УДК 351.824.11

DOI: https://doi.org/10.31470/2786-6246-2024-9-142-150

Помаза-Пономаренко Аліна, доктор наук з державного управління, старший дослідник, начальник наукового відділу з дослідження проблем державної безпеки науково-дослідного центру Національного університету цивільного захисту України

Pomaza-Ponomarenko Alina, Doctor of Sciences in Public Administration, Senior Researcher, Head of the Scientific Department for State Security Problems of Research Centre of the National University of Civil Protection of Ukraine

ORCID ID: https://orcid.org/0000-0001-5666-9350

Тарадуда Дмитро, кандидат технічних наук, доцент, заступник начальника кафедри організації та технічного забезпечення аварійно-рятувальних робіт Національного університету цивільного захисту України

Taraduda Dmytro, PhD in Technical Science, Associate professor, Deputy Head of Department of Organization and Technical Support of Emergency Rescue Works, National University of Civil Protection of Ukraine

ORCID ID: https://orcid.org/0000-0001-9167-0058

СВІТОВИЙ ДОСВІД ПРОТИСТОЯННЯ ВПЛИВУ ГІБРИДНОЇ ВІЙНИ НА НАЦІОНАЛЬНУ Й ЕНЕРГЕТИЧНУ БЕЗПЕКУ ТА ЇЇ ОБ'ЄКТИ

GLOBAL EXPERIENCE OF COUNTING THE IMPACT OF HYBRID WARFARE ON NATIONAL AND ENERGY SECURITY AND ITS OBJECTS

Анотація. Виявлено, що характеристика складових національної безпеки дає підстави наполягати на важливості реалізації комплексу заходів, спрямованих на підтримку на належному рівні енергетичної та соціальної безпеки, що функціонує в умовах гібридної війни. Ця війна негативно позначається на всіх країнах світу, у т.ч. на Україні. Виявлено, що внаслідок значного розвитку інформаційно-комунікаційних технологій і зростаючої залежності від них з'явилася нова сфера протистояння, одним з супротивників якої є рф, вплив якої згубно позначається на політичних та військових функціях НАТО загалом і України зокрема. З'ясовано, що деструктивний вплив рф на енергетичну сферу України та держав-членів НАТО проявляється не тільки, починаючи з 2022 р., його очевидні наслідки можна знайти ще у 2009 р. під час роботи об'єктів енергетичної інфраструктури Німеччини та інших країн. Крім того, можна знайти опосередкований російський слід впливу на енергетичну безпеку різних країн світу (зокрема, через Іран). Акцентовано, що повсюдність цифрового підключення, здатність заперечувати причетність до нападів та переваги порушення роботи критично важливої енергетичної інфраструктури за допомогою операцій, що залежать від мереж, стали рушійною силою в еволюції гібридної війни рф. Ще більшої складності ситуації в Україні становлять масовані атаки держави-агресора на вітчизняні об'єкти критичної інфраструктури. Це робиться, у тому числі з метою дестабілізації розвитку українського суспільства, збільшення серед нього невдоволення, апатії, агресії, конфліктів тощо. На цій підставі наполягається на подвійній ролі вітчизняних державних органів у протистоянні неоголошеній війні рф. Допомогти в цьому може міжнародна технічна допомога, зокрема НАТО. Аргументовано, що НАТО перебуває в унікальному становищі, яке дозволяє цьому Альянсу посилити роботу держав-членів, покликану усунути фактори вразливості, та узагальнити уроки, що були засвоєні в цій сфері. Установлено, що перед Альянсом стоїть завдання вийти на належний

рівень оперативної взаємодії, щоб стримувати потенційно руйнівні гібридні напади рф на енергетичну інфраструктуру й її відновлення після них.

Ключові слова: публічне управління, державна політика, національна безпека, енергетична безпека, соціальна безпека, гібридна війна, критична інфраструктура, об'єкти підвищеної небезпеки, кібератаки, НАТО.

Annotation. It was revealed that the characteristics of the components of national security give reasons to insist on the importance of implementing a set of measures aimed at maintaining an adequate level of energy and social security functioning in the conditions of a hybrid war. This war has a negative impact on all countries of the world, including in Ukraine. It was revealed that due to the significant development of information and communication technologies and the growing dependence on them, a new sphere of confrontation has appeared, one of whose opponents is the Russian Federation, whose influence has a detrimental effect on the political and military functions of NATO in general and Ukraine in particular. It was found that the destructive influence of the Russian Federation on the energy sphere of Ukraine and NATO member states is manifested not only starting from 2022, its obvious consequences can be found as early as 2009 during the operation of energy infrastructure facilities in Germany and other countries. In addition, one can find an indirect Russian trace of influence on the energy security of various countries of the world (in particular, through Iran). It is emphasized that the ubiquity of digital connectivity, the ability to deny involvement in attacks, and the benefits of disrupting critical energy infrastructure through network-dependent operations have become a driving force in the evolution of Russian hybrid warfare. The situation in Ukraine is even more complicated by massive attacks by the aggressor state on domestic critical infrastructure facilities. This is done, including with the aim of destabilizing the development of Ukrainian society, increasing discontent, apathy, aggression, conflicts, etc. among it. On this basis, he insists on the dual role of domestic state bodies in opposing the undeclared war of the Russian Federation. International technical assistance, in particular NATO, can help in this. It is argued that NATO is in a unique position that allows the Alliance to strengthen the work of member states to address vulnerabilities and to generalize lessons learned in this area. It has been established that the Alliance faces the task of reaching the appropriate level of operational cooperation in order to deter potentially destructive hybrid attacks by the Russian Federation on the energy infrastructure and its recovery after them.

Keywords: public administration, public policy, national security, energy security, social security, hybrid warfare, critical infrastructure, objects of increased danger, cyber attacks, NATO.

Постановка проблеми. Із початку XXI ст. енергетична безпека стала одним із ключових стратегічних секторів, що закріплюється у військових доктринах і стратегіях нацбезпеки. Як показують нещодавні події, енергетична безпека стала однією з найважливіших і зростаючих проблем для України та країн-членів НАТО в епоху гібридної боротьби. Складності ситуації для нашої держави додає неоголошена війна рф, що постійно обстрілює об'єкти критичної інфраструктури України. Критична інфраструктура представляє собою один із ключових факторів соціально-економічного розвитку, забезпечення обороноздатності держави. Критична інфраструктура має забезпечувати задоволення найважливіших інтересів держави, суспільства та громадян. У цьому контексті набувають актуальності аспекти, пов'язані з дослідженням особливостей забезпечення енергетичної безпеки в епоху гібридної війни. Адже незабезпечення енергетичної безпеки може зумовлювати соціальну апатію, хаос, невдоволення, кризу, суспільні конфлікти та інші негативні соціальні процеси й явища [3; 4]. Відтак, важливим завданням будь-якої держави є підтримка системи національної безпеки, що включає соціальну, енергетичну, економічну та ін. Усе це визначає актуальність обраної проблематики дослідження.

Аналіз останніх досліджень і публікацій. Особливості публічного управління у сфері енергетичної безпеки є предметом дослідження закордонних і вітчизняних учених Л. Антонової, В. Бутрімас, А. Гогореліані, А. Граніцас, І. Драгана, А.К. Дюпюї, В. Євдокімова, С. Калояннідіса, Е.Дж. Кіршнера, О. Крюкова, С. Лінгаас, С. Майстра, Д. Нуссбаум, Дж. Слоуїк, О. Стоян, Є. Шульги, А. Хіггінс та ін.

Постановка завдання. Метою статті є дослідження особливостей впливу гібридної війни на енергетичну безпеку як складника національної безпеки.

Виклад основного матеріалу. Термін «гібридна загроза» означає дії державних або недержавних суб'єктів із метою підриву сталого розвитку або нанесення шкоди відкритими та/або латентними військовими та невоєнними засобами [1; 2]. При гібридних загрозах дезінформація, кібератаки, економічний тиск, розгортання нерегулярних збройних груп та застосування регулярних сил використовуються в комплексі, причому часто протягом тривалого часу [там само].

Держава-агресор належить до тих, хто найбільш активно веде гібридну боротьбу, і найефективніше вона проявляється під час ведення неоголошеної війни проти України. Ця війна розпочалась через незаконну анексію Криму в 2014 р. рф продовжує вести гібридну війну проти нашої держави й сьогодні, а також по відношенню до інших країн, щоб досягти бажаних політичних результатів, наприклад, підриву прозахідних урядів, розколу та ослаблення впливу НАТО або просування своїх власних економічних інтересів.

Останнім часом Китай також почав проводити кібератаки та дезінформаційні кампанії, націлені на країни НАТО, і становить серйозний ризик для критично важливої інфраструктури, включаючи енергетичну інфраструктуру, як наголошено в нещодавній доповіді експертів НАТО-2030 [1; 12].

Зрештою, проблеми, які гібридна війна представляє для енергетичного сектора, потенційно можуть порушити політичну, соціальну та військову ефективність, а також злагодженість в роботі НАТО. Для подолання цих загроз знадобиться час і зусилля, щоб Альянс вирішив питання залежності своїх членів і виступив як платформа для створення загальної картини комплексного оперативного ризику та факторів уразливості.

Енергетичний сектор є однією ж важливих цілей функціонування будь-якої держави та міжнародних об'єднань. Вони змушені швидко адаптуватися до умов зростаючої гібридної війни. Власне кажучи, протягом останніх десяти років гібридні загрози різко зросли у всьому світі: від кібератак до дезінформаційних кампаній та потайних військових операцій [1; 12]. Загрози виникають усе частіше, набуваючи більш комплексного, руйнівного та силового характеру. Наслідки гібридної боротьби важливі як для економіки, так і для державної політики, особливо стосовно енергетичного сектору.

Держава-агресор створила низку гібридних загроз проти енергетичних об'єктів, зокрема й критичної інфраструктури загалом в Україні, а також проти політики держав-членів НАТО, інших країн світу. Власне, рф пустила в хід політичні й економічні важелі у поєднанні з дезінформаційними кампаніями проти Болгарії та Румунії, щоб підірвати зусилля щодо зниження залежності цих країн від російських джерел енергії [8]. Зрив поставок використовувався і раніше, зокрема щодо країн Балтії й України у 2009 р., і нещодавно – проти Болгарії. Держава-агресор також використала свою економічну міць у поєднанні з політичним впливом для просування свого енергетичного порядку денного в Угорщині, де зараз триває робота з розширення атомної електростанції Пакш за

ISSN 2786-6246 (print) ● ISSN 2786-9091 (online)

російською енергетичною технологією [10]. Рф використовує свої комерційні та політичні зв'язки також у Німеччині, щоб просувати спірний нафтопровід «Північний потік – 2» вартістю 12 млрд. євро, який вже майже було завершено. Крім того, російська група Berserk Bear APT підозрюється у скоєнні кібернападів у 2020 р. на німецькі енергетичні компанії, і вона була причетна до попередніх кібернападів на німецькі об'єкти комунального господарства у 2018 р. [11].

У низці інших країн НАТО, зокрема Великій Британії, Польщі, Туреччині та США, було виявлено кібернапади на енергетичні об'єкти, скоєні за підтримки рф. У деяких випадках ці кібернетичні кампанії велися паралельно з іншими гібридними загрозами щодо енергетичних об'єктів, наприклад, надання шкідливого впливу та скорочення постачання природного газу. Якщо скласти все це разом, то стає очевидним, що в останні десять років рф веде регулярну гібридну кампанію, спрямовану на підрив енергетичної безпеки різних країн світу, причому зі зростаючою силою.

Серед країн-партнерів НАТО в той же період російська гібридна кампанія була найбільш помітною в Україні: зриви поставок, кібератаки, вплив на економіку та політику, дезінформація з метою підриву енергетичної безпеки країни та створення політичної нестабільності. Найбільше рф вдалося порушити нормальне функціонування в 2009 р., коли було припинено постачання природного газу [14]. Проте напади тривають і набувають все більш комплексного та силового характеру, зокрема, починаючи з повномасштабної агресії рф у 2022 р.

Відомий приклад – скоєний у грудні 2015 р. кібернапад групи Black Energy на західноукраїнську електростанцію, унаслідок чого майже чверть мільйона жителів на шість годин відключила електрику. Через рік за допомогою шкідливого програмного забезпечення CrashOverride/Industroyer було скоєно більш витончений напад на мережу електропостачання столиці країни – Києва. Хоча за своєю тривалістю та масштабом цей напад був меншим за попередній, за своїм характером він був набагато страшнішим: мета нападу полягала в тому, щоб вивести з ладу реле електробезпеки, які використовуються для захисту обладнання енергосистем. Якби аналітики не виявили його, в результаті заключного етапу нападу було б фізично знищено дороге і важко замінне обладнання, крім короткострокового зриву електропостачання.

За межами євроатлантичного регіону Іран і, як підозрюють, інші держави ведуть наразі комплексну гібридну кампанію проти енергетичних об'єктів Саудівської Аравії. На прикладі цієї кампанії можна, ймовірно, скласти уявлення про майбутнє гібридної боротьби, зокрема у сфері енергетичної безпеки. З допомогою латентних і відкритих військових операцій, і використовуючи підставні сили Іран неодноразово порушував функціонування саудівської енергетичної інфраструктури та завдав по ній ударів.

Можлива змова вороже настроєних сил у іранській кампанії проти Саудівської Аравії, що триває, викликає особливе занепокоєння і може спричинити наслідки для країн НАТО. Зокрема, у результаті кібератаки на комплекс Petro Rabigh у 2017 р. довелося зупинити об'єкт і провести ретельне очищення, що було пов'язано з великими матеріальними витратами, більше того, мало не стався неконтрольований витік газу та вибух. Незважаючи на початкові припущення про те, що відповідальність за застосування небезпечного шкідливого програмного забезпечення Triton, використаного при нападі, належить лише Ірану. США дійшли висновку про те, що це програмне забезпечення було розроблене рф, і наклали санкції на науково-дослідну установу, пов'язану з його

розробкою. Це шкідливе програмне забезпечення було також задіяне під час нападів на енергетичні компанії в США [15].

До інших заходів, застосованих по відношенню до рф, як підозрюється, під час іранської кампанії, відносяться два удари із застосуванням БПЛА хуситами-союзниками Ірану по саудівських нафтопереробних заводах, напади в Перській затоці на два нафтові танкери, зареєстровані в Саудівській Аравії, і скоєні нещодавно напади на два іноземних танкери в саудівських портах у Червоному морі. Зокрема, внаслідок удару із застосуванням БПЛА по НПЗ «Сауді Арамко» в Абкаїці наприкінці 2019 р., відповідальність за який взяли на себе сили хуситів, у Ірану з'явилася можливість заперечувати свою причетність, і водночас це допомогло виявити слабкість протиповітряної оборони Саудівської Аравії.

Керівники країн НАТО наголошують на важливості енергетичної безпеки, на їх погляд, стабільне та надійне енергопостачання, диверсифікація шляхів імпорту, постачальників та енергоресурсів, а також взаємопов'язаність енергомереж мають ключове значення та підвищують стійкість перед політичним й економічним тиском. Хоча за ці питання відповідає, насамперед, державна влада, події в енергетичній сфері можуть мати значні політичні наслідки та наслідки для безпеки країн НАТО, а також торкнутися партнерів Альянсу [6].

Критично важливі об'єкти енергетичної інфраструктури – це потенційні цілі, що могло б дати противнику привабливі переваги, такі як:

1) зрив енергопостачання;
2) порушення роботи громадянської інфраструктури, від якої залежать збройні сили, що може також підірвати соціальну згуртованість;
3) демонстрація руйнівних можливостей з метою залякування тощо.

Шкідлива кібернетична діяльність є ефективною, дешевою (для держави), і вона дозволяє заперечувати свою причетність до неї. У міру того, як світ отримує користь і все більше залежить від нових технологій – Інтернету речей та промислового Інтернету речей, – суспільство та інфраструктура стають більш вразливими. В енергетичному секторі взаємопов'язаність глобальної мережі енергопостачання дозволяє досягти більшої результативності й економії ресурсів. Однак через те, що розширюється доступ до експлуатаційної технології енергосфери та зростає її взаємопов'язаність з системою безпеки, виникають численні можливості для нападів. Зі збільшенням глобальної енергетичної інфраструктури, її інтеграцією та зростаючою залежністю від можливості об'єднання вже спостерігається збільшення кількості кіберзлочинців, які часто користуються підтримкою держав та застосовують шкідливе програмне забезпечення, здатне порушувати розподіл енергії у дедалі більшому районі.

Суперечки навколо Huawei/5G, які велися протягом минулих років, свідчать про ще один фактор, що викликає велике занепокоєння. Якщо засоби зв'язку Huawei будуть розгорнуті в державах-членах НАТО, чи може уряд Китаю проникнути в них чи створити загрозу якимось іншим чином, чи гібридна загроза набуває нового виміру, чи маємо ми відтепер турбуватися не лише про кібератаки, а й про фізичні апаратні засоби, що встановлюються на критично важливих об'єктах інфраструктури, особливо якщо ці апаратні засоби виробляються у потенційно ворожих країнах і можуть бути перехоплені та зламані під час доставки споживачеві. Подібні фактори уразливості виникають і в енергетичному секторі.

Райони бойових дій усе більше і більше функціонують у дедалі більшому взаємозв'язку та залежності від енергетичної та комунікаційної інфраструктури. Таким чином, з'являється безліч векторів нападу, за допомогою яких противник

ISSN 2786-6246 (print) ● ISSN 2786-9091 (online)

може вчепитись, зриваючи потік рідкого палива або електроживлення в район бойових дій. Навіть короткострокова або періодична відмова в обслуговуванні може позначитися на здатності сил НАТО до пересування і мати згубний вплив на виконання оперативного завдання в контексті колективної оборони за статтею 5 основного договору НАТО. У Стратегічній концепції НАТО зазначено, що Альянс повинен створювати та підтримувати мобільні готові до розгортання сили для виконання зобов'язань за статтею 5, а також проведення експедиційних операцій, у тому числі за допомогою Сил реагування НАТО. Саме цей недолік мобільності був підкреслений у доповіді One Flank, One Threat, One Presence: A Strategy for NATO's Eastern Flank («Один фланг, одна загроза, одна присутність: стратегія для східного флангу НАТО»), підготовленої у травні 2020 р. Центром європейського політичного аналізу.

Альянс визнає загрозу енергетичній безпеці та загрозу гібридної війни. Ще на зустрічі на найвищому рівні в Бухаресті в 2008 р. країни НАТО відзначили роль Альянсу в забезпеченні енергетичної безпеки, і у 2012 р. у Вільнюсі було створено Центр передового досвіду НАТО з енергетичної безпеки [7]. За підтримки НАТО було створено Європейський центр передового досвіду боротьби з гібридними загрозами, урочисте відкриття якого відбулося у жовтні 2017 р. в Гельсінкі.

У 2020 р. Науково-технічна рада НАТО дала офіційний дозвіл на створення цільової науково-дослідної групи, яка займеться проблемою енергетичної безпеки в епоху гібридної війни. Цільова група, до складу якої увійде понад 80 вчених із більш ніж десятки країн світу, аналізуватиме гібридну енергетичну загрозу та її вплив на готовність НАТО та його здатність до виконання завдання, стійкість інфраструктури держав-членів Альянсу та їхню здатність до участі в місіях НАТО [9]. Отже, одним із ключових аспектів роботи цільової науково-дослідної групи є складання загальної картини енергетичної безпеки Альянсу. Дослідницька група має виявляти уразливі точки у разі гібридної енергетичної боротьби у таких галузях, як боєздатність сил Альянсу, збереження життєво важливих послуг в енергетичному секторі, що надаються суспільству, довіри громадськості до державних установ та ін. Дослідницька робота також спрямована на те, щоб визначити низку можливих стратегій пом'якшення наслідків та контрзаходів, які могли б зробити НАТО і держави-члени.

Висновки. Таким чином, характеристика складових національної безпеки дає підстави наполягати на важливості реалізації комплексу заходів, спрямованих на підтримку на належному рівні енергетичної та соціальної безпеки, що функціонує в умовах гібридної війни. Вона негативно позначається на всіх країнах світу, у т.ч. на Україні. Виявлено, що внаслідок значного розвитку інформаційно-комунікаційних технологій і зростаючої залежності від них з'явилася нова сфера протистояння, одним з супротивників якої є рф, вплив якої згубно позначається на політичних та військових функціях НАТО загалом і України зокрема. Акцентовано, що повсюдність цифрового підключення, здатність заперечувати причетність до нападів та переваги порушення роботи критично важливої енергетичної інфраструктури за допомогою операцій, що залежать від мереж, стали рушійною силою в еволюції гібридної війни. Ще більшої складності ситуації в Україні становлять масовані атаки рф на вітчизняні об'єкти критичної інфраструктури. Це робиться, у тому числі з метою дестабілізації розвитку українського суспільства, збільшення серед нього невдоволення, апатії, агресії, конфліктів тощо. На цій підставі наполягається на подвійній ролі вітчизняних державних органів у протистоянні неоголошеній війні

рф: відстоювання власного суверенітету й територіальної цілісності, а також захист енергетичної безпеки й об'єктів критичної інфраструктури від руйнівного впливу рф. Допомогти в цьому може міжнародна технічна допомога, зокрема НАТО. З'ясовано, що НАТО перебуває в унікальному становищі, яке дозволяє цьому Альянсу посилити роботу держав-членів, покликану усунути фактори вразливості, та узагальнити уроки, що були засвоєні в цій сфері. Установлено, що з цією метою було створено Центр передового досвіду НАТО з енергетичної безпеки у 2012 р. у Вільнюсі. Крім того, за підтримки НАТО було створено Європейський центр передового досвіду боротьби з гібридними загрозами у 2017 р. в Гельсінкі. Перед Альянсом стоїть завдання вийти на належний рівень оперативної взаємодії, щоб стримувати потенційно руйнівні гібридні напади рф на енергетичну інфраструктуру й її відновлення після них.

Список використаних джерел:

1. Домбровська С.М., Помаза-Пономаренко А.Л., Крюков О.І., Порока С.Г. Інформаційні загрози та комунікативна інфраструктура в державному секторі: монографія. Харків: НУЦЗУ, 2024. 244 с.
2. Помаза-Пономаренко А.Л., Новіков В.О. Шляхи трансформації інституційних механізмів публічного управління в Україні: від інформаційних загроз до гібридних війн. *Державне будівництво: електронний журнал.* 2023. № 1 (33). URL: https://periodicals.karazin.ua/db/article/view/22921 (дата звернення: 30.06.2024).
3. Помаза-Пономаренко А.Л., Тарадуда Д.В. Закордонний досвід забезпечення соціальної безпеки шляхом стійкого функціонування об'єктів критичної інфраструктури та підвищеної небезпеки. *Наука і техніка сьогодні*. 2024. № 4 (32). С. 371–384.
4. Помаза-Пономаренко А.Л., Тарадуда Д.В. Забезпечення стійкості системи державного регулювання об'єктів підвищеної небезпеки. *Державне управління: удосконалення та розвиток*. 2024. № 4. URL: https://www.nayka.com.ua/index.php/dy/article/view/3461. (дата звернення: 30.06.2024).
5. Помаза-Пономаренко А.Л., Тарадуда Д.В. Механізми забезпечення цивільної безпеки України: аспекти попередження НС на об'єктах військово-промислового комплексу. *Публічне адміністрування та національна безпека.* 2024. № 3 (44). URL: https://www.inter-nauka.com/issues/administration2024/3/9732 (дата звернення: 30.06.2024).
6. Dupuy A.C., Nussbaum D., Butrimas V., Granitsas A. Energy Security in the Age of Hybrid Warfare. January 13, 2021. URL: https://www.nato.int/docu/review/ru/articles/2021/01/13/energeticheskaya-bezopasnost-v-epohu-gibridnoj-bor-by/index.html (дата звернення: 30.06.2024).
7. Gogoreliani A. Energy efficiency and renewable energy solutions in NATO and PfP countries' military operations. September 10, 2021. URL: https://www.enseccoe.org/publications/energy-efficiency-and-renewable-energy-solutions-in-nato-and-pfp-countries-military-operations/ (дата звернення: 30.06.2024).
8. Higgins A. Russian Money Suspected Behind Fracking Protests. *The New York Times.* November 30, 2014. URL: https://www.nytimes.com/2014/12/01/world/russian-money-suspected-behind-fracking-protests.html (дата звернення: 30.06.2024).
9. Energy Security n the Era of Hybrid Warfare. *Empowering NATO`s Technological Edge.* 2020. URL: https://www.sto.nato.int/Lists/STONewsArchive/displaynewsitem.aspx?ID=524 (дата звернення: 30.06.2024).
10. Illicit Influence – Part Two – The Energy Weapon. *Alliance for Securing Democracy.* 2019. URL: https://securingdemocracy.gmfus.org/illicit-influence-part-two-energy-weapon/ (дата звернення: 30.06.2024).
11. Lyngaas S. German intelligence agencies warn of Russian hacking threats to critical infrastructure. May 26, 2020. URL: https://cyberscoop.com/german-intelligence-memo-berserk-bear-critical-infrastructure/ (дата звернення: 30.06.2024).
12.

13. NATO 2030: United for a new era. Analysis and Recommendations of the Reflaction Group Appointed by the NATO Secretary General. 2020. URL: https://www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf (дата звернення: 30.06.2024).
14. Pomaza-Ponomarenko A., Taraduda D., Leonenko N., Poroka S., Sukhachov M. Ensuring the safety of citizens in times of war: aspects of the organization of civil defense. *AD ALTA: Journal of Interdisciplinary Research*. 2024. Vol. 14. Issue 1. Pp. 216–220.
15. Slowik J. CRASHOVERRIDE: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack. Augest 15, 2019. URL: https://www.dragos.com/wp-content/uploads/CRASHOVERRIDE.pdf (дата звернення: 30.06.2024).
16. Treasury Sanctions Russian Government Research Institution Connected to the Triton Malware. *U.S. Department of the treasury.* October 23, 2020. URL: https://home.treasury.gov/news/press-releases/sm1162 (дата звернення: 30.06.2024).

References

1. Dombrovska, S.M., Pomaza-Ponomarenko, A.L., Kryukov, O.I., & Poroka, S.G. (2024). *Informatsiyni zahrozy ta komunikatyvna infrastruktura v derzhavnomu sektori* [*Information threats and communication infrastructure in the public sector].* NUCZU, Kharkiv [in Ukrainian].
2. Pomaza-Ponomarenko, A.L., & Novikov, V.O. (2023). Ways of transformation of institutional mechanisms of public administration in Ukraine: from informational threats to hybrid wars. *Derzhavne budivnytstvo*, *1 (33).* Retrieved from https://periodicals.karazin.ua/db/article/view/22921 [in Ukrainian].
3. Pomaza-Ponomarenko, A.L., & Taraduda, D.V. (2024). Foreign experience of ensuring social security through the sustainable functioning of critical infrastructure objects and increased danger. *Nauka i tekhnika s'ohodni*, *4,* 371–384 [in Ukrainian].
4. Pomaza-Ponomarenko, A.L., & Taraduda, D.V. (2024). Ensuring the stability of the system of state regulation of increased danger facilities and critical infrastructure facilities. *Derzhavne upravlinnya: udoskonalennya ta rozvytok, 4*. Retrieved from https://www.nayka.com.ua/index.php/dy/article/view/3461 [in Ukrainian].
5. Pomaza-Ponomarenko, A.L., &Taraduda, D.V. (2024). Mechanisms for ensuring civil security of Ukraine: aspects of emergency prevention at the facilities of the military-industrial complex. *Publichne administruvannya ta natsional'na bezpeka, 3 (44)*. Retrieved from https://www.inter-nauka.com/issues/administration2024/3/9732 [in Ukrainian].
6. Dupuy, A.C., Nussbaum, D., Butrimas, V., & Granitsas, A. (2021). Energy Security in the Age of Hybrid Warfare. *www.nato.int.* Retrieved from https://www.nato.int/docu/review/ru/articles/2021/01/13/energeticheskaya-bezopasnost-v-epohu-gibridnoj-bor-by/index.html [in English].
7. Gogoreliani, A. (2021). Energy efficiency and renewable energy solutions in NATO and PfP countries' military operations. *www.enseccoe.org.* Retrieved from https://www.enseccoe.org/publications/energy-efficiency-and-renewable-energy-solutions-in-nato-and-pfp-countries-military-operations/ [in English].
8. Higgins, A. (2014). Russian Money Suspected Behind Fracking Protests. *The New York Times*. Retrieved from https://www.nytimes.com/2014/12/01/world/russian-money-suspected-behind-fracking-protests.html [in English].
9. The official site of NATO (2020). Energy Security n the Era of Hybrid Warfare. *www.sto.nato.int.* Retrieved from https://www.sto.nato.int/Lists/STONewsArchive/displaynewsitem.aspx?ID=524 [in English].
10. Alliance for Securing Democracy (2019). Illicit Influence – Part Two – The Energy Weapon. *securingdemocracy.gmfus.org.* Retrieved from https://securingdemocracy.gmfus.org/illicit-influence-part-two-energy-weapon/ [in English].

11. Lyngaas, S. (2020). German intelligence agencies warn of Russian hacking threats to critical infrastructure. *cyberscoop.com.* Retrieved from https://cyberscoop.com/german-intelligence-memo-berserk-bear-critical-infrastructure/ [in English].
12. The official site of NATO (2020). NATO 2030: United for a new era. Analysis and Recommendations of the Reflaction Group Appointed by the NATO Secretary General. *www.nato.int.* Retrieved from https://www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf [in English].
13. Pomaza-Ponomarenko, A., Taraduda, D., Leonenko, N., Poroka, S., & Sukhachov, M. (2024). Ensuring the safety of citizens in times of war: aspects of the organization of civil defense. *AD ALTA: Journal of Interdisciplinary Research*, *14, 1,* 216–220 [in English].
14. Slowik, J. (2019). CRASHOVERRIDE: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack. *www.dragos.com*. Retrieved from https://www.dragos.com/wp-content/uploads/CRASHOVERRIDE.pdf [in English].
15. The official site of U.S. Department of the treasury (2020). Treasury Sanctions Russian Government Research Institution Connected to the Triton Malware. *home.treasury.gov.* Retrieved from https://home.treasury.gov/news/press-releases/sm1162 [in English].

Подано до редакції 01.07.24 р.
Прийнято до друку 11.08.24 р.