DOI 10.33099/2618-1614-2025-29-2-17-26
УДК 321+342.6+355/358

О. М. Суходоля,
доктор наук державного управління, професор,
Національний інститут стратегічних досліджень

Розвиток спроможностей сектору безпеки та оборони України щодо захисту критичної інфраструктури: світові тенденції та уроки війни в Україні

Посилення ролі сил оборони в забезпечення безпеки критичної інфраструктури (КІ) в останні десятиліття стає пріоритетним завданням оборонної політики різних країн світу. Поряд з безпосереднім завданням забезпечення захисту критичної військової інфраструктури дедалі чіткіше проявляється тенденція щодо уповноваження збройних сил на захист цивільної інфраструктури, передусім тієї, від якої залежить виконання визначених для них місій. Досвід України в реагуванні на воєнні загрози функціонування КІ в умовах повномасштабної війни засвідчує необхідність ще більшого посилення ролі сектору оборони України та його спроможностей забезпечити безпеку КІ. Сценарне планування реагування на загрози може виступати практичним інструментом визначення необхідних спроможностей сил оборони та планування заходів захисту КІ. Запропоновані концептуальні підходи до розроблення сценаріїв дають змогу визначити заходи реагування на загрози різного рівня критичності та узгодити їх реалізацію окремими суб'єктами національної системи захисту КІ.

Ключові слова: захист критичної інфраструктури, сектор безпеки та оборони, загрози інфраструктурі, сценарне планування, розвиток спроможностей сил оборони.

Захист критичної інфраструктури (КІ) є одним з пріоритетів забезпечення національної безпеки. Вагомість даного питання, починаючи з 2000-х років (передусім з моменту терактів 11 вересня 2001 р. у США) невпинно зростає. Це зумовлюється тим, що стале функціонування інфраструктури (енергетики, транспорту, зв'язку тощо) є основою функціонування суспільства та обороноздатності країни, а спектр загроз суттєво розширився.

Природні катаклізми, техногенні аварії формують суттєві виклики сталості функціонування інфраструктури. Зловмисні дії (кібератаки, терористичні акти, гібридні впливи) проти КІ стають дедалі масштабнішими та загрожують уже не тільки роботі окремих об'єктів інфраструктури, а й життєдіяльності суспільства загалом. Збройна агресія РФ проти України та застосування нею стратегії цілеспрямованого руйнування інфраструктури як інструменту примусу до капітуляції стала наочною демонстрацією актуальності захисту КІ.

Питання захисту, забезпечення безпеки і стійкості КІ, надання життєво важливих послуг та функцій широко досліджувалось українськими та зарубіжними науковцями. Водночас публікацій, відкритих для широкого загалу, де досліджуються роль та завдання сил оборони із цих питань, є досить небагато. Серед них слід відзначити роботи Д. Брауна, К. Еванса, П. Осервальда, Д. Кавелті, Д. Кенана, Р. Літтла, А. Якуха, О. Батюка, С. Бєлая, О. Єрменчука, М. Коваля, В. Коваля та інших. При цьому варто зазначити, що сучасна динаміка загроз КІ вимагає суттєвого посилення повноважень сил оборони в цій сфері.

Починаючи з 2014 р. Україна розвиває науково-теоретичні засади концепції захисту КІ та розробляти необхідну законодавчу базу [1]. Формальне закріплення завдання створення державної системи захисту КІ України відобразилось у прийнятті наприкінці 2021 р. Закону України «Про критичну інфраструктуру» [2] з одночасним внесенням змін до низки законів, що регулюють діяльність сектору безпеки та оборони України.

Імплементувати новоприйняте законодавство в практичну площину Україна вчасно не встигла. Повномасштабне збройне вторгнення російської армії, яке розпочалось 24 лютого 2022 р. продемонструвало початкову неготовність сил сектору безпеки та оборони України до захисту об'єктів КІ. На момент російського вторгнення Україна не мала достатніх сил та адекватних засобів захисту. Наслідком стало масштабне руйнування КІ України, передусім енергетичної, транспортної інфраструктури, систем забезпечення життєдіяльності громад.

Гіпотеза та мета. Запровадження практики випереджального планування і розвиток спроможностей сил оборони до реагування на загрози різного виду

забезпечать базовий рівень безпеки і стійкості функціонуванню КІ, життєдіяльності суспільства та обороноздатності країни. Для запровадження такого проактивного підходу, насамперед необхідно: уточнити роль сил безпеки та оборони країни з питань захисту КІ, зокрема від воєнних загроз, та розробити концептуальні підходи планування розвитку спроможностей сил оборони до виконання завдань із захисту КІ та їхньої взаємодії з іншими учасниками реагування.

Методи і результати дослідження. Вирішення поставлених завдань стало можливим завдяки визначенню на основі огляду доступних джерел тенденцій трансформації ролі сил оборони країн світу з питань захисту КІ, аналізу положень законодавства щодо завдань збройних сил у цій сфері. Водночас досвід реагування України на порушення функціонування критичної енергетичної інфраструктури, отриманий у період 2022–2024 рр. [3], дав змогу виокремити основні напрями вдосконалення політики країни й уточнити завдання сил оборони у сфері захисту КІ та запропонувати механізм планування розвитку необхідних спроможностей.

Огляд концептуальних підходів та положень законодавства щодо завдань збройних сил у сфері захисту КІ

Проведений аналіз наукових публікацій щодо застосування сил оборони різними країнами свідчить, що збройні сили відіграють важливу роль у захисті КІ. Однак переважна більшість публікацій стосується дій збройних сил у мирний час та лише стосовно окремих видів загроз.

На межі XXI століття питання захисту КІ часто розглядалося з огляду на спадок «холодної війни». Наприклад, у публікації Національної академії наук США аналізується можливість підземного розміщення об'єктів КІ [4]. Проте зазначається, що серед багатьох перешкод такому традиційному вирішенню завдання фізичного захисту, найголовнішим питанням є вартість підземних споруд для захисту КІ. Однак зі зростанням площі підземних споруд вартість такого типу захисту знижується, а з урахуванням повного життєвого циклу великих споруд стає навіть привабливою [5].

Із завершенням «холодної війни» та прискоренням глобалізації на перший план вийшла проблематика спроможності країн реагувати на загрози мирного періоду, коли терористичні акти і кібератаки виступають максимальним рівнем зловмисного впливу на КІ. При цьому дослідження зосереджувалися на різних аспектах реагування на терористичні загрози.

Так, Дж. Стівенсон, провівши порівняльний аналіз законодавства США та Великої Британії щодо залучення збройних сил до реагування на терористичні загрози, вносить пропозиції щодо підвищення залученості військових до забезпечення безпеки КІ країни та надання допомоги цивільній владі [6]. Ураховуючи, що більшість інфраструктурних систем перебувають у приватній власності, П. Осервальд наголошує на важливості налагодження ефективного державно-приватного партнерства [7]. Водночас інші автори наголошують, що хоча співпраця з приватним сектором є необхідною, держава має координувати захист КІ, особливо перед комплексними загрозами [8]. Паралельно розвивалися математичні моделі аналізу ситуації прийняття рішення оптимізації захисту КІ проти терористичних атак Д. Браун [9].

Із часом відбувається розширення фокусу уваги дослідників на інші загрози, зокрема досліджується плив природних загроз на КІ. Прикладом подібного аналізу є дослідження, де аналізується вплив зміни клімату на функціонування критичної енергетичної інфраструктури, яка забезпечує функціонування сил оборони [10].

Широко досліджувалися питання, пов'язанні з гібридними загрозами та намаганням окремих країни використовувати критичну інфраструктуру як зброю [11–13]. У зв'язку із цим К. Еванс обґрунтовує необхідність уточнення ролі й завдань сил оборони у протидії таким загрозам з урахуванням їхнього впливу на надання життєво важливих послуг [14].

Окремі публікації аналізують роль і завдання національної гвардії як складової сектору оборони країни. Так, У США виокремлюються два основні завдання Національної гвардії США: розроблення планів захисту визначеної КІ у співпраці з іншими державними та приватними стейкхолдерами; створення сил швидкого реагування для реагування на виклики, коли можливостей інших сторін буде недостатньо [15]. Українські науковці досліджують питання вдосконалення службово-бойової діяльності підрозділів Національної гвардії України з організації захисту (оборони) та забезпечення безпеки (охорони) функціонування об'єктів КІ як у мирний час, так і в особливий період [16].

З погляду практичної імплементації напрацьованих науковцями концепцій слід відзначити зусилля США. Міністерство оборони США розробило рекомендації щодо планування стійкості КІ, необхідної для виконання збройними силами визначених їм місій. У структурі міністерства створений підрозділ, який опікується імплементацією Програми захисту критичної інфраструктури (the Defense Critical Infrastructure Program (DCIP)) [17]. Метою цієї програми є координація ідентифікації, оцінювання, захисту й моніторингу в режимі реального часу фізичної та кіберінфраструктури, необхідної для виконання національної воєнної стратегії.

Європейські країни також передбачали у своєму законодавстві завдання для сил безпеки та оборони щодо захисту КІ [18]. Водночас такі завдання мали допоміжний характер. У рамках міжнародної співпраці країни НАТО тривалий час орієнтувалися на розвиток рекомендацій та поширення кращого досвіду щодо захисту КІ через центри передового досвіду НАТО [19]. Прикладом цього є навчальний посібник НАТО, де аналізуються загрози КІ, правові, організаційні засади розбудови системи захисту КІ, а також роль збройних сил у контексті колективної безпеки НАТО [20].

Розширення спектру загроз для КІ формує нові виклики перед сектором безпеки та оборони будь-якої країни, що відображається в пошуках шляхів удосконалення планування розвитку його спроможностей. Зокрема, в роботі Д. Кенана розглядаються підходи до планування стійкості інфраструктури, що охоплює одночасно військову та цивільну сфери [21].

Загалом більшість досліджень сходиться на тому, що основна відповідальність за захист КІ лежить на цивільних структурах і власниках об'єктів, але військові відіграють вирішальну роль у випадках, коли загроза або шкода перевищують можливості цивільних служб. Водночас відзначається, що сили оборони залежать від цивільної інфраструктури для виконання своїх функцій. Таким чином, збройні сили зацікавлені у зміцненні захищеності КІ не лише для захисту населення, а й для забезпечення власної спроможності виконувати свою місію. Інакше кажучи, синергія цивільної та військової стійкості розглядається як передумова успішної оборони. Своєрідним проявом усвідомлення широким загалом такої концепції є створення спільної групи ЄС – НАТО з питань захисту КІ та оприлюднення першого звіту щодо пріоритетів спільних дій у цій сфері [22].

Водночас суттєвих змін в оборонній політиці багатьох країн поки не було запроваджено, повноваження і роль сектору оборони в цій сфері залишаються нечіткими. Переважна більшість країн виходить з переконання, що їхні збройні сили відіб'ють усі атаки агресора та захистять КІ. Нещодавно прийнята ЄС Директива CER хоча встановлює вимоги щодо діяльності суб'єктів забезпечення стійкості функціонування КІ в мирний час, однак не дає розуміння щодо завдань збройних сил країн – членів ЄС у процесі захисту КІ [23].

Одержаний Україною досвід забезпечення безпеки і стійкості функціонування КІ, передусім енергетичної, є серйозним застереженням для більшості країн ЄС та НАТО щодо готовності їхніх збройних сил до реагування та пропозицією до уточнення ролі в захисті КІ від воєнних загроз, подібні тим з якими зіткнулась Україна [24].

Проблеми забезпечення захисту об'єктів критичної енергетичної інфраструктури: досвід України

В Україні, як і в більшості країн світу, завдання забезпечення захисту КІ ставилося в основному перед правоохоронною системою (поліцією, службою охорони) та перед Національною гвардією України (стосовно обмеженого кола об'єктів енергетики). При цьому безпосередньо фізичну охорону об'єктів здійснювали державні або приватні охоронні структури (компанії), які не мали на озброєнні засобів протидії повномасштабній агресії. Збройні Сили України в цій сфері мали завдання лише щодо захисту критичної військової інфраструктури та протиповітряного прикриття важливих державних об'єктів [25].

До початку повномасштабного збройного вторгнення РФ Україна не встигла повноцінно імплементувати законодавчі зміни, зумовлені прийняттям Закону України «Про критичну інфраструктуру». Механізми та процедури залучення сил та засобів Збройних Сил України до захисту (оборони, прикриття) КІ не були уточнені та реалізовані вчасно. Зокрема, оцінювання ризиків порушення роботи КІ від реалізації воєнних загроз та підготовка планів реагування сектору безпеки та оборони країни не було проведене до початку війни.

З моменту вторгнення російських військ спостерігалася початкова неготовність до такого розвитку ситуації та нескоординованість дій сил сектору безпеки та оборони України щодо захисту об'єктів КІ. Прикладом цього є практично миттєве захоплення російськими військами території Зони відчуження Чорнобильської АЕС, Каховської ГЕС та Запорізької АЕС. Захист Запорізької АЕС здійснювали підрозділ територіальної оборони (блокування просування російських військ на підступах до станції) та підрозділ Національної гвардії України (захист периметру станції), які не мали важкого озброєння [3].

Проявилася суттєва недостатність засобів захисту КІ від ударів з повітря. Заздалегідь підготовлених як активних, так і пасивних заходів захисту (охорони, оборони, інженерно-технічного захисту, засобів радіоелектронної боротьби, протиповітряного прикриття від різних типів засобів ураження тощо) було недостатньо [24, 26]. Протиповітряне прикриття КІ законодавством України передбачалося лише щодо обмеженого переліку об'єктів КІ. Водночас різноманітність засобів ураження з повітря, масштабність атак, поширеність атак на всю територію країни призвели до перенасичення наявних спроможностей сил протиповітряного захисту та руйнувань КІ.

Проявилися також проблеми організаційного характеру, зокрема пов'язані з узгодженням дій між

цивільним та військовим суб'єктами реагування. На початковому етапі війни відзначалася неготовність створених військових адміністрацій до запровадження та здійснення заходів захисту КІ. Виконання Генеральним штабом Збройних Сил України завдання щодо спрямування, координації та контролю за діяльністю обласних військових адміністрацій з питань захисту КІ потребувало посилення та унормування. Не був запроваджений нормативно-правовий акт, яким регулюється посилення охорони об'єктів КІ в період дії правового режиму воєнного стану [27].

Очевидною стала невідповідність бюджетного фінансування сектору безпеки та оборони України рівню викликів, особливо стосовно захисту КІ країни. Реалізації концепції «Країна-фортеця»[1] [26], розробленої в терміновому порядку у 2022 р., розпочалася лише з 2023 р., після формування законодавчої бази фінансування підготовлених інженерно-технічних рішень із захисту об'єктів енергетичної інфраструктури.

Новосформовані військові підрозділи, яким визначалося завдання захисту окремих об'єктів КІ, також потребували фінансування для оснащення необхідним обладнанням та засобами ураження, тож досягнення необхідного рівня ефективності виконання ними поставлених завдань також потребувало певного часу. При цьому слід урахувати необхідність оперативного дооснащення визначених підрозділів новими видами озброєння відповідно до зміни противником засобів та способів ураження об'єктів [24].

При цьому слід відмітити не лише постійну модифікацію агресором стратегії та тактики атак проти КІ, а й ризик виникнення ефекту зміщення загроз. Зокрема, починаючи з 2024 р., відзначається зростання кількості диверсійних дій проти об'єктів КІ України. Прогнозується, що такий вид загроз стане основним в умовах тривалого збереження збройного конфлікту низької інтенсивності («заморожування війни»). Реагування на зміни потребуватиме запровадження інших вимог до захисту та взаємодії різних суб'єктів реагування, в тому числі військових формувань. Тож Збройні Сили України мають бути готові й до виконання завдань з реагування на інші види загроз різного рівня складності.

Загалом збройна агресія РФ продемонструвала, що завдання сектору безпеки та оборони у сфері захисту КІ мають бути суттєво уточненні, а необхідні для їх виконання спроможності посилені. І це є одним з основних уроків, який слід засвоїти всім демократичним країнам. Необхідно бути готовими до застосування агресором стратегії цілеспрямованого руйнування об'єктів КІ шляхом використання всього спектра озброєння, наявного на світовому ринку.

Уже зараз цьому питанню приділяється дедалі більше уваги. Зокрема, Міністерство оборони Німеччини оголосило про модернізацію збройних сил країни, щоб бути готовим до майбутніх викликів [28]. Велика Британія, враховуючи уроки України, вирішила суттєво посилити протиповітряне прикриття КІ [29]. У США розробляється нова концепції захисту КІ (The Multi-Domain Resiliency Zone Concept), яка має на меті захистити не лише військову критичну інфраструктуру (що забезпечує виконання місії збройних сил), а й цивільну інфраструктуру, від якої відповідні підрозділи залежать [30].

Отже, актуальним є завдання створення системи планомірного розвитку спроможностей країни до забезпечення безпеки і стійкості функціонування КІ. Першим кроком у цьому напрямі має стати чітке визначення завдань сил сектору безпеки та оборони у сфері захисту КІ. Наступним кроком має бути вдосконалення оборонного планування підготовки сил оборони з урахуванням завдань щодо захисту КІ.

Планування розвитку спроможностей сектору безпеки та оборони для виконання завдань у сфері захисту критичної інфраструктури

Дослідження існуючих підходів та положень законодавства щодо завдань збройних сил у сфері захисту КІ свідчить про світову тенденцію щодо посилення ролі сил оборони у сфері захисту КІ. Однак, ураховуючи чутливість питання, інформація щодо планування розвитку спроможностей не є широко представленою у відкритих джерелах. Водночас, базуючись на міжнародному та українському досвіді реагування на кризові ситуації, доцільним убачається застосування сценарного планування залучення сил безпеки та оборони до реагування на різні види загроз та рівні їхнього впливу.

Прикладом такого підходу є Національна система управління інцидентами США (The National Incident Management System, NIMS), котра являє собою механізм координації зусиль державних та недержавних суб'єктів з метою спільного запобігання, захисту, пом'якшення, реагування та відновлення після інцидентів, спричинених різними загрозами. Як інструмент планування необхідних спроможностей суб'єктів NIMS вимагає розроблення сценаріїв реагування

[1] Концепція «Країна-фортеця» – розроблена українськими науковцями та інженерами модель побудови перспективної системи інженерного захисту об'єктів КІ. Під інженерним захистом розуміється сукупність заходів з інженерного обладнання елементів об'єктів критичної інфраструктури з метою підвищення їхньої живучості, безпеки персоналу та стійкого функціонування КІ в інтересах забезпечення життєвих потреб суспільства. Така система покликана забезпечити інтегральний захист території, об'єктів, громадян та суспільства загалом від засобів повітряного нападу [26].

відповідно до п'яти рівнів складності інцидентів (Type 1 to 5) та встановлення відповідних вимог щодо спроможності залучених учасників узгоджено взаємодіяти в ситуаціях різного рівня складності[2] [31].

В Україні подібний підхід реалізований у системі реагування на надзвичайні ситуації різного рівня (розроблено та напрацьовано методологічну, нормативну та організаційну базу планування розвитку необхідних спроможностей за рівнями ситуації) [32]. Подібний підхід відображений і в законодавстві щодо реагування на терористичні акти. Зокрема наголошується на прийнятті рішень щодо реагування залежно від ступеня їхньої суспільної небезпеки, що, відповідно, визначатиме необхідні ресурси для реагування на визначений рівень критичності впливу (ст. 11 Закону України «Про боротьбу з тероризмом») [33]. У сфері оборони також заявлено про необхідність запровадження сценарного підходу до визначення шляхів досягнення цілей і реалізації пріоритетів державної політики у воєнній сфері, сферах оборони та військового будівництва (ст. 28 Закону України «Про національну безпеку») [34].

Виходячи із зазначеного, пропонується узгодити наявні підходи та внормувати планування спроможностей сил безпеки та оборони до реагування на загрози КІ на основі сценарного планування.

Передусім слід чітко врегулювати відповідальність залучених суб'єктів за здійснення заходів захисту КІ залежно від типу загрози. У частині сектору оборони йдеться про чітке законодавче регламентування завдань та повноважень сил оборони в цій сфері та забезпечення їх необхідними засобами та ресурсами (окремі пропозиції будуть наведені у висновках).

Наступним кроком має стати розроблення та затвердження переліку загроз КІ з визначенням відповідальних за реагування[3]. Це дасть змогу врегулювати розподіл відповідальності за реагування на окремі види загроз КІ, зокрема відповідальності сил оборони за забезпечення захисту КІ від загроз воєнного характеру. Орієнтовний приклад такого переліку наведений у *таблиці 1*.

Визначений відповідальний за реагування суб'єкт у рамках подальшого оборонного планування, використовуючи сценарний підхід до планування, визначає заходи захисту КІ та необхідні сили та засоби для реагування. Пропозиції щодо концептуальних підходів щодо розроблення сценаріїв для різних рівнів критичності впливу загроз наведені в *таблиці 2*. Зазначимо, що загальні підходи до визначення рівнів критичності впливу загроз та розподілу відповідальності за реагування базуються на вивчені досвіду реагування України на випадки руйнування КІ під час війни [3, 24, 35].

Таблиця 1

Перелік загроз КІ та відповідальних за організацію реагування (приклад)

Загроза	Короткий опис загрози	Відповідальний за реагування
Повінь	Затоплення значних територій, населених пунктів та підприємств, спричинене значними атмосферними опадами, таненням снігів чи проривом дамб водосховищ	Державна служба України з надзвичайних ситуацій
Спалах пандемії людини	Серйозний спалах пандемічного захворювання (наприклад грипу) із загальним рівнем клінічних випадків понад 25%	Міністерство охорони здоров'я України
Розлив чи викид хімічної речовини	Аварія, коли відбувається викид великого обсягу хімічної речовини (з хімічного заводу, сховища чи способу транспортування)	Державна служба України з надзвичайних ситуацій
Кібератака проти КІ	Вплив на функціонування КІ шляхом спотворення роботи інформаційно-комунікаційної системи управління (вплив на фізичний вимір здійснення порушення технологічного процесу)	Держспецзв'язок
Теракт проти КІ	Вплив на функціонування КІ шляхом застосування зброї, вчинення вибуху, підпалу чи інших дій, які здійснюються недержавними суб'єктами	Служба безпеки України
Атака КІ з повітря за допомогою безпілотни літальних апаратів	Застосування легких (побутових) безпілотних літальних апаратів для фізичного порушення роботи чи пошкодження КІ	Міністерство внутрішніх справ України
Повномасштабне збройне вторгнення	Атака збройних сил іншої держави (держав) на територію України та КІ із застосуванням усього спектру засобів ураження	Міністерство оборони України

[2] Рівень складності (Type 1–5) – це сукупність факторів, що впливають на спроможність реагування на інцидент. Складність інциденту враховується під час прийняття рішень щодо рівня управління інцидентами, наприклад інцидент можна врегулювати на місцевому рівні чи він потребує залучення ресурсів федерального рівня, аж до виключно федерального рівня відповідальності.

[3] З огляду на нові загрози та динаміку рівня їхнього впливу пропонується такий перелік затверджувати рішенням Ради національної безпеки і оборони України.

Таблиця 2

Концептуальні підходи щодо розроблення сценаріїв та визначення розподілу відповідальності за реагування для різних рівнів критичності впливу загроз

Рівні впливу	Базові елементи опису сценарію впливу загроз	Критерії ранжування сценарію за ймовірними наслідками впливу	Відповідальні за реагування
1	Відсутній вплив на населення та території, де розміщений об'єкт КІ. Відсутність необхідності евакуації персоналу об'єкта КІ та населення на прилеглій території. Наслідки впливу загроз можуть бути врегульовані наявними силами та ресурсами на місці (самостійно оператором КІ). Підготовлені плани реагування, персонал готовий до реагування, залучення зовнішніх стейкхолдерів не потрібне. Дії, події або умови, які спричинили вплив на КІ, не зберігаються. Немає ймовірності каскадних ефектів або загострення ситуації	Низька ймовірність порушення роботи окремого об'єкта КІ чи зниження рівня надання основної послуги. Очікувана тривалість реагування (проведення стабілізаційних дій) не перевищує 12 годин	Оператор КІ
2	Незначний вплив на населення та території, де розміщений об'єкт КІ. Відсутність необхідності евакуації населення суміжних територій під час реагування, можлива евакуація (переміщення) персоналу об'єкта КІ. Дії, події або умови, які спричинили вплив на КІ, не зберігаються. Немає ймовірності каскадних ефектів або загострення ситуації. Незначний негативний вплив на функціонування об'єкта КІ та ключові ресурси оператора КІ. Наслідки впливу загроз можуть бути врегульовані завдяки реалізації плану реагування оператора КІ (використання сил та ресурсів на випадок кризи) та місцевих планів реагування (використання сил та ресурсів територій (громад) навколо об'єкта КІ). Плани реагування виконуються, персонал оператора КІ та залучених стейкхолдерів дотримуються процедур реагування, відбувається координація дій	Помірна ймовірність порушення роботи критичного об'єкта КІ; незначне зниження рівня надання основної послуги понад 10%; очікувана тривалість реагування та/або зниження рівня надання основної послуги на період до трьох днів	Оператор КІ; органи виконавчої влади місцевого рівня; суб'єкти в рамках реагування відповідно до законодавства
3	Відчутний вплив на населення та території, вплив поширюється на кілька територіальних громад (районів). Можлива необхідність проведення евакуації населення та персоналу низки об'єктів КІ під час реагування. Дії, події або умови, які спричинили вплив на КІ, зберігаються. Можливе загострення поточного інциденту, можливі повторні інциденти та існує ймовірність виникнення каскадних подій. Наявний суттєвий вплив на функціонування КІ та ключові ресурси оператора та навколишньої території. Урегулювання наслідків впливу загроз потребує задіяння державних систем реагування (залучення сил та ресурсів територіального рівня) на додачу до місцевих планів реагування та планів оператора КІ. Урегулювання інциденту передбачає координацію дій усіх залучених стейкхолдерів у порядку, визначеному законодавством, та здійснюється в рамках функціонування відповідальної державної системи реагування (відповідно до компетенції (виду загрози, що зумовила кризову ситуацію)). Потребує запровадження системи моніторингу розвитку ситуації та обміну інформацією з вищими рівнями державного управління	Суттєва ймовірність порушення роботи критичного об'єкта КІ або дво-трьох об'єктів КІ; суттєве зниження рівня надання основної послуги/функції понад 30%; очікувана тривалість реагування та/або зниження рівня надання основної послуги на період до семи днів	Місцеві та центральні органи державної влади на відповідних територіях; територіальні формування сектору безпеки та оборони відповідно до законодавства; оператор КІ

Закінчення таблиці 2

Рівні впливу	Базові елементи опису сценарію впливу загроз	Критерії ранжування сценарію за ймовірними наслідками впливу	Відповідальні за реагування
4	Значний вплив на населення та території; вплив поширюється на кілька регіонів (областей). Необхідність проведення евакуації населення та персоналу (в зоні реагування). Дії, події або умови, які спричинили вплив на КІ, зберігаються. Можливе загострення поточного рівня впливу загрози, існує ймовірність повторних інцидентів на різних об'єктах та територіях. Виникнення каскадних подій. Наявні в суб'єктів реагування ресурси зазвичай не відповідають потребам реагування протягом перших кількох днів. Можуть знадобитися додаткові види ресурсів для реагування. Урегулювання інциденту потребує задіяння державних систем реагування (залучення сил та ресурсів загальнодержавного рівня), місцевих спроможностей, спроможностей оператора КІ та інших можливих стейкхолдерів. Подолання інциденту потребує координації дій усіх залучених стейкхолдерів на загальнодержавному рівні (у рамках функціонування відповідальної державної системи реагування (виду загрози, що зумовила кризову ситуацію)). Потребує запровадження загальнодержавного координаційного штабу	Висока імовірність припинення роботи більше трьох об'єктів КІ в одному секторі; значне зниження рівня надання основної послуги/функції понад 50%; очікувана тривалість реагування та/або зниження рівня надання основної послуги на період до одного місяця	Центральні та місцеві органи державної влади; військове командування (при воєнному стані); формування сектору безпеки та оборони відповідно до законодавства; оператор КІ
5	Критичний вплив на населення та території всієї країни. Вимушеність масової евакуації населення та персоналу значної кількості об'єктів КІ. Дії, події або умови, які спричинили вплив на КІ, мають тривалий характер. Очікується загострення ситуації внаслідок тривалого терміну впливу, повторних інцидентів на різних об'єктах КІ та територіях. Очікується виникнення каскадних подій у різних секторах КІ та територіях. Наявні в суб'єктів реагування ресурси не відповідають потребам реагування протягом тривалого періоду. Гостра необхідність у додаткових численних видах ресурсів для реагування. Задіяння державних систем реагування загальнодержавного рівня та мобілізації всіх доступних сил та ресурсів інших стейкхолдерів. Запровадження спеціального правового режиму (надзвичайний стан, воєнний стан). Координація дій здійснюється окремо створеною координаційною структурою відповідно до законодавства про запровадження правового режиму	Висока імовірність припинення роботи понад десяти об'єктів КІ в одному секторі або порушення роботи понад трьох об'єктів у понад трьох секторах; значне зниження рівня надання основної послуги/функції понад 70%; очікувана тривалість реагування та/або зниження рівня надання основної послуги на період понад місяць	Військове командування; центральні органи державної влади; військові адміністрації; формування сили сектору безпеки та оборони, відповідно до законодавства

Розроблення детальних сценаріїв сприятиме підготовці визначеними суб'єктами планів заходів та процедур реагування залежно від рівня критичності ситуації. Напрацьовані заходи надалі мають бути враховані під час формування Плану оборони країни, мобілізаційних планів України та окремих секторів КІ.

Для формування надійних джерел фінансування заходів захисту КІ слід на законодавчому рівні визначити механізми фінансування сектору безпеки та оборони на цілі захисту КІ. Обсяги фінансових видатків доцільно визначати з огляду на перелік заходів, сформованих за результатами сценарного планування.

Таким чином, буде сформовано механізм планування розвитку спроможностей сектору безпеки та оборони, необхідних для реагування на визначені види загрози та рівні критичності їхнього впливу.

Висновки та рекомендації

Аналіз сучасних тенденцій розвитку систем захисту КІ у світі демонструє посилення ролі сил оборони в забезпеченні безпеки КІ. У мирний час збройні сили країн виконують допоміжну роль, підтримуючи дії цивільних суб'єктів реагування. Водночас поряд з безпосереднім завданням забезпечення захисту критичної військової інфраструктури дедалі чіткіше проявляється тенденція до уповноваження збройних сил на захист цивільної інфраструктури, передусім тієї від якої залежить виконання ними визначених для них місій. Досвід України в реагуванні на воєнні загрози КІ в умовах повномасштабної війни засвідчує необхідність ще більшого посилення ролі сектору оборони та його спроможностей забезпечити захист КІ.

Пропоноване сценарне планування з урахуванням рівнів критичності впливу стає практичним інструментом визначення необхідних спроможностей сил оборони та планування заходів захисту КІ. Запропоновані концептуальні підходи до розроблення сценаріїв дають підстави визначити заходи реагування на загрози різного рівня критичності та розмежувати їх за окремими суб'єктами реагування. У загальному підсумку запровадження сценарного планування забезпечить створення проактивного механізму розвитку спроможностей сил оборони та забезпечення безпеки і стійкості функціонування КІ.

Дослідження також дало змогу визначити напрями вдосконалення законодавства та розвитку спроможностей сил оборони, зокрема:

- визначення збройним силам ширшого завдання щодо організації захисту та забезпечення оборони (прикриття) об'єктів КІ;
- надання права збройним силам застосовувати і використовувати зброю та бойову техніку в мирний час для відбиття ударів засобів повітряного та підводного нападу на об'єкти КІ;
- включення до документів оборонного планування та застосування збройних сил, інших складових сил оборони положень щодо до захисту КІ України від воєнних загроз;
- уточнення положень про Міністерство оборони України та Генеральний штаб Збройних Сил України, інших суб'єктів сектору безпеки та оборони в частині деталізації їхньої ролі й завдань з питань захисту КІ;
- створення окремих структурних підрозділів суб'єктів сектору безпеки та оборони для забезпечення постійного процесу ідентифікації загроз КІ (та їхньої динаміки) й оцінювання ризиків порушення функціонування КІ (на стратегічному та оперативно-тактичному рівнях);
- розроблення сценаріїв застосування сил оборони для захисту КІ від воєнних загроз для різних рівнів критичності їхнього впливу та відповідних заходів захисту КІ;
- розроблення та внесення заходів забезпечення безпеки і стійкості функціонування КІ до Плану оборони країни, мобілізаційних планів України та планів окремих секторів КІ, планів територіальної оборони;
- запровадження цільового бюджетного фінансування заходів забезпечення захисту КІ від реалізації воєнних загроз;
- запровадження практики вивчення уроків, аналізу кращого досвіду забезпечення захисту КІ та поширення висновків у рамках системи підготовки персоналу сектору безпеки та оборони України;
- запровадження навчальних та освітніх програм з питань забезпечення безпеки і стійкості функціонування КІ силами оборони, а також програм перепідготовки персоналу.

Розроблення методології сценарного планування, напрацювання нормативної та методичної бази щодо розроблення заходів захисту відповідно до виду та рівня загроз, розроблення процедур взаємодії різних суб'єктів національної системи захисту КІ для адекватного реагування на воєнні загрози КІ стануть напрямами подальших досліджень.

Перелік літератури

1. Зелена книга з питань захисту критичної інфраструктури в Україні : зб. матеріалів міжнар. експерт. нарад / упоряд. Д. С. Бірюков, С. І. Кондратов ; за заг. ред. О. М. Суходолі ; Нац. ін-т стратег. дослідж. – К. : НІСД, 2016. – 174 с.

2. Про критичну інфраструктуру [Електронний ресурс] : Закон України № 1882-IX від 16 листопада 2021 р. // Верховна Рада України. Законодавство України. – Режим доступу : https://zakon.rada.gov.ua/laws/show/1882-20#n216.

3. *Sukhodolia O.* Ukrainian Energy Sector under Military Attack: Lessons for Resilience [Електронний ресурс] / O. Sukhodolia // War and Energy Security: Lessons for The Future / T. Jermalavičius (ed.), V.-P. Tynkkynen, A. Prokip et al. ; International Centre for Defence and Security. – 2023. –

P. 46–59. – Режим доступу : https://icds.ee/en/war-and-energy-security-lessons-for-the-future.

4. Use of Underground Facilities to Protect Critical Infrastructures: Summary of a Workshop [Електронний ресурс] / editors R. G. Little, P. B. Pattak, W. A. Schroeder ; National Research Council // National Academies. – Режим доступу : https://doi.org/10.17226/6285.

5. *Linger D. A.* Applications of Underground Structures for the Physical Protection of Critical Infrastructure / D. A. Linger, G. H. Baker, R. G. Little // North American Tunneling 2002 : Proceedings of the NAT Conference, 18–22 May 2002, Seattle / L. Ozdemir (ed.). – Leiden : CRC Press, 2002. – P. 333–341.

6. *Stevenson J.* The Role of the Armed Forces of the United Kingdom in Securing the State Against Terrorism [Електронний ресурс] / J. Stevenson // Connections. – 2005. – Vol. 4, No 3. – P. 121–133. – Режим доступу : https://www.jstor.org/stable/26323188.

7. The Challenge of Protecting Critical Infrastructure [Електронний ресурс] / P. Auerswald, L. M. Branscomb, T. M. La Porte et al. // Issues in Science and Technology. – 2005. – Vol. 22, No 1. – P. 77–83. – Режим доступу : https://www.jstor.org/stable/43314287

8. *Dunn-Cavelty M.* Public-Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection [Електронний ресурс] / M. Dunn-Cavelty, M. Suter // International Journal of Critical Infrastructure Protection. – 2009. – Vol. 2, issue 4. – P. 179–187. – Режим доступу : https://doi.org/10.1016/j.ijcip.2009.08.006.

9. Defending Critical Infrastructure [Електронний ресурс] / G. Brown, M. Carlyle, J. Salmerón, K. Wood // Interfaces. – 2006. – Vol. 36, No 6. – P. 530–544. – Режим доступу : https://www.jstor.org/stable/20141442.

10. *Tavares Da Costa R.* Impacts of climate change on defence-related critical energy infrastructure [Електронний ресурс] / R. Tavares Da Costa, E. Krausmann, C. Hadjisavvas // Publications Office of the European Union. – Режим доступу : https://doi.org/10.2760/116974.

11. *Jacuch A.* Countering Hybrid Threats: Resilience in the EU and NATO's Strategies [Електронний ресурс] / A. Jacuch // The Copernicus Journal of Political Studies. – 2020. – No 1. – P. 5–26. – Режим доступу : https://doi.org/10.12775/CJPS.2020.001.

12. *Суходоля О. М.* Захист критичної інфраструктури в умовах гібридної війни: проблеми та пріоритети державної політики України / О. М. Суходоля // Стратегічні пріоритети. – 2016. – № 3. – С. 62–76.

13. Hybrid warfare against Critical Energy Infrastructure: The Case of Ukraine [Електронний ресурс] / V. Butrimas, J. Hajek, O. Sukhodolia et al. ; NATO Energy Security Centre of Excellence // NATO Energy Security Centre of Excellence. – Режим доступу : https://www.enseccoe.org/publications/hybrid-warfare-against-critical-energy-infrastructure-the-case-of-ukraine.

14. *Evans C. V.* Future Warfare: Weaponizing Critical Infrastructure [Електронний ресурс] / C. V. Evans // Parameters. – 2020. – Vol. 50, No 2. – P. 35–42. – Режим доступу : https://doi.org/10.55540/0031-1723.1017.

15. *Tussing B.* Reinforcing the First Line of Defense: The Role of the National Guard in Critical Infrastructure Protection (CSL Issue Paper, Volume 12-05, August 2005) [Електронний ресурс] / B. B. Tussing, J. O. Kievit, R. W. Dillon ; Center for Strategic Leadership, U.S. Army War College // Defense Technical Information Center. – Режим доступу : https://apps.dtic.mil/sti/citations/ADA439253.

16. *Batiuk O.* National Guard of Ukraine military units critical infrastructure protection and defense assigned tasks [Електронний ресурс] / O. Batiuk, S. Bielai, V. Harmash // Honor and Law. – 2024. – Vol. 4, No 91. – P. 15–21. – Режим доступу : https://doi.org/10.33405/2078-7480/2024/4/91/324059.

17. Assistant Secretary of Defense for Homeland Defense and Global Security. DoD Protected Critical Infrastructure Program [Електронний ресурс] // Under Secretary of Defense for Policy. U.S. Department of Defense. – Режим доступу : https://policy.defense.gov/OUSDP-Offices/ASD-HDGS/Defense-Critical-Infrastructure-Program.

18. *Єрменчук О. П.* Основні підходи до організації захисту критичної інфраструктури в країнах Європи: досвід для України : монографія / О. П. Єрменчук ; Дніпроп. держ. ун-т внутр. справ. – Дніпро : ДДУВС, 2018. – 180 с.

19. Centres of Excellence [Електронний ресурс] // NATO. – Режим доступу : https://www.nato.int/cps/eb/natohq/topics_68372.htm.

20. Enabling NATO's Collective Defense: Critical Infrastructure Security and Resiliency (NATO COE-DAT Handbook 1) [Електронний ресурс] / C. V. Evans, C. Anderson, M. Baker et al. // US Army War College Press. – Режим доступу : https://press.armywarcollege.edu/monographs/955.

21. The role of science in resilience planning for military-civilian domains in the U.S. and NATO [Електронний ресурс] / J. M. Keenan, B. Trump, E. Kytömaa et al. // Defence Studies. – 2024. – Vol. 24, issue 4. – P. 493–524. – Режим доступу : https://doi.org/10.1080/14702436.2024.2365218.

22. EU–NATO Task Force on the resilience of critical infrastructure: Final assessment report [Електронний ресурс] // European Commission. – Режим доступу : https://commission.europa.eu/document/34209534-3c59-4b01-b4f0-b2c6ee2df736_en.

23. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (Text with EEA relevance) [Електронний ресурс] : Document 32022L2557 // European Union. EUR-Lex. – Режим доступу : http://data.europa.eu/eli/dir/2022/2557/oj

24. The Staying Power of Ukrainian Lights. Lessons of Wartime Resilience of the Electricity Sector [Електронний ресурс] / T. Jermalavičius (ed.), H. Roigas, O. Sukhodolia, D. Teperik // International Centre for Defence and Security. – Режим доступу : https://icds.ee/en/the-staying-power-of-ukrainian-lights-lessons-of-wartime-resilience-of-the-electricity-sector.

25. Про Збройні Сили України [Електронний ресурс] : Закон України від 6 грудня 1991 р. № 1934-XII // Верховна Рада України. Законодавство України. – Режим доступу : https://zakon.rada.gov.ua/laws/show/1934-12#Text.

26. Організаційно-технічні засади побудови системи інженерного захисту об'єктів критичної інфраструктури енергетичної галузі України [Електронний ресурс] / М. В. Коваль,

В. В. Коваль, В. І. Коцюруба, А. С. Білик // Наука і оборона. – 2022. – № 3–4. – С. 11–16. – Режим доступу : https://doi.org/10.33099/2618-1614-2022-20-3-4-11-16.

27. Про правовий режим воєнного стану [Електронний ресурс] : Закон України від 12 травня 2015 р. № 389-VIII // Верховна Рада України. Законодавство України. – Режим доступу : https://zakon.rada.gov.ua/laws/show/389-19#Text.

28. Bundeswehr der Zeitenwende: Kriegstüchtig sein, um abschrecken zu können [Електронний ресурс] // Bundesministerium der Verteidigung. – Режим доступу : https://www.bmvg.de/de/aktuelles/bundeswehr-der-zeitenwende-kriegstuechtig-sein-um-abzuschrecken-5765386.

29. Britain looking at options for air defence to defend UK [Електронний ресурс] // UK Defence Journal. – Режим доступу : https://ukdefencejournal.org.uk/britain-looking-at-options-for-air-defence-to-defend-uk.

30. *Smith B.* U.S. Army North highlights new concept to protect critical infrastructure [Електронний ресурс] / B. Smith // U.S. Army. – Режим доступу : https://www.army.mil/article/279940/u_s_army_north_highlights_new_concept_to_protect_critical_infrastructure.

31. National Incident Management System Incident Complexity Guide: Planning, Preparedness and Training [Електронний ресурс] // FEMA. – Режим доступу : https://www.fema.gov/sites/default/files/documents/nims-incident-complexity-guide.pdf.

32. Порядок класифікації надзвичайних ситуацій за їх рівнями [Електронний ресурс] : затверджений постановою Кабінету Міністрів України № 368 від 24 березня 2004 р. // Верховна Рада України. Законодавство України. – Режим доступу : https://zakon.rada.gov.ua/laws/show/368-2004-п#Text.

33. Про боротьбу з тероризмом [Електронний ресурс] : Закон України № 638-IV від 20 березня 2003 р. // Верховна Рада України. Законодавство України. – Режим доступу : https://zakon.rada.gov.ua/laws/show/638-15#Text.

34. Про національну безпеку України [Електронний ресурс] : Закон України № 2469-VIII від 21 червня 2018 р. // Верховна Рада України. Законодавство України. – Режим доступу : https://zakon.rada.gov.ua/laws/show/2469-19#Text.

35. *Суходоля О. М.* Стійкість критичної інфраструктури та життєво важливих функцій і послуг: формалізація завдань і змісту дій суб'єктів забезпечення [Електронний ресурс] / О. М. Суходоля // Стратегічна панорама. – 2023. – № 2. – С. 5–20. – Режим доступу : https://doi.org/10.53679/2616-9460.2.2023.01.