінки терористичних загроз та підходах Російської Федерації до протидії тероризму» відзначає: метод поділу на своїх і чужих не спрацьовує, коли мова заходить про «просторово-розподіленого»

⁶⁰ Григорьев В.Р. Информационные вирусы – новое оружие массового поражения // Информационные войны. — 2008. — № 3. — С. 2–29.

⁶¹ Hutchinson W. Information terrorism: networked influence. [Електронний ресурс]. — Режим доступу: URL: http://scissec.scis.ecu.edu.au/proceedings/2006/iwar/Hutchinson%20-%20Information%20terrorism_%20networked%20influence.pdf.

⁶² Облачные вычисления – стратегический ресурс ведения сетевых войн [Текст] / В. Р. Григорьев, А. А. Новиков // Вестник РГТУ. — 2013. — № 14: Серия «Информатика, защита информации, математика». — С. 75-100.

супротивника. Нова модель тероризму – це спосіб досягнення політичних цілей не якоїсь конкретної держави або навіть угруповання. Це спосіб встановити суспільний устрій, який учасниками даного руху здається справедливим⁶³.

В інформаційній сфері Е. Ільїн окремо визначає війни, спрямовані на розмиття уявлень про добро і зло, на дискредитацію історії та культури держави-жертви (внаслідок чого нація втрачає навіть бажання супротиву прямому військовому вторгненню), на залякування (з метою введення заходів, спрямованих на закабалення народу під виглядом засобів усунення загрози тероризму).

Об'єм інформації, швидкість, мультимедійність, анонімність, низькі витрати та глобальність дали можливість терористам подолати т.зв. «управління сприйняттям» («perception management»). Терористи можуть зобразити себе точно такими, якими хочуть здаватись, а також уникнути фільтрів, що накладаються традиційними ЗМІ⁶⁴.

Зміну методів комунікації терористів з цільовими аудиторіями можна відстежити за звітами Європолу 2007-2015 років [6]. У 2015 році Європол вже прямо заявляє про нові якості та можливості терористичної пропаганди, що з'явилися завдяки розвитку інструментарію соціальних мереж⁶⁵.

За цих обставин у складі Європолу розпочато створення нових відділень, чия діяльність повинна бути спрямована на комунікативну протидію тероризму, а 1 липня 2015 року було засновано підрозділ Європейського Союзу по роботі в мережі Інтернет з метою боротьби з мережевою терористичною пропагандою та пов'язаною з цим екстремістською діяльністю. Також можливості антитерористичного

⁶³ Ильин Е. П. Об оценках террористических угроз и подходах Российской Федерации к противодействию терроризму / Е.П. Ильин // *Herald of the National Antiterrorism Committee*. — 2012. — № 2 (07). — P. 11–13.

⁶⁴ Hoffman B. *Inside Terrorism / Rev. and expanded ed.* N.Y. : Columbia University Press. — 2006. — P. 202.

⁶⁵ *EU Terrorism Situation and Trend Report (TE-SAT) 2015 / Europol*. — The Hague, 2015. [Електронний ресурс]. — Режим доступу: URL: https://www.europol.europa.eu/sites/default/files/publications/p_europol_tsat15_09jun15_low-rev.pdf.

співробітництва закладено у підсумкових документах нарад ОБСЄ у Гельсінкі, Мадриді, Відні. Центрами планування запобігання міжнародному тероризму стають міжнародні організації. Генеральною Асамблеєю ООН разом з регіональними об'єднаннями представлена формула: запобігання – захист – переслідування – відплата.

В частині запобігання та захисту, беззаперечно, повинні підлягати доопрацюванню питання моніторингу загроз терористичного характеру. Необхідна уніфікація відомчих та міждержавних підходів до статистичних даних, створення єдиного банку інформації та відповідного режиму інформаційного обміну, узгодження статистичної звітності про терористичні злочини, розробка і втілення методики оцінювання наслідків таких злочинів⁶⁶.

Стосовно моніторингу слід зауважити, що об'єм інформації, яка передається за допомогою засобів масової комунікації, потребує ретельного відпрацювання алгоритму пошуку, виявлення особливостей комунікації за допомогою контентного аналізу, виділення семантичних характеристик образу комунікатора. Моніторинг повинен враховувати стиль комунікації та виокремлювати ознаки маніпулювання (захоплення комунікативної ініціативи, домінування у спілкуванні тощо). Крім того, потрібно пам'ятати, що вплив на аудиторію здійснюється зловмисниками шляхом спонукання до дії, зміни думки тощо, а реалізується такий вплив не лише вербальним шляхом, а й за допомогою відеофрагментів і текстових матеріалів відповідної тематики⁶⁷. Для більш якісної класифікації результатів моніторингу і подальшої аналітичної роботи доречно використовувати відповідним чином підготовлений реєстр загроз терористичного характеру (ЗТХ).

⁶⁶ Антонович И.И. *Международный опыт профилактики терроризма. Предложения в сфере международного взаимодействия по противодействию распространения идеологии терроризма.* / И.И. Антонович, О.М. Особенков, Л.Н. Панкова, В.А. Щегорцов. — М. : Университетская книга. — 2010. — 132 с.

⁶⁷ Злоказов К. В. *Образы коммуникаторов и стратегии воздействия при пропаганде идей террористической организации «Исламское Государство»* / К. В. Злоказов, А. Ю. Софронова // *Политическая лингвистика.* — 2015. — № 2 (52). — С. 247-253.

Вже доведено, що аналіз динаміки змін показників реєстру ЗТХ дозволяє своєчасно викривати зовнішній вплив на стан соціальної напруженості і виявляти його джерела, що, у свою чергу, надає можливість здійснювати компенсаційний вплив на інформаційне середовище у регіоні, щодо якого здійснюється моніторинг. Вивчення існуючих підходів до аналізу соціальної напруженості та протестного потенціалу показало, що незважаючи на наявність низки методів та методик оцінки соціальної напруженості в суспільстві, в тому числі і формалізованих, досі відкритим залишається питання розробки методики здійснення інтегральної оцінки і соціальної напруженості та протестного потенціалу в суспільстві, і впливу окремих чинників соціальної напруженості на активізацію протестних настроїв (досліджувалось у попередніх публікаціях автора).

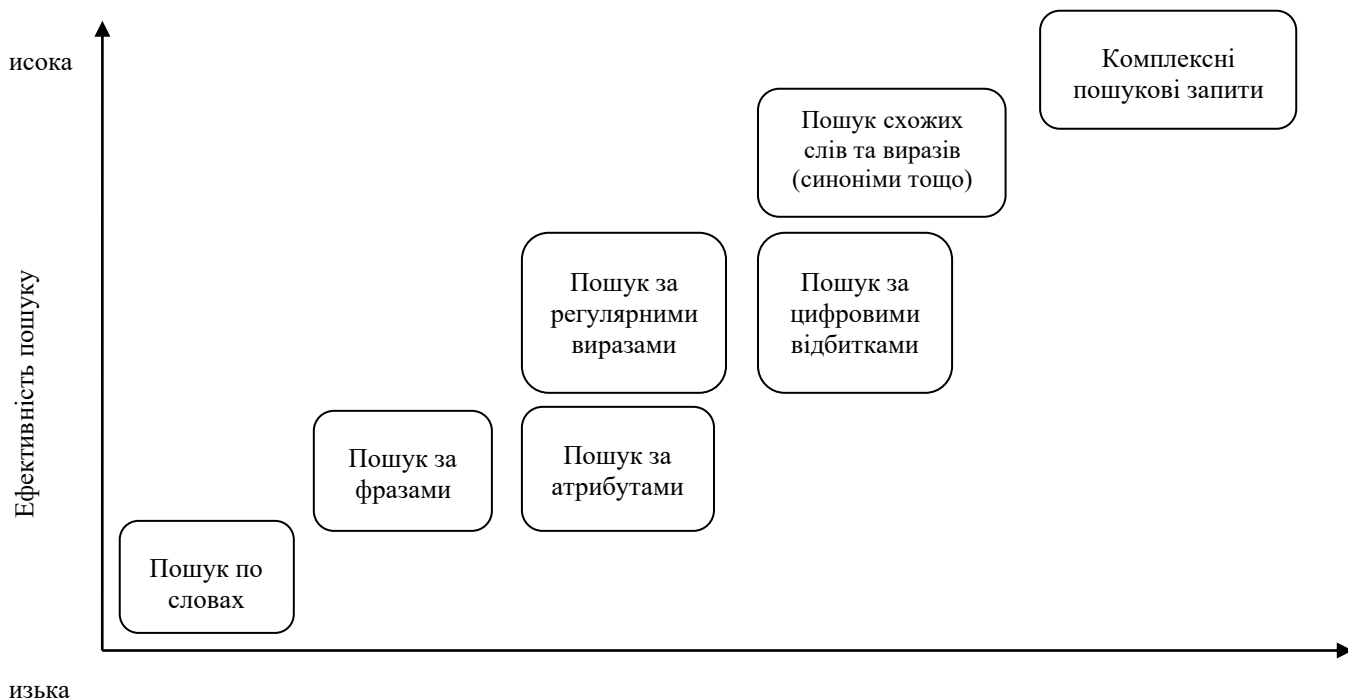
На теперішній час головним джерелом інформації для виявлення тенденцій у сфері досліджень терористичної загрози за допомогою спеціальних аналітичних інструментів або без них є сучасні відкриті мережеві ресурси (веб-сайти, соціальні мережі тощо). Найбільш цікавими для аналізу в умовах сьогодення стають соціальні мережі, які цілком легально надають інформацію про осіб, а в багатьох випадках саме через такі мережі здійснюється маніпулювання даними, активне інформаційне протистояння і навіть мережева мобілізація.

Стосовно виявлення кола користувачів соціальних мереж, інформаційна діяльність яких може свідчити про можливий зв'язок з терористичними організаціями, така робота повинна проводитись методами OSINT (Open Source Intelligence, англ. – розвідка на основі відкритих джерел). Доступність та спектр відкритої інформації дає можливість за допомогою OSINT-операцій отримувати та аналізувати дані без використання спеціалізованих людських або технічних засобів, встановлювати об'єкти для дослідження та інформаційні ресурси, що з ними пов'язані, виявляти користувачів Інтернету, які проявляють інтерес до

тематики терористичної діяльності та можуть, у свою чергу, стати новими джерелами отримання інформації.

Застосування відповідним чином підготовленого «словника стоп-слів та висловів» дозволяє виділити окремі акаунти, стосовно яких можна отримати відомості про діяльність, проаналізувати тематику найбільш часто розміщуваних на таких сторінках публікацій, години найбільшої активності користувача у мережі (що дозволить зробити попередні висновки про місцезнаходження власника акаунта), які вислови частіше за все використовуються і, що важливо, виявити, яким чином пов'язані між собою «друзі» у соціальній мережі та побудувати графи зв'язків. Проте, необхідно враховувати, що інформаційні ресурси в мережі Інтернет мають можливість навмисно або ненавмисно модифікувати та фільтрувати інформацію, яку розміщують, з метою маніпуляції громадською думкою тощо. Тому ключовими факторами для успішного аналізу є чітке розуміння мети роботи, неупередженість, збір даних з максимального кола можливих джерел.

Для найбільш ефективного пошуку необхідно враховувати, що його якість прямо залежить від заданих критеріїв, які можуть містити в собі як окремі слова, так і фрази, атрибути, цифрові відбитки тощо (див. Мал. 1).



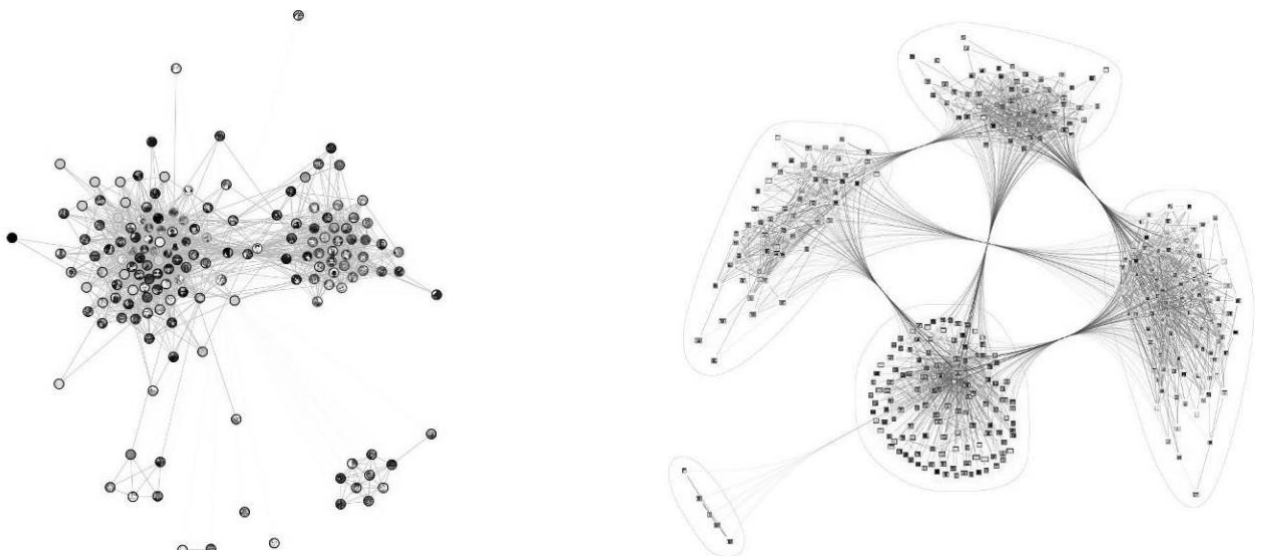
Мал.1. Залежність ефективності пошуку від заданих критеріїв.

Проте, навіть у разі використання ретельно підібраних комплексних запитів, звичні пошукові системи (наприклад, Google або Yandex) видають лише знайдені збіги без будь-яких аналітичних викладок. За деякими висновками, більш ніж 97% критичної онлайн-інформації неможливо знайти, використовуючи традиційні пошукові системи⁶⁸. Експерти вважають, що лише близько 10-15% необхідної інформації можна знайти у готовому вигляді, а решту можна отримати шляхом порівняння, інтеграції та аналізу чисельних розпорошених даних. Необхідно використовувати методи виявлення неочевидних (як практичних, так і теоретичних) зв'язків та закономірностей, які дозволили б застосовувати відповідні математичні методи (наприклад, побудувати матриці і графи зв'язків). Тому, у якості експерименту, для аналізу акаунтів соціальної мережі vk.com (ВКонтакте) та візуалізації їхніх контактів використовувались можливості наданого розробниками цієї соціальної мережі API (application programming interface) та сервісу Yasiv (доречі, цей сервіс створено та активно доробляється українцем – Андрієм Кащею). Аналіз відомостей у мережі Facebook здійснювався іншим методом – за допомогою так званої системи вилучення знань Wolfram Alpha, розробленого британським фізиком, математиком, програмістом Стівеном Вольфрамом (див. Мал. 2).

⁶⁸ Ландэ Д. Школа веб-разведки. Инструменты и источники / Д. Ландэ, В. Прищепя. // Телеком. — 2007. — № 7-8. — С. 46-49.

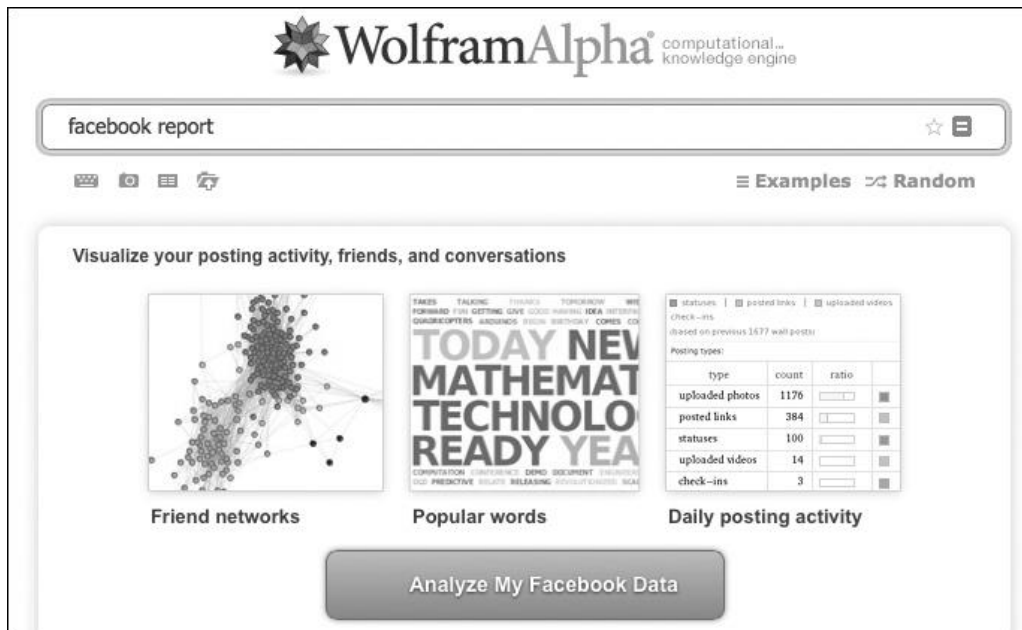
Мал.2. Приклади побудови графів зв'язків у мережах vk.com та Facebook.

На відміну від традиційних пошукових систем, Wolfram Alpha не намагається знайти відповідь на запит у мережі, а вираховує її, використовуючи чисельні відкриті джерела інформації. Ця система здійснює оцінку кількості записів у Facebook, типи розміщених матеріалів (фото, відео, посилання, статуси тощо) (див. Мал. 3).



Аналіз отриманих графів зв'язків у

будь-якому випадку необхідно здійснювати з урахуванням того, що кількість контактів координаторів з учасниками кола досліджуваної групи, як правило, мінімальна. Тому доречно звертати увагу на акаунти, що потрапили до графу та мають найменшу кількість зв'язків та/або «друзів». Саме такі користувачі мають найбільшу потенційну можливість збирати та розповсюджувати інформацію і тому являють собою максимальний інтерес та підлягають більш детальному вивченню.



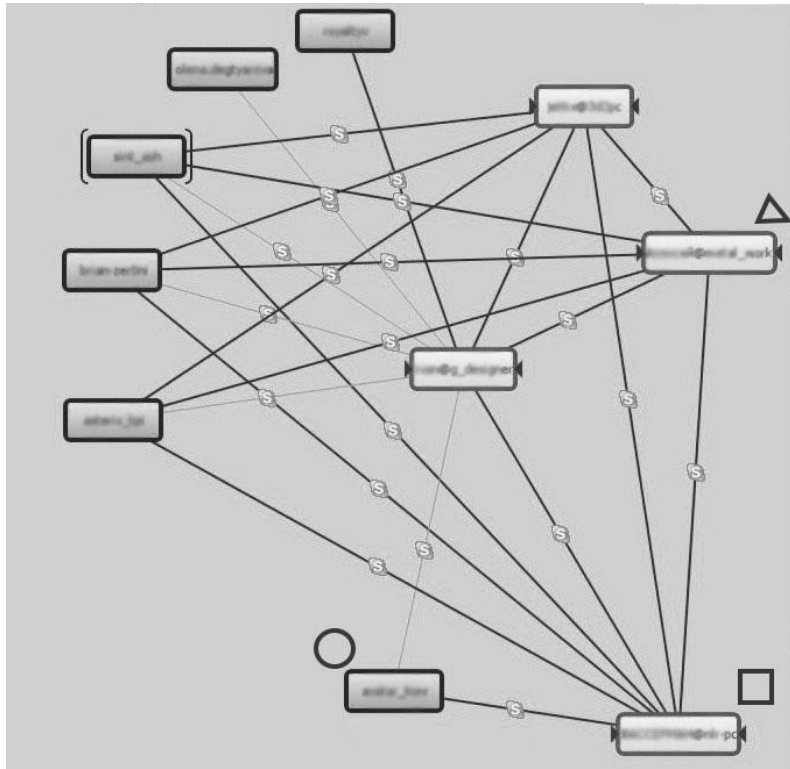
Мал.3. Комплексний аналіз контактів Facebook за допомогою Wolfram Alpha.

Дослідження інформаційного простору за допомогою методів OSINT – лише перший (але дуже важливий) крок, який мінімізує бюрократичні процедури та обмеження і передусє подальшому вивченню виявлених осіб за допомогою технічних засобів. Методика ж деталізованого моніторингу може полягати у цільовому перехопленні мережевого трафіку, вилучення з нього повідомлень та файлів для подальшого аналізу.

Таким способом можна отримувати повідомлення та вкладення електронної пошти (у тому числі такої, що відправлена за допомогою веб-інтерфейсу); дані, відправлені з використанням інтернет-браузерів у чати, блоги, форуми та соціальні мережі, а також запити до пошукових систем; файли, що отримувались або відправлялись по FTP-протоколу, за допомогою служб миттєвих повідомлень (наприклад, ICQ) або через соціальні мережі; документи хмарних сховищ даних. Використання недоліків у захисті інформації та непрофесійні дії більшості користувачів Інтернету дозволяють також здійснювати моніторинг операцій користувачів із файлами, що зберігаються на файлових серверах. Проте, такі дії доцільно здійснювати, спираючись на результати первинного моніторингу, та застосовувати до виявлених під час нього потенційних зловмисників лише враховуючи вимоги

чинного законодавства у сфері оперативно-розшукової, розвідувальної та контррозвідувальної діяльності.

На Мал. 4 наведено приклад цільового перехоплення спілкування у службі миттєвих повідомлень Skype та побудова відповідного графу зв'язків (ілюстрацію подано у спрощеному вигляді).



Мал.4. Приклад побудови графу зв'язків у Skype.

На початку дослідження один з контактів (позначений трикутником) через свої дії у соціальних мережах викликав підозру у поширенні сепаратистських настроїв. Подальший моніторинг його спілкування у Skype дозволив побудувати відповідний граф зв'язків (вершини графу – об'єкти спілкування, грані – наявність трафіку між співрозмовниками, а товщина граней – об'єм трафіку). Одна з вершин графу підпадає під підозру у якості координатора (позначена колом) – можна побачити мінімальну кількість контактів для спілкування, проте один із співрозмовників (позначений квадратом) має зв'язок майже з усіма іншими вершинами графу, а кількість повідомлень, що циркулюють між ним та іншими практично дорівнює трафіку між ним та потенційним координатором. Після отримання

попередніх висновків можна знову повернутись до методів OSINT, але тепер – стосовно обох нових встановлених осіб.

У матеріалі було розглянуто підходи до моніторингу інформаційного простору з урахуванням останніх звітів Європолу стосовно терористичних загроз. Приділено увагу альтернативним пошуково-аналітичним системам та особливостям їхнього використання. Дослідження можливостей моніторингу та аналізу інформації у мережі Інтернет (насамперед, у соціальних мережах) підтвердило ефективність використання реєстру загроз терористичного характеру у якості класифікатора отриманої інформації. Крім цього, стало зрозуміло, що для подальшої уніфікації реєстру загроз терористичного характеру необхідно не тільки здійснювати сортування результатів моніторингу за відповідними розділами реєстру, а й здійснити його модернізацію, що полягатиме у формуванні та внесенню до нього окремими підпунктами підготовлених і сформульованих типових термінів комплексних пошукових запитів. Такий крок дозволить суттєво оптимізувати моніторинг у Інтернеті та надасть змогу в подальшому автоматизувати класифікацію отриманих результатів відповідно до розділів реєстру загроз терористичного характеру.

10. МОДЕЛЬ ЗВ'ЯЗКІВ МІЖ ЗАГРОЗАМИ ТЕРОРИСТИЧНОГО ХАРАКТЕРУ ТА РЕАКЦІЄЮ СУСПІЛЬСТВА НА ЇХ ВПЛИВИ

Події останніх місяців в нашій державі свідчать про недосконалість сучасних стратегій протидії тероризму на усіх рівнях їх реалізації. Як наслідок неопрацьованості тактико-спеціального та військово-технічного аспекту боротьби з тероризмом, недосконалісті науково-методологічної основи антитерористичних технологій ми маємо чисельні жертви терористичних атак. Вдосконалення державної системи боротьби з тероризмом вимагає пошуку нових методик дослідження тероризму, прогнозування та моделювання загроз терористичного характеру, виявлення та мінімізації його суспільно-небезпечних наслідків.

Осмилення тероризму як суспільно небезпечного явища стало предметом активних наукових розвідок наприкінці ХХ ст., перш за все в напрямку опрацювання окремих аспектів: юридичного, воєнно-технічного, історичного. Сьогодні вивчення феномена тероризму активізувалося як в країнах, що зазнали терористичних нападів, так і в державах, що усвідомлюють його потенційну небезпеку, зокрема в Україні. Сучасні наукові розвідки тероризму зводяться до кількох напрямів: антологія масового терору й історіографічні нариси здійснених терористичних актів, кримінально-правові дослідження, організаційно-правові основи становлення системи боротьби з тероризмом, тактика й технологія антитерористичних дій тощо. До дослідження тероризму долучалися також аналітики відповідних силових структур, завдання яких відрізнялись від цілей суто наукових.

Аналіз літературних джерел з цієї тематики дозволяє зробити висновок, що в даний час в Україні не сформована цілісна система протидії тероризму та не визначена її цільова функція. Відсутні також науково обґрунтовані процедури оцінювання та прогнозування загроз терористичного характеру та

їх впливу на визначальні сфери життєдіяльності суспільства та держави, що і визначає актуальність даної статті. У наведених публікаціях та у інших наукових працях, з якими змогли ознайомитися автори, відсутні моделі, по яким можна було б кількісно оцінювати реакцію суспільства на виклики сучасного тероризму.

Особливу актуальність пошук оптимальних стратегій та впровадження наукоємних технологій боротьби з тероризмом набуває зараз, у зв'язку з проведенням антитерористичної операції підвищеним ризиком прояву загроз терористичного характеру. Усунення або мінімізація дії чинників, що сприяють виникненню та поширенню тероризму, прогнозування, виявлення та усунення терористичних загроз визначені в Державній концепції боротьби з тероризмом як основні заходи по запобіганню терористичній діяльності⁶⁹.

В основі концептуальної моделі профілактики тероризму знаходиться цільова функція - визначення умов, при яких соціальний конфлікт буде дозволений насильницьким шляхом із застосуванням терористичних методів. Рішення цієї функції припускає виявлення й оцінку стана механізмів, що визначають процес розвитку терористичних загроз, як елемента еволюційного процесу соціальної системи.

Аналіз резонансних загроз терористичного характеру у світі в останні роки свідчить, що об'єднуючою характеристикою реакції суспільства на їх прояв є зростання соціально-політичної напруженості (СПН) в державі. Слід зазначити, що рівень СПН є також одним із основних критеріїв оцінювання рівня національної безпеки держави. Зазначене свідчить про його високу репрезентативність при оцінюванні соціально-політичних процесів у суспільстві, до яких відноситься як терористична діяльність, так і протидія цій діяльності.

Визначено основні складові та функції системи забезпечення національної безпеки, але протидія загрозам терористичного характеру

⁶⁹ Концепція боротьби з тероризмом. [Електронний ресурс].– Режим доступу: <http://zakon4.rada.gov.ua/laws/show/230/2013>

розглянута лише у загальному вигляді, що не дозволяє провести їх структурну класифікацію, сформувані структуровані бази даних, з використанням яких можна було б здійснювати сценарний аналіз ЗТХ⁷⁰. У загальному виді сформульовано критерій забезпечення національної безпеки та запропоновано математичну модель оцінювання рівня соціально-політичної стабільності, надано рекомендації щодо оцінювання його динаміки у часі, що може бути з певною трансформацією під загрози терористичного характеру використано для розробки моделі зв'язків між загрозами терористичного характеру та реакцією суспільства на їх впливи.

Оцінка (мірило) за даним критерієм може проводитися як окремо, за кожним з визначених вражаючих факторів терористичної загрози, так і за їх сукупним впливом, зокрема, методами експертних оцінок або інших, наприклад, методом **SWOT – аналіза** (SWOT - це аббревіатура чотирьох англійських слів: S - Strengths - сильні сторони, W - weaknesses - слабкі сторони, O - Opportunities - можливості, T - Threats - загрози. SWOT-аналіз це відносно легкий у застосуванні інструмент для оцінки стратегічного стану будь-якого об'єкту⁷¹. Метод SWOT дозволяє встановити лінії зв'язку між зовнішніми можливостями і загрозами та сильними і слабкими сторонами об'єкту можливого терористичного нападу. Така робота спрямована на те, щоб стратегія антитерористичного захисту якнайкраще поєднувала зовнішню ситуацію (можливості і загрози) з антитерористичним потенціалом об'єкту (сильними і слабкими сторонами)). Частково даний метод може бути використаний при аналізі ЗТХ.

⁷⁰ Богданович В.Ю., Свида І.Ю., Скулиш Є.Д. *Теоретико-методологічні основи забезпечення національної безпеки України: Монографія.* : у 7 т..-Т.1.Теоретичні основи, методи й технології забезпечення національної безпеки України / В.Ю.Богданович, І.Ю.Свида, Є.Д.Скулиш; за заг. ред. Є.Д.Скулиша.-К.:Наук.-вид. відділ НА СБ України, 2012.-548с.

Богданович В.Ю., Свида І.Ю., Скулиш Є.Д. *Теоретико-методологічні основи забезпечення національної безпеки України: Монографія.* : у 7 т..-Т.4. Воєнна безпека держави та шляхи її забезпечення / В.Ю.Богданович, І.Ю.Свида, Є.Д.Скулиш; за заг. ред. Є.Д.Скулиша.-К.: Наук.-вид. відділ НА СБ України, 2012.-464с.

⁷¹ Олена Кадишева *Методика проведення SWOT-анализу. [Електронний ресурс].-Режим доступу: <http://www.businessstuning.ru/pm/80-swot-analiz-cto-eto-metodika-provedeniya-swot-analiza.html>*

Метод «Діаграма Ісікави», який дозволяє у простій і доступній формі систематизувати потенційні причини розглядаємих проблем, виділяти найбільш суттєві та проводити порівневий пошук першопричин⁷². При певній модифікації методу його можна використати для систематизації і ранжування ЗТХ.

Оскільки множина ЗТХ має тенденцію до розширення, то їх аналіз об'єктивно потребує їх об'єднання у деякі класи, групи, кластери по ряду спільних ознак. У попередніх публікаціях нами було запропоновано 13 кластерів ЗТХ, що дає змогу суттєво полегшити їх аналіз та організацію протидії виявленим загрозам. Такий аналіз здійснюється у два етапи. На першому етапі виявлена ЗТХ ідентифікується з одним із кластерів, на другому етапі - з типом загрози, яка згідно класифікації віднесена до даного кластера, або виділяється як загроза нового типу (нова загроза).

Реакцію на загрозу можна порівняти з реакцією організму людини на певне захворювання (наприклад, підвищення температури, тиску, слабкість, тошнота і ін.). А щоб організувати ефективну протидію виявленій ЗТХ необхідно провести її оцінювання (встановити діагноз). Чим точніше буде проведене оцінювання, тим менші збитки будуть нанесені суспільству, об'єктам, людям тощо. На превеликий жаль, у аналітиків та експертів немає точного інструменту оцінювання ЗТХ, що призводить до низької точності їх оцінювання з усіма витікаючими із цього наслідками. Найбільш вживаним на сьогодні є метод SWOT-аналізу⁷³. Даний метод оперує з якісною інформацією, не передбачає отримання кількісних оцінок, тому дає занадто неточні оцінки. Точність методу суттєво залежить від кваліфікації експертів, що залучаються до оцінювання та прогнозування, а також від повноти та

⁷² Метод «Діаграма Ісікави». [Електронний ресурс].- Режим доступу: <http://www.inventech.ru/pub/methods/metod-0019/>

⁷³ Саати Т., Кернс К. Аналитическое планирование. Организация систем / Пер. с англ. – М.: Радио и связь, 1991. – 224 с.

точності інформації, що надається експертам для обробки, яка дуже рідко буває повною та достовірною.

Для розв'язання нашої задачі пропонується комбінований метод побудови моделі ЗТХ, який дозволяє ідентифікувати виявлену ЗТХ з певним кластером за допомогою методу SWOT-аналізу, вибір та уточнення типу загрози в кластері, і на цій основі побудова трьохрівневої ієрархічної моделі здійснюється по технології удосконаленого методу аналізу ієрархій, а відбір сфер (факторів) та показників реалізації ЗТХ в кожній сфері здійснюється по методу Ісікави з модифікованою оболонкою. Методом SWOT-аналізу здійснюється вербальний опис виявленої (прогнозованої) ЗТХ, зокрема джерело, масштаб, спрямування, у який спосіб і чим ця загроза може бути підсилена, які сфери життєдіяльності суспільства зачіпає, через які конкретні дії, акції може проявлятися. Тобто, ми використовуємо метод не у класичному виді, а лише у тій частині, що стосується оцінки сильних сторін ЗТХ і тих наслідків, які вона може спричинити у визначальних сферах життєдіяльності суспільства.

Суть модифікації методу Ісікави зводиться до наступного. По-перше, з правого боку записується мета оцінювання виявленої або прогнозованої ЗТХ – реакція суспільства на деструктивний вплив ЗТХ, рис. 1, яка у подальшому буде кількісно визначатися рівнем соціально-політичної нестабільності $K_{спн}(t)$ у межах від 0 до 1 (перший рівень ієрархічної моделі зв'язків). По-друге, з лівого боку на основі оцінки теророгенної обстановки у формалізованому виді записується виявлена ЗТХ, що віднесена до конкретного кластеру і описана методом SWOT-аналізу. По-третє, на лінію зі стрілкою, що з'єднує другу дію з першою під кутом, що менший 90 градусів, проводяться стрілки, які описують виявлений вплив на зростання соціально-політичної нестабільності у найважливіших сферах життєдіяльності суспільства (держави) (другий рівень ієрархічної моделі зв'язків). На лінії по кожній сфері s ($s = 1, S$) експертами наносяться лінії, що характеризують конкретні (часткові) впливи, які деякі дослідники називають показниками,

індикаторами впливу P_{sn} , ($n = 1, N$), які представляють третій (нижній) рівень ієрархічної моделі зв'язків, як це зображено на рис.2. Якщо оцінювання $K_{спн}(t)$ здійснюється з використанням відомої комп'ютерної технології $M7$ [2,3], то кількість сфер і кількість показників по кожній сфері бажано вибирати не більше дев'яти ($S \leq 9$, $N \leq 9$). Детально процедури оцінювання та прогнозування $K_{спн}(t)$ описані⁷⁴. Отримане значення прогнозованого на час t_1 рівня соціально-політичної нестабільності, що «провокується» виявленою ЗТХ, порівнюється з рівнем соціально-політичної нестабільності до виявлення даної ЗТХ на момент часу t_0 . Отримане зростання рівня соціально-політичної нестабільності

$$\Delta K_{спн}(t_1) = K_{спн}(t_1) - K_{спн}(t_0)$$

характеризує інтегральну реакцію суспільства на прояв виявленої (прогнозованої на момент часу t_1) загрози терористичного характеру.

Подальшим розвитком даної моделі може бути прогнозування можливих сценаріїв реалізації даної загрози у часі або у просторі і прогнозування відповідно до цих сценаріїв рівня соціально-політичної нестабільності.

Отримуване кількісне значення зростання рівня соціально-політичної нестабільності може мати широке застосування при організації протидії тероризму. На його основі можна формулювати цільову функцію системи протидії тероризму як недопущення зростання рівня соціально-політичної нестабільності вище визначеного порогу, що в свою чергу дає змогу обґрунтовувати завдання, структуру, режими функціонування, оснащення, обсяги ресурсного, фінансового та інших видів забезпечення системи тощо.

⁷⁴ Богданович В.Ю., Свида І.Ю., Скулиш Є.Д. Теоретико-методологічні основи забезпечення національної безпеки України: Монографія. : у 7 т..-Т.1.Теоретичні основи, методи й технології забезпечення національної безпеки України / В.Ю.Богданович, І.Ю.Свида, Є.Д.Скулиш; за заг. ред. Є.Д.Скулиша.-К.:Наук.-вид. відділ НА СБ України, 2012.-548с.

Богданович В.Ю., Свида І.Ю., Скулиш Є.Д. Теоретико-методологічні основи забезпечення національної безпеки України: Монографія. : у 7 т..-Т.4. Воєнна безпека держави та шляхи її забезпечення / В.Ю.Богданович, І.Ю.Свида, Є.Д.Скулиш; за заг. ред. Є.Д.Скулиша.-К.: Наук.-вид. відділ НА СБ України, 2012.-464с.

Таким чином, запропонована ієрархічна модель реагування суспільства на прояв виявленої (прогнозованої на момент часу t_1) загрози терористичного характеру дозволяє враховувати класи і типи загроз, їх характер, масштаб, спрямування, можливі деструктивні наслідки у визначальних сферах життєдіяльності суспільства і держави і на цій основі визначати рівень соціально-політичної нестабільності по шкалі від 0 до 1. Вихідна інформація моделі дає змогу також кількісно оцінювати ефективність функціонування державної системи протидії тероризму та визначати межі юридичної відповідальності посадових осіб, що приймають управлінські рішення у системі.

У подальших публікаціях буде запропонована методика оцінювання ефективності функціонування державної системи протидії виявленим (прогнозованим) загрозам, зокрема при обробці конкретних результатів роботи з формування Реєстру загроз терористичного характеру, розпочатої на підставі розпорядження керівника АТЦ на базі аналітичних підрозділів Штабу АТЦ при СБ України із залученням особового складу НОЦ НА СБ України та помічників начальників регіональних органів СБУ з координації антитерористичної діяльності.

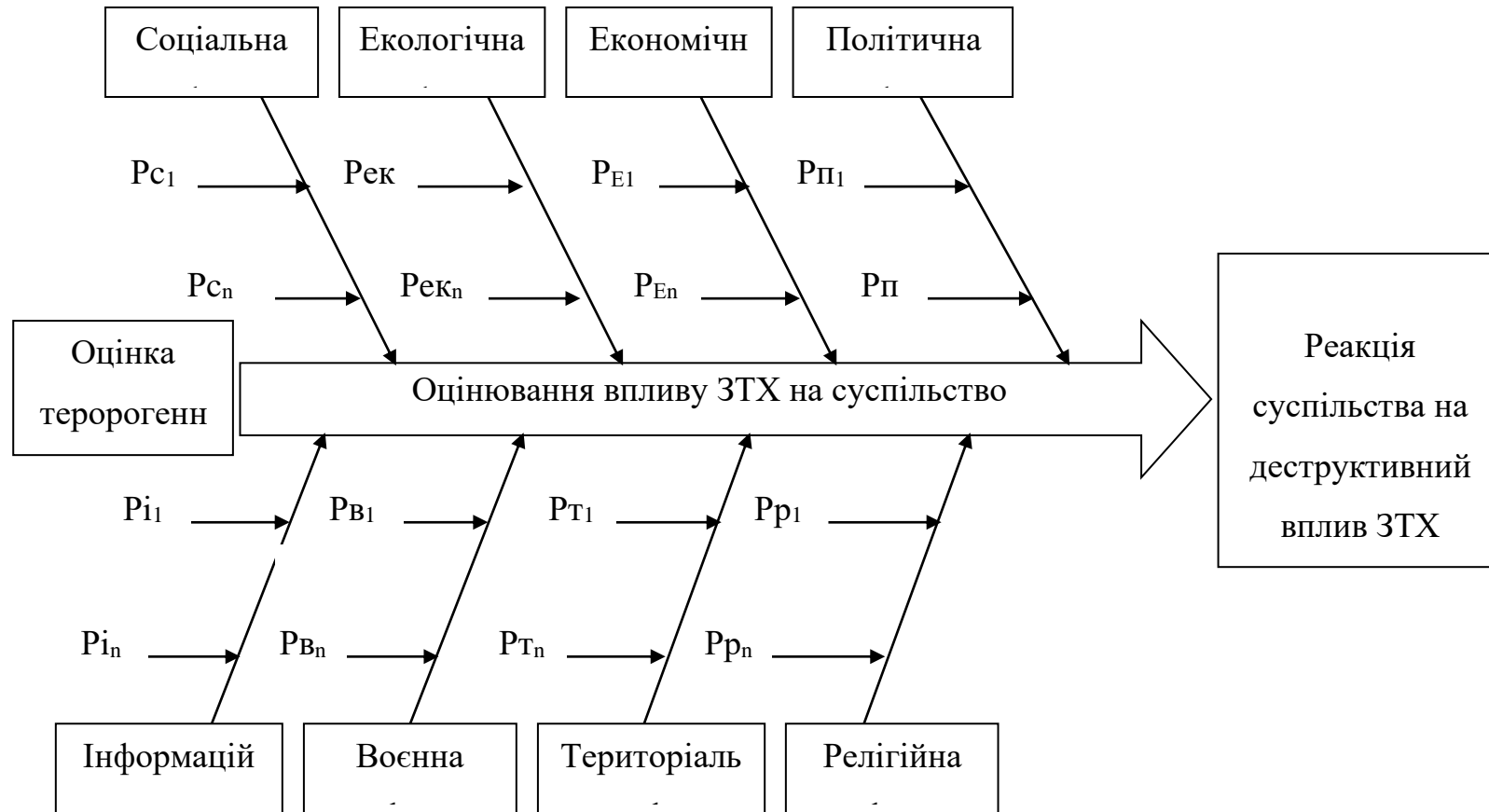


Рис. 1. Формалізація деструктивного впливу ЗТХ на суспільство

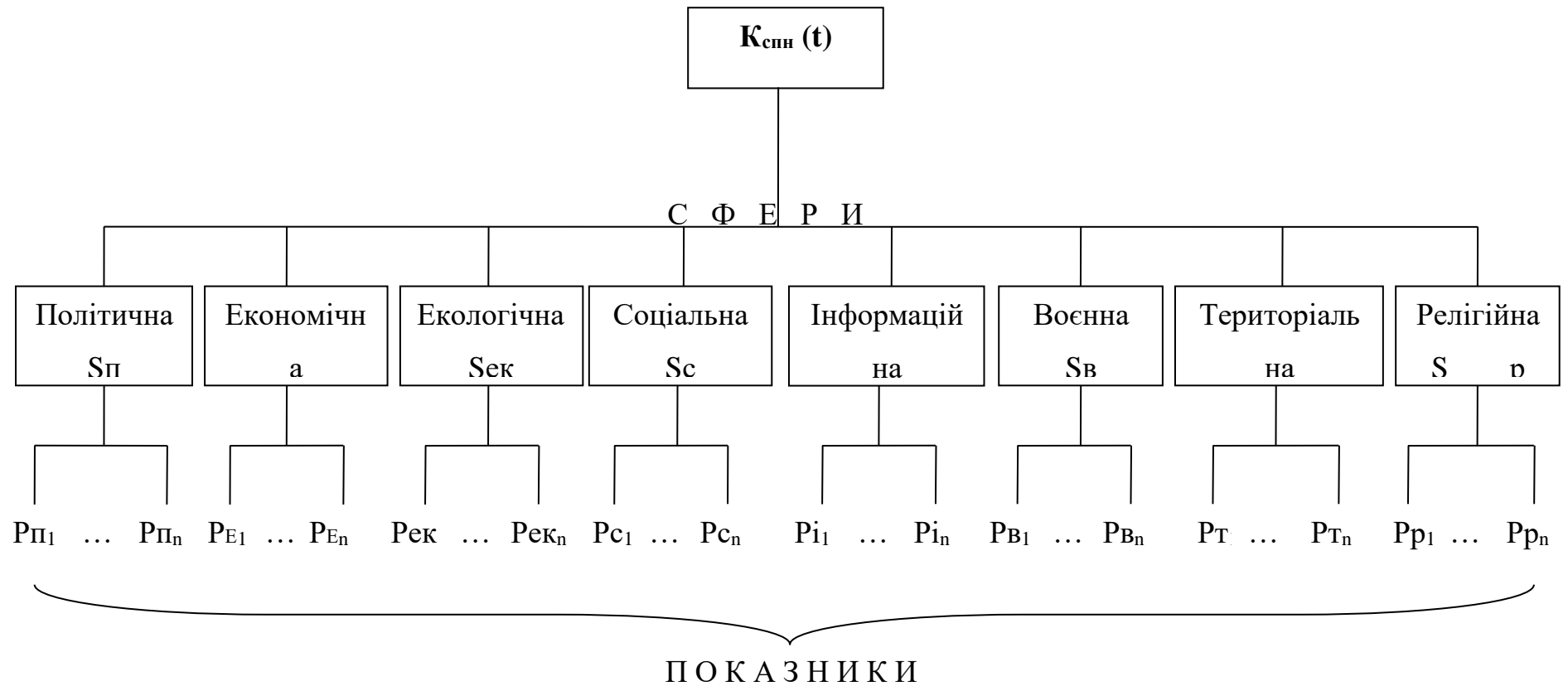


Рис. 2. Ієрархічна модель оцінювання впливу ЗТХ на рівень СПН суспільства

11. МЕТОДИКА ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ ПРОТИДІЇ ЗАГРОЗАМ ТЕРОРИСТИЧНОГО ХАРАКТЕРУ ОСОБИ АБО МАЛІЙ ГРУПИ ЛЮДЕЙ

Актуальність проблеми визначається необхідністю методичного підходу до визначення ЗТХ та створення адекватної ефективної системи протидії задля забезпечення своєчасного виявлення і блокування (нейтралізації) ЗТХ, в результаті реалізації яких можливе настання неприйнятних негативних наслідків національній безпеці.

Успіх реалізації систем управління ефективністю – багатогранна проблема, що припускає використання різних підходів і методик. Для оцінювання ефективності системи протидії ЗТХ застосовуються, як правило, методи, що враховують статистику терористичної активності й (або) боєготовність і боєздатність спеціальних підрозділів (іноді з показовою імітацією спеціальної операції).

Зазначене свідчить про актуальність та нагальну необхідність створення дієвої системи аналізу ЗТХ та оцінювання їх впливу на найважливіші сфери забезпечення національної безпеки, яка б базувалася на сучасних інформаційних технологіях та забезпечувала оперативну протидію цим загрозам⁷⁵.

Більшість сучасних наукових доробок як вітчизняних, так і закордонних науковців присвячено розробці оперативно-тактичних прийомів боротьби з терористичною діяльністю. Аналіз літературних джерел з цієї тематики дозволяє зробити висновок, що принципово важливим моментом у забезпеченні антитерористичної безпеки є уточнення функцій та завдань суб'єктів, розробка алгоритмів їхніх дій у тих чи інших умовах.

⁷⁵ Федюкин, В. К. *Управління якістю процесів / Спб.: Питер, 2005. — 202 с.*

Науковому супроводженню цих питань, дослідженню та формальному опису загроз у сфері національної безпеки приділяється неабияка увага, зокрема у контексті визначення індикаторів та розробки паспортів загроз задля можливості подальшого використання механізмів прогнозування. Про це свідчать публікації таких вітчизняних авторів, як: В.І. Абрамов, В.В. Крутов, А.Б. Качинський, В.А. Ліпкан, В.А. Мандрагеля, А.І. Семенченко, В.І. Строгий, І.В. Романов, І.В. Вещицький та інших вчених-дослідників. Проте, технології, за допомогою яких система боротьби з тероризмом може оцінювати свій поточний стан і виробляти ефективні та результативні стратегії майбутнього розвитку, зазнають значних змін. Науково-методична база формалізації загроз терористичного характеру та механізмів їх моделювання потребує розширення та подальшого удосконалення, що передбачає конкретизацію вибору методів аналізу, оцінювання, прогнозування тощо, як під час отримання необхідної інформації, так і під час її аналізу та оброблення.

Методика заснована на системному підході до функціонування системи протидії ЗТХ. Застосування принципу системності вимагає врахування співвідношення та взаємодії між складовими цієї системи та системою вищого рівня. Важливими складовими системи протидії є підсистеми інформаційного забезпечення та планування спеціальних заходів. Ефективність їх застосування залежить від обсягів, повноти, достовірності і своєчасності отримання інформації, оперативності і точності її оброблення, рівня підготовки, оснащення, навченості особового складу, якості управління та взаємодії в ході нейтралізації ЗТХ. Але процес визначення всіх цих показників ефективності ускладнюється труднощами їхньої формалізації та відсутністю відповідних методик оброблення інформації, що вносить в реальні оцінки і прогнози істотні похибки й суб'єктивізм.

Одним із шести відносно самостійних етапів запропонованої авторами загальної методики організації протидії ЗТХ є етап формування системи

показників та оцінювання ефективності протидії ЗТХ. Основними завданнями цього етапу є:

- визначення вектора показників оцінювання ефективності протидії ЗТХ та їх структурування;
- визначення інтегрального критерію ефективності протидії ЗТХ;
- розробка методики оцінювання ефективності протидії ЗТХ.

Враховуючи, що спектр ЗТХ є досить широким, а збитки визначаються множинами факторів, що залежать від класу, характеру, типу, масштабу і інших характеристик цих загроз, то й ефективність протидії буде визначатися у залежності від класу ЗТХ, що розглядається.

Розробку методики оцінювання ефективності протидії в системі забезпечення національної безпеки проведемо для класу загроз особі або малій групі людей (МГЛ). Для зручності будемо вважати, що підсистема інформаційного забезпечення виконує свої функції з ефективністю 100% і забезпечує підсистему планування спеціальних заходів інформацією про ЗТХ у повному обсязі (наприклад, з використанням SWOT-аналізу). Це означає, що ефективність системи протидії ЗТХ в системі забезпечення національної безпеки буде визначатися ефективністю підсистеми планування спеціальних заходів.

Звідси можна сформулювати *цільову функцію системи протидії ЗТХ*, що обумовлює її функціональну ознаку, як *обґрунтування і впровадження спеціальних заходів щодо мінімізації збитку від ЗТХ до рівня, при якому загальний збиток для особи (МГЛ) не перевищує допустимий*.

Якщо життя особи (МГЛ), проти якої приведено в дію загрозу, не вдалося зберегти, то ефективність системи протидії приймається рівною нулю, що слід вважати основним обмеженням.

Загальний збиток для особи (МГЛ) визначається векторною сумою часткових збитків в основних сферах життя людини (МГЛ): соціальній, політико-іміджевій, економічній, інформаційно-психологічній, релігійній, фізичного здоров'я тощо.

Формування системи показників оцінювання очікуваного збитку за кожною s -ю сферою (P_{s1} - P_{sn}) можна здійснити методом причинно-наслідкових зв'язків (діаграма Ісікави) (мал.1) з використанням відомих методів експертного опитування⁷⁶.

Такий підхід дає змогу побудувати модель оцінювання ефективності протидії ЗТХ у вигляді трирівневої ієрархії, де на першому (вищому) рівні розміщений загальний збиток для особи (МГЛ) $K_{збо}(t)$ ($K_{збмгл}(t)$), на другому рівні знаходяться S сфер ($s = 1,9$), у яких цей збиток мінімізується системою протидії, а на третьому (нижньому) рівні знаходяться показники оцінювання ефективності заходів P_{sn} , ($n = 1,9$), що впроваджуються у кожній сфері системою протидії, як це зображено на мал.2.

Якщо оцінювання $K_{збо}(t)$ ($K_{збмгл}(t)$) здійснюється з використанням відомої комп'ютерної технології M7, то кількість сфер і кількість показників по кожній сфері бажано вибирати не більше дев'яти ($S \leq 9$, $N \leq 9$). Детально процедури оцінювання та прогнозування $K_{збо}(t)$ ($K_{збмгл}(t)$) описані у монографіях [2, с.341-347, 3, с.268-299].

Особливістю побудованої ієрархічної моделі є те, що вона дозволяє кількісно оцінювати за технологією удосконаленого методу аналізу ієрархій як очікуваний загальний збиток особі (МГЛ), так і залишковий збиток, який не вдалося відвернути системі протидії в ході проведених спецзаходів. Виходячи з цього, ефективність системи протидії ЗТХ $E_{пзо}(t)$ можна оцінити величиною збитку особі (МГЛ) (об'єкту), який вдалося попередити (відвернути) завдяки впровадженню системою протидії спецзаходів, тобто наскільки ці заходи відновили економічні, інформаційно-психологічні, політичні, іміджові, релігійні та інші втрати особи (МГЛ), мал.3, жирна лінія 2.

Звісно, що позитивний ефект буде проявлятися лише у випадку, коли заходи, що приймаються системою протидії, будуть призводити до зниження загального збитку. Зрозуміло, що повністю нейтралізувати нанесений ЗТХ

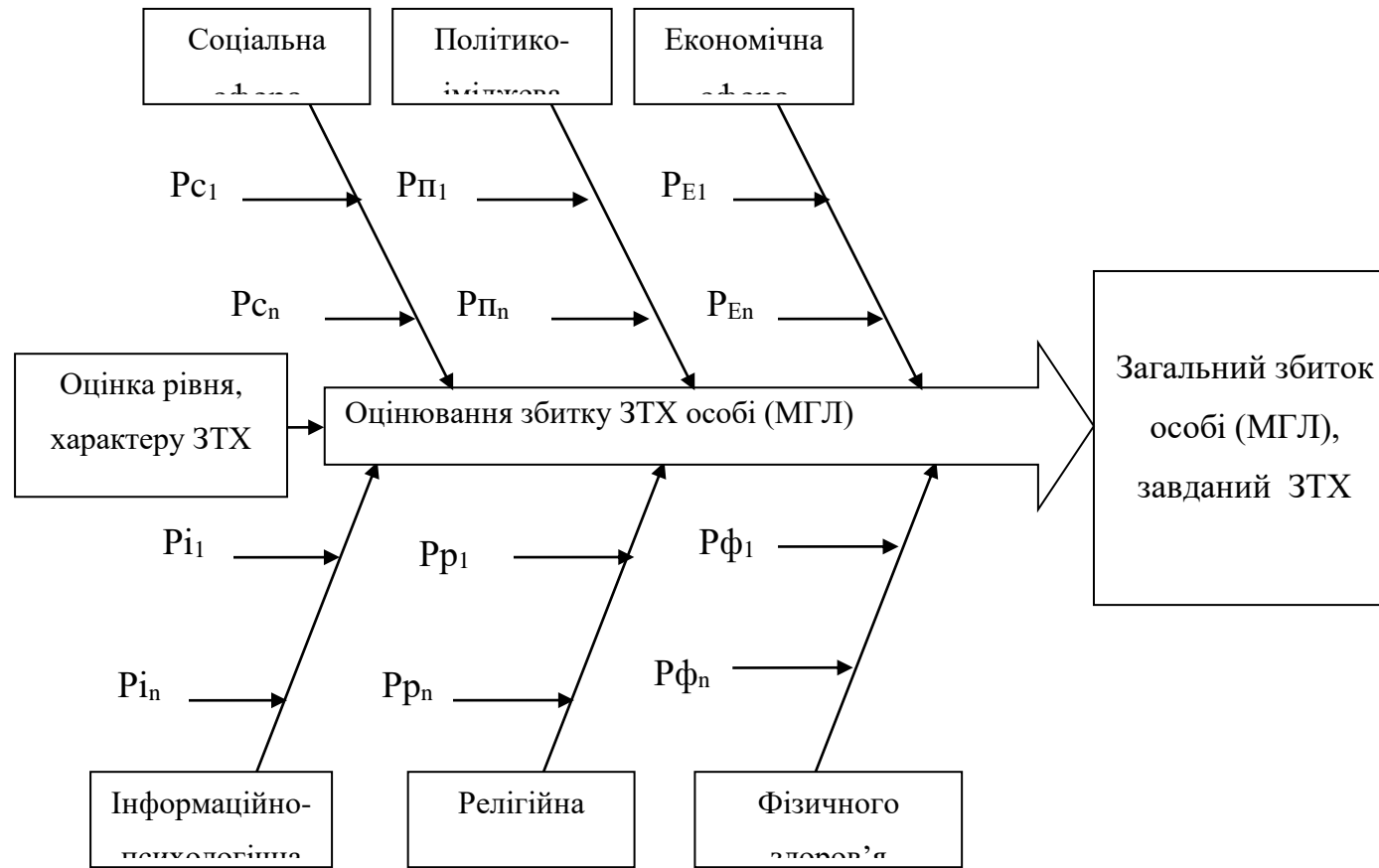
⁷⁶ Ісікава К. Японські методи управління якістю / Сокр.пер. с англ. / Під. Ред. А. В. Гличева. — М: Економіка, 1988. — 214 с.

збиток неможливо, перш за все через морально-психологічні обставини, тому доцільно ввести допустимий рівень загального збитку для особи (МГЛ)

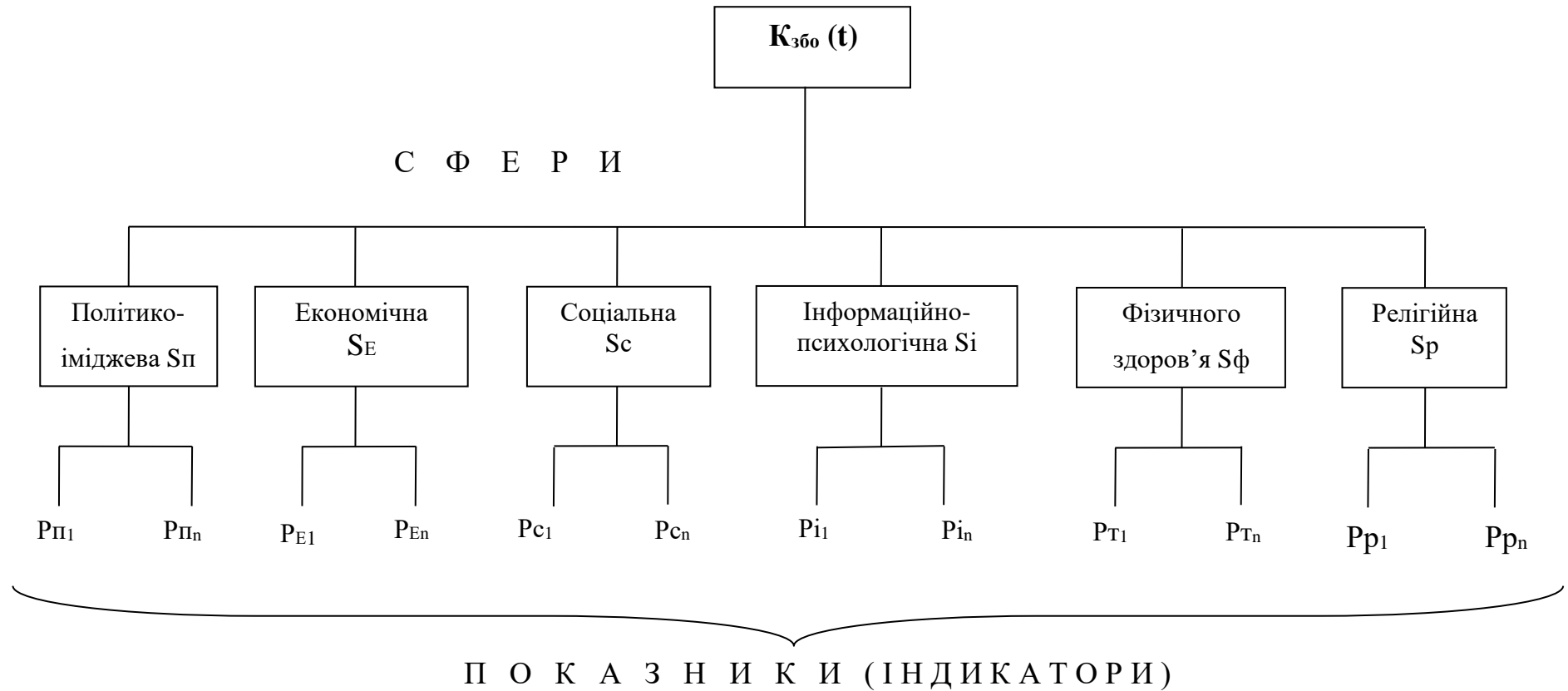
$K_{збодоп}(t)$, який гарантував би їй задовільний морально-психологічний, економічний, фізіологічний, іміджевий стан життєдіяльності тощо.

Допустимий рівень загального збитку для особи (МГЛ) одночасно може бути порогом прийняття рішення щодо зупинення протидії. Проте на практиці зупинення протидії може відбутися як раніше, так і пізніше (наприклад, переслідування терористів після звільнення особи-заручника).

Методика визначення допустимого рівня загального збитку для особи (МГЛ) представляє собою самостійне дослідження, якому буде присвячена окрема публікація.



Мал.1. Формалізація задачі оцінювання ефективності протидії ЗТХ методом причинно-наслідкових зв'язків



Мал.2. Трьохрівнева ієрархія задачі оцінювання збитку особі (МГЛ) від ЗТХ

Використання удосконаленого методу аналізу ієрархій дає змогу представити математичну модель оцінювання ефективності системи протидії ЗТХ у вигляді

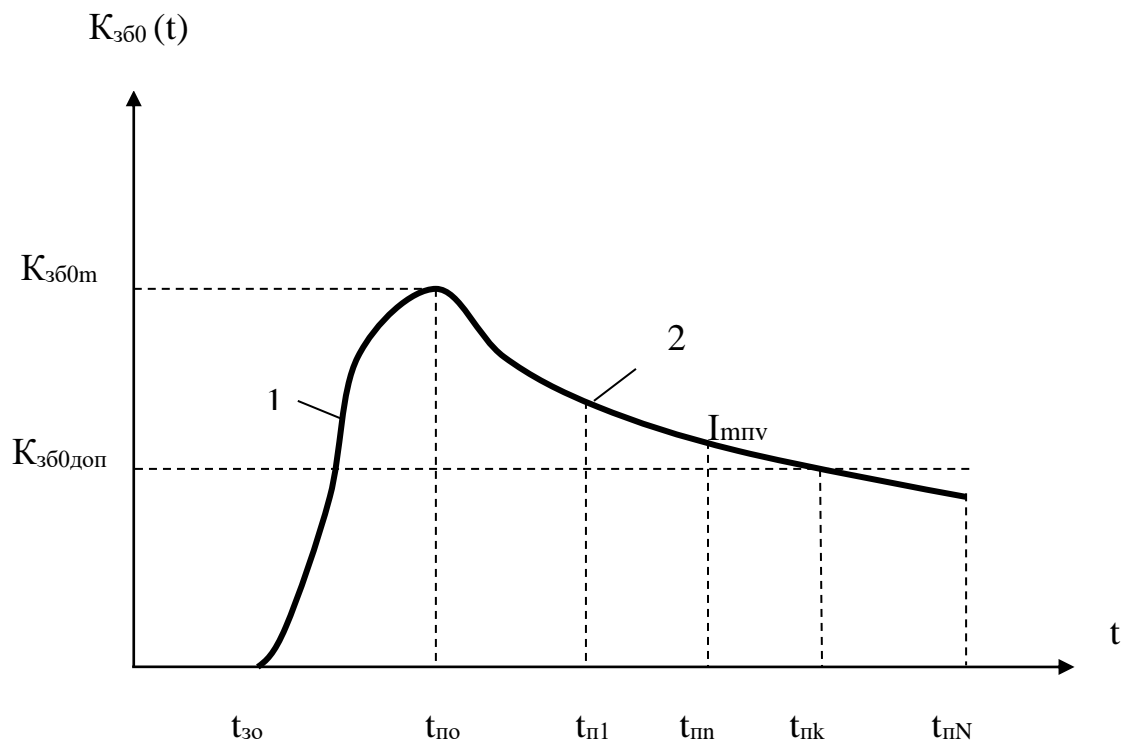
$$E_{\text{пзо}}(t) = K_{\text{збom}}(t_{\text{по}}) - K_{\text{збо}}(t_{\text{пн}}),$$

де $K_{\text{збom}}(t_{\text{по}})$ – очікуваний максимальний загальний збиток особи (МГЛ) від реалізації ЗТХ в момент початку протидії загрози $t_{\text{по}}$;

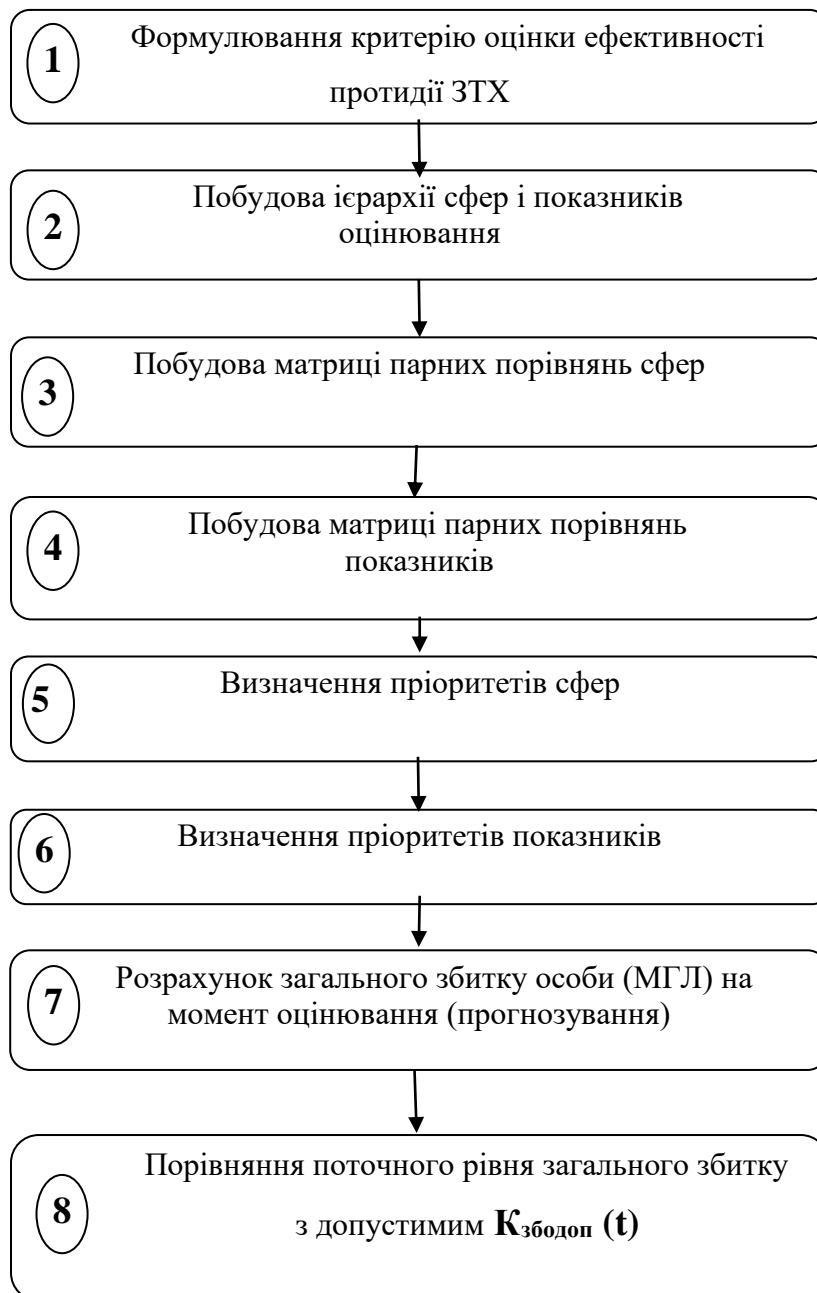
$K_{\text{збо}}(t_{\text{пн}})$ - загальний збиток особи (МГЛ) від реалізації ЗТХ в ході здійснення протидії в момент оцінювання $t_{\text{пн}}$ (див. мал.3).

Критерієм прийняття рішення щодо завершення протидії можна вибрати

$$E_{\text{пзов}}(t) = K_{\text{збom}}(t_{\text{по}}) - K_{\text{збодоп}}(t_{\text{пк}})$$



Мал.3. Гіпотетичний приклад протидії загрозі терористичного характеру: 1 – функція, що описує зростання загального збитку від моменту початку реалізації ЗТХ; 2 – функція, що описує нейтралізацію загального збитку від початку протидії і до досягнення його допустимого рівня (завершення протидії $t_{\text{пк}}$).



Мал.4. Блок-схема методики оцінювання загального збитку особи (МГЛ) від ЗТХ

Для перевірки працездатності методики проведемо чисельний експеримент. Розглянемо гіпотетичну загрозу захоплення у заручники генерального директора продовольчого мегамаркета Іванова І.І. двома озброєними АКМ терористами, які вимагали викуп в 1 млн грн і літак до Туреччини, та погрожували застрелити заручника, якщо не будуть виконані їхні умови. У Іванова є дружина і 3 доньки, автомобіль, дача тощо. Він є депутатом міської ради. У цей день Іванов І.І. мав бути на засіданні ради міста, де зокрема повинні були розглядатися питання щодо направлення спонсорських коштів на модернізацію дитячого садка для дітей з особливими потребами. Проте, з огляду на надзвичайну подію, міськрада розглядала у робочому порядку виділення цих грошей на викуп чиновника у терористів, що було зафіксовано запрошеними на захід журналістами та поширено ЗМІ.

Операція по звільненню тривала 1,5 години. Було задіяно 10 співробітників «Альфи», 20 співробітників поліції (лінія оточення). Про подію знало керівництво місцевої поліції та СБУ. Під час звільнення заручник був травмований терористами і направлений до лікарні. Про подію дізналися журналісти місцевих теле- і радіо- каналів, місцеві блогери соціальних мереж.

Результати експертного оцінювання з використанням 9-ти бальної шкали⁷⁷ максимального та попередженого збитків наведені у таблиці 1.

Таблиця 1. Експертна оцінка максимального та попередженого збитку

Сфера	Показники	Експерт	Експертн
-------	-----------	---------	----------

⁷⁷ Саати Томас. *Принятие решений: Метод иерархий*. — М.: Радио и связь, 1993. — 320 с.

впливу та її пріоритет	(наслідки) прояву	на оцінка максимального збитку	а оцінка попередженого збитку
Політич на (9)	П1-можливе позбавлення депутатства;	9	7
	П2-виявлення незадекларованого майна;	7	5
	П3-звинувачення у корупції;	9	5
	П4-нанесення шкоди іміджу	7	3
Економі чна (9)	Е1-перевірка діяльності фіскальною службою;	9	7
	Е2-нецільове використання коштів;	7	7
	Е3-пошкодження службового автомобіля;	5	5
	Е4-пошкодження службового телефону.	3	3
Соціаль на (7)	С1-подання у відставку;	7	5
	С2-бойкот роботи мегамаркету;	5	3
	С3-порча товарів.	7	3
Інформа ційно- психологічна (9)	Іп1-негативні відгуки про депутата та його політичну силу;	9	5
	Іп2-образи від знайомих;	5	3
		7	1
		9	5

	<p>Іп3-петиції у соціальних мережах;</p> <p>Іп4-негативні публікації в ЗМІ та Інтернет;</p> <p>Іп5-негативні публікації про його приватне життя.</p>	9	5
Релігійна (3)	<p>Р1-втрата довіри місцевої релігійної громади;</p> <p>Р2-поширення негативної інформації серед прихожан.</p>	3 5	3 3
Фізичне здоров'я (5)	<p>Ф1-психічні розлади;</p> <p>Ф2-зламани ребра і рука;</p> <p>Ф3-простуда.</p>	7 7 3	5 7 3

Використовуючи модель (інформаційну технологію) М7, отримуємо значення очікуваного максимального загального збитку особи:

$$K_{зб\text{ом}}(t_0) = 0,876$$

Загальний збиток особи від реалізації ЗТХ в ході здійснення протидії через 1,5 години після початку загрози складає

$$K_{зб\text{о}}(t=1,5) = 0,587$$

Ефективність системи протидії складає

$$E_{пзо}(t=1,5) = K_{зб\text{ом}}(t_{по}) - K_{зб\text{о}}(t=1,5) = 0,876 - 0,587 = 0,289 \text{ (28,9 \%)}.$$

Отримані результати свідчать про працездатність методики.

Таким чином, запропонована методика дає змогу оцінювати ефективність протидії ЗТХ, що спрямовуються проти особи або малої групи людей в загальній системі забезпечення національної безпеки шляхом оцінювання очікуваного (прогнозного) рівня загального збитку особі (малій групі людей) на момент початку протидії виявленій загрозі, динаміку нейтралізації загального збитку спеціальними заходами, що реалізуються системою протидії. Це дозволяє спрямовувати протидію таким чином, щоб найбільш оперативно нейтралізувати загальний збиток (до рівня допустимого), що гарантувало би особі (МГЛ) задовільний морально-психологічний, економічний, фізіологічний, іміджевий та інший стан життєдіяльності.

Завдяки отримуваним кількісним оцінкам ефективності з'являється можливість більш зважено та цілеспрямовано обґрунтовувати ресурсне, інформаційне та кадрове забезпечення заходів з протидії загрозам терористичного характеру.

Слід зазначити, що отримувана за допомогою представленої методики інформація носить рекомендаційний характер для осіб, що приймають рішення з питань протидії терористичній діяльності.

12. КОНЦЕПТУАЛЬНІ ПІДХОДИ ДО ПОБУДОВИ СИСТЕМИ ПРОТИДІЇ ЗАГРОЗАМ ТЕРОРИСТИЧНОГО ХАРАКТЕРУ

У сучасному суспільстві тероризм, як негативний соціальний феномен, набув небувалого поширення у всьому світі. Він постійно змінює форми та набуває глобального масштабу, його методи стають все більш витонченими і руйнівними. Зростаюче число жертв насильства, нездатність держав зупинити терор, могутній суспільний резонанс, неконтрольована діяльність ЗМІ сприяють зростанню напруженості і соціально-політичній нестабільності.

Той факт, що вже досить тривалий час Україні проводиться масштабна антитерористична кампанія змушує переосмислити загальні підходи до проблеми тероризму та боротьби з ним, визнаючи, що зведення протидії тероризму тільки до певного виду діяльності – боротьби з терористами, являє собою занадто спрощений варіант вирішення такої глобальної проблеми, а стратегії боротьби з терористичною діяльністю по факту її реалізації втратили свою дієздатність. Суспільство, яке потерпіло від терористичних атак, потребує забезпечення почуття впевненості у власній безпеці, гарантій ефективності функціонування системи забезпечення національної безпеки в умовах загроз терористичного характеру для свого гармонійного розвитку та душевної рівноваги.

Більшість сучасних наукових доробок як вітчизняних, так і закордонних науковців-терорологів, присвячено кримінологічному аспекту тероризму та розробці оперативно-тактичних прийомів боротьби з терористичною діяльністю на рівні організації та планування антитерористичної операції. Аналіз літературних джерел з цієї тематики дозволяє зробити висновок, що в даний час в Україні у різних прошарках населення неоднозначне тлумачення термінів «терорист» і «терористичний

акт», недостатньо відпрацьовані рекомендації щодо дій у разі здійснення терористичного акту, відсутня належна система підготовки фахівців для проведення переговорів з терористами та інші.

Загрози терористичного характеру (далі – ЗТХ) займають особливе місце в загальній картині загроз національній безпеці. Здатність суспільства завчасно виявляти наміри щодо приведення в дію ЗТХ – запорука його антитерористичної безпеки. Зазначене свідчить про актуальність та нагальну необхідність створення дієвої системи аналізу ЗТХ та оцінювання їх впливу на найважливіші сфери забезпечення національної безпеки (далі система протидії ЗТХ), яка б базувалася на сучасних інформаційних технологіях та забезпечувала протидію цим загрозам у масштабі часу, наближеному до реального.

Спеціалізовані інформаційні ресурси суб'єктів боротьби з тероризмом, які актуальні на цей час, мають всі необхідні вхідні дані, які потрібні та можуть бути використаними підчас моделювання терористичної загрози потенційним об'єктам на території України з метою визначення достатності рівня захищеності від терористичних посягань. Ефективність їх використання безпосередньо визначається рівнем компетентності фахівців, які розробляють рекомендації щодо інституціональної та технологічної складових систем забезпечення антитерористичної безпеки.

Поширеною в багатьох країнах світу концепцією реалізації системи заходів антитерористичного захисту є організація багатоступінчастого процесу аналізу і планування, який включає в себе виявлення ризиків, подальшу перевірку і, за необхідності, адаптацію технологічних, будівельних, організаційних, інформаційних, кадрових та інших заходів захисту.

Основні складові та функції системи забезпечення національної безпеки опрацьовано, але протидія загрозам терористичного характеру наведена лише у загальному вигляді, що не дозволяє провести їх структурну

класифікацію, сформувати структуровані бази даних, з використанням яких можна було б здійснювати сценарний аналіз ЗТХ та протидіяти цим загрозам.

Аналогічна ситуація і з опрацюванням методологічних підходів до автоматизації інформаційно-аналітичних процесів безпекового супроводу реалізації національних інтересів, але загрози терористичного характеру розглянуті лише у концептуальному плані.

Зважаючи на викладене, науково-методична база формалізації загроз терористичного характеру, механізмів їх аналізу, моделювання, прогнозування та протидії потребує розширення та подальшого удосконалення.

Організація протидії ЗТХ – це складний процес діяльності суб'єктів, на які покладено повноваження і відповідальність за забезпечення національної безпеки. У цьому процесі суб'єкт управлінської діяльності послідовно переходить від якісних етапів пізнання взаємовідносин в ході організації протидії ЗТХ до розуміння сутності цих взаємовідносин та отримання більш достовірних знань про них. Розглянемо концептуально ці етапи і зосередимося у даній публікації на розробці загальної методики виявлення, аналізу та організації протидії ЗТХ.

Організація протидії ЗТХ має проходити певні етапи, які повинні відображати сутність розробки інформаційно-аналітичного забезпечення заходів щодо протидії або, іншими словами, визначати функціональну структуру системи. Узагальнену характеристику цих етапів наведено у табл.1.

Під час проектування етапів програми організації протидії ЗТХ слід виходити з того, що її розроблення має два аспекти. З одного боку, програма є основним документом наукового пошуку, який забезпечує наукову обґрунтованість розв'язання поставленого завдання, з іншого боку – є, по суті, методологічним інструментарієм дослідження, в якому визначаються методологічні принципи побудови, цілі, функції та завдання системи.

Таблиця 1

Характеристика етапів розробки системи протидії ЗТХ

Етап	Зміст етапу	Основні очікувані результати
Програмування	Розроблення методології побудови системи протидії.	Функціональна структура системи протидії ЗТХ.
Інформаційний	Застосування методів та технологій отримання достовірної інформації щодо процесів, які протікають в системі.	Інформація щодо виконання часткових завдань організації протидії.
Аналітичний	Аналіз отриманої інформації, її узагальнення, виявлення тенденцій, закономірностей, кореляційних зв'язків тощо.	<ul style="list-style-type: none"> - Опис та пояснення процесу організації протидії ЗТХ; - методичний апарат оцінювання ЗТХ та обґрунтування рішень, що приймаються вищим керівництвом держави щодо протидії ЗТХ; - критерії, модель та методика оцінювання ефективності протидії ЗТХ та їх впливу на визначальні сфери життєдіяльності держави.
Практичного впровадження	Розроблення рекомендацій щодо практичного застосування системи протидії ЗТХ.	<p>Рекомендації щодо:</p> <ul style="list-style-type: none"> - оптимізації функціональної структури системи протидії ЗТХ; - щодо вибору перспективної моделі інформаційно-аналітичного забезпечення системи протидії ЗТХ; - пропозиції щодо вибору

		<p>методів та порогів реагування вищим політичним керівництвом держави при організації протидії ЗТХ;</p> <p>- щодо підготовки та підвищення кваліфікації аналітиків для інформаційно-аналітичного супроводу функціонування системи протидії ЗТХ.</p>
--	--	--

До основних функцій програми віднесено:

- *методологічну*, яка полягає у визначенні методології, яку передбачається використовувати під час розробки системи;

- *методичну*, що передбачає конкретизацію вибору методів аналізу, оцінювання, прогнозування тощо, як під час отримання необхідної інформації, так і під час її аналізу та оброблення;

- *гносеологічну*, яка забезпечує зниження рівня невизначеності у розумінні процесу організації протидії ЗТХ після розроблення програми порівняно з його розумінням до її розроблення;

- *моделювальну*, яка полягає у представленні процесу організації протидії ЗТХ у вигляді деякої моделі, а також окремих, відносно самостійних етапів та процедур;

- *програмувальну*, яка полягає у розробленні програми як такої, що моделює та впорядковує сам процес організації протидії ЗТХ. Ця функція реалізується саме через розроблення загальної функціональної структури системи протидії ЗТХ.

На нашу думку, організації ефективної протидії ЗТХ заважає недосконалість існуючого науково-методологічного апарату їхнього виявлення, аналізу та прогнозування деструктивних впливів на життєво важливі сфери життєдіяльності держави.

Фактором, що ускладнює процес організації протидії ЗТХ, є різке посилення інформаційного протиборства за рахунок використання новітніх інформаційних технологій, що дають змогу терористичним елементам безперешкодно і приховано отримувати засоби здійснення терористичних актів, атак тощо, дистанційно приводити їх в дію, послабляти або завдавати значної шкоди безпеці держав в умовах недостатньо дієвих систем захисту від ЗТХ.

Беручи до уваги базове тлумачення поняття загрози національній безпеці, поняття загрози терористичного характеру – це наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України внаслідок скоєння терористичного акту. Під загрозою терористичного характеру розуміють потенційні дії або події, що прямо чи опосередковано сприяють виникненню терористичної діяльності.

У процесі реалізації принципу системності в загальнодержавному процесі боротьби з тероризмом особливе місце відводиться організації та забезпеченню дієвості системи превентивних заходів. Основною метою є відпрацювання комплексного усунення причин та умов, що сприяють виникненню злочинних проявів, у тому числі терористичної спрямованості.

Забезпечення національної безпеки в умовах дії сучасного спектру загроз різного характеру, у т.ч. і терористичного, потребує використання методології системного аналізу, з урахуванням специфічних особливостей ЗТХ⁷⁸.

По-перше, прийняття рішення щодо реалізації ЗТХ, планування та вибір моменту її початку – прерогатива тієї сили (сил), що її реалізує. Успіх зусиль щодо протидії залежить від часових параметрів процесів виявлення, розпізнавання та фіксації моменту і місця реалізації ЗТХ, прийняття рішення щодо організації протидії, впровадження контрзаходів тощо. Це означає, що

⁷⁸ Богданович В.Ю. *Методологічний підхід до автоматизації інформаційно-аналітичних процесів безпекового супроводу реалізації національних інтересів* / В.Ю.Богданович, А.Л.Висідалко // Київ: ДУТ: Сучасний захист інформації, № 3, 2014, с.4-10

система організації протидії ЗТХ повинна бути налаштована на мінімальний час реагування.

По-друге, мінімізація часу реагування системою повинна досягатися впровадженням багатоканального (паралельного) моніторингу ЗТХ та багатоканального виходу системи. Часткові заходи щодо протидії, які передаються по багатоканальному виходу, визначаються характером, масштабом та іншими характеристиками ЗТХ, що виявлені в ході моніторингу, попередньо обґрунтовуються з використанням розробленого інструментарію інформаційно-аналітичного забезпечення. Для оцінювання результативності цих заходів повинна бути сформована відповідна система показників (індикаторів).

Таким чином, загальне уявлення про процес організації протидії ЗТХ буде визначатися обсягом показників (індикаторів), які найбільшою мірою будуть характеризувати ефективність системи протидії ЗТХ в системі забезпечення національної безпеки держави.

В даний час очевидним є те, що для розвитку ефективної національної антитерористичної системи необхідна консолідація зусиль владних і силових структур, з одного боку, і громадянського суспільства - з іншого. Розвиток та запровадження концепції протидії загрозам терористичного характеру дозволяє застосувати системний підхід до оцінки терористичних ризиків для її елементів, але висуває на передній план проблему оцінки терористичних ризиків і терористичних загроз національній безпеці.

Прогнозні сценарії, які будуються на основі аналізу стану національної безпеки мають передбачати, зокрема, визначення порядку дій у кризових ситуаціях, який би комплексно об'єднував заходи політичного, воєнного, економічного, інформаційного та іншого характеру.

При розробці методологічних підходів до оцінки ризиків терористичних загроз доцільно використовувати зарубіжний і національний досвід, набутий на інших напрямках антитерористичної діяльності.

У процесі реалізації концепції протидії ЗТХ особливу увагу необхідно приділяти організації та забезпеченню дієвості системи превентивних загальнодержавних і правоохоронних заходів. Основною метою таких заходів є виявлення й усунення причин соціальних конфліктів, що визначають виникнення злочинних проявів терористичної спрямованості. Особливе місце в розвитку системи превентивних заходів протидії тероризму приділяється дослідженню його багаторівневої причинно-наслідкової детермінації в контексті реалій часу, науковому прогнозуванню активності тероризму.

У разі свого запровадження, результативність застосування концептуального підходу до протидії ЗТХ, залежатиме від розвитку методологічних інструментів оцінки терористичних ризиків. У свою чергу, на ефективне використання такого інструментарію буде безпосередньо впливати діяльність розвідувальних і правоохоронних органів, а також спецслужб щодо збору та аналізу інформації та даних про терористичні загрози.

13. ФОРМУВАННЯ ВИМОГ АНТИТЕРОРИСТИЧНОГО ЗАХИСТУ ТИПОВИХ КАТЕГОРІЙ ОБ'ЄКТІВ МОЖЛИВИХ ТЕРОРИСТИЧНИХ ПОСЯГАНЬ

Відповідно до підпункту 3 пункту 2 Положення про єдину державну систему запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків, затвердженого постановою Кабінету Міністрів України від 18 лютого 2016 р. № 92, до об'єктів можливих терористичних посягань належать: 1) об'єкти, щодо яких здійснюється державна охорона; 2) важливі державні об'єкти; 3) об'єкти підвищеної небезпеки; 4) об'єкти єдиної транспортної системи України; 5) особливо важливі об'єкти електроенергетики; 6) закордонні дипломатичні установи, консульські та інші представництва іноземних держав на території України; 7) установи кримінально-виконавчої системи; 8) місця масового перебування людей⁷⁹. Для формування визначальних вимог до антитерористичного захисту (АТЗ) вказаних категорій об'єктів необхідно розглянути кожену групу об'єктів докладніше.

Статтею 9 Закону України "Про державну охорону органів державної влади України та посадових осіб" визначено, що державна охорона здійснюється щодо будинків, де працюють Верховна Рада України, Президент України, Кабінет Міністрів України, Конституційний Суд України, Верховний Суд України, споруд і спеціальних транспортних засобів, що перебувають в їх користуванні, інших місць постійного і тимчасового перебування осіб, які охороняються відповідно до цього Закону, важливих державних об'єктів та прилеглих до них територій і акваторій,

⁷⁹ Про затвердження Положення про єдину державну систему запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків : постанова Кабінету Міністрів України від 18.02.2016 р. № 92 [Електронний ресурс]. — Режим доступу : <http://zakon3.rada.gov.ua/laws/show/92-2016-n>.

визначених Президентом України⁸⁰. Указом Президента України від 13 січня 2006 року № 3/2006 до важливих державних об'єктів, охорона яких покладена на Управління державної охорони України, віднесені: державні резиденції на території будинку відпочинку "Пуца-Водиця", державні резиденції та прилеглі до них території по вул. Грушевського, 5а та 24/2, вул. Липській, 4; території і будинки державної резиденції "Залісся"; будівлі по вул. Банковій, 10 та 11а, вул. Шовковичній, 12 та 14, вул. Каменєва, 8; територія будинку відпочинку "Конча-Заспа" та розташовані на ній державні дачі⁸¹.

Одночасно, чинним законодавством України (постанова Кабінету Міністрів України від 19 червня 2013 р. № 421) передбачено визначення Переліку окремих особливо важливих об'єктів права державної власності, охорона яких здійснюється виключно державними підприємствами та організаціями⁸². Включення об'єктів до зазначеного переліку здійснюється відповідно до критеріїв, затверджених Наказом МВС України від 01.09.2015 № 1053⁸³. Постановою Кабінету Міністрів України від 10 серпня 1993 р. № 615 визначено Перелік об'єктів, що підлягають обов'язковій охороні підрозділами Державної служби охорони при Міністерстві внутрішніх справ за договорами⁸⁴.

⁸⁰ Про державну охорону органів державної влади України та посадових осіб : закон України від 4.03.1998 р. № 160/98-ВР [Електронний ресурс]. — Режим доступу : <http://zakon5.rada.gov.ua/laws/show/160/98-вр>.

⁸¹ Про державну охорону важливих державних об'єктів : указ Президента України від 13.01.2006 року № 3/2006 [Електронний ресурс]. — Режим доступу : <http://zakon5.rada.gov.ua/laws/show/3/2006>.

⁸² Про затвердження Порядку визначення переліку окремих особливо важливих об'єктів права державної власності, охорона яких здійснюється виключно державними підприємствами та організаціями : постанова Кабінету Міністрів України від 19.06.2013 р. № 421 [Електронний ресурс]. — Режим доступу : <http://zakon2.rada.gov.ua/laws/show/421-2013-п>.

⁸³ Про затвердження Критеріїв, відповідно до яких об'єкти включаються до переліку окремих особливо важливих об'єктів права державної власності, охорона яких здійснюється виключно державними підприємствами та організаціями на підставі договорів про надання охоронних послуг : наказ Міністерства внутрішніх справ України від 01.09.2015 р. № 1053 [Електронний ресурс]. — Режим доступу : <http://zakon0.rada.gov.ua/laws/show/z1124-15>.

⁸⁴ Про заходи щодо вдосконалення охорони об'єктів державної та інших форм власності :

Об'єктом підвищеної небезпеки, згідно з Законом України "Про об'єкти підвищеної небезпеки", є об'єкт, на якому використовуються, виготовляються, переробляються, зберігаються або транспортуються одна або кілька небезпечних речовин чи категорій речовин у кількості, що дорівнює або перевищує нормативно-встановлені порогові маси, а також інші об'єкти як такі, що відповідно до закону є реальною загрозою виникнення надзвичайної ситуації техногенного та природного характеру⁸⁵. Нормативи порогових мас небезпечних речовин для ідентифікації об'єктів підвищеної небезпеки, порядок їх ідентифікації та обліку затверджено постановою Кабінету Міністрів України від 11 липня 2002 р. N 956 ⁸⁶. Державний реєстр об'єктів підвищеної небезпеки веде Державна служба України з питань праці.

Єдину транспортну систему України становлять: транспорт загального користування (залізничний, морський, річковий, автомобільний і авіаційний, а також міський електротранспорт, у тому числі метрополітен); промисловий залізничний транспорт; відомчий транспорт; трубопровідний транспорт; шляхи сполучення загального користування (ст. 21 Закону України "Про транспорт") ⁸⁷.

Згідно з Законом України "Про електроенергетику", до особливо важливих об'єктів електроенергетики відносяться об'єкти, які забезпечують стаке функціонування об'єднаної енергетичної системи України, руйнація або пошкодження яких призведе до порушення електропостачання господарюючих суб'єктів і населення, можливих людських жертв і значних

постанова Кабінету Міністрів України від 10.08.1993 р. № 615 [Електронний ресурс]. — Режим доступу : <http://zakon3.rada.gov.ua/laws/show/615-93-n>.

⁸⁵ *Про об'єкти підвищеної небезпеки : закон України [Електронний ресурс]. — Режим доступу : <http://zakon2.rada.gov.ua/laws/show/2245-14>*

⁸⁶ *Про ідентифікацію та декларування безпеки об'єктів підвищеної небезпеки : постанова Кабінету Міністрів України від 11.07.2002 р. № 956 [Електронний ресурс]. — Режим доступу : <http://zakon5.rada.gov.ua/laws/show/956-2002-n>.*

⁸⁷ *Про транспорт : закон України від 10.11.1994 р. № 232/94-ВР [Електронний ресурс]. — Режим доступу : <http://zakon5.rada.gov.ua/laws/show/956-2002-n>.*

матеріальних збитків⁸⁸. Постановою Кабінету Міністрів України від 28 липня 2003 р. № 1170 затверджено Перелік особливо важливих об'єктів електроенергетики, які підлягають охороні відомчою воєнізованою охороною у взаємодії із спеціалізованими підрозділами інших центральних органів виконавчої влади, до якого входять: об'єкти державного підприємства НЕК "Укренерго", теплоелектростанції, гідроелектростанції, теплоелектроцентралі та 4 атомні електростанції (Запорізька, Рівненська, Хмельницька, Южно-Українська)⁸⁹. Ядерні установки, ядерні матеріали і радіоактивні відходи, інші джерела іонізуючого випромінювання підлягають охороні Національною гвардією України.

Також, постановою Кабінету Міністрів України від 4 березня 2015 р. № 83 затверджено Перелік об'єктів державної власності, що мають стратегічне значення для економіки і безпеки держави⁹⁰.

Правовий статус закордонних дипломатичних установ, консульських та інших представництв іноземних держав на території України визначено Положенням про дипломатичні представництва та консульські установи іноземних держав в Україні, затвердженим Указом Президента України від 10 червня 1993 року № 198/93⁹¹. Відповідно до Положення про організацію та несення служби з охорони дипломатичних представництв, консульських установ іноземних держав, представництв міжнародних організацій в Україні

⁸⁸ Про електроенергетику : закон України від 16.10.1997 р. № 575/97-ВР [Електронний ресурс]. — Режим доступу : <http://zakon5.rada.gov.ua/laws/show/575/97-vp/print1454001134311413>.

⁸⁹ Про затвердження переліку особливо важливих об'єктів електроенергетики, які підлягають охороні відомчою воєнізованою охороною у взаємодії із спеціалізованими підрозділами інших центральних органів виконавчої влади : постанова Кабінету Міністрів України від 28.07.2003 р. № 1170 [Електронний ресурс]. — Режим доступу : <http://zakon3.rada.gov.ua/laws/show/1170-2003-n>.

⁹⁰ Про затвердження переліку об'єктів державної власності, що мають стратегічне значення для економіки і безпеки держави : постанова Кабінету Міністрів України від 4.03.2015 р. № 83 [Електронний ресурс]. — Режим доступу : <http://zakon5.rada.gov.ua/laws/show/83-2015-n>.

⁹¹ Про Положення про дипломатичні представництва та консульські установи іноземних держав в Україні : указ Президента України 10.06.1993 р. № 198/93 [Електронний ресурс]. — Режим доступу : <http://zakon2.rada.gov.ua/laws/show/198/93>.

військовими частинами і підрозділами Національної гвардії України, затвердженого наказом МВС України від 02.02.2016 № 74, виконання завдань з припинення терористичних актів щодо дипломатичних представництв покладено на відповідні військові частини і підрозділи з охорони дипломатичних представництв, консульських установ іноземних держав, представництв міжнародних організацій в Україні Національної гвардії України⁹².

Відповідно до підпунктів 2-6 ст. 11 Кримінально-виконавчого кодексу України, установами виконання покарань є: арештні доми, кримінально-виконавчі установи, спеціальні виховні установи (далі - виховні колонії), слідчі ізолятори у випадках, передбачених цим Кодексом⁹³. Кримінально-виконавчі установи поділяються на кримінально-виконавчі установи відкритого типу (далі - виправні центри) і кримінально-виконавчі установи закритого типу (далі - виправні колонії). Виправні колонії поділяються на колонії мінімального, середнього і максимального рівнів безпеки. Виправні колонії мінімального рівня безпеки поділяються на колонії мінімального рівня безпеки з полегшеними умовами тримання і колонії мінімального рівня безпеки із загальними умовами тримання. У виправних колоніях середнього рівня безпеки можуть створюватися сектори максимального рівня безпеки для відбування покарання чоловіками, засудженими до довічного позбавлення волі. У виправних колоніях мінімального рівня безпеки із загальними умовами тримання можуть створюватися сектори середнього рівня безпеки для відбування покарання жінками, засудженими до довічного позбавлення волі.

⁹² Про затвердження Положення про організацію та несення служби з охорони дипломатичних представництв, консульських установ іноземних держав, представництв міжнародних організацій в Україні військовими частинами і підрозділами Національної гвардії України : наказ Міністерства внутрішніх справ України від 02.02.2016 № 74 [Електронний ресурс]. — Режим доступу : <http://zakon3.rada.gov.ua/laws/show/z0320-16>.

⁹³ Кримінально-виконавчий кодекс України від 11.07.2003 р. № 1129-IV [Електронний ресурс]. — Режим доступу : <http://zakon2.rada.gov.ua/laws/show/1129-15/print1478000737269448>.

Поняття місця масового перебування людей чинними законодавчими актами України чітко не визначене. За офіційною заявою прес-служби Державної служби України з надзвичайних ситуацій від 07.02.2013, до об'єктів з масовим перебуванням людей відносяться об'єкти з постійним або тимчасовим перебуванням у них від 50 та більше осіб⁹⁴. Згідно з Інструкцією щодо вимог пожежної безпеки під час проектування автозаправних станцій, затвердженої наказом Міністерства України з питань надзвичайних ситуацій та у справах захисту населення від наслідків Чорнобильської катастрофи від 06.12.2005 № 376, місцями масового перебування людей є місця з одночасним перебуванням 100 людей і більше (зупинки громадського транспорту, ринки, майданчики для ігор дітей, занять фізкультурою тощо)⁹⁵.

Для формування вимог до АТЗ типових категорій об'єктів терористичних посягань (ОТП) різних форм власності та відомчої належності необхідно провести їх категорювання. Метою категорювання є формування комплексу диференційованих вимог до систем АТЗ. Виконання зазначених вимог повинно забезпечувати мінімально необхідні та достатні рівні безпеки об'єктів відповідно до їх категорій значущості (важливості) і небезпеки.

Категорії значущості (важливості) і небезпеки об'єктів формуються з урахуванням оцінки можливих збитків інтересам особистості, суспільства і держави при реалізації щодо об'єктів терористичних діянь, у тому числі шляхом перешкоджання (порушення) їх нормального функціонування⁹⁶. Без розроблення типових переліків вимог до АТЗ кожної категорії об'єктів

⁹⁴ *Забезпечення пожежної та техногенної безпеки місць з масовим перебуванням людей під особливою увагою Уряду [Електронний ресурс]. — Режим доступу : http://www.kmi.gov.ua/control/publish/article?art_id=246039168.*

⁹⁵ *Про затвердження Інструкції щодо пожежної безпеки під час проектування автозаправних станцій : наказ Міністерства України з питань надзвичайних ситуацій та у справах захисту населення від наслідків Чорнобильської катастрофи від 06.12.2005 № 376 [Електронний ресурс]. — Режим доступу : <http://zakon5.rada.gov.ua/laws/show/z0291-06>.*

⁹⁶ *Технические средства обнаружения проникновения и угроз различных видов. Особенности выбора, эксплуатации и применения в зависимости от степени важности и опасности объектов. Рекомендации (Р 78.36.028-2012). — М. : НИЦ "Охрана", 2012. — 359 с.*

процедура категорювання об'єктів буде носити формальний характер та не матиме ніякого практичного значення.

Виходячи з визначення терористичного ризику як функції терористичної загрози, уразливості об'єкта та наслідків терористичних атак, категорювання ОТП може бути поетапно здійснено за наступними критеріями: 1) за рівнем терористичної загрози; 2) за рівнем уразливості об'єкта до терористичних загроз; 3) за рівнем суспільно-небезпечних наслідків. Кінцевою метою категорювання за цими критеріями має стати визначення категорії об'єкта за рівнем терористичного ризику.

Ймовірно-статистичні методи розрахунку терористичних ризиків мають деякі недоліки та створюють суттєву невизначеність в оцінку ризику, найбільший внесок в яку дає етап оцінки терористичної загрози. Якщо для оцінки наслідків терористичних актів можуть бути використані вже розроблені моделі та розрахунки для природних та техногенних надзвичайних ситуацій, то для оцінки загроз це зробити неможливо, адже вона базується на інформації про цілі, мотиви та можливості терористів. І якщо можливості та тактика дій терористів ще можуть бути більш-менш адекватно передбачені, то оцінити ОТП, який стане ціллю, можна дуже приблизно⁹⁷.

На думку автора, статистичні методи для розрахунку терористичних ризиків є не зовсім придатними, оскільки для них необхідний великий обсяг статистичної інформації, яку не завжди можна отримати в контексті скоєння терористичних актів стосовно конкретного ОТП. Зокрема, обсяг спостережень повинен перевищувати деяку величину N_1 , яка залежить від ймовірності, що оцінюється, при цьому число реалізованих негативних подій за один рік повинно бути більше 100^{98} . До того ж, як відзначають Г. Г. Браун

⁹⁷ *Estimating terrorism risk [Електронний ресурс]. — Режим доступу : https://docviewer.yandex.ua/?url=http%3A%2F%2Fwww.rand.org%2Fcontent%2Fdam%2Frand%2Fpubs%2Fmonographs%2F2005%2FRAND_MG388.pdf&name=RAND_MG388.pdf&lang=en&c=5843ffec4f1f.*

⁹⁸ *Вишняков Я.Д., Радаев Н. Н. Общая теория рисков : учеб. пособие для студ. высш. учеб.*

та Л. А. Кокс, традиційний ймовірнісний аналіз ризиків (probabilistic risk assessment), призначений для розрахунку ризиків природних та інженерних систем, містить суттєві відмінності від аналізу терористичних ризиків. Основні з них полягають в тому, що терористи можуть бути обізнані про посилення антитерористичних заходів правоохоронними органами і проводити власні дослідження ризиків перед проведенням атак. У той же час, правоохоронці оцінюють терористичні загрози виходячи з інформації, відомої про терористів. При цьому, правоохоронним органам достеменно не відомо про обсяг інформації, яку терористи можуть знати про особливості функціонування систем антитерористичного захисту і яка може вплинути на прийняття ними рішень стосовно майбутніх атак. Такі застереження не можуть бути застосовані для інженерних систем та стихійних лих⁹⁹.

Ураховуючи викладене, для розрахунку терористичних ризиків більш придатними вважаються евристичні методи, до яких належить метод експертного оцінювання, що заснований на використанні суб'єктивних ймовірностей, отриманих під час експертного оцінювання, та дозволяє провести якісно-кількісне ранжування ризиків. Сутність експертного методу оцінки показників ризику полягає в тому, що експертам пропонують відповісти на питання про стан або майбутню поведінку об'єктів, що характеризуються невизначеними параметрами або недослідженими властивостями. Експертні оцінки оформляють, зокрема, у вигляді якісних характеристик або кількісних значень ймовірностей подій, що розглядаються, віднесених до певного відрізка часу. Важливе значення при цьому надають формуванню оціночної шкали, яка використовується експертами. Оптимальна оціночна шкала повинна мати порівняно невелике число градацій (від 3 до 8); кожній градації приписують певний ймовірнісний

заведений / Я. Д. Вишняков, Н. Н. Радаев. — 2-е изд., испр. — М. : Издательский центр "Академия", 2008. — 368 с.

⁹⁹ Brown G. G., Cox L. A. *How Probabilistic Risk Assessment Can Mislead Terrorism Risk Analysts [Electronic resource]* / G. G. Brown, L. A. Cox // *Risk Analysis*. — 2011. — Vol. 31. — № 2. — P. 196 — 204. — Mode of access : <http://onlinelibrary.wiley.com/doi/10.1111/j.1539-6924.2010.01492.x/full>.

інтервал. Крім того, кожна градація повинна супроводжуватися короткою текстовою якісною характеристикою. Для інтерпретації та математичної обробки експертних даних можна залучати математичні моделі. Підвищення достовірності експертних оцінок вимагає відповідних процедур відбору експертів за багатьма критеріями і кількісних методів обробки їх думок. За умов правильної організації процедури експертизи та перевірки узгодженості думок експертів забезпечується достатня достовірність оцінок.

Для обробки суджень експертів під час розрахунку терористичного ризику будемо використовувати метод аналітичних мереж (МММ) та його спрощений варіант – метод аналізу ієрархій (МАІ), запропоновані американським математиком Томасом Сааті на початку 70-х років ХХ століття, які використовуються в процесі експертного оцінювання¹⁰⁰. Зауважимо, що МММ та МАІ допомагають структурувати проблему (у тому числі ту, що погано формалізується), побудувати набір альтернатив, виділити фактори, які характеризують ці альтернативи, задати значимість самих факторів, оцінити альтернативи по кожному з факторів, знайти неточності і суперечності в судженнях експертів, проранжувати альтернативи, провести аналіз рішення та обґрунтувати отримані результати¹⁰¹. Методи засновані на декомпозиції задачі і представлення її у вигляді аналітичних мереж (ієрархічних структур), що дозволяє використати всі наявні у експертів, які залучаються до дослідження, знання з розв'язуваної проблеми і подальшій обробці їх суджень. У результаті може бути виявлена відносна ступінь взаємодії елементів в ієрархії, які потім виражаються чисельно. МММ (МАІ) включають процедури синтезу множинних суджень, отримання пріоритетності критеріїв і знаходження альтернативних рішень.

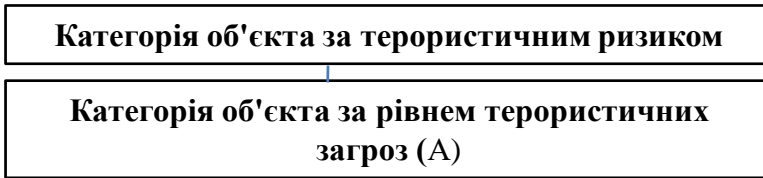
¹⁰⁰ Саати Т. Л. *Принятие решений при зависимостях и обратных связях [Текст] : аналитические сети / Т. Л. Саати ; пер. с англ. О. Н. Андрейчикова ; науч. ред. А. В. Андрейчиков, О. Н. Андрейчикова. — М. : ЛКИ, 2008. — 357 с.*

¹⁰¹ Бочков А. В. *Использование метода анализа иерархий для целей категорирования критически важных объектов по степени совокупного ущерба и риску противоправных действий / А. В. Бочков // Проблемы анализа риска. — 2008. — Том № 5. — № 4 — С. 23 — 27.*

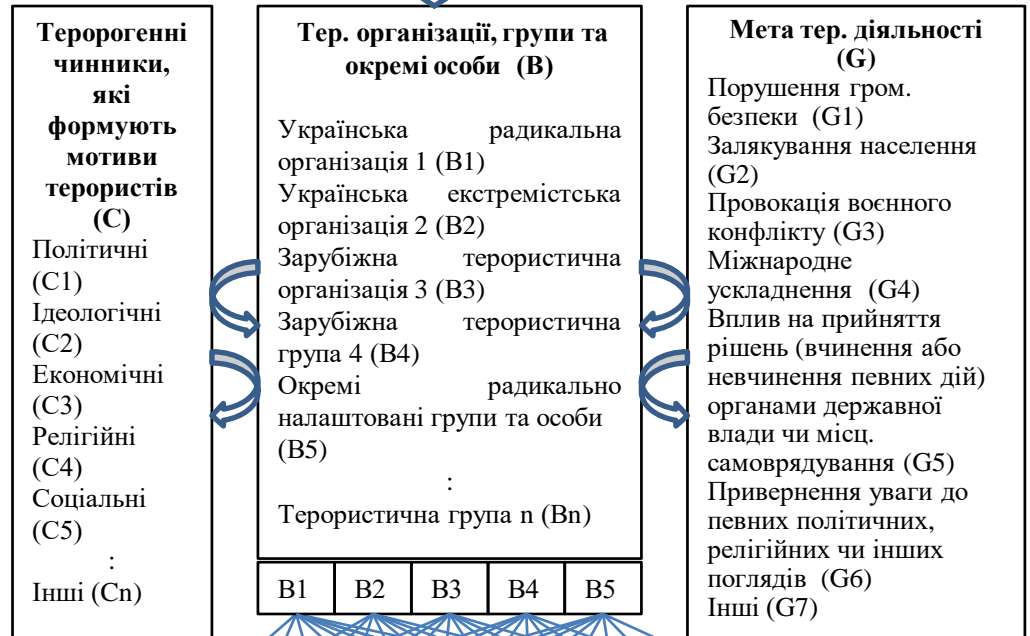
На першому етапі застосування МАМ (MAI) проводиться структурування проблеми вибору у вигляді ієрархії або мережі. У найбільш загальному вигляді ієрархія будується з вершини (мети), через проміжні рівні - критерії (параметри) до самого нижнього рівню, який, як правило, є набором альтернатив. Логіка вказаного алгоритму дозволяє формулювати питання до експертів, які нададуть можливість визначити категорію об'єктів, зокрема: від кого необхідно захищати об'єкт, яка ймовірність нападу на нього, які види протиправних дій він може вчиняти, яка уразливість об'єкта щодо кожного виду нападу, які суспільно небезпечні наслідки можуть виникнути внаслідок кожного виду нападу, до якої категорії за рівнем терористичного ризику необхідно віднести об'єкт. Ієрархічні рівні задачі категорювання ОТП зображені на мал. 1.

Кінцева мета

Визначити
тер. загрозу
(Рівень А)

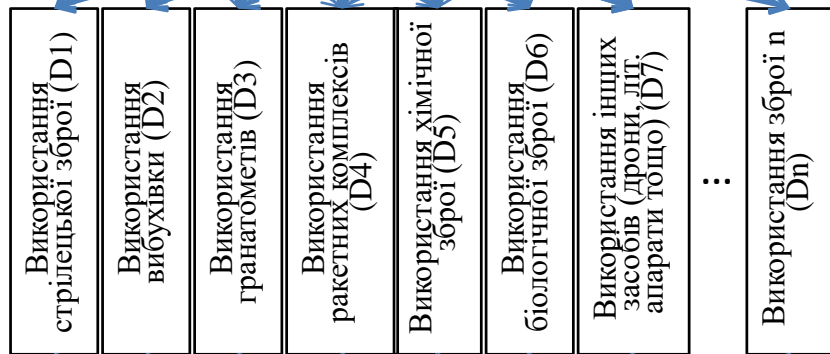


(Рівні В, С та G)

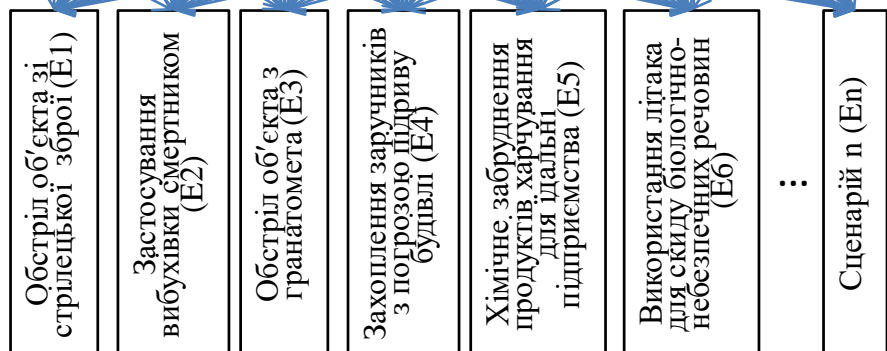


Модель загроз

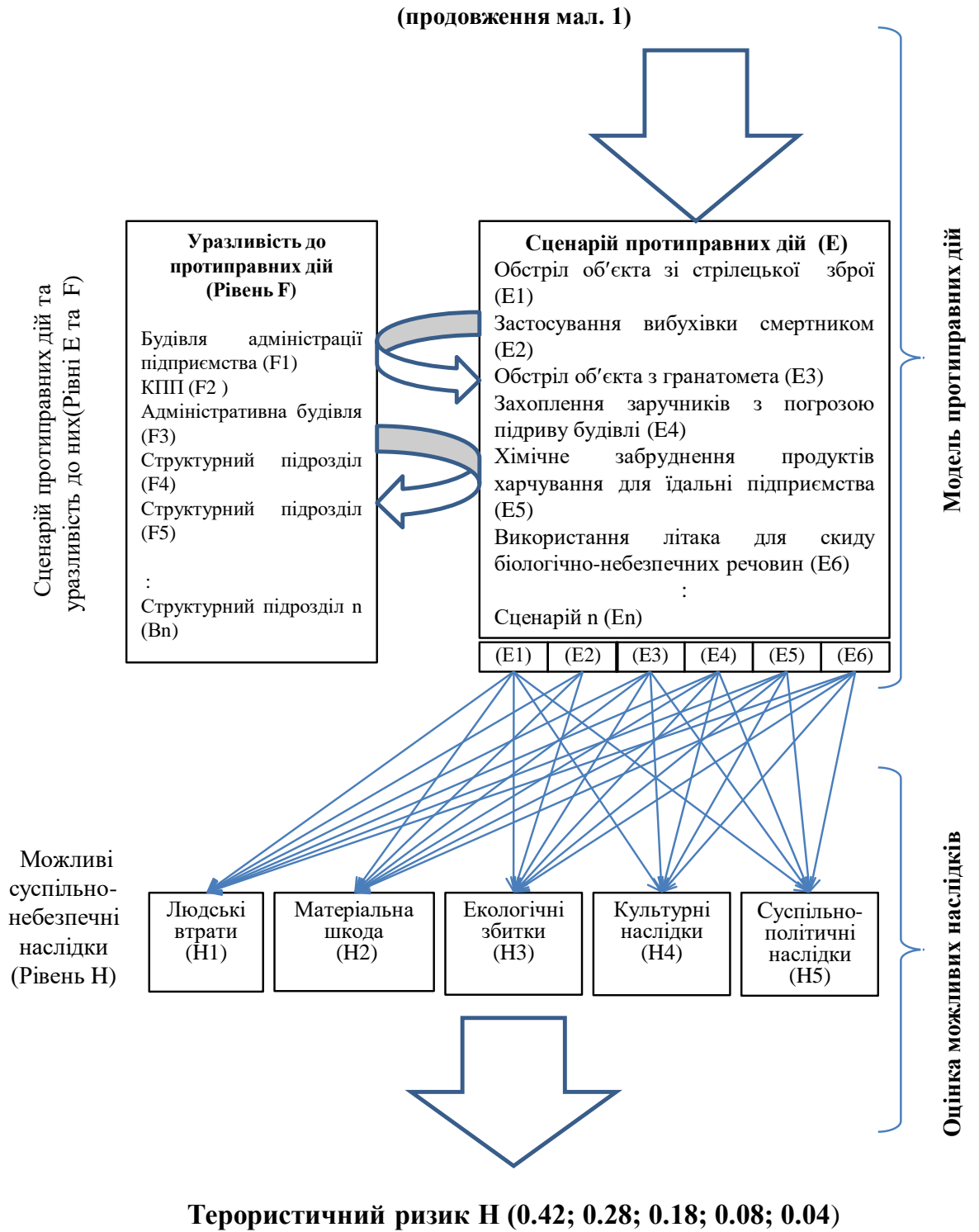
Засоби ураження та форми прогипправної діяльності, які найбільш ймовірно можуть бути використані терористами для атак (Рівень D)



Сценарій прогипправних дій (Рівень E)



Модель прогипправних дій



Мал. 1. Структурна схема категорювання об'єкта за рівнем терористичного ризику методами МАМ та МАІ

Завдання експертів на кожному рівні ієрархії провести попарні порівняння елементів ієрархії за критерієм, встановленим на більш вищому рівні ієрархії. Шкала, яка використовується експертами для оцінок, наведена в таблиці 1.

Таблиця 1. Зміст експертних оцінок в МАІ

Шкала інтенсивності	Якісні судження
1	рівна важливість
3	помірна перевага одного над іншим
5	суттєва перевага одного над іншим
7	значна перевага одного над іншим
9	найбільша перевага одного над іншим
2, 4, 6, 8	відповідні проміжні значення
1/2, 1/3, 1/4 ... 1/9	зворотні значення для наведених вище чисел

Так, для рівня В(терористичні організації, групи та окремі особи) матриця парних порівнянь за критерієм рівня А (терористичні загрози) може мати вигляд зворотно симетричної матриці:

A	B1	B2	B3	B4	B5
B1	1.00000	3.00000	6.00000	9.00000	7.00000
B2	0.33333	1.00000	3.00000	7.00000	5.00000
B3	0.16667	0.33333	1.00000	4.00000	3.00000
B4	0.11111	0.14286	0.25000	1.00000	3.00000
B5	0.14286	0.20000	0.33333	0.33333	1.00000

Запис в другому стовпчику першої стрічки матриці 3 означає, що елемент B1 має помірну перевагу в ймовірності загрози щодо ОТП у порівнянні з B2, запис в третьому стовпчику першої стрічки 6 означає, що B1 має суттєву перевагу над B3 і т. ін. При порівнянні елементів між собою (перший стовпчик першої стрічки) маємо 1 (діагональні елементи цієї

матриці завжди будуть дорівнювати 1). Оскільки ця матриця є зворотно симетричною, зважаючи на її властивості, якщо при порівнянні одного фактора i з іншим j отримано $b_{ij} = c$, то при порівнянні другого фактора з першим автоматично отримуємо $b_{ji} = 1/c$.

Для визначення відносної цінності кожного елемента необхідно знайти геометричне середнє кожної строки для чого перемножити елементів b_{ij} кожної строки ($i = 1, 2, 3, \dots, n$) і з отриманого результату знайти корінь n -го ступеня. Отримані числа необхідно нормалізувати. Формула для винайдення середнього геометричного має вигляд:

$$Q_i = \sqrt[n]{b_{i1} b_{i2} b_{i3} \dots b_{in}} \quad (1)$$

Для нашої матриці розмірність $n=5$. Знайдемо добуток елементів, що знаходяться в кожній стрічці. Для першої строки $\omega_1 = \sqrt[5]{1 \cdot 3 \cdot 6 \cdot 9 \cdot 7} = 4.082$, для другої $\omega_2 = \sqrt[5]{1/1 \cdot 1/3 \cdot 1/6 \cdot 1/9 \cdot 1/7} = 2.036$, для третьої $\omega_3 = 0.922$, $\omega_4 = 0.412$, $\omega_5 = 0.316$.

Далі проводимо нормалізацію отриманих чисел, для чого вираховуємо нормуючий множник за формулою $q = \omega_1 + \omega_2 + \omega_3 + \dots + \omega_n$ (2), кожне ω_i ділимо на q та отримуємо вектор пріоритетів $B = (\omega_1/q; \omega_2/q; \omega_3/q; \dots; \omega_n/q)$ або $B = (q_{b1}; q_{b2}; q_{b3}; \dots; q_{bn})$.

Для нашого приклада $q = 7.769$, а вектор пріоритетів має значення B (0.52545; 0.26207; 0.11868; 0.05306; 0.04073). Зазначене свідчить, що українська радикальна організація 1(B1) має більшу ймовірність загрози по відношенню до нашого об'єкта у порівнянні з іншими терористичними організаціями, групами та особами. Доповнюємо нашу матрицю стовпчиком значень ω_i та вектором пріоритетів $B = (q_{b1}; q_{b2}; q_{b3}; \dots; q_{bn})$

A	B1	B2	B3	B4	B5	ω		$q(b)$
B1	1.00000	3.00000	6.00000	9.00000	7.00000	4.08247	$q_{b1} =$	0.52545
B2	0.33333	1.00000	3.00000	7.00000	5.00000	2.03617	$q_{b2} =$	0.26207
B3	0.16667	0.33333	1.00000	4.00000	3.00000	0.92211	$q_{b3} =$	0.11868
B4	0.11111	0.14286	0.25000	1.00000	3.00000	0.41223	$q_{b4} =$	0.05306
B5	0.14286	0.20000	0.33333	0.33333	1.00000	0.31647	$q_{b5} =$	0.04073

Для підвищення достовірності суджень експертів в оцінці ймовірностей атак з боку конкретної терористичної організації, групи чи особи по відношенню до ОТП доцільно використати метод "чек-листів" (checklist method) зі зваженими коефіцієнтами. Чек-лист уявляє собою список контрольних пунктів, виконання яких необхідне для успішного завершення всього обсягу роботи або процедури¹⁰². Для нашої задачі чек-лист повинен включати список питань (критеріїв), які експерт має прийняти до уваги для оцінки та подальшого порівняння ймовірностей терористичних загроз. До цього списку, зокрема, доцільно включити питання, які можуть свідчити на як на користь збільшення ймовірності терористичної діяльності, так і у напрямку її зменшення. З урахуванням часткового запозичення досвіду Департаменту оборони США в оцінці терористичних загроз¹⁰³, чек-лист може містити наступні питання:

з/п	Контрольне питання (критерій оцінки)	Оцінк а збільшення ймовірності загрози (+)	Оцінк а зменшення ймовірності загрози (-)
	Кількість здійснених (спроб здійснення) тер. актів за останні 3-4 роки з боку цієї організації (групи, особи) стосовно ОТП такого типу в даному регіоні/в країні в цілому		
	Можлива наявність оперативних		

¹⁰² Checklist method [Electronic resource]. — Mode of access : <https://www.slideshare.net/mobile/bibinssb/checklist-method>.

¹⁰³ DoD Antiterrorism handbook [Electronic resource]. — Mode of access : https://docviewer.yandex.ua/?url=http%3A%2F%2Fdownload.cabledrum.net%2Fwikileaks_archive%2Ffile%2Fus-dod-anti-terrorism-handbook-2004.pdf&name=us-dod-anti-terrorism-handbook-2004.pdf&lang=en&c=588f8d80b6d1

	даних про спрямування з боку цього суб'єкта тероризму до ОТП такого типу		
	Загальна оцінка рівня терористичної загрози для регіону, визначена Штабом АТЦ при СБУ		
	Кількість припинених правоохоронними органами замахів на скоєння тер. актів/розпочатих кримінальних проваджень/затриманих осіб		
	Доступність та привабливість ОТП для скоєння тер. акту		
	Наявність інформації про обізнаність терористів про особливості системи антитерористичного (фізичного) захисту ОТП		
	Це тільки початок, я цей перелік суттєво доповню		
	Сума зважених коефіцієнтів	Сума 1	Сума 2
	Різниця	$X_i = (\text{Сума 1}) - (\text{Сума 2})$	

Зазначений перелік не є вичерпним та може доповнюватися. Для оцінки збільшення/зменшення ймовірності терористичної загрози доцільно використовувати зважені коефіцієнти (наприклад, за шкалою від 0 до 1 або від 1 до 5). Вказані коефіцієнти будуть свідчити про те, наскільки вказане питання (критерій) збільшує або зменшує ймовірність терористичної загрози з боку цієї організації, групи або особи. Після підсумування зважених коефіцієнтів (окремо по колонках "збільшення"/"зменшення") та вирахування їх різниці отримуємо деяке значення X_i , яке буде різним для кожної

організації, групи або особи. Пропорційне співвідношення між X_i є еквівалентним пропорційному співвідношенню ймовірностей терористичних загроз між визначеними на рівні B терористичними організаціями, групами або особами, що можна використовувати при складанні матриці парних порівнянь.

Джерелами інформації для надання відповідей на питання чек-листа можуть бути: 1) джерела інформації з обмеженим доступом (інформація БД ЄСІЗ "Синтез" СБ України, матеріали контррозвідувальних та оперативно-розшукових справ, довідки про оперативну обстановку по лінії боротьби з тероризмом, інформація розвідувальних та інших взаємодіючих правоохоронних органів тощо); 2) відкриті джерела інформації (мережа Інтернет, матеріали ЗМІ, телебачення, офіційні повідомлення державних органів, заяви посадових осіб і т. ін.).

Під час використання МАІ необхідно враховувати, що будь-яка матриця суджень у загальному випадку не узгоджена, так як судження відображають суб'єктивні думки експертів, а порівняння елементів, які мають кількісні еквіваленти, може бути неузгодженим із-за присутності похибки під час оцінювання. Досконалої узгодженості парних порівнянь навіть в ідеальному випадку на практиці досягти важко. Потрібен спосіб оцінки ступеня узгодженості при вирішенні конкретної задачі. МАІ дає можливість провести таку оцінку.

Після заповнення і обчислення матриць парних порівнянь необхідно встановити міру оцінки ступеня відхилення суджень експертів від узгодженості. Коли такі відхилення перевищують встановлені межі, їх необхідно переглянути. З цією метою потрібно визначити індекс узгодженості (ІУ) та відношення узгодженості.

Для обчислення ІУ вираховується сума кожного j -го стовпця матриці суджень

$$s_j = b_{1j} + b_{2j} + b_{3j} \dots + b_{nj}, \text{ де } j = 1, 2, 3, \dots, n \quad (3)$$

Потім отриманий результат множиться на j -ю компоненту нормалізованого вектора пріоритетів q_j , тобто суму суджень першого стовпця на першу компоненту, суму суджень другого стовпчика - на другу і т. д.

$$p_j = s_j * q_j, \text{ де } j = 1, 2, 3, \dots, n \quad (4)$$

Сума чисел p_j відображає пропорційність переваг, чим ближче ця величина до n (кількості об'єктів і видів дії в матриці парних порівнянь), тим більш узгоджені судження

$$\lambda_{\max} = p_1 + p_2 + p_3 + \dots + p_n \quad (5)$$

$$\text{Відхилення від узгодженості виражається } I_U, I_U = (\lambda_{\max} - n) / n - 1 \quad (6)$$

Для визначення того, наскільки точно індекс узгодженості I_U відображає узгодженість суджень, його необхідно порівняти з випадковим індексом узгодженості (VI_U), середні значення якого (в залежності від розміру випадкових матриць) наведені в таблиці 2.

Таблиця 2. Середні значення VI_U для випадкових матриць суджень різного розміру.

Розмір матриці	1	2	3	4	5	6	7	8
Середні значення VI_U	0	0	0.58	0.9	1.12	1.24	1.32	1.41

Відношення I_U до середнього значення VI_U називається відношенням узгодженості (V_U)

$$V_U = I_U / VI_U \quad (7)$$

Допустиме значення V_U , як правило, не повинно перевищувати 0.1 (10%). У деяких випадках допускається значення V_U не більше 0.2 (20%). Якщо ця вимога не дотримується, необхідно попросити експертів, що приймають участь в опитуванні, додатково перевірити свої судження¹⁰⁴.

¹⁰⁴ Бочков А. В. Использование метода анализа иерархий для целей категорирования критически важных объектов по степени совокупного ущерба и риску противоправных действий / А. В. Бочков // Проблемы анализа риска. — 2008. — Том № 5. — № 4 — С. 23 — 27.

Для нашого прикладу $s_1 = 1.75397$, $p_1 = s_1 * q_1 = 0.92162$; $s_2 = 4.67619$, $p_2 = s_2 * q_2 = 1.22551$; $s_3 = 10.58333$, $p_3 = s_3 * q_3 = 1.25607$; $s_4 = 21.33333$, $p_4 = s_4 * q_4 = 1.13191$; $s_5 = 19$, $p_5 = s_5 * q_5 = 0.77393$. $\lambda_{\max} = p_1 + p_2 + p_3 + p_4 + p_5 = 5.30904$. $IY = (\lambda_{\max} - n) / n - 1 = 0.07726$. $VI = IY / VIY = 0.06898$ (є допустимим оскільки не перевищує 0.1). Узагальнена матриця для рівня В має наступний вигляд:

A	B1	B2	B3	B4	B5	ω		q(b)
B1	1.00000	3.00000	6.00000	9.00000	7.00000	4.08247	qb1=	0.52545
B2	0.33333	1.00000	3.00000	7.00000	5.00000	2.03617	qb2=	0.26207
B3	0.16667	0.33333	1.00000	4.00000	3.00000	0.92211	qb3=	0.11868
B4	0.11111	0.14286	0.25000	1.00000	3.00000	0.41223	qb4=	0.05306
B5	0.14286	0.20000	0.33333	0.33333	1.00000	0.31647	qb5=	0.04073
s	1.75397	4.67619	10.58333	21.33333	19.00000	7.76945		1.00000
	p1=	p2=	p3=	p4=	p5=		$L_{\max} =$	5.30904
	0.92162	1.22551	1.25607	1.13191	0.77393		$L_{\max-n} =$	0.30904
							$IY = (L_{\max-n}) / (n-1) =$	0.07726
							$VIY = IY / VIY =$	0.06898

З урахуванням того, що в експертному опитуванні братиме участь декілька експертів, необхідно забезпечити усереднення їх оцінок.

Далі необхідно скорегувати значення вектору ймовірностей В (0.525; 0.262; 0.119; 0.053; 0.041) з урахуванням впливу на рівень В (терористичні організації, групи та окремі особи) рівня С (теророгенні чинники, які формують мотиви терористів). Будемо вважати цей вплив взаємним (рівні мають зворотні зв'язки), у зв'язку з чим необхідно скласти дві групи матриць: 1) оцінювати терористичні організації, групи та окремі особи за критеріями рівня С (для якої терористичної групи цей теророгенний чинник (мотив) є більш пріоритетним); 2) оцінювати теророгенні чинники, які формують мотиви терористів за критеріями рівня В (який теророгенний чинник (мотив) є найбільш визначальним для розглянутих на рівні В терористичних організацій та груп).

З метою отримання вагових коефіцієнтів для рівня В за критерієм порівняння С необхідно скласти 5 матриць наступного виду:

Щодо Сі	В1	В2	В3	В4	В5
В1	1				
В2		1			
В3			1		
В4				1	
В5					1

За результатами заповнення експертами матриці за критерієм оцінки С1, обчислення векторів пріоритетів, λ_{\max} , ВУ результати можуть мати наступний вигляд:

С1	В1	В2	В3	В4	В5	λ		q(b)
В1	1.000	1.000	2.000	4.000	6.000	2.169	qb1=	0.335
В2	1.000	1.000	2.000	5.000	5.000	2.187	qb2=	0.338
В3	0.500	0.500	1.000	3.000	4.000	1.246	qb3=	0.192
В4	0.250	0.200	0.333	1.000	4.000	0.582	qb4=	0.090
В5	0.167	0.200	0.250	0.250	1.000	0.291	qb5=	0.045
s	2.917	2.900	5.583	13.250	20.000	6.474		1.000
	p1=	p2=	p3=	p4=	p5=		$\lambda_{\max} =$	5.120
	0.977	0.980	1.074	1.191	0.899		$\lambda_{\max-n} =$	0.120
				0.120	4.000		$IY = (\lambda_{\max-n}) / (n-1) =$	0.030
				0.030	1.120		$ВУ = IY / BIY =$	0.027

Аналогічні матриці складаються та обраховуються за критеріями С2....С5.

З метою отримання вагових коефіцієнтів для рівня С за критерієм порівняння В необхідно скласти 5 матриць наступного виду:

Щодо	С1	С2	С3	С4	С5
Ві					
С1	1				

C2		1			
C3			1		
C4				1	
C5					1

Для визначення взаємного впливу рівнів В та G (мета терористичної діяльності) також необхідно скласти дві групи матриць: 1) оцінювати терористичні організації, групи та окремих осіб за критеріями рівня G (для якої терористичної групи ця мета тероризму є пріоритетною); 2) оцінювати мету терористичної діяльності за критеріями рівня В (яка мета є найбільш значущою для визначених на рівні В терористичних організацій та груп).

З метою отримання вагових коефіцієнтів для рівня В за критерієм порівняння G необхідно скласти 7 матриць наступного виду:

Щодо	B1	B2	B3	B4	B5
G i					
B1	1				
B2		1			
B3			1		
B4				1	
B5					1

Для отримання вагових коефіцієнтів для рівня В за критерієм порівняння G необхідно скласти 5 матриць наступного виду:

Щодо	G1	G2	G3	G4	G5	G6	G7
B i							
G1	1						
G1		1					

G1			1				
G1				1			
G1					1		
G1						1	
G1							1

Узагальнені результати можна відобразити у вигляді суперматриці розміром 18×18 . У результаті нормування коефіцієнтів вихідної суперматриці, приведення її до стохастичного вигляду та піднесення в граничні степені (для нашого випадку достатньо вже 10 -ї), матриця стає стабільною і вагові коефіцієнти перестають змінюватись. Піднесення матриці в граничні степені еквівалентно неодноразовому врахуванню взаємозв'язків її елементів. Отримані результати відображені в граничній суперматриці. Як видно, вагові коефіцієнти (ймовірності загроз) для рівня В змінилися і становлять (0.453; 0.271; 0.158; 0.078; 0.040).

Вихідна суперматриця взаємної оцінки рівнів В (терористичні організації, групи та окремі особи), С (теророгенні чинники, які формують мотиви терористів) та G (мега терористичної діяльності)

	B1	B2	B3	B4	B5	C1	C2	C3	C4	C5	G1	G2	G3	G4	G5	G6	G7
	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
B1	0.525	0.000	0.000	0.000	0.000	0.335	0.508	0.438	0.497	0.436	0.468	0.504	0.505	0.523	0.516	0.482	0.470
B2	0.262	0.000	0.000	0.000	0.000	0.338	0.239	0.312	0.257	0.295	0.253	0.255	0.219	0.208	0.219	0.267	0.270
B3	0.119	0.000	0.000	0.000	0.000	0.192	0.141	0.146	0.143	0.153	0.156	0.134	0.159	0.157	0.150	0.143	0.141
B4	0.053	0.000	0.000	0.000	0.000	0.090	0.073	0.067	0.066	0.070	0.080	0.073	0.081	0.073	0.076	0.072	0.072
B5	0.041	0.000	0.000	0.000	0.000	0.045	0.037	0.037	0.037	0.045	0.042	0.034	0.035	0.039	0.039	0.036	0.046
C1	0.440	0.458	0.493	0.486	0.536	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
C2	0.280	0.254	0.225	0.271	0.242	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
C3	0.152	0.166	0.163	0.131	0.114	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
C4	0.085	0.081	0.080	0.073	0.068	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
C5	0.043	0.041	0.040	0.039	0.039	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
G1	0.373	0.366	0.356	0.362	0.352	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
G2	0.240	0.233	0.284	0.241	0.270	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
G3	0.184	0.198	0.171	0.188	0.179	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
G4	0.091	0.089	0.082	0.091	0.091	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
G5	0.055	0.055	0.050	0.054	0.051	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
G6	0.033	0.036	0.035	0.038	0.034	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
G7	0.024	0.024	0.023	0.024	0.023	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000

Начальні значення
вектору В

Гранична суперматриця взаємної оцінки рівнів В (терористичні організації, групи та окремі особи), С (тероритичні чинники, які формують мотиви терористів) та G (мега терористичної діяльності)

	B1	B2	B3	B4	B5	C1	C2	C3	C4	C5	G1	G2	G3	G4	G5	G6	G7
	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
B1	0.453	0.000	0.000	0.000	0.000	0.453	0.000	0.000	0.000	0.000	0.453	0.453	0.453	0.453	0.453	0.453	0.453
B2	0.271	0.000	0.000	0.000	0.000	0.271	0.271	0.000	0.000	0.271	0.271	0.271	0.271	0.271	0.271	0.271	0.271
B3	0.158	0.000	0.000	0.000	0.000	0.158	0.158	0.158	0.000	0.158	0.158	0.158	0.158	0.158	0.158	0.158	0.158
B4	0.078	0.000	0.000	0.000	0.000	0.078	0.078	0.078	0.078	0.078	0.078	0.078	0.078	0.078	0.078	0.078	0.078
B5	0.040	0.000	0.000	0.000	0.000	0.040	0.040	0.040	0.040	0.040	0.040	0.040	0.040	0.040	0.040	0.040	0.040
C1	0.000	0.460	0.460	0.460	0.460	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
C2	0.000	0.262	0.262	0.262	0.262	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
C3	0.000	0.155	0.155	0.155	0.155	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
C4	0.000	0.082	0.082	0.082	0.082	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
C5	0.000	0.041	0.041	0.041	0.041	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
G1	0.000	0.367	0.367	0.367	0.367	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
G2	0.000	0.246	0.246	0.246	0.246	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
G3	0.000	0.186	0.186	0.186	0.186	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
G4	0.000	0.089	0.089	0.089	0.089	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
G5	0.000	0.054	0.054	0.054	0.054	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
G6	0.000	0.034	0.034	0.034	0.034	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
G7	0.000	0.024	0.024	0.024	0.024	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000

Скореговані значення вектору В

Особи, групи та організації уявляють собою терористичну загрозу лише у тому випадку, якщо вони мають намір та відповідні можливості завдати шкоди об'єкту посягань. Ані наміри без наявності можливостей, ані можливості для скоєння терористичного акту без наявності намірів не створюють терористичної загрози. Загроза існує лише тоді, коли наміри та можливості разом притаманні особі, групі або організації¹⁰⁵. У зв'язку з цим, необхідно оцінити потенційні можливості терористів до здійснення атак, виходячи з можливо наявних у них засобів та знарядь для скоєння терористичних злочинів. Для цього вводимо наступний рівень ієрархії (D) - засоби ураження та форми протиправної діяльності (ППД), які найбільш ймовірно можуть бути використані терористами для атак. Задача експертів для цього рівня - здійснити порівняння можливих засобів нападу та пов'язаних з ними форм ППД для кожної з терористичної груп та організацій, з урахуванням специфіки нашого об'єкту (типового об'єкту з групи однорідних об'єктів).

З метою отримання вагових коефіцієнтів для рівня D за критерієм порівняння B1.....B5 необхідно скласти 5 матриць наступного виду:

Щодо Ві	D1	D2	D3	D4	D5	D6	D7
D1	1						
D2		1					
D3			1				
D4				1			
D5					1		
D6						1	

¹⁰⁵ *Estimating terrorism risk [Електронний ресурс]. — Режим доступу : https://docviewer.yandex.ua/?url=http%3A%2F%2Fwww.rand.org%2Fcontent%2Fdam%2Frand%2Fpubs%2Fmonographs%2F2005%2FRAND_MG388.pdf&name=RAND_MG388.pdf&lang=en&c=5843ffec4f1f.*

D7							1
----	--	--	--	--	--	--	---

За результатами заповнення матриць експертами, обчислення векторів пріоритетів, λ_{max} , ВУ результати можна відобразити у вигляді матриці, стовпцями якої будуть вектори пріоритетів (qd1; qd2; qd3;.....qd7) для кожного критерію В1...В5.

qd(для В1)	qd(для В2)	qd(для В3)	qd(для В4)	qd(для В5)
0.354	0.388	0.390	0.375	0.331
0.256	0.233	0.244	0.249	0.183
0.186	0.182	0.165	0.180	0.275
0.092	0.087	0.090	0.086	0.097
0.056	0.053	0.054	0.052	0.057
0.033	0.033	0.032	0.033	0.034
0.024	0.023	0.025	0.025	0.023

Для визначення узагальнених пріоритетів засобів ураження та форм ППД терористів (з урахуванням скорегованих раніше значень ймовірностей реалізації терористичних загроз з боку визначених організацій, груп та окремих осіб на рівні В) необхідно перемножити цю матрицю на вектор В. У результаті получимо вектор пріоритетів (ймовірностей) D. Для нашого прикладу ця операція матиме вигляд:

$$D=q(d)*B= \begin{array}{c} \text{qd(для} \\ \text{В1)} \\ \text{qd(для} \\ \text{В2)} \\ \text{qd(для} \\ \text{В3)} \\ \text{qd(для} \\ \text{В4)} \\ \text{qd(для} \\ \text{В5)} \end{array} \begin{array}{c} \left| \begin{array}{c} 0.354 \\ 0.256 \\ 0.186 \\ 0.092 \\ 0.056 \\ 0.033 \\ 0.024 \end{array} \right. \\ \left| \begin{array}{c} 0.388 \\ 0.233 \\ 0.182 \\ 0.087 \\ 0.053 \\ 0.033 \\ 0.023 \end{array} \right. \\ \left| \begin{array}{c} 0.390 \\ 0.244 \\ 0.165 \\ 0.090 \\ 0.054 \\ 0.032 \\ 0.025 \end{array} \right. \\ \left| \begin{array}{c} 0.375 \\ 0.249 \\ 0.180 \\ 0.086 \\ 0.052 \\ 0.033 \\ 0.025 \end{array} \right. \\ \left| \begin{array}{c} 0.331 \\ 0.183 \\ 0.275 \\ 0.097 \\ 0.057 \\ 0.034 \\ 0.023 \end{array} \right. \end{array} \times \begin{array}{c} \left| \begin{array}{c} \text{В} \\ 0.453 \\ 0.271 \\ 0.158 \\ 0.078 \\ 0.040 \end{array} \right. \\ \left| \begin{array}{c} \text{D} \\ 0.370 \\ 0.244 \\ 0.185 \\ 0.090 \\ 0.055 \\ 0.033 \\ 0.024 \end{array} \right. \end{array} =$$

Наступний етап ієрархії – встановлення пріоритетів можливих сценаріїв ППД та порівняння їх за критеріями більш вищого рівня (рівень D - засоби ураження та форми ППД, які найбільш ймовірно можуть бути

використанні терористами для атак). Для цього вводиться рівень E - сценарій ППД, для якого експертами розробляються конкретні сценарії нападу на об'єкт. Як приклад, сценарій E1 - обстріл об'єкта зі стрілецької зброї, E2 - застосування вибухівки смертником, E3 - обстріл об'єкта з гранатомета, E4 - захоплення заручників з погрозою підриву будівлі, E5 - хімічне забруднення продуктів харчування для їдальні підприємства, E6 - використання літака для скиду біологічно-небезпечних речовин. З урахуванням визначення на рівні D 7-ми елементів і на рівні E 6-ти, складається 7 матриць розміром 6x6. У результаті обчислення вагових коефіцієнтів q_e , формування з них відповідної матриці та множення її на вектор пріоритетів D отримуємо вектор прогнозних сценаріїв E.

$$E=q(e)*D= \begin{matrix} & q_e(\text{для} & q_e(\text{для} & q_e(\text{для} & q_e(\text{для} & q_e(\text{для} & q_e(\text{для} & q_e(\text{для} & & & \\ & D1) & D2) & D3) & D4) & D5) & D6) & D7) & & D & E \\ q_{e1} & 0.565 & 0.053 & 0.071 & 0.167 & 0.073 & 0.079 & 0.071 & \times & \begin{matrix} 0.370 \\ 0.244 \\ 0.185 \\ 0.090 \\ 0.055 \\ 0.033 \\ 0.024 \end{matrix} & = & \begin{matrix} 0.258 \\ 0.191 \\ 0.176 \\ 0.171 \\ 0.102 \\ 0.102 \end{matrix} \\ q_{e2} & 0.053 & 0.551 & 0.071 & 0.167 & 0.073 & 0.079 & 0.071 & & & & \\ q_{e3} & 0.053 & 0.061 & 0.643 & 0.167 & 0.073 & 0.079 & 0.071 & & & & \\ q_{e4} & 0.223 & 0.212 & 0.071 & 0.167 & 0.076 & 0.079 & 0.071 & & & & \\ q_{e5} & 0.053 & 0.061 & 0.071 & 0.167 & 0.632 & 0.095 & 0.071 & & & & \\ q_{e6} & 0.053 & 0.061 & 0.071 & 0.167 & 0.073 & 0.591 & 0.643 & & & & \end{matrix}$$

Перед переходом до наступного етапу – встановлення пріоритетів суспільно-небезпечних наслідків – необхідно оцінити уразливість об'єкта до кожного з прогнозних сценаріїв ППД. Для цього вводиться рівень ієрархії F (уразливість об'єкта до ППД). Аналіз уразливості використовується для визначення чутливості об'єктів до атак від загрози, виявленої на етапі аналізу загроз. Аналіз уразливості повинен відповісти на питання "до якого виду атак об'єкт є найбільш/найменш уразливим?". Уразливість притаманна кожному об'єкту, на який направлена терористична загроза. Уразливість існує завжди, незалежно від політик, процедур, структури та захисного обладнання. Враховуючи те, що терористичні загрози досить важко контролювати, вони піддаються оцінці і уразливість об'єкта до цих загроз можуть бути знижена. Ідентифікація і розуміння уразливості є важливим для визначення достатності захисту об'єктів від потенційних втрат. З урахуванням того, що

уразливість є компонентом терористичного ризику, потенційний терористичний ризик для об'єкта можна знизити шляхом зниження уразливості.

Для методології оцінки уразливості важливим етапом є визначення критеріїв, за допомогою яких можливо проводити відповідну оцінку. Як приклад, Департамент оборони США розробив декілька інструментів для допомоги у проведенні оцінки уразливості, найбільш відомими з яких є методи MSHARPP (Mission, Symbolism, History, Accessibility, Recognizability, Population, and Proximity) та CARVER (Criticality, Accessibility, Recuperability, Vulnerability, Effect, and Recognizability), які використовують різні критерії оцінки¹⁰⁶.

Зокрема, назва методу MSHARPP є акронімом, яка складається з назв критеріїв уразливості, таких як функціональність (mission), символізм (symbolism), доступність (accessibility), розпізнаваність (recognizability), людський фактор (Population) та близькість (proximity).

Назва CARVER відбиває в собі такі критерії як критичність (criticality), доступність (accessibility), відновлюваність (recuperability), уразливість (vulnerability), вплив на населення (effect on the population), розпізнаваність (recognizability).

Для оцінки уразливості кожного структурного елемента F об'єкта терористичних посягань до кожного сценарію протиправних дій, необхідно враховувати те, що ефективність кожного сценарію ППД знижується внаслідок існування різного рівня уразливості кожного компонента F об'єкта терористичних посягань. Враховуючи це, будемо вважати, що між елементами рівнів E та F існують взаємні зв'язки. Для отримання скорегованих вагових коефіцієнтів для рівня E, згідно з розглянутою вище методикою МАМ, необхідно скласти 2 групи відповідних матриць,

¹⁰⁶ DoD Antiterrorism handbook [Electronic resource]. — Mode of access : https://docviewer.yandex.ua/?url=http%3A%2F%2Fdownload.cabledrum.net%2Fwikileaks_archive%2Ffile%2Fus-dod-anti-terrorism-handbook-2004.pdf&name=us-dod-anti-terrorism-handbook-2004.pdf&lang=en&c=588f8d80b6d1

обчислити вагові коефіцієнти q_{fn} та q_{ep} , сформувати суперматрицю, привести її до стохастичного вигляду та піднести в граничні степені. Як видно з граничної суперматриці, ймовірності сценаріїв протиправних дій (вектор E) змінилися.

**Вихідна суперматриця взаємної оцінки рівнів E (сценарій протиправних дій) та
F (уразливість до протиправних дій)**

	E1	E2	E3	E4	E5	E6	F1	F2	F3	F4	F5
	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000
E1	0.25843	0.00000	0.00000	0.00000	0.00000	0.00000	0.54566	0.50575	0.42287	0.48336	0.37434
E2	0.19062	0.00000	0.00000	0.00000	0.00000	0.00000	0.11071	0.14123	0.16169	0.15724	0.29914
E3	0.17650	0.00000	0.00000	0.00000	0.00000	0.00000	0.06121	0.05880	0.06128	0.05196	0.09213
E4	0.17095	0.00000	0.00000	0.00000	0.00000	0.00000	0.17505	0.17723	0.22333	0.19733	0.12589
E5	0.10198	0.00000	0.00000	0.00000	0.00000	0.00000	0.04751	0.04896	0.05944	0.05559	0.05425
E6	0.10153	0.00000	0.00000	0.00000	0.00000	0.00000	0.05986	0.06803	0.07139	0.05451	0.05425
F1	0.00000	0.57816	0.55638	0.47751	0.41703	0.31706	0.00000	0.00000	0.00000	0.00000	0.00000
F2	0.00000	0.06614	0.09378	0.13568	0.16602	0.19289	0.00000	0.00000	0.00000	0.00000	0.00000
F3	0.00000	0.05271	0.05627	0.06125	0.08108	0.10595	0.00000	0.00000	0.00000	0.00000	0.00000
F4	0.00000	0.24541	0.23124	0.25828	0.26529	0.31966	0.00000	0.00000	0.00000	0.00000	0.00000
F5	0.00000	0.05758	0.06232	0.06729	0.07058	0.06446	0.00000	0.00000	0.00000	0.00000	0.00000

Гранична суперматриця взаємної оцінки рівнів E (сценарій протиправних дій) та F (уразливість до протиправних дій)

	E1	E2	E3	E4	E5	E6	F1	F2	F3	F4	F5
	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
E1	0.509	0.000	0.000	0.000	0.000	0.000	0.509	0.509	0.509	0.509	0.509
E2	0.140	0.000	0.000	0.000	0.000	0.000	0.140	0.140	0.140	0.140	0.140
E3	0.061	0.000	0.000	0.000	0.000	0.000	0.061	0.061	0.061	0.061	0.061
E4	0.181	0.000	0.000	0.000	0.000	0.000	0.181	0.181	0.181	0.181	0.181
E5	0.051	0.000	0.000	0.000	0.000	0.000	0.051	0.051	0.051	0.051	0.051
E6	0.060	0.000	0.000	0.000	0.000	0.000	0.060	0.060	0.060	0.060	0.060
F1	0.000	0.535	0.535	0.535	0.535	0.535	0.000	0.000	0.000	0.000	0.000
F2	0.000	0.094	0.094	0.094	0.094	0.094	0.000	0.000	0.000	0.000	0.000
F3	0.000	0.060	0.060	0.060	0.060	0.060	0.000	0.000	0.000	0.000	0.000
F4	0.000	0.249	0.249	0.249	0.249	0.249	0.000	0.000	0.000	0.000	0.000
F5	0.000	0.061	0.061	0.061	0.061	0.061	0.000	0.000	0.000	0.000	0.000

Скореговані значення вектору E (сценарій протиправних дій)

Скореговані значення вектору F (уразливість структурних підрозділів об'єкта терористичних посягань)

Для категорювання за рівнем суспільно-небезпечних наслідків необхідно визначити можливі види цих наслідків внаслідок терористичних атак. Загальноприйняті в ЕС процедури виявлення і встановлення європейських критичних інфраструктур ("ECIs") і проведення оцінки необхідності посилення їхнього захисту, формування критеріїв значущості об'єктів, зокрема, в контексті наслідків можливих терористичних посягань, є комплексними та мають враховувати¹⁰⁷:

а) критерій за кількістю жертв (оцінка проводиться з урахуванням кількості потенційних загиблих або поранених);

б) критерій, пов'язаний з економічними наслідками (оцінка проводиться з точки зору значущості економічних втрат та/або ступеня погіршення якості продуктів або послуг, включає можливі наслідки для навколишнього середовища);

с) критерій впливу на населення (оцінка проводиться з точки зору впливу на суспільну довіру, фізичних страждань і порушення у повсякденному житті, включаючи втрату можливості надання важливих послуг).

Такий підхід є оптимальним для оцінки диверсійно-терористичних впливів, якщо мова йде лише про загрозу впливу на об'єкт та оточуюче його середовище, враховуючи й соціальне. Але не йдеться про впливи на соціально-політичні алгоритми управління в суспільстві, зміна або примусова корекція яких, власне, і є головною метою терористичної діяльності¹⁰⁸. Тому однією із складових можливих наслідків терористичного

¹⁰⁷ Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection [Електронний ресурс]. — Режим доступу : http://eur-lex.europa.eu/search.html?lang=en&text=Council+directive+No.+2008%2F114%2FEC+On+the+id+entification+and+designation+of+european+critical+infrastructures+and+the+assessment+of+the+need+to+improve+their+protection&qid=1480852873267&type=quick&scope=EURLEX&DD_YE AR=2008.

¹⁰⁸ Рижов І. М., Кудінов С. С. Цілевизначення та методичні засади ідентифікації об'єктів можливих терористичних посягань / І. М. Рижов, С.С. Кудінов // Збірник наукових праць. — 2015. — № 57. — С. 80 – 86.

акту є соціально-політична реакція суспільства на небезпеку внаслідок сукупного впливу на даний об'єкт вражаючих факторів терористичних загроз.

Для визначення ризику настання суспільно-небезпечних наслідків (з урахуванням скорегованих раніше значень сценаріїв на рівні E) необхідно перемножити матрицю, складену зі значень qh_1, qh_2, \dots, qh_6 , на скорегований вектор прогнозних сценаріїв E. У результаті отримуємо вектор ймовірностей ризику настання суспільно-небезпечних наслідків H. Для нашого прикладу ця операція матиме вигляд:

$$N=q(f)*E= \begin{matrix} & \begin{matrix} qh(\text{для} \\ E1) \end{matrix} & \begin{matrix} qh(\text{для} \\ E2) \end{matrix} & \begin{matrix} qh(\text{для} \\ E3) \end{matrix} & \begin{matrix} qh(\text{для} \\ F4) \end{matrix} & \begin{matrix} qh(\text{для} \\ E5) \end{matrix} & \begin{matrix} qh(\text{для} \\ E6) \end{matrix} \\ \begin{matrix} qh1 \\ qh2 \\ qh3 \\ qh4 \\ qh5 \end{matrix} & \begin{vmatrix} 0.411 & 0.408 & 0.333 & 0.416 & 0.456 & 0.531 \\ 0.267 & 0.298 & 0.353 & 0.311 & 0.271 & 0.231 \\ 0.189 & 0.151 & 0.223 & 0.178 & 0.188 & 0.147 \\ 0.088 & 0.100 & 0.065 & 0.064 & 0.046 & 0.050 \\ 0.044 & 0.043 & 0.027 & 0.031 & 0.038 & 0.041 \end{vmatrix} & \times & \begin{vmatrix} 0.509 \\ 0.140 \\ 0.061 \\ 0.181 \\ 0.051 \\ 0.060 \end{vmatrix} & = & \begin{vmatrix} 0.416 \\ 0.283 \\ 0.181 \\ 0.080 \\ 0.040 \end{vmatrix} \end{matrix}$$

Отже, терористичний ризик є багатокритеріальною (векторною) величиною, яка включає в себе ймовірності настання людських втрат, матеріальних збитків, екологічних, культурних та суспільно-політичних наслідків.

Для обраного методу будемо вважати прийнятним ризик, який дорівнює 0,2 (теоретично можливий випадок коли всі елементи вектору H дорівнюють 0,2). Якщо значення найбільшого елементу вектору H не буде перевищувати 0,25 будемо вважати ризик низьким, від 0,25 до 0,33 – середнім, понад 0,33 – високим. Відповідно ОТП за категоріями терористичного ризику можуть бути розподілені як об'єкти третьої категорії (об'єкти з низьким терористичним ризиком), другої (з середнім ризиком) та першої (з високим ризиком). Подальше завдання полягає в нормативно-правовому розробленні вимог до антитерористичного захисту

типових категорій об'єктів ОТП в залежності від рівня терористичного ризику – низький, середній та високий.

Висновки.

Під терористичним ризиком пропонується розуміти багатокритеріальну (векторну) величину, яка характеризує ймовірність настання певних видів суспільно-небезпечних наслідків у разі ймовірної реалізації терористичної загрози. Терористичний ризик є функцією трьох компонент: терористичної загрози, уразливості ОТП до цієї загрози та можливих суспільно-небезпечних наслідків у випадку успішної реалізації такої загрози.

Для обчислення рівня терористичної загрози як одного з компонентів терористичного ризику перевагу слід надавати евристичним методам, оскільки ймовірнісно-статистичні методи можуть створювати значну похибку та призвести до невірної оцінки величини загрози та, як наслідок, терористичного ризику. Як вже зазначалось вище, основною причиною цього є суттєві відмінності методології аналізу ризиків природних та інженерних систем від аналізу терористичних ризиків. Оцінка ймовірностей терористичної загрози потребує наявності та оцінки оперативної (розвідувальної) інформації про плани та наміри терористів, врахування їх можливої обізнаності у посиленні антитерористичного захисту окремих ОТП з боку правоохоронних органів, проведення розподілу (перерозподілу) захисних ресурсів.

Розглянута методологія визначення терористичного ризику, яка поєднує методи експертного оцінювання, аналітичних мереж, аналізу ієрархій, чек-листів зі зваженими коефіцієнтами, містить ряд переваг, а саме:

створюється можливість отримання якісно-кількісних характеристик компонентів терористичного ризику - загрози, уразливості та наслідків;

визначені ймовірності складових терористичного ризику надають змогу застосовувати методологію управління ризиками (risk assessment). Управляти ризиком можна шляхом впливу на його компоненти: загрози (використання активних заходів розвідки та контррозвідки, профілактична

робота), уразливість об'єкта (удосконалення системи АТЗ) та наслідки (вжиття превентивних заходів з мінімізації можливих збитків, організація захисту населення, створення додаткових запасів продовольства, медикаментів тощо);

поруч з кількісними оцінками компонент терористичного ризику стає доступною їх якісна оцінка (яка терористична організація, група та особа становить найбільшу загрозу для ОТП, який саме структурний підрозділ ОТП є найбільш уразливим до терористичних загроз, ризик якого виду суспільно-небезпечних наслідків є найвищим тощо);

з'ясування величини терористичного ризику та його компонент є визначальною умовою для превентивного планування АТЗ, метою якого має стати розроблення антитерористичних заходів, спрямованих на зниження ймовірнісних значень структурних компонент терористичного ризику;

практичне значення запропонованого підходу полягає в можливості розмежування процесу аналізу та оцінки ризиків між різними суб'єктами боротьби з тероризмом. Зокрема, оцінку рівня терористичної загрози можуть проводити експерти СБ України із залученням представників розвідувальних та інших правоохоронних органів. Розрахунок уразливості об'єкта до загрози та можливих наслідків доцільно покласти на представників служб охорони ОТП та експертів зі складу профільних міністерств і відомств.

Категорювання об'єктів як попередній етап для подальшого формування вимог до їх АТЗ може бути доцільним та мати практичне значення лише в межах певної групи типових ОТП (так би мовити "однорідних" об'єктів або об'єктів однієї галузево-відомчої належності). Встановлення категорій об'єктів без урахування їх цільового призначення, особливостей функціонування, наявності матеріальних цінностей, небезпечних речовин, особливостей охорони не дозволить сформулювати вимоги до їх захисту (об'єктами 1-ї категорії можуть виявитися як обласні державні адміністрації, так і атомні електростанції, а підходи до організації їх захисту принципово різняться).

З урахуванням того, що згідно з постановою Кабінету Міністрів України від 18 лютого 2016 р. № 92, до ОТП відносяться 8 груп типових об'єктів різної відомчо-галузевої належності, які мають різні внутрішньовідомчі інструкції (накази) щодо охорони та оборони належних їм об'єктів (в основному обмеженого доступу), подальше самостійне (без залучення фахівців суб'єктів боротьби з тероризмом) нормативно-правове розроблення фахівцями НА СБУ вимог до антитерористичного захисту ОТП в залежності від рівня терористичного ризику є недоцільним, оскільки воно не буде враховувати особливостей вже існуючої системи охорони та оборони цих об'єктів (як вже зазначалося вище, о х о р о н у о р г а н і в д е р ж а в н о ї в л а д и з а б е з п е ч у є У Д О, установ кримінально-виконавчої системи - Державна пенітенціарна служба України, об'єктів ядерної енергетики, закордонних дипломатичних установ - Національна гвардія України, окремих державних об'єктів - ДСО при МВС України, місць масового перебування людей - підрозділи патрульної поліції Національної поліції України). Вказану роботу необхідно проводити за участю експертів зацікавлених суб'єктів боротьби з тероризмом.

14. КОМПЕТЕНЦІЯ СУБ'ЄКТІВ БОРОТЬБИ З ТЕРОРИЗМОМ В УКРАЇНІ У ПРОТИДІЇ ЗАГРОЗАМ ТЕРОРИСТИЧНОГО ХАРАКТЕРУ

Тероризм є справжньою небезпекою як на внутрішньодержавному так і на міжнародному рівні. Це явище формувалось протягом довгого часу, при цьому зазнавало змін в ідеологічному аспекті та залежало від світоглядної платформи терористів, а також від певної політичної мети, для досягнення якої і проводилась така суспільно загрозлива діяльність. Ступінь його суспільного ризику безперервно росте, і актуальною стає з кожним днем стає проблема забезпечення національної безпеки, і більше всього в умовах продовження антитерористичної операції на східних теренах України, а також у світлі інтеграційних процесів нашої держави до європейського простору безпеки.

Відповідно до Основного Закону Україна є суверенною, незалежною, демократичною, соціальною, правовою державою, найвищою соціальною цінністю якої є людина, її життя та здоров'я, честь і гідність, недоторканість і безпека¹⁰⁹. Проте, варто відзначати, що на сьогоднішній день фігурують негативні явища, ціллю котрих є створення загрози для основних цінностей, проголошених Конституцією України. Мова йде про таке явище, як тероризм — суспільно небезпечну діяльність, суттю котрої є навмисне, цілеспрямоване застосування насильства через такі події як захоплення заручників, залякування мирних жителів, підпали, убивства, насильницька протидія органам влади, а також організація та реалізація інакших посягань на життя чи здоров'я людей. З метою протидії вищезгаданому загрозливому явищу в Україні існують суб'єкти протидії тероризму.

¹⁰⁹ Конституція України: Закон України від 28.06.1996 // [Електронний ресурс]. — Режим доступу: <http://zakon.rada.gov.ua>.

Згідно з положенням ст.1 Закону України «Про боротьбу з тероризмом» від 20.03.2003 № 638-IV боротьба з тероризмом — це діяльність щодо запобігання, виявлення, припинення, мінімізації наслідків терористичної діяльності¹¹⁰. На основі цього визначення, можна стверджувати, що суб'єктами протидії тероризму в Україні є учасники правовідносин у сфері протидії тероризму, котрі мають визначені законом певні повноваження з питань виявлення, відвернення, знищення та зменшення негативного впливу терористичної діяльності.

На нашу думку, з практичної точки зору доречно поставити наголос не стільки на боротьбі з тероризмом, яка за своєю суттю торкається уже існуючих і виявлених груп терористів, скільки на протидії. Можемо стверджувати, що протидія тероризму є більш ширшим поняттям, яке є відповідним до сучасних параметрів тероризму, його суспільного значення і реальній неможливості його знищення.

Під протидією тероризму пропонується розуміти: діяльність органів державної влади і органів місцевого самоврядування, об'єднань громадян, окремих громадян з: а) профілактики тероризму — виявлення і подальшого усунення причин і умов, що сприяють здійсненню терористичної діяльності; б) боротьби з тероризмом — виявлення, попередження, припинення, розкриття і розслідування терористичних злочинів; в) мінімізації і (або) ліквідації наслідків терористичної діяльності.

Системою суб'єктів протидії загрозам терористичного характеру є визначена на законодавчому рівні певна сукупність суб'єктів, основною метою яких є взаємодія один з одним шляхом відвернення, виявлення, знищення та зменшення негативного впливу терористичної діяльності. Для конкретизації цього поняття потрібно визначити сутність та місце у цій системі кожного з суб'єктів протидії загрозам терористичного характеру.

Система суб'єктів боротьби з тероризмом складається з двох рівнів:

¹¹⁰ Про боротьбу з тероризмом: Закон України від 20.03.2003 №638-IV // [Електронний ресурс]. — Режим доступу: <http://zakon.rada.gov.ua>.

I. Суб'єкти, що безпосередньо здійснюють боротьбу з тероризмом.

II. Суб'єкти, що можуть у разі необхідності залучатися до боротьби з тероризмом.

Перший рівень суб'єктів, які безпосередньо ЗДІЙСНЮЮТЬ боротьбу з тероризмом у межах своєї компетенції. На сьогодні такими суб'єктами є: Служба безпеки України – головний орган у загальнодержавній системі боротьби з терористичною діяльністю; Міністерство внутрішніх справ України; Національна поліція, Міністерство оборони України; центральні органи виконавчої влади, що забезпечують формування та реалізують державну політику у сфері цивільного захисту; центральний орган виконавчої влади, що реалізує державну політику у сфері захисту державного кордону; центральний орган виконавчої влади, що реалізує державну політику у сфері виконання кримінальних покарань; Управління державної охорони України, центральний орган виконавчої влади, що реалізує державну податкову політику, державну політику у сфері державної митної справи¹¹¹.

До участі у здійсненні заходів, пов'язаних з попередженням, виявленням і припиненням терористичної діяльності, залучаються у разі необхідності також: центральний орган виконавчої влади, що реалізує державну політику у сфері запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, або фінансуванню тероризму; Служба зовнішньої розвідки України; Міністерство закордонних справ України; Державна служба спеціального зв'язку та захисту інформації України; центральні органи виконавчої влади, що забезпечують формування та реалізують державну політику у сфері охорони здоров'я; центральні органи виконавчої влади, що забезпечують формування та реалізують державну політику в електроенергетичному, вугільно-промисловому та нафтогазовому комплексах; центральний орган виконавчої влади, що

¹¹¹ Про боротьбу з тероризмом: Закон України від 20.03.2003 №638-IV // [Електронний ресурс]. — Режим доступу: <http://zakon.rada.gov.ua>.

реалізує державну політику у сфері управління об'єктами державної власності; центральні органи виконавчої влади, що забезпечують формування та реалізують державну політику у сферах транспорту; центральні органи виконавчої влади, що забезпечують формування та реалізують державну фінансову політику; центральні органи виконавчої влади, що забезпечують формування та реалізують державну політику у сфері охорони навколишнього природного середовища; центральні органи виконавчої влади, що забезпечують формування та реалізують державну аграрну політику. До участі в антитерористичних операціях за рішенням керівництва антитерористичної операції можуть бути залучені з дотриманням вимог цього Закону й інші центральні та місцеві органи виконавчої влади, органи місцевого самоврядування, підприємства, установи, організації незалежно від підпорядкованості і форми власності, їх посадові особи, а також громадяни за їх згодою. Координацію діяльності суб'єктів, які залучаються до боротьби з тероризмом, здійснює Антитерористичний центр при Службі безпеки України.

Антитерористичний центр: визначає, аналізує причини і умови, які сприяють виникненню та поширенню тероризму; надає методичну допомогу та рекомендації суб'єктам боротьби з тероризмом щодо виявлення і усунення причин та умов, які сприяють виникненню та поширенню тероризму; координує дії суб'єктів боротьби з тероризмом щодо розширення взаємодії з правоохоронними органами і спеціальними службами іноземних держав, антитерористичними структурами ООН, ОБСЄ, НАТО, ЄС, іншими міжнародними організаціями, що здійснюють боротьбу з тероризмом, на підставі міжнародних договорів¹¹².

У межах своєї компетенції вони здійснюють: заходи із запобігання, виявлення і припинення терористичних актів та злочинів терористичної

¹¹² Положення про єдину державну систему запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків, затверджене постановою Кабінету Міністрів України від 18.02.2016 № 92 // [Електронний ресурс]. — Режим доступу: <http://zakon.rada.gov.ua>

спрямованості; розробляють і реалізують попереджувальні, режимні, організаційні, виховні та інші заходи; забезпечують умови проведення антитерористичних операцій на об'єктах, що належать до сфери їх управління; надають відповідним підрозділам під час проведення таких операцій матеріально-технічні та фінансові засоби, засоби транспорту і зв'язку, медичне обладнання і медикаменти, інші засоби, а також інформацію, необхідну для виконання завдань щодо боротьби з тероризмом.

Отже, головним органом у загальнодержавній системі боротьби та протидії тероризму є Служба безпеки України, що відповідно до Закону України «Про Службу безпеки України» від 25.03.1992 № 2229-XII є державним правоохоронним органом спеціального призначення, який забезпечує державну безпеку України¹¹³. У складі Служби безпеки України діє Антитерористичний центр, який на підставі Положення про Антитерористичний центр та його координаційні групи при регіональних органах Служби безпеки України, затвердженого Указом Президента України від 14 квітня 1999 року № 379/99, є постійно діючим органом при Службі безпеки України, що здійснює координацію діяльності суб'єктів протидії з тероризмом у запобіганні терористичним актам щодо державних діячів, критичних об'єктів життєзабезпечення населення, об'єктів підвищеної небезпеки, актам, що загрожують життю та здоров'ю значної кількості людей, та їх припиненні¹¹⁴.

Іншим державним правоохоронним органом спеціального призначення, на який законодавством України покладено обов'язок щодо безпосереднього здійснення боротьби та протидії тероризму у межах своєї компетенції, є Управління державної охорони, яке згідно із Законом України «Про державну охорону органів державної влади України та посадових осіб» від

¹¹³ Про Службу безпеки України: Закон України від 25.03.1992 №2229-XII // [Електронний ресурс]. — Режим доступу: <http://zakon.rada.gov.ua>.

¹¹⁴ Положення про Антитерористичний центр та його координаційні групи при регіональних органах Служби безпеки України, затверджене Указом Президента України від 14.04.1999 року № 379/99 // [Електронний ресурс]. — Режим доступу: <http://zakon.rada.gov.ua>.

04.03.1998 №160/98-ВР підпорядковане Президентові України та підконтрольне Верховній Раді України і здійснює державну охорону органів державної влади України та посадових осіб, що виражається у реалізації системи організаційно-правових, режимних, оперативно-розшукових, інженерно-технічних та інших заходів з метою забезпечення нормального функціонування органів державної влади України, безпеки посадових осіб та об'єктів, визначених законодавством¹¹⁵. Також варто зауважити, що Закон України «Про боротьбу з тероризмом» поряд із вищезгаданими органами виділяє органи спеціального призначення, для котрих діяльність щодо протидії загрозам терористичного характеру хоч і не є основними повноваженнями, усе ж у передбачених законом випадках вони можуть виконувати функції суб'єктів протидії загрозам терористичного характеру. Йдеться про Службу зовнішньої розвідки України та Державну службу спеціального зв'язку та захисту інформації України. Так, відповідно до ст. 1 Закону України «Про Службу зовнішньої розвідки України» від 01.12.2005 №3160-IV Служба зовнішньої розвідки України є державним органом, який здійснює розвідувальну діяльність у політичній, економічній, військово-технічній, науково-технічній, інформаційній та екологічній сферах; підпорядковується Президентові України та підконтрольний Президентові України і Верховній Раді України. Згідно із Законом України «Про Державну службу спеціального зв'язку та захисту інформації України» від 23.02.2006 №3475-IV Державна служба спеціального зв'язку та захисту інформації України є державним органом, який призначений для забезпечення функціонування та розвитку державної системи урядового зв'язку, національної системи конфіденційного зв'язку, формування та реалізації державної політики в сферах криптографічного та технічного захисту інформації, телекомунікацій, користування радіочастотним ресурсом України, поштового зв'язку спеціального призначення, урядового

¹¹⁵ Про державну охорону органів державної влади України та посадових осіб: Закон України від 04.03.1998 №160/98-ВР // [Електронний ресурс]. — Режим доступу: <http://zakon.rada.gov.ua>.

фельд'єгерського зв'язку, а також інших завдань. Служба спрямовує свою діяльність на забезпечення національної безпеки України від зовнішніх і внутрішніх загроз та є складовою сектору безпеки й оборони України¹¹⁶.

Також відповідно до частини другої ст. 4 Закону України «Про боротьбу з тероризмом» у межах своєї компетенції, визначеної законами та виданими на їх основі іншими нормативно-правовими актами, участь у протидії тероризму беруть центральні органи виконавчої влади.

Варто зауважити, що до кола суб'єктів, які безпосередньо здійснюють боротьбу з тероризмом відносять:

- Міністерство внутрішніх справ України;
- Міністерство оборони України;
- центральні органи виконавчої влади, що забезпечують формування та реалізують державну політику в сфері цивільного захисту;
- центральний орган виконавчої влади, що реалізує державну політику у сфері захисту державного кордону, — Адміністрація Державної прикордонної служби України;
- центральний орган виконавчої влади, що реалізує державну політику в сфері виконання кримінальних покарань, — Державна пенітенціарна служба України.

Тобто законодавець чітко передбачив кількість центральних органів виконавчої влади, які є суб'єктами протидії загрозам терористичного характеру, та у межах власної компетенції реалізують антитерористичну функцію безпосередньо. Для того, щоб діяльність щодо протидії загрозам терористичної діяльності проводилась відповідно до чинного законодавства та до вимог міжнародних спільнот існує державний контроль у сфері боротьби з тероризмом – певна група контролюючих суб'єктів, однією із функцій яких є взаємна діяльність щодо забезпечення підходящих умов для

¹¹⁶ Про Державну службу спеціального зв'язку та захисту інформації України: Закон України від 23.02.2006 №3475-IV // [Електронний ресурс]. — Режим доступу: <http://zakon.rada.gov.ua>.

продуктивного функціонування державної антитерористичної системи за умови стабільного існування внутрішніх та зовнішніх подразників.

Суб'єктами державного контролю у сфері боротьби з тероризмом виступають Верховна Рада України, Президент України, Кабінет Міністрів України, які здійснюють контрольну діяльність в системі державного управління. Зазначені вище суб'єкти утворюють контрольні органи, сукупність яких складає інфраструктуру контролю у сфері боротьби з тероризмом. Суб'єктам державного контролю у сфері боротьби з тероризмом притаманне коло повноважень, провідне значення серед яких посідає формування норм контролю. Отже, як свідчать результати цього дослідження, суб'єктами протидії загрозам терористичного характеру в Україні є учасники правовідносин у сфері протидії тероризму, що мають визначені законом повноваження щодо виявлення, відвернення, знищення та зменшення негативного впливу терористичної діяльності. З системної точки зору на явище тероризму, варто наголосити на необхідності вагомої участі не тільки органів держави, у компетенцію яких входить боротьба з тероризмом та загрозами терористичного характеру, але й інших органів з ціллю розширення їх повноважень у даній сфері та залучення їх до антитерористичної профілактики.

В результаті цього дослідження можна зробити висновки про те, що в Україні створена та закріплена на законодавчому рівні система суб'єктів боротьби із загрозами терористичного характеру. Проаналізовано дворівневу систему суб'єктів боротьби з загрозами терористичного характеру, проте нормативно-правове регулювання взаємовідносин між органами державної влади у сфері протидії тероризму суттєво відривається від вимог дійсності. Тому потрібна важлива кропітка робота з формулювання більш виразних і дійових параметрів спеціальної компетенції державних органів та центральних органів виконавчої влади, враховуючи при цьому норми міжнародного права, досягнення в українській законодавчій сфері та твердження вітчизняних науковців.

15. ОСОБЛИВОСТІ РЕАЛІЗАЦІЇ ЗАГАЛЬНО-ПРОФІЛАКТИЧНИХ ЗАХОДІВ АНТИТЕРОРИСТИЧНОГО ЗАХИСТУ

Як показує суспільна практика, сучасна практика протидії тероризму на державному рівні зосереджена, в основному, на застосуванні правових норм і силове вирішення даної проблеми, що не приводить до бажаних результатів¹¹⁷.

Недосконалість профілактики антитерористичного захисту, ефективних способів їх реалізації, ефективного використання можливостей суспільства із самозбереження та самозахисту указує на певну кризу внутрішніх стратегій боротьби із тероризмом.

Аналіз теоретичних концепцій та побудованих на їх базі програм з протидії проявам тероризму дозволяє констатувати однобічність висвітлення проблеми, недостатню розробленість програми превентивних заходів, що враховує багатоаспектність поля профілактичної діяльності, що включає сегменти державно-правового регулювання, розвитку культури і освіти, оптимізації функціонування ЗМІ, вдосконалення соціально-культурної діяльності громадянського суспільства¹¹⁸.

При формуванні антитерористичних стратегій поза увагою, залишалися можливості науковців у опрацюванні креативних, науково - обґрунтованих рекомендацій щодо розвитку системи антитерористичного захисту. Про це свідчить той факт, що в державі немає спеціалізованих наукових закладів, які б досліджували проблеми антитерористичної безпеки

117 Рижов І.М. Щодо перспектив удосконалення концепцій та оптимізації стратегій боротьби з тероризмом / І.М.Рижов // Юридичний науковий електронний журнал (Запоріжжя). – 2014 – №3 – Режим доступу: http://lsej.org.ua/3_2014/36.pdf. (дата звернення: 15.09.15). – Назва з екрана.

118 Науково-дослідний інститут Організації Об'єднаних Націй з питань злочинності та правосуддя / United Nations Interregional Crime and Justice Research Institute (UNICRI). [Електронний ресурс]. – Режим доступу: <http://www.unicri.it/institute/>

як комплексної наукової дисципліни. Наслідки такої помилки стали фатальними – як не сумно це констатувати.

Під профілактикою тероризму розуміється діяльність, що включає комплекс заходів, спрямованих на виявлення та усунення причин і умов, що сприяють здійсненню терористичної діяльності. Профілактика тероризму здійснюється за трьома основними напрямками:

- організація і здійснення на системній основі протидії ідеології тероризму і екстремізму;
- вдосконалення антитерористичної захищеності потенційних об'єктів терористичних устремлінь;
- посилення контролю за дотриманням адміністративних, правових та інших режимів, що сприяють протидії тероризму.

Організація діяльності щодо профілактики тероризму вимагає забезпечення скоординованої роботи органів державної влади з громадськими організаціями та об'єднаннями, релігійними структурами, іншими інститутами громадянського суспільства та окремими громадянами. Реалізація зазначених завдань здійснюється в рамках створення ефективної системи заходів щодо протидії тероризму.

Організація боротьби з тероризмом вимагає комплексного підходу до аналізу джерел і суб'єктів терористичної діяльності, чіткого визначення функцій і зони відповідальності кожного суб'єкта боротьби, своєчасного визначення пріоритетів у вирішенні поставлених завдань, вдосконалення організації побудови та взаємодії оперативних, оперативно-бойових, військових, слідчих підрозділів на основі впровадження штабного принципу організації управління антитерористичної операції і забезпечення ресурсами, що включають сучасні апаратно-програмні комплекси (автоматизовані системи управління).

Профілактика тероризму передбачає вирішення наступних завдань:

- розробка рекомендацій і здійснення заходів щодо усунення причин та умов, що сприяють виникненню і поширенню тероризму;

- виявлення і прогнозування терористичних загроз, інформування про них органів державної влади та органів місцевого самоврядування, а також громадськості для вжиття заходів щодо їх нейтралізації;

- надання стримуючого і позитивного впливу на поведінку окремих осіб (груп осіб), схильних до екстремістських дій;

- визначення правової регламентації діяльності органів виконавчої влади при введенні режимів терористичних загроз;

- розробка переліку антитерористичних заходів для організації та проведення їх на території України з обов'язковим визначенням джерел їх фінансування;

- розробка та впровадження типових вимог щодо захисту від загроз терористичних актів критично важливих і потенційно небезпечних об'єктів, місць масового перебування людей;

- визначення прав, обов'язків і відповідальності керівників органів виконавчої влади та господарюючих суб'єктів при організації заходів з антитерористичної захищеності підвідомчих їм об'єктів;

- вдосконалення взаємодії органів виконавчої влади з метою вироблення єдиної стратегії і тактики в рамках здійснення міжнародного співробітництва в сфері протидії тероризму.

В рамках діяльності по профілактиці тероризму використовуються політичні, соціально-економічні, інформаційно-пропагандистські, освітні методи, а також методи фізичної, технічної захисту і правової превенції, що мають пріоритетне значення для зниження рівня і масштабу терористичних загроз. Вони покликані надавати цілеспрямований вплив на економічні, політичні, соціальні, національні та конфесійні процеси, які можуть породжувати масштабні суспільні конфлікти і, як наслідок, терористичні прояви; захищати від терористичних устремлінь громадян (групи громадян); попереджати формування терористичних намірів; ускладнювати дії суб'єктів терористичної діяльності. Виходячи з характеру об'єкта профілактичного впливу, використовуються різні форми загальної та адресної профілактики, з

урахуванням його демографічних, етноконфесійних, індивідуально-психологічних та інших особливостей.

До основних груп загально-профілактичних заходів антитерористичного захисту відносяться:

- політичні (заходи щодо нормалізації суспільно-політичної ситуації, вирішення соціальних конфліктів, зниження рівня соціально-політичної напруженості, здійсненню міжнародного співробітництва в сфері протидії тероризму);

- соціально-економічні (заходи з оздоровлення соціально-економічної ситуації в окремих регіонах і вирівнюванню рівня розвитку регіонів, скорочення маргіналізації населення, зменшення майнової диференціації, забезпечення соціального захисту населення);

- правові (адміністративні, кримінальні, організаційні та інші заходи, спрямовані на невідворотність покарання за скоєні діяння терористичного характеру, вдосконалення механізму відповідальності за недотримання вимог антитерористичного законодавства, протидія незаконному обігу зброї, боєприпасів, вибухових речовин, наркотичних і психотропних засобів, радіоактивних матеріалів, небезпечних біологічних речовин і хімічних реагентів, фінансуванню тероризму; регулювання міграційних процесів і порядку використання інформаційно-комунікаційних систем);

- інформаційно-пропагандистські (заходи щодо розкриття сутності та роз'яснення небезпеки тероризму, надання впливу на громадян (груп громадян) з метою виховання у них неприйняття ідеології насильства і залучення їх до участі у протидії тероризму);

- культурно-освітні (заходи по формуванню соціально значущих цінностей в суспільстві і вихованню толерантності);

- організаційно-технічні (розробка і реалізація цільових програм і конкретних заходів щодо забезпечення об'єктів можливих терористичних посягань технічними засобами захисту, вдосконалення механізму відповідальності за недотримання вимог з антитерористичної захищеності

об'єктів терористичних устремлінь і технічного оснащення учасників антитерористичної діяльності).

Складність сприйняття проблемних питань вказаного напрямку полягає в тому, що, розглядаючи профілактику терористичної діяльності правоохоронними та іншими державними органами на території всієї України у мирні часи, необхідно робити її проекцію на район проведення АТО з урахуванням довготривалих широкомасштабних бойових дій, які важко назвати терористичною діяльністю.

Історично склалося так, що на об'єктах, які мають стратегічне значення для безпеки держави, антитерористична безпека забезпечувалася на рівні, що відповідав фінансуванню, розвитку нормативної бази, кваліфікації кадрів, наявністю наглядових функцій з боку держави.

Кадровий склад на цих об'єктах більш-менш був підготовлений до антитерористичної роботи. Іншим чином ситуація складалася для інших потенційно небезпечних і громадських об'єктів, які в силу зміни політичних, економічних, інших обставин почали зазнавати атак терористів, де відсутні кваліфіковані кадри, а грошей вистачає тільки на охорону периметру, захист від пожеж та крадіжок. І це при відсутності законодавчого визначення відповідальності керівників за відсутність забезпечення антитерористичної безпеки.

У разі виникнення терористичної загрози на цих об'єктах, її усунення покладається на персонал підприємства, штатний склад служби безпеки, сформований в основному із пенсіонерів чи інших осіб, залучених до виконання окремих завдань захисту чи охорони. Цей контингент в основному потребує базової антитерористичної підготовки.

Саме цим категоріям працівників поперед усіх можуть бути адресовані освітницькі програми, без засвоєння яких неможливо вести антитерористичну діяльність на об'єкті, правильно оцінити терористичні загрози у повсякденній обстановці чи екстремальних ситуаціях.

Виходячи із аналізу сучасного стану та зростання терористичних загроз, необхідно удосконалювати нормативно-правову базу боротьби з тероризмом, тому числі в частині підготовки населення антитерористичній діяльності на терористично-вразливих об'єктах.

Науковий підхід до планування, розробки та впровадження системи антитерористичного захисту окремого об'єкту може передбачати послідовне виконання конкретних заходів у наступні чотири етапи:

на першому етапі здійснюється: вибір типу системи антитерористичного захисту; спеціальне обстеження об'єкту та визначення передня реальних терористичних загроз; розробка об'єктової концепції антитерористичного захисту та протидії тероризму (на першому етапі повинні бути вирішені дві основні задачі - побудування;

на другому етапі виконуються: розробка довгострокових антитерористичних заходів; антитерористичні плани для типових ситуацій терористичної атаки, розробка антитерористичного паспорту підприємства, оснащення об'єкта необхідними технічними засобами;

на третьому етапі проводиться навчання керівного складу й персоналу діям в екстремальних ситуаціях, готуються заходи по підтримці системи антитерористичного захисту у постійній готовності, оцінюються ТУ об'єкту, заходи по підвищенню антитерористичного захисту;

на четвертому етапі проводиться погодження системи антитерористичного захисту об'єкта; побудування комплексної інтегрованої системи захисту безпеки і антитерористичного захисту об'єкта; у разі необхідності переробка антитерористичного паспорту підприємства.

Робоче проектування системи антитерористичного захисту об'єкту представляє собою процес розробки та прийняття нормативних, організаційних і методичних документів, які служать основою для функціонування усіх суб'єктів антитерористичної діяльності на об'єкті.

Створення та впровадження комплексу спеціальних управлінських документів, а також інструктивно-методичних матеріалів, учбових програм

і учбових посібників для працюючого персоналу – для багатьох діло нове, але в сучасних умовах абсолютно необхідне.

Разом з тим необхідно розуміти важливе – діяльність з антитерористичної безпеки ведеться не «з чистого паперу». Об'єкти функціонують, маються підрозділи безпеки та охорони, впроваджені системи контролю й управління доступом, є системи оповіщення, інженерне укріплення об'єктів, т.і. По лінії цивільного захисту розроблені пам'ятки й методичні рекомендації персоналу по діям у екстремальних ситуаціях техногенного характеру. В окремих випадках розроблялись і методичні рекомендації на випадок вчинення терористичного акту.

Таким чином, є підстави для розгортання та подальшого удосконалення загально профілактичних попереджувальних заходів з антитерористичного захисту.

Точно спланувати свої дії при їх виникненні дуже важко, тому вибирають обмежений перелік типових ситуацій терористичних загроз і завчасно планують організаційні, технічні, інші заходи для кожної з них. Для детального аналізу і конкретизації інструктивно-методичних рекомендацій можливо виділити вісім типових ситуацій:

1) загострення криміногенної обстановки у регіоні чи місці у зв'язку з несприятливими соціально-політичними та економічними процесами у країні; триваючими військовими конфліктами; висловлюваннями терористами погроз у ЗМІ;

2) отримання керівником чи службовцями об'єкту конкретних загроз терористичного характеру по телефону, у вигляді анонімних листів чи через інші засоби комунікації;

3) виявлення персоналом об'єкту предмету з явними ознаками вибухових пристроїв чи іншого вибухонебезпечного предмету, спроможного причинити смерть, тяжкі каліцтва чи суттєву матеріальну шкоду об'єкту;

4) виявлення підозрілих предметів. Що вимагають спеціальної перевірки з метою встановлення їх реальної вибухової, радіаційної хімічної, біологічної небезпеки (предметів імітування);

5) вчинення терористичної акції способом вибуху, що привело до людських жертв, знищення (пошкодження) матеріальних цінностей, паніку, суттєві збитки у бізнесі, тривале відключення електроенергії, тепла, газу;

6) вчинення терористичної акції шляхом захвату чи утримання заручників на території або в приміщеннях об'єкту;

7) взаємодії з правоохоронними органами і іншими відомствами та організаціями, що прибули на об'єкт по факту терористичного акту;

8) відновлення нормального режиму роботи об'єкту, ліквідація наслідків терористичного акту, усунення причин та умов, що сприяли терористичному прояву і виникненню надзвичайної події.

Одним з основних умов підвищення результативності профілактичних заходів у протидії тероризму є отримання упереджувальної інформації про загрози терористичного характеру та можливі ризики їх настання, наявні терористичні структури, їхні плани по здійсненню терористичних актів, прогностні моделі розповсюдження ідеології тероризму і екстремізму і, що переважно значуще, усвідомлення широким загалом та усіяка підтримка заходів з протидії та технологій антитерористичного захисту.

Умовою ефективної організації боротьби з тероризмом є завчасна підготовка сил і засобів суб'єктів боротьби з тероризмом до припинення терористичного акту в ході командно-штабних, тактико-спеціальних, оперативно-тактичних навчань, організованих оперативними штабами на федеральному і регіональному рівнях. Особливий відділ ФБР по боротьбі з тероризмом підготував і представив на своєму сайті матеріал, присвячений мінімальним необхідним запобіжним заходам. Громадянам пропонується ознайомитися з інформацією про місця підвищеної небезпеки, про

рекомендовані дії у разі виявлення сумнівних пакетів і згорток на вулицях, у транспорті та інших публічних місцях. Серед пропонованої інформації є відомості щодо офіційної оцінки рівня терористичної загрози в конкретний момент, а також своєрідний «інструктаж» для тих, хто планує закордонні поїздки в «небезпечні» зони¹¹⁹.

Орієнтування громадян у сфері антитерористичної боротьби є одним з напрямків профілактичної діяльності. Громадянське суспільство має бути безпосередньо залучено до боротьби з тероризмом, тільки тоді можна буде говорити про проведення дійсно загальнонаціональної антитерористичної роботи, однак для цього необхідно, щоб в суспільстві було сформовано єдине розуміння самої суті міжнародного тероризму, масштабу загрози і характеру проведених державою заходів по боротьбі з цим явищем. З цією метою доречним є створення специфічної системи антитерористичного освіти школярів, у рамках якої підростаюче покоління засвоює правила поведінки в екстремальних ситуаціях, а також вчиться відрізняти дійсну загрозу від уявної. Така виховно-ідеологічна робота сприймається як досить складна, проте необхідна, оскільки без неї не можна говорити про згуртування зусиль громадянського суспільства та органів держбезпеки.

З ініціативи Державного департаменту Сполучених Штатів було прийнято рішення використовувати професійні знання співробітників в області антитерористичної боротьби і направити їх на підготовку спеціальної програми, розрахованої як на працівників правоохоронних органів, так і на пересічних громадян. Головною метою «антитерористичної програми Держдепартаменту США» є сприяння в забезпеченні безпеки громадян країни як в щоденному режимі (всередині держави), так і під час зарубіжних туристичних і ділових поїздок. Програма носить не тільки інформаційно-навчальний характер, а й містить у собі елемент пропаганди, спрямованої на налагодження контактів з іноземними посадовими особами для досягнення

119 *Національний Контртерористичний центр / The National Counterterrorism Center (NCTC). [Електронний ресурс]. – Режим доступу: <http://www.nctc.gov/overview.html>*

єдиного розуміння загрози і бажання проведення спільної боротьби з тероризмом. За цією програмою пройшли навчання вже більше 20 000 співробітників з більш ніж 100 країн¹²⁰.

Мабуть, найпоказовішим прикладом залучення громадянського суспільства в здійснення протидії тероризму є функціонуюча в Ізраїлі так звана «народна дружина» - одна з найбільших добровольчих організацій, існуючих на сьогоднішній день в цій країні. Народна дружина Ізраїлю є підрозділом ізраїльської поліції і налічує понад 50 000 добровольців, в той час як число штатних поліцейських становить менше 30 000 чоловік. На «дружинників» покладено функцію патрулювання вулиць, торгових центрів, громадського транспорту (найбільш розповсюджений об'єкт терористичних атак в Ізраїлі). При цьому вони офіційно мають право на носіння зброї і застосування її в разі потреби. Участь в даній роботі вважається в Ізраїлі дуже почесним і користується громадським схваленням¹²¹.

Слід зазначити, що поява таких інститутів громадянського суспільства, як «народна дружина» пояснюється не тільки необхідністю превентивних заходів в боротьбі з тероризмом, але також є результатом проведеної в країні широкомасштабної просвітницької роботи з населенням.

Специфічною формою сучасного тероризму є консцієнтальна війна (лат. *conscientia* – свідомість, сумління) – війна на ураження свідомості, руйнування ідентичності, а також самої здатності людини до самоідентифікації. Сьогодні терористичні акти розраховані на спричинення інформаційно-психологічного шоку, вплив якого на великі маси людей створює сприятливу ситуацію для досягнення терористами своїх цілей. Способи впливу на людську свідомість з кожним днем стають все більш різноманітними й діючими завдяки накопиченому досвіду, а також за

120 Об'єднаний центр по запобіганню терористичних загроз /*Terrorist Threat Integration Center (TTIC)* – Режим доступу: <http://www.encyclopedia.com/doc/1G2-3403300752.html>

121 Інформаційний центр ім. генерала Меїра Аміта по вивченню тероризма / *Meir Amit Intelligence and Terrorism Information Center (ITIC)*. [Електронний ресурс]. – Режим доступу: <http://www.terrorism-info.org.il/ru/index.aspx>

рахунок створення спеціальних технологій спілкування, пропаганди і комунікацій¹²².

Здійснення боротьби з тероризмом передбачає пріоритетне використання методів виявлення, попередження та припинення терористичної діяльності з метою адресного силового та психологічного впливу, зокрема, на національні традиції, до складу яких можна включити у тій чи іншій мірі релігію, мову, культуру, світогляд, славні історичні події та інше, оскільки ідейно-світоглядна монолітність зможе забезпечити як стійкий поступальний розвиток так і надійний захист від зовнішніх загроз.

Засоби масової інформації, висвітлюючи терористичну та антитерористичну тематику, мають стати дієвим засобом боротьби з тероризмом в сучасних умовах. Слід враховувати той факт, що вони, з одного боку, своїми діями здатні посилювати страх і паніку серед населення, а з іншого – лише при грамотному підході, можуть виступати засобом профілактики терористичної діяльності, донесення ідей антитерористичного захисту до широкого загалу. Підвищення рівня антитерористичної підготовленості населення набуває також особливого значення в умовах існуючих на сьогодні значних ризиків трансформації тероризму на інші регіони України.

За допомогою інформаційних технологій, заснованих на знанні соціальної психології, можливо формувати громадську думку в напрямку протидії тероризму, сприяти вихованню у свідомості людей неприйняття методів насильства й шантажу й підтримки дій влади, навчання прийомам особистої й колективної безпеки в ситуаціях, пов'язаних з терористичними погрозами. При цьому основний акцент в інформаційній протидії повинен бути зосереджений на профілактичних і пропагандистських заходах,

122 Рижов І.М., Прозоров А.Ю. Перспективи застосування соціально-психологічних технологій протидії тероризму органами СБ України / І.М. Рижов, А.Ю.Прозоров // Наук вісн НА СБ України. – 2016. – № 60. – С.133-143.

дотримання балансу вимушених обмежувальних заходів, покликаних попереджати й протидіяти використанню сучасних комунікацій терористами.

Позитивним прикладом реалізації загально-профілактичних заходів антитерористичного захисту на рівні міждержавних відносин є використання політики стратегічних комунікацій в практиці публічної дипломатії США. З цією метою створений та активно функціонує Центр стратегічних антитерористичних комунікацій (Center for Strategic Counterterrorism Communications), головною метою діяльності якого визначається координація, направлення та інформування уряду США про всю діяльність активних громадських комунікацій, спрямованих на закордонну аудиторію і орієнтованих на боротьбу з проявами екстремізму та терористичної діяльності. Окрім зовнішньодержавного впливу CSCC також здійснює аналіз, оцінку та функції з планування антитерористичної боротьби разом з Національним центром по боротьбі з тероризмом¹²³.

Сьогодні в багатьох країнах широкого поширення набув підхід, відповідно до якого боротьба з тероризмом визнається завданням спецслужб і правоохоронних органів, за якими ця функція закріплена законодавчо. Сучасні умови диктують інші правила: необхідне згуртування всіх сил та засобів суспільства в профілактиці тероризму. Одне із завдань дії національної антитерористичної системи полягає в створенні умов, за яких кожний громадянин і кожна компетентна структура повинні знайти та зайняти своє місце в процесі протидії терористичній загрозі.

Навіть самий поверхневий аналіз власного досвіду та зарубіжної практики демонструє, що активне залучення інститутів громадянського суспільства до національної антитерористичної системи дозволяє істотно підвищити ефективність її роботи, а ефективна реалізація профілактичних заходів з антитерористичного захисту потребує консолідації зусиль владних

123 *Глобальний Центр Взаємодія (Global Engagement Center) / Under Secretary for Public Diplomacy and Public Affairs. [Електронний ресурс]. – Режим доступу: <https://www.state.gov/r/gec/>*

та силових структур, з одного боку, і громадянського суспільства - з іншого. При цьому, роль громадського суспільства в організації загально-профілактичних заходів антитерористичного захисту об'єктів можливих терористичних посягань в умовах гібридно-інформаційних загроз стрімко збільшується.

На сьогоднішній день громадські структури виступають не тільки в ролі об'єкта впливу державних органів, а й суб'єктом підтримання громадського порядку та обізнаності для ефективного забезпечення антитерористичної безпеки. У зв'язку із цим доволі актуальним постає питання розгляду громадського суспільства саме як головного суб'єкта (системоутворюючого елемента) національних антитерористичних систем з реалізації загально-профілактичних заходів антитерористичного захисту.

16. СВІТОВИЙ ДОСВІД У ПРОТИДІ ЗАГРОЗАМ ТЕРОРИСТИЧНОГО ХАРАКТЕРУ ТА РЕКОМЕНДАЦІЇ ДЛЯ УКРАЇНИ

Стан антитерористичної безпеки України, з огляду на проведення масштабної антитерористичної операції, яка проводиться на сході країни, вимагає від держави вдосконалення не тільки вже розроблених механізмів боротьби з тероризмом, а й впровадження передового досвіду країн Європи. Це не тільки ратифікування міжнародних нормативних актів, або використання вже існуючих регулюючих норм із відповідним корегуванням відносно сучасної української терористичної загрози. Це також активізація взаємодії та міжнародного співробітництва у питаннях антитерористичної безпеки, залучення представників закордонних антитерористичних органів та структур, впровадження передового досвіду боротьби з тероризмом.

Україна повинна активно вивчати та впроваджувати у життя європейський досвід та досвід участі країн НАТО в антитерористичній операції щодо боротьби з тероризмом, адекватного реагування на сучасні виклики та загрози національній безпеці. Для цього необхідно вивчати питання інформаційного супроводження спеціальних антитерористичних операцій, ініціювати залучення експертів НАТО, зокрема США та Великобританії, які мають досвід підготовки персоналу до участі в спецопераціях в Афганістані та інших країнах.

У період після нападу 11 вересня 2001 року дослідження проблем тероризму пройшли значну трансформацію та з незначної галузі дослідження проблем безпеки переросли у велику самостійну галузь науки¹²⁴.

¹²⁴ Critical Terrorism Studies: A New research Agenda by Richard Jackson, Marie Smyth, Jeroen Gunning. – New York: Taylor&Francis, 2009. - 274 p.

Слід зазначити, що погляди на терористичну загрозу доволі різноманітні та мають свої особливості залежно від походження науковця та тієї терористичної ситуації, яка складається в його країні.

Так, американський дослідник Томас Москаїтіс вводить таке поняття як «новий тероризм». Вчений стверджує, що військових дій вже недостатньо для ефективної боротьби. Успіх, насамперед, залежить від економічних і політичних реформ у країнах Європи та тісної співпраці представників різних країн у антитерористичних операціях¹²⁵.

Б. Леві та В. Сідель досліджують явище тероризму в аспекті безпеки здоров'я людей та аналізують системи захисту таких важливих для життя та здоров'я людей інфраструктур як водопостачання, громадське харчування та ін.. Основним завданням, на думку авторів, є укріплення інфраструктури системи охорони громадського здоров'я. Існування саме такої системи може дозволити запобігти масштабу масовості діям терористичного характеру¹²⁶.

Проаналізувавши історію розвитку соціуму та охарактеризувавши її у розрізі безпеки, то кожне століття можна оцінити за основними безпековими показниками. Так, якщо ХХ століття можна назвати століттям наймасовішого збройного протистояння – Перша та Друга світові війни, то ХХІ століття – це століття терористичної небезпеки. Під час світових війн були окреслені fronti бойових дій, були відомі сторони військового протистояння. На сьогоднішній день обличчя терористичної небезпеки є варіативним, мінливим від впливу політичних, економічних подій та явищ, впливу релігійних течій.

Терористична небезпека може мати обличчя як релігійного фанатика-одинака, так і цілої розгалуженої системи терористичних груп та організацій. Джерело небезпеки непостійне і як тільки знаходиться та впроваджується

¹²⁵ The "new" terrorism: myths and reality by Thomas R. Mockaitis. – New-York: Westport, Conn., 2007. – 176 p.

¹²⁶ Terrorism and public health: a balanced approach to strengthening systems and protecting people, edited by Barry S. Levy, Victor W. Sidel. – Oxford: Oxford University Press, 2007. – 383 p.

конкретна система захисту від впливу терористичних організацій – виявляються все нові і нові засоби розповсюдження так званого віртуального страху, – основної мети діяльності терористичних організацій для його використання як інструменту для досягнення своїх цілей.

Тероризм виявився «топовою» темою порядку денного міждержавних перемовин країн не тільки Європейського Союзу, але й усього світу. Причиною цього стало проведення на території України антитерористичної операції, терористичні напади у Парижі, масштабні збройні конфлікти на території Близького Сходу. Лідери країн Європи – члени ЄС обговорюють ряд спільних тем та заходів, які необхідно реалізувати у рамках національних антитерористичних систем.

Після терактів у Лондоні, Мадриді, Парижі стало зрозумілим, що з метою попередження вчинення терактів у майбутньому держави-члени ЄС повинні активізувати своє співробітництво. Основною метою антитерористичних заходів, які плануються в ЄС, є забезпечення для громадян усіх країн європейської співдружності можливості жити в умовах свободи, миру та безпеки. Задача згуртованості зусиль покладається першочергово на громадське суспільство, так як необхідні законодавча та технічна бази вже створені. Однак в екстрених ситуаціях, коли небезпека терористичної діяльності переходить в активну фазу, а саме безпосереднє вчинення терористичного акту, який загрожує життю та здоров'ю великій кількості населення або й усій державі в цілому, країна веде антитерористичну роботу самостійно.

Метою публічної дипломатії США є підтримка досягнення державою зовнішньополітичних цілей та задач, просування національних інтересів та укріплення національної безпеки шляхом інформування та впливу на міжнародне суспільство, а також шляхом розширення та укріплення відносин

між суспільством, Урядом Сполучених Штатів Америки та громадянами інших країн¹²⁷.

Окрім зміцнення та налагодження зовнішніх відносин публічна дипломатія США спрямовується і на забезпечення антитерористичної безпеки шляхом використання стратегічних комунікацій.

Стратегічна комунікація (strategic communication) являє собою комплекс заходів, які реалізуються Міністерством оборони та іншими державними органами Сполучених Штатів Америки з метою інформаційного впливу на зарубіжне суспільство¹²⁸.

У більш широкому розумінні «стратегічні комунікації» полягають у цілеспрямованому впливі органів державної влади США на інформаційне суспільство (суспільство, в якому інформація і знання продукуються в єдиному інформаційному просторі¹²⁹ з метою створення та забезпечення сприятливих умов для реалізації зовнішньої політики. Проте не слід ототожнювати стратегічні комунікації із односторонніми формами впливу на аудиторію. Основна відмінність полягає у тому, що стратегічні комунікації мають діалоговий характер, тобто забезпечують двосторонній обмін інформацією, в той час як традиційний односторонній вплив спрямований лише на її поширення.

Вперше концепція стратегічних комунікацій законодавчо закріплюється в Указі Президента США Б. Обама 09 вересня 2011 року. Цим Указом була затверджена розробка комплексної ініціативи зі стратегічних комунікацій, націленої на боротьбу з проявами тероризму як на території США, так і за її межами. Оскільки цей Указ був прийнятий у відповідь на зростаючі терористичні загрози, насамперед в середині США, то й терористична загроза постає в особі Аль-Каїди.

¹²⁷ [/https://www.state.gov/r/index.htm/](https://www.state.gov/r/index.htm/)

¹²⁸ [/https://ru.wikipedia.org/wiki/Стратегическая_коммуникация/](https://ru.wikipedia.org/wiki/Стратегическая_коммуникация/)

¹²⁹ https://uk.wikipedia.org/wiki/Інформаційне_суспільство/)

Стратегічні комунікації спрямовані на протидію ідеології тероризму та екстремізму шляхом розповсюдження та обміну інформацією, яка покликана позитивно впливати на елементи населення, сприятливого до радикалізації, вербування терористичними організаціями та схильного до сугестивності.

З метою координації та здійснення зовнішньої політики США у сфері стратегічних комунікацій був створений Центр стратегічних антитерористичних комунікацій (Center for Strategic Counterterrorism Communications). Головною метою діяльності CSCC визначається координація, направлення та інформування уряду США про всю діяльність активних громадських комунікацій, спрямованих на закордонну аудиторію і орієнтованих на боротьбу з проявами екстремізму та терористичної діяльності. Проте окрім зовнішньодержавного впливу CSCC також здійснює аналіз, оцінку та функції з планування антитерористичної боротьби разом з Національним центром по боротьбі з тероризмом¹³⁰.

Можна виділити такі основні напрямки діяльності CSCC:

- моніторинг і оцінка подій за кордоном, які можуть мати загрозу для державної безпеки та інтересів США;
- розробка та реалізація стратегій роботи з громадськістю для протидії проявам екстремізму та тероризму;
- виявлення та відслідковування тенденцій до проявів терористичної загрози безпеці США;
- сприяння використанню сучасних комунікаційних технологій, обміну та застосування передового досвіду, залучення фахівців з інших установ та відомств;
- виявлення та виправлення недоліків роботи CSCC, а також інших урядових організацій спрямованих на боротьбу з тероризмом.

З метою впровадження заходів у сфері суспільної комунікації, спрямованих проти насильницького екстремізму, сприяння діяльності та фінансуванню терористичних організацій та інших дій, які можуть

¹³⁰ <https://www.state.gov/r/gec/>

загрожувати безпеці США, було створено Управління з підтримки антитерористичних комунікацій (Counterterrorism Communications Support Office).

CCSO здійснює функції з:

- дослідження цільових аудиторій за кордоном;
- сприяння інформаційній боротьбі проти закордонних терористичних організацій;
- розроблення та реалізація цілеспрямованих інформаційних кампаній у соціальних мережах.

З метою конкретизації практичного застосування стратегічних комунікацій у сфері публічної дипломатії США, а також у світлі постійного розповсюдження та мінливості терористичної загрози Президентом США Б. Обамою 14 березня 2016 року був підписаний новий Указ.

Для здійснення координації діями урядових організацій у сфері комунікаційної діяльності спрямованої на іноземні аудиторії для попередження та зменшення впливу міжнародних терористичних організацій (ІДІЛ, Аль-Каїда та інших агресивно налаштованих іноземних екстремістських угруповань) був заснований Центр міжнародної співучасті (Global Engagement Center)¹³¹.

Серед основних обов'язків, які покладаються на ГЕС виділяють:

- координація та супроводження усіх зв'язків уряду США з громадськістю;
- цілеспрямований вплив на закордонну аудиторію з метою зменшення впливу на них терористичних організацій;
- розробка та реалізація стратегій по боротьбі з тероризмом;
- залучення до співучасті установ, організацій, громадських організацій, фахівців з метою сприяння уряду США у забезпеченні антитерористичної безпеки;

¹³¹ / <https://www.state.gov/r/pa/prs/ps/2016/07/259376.htm/>

- пошук, виявлення та залучення найкращих науковців для підтримки виконання функцій GEC;
- пошук та виправлення недоліків роботи GEC, вдосконалення роботи Центру;
- підтримка мережі урядових та неурядових організацій, партнерів з метою обміну інформацією.

Керівництво GEC здійснює секретар, який створює керівний комітет, до складу якого входять представники таких відомств: Міністерство оборони, Міністерство юстиції, Міністерство внутрішньої безпеки, Міністерство фінансів, Управління у справах малого бізнесу, Національний центр по боротьбі з тероризмом, Об'єднаний комітет начальників штабів, Антитерористичний центр Центрального розвідувального управління, Агентство США з міжнародного розвитку. Також за рішенням секретаря до складу GEC можуть бути запрошені й інші фахівці.

Слід зазначити, що поряд із GEC була запроваджена тимчасова організація – Координаційний офіс Центру міжнародної співучасті (Global Engagement Center Coordination Office), метою створення якого було надання ним технічної, управлінської, оперативної підтримки GEC, а також здійснення досліджень з оцінки діяльності GEC.

При аналізі процесу розвитку антитерористичних структур і практичної боротьби з тероризмом у Європейському Союзі можна виокремити як безсумнівні досягнення антитерористичного курсу, так і об'єктивні його слабкості.

Здійснивши аналіз міжнародного співробітництва в боротьбі з тероризмом в рамках Європейського Союзу, слід зазначити, що були створені інструменти боротьби з тероризмом та розроблені й прийняті такі нормативні документи, як¹³²:

1. ¹³² Рижов І.М., Сігарьов С.С., Гавлилюк К.І. Антитерористична безпека: досвід країн ЄС / І.М.Рижов, С.С.Сігарьов, К.І. Гавлилюк // Збірник наукових праць НА СБ України. – 2016. – № 60. – С.108-115.

- Європейська конвенція про ліквідацію тероризму і Протокол з поправками;
- Європейська конвенція про екстрадицію, перший і другий Додаткові протоколи;
- Європейська конвенція про надання судової взаємодопомоги з кримінальних справ і перший і другий Протоколи;
- Європейська конвенція про передачу судових матеріалів;
- Європейська конвенція про компенсацію жертвам злочинів із застосуванням насильства;
- Європейська конвенція про відмивання грошей, пошук, арешт та конфіскацію доходів від злочинної діяльності;
- Європейська конвенція про кібер-злочинність і Додатковий протокол щодо судового переслідування актів расистського і ксенофобного характеру, які здійснюються за допомогою комп'ютерних систем.

Комітетом Міністрів Ради Європи, як інструмент боротьби з тероризмом, були прийняті такі документи, як:

- Декларація про тероризм (1978 р.);
- Тристороння декларація про терористичні акти (1986 р.);
- Резолюція про міжнародний тероризм;
- Рекомендація про міжнародне співробітництво в галузі переслідування терористичних актів і покарання за них, а також Меморандум;
- Рекомендація про основні принципи в боротьбі з організованою злочинністю (2001 р.);
- Декларація про боротьбу з міжнародним тероризмом (2001 р.);
- Основні принципи у сфері прав людини і тероризму (2002 р.);

Ситуація терористичної небезпеки, яка складається як у всьому світі, так і у Європейському Союзі зокрема, вимагає від спецслужб принципово нових методів роботи та більш злагоджених дій з іншими державними

органами, інститутами громадського суспільства. Досягненням ЄС у боротьбі з тероризмом можна назвати інтеграцію роботи національних органів безпеки у загальноєвропейську систему, що дозволяє на сьогоднішній день проводити більш злагоджені антитерористичні операції.

Так, у листопаді 2004 року, міністрами внутрішніх справ та юстиції країн ЄС була прийнята Гаагська програма – п'ятирічний план співробітництва у боротьбі з тероризмом, котрий, поряд з Антитерористичною стратегією Європейського Союзу, яка прийнята у листопаді 2005 року, став одним з основних документів, що визначає напрямок інституалізації антитерористичної діяльності у ЄС.

Концентрація зусиль антитерористичних відомств та керуючих органів ЄС по боротьбі з тероризмом в середині Євросоюзу призвело до створення нових антитерористичних структур. Передусім, була сформована система консультативно-експертних органів. Діяльність Комітету експертів по боротьбі з тероризмом (CODEXTER), створеного у 2003 році, дозволила поставити на наукову основу аналіз терористичної загрози та потенціалу силових структур у боротьбі із нею, які базуються на даних, отриманих оперативним шляхом¹³³. Крім того, Комітет експертів почав пропонувати у загальноєвропейському масштабі заходи, які направлені на перекриття доступу терористів до джерел фінансування, а також здійснення захисту, підтримки, виплати компенсацій постраждалим від терористичних актів, оцінку ефективності національних судових систем у протидії тероризму. Також важливу роль у формуванні та розвитку загальноєвропейської спільноти експертів із проблем безпеки зіграло створення у 2002 році Антитерористичного підрозділу ОБСЄ.

Іншим важливим напрямком інституційної боротьби з тероризмом у 2001-2015 рр. стало формування та розвиток єдиного європейського

¹³³ 1090 Meeting, 7 July 2010. 10.1 Committee of Experts on Terrorism (CODEXTER) / Council of Europe. - [Електронний ресурс]. – Режим доступу: <http://www.coe.int/document-library/default.asp?urlwcd=https://wcd.coe.int/ViewDoc.jsp?id=1631017>

правового простору, встановлення єдиних норм судової практики щодо осіб, які звинувачуються у тероризмі. Євроюст, який був сформований у 2001 році, відіграв важливу роль у європейській інтеграції судових установ, встановив низку угод, які дозволяють обмінюватись судовою практикою та анкетними даними між Європолем, Європейським відомством з боротьби із шахрайством, Колледжем європейської поліції, Європейською мережею з навчання співробітників юстиції, а також органами безпеки ряду країн, які не входять до складу Європейського Союзу¹³⁴.

Конкретні успіхи в інституціоналізації боротьби з тероризмом були досягнуті і на національному рівні. Так, після 11 вересня 2001 року французькі силові структури, такі як митниця або жандармерія активізували технічний моніторинг інформації відносно тероризму. У Великобританії у 2003 році була прийнята національна антитерористична стратегія CONTEST, в рамках якої більш суттєвою, порівняно із попередніми періодами, стає роль попередження терористичних актів, передусім, через контакти із «групами ризику», у котрі входять потенційні прихильники терористичних організацій¹³⁵. З 2001 року більш активно приймати участь у загальноєвропейських ініціативах у галузі безпеки почала влада Іспанії. У Німеччині створюються національні аналітичні структури (14 грудня 2004 року почав свою роботу Об'єднаний антитерористичний центр). Разом із тим, національні структури країн Європейського Союзу активно співпрацюють у рамках двосторонніх (або об'єднуючих більшу кількість країн) проектів. Ці та багато інших заходи з розвитку антитерористичних відомств у ЄС свідчать про перехід політики європейської безпеки на новий, дійсно загальноєвропейський шлях розвитку.

¹³⁴ Євроюст – общая правовая характеристика [Електронний ресурс]: Астапенко В., Лойша Д. // Журнал международного права и международных отношений. – 2005. - № 4. – Режим доступу: <http://evolutio.info/content/view/783/113/>

¹³⁵ CONTEST, UK strategy for countering terrorism: annual report for 2014 . - [Електронний ресурс]. – Режим доступу: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/415708/contest_annual_report_for_2014.pdf

Таким чином, була сформована загальноєвропейська система антитерористичних відомств.

Водночас, необхідно відзначити й певні слабкості антитерористичного курсу ЄС. Так, не дивлячись на стрімку і в цілому успішну боротьбу з тероризмом, в країнах Європейського Союзу не були викоренені соціальні фактори збереження терористичної загрози, такі як безробіття, масова міграція з країн Близького Сходу, їх геттоізація.

Додатковим фактором загострення міжнаціональних відносин стала участь військового контингенту ряду країн ЄС у конфліктах на Близькому Сході у 2015 році. Особливо масове перетинання групами населення кордонів сколихнула країни ЄС та змусила їх керівництво обмежити та посилити умови в'їзду. Але дії, які виконуються керівництвами країн ЄС, не гарантують абсолютної неможливості вчинення терористичних актів.

Низький рівень освіти більшості мігрантів, слабкість роботи державних органів з інтеграції мігрантів у більш кваліфіковану трудову діяльність, а також майже повна відмова мігрантів від асиміляції та прийняття місцевих норм культури, моралі та інших встановлених соціальних норм – все це робить їх потенційною цільовою аудиторією терористичної пропаганди, яка апелює до походження спільноти або релігії.

У документах національних та міжнаціональних урядових структур ЄС, поряд із призовом до толерантності по відношенню до представників інших націй, релігій і т.п., головним став заклик до боротьби з «джихадизмом», «ісламізмом», що створює стійку асоціацію релігії з терористичною діяльністю. Провідними експертами у дискусіях з проблем тероризму в ЄС стали саме експерти у галузі релігії. Це управлінське рішення призвело до ефекту, зворотного очікуваному: терористичні організації представили боротьбу з тими або іншими релігійними або політичними течіями, як прояв національної нетерпимості.

Тероризм швидкими темпами активізується і набуває міжнародного характеру. Терористична небезпека висуває перед міжнародним співтовариством гостру необхідність рішуче покінчити з цим явищем.

Важливою рушійною силою у сфері розвитку міжнародно-правової боротьби з тероризмом являє собою розвиток і зміцнення міжнародного співробітництва.

В арсеналі заходів міжнародно-правового характеру, спрямованих на боротьбу з тероризмом на сучасному етапі, міститься:

- повний комплекс правових актів, формування та розвиток єдиного європейського правового простору, встановлення єдиних норм судової практики щодо осіб, які звинувачуються у тероризмі;
- сформування системи консультативно-експертних органів (Комітет експертів по боротьбі з тероризмом);
- прийняття національних антитерористичних стратегій (національна антитерористична стратегія CONTEST у Великобританії);
- створення національних аналітичних структур.

Загальний аналіз заходів, вжитих європейським співтовариством по боротьбі з тероризмом, свідчать про рішучість міжнародного співтовариства покінчити з цим явищем, однак проблема досі залишається актуальною і необхідність її вирішення досить украй необхідна.

Серед конкретних заходів, які, на нашу думку, мають бути втілені владою України для упередження терористичних загроз, а також мінімізування їх наслідків, є:

- інтегрування в українське законодавство такого поняття як «критична інфраструктура» та переліку об'єктів, які мають до неї відноситися. Хоча це поняття неодноразово зустрічається, але досі так і не отримало чіткого визначення в українському законодавстві. Найбільш широке визначення цього терміну дає чинне законодавство Сполучених Штатів Америки, де вказується, що це є перелік життєво важливих об'єктів інфраструктури, пошкодження або знищення яких може загрожувати

національній економічній, політичній безпеці держави, а також життю та здоров'ю населення; [8]

- розробка системи попередження населення про атаки терористів. Як зразок, така система використовується у Великій Британії («Пріоритетна система тривоги»), Ізраїлі та ін.;

- перехід від міждержавного співробітництва тільки в режимі обміну інформацією до уніфікації системи рівнів терористичної загрози та попередження сусідніх держав про підготовки терористичних актів на об'єктах «критичної інфраструктури» (атомні електростанції, посольства, місця громадських та релігійних центрів скупчення населення та ін.);

- застосування основ ризик-менеджменту та його перехід від економічної галузі використання в аспект попередження терористичних загроз. Тобто прогнозування настання умов до вчинення терористичних атак, що дає можливість їх попереджувати, а тому запобігати їх вчиненню. [9]

Методи боротьби з тероризмом можуть бути різними, однак суспільство завжди знаходиться у приблизно одному стані – страху, розчаруванні у діях влади, бажанні перемогти та відвернути майбутню загрозу. Така єдність у прагненні громадян має бути використана владою країн ЄС з метою згуртування сил держав у війні з терором.

Україна знаходиться у стані збройного протистояння, яке із поодиноких терористичних актів переросло у масштабний збройний конфлікт. Головна мета влади країни, на нашу думку, полягає у консолідації зусиль у боротьбі з проявами тероризму та максимальному використанню досвіду країн світу та Європи. Саме досвід є вагомим теоретичною базою та, власне в чому на нашу думку вбачається від цього найбільша користь, - готові результати від його практичного використання. Втілені у життя заходи дають нам можливість впроваджувати найефективніші, найрезультативніші міри та прогнозувати їх наслідки у боротьбі з головною ціллю – небезпекою терористичної діяльності.

17. РЕКОМЕНДОВАНА ЛІТЕРАТУРА.

1. Коростиленко А.В. Визначення у чинному законодавстві України поняття пропаганди та поширення ідеології тероризму // Науковий вісник. – 2011. – № 39. – С. 95-104. Реєстр. № 7176.
2. Ліпкан В.А. Захист національної безпеки України органами внутрішніх справ від тероризму : Автореферат дисертації. – К.: НА СБУ, 2000. – 17 с. Реєстр. № 5141.
3. Методичні рекомендації щодо моніторингу обстановки у державі та підготовки аналітичних документів з актуальних проблем національної безпеки : Навчально-практичний посібник. – К.: ІАУ СБУ, 1998. – 16 с. Реєстр. № 711/кф.
4. Ришов І.М., Кудінов С.С. Цілевизначення та методичні засади ідентифікації об'єктів можливих терористичних посягань. // Збірник наукових праць. – 2015. – № 57. – С. 80-86. Реєстр. № 8000.
5. Цуркан М.О. Розробка методичної бази для дослідження сучасного конфліктного потенціалу України як похідної від якості життя населення. // Державна безпека України. – 2006. – № 3(7). – С. 70-74. Реєстр. № 6433.
6. Давиденко М.О. Особливості використання релігійного чинника спецслужбами іноземних держав в умовах збройної боротьби. // Збірник наукових праць. – 2014. – № 52. – С. 142-146. Реєстр. № 7795.
7. Христенко О., Яцкевич О. Поширення правового радикалізму в Європі. // Вісник СБУ. – 2014. – № 67. – С. 18-33. Реєстр. № 7718.
8. Антипенко В.Ф. Сучасний тероризм та воєнні методи боротьби з ним. // Науковий вісник. – 2001. – № 13. – С. 85-93. Реєстр. № 5384.
9. Козьяков І.М. Підземна споруда як об'єкт антитерористичного захисту: поняття та правові ознаки. // Науковий вісник. – 2012. – № 44. – С. 122-130. Реєстр. № 7383.
10. Коростиленко А.В. Правові аспекти протидії пропаганді та поширенню ідеології тероризму в Україні. // Науковий вісник. – 2010. – № 33. – С. 85-90. Реєстр. № 6880.
11. Коростиленко А.В. Протидія Службою безпеки України пропаганді та поширенню ідеології тероризму: Автореферат дисертації. – К.: НА СБ України, 2013. – 20 с. Реєстр. № 7568.
12. Коростиленко А.В. Шляхи удосконалення правового забезпечення протидії окремим видам терористичної діяльності в Україні. // Збірник наукових праць. – 2013. – № 44. – С. 94-104. Реєстр. № 7501.
13. Коростиленко А.В., Печериця С.В., Тирлич В.Л. Проблемні правові питання, що впливають на ефективність протидії окремим видам

- терористичної діяльності в Україні. // Науковий вісник. – 2012. – № 44. – С. 131-139. Реєстр. № 7383.
14. Крутов В.В. Политический экстремизм и терроризм в современных условиях. // Исламский экстремизм: Материалы семинара 12-15 октября. – К., 2000. – С. 78-81. Реєстр. № 5122.
15. Крутов В.В. Теоретико-правовые и тактико-специальные проблемы борьбы с терроризмом: Диссертация. – К.: Академия СБУ, 1998. – 391 л. Реєстр. № 4668.
16. Крутов В.В. Теоретико-правовые и тактико-специальные проблемы борьбы с терроризмом (опыт системного исследования): Монография. – К.: Изд-во Академия СБУ, 1998. – 284 л. Реєстр. № 4663.
17. Лапутіна Ю.А. Представництво СБУ у безпекових структурах Ради Європи питань боротьби з тероризмом як ефективний механізм реалізації європейського вектору розвитку держави. // Збірник матеріалів науково-практичної конференції., 16 березня 2012 р. – К., 2012. – С. 124-127. Реєстр. № 7282.
18. Ледок С. Об'єкти можливого терористичного спрямування в Україні. // Вісник СБУ. – 2003. – № 2. – С. 31-33. Реєстр. № 5732.
19. Леонов Б.Д. Концептуальні засади запобігання тероризму: монографія. – К.: НА СБУ, 2014. – 364 с. Реєстр. № 7748.
20. Леонов Б.Д. Кримінологічні засади запобігання тероризму: теоретичні та прикладні проблеми. : Автореферат дисертації. – К.: НА СБУ, 2014. – 34 с. Реєстр. № 7754.
21. Леонов Б.Д. Кримінально-правові норми про терористичні злочини: порівняльно-правовий аспект. // Науковий вісник. – 2012. – № 43. – С. 168-177. Реєстр. № 7330.
22. Леонов Б.Д. Правові аспекти протидії фінансуванню тероризму. // Державна безпека України. – 2011. – № 21. – С. 96-100. Реєстр. № 7095.
23. Леонов Б.Д. Терористична злочинність крізь призму теорій походження злочинності. // Науковий вісник. – 2014. – № 51. – С. 138-144. Реєстр. № 7712.
24. Леонов Б.Д. Типологія осіб, які вчиняють терористичні злочини. // Науковий вісник. – 2012. – № 41. – С. 146-153. Реєстр. № 7267.
25. Леонов Б.Д., Богатирьов О.М. Проблеми визначення організацій терористичними. // Науковий вісник. – 2015. – № 55. – С. 143-148. Реєстр. № 7881.
26. Мишко М.Ю. Види сучасного тероризму. // Актуальні питання ОСД СБУ: матеріали науково-практичної конференції, 18 травня 2010 р. – Ч.1. – С. 281-282. Реєстр. № 2300/дск.
27. Морозов О.М. Причини. Визначення та види тероризму. // Збірник наукових праць. – 2003. – № 10. – С. 95-101. Реєстр. № 5887.
28. Мусієнко І.І., Коростиленко А.В. Удосконалення правової регламентації протидії окремим видам терористичної діяльності в Україні. // Збірник наукових праць. – 2013. – № 45. – С. 19-24. Реєстр. № 7550.
29. Мусієнко І.І., Остроухов В.В., Рижов І.М. Екстремізм і тероризм:

- актуальні питання гіпотези соціально-правового дослідження. // Науковий вісник. – 2014. – № 53. – С. 143-151. Реєстр. № 7799.
30. Мусієко І.І., Талалай Д.В. Питання вдосконалення організаційно-правових засад протидії терористичній діяльності. // Збірник наукових праць. – 2014. – № 53. – С. 126-135. Реєстр. № 7817.
31. Найда В.А. Особливості функціонування в Україні загальнодержавної системи боротьби з тероризмом. // Вісник СБУ. – 2013. – № 64. – С. 24-28. Реєстр. № 2694/дск.
32. Напрями розвитку теорії та удосконалення практики участі Збройних Сил України у боротьбі з тероризмом. Використання інноваційних технологій безпеки для забезпечення захисту особового складу та військових об'єктів Збройних Сил України від диверсій та терористичних актів.: Матеріали науково-практичної семінару (23 червня 2005 р., м. Київ). – К.: ННДЦ ОТ 1 ВБУ, 2005. – 127 с. Реєстр. № 1502/дск.
33. Настюк В.Я., Бєлевцева В.В. Проблеми регулювання адміністративно-правового режиму захисту прав людини в умовах протидії тероризму. // Державна безпека України. – 2010. – № 18-19. – С. 32-37. Реєстр. № 6985.
34. Парфіло О.А. Джерела фінансування міжнародного тероризму та їх класифікація. // Державна безпека України. – 2009. – № 15-16. – С. 90-94. Реєстр. № 6737.
35. Парфіло О.А. Питання протидії фінансуванню міжнародного тероризму та легалізації (відмиванню) брудних грошей. // Державна безпека України. – 2009. – № 17. – С. 110-114. Реєстр. № 6843.
36. Парфіло О.А. Поняття фінансування тероризму: правові аспекти. // Державна безпека України. – 2006. – № 2(6). – С. 7986. Реєстр. № 6409.
37. Парфіло О.А. Схеми фінансування тероризму: поняття та характеристика. // Державна безпека України. – 2008. – № 13-14. – С. 123-130. Реєстр. № 6689.
38. Політі А. Нові транснаціональні ризики і європейська безпека: Монографія (переклад з французької). – К., 1997. – 52 с. Реєстр. № 651/кф.
39. Рижев І.М. Базові концепти моніторингу тероризму: монографія. – К.: НА СБУ, 2012. – 247 с. Реєстр. № 7320.
40. Рижев І.М. Віртуальний страх як кримінологічна ознака сучасного тероризму. // Збірник наукових праць. – 2012. – № 41. – С. 161-165. Реєстр. № 7311.
41. Рижев І.М. Застосування соціально-інформаційних технологій у вирішенні основних завдань СБ України із запобігання кризових явищ соціального характеру та протидії тероризму. // Науковий вісник. – 2012. – № 43. – С. 101-107. Реєстр. № 7330.
42. Рижев І.М. Моніторинг тероризму в контексті пріоритетних завдань органів і підрозділів СБУ. // Удосконалення наукової діяльності НА СБУ: проблеми та перспективи: Матеріали конференції, 29 січня 2013 р.,

- м. Київ. – К., 2013. – С. 286-290. Реєстр. № 2635/дск.
- 43.Рижов І.М. Моніторинг тероризму в контексті пріоритетних завдань органів і підрозділів СБУ. // Перспективи діяльності СБУ у сфері запобігання та протидії злочинності. : Матеріали науково-практичної конференції, 31 травня 2013 р., м. Київ. – К., 2013. – С. 280-283. Реєстр. № 7593.
- 44.Рижов І.М. Моніторинг тероризму та пріоритетні завдання органів і підрозділів СБУ. // Науковий вісник. – 2013. – № 47. – С. 98-105. Реєстр. № 7468.
- 45.Рижов І.М. Моніторинг як складова системи боротьби з тероризмом. // Науковий вісник. – 2000. – № 10-11. – С. 51-54. Реєстр. № 5166.
- 46.Рижов І.М. Основи моделювання теророгенності соціальних систем: Монографія. – К.: Вид-во НА СБУ, 2006. – 168 с. Реєстр. № 6368.
- 47.Рижов І.М. Принципи структурно-факторного моделювання тероризму як соціальної системи. // Збірник наукових праць. – 2000. – № 3. – С. 37-40. Реєстр. № 5199.
- 48.Рижов І.М. Проблемні питання контролю за діяльністю державної системи боротьби з тероризмом в Україні. // Науковий вісник. – 2012. – № 40. – С. 69-74. Реєстр. № 7218.
- 49.Рижов І.М. Тероризм як можливий варіант вирішення соціального конфлікту. // Збірник наукових праць. – 2001. – № 4. – С. 9-11. Реєстр. № 5265.
- 50.Рижов І.М. Соціальна віктимність як достатня умова тероризму. // Збірник наукових праць. – 2000. – № 2. – С. 44-45. Реєстр. № 5195.
- 51.Рижов І.М. Сучасні концепції протидії тероризму та напрями їх удосконалення. // Науковий вісник. – 2012. – № 41. – С. 110-115. Реєстр. № 7267.
- 52.Рижов І.М. Сутність тероризму: соціально-філософські розвідки. // Академія – провідний науковий заклад у системі СБУ.: Матеріали II звіт. наукової конференції, 28 січня 2010 р., Ч.2. – К., 2010. – С. 72-77. Реєстр. № 6853/дск.
- 53.Рижов І.М. Теророгенний потенціал: сутність та складові. // Науковий вісник. – 2012. – № 42. – С. 129-135. Реєстр. № 7303.
- 54.Рижов І.М., Авілова Н.О. Проблемні питання наукового забезпечення боротьби з тероризмом. // Удосконалення наукової діяльності НА СБУ: органічна єдність відомчої науки та практики: Матеріали наукової конференції, 10 жовтня 2014 р., м. Київ. – К., 2015. – С. 158-163. Реєстр. № 3025/дск.
- 55.Рижов І.М., Величко М.В., Мірошник М.В., Кирилюк О.С. Перспективи реагування на зовнішні терористичні загрози техногенного характеру. // Збірник наукових праць. – 2015. – № 54. – С. 111-116. Реєстр. № 7874.
- 56.Рижов І.М., Гусейніков Ю.В. Шляхи удосконалення системи стратегічного планування боротьби з тероризмом в Україні. // Збірник наукових праць. – 2011. – № 40. – С. 87-92. Реєстр. № 7179.
- 57.Рижов І.М., Кудінов С.С. Актуальні питання формалізації об'єктів

- можливих терористичних посягань. // Науковий вісник. – 2015. – № 56. – С. 93-100. Реєстр. № 7934.
- 58.Рижов І.М., Кудінов С.С., Авілова Н.О. Тероризм як об'єкт наукових досліджень: проблеми й перспективи. // Науковий вісник. – 2015. – № 55. – С. 149-157. Реєстр. № 7881.
- 59.Рижов І.М. Л.М. Стрельбицька М.П. Стрельбицький В.І. Строгий Виклики тероризму в Україні та адекватні концепти державної безпеки: навчальний посібник. – К.: Центр навч., наук. та період. вид. НА СБ України, 2015. – 172 с.
- 60.Тероризм:визначення і сутність : монографія [А.В. Коростиленко, Б.Д. Леонов, І.М. Рижов и др.] під заг. ред. В.В. Крутова, І.І. Мусієнка, В.О. Глушкова. – К. Нац. акад. СБУ. 2015. – 192 с.
61. Рижов І.М. Сепаратизм: сутність, кваліфікація, досвід протидії : огляд / В.В. Остроухов, І.М. Рижов, Л.Г. Глущенко, В.М. Дерновий. – Київ : Нац. акад. СБУ, 2016. – 64 с.
- 62.Рижов І.М. Базові концепти антитерористичної безпеки : монографія / І. М. Рижов ; Нац. акад. Служби безпеки України. - Київ : Нац. акад. СБУ, 2016. – 327 с.
- 63.Рижов І.М., Мусієнко І.І., Глущенко Л.Г., Сігарьов С.С. Антитерористична безпека ЄС у нормативно-правових актах і документах : огляд / І.М.Рижов, І.І.Мусієнко, Л.Г.Глущенко, С.С.Сігарьов. – Київ : Нац. акад. СБУ, 2016. – 176 с.
- 64.Розвадовський О.Б., Розвадовський Б.Л. Класифікація рівнів терористичних загроз та зміст першочергових заходів щодо їх запобігання. // Науковий вісник. – 2015. – № 56. – С. 101-108. Реєстр. № 7934.
- 65.Савчин Я. Районні й міжнародні підрозділи регіональних управлінь СБ України – на лінії захисту національної державності та боротьби з тероризмом. // Вісник СБУ. – 2007. – № 47. – С. 46-50. Реєстр. № 6464.
- 66.Сав'юк О.В. Використання оперативно-розшукових засобів і методів у протидії терористичним актам. // Науковий вісник (МВС). – 2008. – № 1 (Ч.2). – С. 41-49. Реєстр. № 6612.
- 67.Сервецький І.В., Ліпкан В.А. Оперативний пошук ознак, що свідчать про формування, планування та підготовку терористичного акту. // Збірник наукових праць. – 2000. – № 1. – С. 35-40. Реєстр. № 5127.
- 68.Степанов Ю.В., Белянська В.В. Запобігання проявам тероризму в Україні: інформаційні заходи антитерористичної діяльності. // Науковий вісник. – 2013. – № 46. – С. 158-165. Реєстр. № 7465.
- 69.Старожицький С.В. Політичний екстремізм і тероризм та комплекс заходів СБУ спрямованих на боротьбу з ними: Лекція. – К.: НА СБУ, 2002. – 27 арк. Реєстр. № 1530/дск.
- 70.Тарнавський Ю.Є. Щодо необхідності відпрацювання єдиної термінології в антитерористичній діяльності. // Роль і місце спеціальних підрозділів СБУ в державній системі боротьби з тероризмом: Збірник матеріалів науково-практичного семінару № 1, 31 жовтня 2002 р., м. Київ. – К.:

- Вид-во НА СБУ, 2003. – С. 36-39. Реєстр. № 5838.
71. Шевченко О.А. Протидія Служби безпеки України фінансуванню тероризму : Автореферат дисертації. – К.: НА СБУ, 2010. – 20 с. Реєстр. № 6942.
72. Яценко О.О. Шляхи подальшого удосконалення національної законодавчої бази у сфері протидії міжнародному тероризму. // Науковий вісник. – 2012. – № 40. – С. 74-84. Реєстр. № 7218.
73. Журило С. Організація системи антитерористичного захисту об'єктів електроенергетики. // Вісник СБУ. – 2011. – № 58. – С. 31-36. Реєстр. № 7088.
74. Западнюк О.Б. Печериця С.В. Антитерористичне забезпечення міжнародних масових спортивних заходів органами СБ України (теоретико-правові та організаційно-практичні аспекти). // Збірник наукових праць. – 2009. – № 28. – С. 39-49. Реєстр. № 6734.
75. Мусієнко І.І., Гребенюк М.В., Леонов Б.Д. Гібридна війна: проблеми постійного апарату. // Збірник наукових праць. – 2014. – № 53. – С. 156-162. Реєстр. № 7817.
76. Мусієнко І.І., Ришов І.М., Сігарьов С.С. Антитерористична компетенція як фактор національної безпеки України. // Науковий вісник. – 2015. – № 55. – С. 171-177. Реєстр. № 7881.
77. Пахнюк В. Антитерористичне забезпечення фінальної частини Євро-2012. // Вісник СБУ. – 2009. – № 53-54. – С. 58-61. Реєстр. № 6771.
78. Печериця В.В., Ковальчук Г.М. Взаємодія органів СБ України із засобами масової інформації під час проведення антитерористичної операції. // Науковий вісник. – 2012. – № 42. – С. 136-144. Реєстр. № 7303.
79. Плетньов О.В. Службово-бойова діяльність Служби безпеки України при проведенні антитерористичних заходів. : Автореферат дисертації. – Одеса: ОДУВС, 2013. – 18 с. Реєстр. № 7607.
80. Ришов І.М. Особливості діяльності СБ України у десепаратизованих зонах після проведення активної фази антитерористичної корупції. // Збірник наукових праць. – 2014. – № 52. – С. 120-126. Реєстр. № 7795.
81. Ришов І.М. Особливості формування акмеологічного потенціалу антитерористичної діяльності. // Збірник наукових праць. – 2014. – № 50. – С. 114-120. Реєстр. № 7697.
82. Ришов І.М., Сігарьов С.С., Волошин О.В. Підготовка населення у сфері антитерористичної безпеки як один із шляхів підвищення ефективності боротьби з тероризмом. // Науковий вісник. – 2015. – № 57. – С. 127-135. Реєстр. № 7957.
83. Ришов І.М., Хлань В.Г., Мірошник М.В. Досвід Федеративної Республіки Німеччини з формування концепції антитерористичного захисту критичної інфраструктури. // Збірник наукових праць. – 2014. – № 51. – С. 134-140. Реєстр. № 7737.
84. Слючарчук І.В., Авдошин І.В. Методологічні проблеми антитерористичної операції крізь призму права збройних конфліктів. // Збірник наукових праць. – 2014. – № 52. – С. 126-136. Реєстр. № 7795.

- 85.Талалай Д.В. Завдання і функції Антитерористичного центру при СБ України: постановка проблеми. // Збірник наукових праць. – 2013. – № 47. – С. 78-85. Реєстр. № 7595.
- 86.Українчук О.В. Можливі ознаки фінансування тероризму в діяльності юридичних осіб під час проведення АТО. // Науковий вісник. – 2014. – № 53. – С. 182-194. Реєстр. № 7799.
- 87.Чеховська М.М., Шлапаченко В.М. Захист об'єктів інфраструктури залізничного транспорту в умовах проведення антитерористичної операції. // Науковий вісник. – 2015. – № 56. – С. 133-141. Реєстр. № 7934.
- 88.Шамара О.В. Шляхи удосконалення антитерористичного законодавства України. // Науковий вісник. – 2012. – № 40. – С. 154-164. Реєстр. № 7218.
- 89.Шамара О.В. Шляхи удосконалення антитерористичного законодавства України в контексті протидії пропаганді і поширенню ідеології тероризму. // Збірник наукових праць. – 2011. – № 38. – С. 136-142. Реєстр. № 7041.
- 90.Шутий А.С. Запобігання органами СБ України підривній діяльності членів та прибічників закордонних терористичних організацій. // Актуальні питання ОСД СБУ: матеріали науково-практичної конференції, 18 травня 2010 р., – Ч.2. – С. 164-167. Реєстр. № 2301/дск.
- 91.Яценко О.О. Міжнародні антитерористичні операції та оцінка їх ефективності. // Актуальні питання ОСД СБУ: матеріали науково-практичної конференції, 18 травня 2010 р., – Ч.2. – С. 171-175. Реєстр. № 2301/дск.
- 92.Абсалямов О.Г. Практика организации контрразведывательной работы по противодействию проявлениям экстремизма, предупреждению и пресечению противоправной деятельности со стороны представителей политизированных объединений КТНД радикальной направленности и этнических криминальных группировок. // Исламский экстремизм: Материалы семинара. – К., 2000. – С. 103-109. Реєстр. № 5122.
- 93.Веденєєв Д.В. Діяльність спецпідрозділів угруповань екстремістської спрямованості як фактор загрози національній безпеці України. // Збірник наукових праць. – 2003. – № 10. – С. 110-114. Реєстр. № 5887.
- 94.Іваненко С., Афонін О. Скінхеди: З практики організації протидії проявам ксенофобії. // Вісник СБУ. – 2008. – № 51. – С. 22-27. Реєстр. № 6628.
- 95.Косьмій В.М. Організація контррозвідувальної діяльності по недопущенню екстремістських та інших протиправних дій з боку радикально налаштованих осіб з числа кримських татар. // Кримськотатарська проблема в контексті національної безпеки України: оцінки і прогноз ситуації: Матеріали науково-практичної конференції. – К., 2000. – С. 10-18. Реєстр. № 5165.
- 96.Потієвський С., Березницький Є. Діяльність міжнародної релігійно-екстремістської організації "Хізб ут-Тахрір аль-Ісламі". // Вісник СБУ. – 2014. – № 65. – С. 40-46. Реєстр. № 7686.

97. Семенюк О.Г. Запобігання тероризму Службою безпеки України. : Автореферат. – К.: НА СБУ, 2010. – 21 с. Реєстр. № 6862.
98. Ткачов І.В. Стан та перспективи дослідження проблем боротьби з тероризмом. // Академія – провідний науковий заклад у системі СБУ.: Матеріали II звіт. наукової конференції, 28 січня 2010 р., м. Київ. – Ч.2. – К., 2010. – С. 34-38. Реєстр. № 6853/дск.
99. Федосов Е.В. Організація і тактика боротьби оперативних підрозділів МВС України із кримінальним екстремізмом. – К.: НА ВС МВС, 2014. – 20 с. Реєстр. № 7794.
100. Філь П.І. Актуальні проблеми захисту національної державності України, протидії спробам іноземного втручання в її внутрішні справи, боротьби з екстремізмом та тероризмом. : Лекція. – К.: НА СБУ, 2007. – 19 с. Реєстр. № 6498.
101. Бо Форссберг Угруповання, які підтримують ідеологію "Аль-Каїди", та Сирія. // Вісник СБУ. – 2013. – № 64. – С. 56-58. Реєстр. № 2694/дск.
102. Щербина А.В. Поширення радикалізму та екстремізму в сучасному молодіжному середовищі як загроза національній безпеці України. // Збірник наукових праць. – 2014. – № 53. – С. 135-140. Реєстр. № 7817.
103. Пудрій О.О. Удосконалення правового врегулювання протидії органів СБ України пропаганді і поширенню ідеології неонацизму. // Актуальні питання ОСД СБУ: матеріали науково-практичної конференції, 18 травня 2010 р., – Ч.2. – С. 48-52. Реєстр. № 2301/дск.
104. Строяновський В.В. Протидія СБ України сепаратизму та намаганням автоматизації за етнічними ознаками окремих регіонів України. : Лекція. – К.: НА СБУ, 2015. – 28 арк. Реєстр. № 2993/дск.
105. Щербина А.В. Нормативно-правове забезпечення діяльності органів СБ України з протидії молодіжним радикальним організаціям. // Науковий вісник. – 2014. – № 53. – С. 152-156. Реєстр. № 7799.
106. Щербина А.В. Протидія органів СБ України протиправній діяльності неформальних праворадикальних структур. // Збірник наукових праць. – 2014. – № 52. – С. 136-141. Реєстр. № 7795.
107. Баланда А.Л. Соціально-економічні детермінанти протесаної поведінкової стратегії населення України. // Збірник наукових праць. – 2010. – № 37. – С. 13-20. Реєстр. № 6964.
108. Западнюк О.Б. Щодо окремих правових аспектів забезпечення правопорядку під час проведення міжнародних масових спортивних заходів (на прикладі УЄФА/ЄВРО 2008-2012). // Актуальні питання адаптації діяльності органів і підрозділів СБУ до роботи в умовах нового КПК: матеріали науково-практичної конференції, 25 квітня 2014 р. – К., 2014. – С.55-59. Реєстр. № 2819/дск.
109. Погорецький М.А., Сергеев Д.Б., Чорний Р.Л. Розслідування масових заворушень: кримінально-правові, кримінально-процесуальні та криміналістичні аспекти. : навчальний посібник за ред. професора М.А.Погорецького. – К.: НА СБУ, 2015. – 155 с. Реєстр. № 3059/дск.
110. Пономарев В.П. Основні фактори виникнення масових беспорядків. //

- Науковий вісник. – 1993. – № 1. – С. 50-58. Реєстр. № 340.
111. Дідик О.В. Оперативний розшук і пошук у процесі встановлення авторів, виконавців і розповсюджувачів анонімних документів. // Збірник наукових праць. – 2010. – № 33. – С. 18-23. Реєстр. № 6817.
112. Дідик О.В. Профілактика злочинів антиконституційного характеру, погрози вчинення яких надходять анонімно. // Науковий вісник. – 2010. – № 32. – С. 75-82. Реєстр. № 6848.
113. Колосков В.В. Некоторые вопросы противодействия политическому экстремизму и терроризму. // Исламский экстремизм: Материалы семинара 12-15 октября. – К., 2000. – С.81-86. Реєстр. № 5122.
114. Старожицький С.В. Організація розшуку авторів і розповсюджувачів анонімних документів. : навчальний посібник. – 3-є видання, перероблене і доповнене. – К.: НА СБУ, 2014. – 305 с. Реєстр. № 2918/дск.
115. Хома М.Я., Старожицький С.В. Особливості розшуку авторів і виконавців анонімних документів, що поширюються через Інтернет. // Науковий вісник. – 2008. – № 28. – С. 83-90. Реєстр. № 6593.
116. Богданов А., Петрик В. Межконфессиональные конфликты: причины возникновения и пути решения. // Вестник СБУ. – 1999. – № 3-4. – С.148-152. Реєстр. № 5112.
117. Гринько В.В. Вживання спеціальної термінології у роботі органів та підрозділів СБ України по лінії протидії загрозам національній безпеці України у релігійній сфері. // Науковий вісник. – 2007. – № 27. – С. 12-14. Реєстр. № 6462.
118. Гринько В.В. Організація діяльності СБ України по лінії протидії загрозам національній безпеці у релігійній сфері. : Практичний посібник. – К.: НА СБУ. – 2007. – 96 с. Реєстр. № 6523.
119. Гринько В.В. Релігійний тероризм: тенденції розвитку та шляхи протидії його проявам. : Навчальний посібник. – К., НА СБУ. – 2007. – 52 с. Реєстр. № 1786/дск.
120. Давиденко М.О. Використання релігійного чинника в проведенні Російською Федерацією розвідувально-підривної діяльності на території України. // Сучасні виклики і загрози – проблеми контррозвідувальної діяльності СБУ. : Матеріали круглого столу 25 червня 2014 р. – К., 2014. – С. 266-268. Реєстр. № 7727.
121. Давиденко М.О. Діяльність закордонних клерикальних центрів: вплив на релігійну ситуацію в Україні в умовах проведення антитерористичної операції. // Збірник наукових праць. – 2015. – № 55. – С. 126-133. Реєстр. № 7911.
122. Давиденко М.О. Особливості використання релігійного чинника спецслужбами іноземних держав в умовах збройної боротьби // Збірник наукових праць. – 2014. – № 52. – С.142-146. Реєстр. № 7795.
123. Давиденко М.О. Проблеми діяльності підрозділів захисту національної державності по попередженню конфліктів на релігійному ґрунті в Україні. // Актуальні питання адаптації діяльності органів і підрозділів

- СБУ до роботи в умовах нового КПК.: Матеріали науково-практичної конференції, 25 квітня 2014 р., м. Київ. – К. – 2014. – С. 29-232. Реєстр. № 2819/дск.
124. Давиденко М.О. Роль і місце СБ України в попередженні і припиненні конфліктів на релігійному ґрунті в Україні. // Науковий вісник. – 2014. – № 50. – С. 151-155. Реєстр. № 7637.
125. Давиденко М.О. Сучасні особливості протидії органів СБ України закордонним клерикальним центрам США. // Збірник наукових праць. – 2014. – № 50. – С. 109-114. Реєстр. № 7697.
126. Етноконфесійна складова національної безпеки: загрози суверенітету та територіальній цілісності. // Матеріали науково-практичної конференції, 29 листопада 2011 р., м. Київ. – К.: НА СБУ, 2012. – 177 с. Реєстр. № 7219.
127. Петрик В.М. Захист національної безпеки від антиконституційних дій представників деструктивних неокультурів. : Навчальний посібник. – К.: НА СБУ. – 2002. – 92 с. Реєстр. № 5509.
128. Петрик В.М. Захист українського суспільства від антиконституційних дій з боку представників неокультурів. // Науковий вісник. – 1999. – № 9. – С. 105-110. Реєстр. № 5094.
129. Ткач С. Особливості боротьби з міжнародним релігійним тероризмом. // Вісник СБУ. – 2002. – № 1. – С. 71-75. Реєстр. № 5497.
130. Ткач С.П. Підрозділи захисту національної державності – основні структурні ланки системи СБУ по недопущенню використання релігійного фактора як засобу підриву національної безпеки України. // Збірник наукових праць. – 2000. – № 3. – С. 40-46. Реєстр. № 5199.
131. Ярмоленко П.П. Організація роботи по протидії антиукраїнській діяльності зарубіжних клерикальних і єврейських центрів. // Матеріали семінару-наради у Криму 22-23 березня 1995 р. – К.: Управління «Т». – 1995. – С. 70-74. Реєстр. № 3831.
132. Ярмоленко П.П. Особливості організації роботи по виявленню та запобіганню розпалювання міжнаціональної та міжконфесійної ворожнечі, проявів сепаратизму. // Матеріали семінару-наради у Криму (22-23 березня 1995 р.). – К.: Упр. "Т", 1995. – С. 75-83. Реєстр. № 3831.
133. Назаров Н. Некоторые вопросы теории и практики борьбы с терроризмом. // Вестник СБУ. – 1995. – № 3-4. – С. 124-130. реєстр. № 3820.
134. Рижов І.М., Хлань В.Г., Петриченко В.Г. Інформаційно-аналітичне супроводження врегулювання кризових явищ соціального характеру. // Науковий вісник. – 2014. – № 51. – С. 56-63. Реєстр. № 7712.
135. Рижов І.М. Перспективи формування уніфікованого інформаційного середовища у сфері протидії загрозам терористичного характеру / І.М. Рижов // Інформаційна безпека людини, суспільства, держави. – 2014. – №3(16) . – С.56-62
136. Композитна стратегія протидії мережевим та гібридним викликам сучасного тероризму / Леонов Б.Д., Рижов І.М. // Правова інформатика

- 2013. – № 1(45)/2015 – С.68-74.
137. Рижов І.М. Перспективи реагування на зовнішні терористичні загрози техногенного характеру / І.М. Рижов, М.В. Величко, О.С. Кирилюк/ Зб. наук. пр. НА СБ України. – 2015. – № 54. – С.111-117. – Інв. № . – Таємно.
138. Рижов І.М. Особливості нормативно-правового регулювання профілактики тероризму / І.І. Мусієнко, І.М. Рижов, А.В. Коростиленко/ Зб. наук. пр. НА СБ України. – 2015. – № 54. – С.99-105. – Інв. № . – Таємно.
139. Рижов І.М. Тероризм як об'єкт наукового дослідження: проблеми й перспективи/ С.С. Кудінов, І.М., І.М. Рижов, П.О. Авілова/ Наук вісн НА СБ України. – 2015. – № 55. – С.149-158. – Інв. № . – Таємно
140. Рижов І.М. Антитерористична компетенція як фактор національної безпеки України / І.І. Мусієнко, І.М. Рижов, С.С. Сігарьов/ Наук вісн НА СБ України. – 2015. – № 55. – С.149-158. – Інв. № . – Таємно
141. Рижов І.М. І.І. Мусієнко О.С. Войтюк Негласна профілактика тероризму: погляд сьогодення / Мусієнко І.І., Рижов І.М., Войтюк О.С. Збірник наукових праць НА СБ України. – 2015. – № 55. – С.119-125.
142. Рижов І.М. С.С. Кудінов Актуальні питання формалізації об'єктів можливих терористичних посягань Науковий вісник НА СБ України. – 2015. – № 56. – С. 93-101.
143. Рижов І.М., Сігарьов С.С., Волошин О.В. Підготовка населення в сфері антитерористичної безпеки як один із шляхів підвищення ефективності боротьби з тероризмом / С.С.Сігарьов, О.В.Волошин, І.М.Рижов // Наук вісн НА СБ України. – 2015. – № 57. – С.121-127.
144. Рижов І.М., Строгий В.І. Актуальні проблеми антитерористичної підготовки громадянського суспільства / І.Рижов, В.Строгий// Науковий вісник Львівського державного університету внутрішніх справ:Серія юридична. – 2015, – №1, С. 348-355.
145. Рижов І.М., Строгий В.І. Формування здатності громадянського суспільства протистояти тероризму / І.Рижов, В.Строгий // Науковий вісник Львівського державного університету внутрішніх справ:Серія юридична. – 2015, – №3, С. 318-325.
146. Рижов І.М., Строгий В.І. Стратегії боротьби з тероризмом в умовах урегулювання кризових ситуацій соціального характеру/ І.Рижов, В.Строгий// Митна справа. – 2013. № 2. – Частина 2, книга 1. – С.70-77.
147. Рижов І.М., Кудінов С.С. Цілевизначення та методичні засади ідентифікації об'єктів можливих терористичних посягань/ С.С. Кудінов, І.М., І.М. Рижов / Збірник наукових праць НА СБ України. – 2015. – № 55. – С.80-87.
148. Рижов І.М., Мусієнко І.І. Варенье Н.М. Теоретичні засади соціальної детермінації ризиків та загроз терористичного характеру/ І.М. Рижов, І.І. Мусієнко, Н.М. Варенье // Наук вісн НА СБ України. – 2015. – № 58. – С.108-115.
149. Рижов І.М., Кудінов С.С. Проблемні аспекти інтелектуального

- забезпечення інноваційного розвитку боротьби з тероризмом / І.М.Рижов, С.С. Кудінов // Наук вісн НА СБ України. – 2015. – № 58. – С.115-121.
150. Рижов І.М., Кудінов С.С., Глущенко Л.Г. Антитерористичні пріоритети у забезпеченні прав людини Збірник наукових праць НА СБ України / І.М.Рижов, С.С. Кудінов, Л.Г. Глущенко // – 2016. – № 58. – С.85-93.
151. Рижов І.М., Гуськов І.І., Варенья Н.М. Консцієнтальні загрози терористичного характеру / І.М.Рижов, І.І.Гуськов, Н.М. Варенья // Збірник наукових праць НА СБ України. – 2016. – № 58. – С.76-85.
152. Рижов І.М., Волошин О.В. Проблемні питання антитерористичного захисту об'єктів можливих терористичних посягань / І.М.Рижов, О.В.Волошин // Збірник наукових праць НА СБ України. – 2016. – № 59. – С.142-148.
153. Богданович В.Ю., Рижов І.М., Варенья Н.М. Методика оцінювання ефективності протидії загрозам терористичного характеру особі або малій групі людей / В.Ю.Богданович, І.М.Рижов, Н.М.Варенья // Збірник наукових праць НА СБ України. – 2016. – № 59. – С.109-119.
154. Гребенюк М.В., Рижов І.М., Кузьмін С.П. Перспективи інноваційного розвитку антитерористичних стратегій / М.Гребенюк, І.Рижов, С.Кузьмін // Вісник прокуратури. – 2016. – 5 (179). – С.19-28.
155. Рижов І.М. Досвід ФРН з формування концепції антитерористичного захисту критичної інфраструктури / І.Рижов// Бизнес и безопасность. – 2016., – №4. – С.10-12.
156. Богданович В.Ю., Рижов І.М., Варенья Н.М. Концепція побудови системи протидії загрозам терористичного характеру як складової системи забезпечення національної безпеки / В.Ю.Богданович, І.М.Рижов, Н.М.Варенья // Збірник наукових праць НА СБ України. – 2016. – № 60. – С.85-93.
157. Рижов І.М., Сігарьов С.С., Гавлилюк К.І. Антитерористична безпека: досвід країн ЄС / І.М.Рижов, С.С.Сігарьов, К.І. Гавлилюк // Збірник наукових праць НА СБ України. – 2016. – № 60. – С.108-115.
158. Рижов І.М. Актуальні питання технічного регулювання антитерористичного захисту об'єктів можливих терористичних посягань/І.М.Рижов// Збірник наукових праць НА СБ України. – 2016. – № 61. – С.102-110.
159. Богданович В.Ю., Рижов І.М. Модель зв'язків між загрозами терористичного характеру та реакцією суспільства на їх впливи / В.Ю. Богданович, І.М. Рижов // Наук вісн НА СБ України. – 2016. – № 61. – С.105-113.
160. Рижов І.М., Голінко В.В. Щодо питання вдосконалення антитерористичної складової територіальної оборони/ І.М. Рижов, В.В. Голінко // Наук вісн НА СБ України. – 2016. – № 60. – С.127-133.
161. Рижов І.М., Прозоров А.Ю. Перспективи застосування соціально-психологічних технологій протидії тероризму органами СБ України / І.М. Рижов, А.Ю.Прозоров // Наук вісн НА СБ України. – 2016. – № 60.

– С.133-143.

162. Рижов І.М. Глущенко Л.Г Горб В.В. Профілактика тероризму: проблемні питання захисту прав і свобод людини і громадянина / І.М. Рижов, Л.Г. Глущенко, В.В. Горб // Наук вісн НА СБ України. – 2016. – № 61. – С.131-136.
163. Гелемей М.О. Роль негласного апарату під час виявлення та документування екстремістських виявів, що вчиняються молодіжними угруповування. // Науковий вісник (ВС). – 2013. – № 1(30). – С. 132-140. Реєстр. № 7507.
164. Коростиленко А.В. Шляхи підвищення ефективності використання негласного апарату СБ України у протидії окремим видам терористичної діяльності в умовах проведення АТО. // Науковий вісник. – 2014. – № 53. – С. 176-182. Реєстр. № 7799.
165. Філь П.І., Щербина А.В. Деякі особливості агентурної роботи в радикальних молодіжних угрупованнях // Збірник наукових праць. – 2013. – № 47. – С. 94-101. Реєстр. № 7595.
166. Щербина А.В. Особливості агентурної роботи у середовищі представників неформальних молодіжних угруповань радикальної спрямованості. // Удосконалення наукової діяльності НА СБУ: проблеми та перспективи: Матеріали конференції, 29 січня 2013 р., м. Київ. – К., 2013. – С. 244-250. Реєстр. № 2635/дск.
167. Абсальямов О.Г. Практика организации контрразведывательной работы по противодействию проявлениям экстремизма, предупреждению и пресечению противоправной деятельности со стороны представителей политизированных объединений КТНД радикальной направленности и этнических криминальных группировок. // Исламский экстремизм: Материалы семинара 12-15 октября. – К., 2000. – С. 103-109. Реєстр. № 5122.
168. Богданов О.П., Ваврик Б.Й., Христенко О.Б. Огляд за справою оперативної перевірки «Мінотавр». – К.: НА СБУ, 2001. – 24 с. Реєстр. № 5374.
169. Колодяжний В.С. Дніпропетровські теракти – бій з тінню. // Інформаційний вісник (ОД). – 2015. – № 84. –С. 41-51. Реєстр. № 7980.
170. Колосков В.В., Полусмак А.І., Денисюк О.І. Огляд за справою оперативної розробки «Баунті» (за матеріалами Управління «Т» ДЗНД СБУ). – К.: НА СБУ, 2001. – 27 с. Реєстр. № 5381.
171. Петрик В.М., Ткач С.П. Робота по оперативно-розшукових справах як форма протидії підрозділів СБУ посяганням на національну безпеку України з боку представників закордонних клерикальних центрів.: Лекція. – К.: НА СБУ. – 2000. – 14 арк. Реєстр. № 5231.
172. Печериця С.В. Використання деяких новітніх методів оперативного розшуку осіб, які готують або вчинили терористичний акт. // Сучасний тероризм: витоки, джерела і реалії. : Матеріали засідання «круглого столу», 26 червня 2002 р. – К. – 2002. – С. 90-97. Реєстр. № 5616.
173. Богданов О.П. Застосування криміналістичних методів і засобів щодо

- попередження і профілактики проявів терористичного характеру. // Актуальні питання адаптації діяльності органів і підрозділів СБУ до роботи в умовах нового КПК. : Матеріали науково-практичної конференції, 25 квітня 2014 р., м. Київ. – К., 2014. – С.104-107. Реєстр. № 2819/дск.
174. Вавринчук М., Шмай А., Гапієнко А. Попередження зазіхань на конституційний лад і державний суверенітет. // Вісник СБУ. – 2001. – № 3. – С. 15-18. Реєстр. № 5389.
 175. Дідик О.В. Профілактика злочинів антиконституційного характеру, погрози вчинення яких надходять анонімно. // Науковий вісник. – 2000. – № 32. – С. 75-82. Реєстр. № 6848.
 176. Ємельянов В.П., Ришов І.М. Деякі особливості віктимологічної профілактики тероризму. // Науковий вісник. – 2013. – № 46. – С.136-142. Реєстр. № 7465.
 177. Коростилєнко А.В. Проблеми здійснення Службою безпеки України профілактики терористичної діяльності. // Збірник наукових праць. – 2011. – № 40. – С. 78-87. Реєстр. № 7179.
 178. Коростилєнко А.В. Суспільна небезпечність пропаганди та поширення ідеології тероризму як підстава їх криміналізації. // Науковий вісник. – 2013. – № 47. – С. 152-163. Реєстр. № 7468.
 179. Леонов Б.Д. Особливості спеціально-кримінологічного запобігання тероризму // Збірник наукових праць.- 2013.- №48.- С.148-156. реєстр. № 7613.
 180. Мусієнко І.І., Коростилєнко А.В. Особливості проведення підрозділами СБ України профілактичної безпеки як один із шляхів підвищення ефективності боротьби з тероризмом //Науковий вісник.-2015.-№57.- С.121-127. реєстр. №7957.
 181. Мусієнко І.І., Ришов І.М., Войтюк О.С. Негласна профілактика тероризму: сучасний стан //Збірник наукових праць.-2015.-№55.-С.119-125. реєстр. №7911.
 182. Мусієнко І.І., Ришов І.М., Коростилєнко А.В. Особливості нормативно-правового регулювання профілактики тероризму // Збірник наукових праць.-2015.-№54.-С.99-104. реєстр. №7874.
 183. Вандышев А.С. Взаимодействие органов государственной безопасности и охраны общественного порядка в работе по выявлению и профилактике нелегальных религиозных формирований. С.102-111. реєстр. № 3163.
 184. Онопрієнко В.М. Оперативне попередження антиконституційної діяльності політизованих структур, що сповідують ідеологію фашизму // Теорія та практика ОРД СБУ/ матеріали науково-практичної конференції, 23-24 квітня 1996р./, К.-1996.-С.104-107. реєстр. № 3877.
 185. Печериця С.В. Профілактична діяльність органів СБУ щодо проявів терористичного характеру //Збірник наукових праць.-2003.-№7.-С.70-77. реєстр. №5702.
 186. Печериця С.В., Романов І.В. Попередження терористичних актів і

диверсій на важливих державних та військових об'єктах України під час проведення антитерористичної операції //Науковий вісник .-2014.-№52.- С.163-177. реєстр. №7767.

187. Предупреждение массовых столкновений возникающих на межнациональной и религиозной основе.: Методические рекомендации.-К.-ИПК СБУ.-1992.-20с. реєстр. № 24/дсп.
188. Рижов І.М. Деякі технологічні аспекти профілактики тероризму у сучасному мережевому інформаційному просторі. // Збірник наукових праць.-2012.-№42.-С.106-111. реєстр. №7382.
189. Семенюк О.Г. Запобігання тероризму Службою безпеки України: Автореферат.-К.-НА СБУ.- 2010.- 21 с. реєстр. №6862.
190. Семенюк О.Г. Індивідуальне запобігання терористичній поведінці силами та засобами СБ України // Збірник наукових праць.-2011.-№39.- С.58-66. реєстр. №7107.
191. Серода Д., Назаров М. Социально-экономический аспект профилактики авторов и исполнителей анонимных документов //Вестник СБУ.-1994.- №1.-С.30-32. реєстр. №3703.
192. Трепак В. Межконфессиональные конфликты и их влияние на оперативную обстановку в области //Вестник СБУ.-1997.-№1-2.-С.107-109. реєстр. №4015.
193. Філь П.І. Профілактичні заходи органів СБУ з метою попередження державних злочинів та різних негативних проявів на політичній, національній та релігійній основі, які дестабілізують суспільно-політичну ситуацію в Україні і завдають іншої шкоди інтересам держави: Лекція.-К.-НА СБУ.-2006.-16арк. реєстр. №1656/дск.
194. Ходус Д. Из опыта работы по пресечению деятельности незаконных военизированных формирований //Вестник СБУ.-1997.-№1-2.- С.102-107. реєстр. № 4015.
195. Щербина А.В. Профілактичні заходи органів СБ України з попередження і припинення екстремістської діяльності радикальних молодіжних угруповань //Збірник наукових праць.-2015.-№57.-С.44-49. реєстр. № 8000.
196. Ященко О.О. Напрями удосконалення міжнародного права у сфері попередження терористичних актів на об'єктах авіаційного транспорту // Науковий вісник.-2012.-№42.-С.144-151. реєстр. №7303.
197. Ященко О.О. Попередження Службою безпеки України терористичних актів на об'єктах авіаційного транспорту: Автореферат дисертації.-К.: НА СБУ.-2012.-20с. реєстр. № 7344.
198. Авдошин І.В. Формування принципів організації співробітництва СБУ з іноземними спецслужбами у сфері забезпечення державної безпеки //Удосконалення наукової діяльності НА СБУ: проблеми та перспективи.-Матеріали конференції, 29 січня 2013р, Київ,-К.-2013.- С.99-105. реєстр. № 2635/дск.
199. Гавдьо Ю.Р. Розвиток нових уніфікованих форм міжнародно-правового співробітництва у боротьбі з міжнародним тероризмом // Збірник

- наукових праць.- 2009.-№32.-С.44-50. реєстр. №6787.
200. Гончаров Ю. З досвіду єгипетських правоохоронних органів у сфері боротьби з тероризмом // Вісник СБУ. – 2002.-№3.-С.84-87. реєстр. №5622.
201. Гуцало М. Протидія терористичній загрозі в контексті українсько-польського співробітництва під час проведення фінальної частини чемпіонату Європи – 2012 з футболу //Вісник СБУ .-2011.-№60-61.-С.33-42. реєстр.№7205.
202. Двірний Ю.І. Організація та виконання оперативних заходів при виникненні загрози проведення терористичних актів в багатолюдних місцях або на об'єктах стратегічного значення //Інформаційний вісник (ОД).-2012.-№1(76).-С.37-40. реєстр. № 7226.
203. Журило С. Боротьба з тероризмом – у полі зору експертів ООН і США // Вісник СБУ.- 2008.-№51.-С.77-80. реєстр. №6628.
204. Коваленко С. Взаємодія органів державної влади і Служби безпеки України під час проведення антитерористичної організованої злочинності та тероризму // Збірник наукових праць.- 2001.-№4.-С.95-99. реєстр. №5265.
205. Колосков В.В. Проблеми взаємодії підрозділів СБУ та органів внутрішніх справ по СОП анонімів //Науковий вісник.-2000.-№10-11.-С.45-51. реєстр. №5166.
206. Колосков В.В, Полусмак А.І., Денисюк О.І. Огляд за справою оперативної розробки «Баунті»: за матеріалами Управління «Т» ДЗНД СБУ.-К, НА СБУ.-2001.- 27с. реєстр. №5381.
207. Колосков В.В, Хома В.О. Окремі аспекти використання можливостей інспекторського складу прикордонних військ України у боротьбі з міжнародним тероризмом // Науковий вісник НА ВСУ.-ч.2.-2003.-№2.-С.24-28. реєстр. №5741.
208. Крутов В.В. Теоретико-правовые и тактико-специальные проблемы борьбы терроризмом (опыт системного исследования): Монография.-К, Академия СБУ.- 1998.-284 с. реєстр. №4663.
209. Леонов Б.Д. Міжнародне інституційне співробітництво у сфері боротьби з тероризмом //Науковий вісник.- 2013.-№46.-С.142-149. реєстр. №7465.
210. Мусієнко І.І., Талалай Д.В. Питання вдосконалення організаційно-правових засад протидії терористичній діяльності // Збірник наукових праць.- 2014.-№53.-С.126-135. реєстр. №7817.
211. Печериця В.В., Ковальчук Г.М. Взаємодія органів СБ України із засобами масової інформації під час проведення антитерористичної операції //Науковий вісник.-2012.-№42.-С.136-144. реєстр. №7303.
212. Сосновий В.Й. Взаємодія підрозділів центрального апарату ГУК з УСБУ на місцях, щодо усунення фактів можливого екстремізму в робітничому середовищі // Діяльність неурядових організацій в Україні:Збірник матеріалів.-1999.-С.59-62. реєстр. № 5114.
213. Сотсков О.В., Друзенко І.В. Особливості взаємодії сектору ОД та сектору захисту національної державності Керченського МВ ГУ СБУ в

- АР Крим під час реалізації оперативно-розшукових справ //Інформаційний вісник ОД.-2012.-№2(77).-С.27-34. реєстр. №7318.
214. Ткачов І.В. Співробітництво держав у боротьбі із захопленням заложників (міжнародно-правові аспекти) // Збірник наукових праць.- 2000.-№3.-С.47-56. реєстр. №5199.
215. Ткачов І.В. Участь зовнішньої розвідки у протидії терористичній діяльності //Науковий вісник.- 2003.-№16-17.-С.106-114. реєстр. №5665.
216. Участь Служби зовнішньої розвідки України у боротьбі з тероризмом: актуальні проблеми і перспективи: Матеріали першої міжвідомчої науково-практичної конференції, Київ, 25 жовтня 2007 р. //К.-СЗРУ.- 2008.-194с. реєстр. №6568.
217. Шамара О.В. Участь у боротьбі з тероризмом як одна із функцій зовнішньої розвідки України //Державна безпека України.-2009.-№15-16.-С.104-109. реєстр. №6737.