ПУБЛІЧНА ПОЛІТИКА ТА МЕХАНІЗМИ ДЕРЖАВНОГО УПРАВЛІННЯ У СФЕРІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

УДК 351/354+355

Суходоля О.М.
доктор наук з державного управління, професор,
завідувач відділу енергетичної та техногенної безпеки
Національного інституту стратегічних досліджень

ЗАХИСТ КРИТИЧНОЇ ІНФРАСТРУКТУРИ: СУЧАСНІ ВИКЛИКИ ТА ПРІОРИТЕТНІ ЗАВДАННЯ СЕКТОРУ БЕЗПЕКИ

Стаття присвячена дослідженню пріоритетних напрямів удосконалення діяльності сектору безпеки в системі забезпечення національної безпеки. Обґрунтовується необхідність, в умовах виникнення сучасних викликів та загроз гібридного типу, визначення предмету діяльності сектору безпеки крізь призму забезпечення національної стійкості. Наводиться теоретично-методологічне обґрунтування визначення засад та принципів діяльності сектору безпеки у сфері захисту критичної інфраструктури. Визначаються пріоритетні напрями удосконалення практичного інструментарію та механізмів взаємодії сектору безпеки із іншими складовими системи забезпечення національної безпеки. Визначаються першочергові завдання з формування державної системи захисту критичної інфраструктури, і зокрема основні завдання органів сектору безпеки.

Ключові слова: *завдання сектора безпеки, розвідка та контррозвідка, гібридні загрози*

CRITICAL INFRASTRUCTURE PROTECTION: MODERN CHALLENGES AND PRIORITY TASKS OF SECURITY SECTOR

The article is devoted to analysis and tuning of a security sector tasks (intelligence and counterintelligence) within the system of national security. Defining of security sector tasks is described through prism of national resilience approach in conditions of modern challenges and hybrid threats to national security. In the article is given a methodological approach for shaping of principles and prioritizing of tasks of security sector performance in a field of critical infrastructure protection. The improvement of working instruments as well as mechanisms of interaction between security sector and other agencies of the national security system are determined. The article suggests key steps for establishing the national critical infrastructure protection system in general and main tasks of security sector agencies in particular.

Key words: *security sector tasks, intelligence and counterintelligence, hybrid threats*

Постановка проблеми та її зв'язок із важливими науковими чи практичними завданнями. Реформування системи забезпечення національної безпеки сьогодні стало одним із найактуальніших питань для української держави. Це пов'язано не тільки із розв'язанням гібридної війни проти України, але й динамікою соціальних, економічних, політичних і навіть технологічних процесів, що відбуваються у світі.

Серед основних безпекових викликів сьогодення є розмивання раніше чітко визначених меж між станом війни та миру, меж повноважень національних та міжнародних систем безпеки, прогресуючим ускладненням регулювання міжнародних економічних, політичних та безпекових відносин, а також зростанням екстремізму, нівелюванням морально-етичних обмежень на застосування насилля як з боку окремих країн, так і громадян, появою нових загроз внаслідок поширення сучасних технологічних новацій, що

змушують кардинально переглянути систему національної безпеки.

Зазначені виклики формують перед сектором безпеки і оборони кожної країни надскладні завдання одночасного посилення захисту національних інтересів та безпеки держави, поряд із забезпеченням свободи громадян та вільне проявлення та реалізацію своїх прав, а також збереженням переваг лібералізованої глобальної економіки, зокрема вільним рухом товарів, капіталів, технологій та людей.

Ще більш складна ситуація постала в Україні. Система забезпечення національної безпеки України, яка до останнього часу базувалась, в значній мірі, на радянських моделях функціонування, фактично, виявилась неспроможною адекватно відреагувати на виклики та загрози сьогодення. Саме неготовність сектору безпеки і оборони до протидії сучасним загрозам, реалізованим в концепції "гібридних війн" поставило Україну у ситуацію екзистенційної кризи та безальтернативності модернізації своєї моделі життєдіяльності та системи безпеки [1]

Формулювання мети статті. Ситуація, що склалась вимагає суттєвого удосконалення діяльності сектору безпеки і оборони, як з точки зору перегляду теоретично-методичних засад та принципів діяльності сектору безпеки та оборони, так і з точки зору удосконалення його практичного інструментарію та механізмів взаємодії із іншими складовими системи забезпечення національної безпеки.

Саме на дослідження зазначеного завдання і спрямовується дана робота. Зокрема, ***метою*** публікації є виділення та обґрунтування пріоритетних напрямів уточнення змісту, механізмів та інструментів дій сектору безпеки держави, виходячи із розвитку сучасних концепцій забезпечення захисту національної безпеки.

Виклад основного матеріалу дослідження. *Теоретичне обґрунтування.* Проблематика удосконалення сектору безпеки і оборони детально досліджувалась у роботах багатьох науковців як вітчизняних, так і зарубіжних. Останнім часом, зазначені дослідження концентрувались на дослідженні проблематики удосконалення діяльності сектору

безпеки, виходячи із розуміння надійності функціонування міжнародної системи безпеки та пріоритету прав людини. Водночас, відверте намагання Росією відновити "право сили" на міжнародній арені та застосування гібридної методів ведення війни, фактично поставило дослідників перед необхідністю переглянути свої підходи, включивши в аналіз проблематику війн нового покоління [1-6].

Питання удосконалення діяльності сектору безпеки України також стало актуальним як у теоретичній, так і практичній площині. На сьогодні постало питання застосування принципово нових методів та інструментів діяльності сектору безпеки, що і зумовлює питання прийняття Концепції його реформування [5-7]. При цьому, суттєвий вплив на процес трансформації завдань для сектору безпеки і оборони здійснюють кращі світові сучасні підходи щодо забезпечення національної стійкості, зокрема захист критичної інфраструктури [4,6-8]. Саме тому, на сьогодні, у процесі є реформування сектору безпеки необхідно проаналізувати пріоритетні напрями уточнення функцій та повноважень державних органів сектору безпеки виходячи із сучасних концепцій забезпечення національної стійкості.

Концепція захисту критичної інфраструктури в системі забезпечення національної стійкості.

Слід відзначити, що "вимушеність" реформування сектору безпеки в Україні внаслідок неготовності до гібридної війни не є унікальним недоліком країни. Зміни в пріоритетах системи забезпечення національної безпеки внаслідок подій, які демонструють неадекватність діючої на визначений час системи, траплялись в інших країнах також. Зокрема відзначимо події 2001 та 2005 років, які суттєво вплинули на становлення концепції захисту критичної інфраструктури у світі.

Саме у відповідь на трагічні події 11 вересня 2001 року в Нью-Йорку у США, на доповнення до *Стратегії національної безпеки США* [9] була розроблена та затверджена *Національна стратегії внутрішньої безпеки* (липень 2002 р.) [10] завданням якої була мобілізація та організація американського суспільства для цілей захисту від

терористичних атак. На відміну від Стратегії національної безпеки, яка приділила увагу захисту та забезпеченні реалізації національних інтересів США у зовнішньому вимірі на глобальному рівні, Стратегія внутрішньої безпеки орієнтувалась на забезпеченні внутрішньої безпеки та спроможності країни забезпечити стійке функціонування національної економіки, держави та суспільства. Тим не менш обидві стратегії основний акцент робили на забезпечення захисту об'єктів критичної інфраструктури від терористичних атак.

Необхідність усунення прогалин та удосконалення запровадженої системи захисту, знову ж було продемонстрована практикою. Стратегія внутрішньої безпеки США (2007 р.) [11], внаслідок аналізу наслідків урагану "Катріна" (серпень 2005), була доповнена природно-техногенним виміром. Аналіз дій системи захисту та реагування на випадок кризової ситуації[1] призвела до включення в систему національної безпеки розуміння важливості забезпечення стійкості функціонування критичної інфраструктури країни, як "організаційного-функціонального скелету" життєдіяльності суспільства. У Стратегії внутрішньої безпеки даний урок було відображено шляхом істотного посилення ролі забезпечення захисту критичної інфраструктури, у сенсі захисту та запобігання реалізації "усіх типів загроз" та спроможністю до швидкого її відновлення.

У практичній площині, діяльність із забезпечення захисту критичної інфраструктури було формалізовано у

[1] До урагану "Катріна", діяльність щодо забезпечення захисту критичної інфраструктури переважно фокусувалась на організації фізичного "захисту" об'єктів інфраструктури. Ураган продемонстрував необхідність забезпечити "стійкість" функціонування інфраструктури, що вимагає забезпечення не тільки захисту від терористичних атак, але й заходів щодо запобігання, пом'якшення можливих загроз та, на випадок реалізації, заходів швидкого відновлення втрачених функцій (послуг). Для прикладу, колапс нафтопереробної інфраструктури та системи паливо забезпечення півдня США, внаслідок урагану "Катріна", був зумовлений не стільки внаслідок теракту проти об'єктів зазначеної інфраструктури чи її руйнації ураганом, а внаслідок "каскадного ефекту" через руйнування системи постачання електроенергії для функціонування зазначеної інфраструктури.

Національному плані захисту критичної інфраструктури, [12] метою якого було визначено "забезпечення безпеки та стійкості країни (США) через посилення захищеності національної критичної інфраструктури (КІ) шляхом: *запобігання, стримування, нейтралізації або пом'якшення наслідків цілеспрямованих дій з боку терористів* спрямованих на знищення, виведення з ладу або експлуатації КІ; а також *посилення національної готовності, своєчасне реагування та швидке відновлення КІ в разі атаки, стихійного лиха або інших надзвичайних ситуацій*". Слід зазначити, що у подальшому Національний план реалізації і заходи з його реалізації періодично оновлюється в залежності до оцінки поточних викликів та загроз КІ [13].

Усвідомлення зростання терористичних загроз (атака на транспортній інфраструктурі Іспанії в 2004 році) зумовили активізацію дій і в ЄС. Європейська Комісія розробила та у листопаді 2005 р. оприлюднила Зелену книгу щодо Європейської програми захисту критичної інфраструктури, а згодом (2006 р.) була прийнята *Європейська програма захисту критичної інфраструктури* [14]. Особливості підходу ЄС, як об'єднання суверенних держав, у подальшому знайшли своє відображення у Директиві 2008/114/ЕС щодо визначення об'єктів критичної інфраструктури та оцінки потреб у підвищенні рівня їхнього захисту (2008 р.) [15].

Стратегія національної безпеки України (2015 року), поряд із завданнями реформування сектору безпеки, також визначає захист критичної інфраструктури (ЗКІ) у якості пріоритетного напряму безпекової політики. У свою чергу, оновленні доктринальні і концептуальні документи сектору безпеки і оборони України (Воєнна доктрина України, Концепція розвитку сектору безпеки і оборони України, Стратегія кібербезпеки України) формують завдання щодо реалізації цього напряму державної політики.

У розвиток Стратегії національної безпеки, Національним інститутом стратегічних досліджень розроблено Зелену Книгу з питань захисту критичної інфраструктури [8], яка розкриває теоретично-методологічні

засади формування державної системи ЗКІ та окреслює пріоритети системи державної влади у цій сфері[2].

Концепція захисту критичної інфраструктури держави дає можливість сформувати необхідну базу для функціонування спеціального правоохоронного органу держави відповідно до сучасних теоретичних засад та кращої світової практики. Та перш ніж перейти до детальнішого аналізу пріоритетів удосконалення нормативно-правової бази діяльності сектору безпеки з питань забезпечення ЗКІ слід поглянути на роль КІ для забезпечення національної безпеки, а також місце та роль сектору безпеки у забезпеченні стійкості функціонування суспільства та держави з системних позицій.

Системний підхід до визначення предмету діяльності сектору безпеки у сфері захисту критичної інфраструктури.

Подальший аналіз буде здійснюватись з наступних методологічних позицій:

---

[2] Для кращого розуміння публікації наведемо ряд визначень, що визначають зміт діяльності у сфері захисту критичної інфраструктури:

Критична інфраструктура (КІ) - 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;

Критичність – це відносна міра важливості даної інфраструктури, що враховує вплив раптового припинення її функціонування, або функціонального збою на безпеку постачання, тобто забезпечення суспільства важливими товарами і послугами.

Захист КІ – всі види діяльності, спрямовані на забезпечення функціональності, безперервності та цілісності критичної інфраструктури з метою недопущення, пом'якшення та нейтралізації загроз, ризиків та вразливостей.

Загрози КІ – чинники які потенційно можуть призвести до припинення КІ виконання функцій та надання послуг.

Безпека критичної інфраструктури - стан критичної інфраструктури, коли дія зовнішніх та внутрішніх чинників не призводить до аварій чи інших порушень її функціонування;

Стійкість інфраструктури – 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.

–категорія “безпека” нерозривна із категорією “суб’єкт”, оскільки саме явище безпеки є рефлексією суб’єкта;

–суб’єкт існує на матеріалі “об’єкта”, і лише існування матеріалу у визначеній формі та якості гарантує існування суб’єкта та визначає його “безпеку”;

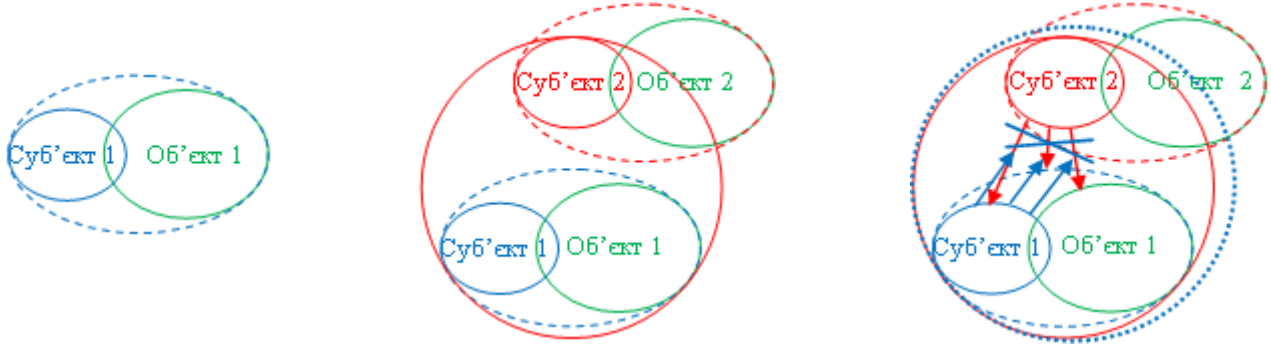
–суб’єкт завжди “охоплює” об’єкт, тобто усвідомлює можливості та має інструменти підпорядкування об’єкта і, тим самим, управляє ним (забезпечує його “розвиток” і “безпеку”). Якщо суб’єкт на має впливу на ту чи іншу частину об’єкта, він не є суб’єктом для цієї частини;

–глобалізація обумовлює конкуренцію “суб’єкт–об’єктних” системних утворень та проблеми їх взаємовідносин. При конкуренції виграє той із суб’єктів, хто перетворив конкурента на свій об’єкт оперування, здійснюючи тим самим вплив на процеси, які відбуваються в його “суб’єкт–об’єктній” системі;

–суб’єкт визначає безпечність існування через оцінку свого місця та ролі в навколишньому середовищі, також конкурентних переваг над іншими суб’єкт-об’єктними системами.

Для цілей даного дослідження, сектор безпеки приймаємо за “суб’єкт” управління, а система життєдіяльності країни виступатиме “об’єктом”. Зміст діяльності суб’єкта визначатиметься забезпеченням конкурентної переваги власної “суб’єкт-об’єктної” системи перед іншими через вплив на існуючі процеси (у зовнішній і внутрішній сфері) які протікають у своїй та конкурентній системі.

Графічне пояснення цього показано на рис.1.



а) б) в)

Рис. 1. Конкурентна боротьба "суб'єкт-об'єктних" систем

Пояснення до рисунку:

а) Суб'єкт 1 управляє своїм об'єктом 1 через здійснення впливу на процеси, що відбуваються у "суб'єкт-об'єктній системі 1";

б) Суб'єкт 2 управляє своєю системою "С2-О2", а також системою "С1-О1" використовуючи наявні в нього методи та інструменти аналізу процесів та впливу на їх протікання в системі "С1-О1".

в) Суб'єкт 1 усвідомив існування впливу С2 та застосовує свої методи та інструменти для збереження стійкості своєї системи "С1-О1".

Враховуючи основні положення концепції захисту критичної інфраструктури, предметом діяльності сектору безпеки має стати - визначення, аналіз та оцінка ефективності застосування методів та інструментів впливу однієї системи на іншу (однієї країни на іншу), а також розробка методів та інструментів *запобігання, стримування, нейтралізації або пом'якшення наслідків такого впливу та сприяння посиленню готовності, своєчасного реагування та швидкого відновлення штатного режиму функціонування системи*.

Для подальшого уточнення предмету діяльності сектору безпеки слід додатково відзначити ряд важливих позицій:

–у сучасному глобалізованому світі методи та інструменти впливу постійно змінюються (поява методів "гібридної війни"), що потребує відповідно реагування з боку системи безпеки, а саме постійної своєрідної "інвентаризації" зазначених методів та інструментів, перевизначення їх предмету та механізму дії;

–предмет діяльності та механізми впливу суб'єкта визначаються ідентифікацією основних процесів життєдіяльності окремої "суб'єкт-об'єктної" системи (на визначеному проміжку її життєдіяльності), на які спрямовані зазначені впливи;

–структурно-функціональне відображення основних процесів, в рамках методології системного підходу, є критичної інфраструктурою (КІ) життєдіяльності "суб'єкт-об'єктної" системи;

–загрози стійкості функціонування КІ системи є фактично загрозами національної безпеки.

Введенні "процеси", які є визначальними для подальшого аналізу, потребують додаткового розкриття. На нашу думку, розкриття об'єкта як системи, з виділенням, поряд із традиційними складниками (елементи, зв'язки, структура), також її матеріального та процесуального складників дає змогу зняти ряд недоліків існуючого підходу[1].

[1] Необхідність розширення змісту категорії "система" за рахунок включення "процесуальності" існування системи, де поряд із такими складниками категорії "система", як "елемент", "структура", "функція", враховується "матеріал" і "процеси" системи, обґрунтовано у роботах

Хоча у знаковій формі показати процеси життєдіяльності системи досить важко, їх "схоплення" суб'єктом дослідження (управління) є дуже важливим, оскільки саме процеси функціонування системи визначають предмет управлінської діяльності. Саме виділення процесів, дозволяє подолати неадекватний сьогоденню підхід щодо акценту на статичному стані системи через виділення набору окремих індикаторів та їх цільових значень (переліків об'єктів захисту, фізичної охорони, наявності ресурсів визначеного обсягу тощо) та внести в управлінську діяльність необхідність врахування динаміки системи. У свою чергу, врахування динаміки дозволяє виходити на проектування "майбутнього" системи, задачу формування конкурентних переваг у конкурентній боротьбі "суб'єкт-об'єктних систем".

Виділення процесів, дозволяє акцентувати увагу на адаптації системи, тобто спроможності перебудувати структуру зв'язків та змінити властивості елементів системи відповідно до нових вимог середовища. Саме до такого ж висновку прийшло розвідувальне співтовариство США, яке у доповіді Національної Розвідувальної Ради (National Intelligence Council) наголошує: "*В умовах несформованого глобального ландшафту, багатого сюрпризами і різкими змінами, найбільш пристосованими до використання таких можливостей будуть стійкі держави і організації, що дозволить їм адаптуватися до умов, що змінюються, витримувати вплив несподіваних несприятливих факторів і вживати заходів для швидкого відновлення. Вони будуть вкладати кошти в інфраструктуру, знання і відносини, які дозволять їм витримувати потрясіння - економічні, екологічні, соціальні або кібернетичні"* [17].

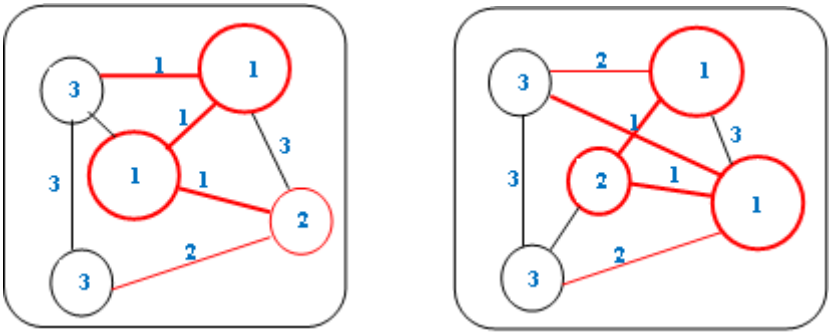
Необхідність розроблення теоретико-методологічної бази для формалізації діяльності спрямованої на забезпечення "стійкості" життєдіяльності держави повертає до необхідності

Г.П.Щедровицького [16] На нашу думку, внесення у розгляд *"матеріального" складника* є фактично інструментом виходу дослідника з теоретичної конструкції у реальність існування об'єкта (окремих сфер об'єкта)*, а "процесуальності"* є виходом на розуміння закономірностей його еволюції і відтак на можливість цілепокладання його розвитку (захисту).

виділення організаційно-функціональної структури відображення основних процесів системи, тобто до виділення КІ системи, яка "схоплює" відповідні процеси.

Загалом процес відображається у зміні "матеріалу" системи, властивостях тих чи інших елементів системи (наприклад, повноваженнях окремого органу державної влади, впливовості форм власності, ідеології), потужності потоку ресурсів через ті чи інші взаємозв'язки між елементами системи.

Ідентифікацію процесу через графічне відображення змін в структурі системи, показано на рис. 2.



а) б)

Рис.2. Ідентифікація процесів в рамках системного представлення об'єкта

Пояснення до рисунку:

а) вихідна організаційно-функціональна структура життєдіяльності системи;

б) організаційно-функціональна структура життєдіяльності системи в результаті відображення процесу, що зумовив зміну характеристик (вагомість впливу) окремих елементів та зв'язків системи.

Вагомість елементів та зв'язків: 1 – важливі; 2 – вагомі; 3 – незначні.

Відповідно до цього, процес розуміється нами як перерозподіл визначеного ресурсу у системі, що

відображається у зміні її організаційно-функціональної структури зв'язків та (або) властивостей елементів відповідно до реальної динаміки життєдіяльності системи. При цьому, важливим є не тільки відображення зміни окремих характеристик системи (відображених через набір індикаторів) у часі, що найчастіше розуміється фахівцями як "динаміка системи", але й зміни організаційно-функціональної структури всередині системи, що відображає реальність життєдіяльності системи та ефективність її функціонування.

Прикладом такого виділення процесу є виділення процесу "рентної експлуатації" енергетики України [18], через зміни організаційно-функціональної структури взаємовідносин у системі енергозабезпечення країни. Виділивши основний процес, який визначає життєдіяльності "суб'єкт–об'єктної" системи, можна адекватно оцінити поточний і спрогнозувати майбутній його стан і, відповідно, запропонувати управлінські рішення стратегічного характеру[2].

Таким чином, визначаючи процеси, що впливають на національну "стійкість", формалізуючи їх через КІ системи можна отримати предмет діяльності всієї системи забезпечення національної безпеки і, зокрема, сектору безпеки.

Базуючись на аналізі останніх досліджень, згадана нами доповідь Національної Розвідувальної Ради виділяє наступні сфери, що визначають національну стійкість [17]:

–*Урядування*. Здатність уряду забезпечити надання необхідних товарів та послуг, відкритість системи прийняття рішень, дотримання законності, що забезпечить довіру свого населення і надасть змогу краще поглинати зовнішні впливи та готувати відповідь;

[2] Так, для припинення існування процесу "рентної експлуатації" енергетики, та, відповідно, пріоритетом забезпечення енергетичної безпеки має стати завершення приватизаційних процесів та ліквідація можливостей непрямого "виведення" ресурсів з енергетики через "державне регулювання" фінансово-економічних взаємовідносин в енергетичному секторі, яке є основними методами "рентної експлуатації" української енергетики. На жаль, рішення щодо припинення процесу "рентної експлуатації" енергетики не приймались до 2015 року.

–*Економіка*. Країни із диверсифікованою економікою, керованим рівнем державного боргу та адекватними фінансовими резервами, сталим приватним сектором, мобільною та адаптивною робочою силою будуть більш стійкими до впливів;

–*Соціальна система*. Освічене, об'єднане та законослухняне суспільство буде більш згуртоване і стійке в умовах різких змін, матиме більш високу терпимість та готовність справитись із тимчасовими неприємностями.

–*Інфраструктура*. Надійність критичної інфраструктури держави, в тому числі диверсифікованість джерел енергозабезпечення, безпечні та дубльовані системи комунікації, інформування, охорони здоров'я, фінансових мережі, зменшить уразливість держави до стихійних лих та спробам зловмисного порушення надання зазначених послуг;

–*Безпека*. Держави, що володіють високим військовим потенціалом, дієздатними і надійними правоохоронними та аварійно-рятувальними службами, хорошим рівнем цивільно-військових відносин, а також входять до надійних міжнародних союзів, будуть в змозі більш ефективніше захиститись від несподіваних атак і відновити внутрішній порядок внаслідок руйнівного впливу.

–*Ресурси та довкілля*. Держави, які мають великі корисні запаси земель, високий рівень біорізноманіття, а також гарну якість повітря, їжі, ґрунту і води будуть більш стійким в разі криз.

Завдання забезпечення національної стійкості стала пріоритетом також і для інших країн та міждержавних об'єднань. Зокрема, нова Глобальна стратегія ЄС із зовнішньої політики та політики безпеки питанням забезпечення стійкості (як енергетичної чи екологічної, так і стійкості держави) приділяє окрему увагу. [19] Завдання щодо забезпечення національної стійкості для країн-членів НАТО , були також визначені Главами держав і урядів країн на Варшавському саміті НАТО у липні 2016 року. [20] Зокрема визначено сім базових вимог (the seven baseline requirements) забезпечення національної стійкості: - безперервність урядування та надання найважливіших державних послуг; -

стійкість енергозабезпечення; - здатність ефективно справлятись з неконтрольованим переміщенням людей; - стійкість водозабезпечення та постачання продовольства; - здатність надавати допомогу великій кількості людей, що отримали пошкодження; - стійкість систем комунікацій; - стійкість транспортної системи.

Практично подібний перелік характеристик системи, що сприятимуть національній стійкості, слід застосовувати і для України. Зокрема пропонується визначити пріоритетом національної безпеки наступні характеристики системи забезпечення життєдіяльності суспільства:

– належні умови життєдіяльності членів суспільства (забезпечення потреб населення);

– гарантованість забезпечення належного рівня послуг: енергозабезпечення, транспортування, водопостачання, продовольчого забезпечення;

– розвиненість та ефективність фінансово-економічної інституційної основи національної економіки та життєдіяльності суспільства;

– мінімальний негативний вплив на довкілля (екологічно сприятливе господарювання);

– надання медичної допомоги членам суспільства та реагування на випадок виникнення кризових ситуацій;

– розвиненість інформаційно-комунікаційної системи суспільства;

– керованість розвитку суспільства та дотримання членами суспільства визначених правил життєдіяльності;

– спроможність нейтралізувати зовнішні негативні впливи (силового, економічного, інформаційного тощо);

Організаційно-функціональна структура, яка "схоплюватиме" процеси, що формують зазначені властивості системи, виділяється в Зеленій книзі з питань захисту критичної інфраструктури України у вигляді 10 секторів КІ[3].

[3] Слід зазначити, що кількість виділених секторів КІ залежить від спроможності суб'єкта управління забезпечити моніторинг, оцінку, запобігання та реагування на випадок реалізації загроз для вибраної кількості критичних елементів. Фактично мова іде про ресурсну та

Саме за стійкістю функціонування цієї інфраструктури пропонується оцінювати безпеку життєдіяльності такої системи як українська держава (Таблиця 1) [8].

Таблиця 1

Переліку секторів критичної інфраструктури та відповідальних відомств

Сектор критичної інфраструктури	**Відповідальні за забезпечення безпеки** (відповідно до повноважень)
1. Паливно-енергетичний комплекс	Міненерговугілля, СБУ, МВС
2. Транспорт	Мінінфраструктури, СБУ, МВС
3. Мережі життєзабезпечення	Мінрегіон, ДСНС
4. Телекомунікації та зв'язок	СБУ, Держспецзв'язок, МВС,
5. Фінансово-банківський сектор	НБУ, Мінфін, СБУ, Держспецзв'язок
6. Органи влади та правопорядку	СБУ, МВС, ДСО
7. Сектор безпеки і оборони	МО, МВС, СБУ
8. Хімічна промисловість	Держпраці, ДСНС, СБУ
9. Служби екстреної допомоги та цивільного захисту	ДСНС, МОЗ
10. Харчова промисловість та агропромисловий комплекс	Мінагрополітики

Відповідно, сектор безпеки України має забезпечити ідентифікацію основних процесів, які відбуваються в Україні, визначити їх організаційно-функціональну структуру (ресурси, організації, люди, інструменти) та запропонувати

кваліфікаційну спроможність держави відстежувати визначену кількість процесів (найбільш важливих на її погляд) та забезпечувати вплив на їх протікання. Перелік секторів, включених до національної критичної інфраструктури США є, очевидно, найбільш повним і включає 16 секторів.

механізми впливу на зазначені процеси з метою недопущення реалізації загроз стійкості функціонування визначеної КІ.

Відповідно детальне визначення завдань та повноважень органів сектору безпеки і оборони потребуватиме аналізу процесів за вибраними секторами. Надалі ж нами проаналізовано процеси та запропоновано зміст діяльності сектору безпеки у сфері забезпечення стійкості національної економіки, як сектору системи життєдіяльності суспільства, що тим чи іншим чином впливає на функціонування всіх секторів КІ та національну стійкість.

Пріоритетні завдання сектору безпеки з питань захисту критичної інфраструктури.

Стратегія національної безпеки визначає пріоритети реформування Служби безпеки України через її трансформацію на спеціальну службу, яка забезпечить контррозвідувальний захист державного суверенітету, життєво важливих інтересів держави, економічного, науково-технічного і оборонного потенціалу України [2,5].

При цьому, відповідно до Стратегії, передбачається передача більшості правоохоронних функцій, крім боротьби зі злочинами проти основ національної безпеки від Служби безпеки України до правоохоронних органів. Досягнення очікуваного результату передбачається шляхом кардинального оновлення змісту й організації інформаційно-аналітичної роботи у діяльності сектору безпеки [2,5,6]. При цьому, вагомість функції захисту КІ національної економічної системи зростає, особливо враховуючи розширення застосування гібридних методів війни.

В аналітичній доповіді Національного інституту стратегічних досліджень щодо реалізації СРСР активних заходів боротьби з США, відзначається узгодженість дій спецслужб та концепції ведення гібридних війн. Зазначається, що гібридна війна розпочинається з прийняття політичного стратегічного рішення державою – суб'єктом впливу на отримання контролю над державою – об'єктом впливу, і фактично не передбачає повноцінної широкомасштабної збройної агресії. Зокрема, "безпосередньою умовою для розв'язання гібридної війни є негативна соціально-економічна

та/або політична ситуація в державі, проти якої чиниться агресія". Для досягнення цього застосовуються "активні заходи" спрямовані на створення умов "приведення до влади компліментарних та контрольованих суб'єктом впливу політичних сил (агентів впливу), здатних скорегувати курс (зовнішньополітичний, економічний, військовий тощо) держави у потрібному цьому суб'єкту напрямі" [21].

У роботі робиться висновок, що оскільки реалізація "активних заходів" є перманентною діяльністю, особливо щодо держав, які потрапляють у сферу інтересів інших держав з амбіціями щодо розширення зони свого впливу, структури сектору безпеки і оборони України мають бути готові протидіяти застосуванню таких впливів. Розбудова національної стійкості в усіх сферах має стати пріоритетом для досягнення більшої гнучкості та адаптивності системи національної безпеки до гібридних викликів.

У той же час поглиблення взаємодії Служби безпеки України з іншими складовими сектору безпеки і оборони, органами державної влади, установами та організаціями має відбуватись на нових засадах, враховуючи подальшу лібералізації економіки України та її інтеграцію до світового розподілу праці. Виходячи із зазначеного, враховуючи недопущення дублювання діяльності окремих органів сектору безпеки, завдання сектору безпеки в частині забезпечення національної стійкості у сфері економіки (КІ національної економіки), для прикладу, можуть бути визначені як визначення загроз, а також виявлення, попередження, запобігання та припинення протиправної діяльності щодо:

втрати спроможності національної економіки задовольнити критичні потреби суспільства та держави у мінімально необхідних обсягах випуску продукції, надання життєво необхідних послуг (сервісів);

безповоротного виведення ресурсів з національної економіки, втрати контролю над об'єктами стратегічного значення та прав власності на критичні та проривні технології, дестабілізації національної кредитно-банківської системи та страхового ринку;

монополізації економіки та створення економічних передумов для тиску на політичну систему та систему державного управління;

створення умов руйнування інфраструктури життєзабезпечення населення та національної економіки, порушення стійкості функціонування енергетичних систем (електро-, нафто (нафтопродукто)-, газо- постачання);

пошкодження інформаційно-комунікаційної інфраструктури, зокрема систем транспорту, поштового зв'язку та ЗМІ, інших систем масової комунікації, створення умов для втрати Україною керованості у своєму інформаційному просторі;

використання інфраструктури для цілей нанесення шкоди населенню (здійснення терористичних актів);

втрати чутливої інформації щодо функціонування КІ, інтелектуальних прав власності, що може призвести до реалізації загроз національній стійкості;

створення умов втрати спроможності національної економіки забезпечити потреби суспільства та держави, зниження рівня продовольчого самозабезпечення країни

створення умов для завдання шкоди здоров'ю людей, довкіллю та виникнення надзвичайних ситуацій;

порушення системи забезпечення населення ліками та системи лікувальних закладів, порушення системи екстреної медицини;

створення умов для блокування конкурентних переваг, диверсифікації ринків та підвищення впливу національної економіки України на зовнішніх ринках.

Детальніше визначення завдань та повноважень органів сектору безпеки і оборони щодо захисту КІ за різними секторами національної економіки, має бути здійснене на основі визначення відповідних реальних процесів в економіці, які обумовлюють стійкість її функціонування.

В частині вибору інструментарію роботи, окрім контррозвідувального захисту на сектор безпеки, пропонується покласти:

–організацію роботи з інформацією з обмеженим доступом в частині захисту КІ;

–участь в оцінці загроз КІ та формуванні вимог щодо захисту КІ на національному (розробка Національної проектної загрози КІ[4]) та секторальному рівні;

–участь у прийнятті рішень щодо зміни режимів функціонування системи захисту КІ;

–участь у віднесенні об'єктів інфраструктури до переліку КІ;

–погодження Паспортів безпеки[5] об'єктів КІ;

–перевірки операторів КІ щодо дотримання вимог законодавства у сфері захисту КІ;

–проведення спеціальної перевірки громадян, які потребують доступу та виконують особливі роботи на об'єктах КІ.

При цьому, пропонується, що паспорти безпеки (інформація, яка в них міститься) мають стати базою для інформаційно-аналітичного забезпечення діяльності державної системи захисту КІ в Україні, зокрема щодо аналізу, прогнозування, розробки заходів запобігання та реагування на кризові ситуації, а також стати базою для формування Національного плану захисту критичної інфраструктури.

В умовах подальшої лібералізації економічних відносин та міжнародної інтеграції України, необхідно враховувати факт наявності приватних операторів КІ та необхідність розбудови державно-приватного партнерства для та забезпечення стійкості функціонування КІ. Питання взаємодії держави та приватних власників (операторів) критичної інфраструктури потребує законодавчого врегулювання, яке

---

[4] Інструмент формалізації, для суб'єктів державної системи захисту КІ, сучасних викликів та загроз КІ сформований на основі розвідувально-аналітичної роботи сектору безпеки. На сьогодні в Україні в державній системі фізичного захисту передбачено розробку та періодичне уточнення проектної загрози щодо ядерних установок та матеріалів, що фактично визначає перелік тих загроз (та їх характеристики), на які повинна бути розрахована система захисту КІ.

[5] Інструмент формалізації вимог до системи захисту об'єктів КІ сформований оператором КІ відповідно до проектної загрози, що включає: заходи запобігання реалізації потенційних загроз, з виділенням їх цільової спрямованості; заходи реагування на загрози: заходи відновлення нормального функціонування.

має врегулювати не тільки питання збирання, оброблення, інформації та розроблення механізмів і процедур реагування на кризові ситуації, але й створення механізмів ресурсного та фінансового забезпечення захисту КІ.

В частині організації роботи з інформацією з обмеженим доступом в частині захисту КІ, сектор безпеки має забезпечити:

– зберігання та комплексний аналіз даних щодо функціонування КІ, в т.ч. інформацію, що надходитиме від розвідувальних служб;

– ведення реєстру КІ, організація роботи із визначення об'єктів критичної інфраструктури;

– забезпечення необхідного обміну "чутливою" інформацією між операторами КІ та органами державної влади залученими до роботи державної системи захисту КІ.

– підготовку аналітичних матеріалів із комплексної оцінки загроз КІ та доведення такої інформації до політичного керівництва держави.

Одними із ключових елементів державної системи ЗКІ має стати державний орган з питань координації захисту критичної інфраструктури. Оптимальним виходом із цієї ситуації є створення спеціалізованого державного органу з особливим статусом, який буде покликаний виконувати функцію координації дій, сприяти взаємодії та обміну інформацією у цій сфері.[6]

Першочергові кроки з нормативно-правового врегулювання

Слід відзначити, що завдання щодо створення системи захисту критичної інфраструктури та уточнення ролі сектору безпеки і оборони уже перейшло на етап практичного вирішення. Рішенням Ради національної безпеки і оборони України від 29 грудня 2016 року "Про удосконалення заходів забезпечення захисту об'єктів критичної інфраструктури", введеного в дію Указом Президента України № 8/2017 від

[6] Прикладом органу з подібними повноваженнями і функціями щодо критичної інфраструктури може бути Урядовий центр з безпеки Республіки Польща (Rządowe Centrum Bezpieczeństwa - http://rcb.gov.pl/en/)

16 січня 2017 року, передбачено розробку і прийняття Концепції створення системи захисту критичної інфраструктури в Україні та прийняття відповідного профільного закону [22]. Національний інститут стратегічних досліджень, на виконання зазначеного рішення, розробив проект Концепції створення системи захисту критичної інфраструктури в Україні та План заходів з її імплементації [23].

Здійснюється підготовка проекту Закону України "Про критичну інфраструктуру та її захист", в якому передбачається врегулювання питань, зокрема, щодо: координації діяльності із захисту критичної інфраструктури в мирний час та в умовах особливого періоду; визначення функцій, повноважень та відповідальності залучених суб'єктів; запровадження єдиної методології проведення оцінки загроз критичній інфраструктурі та реагування на них; засад державно-приватного партнерства та ресурсного забезпечення у сфері захисту критичної інфраструктури тощо.

Поряд із правовим визначенням основних положень нової системи захисту критичної інфраструктури, має бути внесено зміни і до законів України, для забезпечення відповідності завдань та повноважень сектору безпеки новим викликам (*авт. – нижче наводиться мінімально-необхідні зміни з закони України, що регламентують діяльність Служби безпеки України).*

Зокрема доцільним вбачається доповнити ряд статей Закону України "Про Службу безпеки України"[7], окремими положеннями, зокрема:

– статтю 2 – щодо "захисту критичної інфраструктури";

– статтю 10 – щодо створення функціонального підрозділу "захисту критичної інфраструктури" (можливо замість слів "боротьби з корупцією і організованою злочинною діяльністю");

[7] Про Службу безпеки України: Закон України від 25.03.1992 № 2229-XII [Електронний ресурс] Верховна Рада України. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/2229-12

– статтю 11 – щодо створення підрозділів на окремих "об'єктах критичної інфраструктури" (замість слів "державних стратегічних об'єктах");

– підпункт 6 статті 24 – щодо контррозвідувального забезпечення "критичної інфраструктури" (замість слів "енергетики, транспорту, зв'язку, а також важливих об'єктів інших галузей господарства");

– підпункт 17 статті 24 – щодо розроблення та здійснення заходів "захисту критичної інфраструктури" (перед словами "фізичного захисту…" доповнити словами "захисту критичної інфраструктури, у тому числі");

– підпункт 11 статті 25 – щодо направлення військовослужбовців для виконання завдань "захисту критичної інфраструктури" (доповнити після слів "…в інтересах контррозвідки");

Доповнити ряд статей Закону України "Про оперативно-розшукову діяльність",[8] зокрема:

– статтю 5 – щодо залучення функціонального підрозділу "захисту критичної інфраструктури" (можливо замість підрозділу "спеціальними підрозділами боротьби з корупцією і організованою злочинною діяльністю");

– підпункт 2 статті 6 – щодо запитів про перевірку осіб які здійснюють "особливі роботи" (перед словами "з ядерними матеріалами …" слово "роботи" замінити словами "здійснення особливих робіт на об'єктах критичної інфраструктури, у тому числі");

– підпункт 7 викласти у такій редакції "брати участь у здійсненні заходів захисту критичної інфраструктури, а також у проведенні спеціальної перевірки щодо допуску до особливих робіт, зокрема щодо фізичного захисту ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання)".

Доповнити ряд статей Закону України "Про боротьбу з тероризмом",[9] зокрема:

---

[8] Про оперативно-розшукову діяльність: Закон України від 18.02.1992 № 2135-XII [Електронний ресурс] Верховна Рада України. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/2135-12

– статтю 1, визначення терміну "технологічний тероризм" – положенням щодо порушення функціонування "критичної інфраструктури" (після слів "… руйнування" доповнити "об'єктів, внесених до переліку критичної інфраструктури та") та терміну "терористичний акт" (*авт. – пояснення дивись нижче*);

– статтю 5, в частині визначення повноважень суб'єктів розвідувальних органів – положенням щодо збору інформації для протидії загрозам функціонування КІ (після слів "…громадян України" доповнити словами "критичній інфраструктурі").

Поряд із цим слід зазначити, що Закон України "Про боротьбу з тероризмом" під терористичними актами розуміє "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 категорії може бути віднесено зловмисне пошкодження КІ)[10].

Дана ситуація також потребує виправлення та внесення відповідних змін до Кримінального кодексу України в частині віднесення дій спрямованих на зловмисне пошкодження КІ до сфери відповідальності сектору безпеки та врегулювати питання яким чином відобразити це в діяльності системи антитерористичної системи, яка до цього часу не опікується "диверсіями".

Висновки. Отримані Україною уроки протидії гібридній війні свідчить, що порушення функціонування критичної інфраструктури життєдіяльності суспільства та держави стає

---

[9] Про боротьбу з тероризмом: Закон України від від 20.03.2003 № 638-IV [Електронний ресурс]Верховна Рада України. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/638-15

[10] Кримінальний кодекс України: Закон України від 05.04.2001 № 2341-III [Електронний ресурс] Верховна Рада України. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/2341-14

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 концепція захисту критичної інфраструктури є адекватною сучасною відповіддю новим викликам, а державна система захисту 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. Функції та послуги, якими критична інфраструктура забезпечує суспільство та державу, мають лежати в основі визначення предмету діяльності національної системи захисту і, зокрема, визначення завдань сектору безпеки.

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 єдину, скоординовану систему захисту критичної інфраструктури.

Список використаної літератури

1. Світова гібридна війна: український фронт : монографія / за заг. ред. В.П. Горбуліна. – К. : НІСД, 2017. – 496 с.

2. Концептуальні засади розвитку системи забезпечення національної безпеки України: аналіт. доп. / О. О. Резнікова, В. Ю. Цюкало, В. О. Паливода, С. В. Дрьомов, С. В. Сьомін. – К. НІСД, 2016. – 58 с. – [Електронний ресурс] – Режим доступу: http://www.niss.gov.ua/articles/1873

3. Турчинов О. Національна безпека України: виклики та пріоритети / О.Турчинов // Голос України, 17 серпня 2016 року. – [Електронний ресурс]. – Режим доступу: http://www.golos.com.ua/article/274453

4. Реформування і розвиток Служби безпеки в контексті євроінтеграції України: наук.-метод. посіб. / В. Г. Пилипчук, О. Ф. Белов, С. С. Кудінов. – К.: Нац. акад. СБУ, 2017. – 260 с.

5. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року "Про Стратегію національної безпеки України": Указ Президента України від 26.05.2015 № 287/2015 [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/287/2015

6. Про рішення Ради національної безпеки і оборони України від 4 березня 2016 року "Про Концепцію розвитку сектору безпеки і оборони України": Указ Президента України від 14.03.2016 р.№ 92/2016. – [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/92/2016

7. Рада національної безпеки та оборони розгляне Концепцію реформування Служби безпеки України – Офіційне інтернет-представництво Президента України. [Електронний ресурс]. – Режим доступу: http://www.president.gov.ua/news/rada-nacionalnoyi-bezpeki-ta-oboroni-rozglyane-koncepciyu-re-40542

8. 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. – [Електронний ресурс]. – Режим доступу: http://www.niss.gov.ua/articles/2213/

9. The National Strategy of the United States of America, 2002. [Електронний ресурс] U.S. Departament of State. – Режим доступу: https://www.state.gov/documents/organization/63562.pdf

10. The National Strategy for Homeland Security, 2002. [Електронний ресурс] U.S. Departament of Homeland Security. – Режим доступу: https://www.dhs.gov/sites/default/files/publications/nat-strat-hls-2002.pdf

11. The National Strategy for Homeland Security, 2007. [Електронний ресурс] U.S. Departament of Homeland Security. – Режим доступу:

http://www.dhs.gov/xlibrary/assets/nat_strat_homelandsecurity_2007.pdf

12. National Infrastructure Protection Plan, 2006 [Електронний ресурс] U.S. Department of Homeland Security. – Режим доступу: https://www.dhs.gov/xlibrary/assets/NIPP_Plan_noApps.pdf

13. National Infrastructure Protection Plan, 2013. Partnering for Critical Infrastructure Security and Resilience [Електронний ресурс] U.S. Department of Homeland Security. – Режим доступу: https://www.dhs.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf

14. Communication from the Commission on a European Programme for Critical Infrastructure Protection (COM/2006/786 final) [Електронний ресурс] EUR-Lex.europa.eu. – Режим доступу: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52006DC0786&from=EN

15. Council Directive 2008/114/EC of 8 December on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection [Електронний ресурс] EUR-Lex.europa.eu. – Режим доступу: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF

16. Щедровицкий Г.П. Избранные труды / Г.П.Щедровицкий. – М.: Шк. культ. полит., 1995. – 800 с.

17. Global trends: paradox of progress. A publication of the National Intelligence Council. NIC, January 2017 [Електронний ресурс] Office of the Director of National Intelligence. – Режим доступу: http://www.dni.gov/nic/globaltrends

18. Суходоля О.М. Теоретико-методологічні засади забезпечення енергетичної безпеки України / О.М. Суходоля // Стратегічні пріоритети. – 2014. – № 2. – С. 129–139

19. A New EU Strategic Approach to Global Development, Resilience and Sustainability [Електронний ресурс] European Union. – Режим доступу:

http://europa.eu/globalstrategy/en/new-eu-strategic-approach-global-development-resilience-and-sustainability

20. Commitment to enhance resilience [Електронний ресурс] North Atlantic Treaty Organization. – Режим доступу: http://www.nato.int/cps/en/natohq/official_texts_133180.htm?selectedLocale=en

21. "Активні заходи" СРСР проти США: пролог до гібридної війни: аналіт. доп. / Д.В. Дубов, А.В. Баровська, Т.О. Ісакова, І.О. Коваль, В.П. Горбулін; за заг. ред. Д.В. Дубова. – К.: НІСД, 2017. – 88 с. – [Електронний ресурс]. – Режим доступу: http://www.niss.gov.ua/articles/2576/

22. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року "Про удосконалення заходів забезпечення захисту об'єктів критичної інфраструктури": Указ Президента України від 16.01.2017 № 8/2017 – [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/8/2017

23. Щодо створення державної системи захисту критичної інфраструктури: аналітична записка [Електронний ресурс] Національний інститут стратегічних досліджень. – Режим доступу: http://www.niss.gov.ua/content/articles/files/infrastrukt-86de2.pdf

References

1. Svitova hibrydna viyna: ukrayins'kyy front: monohrafiya (2017) (World hybrid war: Ukrainian front: monograph) za zah. red. V.P. Horbulina. Kyiv, 2017, 496 p.

2. *Reznikova O.O., Tsyukalo V. Yu., Palyvoda V. O. and others* (2016) Kontseptual'ni zasady rozvytku systemy zabezpechennya natsional'noyi bezpeky Ukrayiny: analitychna dopovid' (Conceptual framework for the development of the system of ensuring the national security of Ukraine: analytical report). Kyiv, 2016, 496 p. Regime to access: http://lvivacademy.com/visnik12/fail/Didenko.pdf

3. *Turchynov O.* (2016) Natsional'na bezpeka Ukrayiny: vyklyky ta priorytety (National Security of Ukraine: Challenges and

Priorities) *Holos Ukrayiny, 2016, August 17.* Regime to access: http://www.golos.com.ua/article/274453

4. *Pylypchuk V. H., Belov O. F., Kudinov S. S.* (2017) Reformuvannya i rozvytok Sluzhby bezpeky v konteksti yevrointehratsiyi Ukrayiny: nauk.-metod. posib. (Reform and development of the Security Service in the context of Eurointegration of Ukraine: science-method. manual). Kyiv, 2017, 260 p.

5. President of Ukraine (2015), Decree "On the decision of the National Security and Defense Council of Ukraine dated May 6, 2015 "On the Strategy of National Security of Ukraine", available at: http://zakon3.rada.gov.ua/laws/show/287/2015 (Accessed 26 May 2015).

6. President of Ukraine (2016), Decree "On the decision of the Council of National Security and Defense of Ukraine dated March 4, 2016 "On the Concept of Development of the Security and Defense Sector of Ukraine", available at: http://zakon3.rada.gov.ua/laws/show/92/2016 (Accessed 14 March 2016).

7. Official online representation of the President of Ukraine (2017) "The National Security and Defense Council will consider the Concept of Reform of the Security Service of Ukraine", available at: http://www.president.gov.ua/news/rada-nacionalnoyi-bezpeki-ta-oboroni-rozglyane-koncepciyu-re-40542 (Accessed 24 March 2017)

8. Zelena knyha z pytan' zakhystu krytychnoyi infrastruktury v Ukrayini: zb. materialiv mizhnar. ekspert. Narad (2016) "Green book on critical infrastructure protection in Ukraine: Sb. materials international expert. meetings" uporyad. D.S. Biryukov, S.I Kondratov; za zah. red. O.M. Sukhodoli. Kyiv, 2016, 176 p., Regime to access: http://www.niss.gov.ua/articles/2213

9. U.S. Departament of State (2002) The National Strategy of the United States of America, 2002, available at: https://www.state.gov/documents/organization/63562.pdf (Accessed September 2002)

10. U.S. Departament of Homeland Securoty (2007) 10. The National Strategy for Homeland Security, 2002, available at:

https://www.dhs.gov/sites/default/files/publications/nat-strat-hls-2002.pdf (Accessed July 2002)

11. U.S. Departament of Homeland Securoty (2007) The National Strategy for Homeland Security, 2007, available at: http://www.dhs.gov/xlibrary/assets/nat_strat_homelandsecurity_2007.pdf (Accessed October 2007)

12. U.S. Department of Homeland Security (2006) National Infrastructure Protection Plan, 2006, available at: https://www.dhs.gov/xlibrary/assets/NIPP_Plan_noApps.pdf (Accessed 2006)

13. U.S. Department of Homeland Security (2013) National Infrastructure Protection Plan, 2013. Partnering for Critical nfrastructure Security and Resilience, available at: https://www.dhs.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf (Accessed 2013)

14. EUR-Lex.europa.eu (2006) Communication from the Commission on a European Programme for Critical Infrastructure Protection (COM/2006/786 final), available at: –http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52006DC0786&from=EN (Accessed 12 December, 2006)

15. EUR-Lex.europa.eu (2008) Council directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF (Accessed 8 December 2008)

16. *Shchedrovytskyy H.P.* (1995) Izbrannye Trudy (Selected Works). Moscow, 1995, 800p.

17. Office of the Director of National Intelligence (2017) Global trends: paradox of progress. A publication of the National Intelligence Council. NIC, avialeble at: http://www.dni.gov/nic/globaltrends(Accessed January 2017)

18. *Sukhodolya O.M.* (2014) Teoretyko-metodolohichni zasady zabezpechennya enerhetychnoyi bezpeky Ukrayiny (Theoretical and methodological principles of ensuring the energy security of Ukraine) *Stratehichni priorytety,* Kyiv, 2014, no 2, pp. 129-139.

19. European Union (2016) A New EU Strategic Approach to Global Development, Resilience and Sustainability, avialeble at: http://europa.eu/globalstrategy/en/new-eu-strategic-approach-global-development-resilience-and-sustainability (Accessed 14 May 2016)

20. North Atlantic Treaty Organization (2016) Commitment to enhance resilience, avialeble at: http://www.nato.int/cps/en/natohq/official_texts_133180.htm?selectedLocale=en (Accessed 8 July 2016).

21. *Dubov D.V., Barovs'ka A.V., Isakova T.O. and others* (2017) "Aktyvni zakhody" SRSR proty USA: proloh do hibrydnoyi viyny: analit. dop. (Active steps "SSR vs. USA: prologue to hybrid war: analytical report) za zah. red. D.V. Dubova, Kyiv, 2017, p. 88. Regime to access: http://www.niss.gov.ua/articles/2576/

22. President of Ukraine (2017), Decree "On the decision of the Council of National Security and Defense of Ukraine dated December 29, 2016, "On improvement of measures for the protection of objects of critical infrastructure", available at: http://zakon3.rada.gov.ua/laws/show/8/2017 (Accessed 16 January 2017).

23. The National Institute for Strategic Studies (2017) On the creation of a state system for critical infrastructure protection: Analytical note NISS, available at: http://www.niss.gov.ua/content/articles/files/infrastrukt-86de2.pdf (Accessed February 2017).