УДК 351.862.4

І. С. Лавров, С. В. Бєлай

МЕТОДОЛОГІЧНІ ЗАСАДИ ВИВЧЕННЯ ПРОБЛЕМ ЗАХИСТУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Визначено актуальність питання дослідження методологічних засад вивчення проблем захисту об'єктів критичної інфраструктури. Проведено експертне опитування щодо сучасних проблемних питань у сфері захисту об'єктів критичної інфраструктури в Україні. Доведено необхідність розроблення моделей реагування на загрози об'єктам критичної інфраструктури в різних умовах: в особливий період, у мирний час. За результатами експертного опитування сформовано пропозиції щодо поліпшення безпеки об'єктів критичної інфраструктури. Визначено роль і місце Національної гвардії України у виконанні завдань із захисту об'єктів критичної інфраструктури.

Ключові слова: *критична інфраструктура, сектор безпеки й оборони, кризові ситуації, державна безпека, система захисту, експертний аналіз, Національна гвардія України.*

Постановка проблеми. Світові тенденції щодо посилення загроз природного й техногенного характеру, підвищення рівня терористичних загроз, збільшення кількості кібератак і зростання їх складності, а також пошкодження інфраструктурних об'єктів у східних і південних регіонах України внаслідок широкомасштабної збройної агресії російської федерації актуалізують питання захисту систем, об'єктів і ресурсів, які є критично важливими для функціонування і сталого розвитку суспільства, підвищення соціально-економічної стабільності й загалом для забезпечення національної безпеки.

Практично в усіх розвинених країнах світу сьогодні створено національні системи забезпечення безпеки критичної інфраструктури. До 2014 р. Україна перебувала у стані поступової деградації в секторі безпеки й оборони країни, що призвело до відставання на 10–15 років на цьому напрямку від більшості європейських країн і значно більше – від таких провідних країн, як США, Велика Британія та Німеччина.

Міжнародна практика розвитку систем захисту об'єктів критичної інфраструктури в різних країнах світу доводить, що ця проблематика визнається ключовою для забезпечення національної безпеки. Україна так само активно працює над забезпеченням захисту своєї критичної інфраструктури, про що свідчить прийняття низки нормативно-правових актів [1–3]. У цьому аспекті постає завдання з формування системи захисту об'єктів критичної інфраструктури України.

Аналіз останніх досліджень і публікацій. Проблематика захисту об'єктів критичної інфраструктури розглядалась у багатьох наукових дослідженнях як представниками наукової спільноти, так і практиками. Концепцію захисту критичної інфраструктури як елемента загальноєвропейської безпекової політики розробив Д. С. Бірюков [4]. Методологію оцінювання рівня критичності об'єктів критичної інфраструктури опрацював і визначив критерії оцінювання й загрози критичній інфраструктурі Д. Г. Бобро [5, 6]. У межах дисертаційного дослідження за тематикою державного управління забезпеченням безпеки критичної інфраструктури в Україні [7] М. Б. Домарацький підняв питання забезпечення безпеки й підвищення ефективності захисту критично важливих об'єктів на державному рівні [8], нормативного й адміністративного забезпечення державного регулювання критичної інфраструктури в Україні [9] та ін. Сутність і зміст поняття «інфраструктура» в контексті захисту критичної інфраструктури визначив О. П. Єрменчук [10]. Аналітичну доповідь щодо забезпечення координації дій, взаємодії та обміну інформацією в процесі створення державної системи захисту критичної інфраструктури склав С. І. Кондратов [11]. Проблеми та пріоритети державної політики із захисту критичної інфраструктури в умовах гібридної війни досліджував О. М. Суходоля [12].

Таким чином, науковцями і практиками розглянуто значний обсяг проблемних питань захисту об'єктів критичної інфраструктури, однак питанню дослідження методологічних засад вивчення проблем захисту об'єктів критичної інфраструктури не приділялося належної уваги, що й зумовило актуальність дослідження.

Метою статті є визначення проблемних питань захисту об'єктів критичної інфраструктури України, виокремлення найвагоміших і надання рекомендацій щодо їх подальшого вирішення.

Виклад основного матеріалу. Для вивчення сучасних проблемних питань у сфері захисту об'єктів критичної інфраструктури в Україні застосовано метод експертного оцінювання, що є різновидом опитування, де респондентами виступають експерти – фахівці в певній галузі діяльності. Основне призначення метода експертного оцінювання полягає у виявленні найскладніших аспектів досліджуваної проблеми, підвищенні надійності отриманої інформації та висновків. Експертні методи застосовуються для прогнозування якісних і кількісних характеристик, розвиток яких повністю або частково не підлягає математичній формалізації через брак достатньої й вірогідної статистики. Наразі експертне опитування застосовується у вивченні всіх сфер діяльності для діагностики та прогнозування, проєктування, оцінювання стану об'єкта дослідження і прийняття рішення [13].

Формою експертного опитування вибрано разове індивідуальне опитування (анкетування). Анкетування передбачає отримання інформації шляхом письмових відповідей респондентів на систему стандартизованих запитань попередньо підготовлених бланків – анкет [14]. Проведення анкетування засновувалося на ретельному доборі вибірки респондентів – фахівців сфери забезпечення безпеки об'єктів критичної інфраструктури. Такими респондентами стали працівники Служби безпеки України, Національної гвардії України, Управління державної охорони України, Збройних Сил України, Державної прикордонної служби України, Державної служби України з надзвичайних ситуацій, Національної поліції України, які мали практичний досвід організації виконання завдань із захисту об'єктів критичної інфраструктури. Загальна вибірка становила 409 респондентів, анкети між представниками складових сектору безпеки й оборони розподілялися пропорційно.

На початку експертного опитування було проаналізовано рівень кваліфікації респондентів, за результатами аналізу встановлено професійну відповідність респондентів сфері забезпечення безпеки об'єктів критичної інфраструктури. Термін проходження служби: найбільша кількість опитуваних (37 %) – більше 16 років досвіду; 27 % – від 11 до 15 років; 24 % – від 6 до 10 років; 12 % опитуваних мають досвід до 5 років. Віковий поділ: найбільша частка респондентів (39 %) старше 36 років; 28 % – від 31 до 35 років; 25 % – від 26 до 30 років; 8 % – до 25 років. Теоретичний рівень підготовки респондентів у сфері захисту об'єктів критичної інфраструктури: більшість має вищу освіту (67 %), інша частина – середньо-спеціальну та відповідну фахову підготовку. Для проведення експертного опитування було розроблено анкету, яка містила 27 запитань. Розглянемо детальніше результати опитування.

На запитання анкети «Як Ви отримали знання про характер і особливості виконання завдань з захисту об'єктів критичної інфраструктури?» 28 % респондентів вказали заклади освіти. Значна частина (28 %) респондентів – фахівців із захисту об'єктів критичної інфраструктури, набули основні знання й навички у сфері безпеки під час службової підготовки в різних установах і безпосередньо під час здійснення завдань. Важливу роль у наданні знань щодо захисту критичної інфраструктури відігравали також освітні заклади.

На запитання «Чи досить було знань для виконання завдань з захисту об'єктів критичної інфраструктури?» найбільше респондентів відповіли «Так» (65 %). Отже, значна частина фахівців із різних складових сектору безпеки й оборони, хто виконує завдання із захисту об'єктів критичної інфраструктури, вважає, що їхніх знань достатньо для виконання повноважень у цій сфері. Це може свідчити про ефективність процесу навчання й підготовки, а також про стабільність рівня кваліфікації працівників у галузі державної безпеки.

На запитання анкети «Які утруднення Ви зустріли при виконанні завдань з захисту об'єктів критичної інфраструктури?» респонденти зазначили про низку труднощів під час виконання своїх завдань. Ішлося зокрема про таке: недостатнє правове забезпечення діяльності (17 %); відсутність міжвідомчої взаємодії (26 %); брак інформації про явище (19 %). У фахівців, відповідальних за захист об'єктів критичної інфраструктури, існують реальні проблеми й виклики у процесі виконання їхніх завдань. Недостатнє правове забезпечення, брак міжвідомчої взаємодії та інформації – усі ці аспекти можуть ускладнювати роботу фахівців і знижувати ефективність заходів із безпеки критичних об'єктів. Зазначене слід брати до уваги задля подальшого вдосконалення системи захисту критичної інфраструктури.

Відповідаючи на запитання «Як Ви вважаєте, за якими принципами повинно здійснюватися управління з захисту об'єктів критичної інфраструктури?», респонденти висловили різні думки щодо принципів управління, а саме: законність визначили найважливішим принципом 18 % фахівців; завчасна підготовка до дій в особливих умовах – 17 %; оперативність – 15 %; організованість і раціональність – 14 %; внутрішня і зовнішня взаємодія – 11 %. Наведені

результати вказують на різноманітність підходів і перспектив у сфері управління захистом об'єктів критичної інфраструктури. Представники сил безпеки й оборони мають своє бачення щодо принципів, які вважають найважливішими в забезпеченні ефективного управління цими об'єктами. Водночас така різноманітність може вказувати на необхідність комплексного підходу до управління захистом об'єктів критичної інфраструктури, який ураховуватиме різні аспекти та інтереси всіх зацікавлених сторін.

У відповідь на запитання «На Вашу думку, чи відповідає існуюче законодавство вимогам щодо захисту об'єктів критичної інфраструктури?» більша частина респондентів (56 %) визначає, що законодавство не повною мірою відповідає вимогам щодо захисту об'єктів критичної інфраструктури. Такий стан зумовлений зміною технологій, зростанням загроз безпеці чи прогалинами в самому законодавстві, які не враховують сучасні виклики. Відповіді респондентів можуть покладатися в основу подальших реформ у законодавстві щодо захисту об'єктів критичної інфраструктури з метою поліпшення їх безпеки.

Відповідаючи на запитання «На яких принципах повинна ґрунтуватись підготовка щодо захисту об'єктів критичної інфраструктури?», респонденти зазначають різні принципи: завчасність визначили ключовим принципом 21 % фахівців; безперервність – 16 %; планомірність – 15 %. Різноманітність відповідей відображає специфіку роботи складових сектору безпеки й оборони, їхніх завдань, а також спроможності в контексті захисту об'єктів критичної інфраструктури. Так, більший акцент на завчасності, безперервності та планомірності, можливо, пов'язаний із необхідністю передбачення потенційних загроз і розроблення ефективних стратегій захисту.

На запитання «Які проблеми у підготовці особового складу у сфері захисту об'єктів критичної інфраструктури Ви вбачаєте?» респонденти відповіли про необхідність підвищення кваліфікації особового складу й відзначають цей аспект як проблематичний (45 %). З огляду на значення цієї сфери для національної безпеки постійне навчання й підвищення кваліфікації персоналу критично важливі.

На запитання «Як часто у Вашому підрозділі (органі управління) проводяться заняття щодо захисту об'єктів критичної інфраструктури?» серед запропонованих відповідей із конкретною кількістю занять найбільше респондентів відповіли «Інше» (41 %). Це свідчить про те, що в різних підрозділах чи органах управління існують різні підходи до організації підготовки з питань захисту об'єктів критичної інфраструктури. Наприклад, в одних підрозділах заняття можуть проводитися щотижня, тобто проводиться регулярна інтенсивна підготовка, тоді як в інших – щомісяця. Такий стан зумовлений особливостями внутрішньої політики підрозділу, доступністю ресурсів, обсягом завдань та іншими чинниками. Важливою є систематичність підготовки незалежно від її частоти, аби персонал був готовим діяти в разі виникнення загрози для об'єктів критичної інфраструктури.

На запитання «Які, на Ваш погляд, обставини сприяли недолікам при виконанні завдань з захисту об'єктів критичної інфраструктури?» найбільшу кількість голосів було віддано відповіді «Відсутність узгодження спільних дій» (33 %). Такі результати підтверджують, що недоліки у виконанні завдань із захисту об'єктів критичної інфраструктури значною мірою спричинені відсутністю координації та спільних дій між різними силовими структурами чи підрозділами. Отже, механізми співпраці й координації між різними установами потребують поліпшення, аби підвищити ефективність заходів із захисту об'єктів критичної інфраструктури.

На запитання «Як ви оцінюєте рівень підготовки персоналу для реагування на загрози у сфері захисту об'єктів критичної інфраструктури?» найбільше респондентів указали «Середній» (70 %), тобто більшість працівників сил безпеки й оборони оцінює рівень підготовки персоналу для реагування на загрози у сфері захисту об'єктів критичної інфраструктури як середній. Вочевидь, існують певні аспекти, які потребують подальшого вдосконалення чи посилення.

Відповідаючи на запитання «Як ви оцінюєте рівень спроможності персоналу щодо реагування на загрози у сфері захисту об'єктів критичної інфраструктури?», більша частина респондентів (66 %) оцінює рівень спроможності персоналу як середній. Це може вказувати на базовий рівень підготовки та здатність персоналу реагувати на загрози, але, можливо, певні аспекти потребують подальшого підвищення ефективності й компетентності.

Результати відповідей на запитання «Які сфери критичної інфраструктури Ви вважаєте найбільш небезпечними?» такі: хімічна – 51 %, енергетична – 37 %, тобто працівники складових сектору безпеки й оборони сприймають енергетичну й хімічну сфери як особливо небезпечні в контексті захисту критичної інфраструктури. Вочевидь, це пов'язано з потенційними наслідками

аварій чи терористичних атак у цих галузях, які можуть мати серйозний вплив на суспільство й сектори економіки.

На запитання анкети «Які загрози та ризики стосовно ОКІ Ви вважаєте найбільшими?» переважна більшість респондентів (44 %) вказала терористичні атаки. Респонденти вважають терористичні атаки найсерйознішою загрозою для об'єктів критичної інфраструктури, оскільки вони можуть призвести до серйозних наслідків для безпеки нації та функціонування ключових секторів економіки й суспільства.

На запитання «Чи існують внутрішні процедури (відомчі) для оцінки ризиків у сфері захисту об'єктів критичної інфраструктури?» найбільшу кількість голосів респондентів було віддано відповіді «Так» (64 %). Результати відповідей підтверджують, що сили безпеки й оборони мають внутрішні процедури для оцінювання ризиків у сфері захисту об'єктів критичної інфраструктури. Це становить важливий аспект у забезпеченні безпеки та відповідності стандартам безпеки, оскільки дає змогу ефективно виявляти й управляти потенційними загрозами.

На запитання «Як Ви оцінюєте стан технічного забезпечення та засобів зв'язку, які використовуються при виконанні завдань охорони об'єктів критичної інфраструктури?» респонденти відповіли таким чином: достатній – 53 %, потребує покращення – 33 %. Більшість фахівців сил безпеки й оборони оцінюють технічне забезпечення та засоби зв'язку, що використовуються під час виконання завдань охорони об'єктів критичної інфраструктури, як достатні і такі, що потребують поліпшення, тобто залишається простір для подальшого вдосконалення технічного забезпечення задля ефективнішої й безпечнішої роботи фахівців у цій сфері.

На запитання «Як Ви сприймаєте взаємодію з органами/підрозділами сил безпеки та оборони під час виконання спільних завдань з захисту об'єктів критичної інфраструктури?» отримала найбільшу кількість голосів відповідь «Обмежена взаємодія» (58 %). Такі результати свідчать про те, що респонденти сприймають взаємодію з іншими органами/підрозділами сил безпеки й оборони під час виконання спільних завдань із захисту об'єктів критичної інфраструктури як обмежену, тобто існують певні перешкоди у взаємодії між різними силовими структурами, які потребують уваги й подальшого вирішення, аби забезпечити ефективнішу координацію та спільні дії у сфері захисту об'єктів критичної інфраструктури.

На запитання анкети «Як Ви сприймаєте взаємодію з місцевими органами влади та органами місцевого самоврядування при реалізації заходів захисту об'єктів критичної інфраструктури?» найбільше респондентів відповіли: «Обмежена взаємодія» (64 %). Більшість респондентів вважає обмеженою взаємодію з місцевими органами влади та органами місцевого самоврядування у процесі реалізації заходів захисту об'єктів критичної інфраструктури. Вочевидь, існують певні проблеми чи перешкоди у співпраці між цими структурами. Серед можливих причин: недостатній обмін інформацією, недосконаліть процесів координації, недостатня участь одного з партнерів у розробленні та впровадженні стратегій захисту. Такі висновки корисні для подальшого вдосконалення механізмів співпраці й підвищення ефективності заходів захисту критичної інфраструктури.

На запитання «Чи існують стандарти або протоколи для взаємодії з іншими органами/підрозділами сил безпеки та оборони, місцевими органами влади та органами місцевого самоврядування, які задіяні до виконання завдань з захисту об'єктів критичної інфраструктури?» найбільше респондентів дали ствердну відповідь «Так» (63 %). Це свідчить про те, що у сфері захисту об'єктів критичної інфраструктури існують установлені стандарти або протоколи для взаємодії між силами безпеки й оборони з місцевими органами влади та органами місцевого самоврядування. Їх наявність дає змогу забезпечити системну й координовану реакцію на потенційні загрози для критичних об'єктів, ефективність та оперативність у діях із метою запобігання інцидентам і надання необхідної допомоги в разі виникнення небезпеки. Такі стандарти – важливий складник системи безпеки, вони допомагають забезпечити координацію дій і взаємодію між різними органами та підрозділами, що відповідають за захист об'єктів критичної інфраструктури.

На запитання анкети «Які ускладнення в сфері співпраці з органами/підрозділами сил безпеки і оборони, місцевими органами влади та органами місцевого самоврядування виникали при реалізації заходів захисту об'єктів критичної інфраструктури?» найбільшу кількість голосів отримала відповідь «Проблеми з обміном інформацією» (46 %). Таким чином, одні з найпоширеніших проблем у сфері співпраці з органами сил безпеки й оборони, місцевими органами влади та органами місцевого самоврядування під час реалізації заходів захисту об'єктів критичної інфраструктури становить обмін інформацією. Це може бути наслідком недостатньої

координації між різними структурами, а також браку ефективних механізмів обміну необхідною інформацією між ними. Подолання цих ускладнень потребує додаткових заходів із поліпшення комунікаційних та інформаційних систем між відповідними органами й підрозділами.

На запитання «Які недоліки відмічені Вами в управлінських рішеннях щодо захисту об'єктів критичної інфраструктури?» найбільше респондентів (22 %) відповіли: «Неефективна організація роботи місцевих органів державної влади». Ці дані свідчать про те, що фахівці різних силових структур вбачають низку недоліків в управлінських рішеннях щодо захисту об'єктів критичної інфраструктури. Так, неефективна організація роботи місцевих органів влади може ускладнювати реалізацію стратегій і заходів із захисту критичної інфраструктури. Подолати недоліки можливо шляхом удосконалення управлінських процесів, зокрема координації та співпраці між різними рівнями управління, а також через упровадження більш гнучких та адаптивних стратегій в управління кризовими ситуаціями.

На запитання «Які не висвітлені в анкеті проблеми (виклики) в сфері охорони ОКІ Ви б хотіли відзначити?» 37 % респондентів (найбільше) відповіли: «Необхідність покращення комунікаційних систем». Така відповідь вказує на важливу проблему, якої не було враховано в анкеті. Поліпшення комунікаційних систем забезпечить ефективніше передавання й оброблення інформації, що є критичним для управління та реагування на потенційні загрози. Зазначена проблема потребує уваги й вирішення на рівні стратегічного планування та алокації ресурсів для забезпечення стабільності й безпеки критично важливих об'єктів.

Відповідаючи на запитання «Які, на Вашу думку, необхідно ввести зміни щодо захисту об'єктів критичної інфраструктури?», найбільше респондентів зазначили: «Удосконалити організацію взаємодії суб'єктів забезпечення безпеки об'єктів критичної інфраструктури» (26 %); «Удосконалити правову базу сфери захисту об'єктів критичної інфраструктури» (18 %). Таким чином, респонденти вбачають необхідність змін у різних аспектах захисту об'єктів критичної інфраструктури: удосконалення правової бази, організація взаємодії між суб'єктами безпеки. Ці зміни сприятимуть ефективності заходів забезпечення безпеки критично важливих об'єктів.

На запитання анкети «Проведення яких заходів є обов'язковим для поліпшення захисту об'єктів критичної інфраструктури?» найбільшу кількість голосів отримали такі відповіді: «Розроблення моделі реагування складових сектору безпеки і оборони України на загрози об'єктів критичної інфраструктури в особливий період» (36 %); «Розроблення моделі реагування складових сектору безпеки і оборони України на загрози об'єктів критичної інфраструктури в мирний час» (29 %). Фахівці складових сектору безпеки й оборони усвідомлюють необхідність розроблення і впровадження спеціалізованих моделей реагування на загрози критичній інфраструктурі. Такі моделі сприятимуть кращій координації та плануванню дій у випадку потенційних небезпек, що може підвищити загальний рівень безпеки й забезпечити ефективніший захист об'єктів критичної інфраструктури в різних ситуаціях як у мирний час, так і в особливий період. Наведені відповіді підтверджують актуальність дослідження.

На питання «Визначити роль Національної гвардії України у виконанні завдань з захисту об'єктів критичної інфраструктури» респонденти відповіли: «Основна» (37 %), «Провідна» (36 %). Половина респондентів вважають Національну гвардію України провідною у цій ролі. Інша половина вважає її роль основною. Такий погляд пояснюється специфікою роботи та функціональними обов'язками кожної із зазначених структур, а також залежить від досвіду й ефективності у виконанні завдань забезпечення безпеки.

На питання «Визначити місце Національної гвардії України у виконанні завдань з захисту» найбільше респондентів дали відповіді: «В ланці основних виконавців» (48 %); «В ланці управління» (32 %). Таким чином, визнається важлива роль Національної гвардії України в забезпеченні безпеки країни та захисту критичної інфраструктури, хоча її місце в ланці виконавців може різнитися залежно від перспективи й досвіду кожної із зазначених структур.

Відповідаючи на запитання «На Вашу думку, на яку правоохоронну структуру (військове формування) доцільно покласти обов'язки уповноваженого органу у сфері захисту об'єктів критичної інфраструктури?», переважна більшість респондентів зазначила: «Національна гвардія України» (43 %). Отже, Національну гвардію України вони вважають найбільш придатним військовим формуванням для виконання обов'язків уповноваженого органу у сфері захисту об'єктів критичної інфраструктури. Це може відображати специфіку діяльності Національної гвардії України, її спеціалізацію та здатність до оперативності у вирішенні ситуацій забезпечення безпеки. Національна гвардія України має значний ресурсний потенціал, зокрема людський і матеріальний, а також високу оперативність у вирішенні екстрених ситуацій.

У відповідь на запитання «Які можливі заходи чи ініціативи Ви пропонуєте для поліпшення безпеки об'єктів критичної інфраструктури?» респонденти надали свої пропозиції. Основними названо такі напрями:

– зміцнення правової бази (вдосконалення та уточнення законодавства, що регулює сферу захисту об'єктів критичної інфраструктури, зокрема розроблення нових нормативних актів, які враховують сучасні загрози й виклики);

– підвищення кваліфікації персоналу (організація регулярних тренінгів, семінарів і навчань для працівників, які відповідають за безпеку об'єктів критичної інфраструктури, аби покращити їхні знання, навички та вміння в управлінні ризиками й реагуванні на загрози);

– збільшення інвестицій (забезпечення достатнього фінансування для розроблення та впровадження сучасних технологій і систем безпеки на об'єктах критичної інфраструктури);

– посилення міжвідомчої співпраці (сприяння ефективнішій координації й обміну інформацією між різними відомствами і структурами, відповідальними за безпеку об'єктів критичної інфраструктури);

– розвиток інноваційних технологій (прискорення впровадження новітніх технологій, таких як системи відеоспостереження, дрони, сенсорні системи, штучний інтелект, для підвищення ефективності та реакції на загрози);

– просвітня робота із громадськістю (проведення інформаційних кампаній і навчальних заходів для населення з питань безпеки об'єктів критичної інфраструктури та заходів, які вживаються для зменшення ризиків).

Висновки

На основі викладеного можна зазначити таке.

1. Світові тенденції до посилення загроз функціонуванню критичної інфраструктури, а також катастрофічні наслідки пошкодження об'єктів критичної інфраструктури в регіонах України внаслідок широкомасштабної збройної агресії росії актуалізують питання захисту систем, об'єктів і ресурсів, які є критично важливими для функціонування і сталого розвитку суспільства, підвищення соціально-економічної стабільності і загалом для забезпечення національної безпеки. Дотепер дослідженню методологічних засад вивчення проблем захисту об'єктів критичної інфраструктури не приділялося належної уваги, що й зумовило актуальність дослідження.

2. Для вивчення сучасних проблемних питань у сфері захисту об'єктів критичної інфраструктури в Україні проводилося експертне опитування, за результатами якого виявлено низку ключових аспектів щодо захисту об'єктів критичної інфраструктури силами безпеки й оборони України. Загалом результати експертного опитування вказують на те, що безпека об'єктів критичної інфраструктури є актуальною проблемою, потребує комплексного підходу та спільних зусиль різних структур і суб'єктів влади, зокрема постійного вдосконалення законодавства та правової бази у сфері захисту об'єктів критичної інфраструктури.

3. Відповіді респондентів свідчать про потребу в підвищенні кваліфікації персоналу, ефективному управлінні та координації дій між складовими сектору безпеки й оборони, активізують питання розвитку інноваційних технологій для підвищення рівня безпеки захисту об'єктів критичної інфраструктури та обґрунтовують важливість інвестицій у сучасні технології й системи безпеки, аби забезпечити відповідну захищеність об'єктів критичної інфраструктури. Респондентами також порушено питання щодо просвітньої роботи із громадянами й залучення їх до процесу забезпечення безпеки об'єктів критичної інфраструктури.

4. За результатами експертного опитування доведена необхідність розроблення моделей реагування на загрози об'єктам критичної інфраструктури в різних умовах: як в особливий період, так і в мирний час. Такий підхід потребує системного і гнучкого планування та реагування на потенційні загрози незалежно від контексту. Респондентами робиться припущення, що розроблення відповідних моделей дасть можливість підвищити ефективність заходів забезпечення безпеки об'єктів критичної інфраструктури і сприятиме готовності до різних сценаріїв кризових ситуацій.

5. Респонденти визначили роль Національної гвардії України у виконанні завдань із захисту об'єктів критичної інфраструктури як провідну та основну, а щодо місця Національної гвардії України у виконанні завдань із захисту вибрано відповіді: «В ланці основних виконавців»; «В ланці управління». Національна гвардія України також визначена найбільш придатним формуванням серед складових сектору безпеки й оборони, на яке доцільно покласти обов'язки уповноваженого органу у сфері захисту об'єктів критичної інфраструктури.

Отже, напрями наукових досліджень спрямовуються на подальше розроблення науково-методологічного апарату оптимізації діяльності формувань Національної гвардії України із захисту об'єктів критичної інфраструктури.

Перелік джерел посилання

1. Деякі питання об'єктів критичної інформаційної інфраструктури : Постанова Кабінету Міністрів України від 09.10.2020 р. № 943. URL: https://zakon.rada.gov.ua/laws/show/943-2020-%D0%BF (дата звернення: 08.05.2024).
2. Про критичну інфраструктуру : Закон України від 16.11.2021 р. № 1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20 (дата звернення: 08.05.2024).
3. Стратегія забезпечення державної безпеки : Указ Президента України від 16.02.22 р. № 56/2022. URL: https://zakon.rada.gov.ua/laws/show/56/2022#Text (дата звернення: 08.05.2024).
4. Бірюков Д. Концепція захисту критичної інфраструктури як елемент загальноєвропейської безпекової політики. *Наукові записки.* 2019. № 6 (68). С. 106−115.
5. Бобро Д. Г. Методологія оцінки рівня критичності об'єктів критичної інфраструктури. *Стратегічні пріоритети*. 2016. Вип. 3 (40). С. 77–85.
6. Бобро Д. Г. Визначення критеріїв оцінки та загрози критичній інфраструктурі. *Стратегічні пріоритети. Економіка*. 2020. № 4. С. 83–93.
7. Домарацький М. Б. Державне управління забезпеченням безпеки критичної інфраструктури в Україні : дис. … канд. наук з державного управління : 25.00.05. Харків, 2022. 259 с.
8. Домарацький М. Б. Забезпечення безпеки та підвищення ефективності захисту критично важливих об'єктів на державному рівні. *Публічне управління і адміністрування в Україні*. 2019. Вип. 14. С. 82–85.
9. Домарацький М. Б. Нормативне й адміністративне забезпечення державного регулювання критичної інфраструктури в Україні: аналіз і оцінка. *Вісник Національного університету цивільного захисту України*. 2022. Вип. 1 (12). С. 470–475.
10. Єрменчук О. П. Сутність та зміст поняття «інфраструктура» в контексті захисту критичної інфраструктури. *Бюлетень Міністерства юстиції України*. 2017. № 11 (193). С. 35–40.
11. Кондратов С. І. Про забезпечення координації дій, взаємодії та обміну інформацією при створенні державної системи захисту критичної інфраструктури : аналіт. доп. Київ : НСІД, 2018. 30 с.
12. Суходоля О. М. Захист критичної інфраструктури в умовах гібридної війни: проблеми та пріоритети державної політики. *Стратегічні пріоритети*. 2016. Вип. 3 (40). С. 62–75.
13. Кількісні методи експертного оцінювання : науково-методична розробка / уклад. : В. П. Новосад, Р. Г. Селіверстов, І. І. Артим. Київ : НАДУ, 2009. 36 с.
14. Козенюк А. І., Міллер А. Й. Анкетування. Юридична енциклопедія : [у 6 т.] / ред. кол.: Ю. С. Шемшученко (відп. ред.) [та ін.]. Київ : Українська енциклопедія ім. М. П. Бажана, 1998. Т. 1 : А – Г. 672 с.

Лавров Іван Сергійович – ад'юнкт Національної академії Національної гвардії України
https://orcid.org/0009-0005-0706-3711

Бєлай Сергій Вікторович – доктор наук з державного управління, професор, заступник начальника навчально-наукового центру організації освітнього процесу – начальник науково-методичного відділу Національної академії Національної гвардії України
https://orcid.org/0000-0002-0841-9522