БЕЗПЕКА КРИТИЧНОЇ ІНФРАСТРУКТУРИ

УДК 351+355.01:321(477)

ЗАХИСТ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УМОВАХ ГІБРИДНОЇ ВІЙНИ: ПРОБЛЕМИ ТА ПРІОРИТЕТИ ДЕРЖАВНОЇ ПОЛІТИКИ УКРАЇНИ

Суходоля Олександр Михайлович,
доктор наук з державного управління, професор

У роботі аналізується досвід реагування України на загрози пошкодження критичної інфраструктури в умовах розв'язаної проти країни гібридної війни та визначаються пріоритети удосконалення державної політики з питань захисту критичної інфраструктури.

Відзначається розширення використання некласичних методів ведення війни та критичної інфраструктури як об'єкта цілеспрямованого впливу в сучасних концепціях ведення війн. Продемонстровано комплексне та узгоджене застосування Росією методів фізичного впливу (застосування збройних підрозділів, кримінальна діяльність, захоплення неідентифікованими особами) для безпосереднього пошкодження об'єктів критичної інфраструктури та методів політичного, економічного, інформаційного та психологічного впливу на Україну.

Визначено цільову спрямованість зловмисних дій проти критичної інфраструктури на здійснення психологічного тиску, нанесення економічних збитків, отримання локальних переваг в економічній, політичній та воєнній сфері, формування «необхідного іміджу» Росії на міжнародній арені, використання інфраструктури для провокацій.

Зроблено оцінку дій органів державної влади у сфері захисту критичної інфраструктури в умовах гібридної агресії, визначено проблеми реагування та координації їх дій в частині запобігання реалізації загроз стійкості функціонування, організації захисту об'єктів критичної інфраструктури та ліквідації наслідків пошкодження критичної інфраструктури.

Проаналізовано зміни законодавства в частині формування системи захисту критичної інфраструктури, визначено неузгодженості та проблеми його застосування. Розроблено пропозиції щодо пріоритетних напрямів вдосконалення законодавства, формування державної політики та державної системи захисту критичної інфраструктури виходячи з комплексного характеру загроз гібридної війни.

Ключові слова: критична інфраструктура, гібридна війна, захист критичної інфраструктури, охорона та оборона об'єктів, кіберзагрози, резервування та дублювання функцій, сектор безпеки і оборони, реформування системи управління.

Sukhodolia Oleksandr

PROTECTION OF CRITICAL INFRASTRUCTURE IN HYBRID WARFARE: PROBLEMS AND PRIORITIES OF STATE POLICY OF UKRAINE

The paper examines Ukrainian experience of response to threats to damage critical infrastructure in hybrid war unleashed against the country and determines priorities of improvement of the state policy on critical infrastructure protection.

The paper notes an expansion of non-classical methods of warfare and emphasizes the increasing of the use of the critical infrastructure as an object of malicious action in modern concepts of warfare. The impact of comprehensive and complex application of physical impact methods (use of army forces, criminal activity, etc.) to damage critical infrastructure together with methods of political, economic, informational and psychological pressure on country's ability to resist aggressor's attack was demonstrated on example of Ukraine.

The paper describes the goals of malicious acts against critical infrastructure that Russia used in the war against Ukraine, namely: to produce psychological pressure, cause economic damage, get tactic and strategic advantages in the economic, political and military sphere, build a "desired image" of Russia on the international arena, use of the infrastructure for provocations.

It was made a conclusion that damaging of critical infrastructure utilizing terrorist tactics became an important part of Russian state strategy of warfare against Ukraine, not just the strategy of separate terroristic groups as it was thought before.

The paper evaluates actions of Ukrainian institutions in relation to on critical infrastructure protection under conditions of hybrid aggression, defines problems of response and coordination of their actions in order to deter threats to the stable infrastructure functioning, suggests tools to build resilience of critical infrastructure and mitigate the consequences of damage to critical infrastructure.

It was shown that current systems of protection and response properly do not incorporate threats raised by hybrid warfare and there is an urgent need to implement "all hazards" approach to threats analysis and further improvement of legislation, public policy development and designing of critical infrastructure protection system.

The changes in the legislation regarding formation of a unified state system of critical infrastructure protection and proposals on priority directions of state policy on the issue were proposed. The development of Law of Ukraine "On critical infrastructure protection" is the first step that needs to be done.

Keywords: critical infrastructure, hybrid warfare, malicious acts, cyberthreats, protection of critical infrastructure, redundancy and duplication of functions of resilience and response, security and defense sector, response system.

Намагання України реалізувати підтриманий переважною більшістю її громадян євроінтеграційний вибір свого подальшого розвитку викликало шалену протидію з боку Росії. Втративши внаслідок Революції гідності інструменти «несилового» впливу на Українську державу, РФ розпочала наступний етап реалізації своєї політики – війну, що у повній відповідності з формулою К. Клаузевіца «є продовження політики іншими засобами».

Водночас політичні та організаційно-технічні особливості реалізації інтересів керівництва Росії на внутрішній та міжнародній арені обумовили особливість цього етапу – активізацію особливого комплексу методів та засобів ведення війни, які стали маркуватись назвою «гібридна війна»[1].

Вибір такої форми може пояснюватися двома аспектами. З одного боку, це намагання досяг-

[1] На наш погляд, гібридна війна не є новим феноменом, а лише відображає застосування нових методів та інструментів (чи трансформованих до вимог нового часу старих методів) реалізації інтересів країни-агресора. У війні проти України Росія застосувала практику диверсійної діяльності, економічного та психологічного тиску, пропаганди та інформаційного маніпулювання, при широкому залученні кримінальної практики для досягнення цілей, що в комплексі стало несподіваним для не підготовленої до такого розвитку подій сусідньої держави.

нути своїх цілей, використовуючи розвиток технологій суспільного управління в Росії, а саме, розвиток військової науки, практики застосування економічних та політичних методів тиску на інші країни, застосування методів інформаційного та психологічного впливу на суспільство і людину, відпрацьованих передусім на російському народі. З другого боку, це намагання, використовуючи неузгодженості міжнародного права та культурно-політичні суперечності на міжнародній арені, залишитись у рамках визнання міжнародним співтовариством, будь-що закріпити свої позиції як «однієї із лідируючих держав в умовах поліцентричного світу» [1].

Ця особливість і зумовила ту форму гібридної війни, яка в рішенні РНБО України «Про Концепцію розвитку сектору безпеки і оборони України» (Указ Президента України від 14.03.2016 р. № 92/2016) була визначена як «комбінація різноманітних і динамічних дій регулярних сил Російської Федерації, що взаємодіють зі злочинними озброєними угрупованнями та кримінальними елементами, діяльність яких координується і здійснюється за єдиним замислом і планом із активним застосуванням засобів пропаганди, саботажу, навмисного завдання шкоди, диверсій і терору».

Таке розуміння змісту гібридної війни перегукується із роботою американського науковця Ф. Гофмана [2], який визначає гібридну війну як «одночасне і адаптивне застосування складного поєднання звичайних озброєнь, нерегулярної війни, тероризму і кримінальної поведінки в зоні ведення війни задля досягнення політичних цілей».

При такому типі війни порушення спроможності інфраструктури життєдіяльності країни виконувати свої функції стає одним з її інструментів, дія якого спрямовується на підрив спроможності країни протистояти агресору.

Даний аспект ведення війни, зокрема пошкодження критичної інфраструктури як інструмент гібридної війни, є новим напрямом наукових досліджень. При цьому саме український досвід та відповідні публікації українських науковців стають базою для подальших наукових досліджень та формування заходів реагування на нові виклики.

У роботах В. Горбуліна [3,4] та М. Гончара [5,6] аналізуються передумови формування гібридної агресії Росії проти України та формується основа для її операціоналізації у безпековій політиці країни. Питанням захисту критичної інфраструктури (КІ) присвячено працю фахівців Національного інституту стратегічних досліджень під назвою «Зелена книга (ЗК) з питань захисту критичної інфраструктури України» (Бірюков Д.С., Кондратов С.І., Насвіт О.І., Суходоля О.М.) [7] та інші роботи цих авторів, які розкривають теоретичні засади, досвід розробки концепції захисту критичної інфраструктури, пріоритетів формування політики захисту КІ та механізмів її реалізації.

Безпосереднє ж дослідження цілеспрямованих дій проти КІ в рамках розв'язаної гібридної війни, з акцентом на критичній енергетичній інфраструктурі, на сьогодні відображено лише в окремих роботах [5,8,9].

Водночас проблеми реагування системи державної влади на виклики, що породжені гібридною війною, зокрема в частині забезпечення стійкості функціонування КІ, ще не досліджувалися, щонайменше у наявних відкритих публікаціях. Саме на аналіз дій системи органів державної влади щодо захисту КІ та реагування на нові виклики, породжені гібридною агресією, визначення проблем та пріоритетних напрямів формування цього напряму безпекової політики України і спрямована ця робота.

Одним із пріоритетних напрямів безпекової політики України повинно стати підвищення безпеки та стійкості національної КІ[2] до всього спектру загроз і ризиків, оскільки саме КІ забезпечує життєво важливі для населення, суспільства та держави послуги та функції, без яких неможливі їх безпечне існування та добробут, а також належний рівень національної безпеки [7].

Сьогодні це питання набуває особливої уваги. З одного боку, спостерігається загальносвітова тенденція до різкого посилення екстремізму та тероризму, небувале зростання організованої злочинності, у т.ч. міжнародної, що загалом

[2] У «Зеленій книзі...» під КІ розуміють «системи та ресурси, фізичні чи віртуальні, що забезпечують функції та послуги, порушення яких призведе до найсерйозніших негативних наслідків для життєдіяльності суспільства, соціально-економічного розвитку країни та забезпечення національної безпеки».

ускладнює безпекову ситуацію для всіх без винятку країн світу. З другого боку, дії Росії в Україні та Сирії вказують на те, що вплив на функціонування КІ може стає інструментом підриву стабільності соціально-економічної ситуації в країні як шляхом завдання економічної шкоди, так і через здійснення психологічного впливу на політиків та населення країни, підбурювання до соціально-політичних протестів проти уряду країни [9].

Слід зазначити, що і в передвоєнний час Росія активно застосовувала окремі елементи інфраструктури, а саме енергетику, як «енергетичну зброю» для досягнення цілей своєї політики у зовнішньополітичному вимірі. Цей аспект неодноразово відзначався фахівцями у сфері енергетики, хоча багато представників західноєвропейської політичної еліти та аналітиків, бажаючи залишитись у дружніх стосунках із важливим постачальником енергоресурсів, намагались розглядати поведінку Росії виключно в межах економічної раціональності. Для України ж, як і для інших країн колишнього СРСР, застосування Кремлем енергетики як інструменту обмеження суверенітету було реальністю та відображало перманентну «приховану» війну між Україною з її бажанням отримати енергетичну незалежність та Росією, яка намагалася зберегти Україну у сфері своїх політичних, економічних та технічних інтересів [9].

Серед основних цілей такої політики Росії було зберегти залежність української економіки від поставок власних енергоресурсів, законсервувати неефективну систему управління в енергетиці України, що базується на популізмі політиків, зберегти вплив на функціонування критичної енергетичної інфраструктури, зокрема на роботу газотранспортної системи України, об'єднаної енергосистеми України, ключових підприємств енергетичної галузі.

Перейшовши до наступного етапу реалізації своєї політики України – етапу гібридної війни, Росія поставила світове співтовариство перед новим викликом. Руйнування інфраструктури життєдіяльності суспільства стало інструментальним виміром її намагання підпорядкувати Україну не стільки через завдання поразки її Збройним Силам, скільки через невдоволення населення урядом. Фактично Росією продемостровано, що гібридна, інфраструктурна війна як комплекс дій, спрямованих на погіршення умов життєдіяльності населення та функціонування економіки окремої країни, має за мету формування умов для введення на державні посади в країні, стосовно якої здійснюється агресія, людей, готових враховувати інтереси агресора.[3]

В умовах глобалізації економіки та торгівлі, об'єднання інфраструктурних мереж і водночас – порушення міжнародної системи безпеки, знищення інфраструктури життєдіяльності суспільства може навіть виступати інструментом опосередкованого впливу одних країн на інші, навіть на країни, які не причетні до конфлікту. Свідченням цього є міграційний потік із країн, охоплених війною (Сирія, Ірак, Афганістан), до країн ЄС.

У цій ситуації важливим чинником забезпечення національної безпеки є спроможність органів державної влади та суспільства забезпечити адекватне реагування на загрози стійкості[4] функціонування КІ.

Загрози КІ, породжені гібридною агресією

Росія активно використовувала різні гібридні методи порушення стійкості функціонування інфраструктури життєдіяльності України – як опосередкованого характеру (економічні, інформаційні), так і прямого фізичного впливу (руйнування, блокування, захоплення). Серед випадків **цілеспрямованого фізичного впливу** слід виокремити [8,9]:

- фізичне захоплення об'єктів при збереженні їх функціональності (змінювався отримувач ренти від їх функціонування, наприклад захоплення енергетичних активів Криму);

[3] У цій ситуації досить симптоматичними видаються заяви та дії окремих політичних сил та громадських організацій у політико-економічному просторі України у 2015–2016 роках, особливо в частині збереження України, зокрема її енергетичного сектору, під впливом сформульованих в Росії рішень (збереження системи субсидування і, відтак, традиційної системи взаємовідносин в енергетичній сфері, обсягів поставок енергоресурсів, механізмів взаєморозрахунків).

[4] «Зелена книга...» під стійкістю КІ розуміє «здатність надійно функціонувати у нормальному режимі, адаптуватися до умов, що постійно змінюються, протистояти та швидко відновлюватися після аварій та технічних збоїв, зловмисних дій, природних лих та небезпечних природних явищ».

- припинення функціонування об'єктів, у тому числі внаслідок фізичного захоплення, для завдання збитків попередньому власнику чи обміну на «потенційні» переваги в інших сферах (задоволення політичних чи економічних вимог, як-от умови постачання вугілля до України, викуп активів, вплив на ринкову вартість компаній та сировини тощо);
- розукомплектування окремих елементів інфраструктури з метою отримання кримінального доходу (масові факти різання критичної інфраструктури на окупованих територіях Донбасу для продажу у вигляді металобрухту);
- фізичне знищення об'єкта для завдання критичної шкоди, збільшення витрат на подолання стану порушення функціонування інфраструктури (наприклад, неможливість доставити ресурси);
- перешкоджання діяльності з відновлення функціональності енергетичної інфраструктури та формування суспільно-політичного невдоволення.

При цьому зазначені дії спостерігалися не тільки щодо енергетичної, а й щодо транспортної, інформаційно-комунікаційної, комунальної інфраструктури та інших. Більш того, поряд із руйнуванням транспортної інфраструктури на окупованій території Донбасу, Росія вдавалася до блокування транспортної інфраструктури і на кордоні України та Росії. Наприклад, для блокування постачання вугілля на електростанції України не тільки підривали залізничні колії, мости на лінії зіткнення, а й блокувалось постачання вугілля з території Росії. Так, у листопаді-грудні 2014 та 2015 років на українсько-російському кордоні періодично блокувалися тисячі вагонів із вугіллям, яке було критично необхідним для забезпечення стійкості роботи об'єднаної енергосистеми України.

Слід зазначити, що дії з безпосереднього фізичного впливу на інфраструктуру супроводжувалися методами інформаційно-пропагандистського впливу на різні групи населення та політиків.

Російські ЗМІ активно намагалися продемонструвати турботу вищого керівництва Росії про людей України, зокрема пропагуючи російські «гуманітарні» поставки електроенергії та природного газу. Прикладом цього є активне рекламування заяви Д. Медведєва про «газовий гуманітарний конвой» для людей Донбасу[5], постачання електроенергії на Донбас та до Криму, врятування В.Путіним «замерзаючого» Геніческа взимку 2015-2016 років[6]. При цьому російська пропаганда звинувачувала українську сторону через незгоду оплачувати неконтрольовані поставки та припинення постачання води та електроенергії до окупованого Криму.

Кремль намагався навіть залучити дипломатів країн ЄС до формування своєї версії подій. Так, у ситуації підриву опор ліній електропередач та тимчасового припинення електропостачання Криму заява прес-секретаря МЗС Німеччини щодо злочинних дій з припинення електропостачання Криму[7] разом із заявами проросійських політиків в Україні фактично була елементом єдиної інформаційно-пропагандистської кампанії Кремля.

Населенню України активно розповідали про загрози припинення енергопостачання, неспроможність українського уряду врегулювати проблеми стійкості функціонування енергетики України, відключення споживачів від газо-, тепло- чи електропостачання. Паралельно здійснювалася масована інформаційна кампанія щодо критики дій уряду з реформування енергетичного сектору, зокрема системи субсидування.

Саме сукупність таких дій та їх комплексний вплив на спроможність країни протистояти тискові агресора і визначають гібридність методів ведення війни. Аналізуючи вплив зазначених дій на обороноспроможність та стійкість

---

[5] У лютому 2015 р. прем'єр РФ Дмитро Медведєв закликав «Газпром» подумати про поставки газу в Донбас у рамках «гуманітарної допомоги». За повідомленням голови «Газпрому» О.Міллера, до 21 квітня ця компанія неконтрольовано поставила на Донбас 555 млн куб. м газу на 174,2 млн дол. На травень 2016 року «Газпром» уже вимагав сплатити уже 670 млн дол. США. за газ, поставлений на окуповані території в порушення умов контракту. «Нафтогаз» не приймав від «Газпрому» газ на пунктах входу до ГТС на непідконтрольних територіях і не має наміру його оплачувати. Див. повідомлення прес-служби НАК «Нафтогаз України» від 18.05.2016 р.

[6] Інформаційна компанія про звернення мера Геніческа до Путіна (що насправді було видумкою пропаганди) та здійснення за дорученням Путіна гуманітарної місії із забезпечення міста газом.

[7] *Германия* назвала подрыв украинских ЛЭП преступным актом [Електронний ресурс]. – Режим доступу: http://www.dw.com/ru/германия-назвала-подрыв-украинских-лэп-преступным-актом/a-18868997?maca=rus-tco-dw

країни, можемо виділити «енергетичний вимір» інструментарію гібридної війни [9], що працювали на:

- **зниження рівня обороноздатності країни** шляхом руйнування транспортних комунікації, систем зв'язку та забезпечення ресурсами збройних формувань, правоохоронних сил та сил цивільного захисту тощо;
- **завдання економічних збитків** національній економіці та окремим суб'єктам господарювання через захоплення енергетичних об'єктів і ресурсів, необхідність додаткових витрат на відновлення інфраструктури, потребу в додаткових поставках ресурсів чи блокування поставок окремих товарів через кордон та перешкоджання функціонуванню транскордонної інфраструктури;
- **отримання локальних (тактичних) переваг**, як-от досягнення кращої позиції у проведенні окремих операцій (бойові зіткнення, контрактні умови постачання товарів чи політичні переговори тощо), примус до здійснення окремих дій (платежів за товари чи послуги, продажу чи закупівлі ресурсів);
- **здійснення психологічного тиску різні групи населення та політиків** через створення інформаційних приводів з метою поширення панічних настроїв, соціальної напруги та невдоволення керівництвом країни;
- **формування необхідного «іміджу» на міжнародній арені** для досягнення зовнішньополітичних цілей Росії (зняття санкцій, зміна влади та федералізація України, нехтування іншими країнами транзитним потенціалом України, передусім у частині транспортування природного газу);
- **використання інфраструктури для провокацій**, зокрема транспортної інфраструктури та повітряного простору України (як у випадку із трагедією авіарейсу MH17[8]), блокування відновлення КІ в зоні бойових дій, блокування транзиту товарів через російський кордон, звинувачення України у блокуванні транзиту з Росії до країн Європи.

Українське суспільство, передусім на початковому етапі війни, не було готовим до таких дій, а система органів державної влади не усвідомлювала важливості функціонування КІ, виявилася не готовою до реагування на такі методи ведення війни.

Досвід реагування України на гібридні загрози КІ

Серед найбільш істотних проблем слід зазначити відсутність на загальнодержавному рівні узгодженої системи захисту КІ, реагування на випадок виникнення кризи та відповідної законодавчої бази, яка б визначала відповідальність та повноваження відповідних органів державної влади у цій сфері.

Слід мати на увазі, що використання законодавчих можливостей також було обмежене через недосконаліть або ж відсутність необхідних рішень.

Відсутність законодавчо визначеного порядку та рішення щодо запровадження особливого періоду (воєнний стан) фактично спричинила брак чітких та однозначних правил взаємодії держави і суб'єктів господарювання, можливості мобілізувати ресурси суб'єктів господарювання на забезпечення стійкості функціонування КІ, забезпечити адекватну координацію дій суб'єктів господарювання та держави із забезпечення охорони та оборони важливих об'єктів КІ.

Більш того, спостерігалося намагання суб'єктів господарювання, особливо приватного сектору, використати кризову ситуацію на свою користь. У періоди загострення ситуації в зоні АТО, що призводило до пошкодження електроенергетичної інфраструктури (зупинка ТЕС, руйнування підстанцій та ліній електропередач) на межі розмежування, електричні станції на мирній території не тільки зупинялися через брак вугілля, а й на ремонтні роботи, при цьому їх власники скаржились на низькі тарифи на електроенергію, що не дозволяють забезпечити надійну роботу електростанцій[9].

Слід зазначити, що фактично не функціонували плани реагування на випадок терористичних

[8] Серед гіпотез пояснення атаки проти авіалайнера MH17 «Амстердам –Куала-Лумпур» є гіпотеза про намагання Росії отримати причину війни (*casus belli*) для легалізації, перед міжнародним співтовариством, відкритої агресії проти України. За даною гіпотезою, нідерландський MH17 був збитий помилково, замість російського авіалайнера SU2074 за маршрутом «Москва – Ларнака».

[9] Див. повідомлення ЗМІ щодо ситуацій у листопаді-грудні 2014 р. та липні-серпні 2015 р., ряд електростанцій з різних причин було зупинено, і в Україні запроваджувалися графіки відключення споживачів від електропостачання.

актів проти об'єктів КІ, а мобілізаційні плани функціонування економіки та органів державної влади в особливий період, які не переглядалися тривалий час, втратили свою актуальність та дієвість.

Мали місце також запізнення та неефективність дій органів державної влади та силових структур з реагування на загрозу пошкодження КІ та забезпечення її відновлення. Недосконаліть системи захисту призводила й до суттєвих розбіжностей дій окремих органів влади та охоронних підрозділів з параметрами та умовами організації захисту, визначеними міжвідомчими актами.

Фактично досвід протидії гібридній війні в Україні був отриманий, а форми реагування на відповідні загрози – розроблені вже під час цієї війни. На першому етапі Україна реагувала за обставинами, наявними силами та ресурсами, часто без належного законодавчого врегулювання окремих аспектів.

Пізніше були сформовані рішення, які дозволили частково стабілізувати ситуацію в частині забезпечення функціонування КІ, зокрема:

- введення в дію плану територіальної оборони України, формування батальйонів сил територіальної оборони, виконання завдань територіальної оборони, зокрема щодо захисту об'єктів КІ;
- взяття під охорону особливо важливих об'єктів КІ, особливо важливих підприємств економіки та органів державної влади силами правоохоронних органів;
- створення антикризових комісій (центрів) для оперативного вирішення проблем із постачанням наявних ресурсів, важливих для функціонування КІ, та запровадження додаткових організаційно-технічних заходів захисту КІ;
- проведення силами військових та правоохоронців допоміжної роботи: спорудження та укріплення блокпостів на всіх ключових комунікаціях; роз'яснювальна робота з населенням щодо важливості забезпечення функціонування КІ; організація взаємодії підрозділів цивільного захисту з обласними державними адміністраціями (обласними військово-цивільними адміністраціями), місцевими органами влади;
- формування системи комунікацій між ворогуючими сторонами, із залученням представників конфлікту та міжнародного моніторингу для встановлення тимчасового локального перемир'я для проведення робіт із відновлення КІ;
- винесення питань захисту та відновлення КІ у політичну площину та на міжнародний рівень (зокрема мінський переговорний процес).

Водночас слід зазначити, що всі реалізовані заходи фактично були заходами реагування на факти пошкодження КІ (реактивний підхід) та заходами захисту населення; лише в поодиноких випадках здійснювалися кроки в напрямі запобігання виникненню кризової ситуації (проактивний підхід).

Для підвищення рівня спроможності України адекватно реагувати на сучасні виклики КІ, породжені гібридною війною, слід суттєво змінити державною політику та законодавство. Майбутнє слід будувати з огляду на те, що «інфраструктурна війна» стає реальним робочим інструментом. Тому на перший план виходить завдання щодо забезпечення спроможності КІ виконувати свої функції (надавати послуги) навіть у випадку пошкодження окремих об'єктів КІ. Цей напрям відомий у світовій практиці як «планування на випадок кризових ситуацій (*contingency planning*) та застосовується у світовій практиці, як у державному управлінні, так і в діяльності суб'єктів господарювання різних форм власності.

Удосконалення державної політики захисту КІ

Загалом стратегічні документи держави і законодавство у сфері національної безпеки вже давно потребували системного оновлення. Породжені гібридною війною явища зумовили швидкі та суттєві зміни у секторі безпеки і оборони країни, які частково посилили увагу до проблематики захисту КІ.

Було прийнято нову редакцію Стратегії національної безпеки України (Указ Президента України від 26.05.2015 р. № 287/2015), у якій, зокрема, визначено загрози безпеці КІ (недостатній рівень захищеності КІ, у тому числі від терористичних посягань, а також неефективне управління безпекою КІ) та пріоритетні напрями забезпечення її безпеки (посилення охорони об'єктів КІ; розвиток державно-приватного партнерства у цій сфері; обмін інформацією стосовно загроз КІ та захисту чутливої інформації у цій сфері).

РНБО України у липні 2015 р. обговорила проблеми підвищення рівня захисту атомних електростанцій України, за результатами чого було затверджено нову «Проектну загрозу для ядерних установок, ядерних матеріалів, радіоактивних відходів та інших джерел іонізуючого випромінювання в Україні», яка враховує зміни безпекової ситуації внаслідок агресії РФ [11].

Прийнято нову редакцію Воєнної доктрини України, де уточнюються завдання та повноваження окремих органів сектору безпеки і оборони щодо захисту об'єктів КІ.

Також активізовано зусилля щодо посилення захисту від кіберзагроз та створення національного центру кіберзахисту для забезпечення потреб обороноздатності держави в особливий період. Питання кібербезпеки стало предметом окремого рішення РНБО, прийнято Стратегію кібербезпеки України (Указ Президента України від 15.03.2016 р. № 96/2016), де також відображено питання формування правової основи кіберзахисту об'єктів КІ загалом та формування системи захисту інформаційної критичної інфраструктури.

Прийнято Концепцію розвитку сектору безпеки і оборони України (Указ Президента України від 14.03.2016 № 92/2016), де окремо акцентовано увагу на необхідності забезпечення безпеки об'єктів КІ, контррозвідувального захисту КІ, захисту критичної інформаційної інфраструктури, забезпечення відповідного інформаційно-аналітичного супроводу, зокрема шляхом створення мережі ситуаційно-кризових центрів.

Удосконалено низку інших нормативно-правових актів з питань захисту об'єктів та оборони, зокрема, уточнено правові засади діяльності відновленої Національної гвардії України, зокрема щодо охорони органів державної влади, ядерних установок, важливих державних об'єктів та інших об'єктів, що можуть бути віднесені до КІ (постанова Кабінету Міністрів України від 12.11.2014 р. № 628).

Прийняття зазначених стратегічних документів ставить нові завдання для сектору безпеки і оборони щодо посилення спроможності України забезпечити стійкість країни та сталість суспільного розвитку.

Водночас, поряд із формуванням завдань та цілей політики, що на стратегічному рівні адекватно відображають виклики сьогодення, на практиці спостерігається інерційність та нерозуміння проблем у цій сфері.

Кабінет Міністрів України, намагаючись оперативно відреагувати на загрози об'єктам КІ, діяв у традиційній управлінській манері надання завдань та доручень окремим відомствам. За результатами селекторної наради 23.01.2015 р. «з питань безпеки громадян та захисту найважливіших об'єктів інфраструктури» Мінекономрозвитку разом із центральними та місцевими органами виконавчої влади було доручено (доручення Прем'єр-міністра України № 2442/0/1-15) сформувати перелік об'єктів транспортної та іншої КІ, а також місць масового перебування людей, які потребуватимуть першочергового захисту.

При обласних державних адміністраціях (а також районних, міських) були створені оперативні штаби для координації роботи щодо забезпечення безпеки громадян, захисту об'єктів інфраструктури та своєчасного реагування на можливі надзвичайні ситуації. Розпорядженнями визначалися заходи щодо координації дій територіальних підрозділів правоохоронних органів, органів виконавчої влади і місцевого самоврядування, служб цивільного захисту, суб'єктів господарювання щодо забезпечення належного рівня техногенної безпеки та сталого функціонування об'єктів КІ.

У тому ж січні 2015 р. Кабінет Міністрів України затвердив Положення про Державну комісію з питань техногенно-екологічної безпеки та надзвичайних ситуацій і її склад (постанова Кабінету Міністрів України від 26.01.2015 р. № 18), яка теоретично мала б вирішити питання координації дій різних органів державної влади з питання захисту КІ та реагування на випадки її пошкодження. Однак органи державної влади та уповноважені особи фактично продовжували діяти в рамках звичних процедур реагування на надзвичайні ситуації цивільного характеру, спричинені природними та техногенними чинниками, залишаючи поза увагою загрози, породжені гібридною агресією.

За умовчуванням, захист КІ було автоматично переадресовується до сфери відповідальності Державної служби України з надзвичайних ситуацій. Хоча аналіз вказує, що вона не має повноважень (див.Положення про службу) і не

могла здійснювати захист КІ в умовах гібридної агресії. Дії ДСНС лише частково стосувалися забезпечення стійкості функціонування КІ та зосереджувались на забезпечені взаємодії та взаємодопомоги у вирішенні питань захисту населення із збройними та правоохоронними силами, гуманітарному розмінуванню місцевості та об'єктів інфраструктури, організації взаємодії із місцевими органами державної влади. Однак, попри недосконалість взаємодії сил цивільного захисту з військовими та іншими спеціальними формуваннями, зусилля ДСНС дозволили забезпечити нормальні умови життєдіяльності населення та функціонування об'єктів на території, яка підконтрольна українській владі.

Серед «цивільних» відомств найбільше коло завдань у сфері захисту КІ, відповідно до законодавства, має Мінінфраструктури (див. Положення про міністерство). Водночас безпосередня діяльність міністерства щодо її захисту була обмежена організаційними рішеннями про посилення охорони транспортної інфраструктури чи налагодження нових маршрутів постачання товарів, які ще мають довести свою логістичну та економічну привабливість[10]. При цьому слід відзначити діяльність Державної спеціальної служби транспорту, яка входить до сфери управління Мінінфраструктури в частині забезпечення охорони транспортної інфраструктури (мостів, об'єктів транспорту та гідротехнічних споруд), що дало змогу суттєво підвищити рівень їх захищеності.

Міненерговугілля в частині забезпечення функціонування критичної енергетичної інфраструктури мало чи не найсерйозніші проблеми. У найбільш кризовий період (зима 2014–2015 років) Україна була змушена запровадити надзвичайну ситуацію на ринку електроенергії, застосувати аварійні графіки відключення, що дозволило частково стабілізувати добову ситуацію та попередити технологічні порушення в об'єднаній енергосистемі України. У серпні 2015 р. був розроблений «План підготовки паливно-енергетичного комплексу України до осінньо-зимового періоду 2015–2016 років та його проходження», який фактично був побудований за методологією «плану попередження криз» та передбачав заходи щодо запобігання, усунення або пом'якшення ризиків порушення функціонування КІ.

Важким викликом була ситуація із постачанням антрацитового вугілля на електростанції України, враховуючи, що всі шахти, які видобували цей тип вугілля, знаходилися на окупованій території. Спроби налагодити поставки вугілля за імпортом з інших країн не можна назвати цілком успішним. Водночас рішення про постачання вугілля з окупованих територій призвело до створення напівофіційних схем та фактично опосередкованого фінансування Україною війни проти себе. В умовах ведення гібридної війни нечіткість законодавства та нелогічність взаємовідносин створює додаткові ризики для політичної стабільності та додає додаткові важелі впливу агресора на Україну, її посадових осіб та політиків, які і реалізовувались в інформаційному та політичному просторі України.

Що ж до «силових» відомств, то слід відзначити суттєве розширення кола завдань правоохоронних органів. У системі МВС у березні 2014 р. відновлено функціонування Національної гвардії України – військового формування з правоохоронними функціями. Одним із найважливіших завдань Національної гвардії України стало завдання фізичного захисту окремих об'єктів КІ, завдяки чому було забезпечено охорону: органів державної влади, атомних електростанцій, інших ядерних установок та матеріалів, важливих державних об'єктів та спеціальних вантажів, а також важливих стратегічних об'єктів економіки, об'єктів КІ.

Загалом слід зазначити, що загальна активізація «охоронної» діяльності не може трактуватись однозначно.

По-перше, охоронні послуги мають бути оплачені. Постановою Кабінету Міністрів України від 11.11.2015 р. №937 було уточнено перелік об'єктів державної та інших форм власності, які мають охоронятися виключно органами поліції охорони [12]. Причому визначено, що видатки на охорону суб'єктів господарювання мають здійснюватися за їх рахунок (очевидно, з відображенням цього у цінах на послуги та продукцію), а стосовно охорони об'єктів державної власності міністерствам та іншим суб'єктам

[10] Мова іде про налагодження поставок товарів в обхід Росії через порти Чорного моря, зокрема контейнерних перевезень за маршрутом Україна – Кавказ – Китай та, спільно з Міненерговугілля, поставок вугілля з Південної Африки (див. публікації ЗМІ щодо неоднозначності цих проектів).

управління доручалося забезпечити укладення з органами поліції охорони договорів про надання послуг з охорони[11].

Безоплатній охороні підлягали органи державної влади, які визначались у відповідному переліку, затвердженому постановою Кабінету Міністрів України від 25.11.15 р. № 971 «Про затвердження переліку органів державної влади, що підлягають безоплатній охороні Національною гвардією». Однак при цьому зазначені органи влади подавали Міністерству фінансів інформацію про обсяг видатків, які передбачені в кошторисах на 2015 рік та проекті Державного бюджету України на 2016 рік для здійснення оплати послуг з їх охорони.

Цей аспект захисту об'єктів в умовах війни та ресурсних обмежень формує суттєві ризики досягнення цілей такого управлінського рішення.

По-друге, посилення лише фізичного захисту окремих об'єктів не дозволяє вирішити проблему стійкості функціонування більшої системи, що із цих об'єктів складається. Система захисту КІ поряд із таким виміром, як «фізична захищеність», що реалізується через «охорону та захист», має також включати такий вимір, як «стійкість КІ» (*resilience*). Цей аспект захисту має передбачати формування спроможностей забезпечити виконання функцій (надання послуг) навіть у випадку пошкоджень та швидкого відновлення нормального функціонування та реалізовуватися через «резервування», «дублювання» КІ, створення запасів та ресурсів для «відновлення». Слід зазначити, що даний аспект забезпечення стійкості КІ може потребувати значно менших ресурсів, ніж «охорона» всіх об'єктів КІ.

Окрім того, такі сучасні загрози, як кібератаки або ж руйнування об'єкта силами його ж персоналу, перебувають за межами компетенції існуючих охоронних підрозділів.

Нинішній підхід до вирішення проблеми реагування на нові виклики функціонуванню КІ, а саме, збереження традиційного розуміння загроз КІ та можливості їх вирішення традиційними заходами посилення «охорони», покладання на існуючі органи влади додаткових завдань без делегування відповідних функцій та повноважень, на наш погляд, не дозволяє підвищити стійкість КІ в умовах сучасних гібридних загроз.

Пріоритетні завдання формування системи захисту КІ

Функція КІ полягає в забезпеченні постачання населенню, суспільству, бізнесу і державі життєво важливих товарів та послуг. Для виконання зазначеної функції необхідно гарантувати безперебійне, стале функціонування об'єктів КІ, мати спроможність запобігати припиненню їх функціонування та забезпечувати їх швидке відновлення у випадку пошкодження [7].

Ця мета, за діючого законодавства та з урахуванням викликів гібридної війни, потребує залучення щонайменше трьох існуючих державних систем реагування та захисту, зокрема:

- Єдиної державної системи цивільного захисту (Положення затверджене постановою Кабінету Міністрів України від 09.01.2014 р. № 11),
- Єдиної системи запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків (Положення затверджене постановою Кабінету Міністрів України від 15.08.2007 р. № 1051),
- Державної системи фізичного захисту (Порядок функціонування затверджений постановою Кабінету Міністрів України від 21.12.2011 р. № 1337).

На жаль, згадані системи створені для реагування на окремі види загроз та не формують узгодженої системи реагування на загрози комплексні. Більш того, існуюча ситуація відображає свідчить про домінування відомчих підходів до розв'язання безпекових проблем національного масштабу, а узгодження конкуруючих потреб відбувається складно.

Продовжує спостерігатися намагання звести проблематику забезпечення стійкості функціонування КІ до аспектів охоронної діяльності або до захисту населення. Спроба врегулювати ці питання шляхом уточнення завдань Державної комісії з питань техногенно-екологічної безпеки та надзвичайних ситуацій не знайшла свого впровадження на практиці. Загальне розуміння

[11] Наказ МВС від 01.09.2015 р. № 1053 «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» зареєстровано в Міністерстві юстиції України 22.09. 2015 р. за № 1124/27569. Він ще більше розширює перелік підприємств, які мають охоронятися підрозділами МВС.

захисту КІ органами влади та учасниками зазначеної комісії продовжує залишатися в рамках розуміння системи цивільного захисту, тобто захисту населення та території від наслідків надзвичайних ситуацій (природні катастрофи, технологічні аварії).

У сучасних умовах гарантування спроможності КІ виконувати свої функції та надавати послуги потребує зміщення фокусу з ліквідації наслідків на попередження криз. Із згаданих вище систем дві, а саме антитерористична система та система фізичного захисту, зорієнтовані на виконання цього завдання. До них слід віднести також і нову систему боротьби із кіберзагрозами, яка формується на виконання Стратегії кібербезпеки України.

На жаль, ці системи, маючи споріднені цілі, також побудовані різними відомствами та істотно не узгоджені, що формує суттєві ризики їх бездіяльності в окремих випадках.

Антитерористична система, відповідно до Закону України «Про боротьбу з тероризмом», спрямовує зусилля держави на запобігання «терористичних актів». При цьому під терористичними актами розуміють «злочинне діяння у формі застосування зброї, вчинення вибуху, підпалу чи інших дій, відповідальність за яке передбачена статтею 258 Кримінального кодексу України». У свою чергу, Кримінальний кодекс України уточнює, що «терористичний акт» слід пов'язувати з діями, які ведуть до порушення громадського порядку та нанесення шкоди здоров'ю людини, а «диверсію» – з діями, спрямованими на ослаблення держави (саме до цієї категорія може бути віднесено зловмисне пошкодження КІ)[12].

Проблема в тому, що антитерористична система не опікується «диверсіями». Диверсіями опікується система фізичного захисту. Саме вона має забезпечити реагування на «диверсії», однак лише щодо ядерних установок та матеріалів. Фактично, система фізичного захисту має за мету збереження ядерних (радіоактивних) матеріалів у безпечному стані у визначених місцях, відповідно до Закону України «Про фізичний захист ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання».

Через зазначені особливості законодавства, випадки пошкодження КІ (наприклад, підриву ліній електропередач, підстанцій чи трубопроводів) не є предметом розгляду окремо кожної із систем захисту і, відповідно, можуть і не привести до реагування в рамках існуючих процедур.

Окремо слід відзначити проблему розширення загроз КІ, зокрема втручання в систему управління КІ чи технологічний процес. На сьогодні реагування на зазначені загрози лише частково врегульоване законодавством.

Проблема захисту технологічної інформації та систем автоматичного дистанційного управління КІ постала в Україні у зв'язку з першою відомою в історії успішною кібератакою проти енергетичної КІ. У грудні 2015 р. група хакерів здійснила атаку проти трьох регіональних енергопостачальних компаній ОЕС України («Прикарпаттяобленерго», «Чернівціобленерго», «Київобленерго»), що призвело до відключення споживачів різних категорій[13]. Причинами несанкціонованого втручання в систему диспетчерського та технологічного управління електричними мережами стали відсутність загальних обов'язкових вимог до енергетичних компаній (переважно приватних) щодо безпеки систем автоматизації технологічного процесу, недостатня поінформованість та підготовка технічного персоналу в частині кібербезпеки, відсутність внутрішніх структур контролю з кібербезпеки тощо[14].

Також важливим є питання про «внутрішнього порушника», тобто імовірність здійснення зловмисних дій (чи сприяння їм) з боку працівників компаній – операторів КІ. В умовах гібридної війни, при наявності випадків викриття зрадників та шпигунів в лавах силових структур

[12] Див. Закон України «Про боротьбу з тероризмом» та статті 113 і 258 Кримінального кодексу України, які уточнюють визначення «диверсії» та «терористичного акту».

[13] Зловмисники з використанням отриманого завчасно віддаленого доступу до комп'ютерів автоматичної системи дистанційного управління (АСДУ), що перебували всередині корпоративних мереж обленерго, або безпосередньо до серверів АСДУ з використанням клієнтського програмного забезпечення АСДУ, виконали операції з управління вимикачами на розподільчих підстанціях. Перерва в електропостачанні становила від 1 до 3,5 години. Детальніше див. висновки робочої комісії Міненерговугілля.

[14] Раніше були здійснені атаки проти ряду телеканалів та, що особливо важливо, проти системи Центральної виборчої комісії з метою спотворити результати виборів Президента України у травні 2014 р. (з одночасною демонстрацією по телеканалах Росії підтасованих результатів про перемогу яскраво вираженого антиросійського кандидата), а пізніше була виявлена підготовка до здійснення кібератаки проти системи управління одного з аеропортів України.

України, не можна нехтувати імовірністю цілеспрямованого порушення функціонування КІ з боку працівників компаній-операторів. За деякими даними, саме чинник «внутрішнього порушника» міг призвести до успіху кібератаки на енергорозподільчі компанії.

У цьому контексті ми можемо говорити про загрози стійкості функціонування не тільки транспортної чи енергетичної інфраструктури, а й інфраструктури надання послуг інформаційно-культурного характеру[15]. Інфраструктура надання медичних, релігійних чи комунікаційно-інформаційних послуг є не менш важливою в умовах гібридної війни. Використання релігійних об'єктів, медичних закладів, мережі радіо- чи телетрансляції як інструменту гібридної війни широко практикувалося Росією під час агресії проти України, причому значну роль у цьому відігравали працівники цих об'єктів.

У цій ситуації слід уточнити роль та повноваження окремих розвідувальних та контррозвідувальних органів щодо забезпечення захисту КІ. Зокрема, в рамках реформування Служби безпеки України має бути враховано та актуалізовано аспект контррозвідувального захисту КІ, що мають стратегічне значення для функціонування системи життєдіяльності суспільства, національної економіки та держави, і не тільки стосовно забезпечення фізичної охорони окремих об'єктів.

Слід також наголосити на необхідності врахувати в цій діяльності нові підходи до розуміння впливу КІ на функціонування економіки, життєдіяльності суспільства та держави і стану економічної безпеки держави в умовах подальшої лібералізації економічних відносин та міжнародної інтеграції України. Саме функції та послуги, якими забезпечують суспільство та державу об'єкти та системи КІ, мають бути покладені в основу при визначенні предмета діяльності національної системи захисту. «Зелена книга з питань захисту критичної інфраструктури в Україні» наголошує, що формування системної оцінки загроз та ризиків функціонуванню систем КІ має базуватися на оцінці взаємозв'язку між елементами (об'єктами) КІ, оцінки масштабу та часового ефекту впливу реалізованої загрози та важкості можливих наслідків [7, 14].

При цьому всі потенційні об'єкти КІ, які потребують захисту, доцільно розбити на чотири групи:

І група – життєво необхідні об'єкти КІ. Великі об'єкти інфраструктури загальнодержавного значення, які мають розгалужені зв'язки та значний вплив на іншу інфраструктуру, заходи з відновлення яких вимагають значних ресурсів та часу (наприклад АЕС). На таких об'єктах має бути створено адекватну загрозам система фізичного захисту, а вимоги до захисту має встановлювати держава, а захист здійснюватись з використанням державних ресурсів та сил.

ІІ група – життєво важливі об'єкти КІ. На таких об'єктах потрібно як реалізувати заходи з фізичного захисту, так і передбачити можливість якнайшвидшого відновлення функцій за рахунок диверсифікації та резервів (великі нафтобази, електричні підстанції, мостові переходи, джерела питної води тощо). Відповідальність за захист цієї КІ мають нести оператори (власники) та держава на основі державно-приватного партнерства при жорсткому контролі з боку держави за дотриманням вимог та правил з безпеки.

ІІІ група – важливі об'єкти КІ. Пріоритетом захисту такої інфраструктури є забезпечення швидкого відновлення функцій за рахунок диверсифікації та резервів (наприклад, теплові електростанції, автомагістралі тощо). Відповідальність за захист цієї КІ мають нести передусім оператори (власники), а держава має забезпечити умови для диверсифікації та резервування виконання функцій.

ІV група – необхідні об'єкти КІ. Об'єкти інфраструктури, яка не відноситься до критичної, безпосередній захист якої є відповідальністю оператора (власника), який має мати план реагування на кризову ситуацію.

При цьому оператори (власники) КІ усіх форм власності мають розробити «Паспорт безпеки», який би визначав заходи із запобігання реалізації комплексних загроз (з виділенням їх цільової спрямованості: фізичних елементів об'єктів, системи управління та комунікації, персоналу)

[15] В Ізраїлі до об'єктів КІ належать об'єкти символічної (ідеологічна, історична або культурна) значущості для суспільства, об'єкти, від яких залежать основні процеси життєзабезпечення. При цьому об'єкти культурної спадщини Ізраїлю (музеї, архіви, культові споруди та інші пам'ятки) віднесені до числа об'єктів, які повинні бути захищені в першу чергу [13].

та реагування на випадок їх реалізації. У частині реагування «Паспорт безпеки» має передбачити заходи щодо фізичного захисту (попередження та припинення диверсій), технічного захисту (підвищення живучості систем, у тому числі захист від кіберзагроз), захисту персоналу (підготовка та перевірка персоналу), захисту систем управління та зв'язку[16], законодавчого забезпечення (повноваження та взаємодія), відновлення (плани відновлення втрачених функцій).

За цим підходом важливим є не тільки збільшення охоронних підрозділів чи посилення контролю за діяльністю економічною суб'єктів господарювання, а й забезпечення можливостей взаємозаміни обладнання (функцій) об'єктів КІ [17] Ефективність саме такого підходу підтверджується досвідом подолання проблем, породжених дефіцитом антрацитового вугілля у період воєнних дій у зоні АТО (частина електростанцій не могли використовувати інші види вугілля), а також заміни пошкодженого обладнання на прифронтових територіях.

Так, відновлення функціонування Слов'янської ТЕС гальмувалося через відсутність трансформатора, необхідного для заміни пошкодженого пристанційного трансформатора. Станція тривалий час не працювала, поки трансформатор не був демонтований на Вуглегірській ТЕС та з великими складнощами (необхідність вирішувати проблеми габаритних розмірів на шляху слідування) перевезений на Слов'янську ТЕС.

Таким чином, аналіз реагування України на гібридні загрози КІ свідчить про необхідність суттєвого перегляду державної політики у цій сфері. Незважаючи на важливі зміни на рівні стратегічного цілепокладання, практична діяльність органів державної влади, принципи взаємодії цивільного сектору та сектору безпеки і оборони, механізми залучення приватного сектору до діяльності із захисту КІ потребують уточнення.

З метою узгодження цілей та особливостей функціонування різних сфер життєдіяльності та координації дій різних органів влади у цій сфері доцільним є прийняття окремого Закону України «Про критичну інфраструктуру». В ньому мають бути сформульовані принципи державної політики щодо захисту критичної інфраструктури, відображені питання державно-приватного партнерства (розподіл відповідальності), визначені повноваження органів державної влади з побудови системи захисту критичної інфраструктури тощо.

Висновки

Досвід України щодо забезпечення захисту критичної інфраструктури свідчить, що суб'єктом зловмисних дій проти КІ може бути держава-агресор, а не лише окремі групи зловмисників (терористичні групи), як вважалося донедавна.

Гібридна війни Росії проти України супроводжувалася масовими випадками фізичного пошкодження та перешкоджання відновленню функціонування критичної інфраструктури, у тому числі з використанням методів диверсійної роботи, кримінальної поведінки, провокаційних інформаційних меседжів та використання інших методів впливу.

Недавні події на сході України свідчать, що порушення функціонування критичної інфраструктури життєдіяльності суспільства та держави стає інструментом агресора, який використовується для завдання економічних втрат, створення загрози обороноздатності країни, здійснення психологічного впливу на населення і політичного тиску на політиків та уряд країни, яка зазнала агресії.

У цій ситуації система захисту критичної інфраструктури має будуватися виходячи з необхідності реагування на комплекс загроз та їх узгоджену реалізацію і спрямовуватися на забезпечення стійкості функціонування системи життєдіяльності суспільства, національної економіки та держави. Це завдання не може бути забезпечене лише заходами посилення фізичної охорони окремих об'єктів.

Функції та послуги, якими об'єкти та системи критичної інфраструктури забезпечують суспільство та державу, мають лежати в ос-

---

[16] Нині до Сенату США внесено законопроект про повернення до «ручного» керування обладнанням високовольтних трансформаторних підстанцій, з метою уникнення ризиків кібератак та віддаленого їх відключення через мережу Інтернет [15].

[17] У США низка енергетичних компаній планує запустити з 2018 р. спільний страховий фонд критичного електроенергетичного обладнання на випадок терористичних актів, техногенних чи природних аварій. Тим часом у Конгресі США дискутується можливість створення Національного стратегічного резерву трансформаторів [16].

нові визначення предмета діяльності національної системи захисту. Такий підхід вимагає прийняття відповідного законодавства, яке б відобразило нові принципи державної політики щодо захисту критичної інфраструктури, врегулювало питання державно-приватного партнерства (розподіл відповідальності між державою та приватним сектором), забезпечило координацію дій відомчих систем захисту та реагування на окремі типи загроз у єдиній, скоординованій системі захисту критичної інфраструктури.

Список використаної літератури

1. *Указ президента* Российской Федерации от 31.12.2015 г. № 68 «О Стратегии национальной безопасности Российской Федерации» : [Електронний ресурс]. – Режим доступу : http://www.consultant.ru/document/cons_doc_LAW_191669/
2. *Frank G. Hoffman*. Hybrid vs compound war [Електронний ресурс] // Armed Forces Journal. – 2009. – October 1. – Режим доступу : http://www.armedforcesjournal.com/hybrid-vs-compound-war/
3. *Горбулін В.П.* «Гібридна війна» як ключовий інструмент російської геостратегії реваншу / В.П. Горбулін // Стратегічні пріоритети. – 2014. – № 4. – С. 5–12.
4. *Горбулін В.П.* The «Hybrid warfare» ontology / В.П. Горбулін // Стратегічні пріоритети. Серія «Філософія». – 2016. – № 1.– С. 4–13.
5. *Гончар М.* Гібридна війна Кремля проти України і ЄС: енергетичний компонент / Гончар М., Чубик А., Іщук О. // Дзеркало тижня. Україна. – 2014. – 23 жовтня. – № 39.
6. *Гибрессия* Путина. Невоенные аспекты войн нового поколения [Електронний ресурс] / за ред. М. Гончара ; ЦГ «Стратегія XXI» – 2016. – 62 с. – Режим доступу : http://geostrategy.org.ua/images/Hybression_finversion.pdf
7. *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. – К. : НІСД, 2016. – 176 с.
8. *Суходоля О.М.* Проблеми захисту енергетичної інфраструктури в умовах гібридної війни [Електронний ресурс] / О.М. Суходоля. – Режим доступу : http://www.niss.gov.ua/articles/1891/
9. *Суходоля О.М.* Енергетична інфраструктура: інструментальний вимір ведення війн нового покоління / О.М. Суходоля // Невоєнний вимір війн нового покоління. Енергетичний компонент : матер. міжнар. конф. – К. : НІСД, ЦГ «Стратегія XXI», 2016. – С. 42–52.
10. *Германия* назвала подрыв украинских ЛЭП преступным актом [Електронний ресурс]. – Режим доступу : http://www.dw.com/ru/a-18868997?maca=rus-tco-dw
11. *Прес-реліз* за результатами засідання РНБО. 20.07.2015 р. [Електронний ресурс]. – Режим доступу : http://www.rnbo.gov.ua/news/2203.html
12. *Постанова* Кабінету Міністрів України від 11.11.2015 р. № 937 «Питання забезпечення охорони об'єктів державної та інших форм власності» [Електронний ресурс]. –– Режим доступу : http://zakon5.rada.gov.ua/laws/show/937-2015-%D0%BF
13. *Бірюков Д.С.* Про доцільність та особливості визначення критичної інфраструктури в Україні : аналітична записка [Електронний ресурс] / Д.С. Бірюков. – Режим доступу : http://www.niss.gov.ua/articles/1026/
14. *Бобро Д.Г.* Удосконалення методології ранжування об'єктів критичної інфраструктури та їх віднесення до критичної інфраструктури : аналітична записка [Електронний ресурс] / Д.Г. Бобро. – Режим доступу : http://www.niss.gov.ua/content/articles/files/krutuchna_infra-a7636.pdf
15. *Securing* Energy Infrastructure Act would adopt "retro" approach to safeguard against 21st century threat [Електронний ресурс]. – Режим доступу : http://www.king.senate.gov/newsroom/press-releases/king-risch-heinrich-collins-introduce-legislation-to-protect-electric-grid-from-cyber-attacks
16. *Utilities* Seek to Stockpile Essential Parts for Disasters [Електронний ресурс].– Режим доступу : http://www.wsj.com/articles/utilities-seek-to-stockpile-essential-parts-for-disasters-1460076194#livefyre-comment

References

1. *Ukaz Presidenta* Rossiskoi Federatsii ot 31.12.2015 №68 «O Strategii natsionalnoi bezopasnosti Rossiskoi Federatsii» [The Order of President of Russia Federation of 31.12.2015 №68 "On the National Security Strategy of Russian Federation"]. – Retrieved from http://www.consultant.ru/document/cons_doc_LAW_191669/ [in Russian].
2. *Hoffman, Frank G.* (2009). Hybrid vs compound war. *Armed Forces Journal*, October 1.– Retrieved from http://www.armedforcesjournal.com/hybrid-vs-compound-war/ [in English].
3. *Horbulin, V.* (2014). «Hibrydna viyna» yak kluchovyi instrument rosiskoi geostarategii revanshu ["Hybrid war" as a key instrument of Russian geostrategy revenge]. *Stratehichni priorytety – Strategic Priorities*, 4, 5–12 [in Ukrainian].

4. *Horbulin, V.* (2016). The «Hybrid warfare» ontology. *Stratehichni priorytety. Seria "Phylosophia" – Strategic Priorities. Vol. "Philosophy",* 1, 4–13[in Ukrainian].
5. *Honchar, M.,* Chubyck, A., Ishchuk, O. (23 October, 2014). Hibrydna viyna Kremlia proty Ukrainy ta EU: energetychyi component [Kremlin's Hybrid war against Ukraine and EU: energy component]. *Dzerkalo tyzhnia – The Mirror Weekly*,39,, [in Ukrainian].
6. *Honchar, M.* (Ed.). (2016). Gibressia Putina: nevoenni aspecty viyn novogo pokolinnia [Putin's Gibression: Non-military aspects of the new generation of warfare]. SGC "Strategy XXI". Retrieved from http://geostrategy.org.ua/images/Hybression_finversion.pdf [in Russian].
7. *Sukhodolia, O.,* Biriukov, D., Kondratov, S. (Eds.). (2015). Zelena knyga z pytan zahystu crytychnoi infrastructury [The Green Book on Critical Infrastructure Protection]. Kyiv: NISS. [in Ukrainian].
8. *Sukhodolia, O.* (n.d.) Problemy zahustu energetychnoi infrastructury v umovah hibrydnoi viyny [Problems of energy infrastructure in a hybrid war condition]. Retrieved from http://www.niss.gov.ua/articles/1891/ [in Ukrainian].
9. *Sukhodolia, O.* (2016). Energetycha infrastructura: instrumentalniy vymir vedennia viyn novogo pokolinnia [Energy infrastructure: instrumental dimension of driving a new generation of warfare]. In *Nevoennyi vymir viyn novogo pokolinnia: energetychyi component – Non-military Dimension wars of new generation. The energy component.* – Kyiv: NISS, SGS "Strategy XXI" [in Ukrainian].
10. G*ermania* nazvala podryv ukrainckikh LEP prestupnym aktom [Germany called undermining Ukrainian LEP criminal act] (n.d.). Retrieved from http://www.dw.com/ru/ a-18868997?maca=rus-tco-dw [in Russian].
11. Press-reliz za resultatamy zasidannia RNBO. (2015). [Press release after the meeting of the NSDC]. Retrieved from http://www.rnbo.gov.ua/news/2203.html [in Ukrainian].
12. *Postanova* Cabinety Ministriv Ukrainy vid 11.11.2015 № 937 "Pytannia zabezpechennia ohorony obektiv derzhavnoi na inshykh form vlasnosti [The Resolution of the Cabinet Ministers of Ukraine of 11.11.2015 № 937 "The issue of protection of state and other forms of property objects"]. Retrieved from http://zakon5.rada.gov.ua/laws/show/937-2015-%D0%BF [in Ukrainian].
13. *Biriukov, D.* (n.d.) Pro dotsilnist ta osoblyvosti vyznatchennia krytychnoi infrastruktury [On the feasibility and features of the critical infrastructure in Ukraine]. Retrieved from http://www.niss.gov.ua/articles/1026/ [in Ukrainian].
14. *Bobro, D.* (n.d.) Udoskonalennia metodologii ranzhyvannia obektiv krytychnoi infrastruktury ta vidnesennia ikh do krytychnoi infrastruktury [Improving of ranking methodology of critical infrastructure objects and their assignment to critical infrastructure]. Retrieved from http://www.niss.gov.ua/content/articles/files/krutuchna_infra-a7636.pdf [in Ukrainian].
15. *Securing* Energy Infrastructure Act would adopt "retro" approach to safeguard against 21st century threat (n.d.) Retrieved from: http://www.king.senate.gov/newsroom/press-releases/king-risch-heinrich-collins-introduce-legislation-to-protect-electric-grid-from-cyber-attacks [in English].
16. *Utilities* Seek to Stockpile Essential Parts for Disasters (n.d.) Retrieved from: http://www.wsj.com/articles/utilities-seek-to-stockpile-essential-parts-for-disasters-1460076194#livefyre-comment [in English].