ПУБЛІЧНЕ УПРАВЛІННЯ У СФЕРІ ДЕРЖАВНОЇ БЕЗПЕКИ ТА ОХОРОНИ ГРОМАДСЬКОГО ПОРЯДКУ

УДК 349.3:332.1:331.101:352.02
DOI https://doi.org/10.32782/TNU-2663-6468/2024.5/14

Горник В.Г.
Таврійський національний університет імені В.І. Вернадського

Євмєшкіна О.Л.
Таврійський національний університет імені В.І. Вернадського

Сімак С.В.
Таврійський національний університет імені В.І. Вернадського

ІНФОРМАЦІЙНА БЕЗПЕКА УКРАЇНИ: НОВІ ПІДХОДИ ДО ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ У ФОРМУВАННІ ЕНЕРГЕТИЧНОЇ БЕЗПЕКИ

Стаття присвячена розкриттю нових підходів інформаційної безпеки до захисту критичної інфраструктури у формуванні енергетичної безпеки України. Тема, яку було обрано для наукового дослідження, є актуальною, оскільки в межах інформаційної галузі виникло певне протистояння, яке можна розглядати як міждержавне суперництво, що розгортається у принципово новій сфері. У зв'язку з тим, що швидко розвиваються інформаційно-комунікаційні технології, формується глобальний інформаційний простір, з'явилися численні кібернетичні загрози, що пливають на політичне, економічне, соціальне, культурне життя соціуму. Беручи до уваги, що в проєктному середовищі відбуваються постійні прогресивні зміни, що триває воєнний стан, виходячи з наявності постійної невизначеності й нестабільності, можна констатувати, що збільшився ризик небезпечних ситуацій, у яких можуть опинитися території та громадяни, їхня життєдіяльність. Насамперед це проявляється в масованих обстрілах, які підступний ворог наносить по критичній інфраструктурі. Необхідно зауважити, що через російську повномасштабну агресію протягом останніх років на східних українських територіях відбулися значні пошкодження і втрати інфраструктурних об'єктів.

З'ясовано, що інформаційна безпека критичної інфраструктури у формуванні енергетичної безпеки України розглядається як сукупність систем, задіяних у державному управлінні, мета яких – забезпечити обороноздатність об'єктів, у разі збою в роботі яких буде втрачене управління та незворотно зруйнується інфраструктура, якою володіє державна економіка, суб'єкт чи адміністративно-територіальна одиниця країни, а громадяни України довго не почуватимуться в безпеці. Наведено головні завдання забезпечення інформаційної безпеки критичної інфраструктури у формуванні енергетичної безпеки. Виокремлено заходи, які необхідно реалізувати задля забезпечення інформаційної безпеки критичної інфраструктури у формуванні енергетичної безпеки, мета яких полягає в тому, щоб: розробити і вдосконалити головні положення, за допомогою яких відбувається ідентифікація кіберзлочинів, кібертероризму та інформаційних війн; створити взаємопов'язаний, систематизований набір, що містить моделі та сценарії, згідно з якими реалізуються комп'ютерні атаки на низку об'єктів, котрі характеризуються вразливістю з боку кіберзлочинної діяльності, та розробити й запровадити ефективні механізми, моделі та сценарії, завдяки комплексу яких можна буде боротися з подібними явищами.

Ключові слова: *інформаційна безпека, критична інфраструктура, енергетика, енергетична безпека, завдання.*

Постановка проблеми. Іноземними спецслужбами й терористичними та кримінальними структурами здійснюється інтенсивне вдосконалення методів та способів, за допомогою яких використовуються інформаційні технології та засоби для отримання можливості деструктивно інформаційно впливати на потенціал, котрим володіють інформаційно-телекомунікаційні системи, мережі організацій державного й недержавного статусу. Коли інформаційні технології та засоби використовуються саме так, вони стають так званою інформаційною зброєю. Аби державні та суспільні інтереси значно постраждали, інформаційна зброя може бути застосована і в умовах мирного часу, до чого вдаються представники терористичних організацій. Відтак безпека критичної інфраструктури має розглядатися під новим кутом: класичні заходи безпеки варто поєднувати із забезпеченням інформаційної безпеки, яка поширюється на автоматизовані управлінські системи в технологічному процесі.

Узагальнивши та систематизувавши світовий досвід в інформаційній безпеці критичної інфраструктури у формуванні енергетичної безпеки, можна зауважити, що протягом останніх років західними фахівцями особлива увага акцентувалася на тому, щоб оцінити вплив на діяльність життєво важливих об'єктів їхніх держав та його ймовірні наслідки для функціонування державних сфер політичного, економічного, екологічного тощо життя. Зрозуміло, що нині, коли інфраструктура, якою володіють провідні зарубіжні країни, переживає сучасний, дуже інтенсивний розвиток, виведені з ладу наявні численні критично важливі об'єкти, можуть обернутися непередбачуваними важкими й навіть катастрофічними наслідками.

Аналіз останніх досліджень і публікацій. Оскільки ця тематика є актуальною, їй присвятили цікаві дослідження такі автори, як Т. Бубела, А. Войціховський, С. Гончар, Є. Іванова, Г. Леоненко, В. Марков, М. Мельник, О. Назаровець, О. Нестерцова-Собокарь, Л. Рибальченко, Ю. Рудик, А. Русецький, М. Хаджийський, М. Шевченко, О. Юдін та інші. Детально проаналізувавши наукову розробленість проблеми щодо того, як забезпечити інформаційну безпеку критичної інфраструктури у формуванні енергетичної безпеки країни, у працях вітчизняних та зарубіжних науковців, приходимо до висновку, що проблему, яка полягає в тому, щоб формувати і своєчасно оновлювати концептуальні, доктринальні та нормативно-правові засади, на яких базується інформаційна безпека критичної інфраструктури у формуванні енергетичної безпеки країни, варто розглядати як найбільш гостру проблему сьогодення. Українськими та зарубіжними дослідниками осмислюється роль, яку відіграє інформаційна безпека критичної інфраструктури у формуванні енергетичної безпеки країни як системне утворення. Тобто, певні праці займаються дослідженням того, якими головними елементами володіє інформаційна безпека критичної інфраструктури у формуванні енергетичної безпеки країни, акцентуючи на їхній єдності, із застосуванням цілісного підходу: їхніх принципів, категорій, законів, ідей. Однак комплексні дослідження проблеми, що зосереджується на тому, як забезпечується інформаційна безпека критичної інфраструктури у формуванні енергетичної безпеки, є нині рідкістю, відтак неможливе формування панорами поглядів на управлінські проблеми в цій галузі. Водночас існування розбіжностей у користуванні поняттями й термінами, те, що вони не з'ясовані, не розмежовані стосовно обсягу і значення у текстах як наукових досліджень, так і міжнародно-правових актів, доводить, що процес, у ході якого мають бути осмислені ключові поняття, складові елементи системи, яка забезпечує інформаційну безпеку критичної інфраструктури у формуванні енергетичної безпеки, та їхніх багатогранних проявів і наслідків, ще залишається незавершеним.

Постановка завдання. Метою статті є розкриття нових підходів інформаційної безпеки до захисту критичної інфраструктури у формуванні енергетичної безпеки України.

Виклад основного матеріалу. Сучасні умови, в яких розвивається інформаційне суспільство, передбачають, що існування об'єктів критичної інфраструктури неможливе без користування інформаційною інфраструктурою: комп'ютерами й мережами, які представляють, насамперед, системи, що зайняті диспетчерським управлінням та збором інформації, завдяки взаємозалежності котрих відбувається інформаційний обмін, здійснення аналізу згідно зі всіма критично важливими функціями. Можливість управляти цими об'єктами завдяки механізму далекого доступу, що підвищує ефективність та скорочує витрати, призвела до відкриття критичної інфраструктури кіберзагрозам. На сучасній геополітичній арені відбулося перетворення кібератак, якіспрямовані на об'єкти критичної інфраструктури, вони стали «кібервійною», адже, володіючи ресурсом, що порушує критичну інфраструктуру держави, вимикаючи електростанції, руйнуючи нафтопроводи, навіть припиняючи подачу води й тепла комунальним підприємствам, можна оволодіти

значною військовою перевагою. Є безсумнівним, що якраз подібні ситуації значною мірою здатні заподіяти шкоду основам національної безпеки будь-якої світової держави.

У наш час інформаційна безпека є досить важливою складовою для усієї держави. Україні важливо забезпечити власний суверенітет в усіх сферах діяльності. На теперішній час, під час повномасштабного вторгнення інформаційна безпека набула особливого значення. Інформаційна безпека – це захист від дезінформації та кібератак, які зможуть порушити стійкість країни, стан захищеності інформаційного середовища суспільства, особи, організації. Інформаційна безпека країни в основному характеризується ступенем захищеності і стійкістю основних сфер життєдіяльності: науки, економіки, техносфери, військової сфери, сфери управління. Зараз особливо важливо зосередити увагу на функціонуванні системи забезпечення інформаційної безпеки України. Для громадян це не тільки зовнішньополітична інформація, а й усі сфери, до забезпечують повне функціонування держави [1].

Як відомо, первинна класифікація основних джерел загроз інформаційній безпеці передбачає їх поділ на зовнішні та внутрішні. Аналіз показує, що найбільш актуальними, у зв'язку з ситуацією, що склалася на міжнародній арені, є зовнішні передумови, а саме діяльність зарубіжних розвідувальних та інформаційних підрозділів, спрямована проти інтересів країни в інформаційній сфері через створення умов, що передбачають утиск інтересів України у світовому інформаційному просторі та розробка концепцій інформаційних війн. До внутрішніх джерел належать несприятливий стан галузей промисловості, тенденція об'єднання державних та кримінальних структур в інформаційній сфері, а також зниження ступеня захищеності конституційних інтересів громадян та суспільства загалом в інформаційній сфері. Вплив наведених загроз на критичну інформаційну інфраструктуру України може призвести до порушення їхнього функціонування та стати причиною настання тяжких наслідків для держави як в економічній, так і в політичній сферах [2].

В ці роки війни Україна як ніколи постраждала саме в сферах критичної інфраструктури, і держава, працюючи на останній засобах успішно вистояла випробування на темряву, відсутність зв'язку та інше. Однак, якщо дивитись на подібну ситуації через перспективу, то слід сказати про стан мереж зв'язку та інформаційно-телекомунікаційні системи, адже при черговому вимкненні світла людина втрачає можливість робити базову для нашого суспільства річ – дзвонити, може втратитися її конфіденційність інформації, захищеність та інше. За останні роки Україна зробила ряд важливих рішень щодо врегулювання інформаційної безпеки на нормативно-правовому рівні. Загальному мова йдеться про Стратегію інформаційної безпеки, основною метою якої є посилення забезпечення інформаційної безпеки держави, її простору, підтримка охорони і захисту державного суверенітету. Сучасною зброєю є не обов'язково вогнева потужність, а ефективність сучасної зброї все більше визначається ступенем інформаційної забезпеченості. На полі бою все більше використовують інформаційний фронт, тобто сьогодні це потужний засіб війни, оскільки її технічна інноваційність, спроможність наприклад залишити місто без світла чи тепла [3].

Зважаючи на аналіз наслідків військових дій на території України, стає очевидним, що противник, крім звичайної стратегічної мети досягнення перемоги на полі бою, також спрямовує свої дії на завдання значної шкоди інфраструктурі, яка забезпечує життєво важливі функції суспільства. Це має на меті не лише фізичне підкорення території, а й створення психологічного тиску на населення через руйнування та паралізацію систем, що забезпечують безпеку та комфорт життя. Такий підхід є типовим для військової стратегії, спрямованої на деморалізацію та знищення ворожих ресурсів. У контексті захисту національної безпеки, важливою стає організація ефективного захисту критичної інфраструктури. Це включає в себе всі сфери, які необхідні для нормального функціонування суспільства: енергетику, транспорт, комунікації, водопостачання та інші [4].

Останнім часом для багатьох країн світу стало актуальним питанням захисту об'єктів критичної інфраструктури. Під захистом об'єктів критичної інфраструктури розуміються заходи щодо забезпечення безпеки взаємозалежних систем, мереж і активів, що лежать в основі служб, життєво необхідних для функціонування суспільства. Об'єкти критичної інфраструктури можуть бути військовими і цивільними, а також мати подвійне призначення. Як приклади життєво важливими об'єктами матеріальної інфраструктури можна назвати дороги, мости, аеропорти, споруди зв'язку, електростанції, банківська сфера, виробництво і розподіл електроенергії, медичні послуги, державні аварійно-рятувальні служби, а також повітряні і наземні перевезення тощо [5].

Найбільшу загрозу безпеці об'єктів критичної інфраструктури становлять саме скоординовані атаки з використанням програмних вірусів. Такий

вид атаки поєднує підготовчий етап (дії, що створюють на об'єкті нові уразливі місця) та атакуючі дії (використання уразливих місць). Водночас, підготовчі дії можуть здійснюватися значно раніше, ніж сама атака, можуть бути задіяні працівники (інсайдери) підприємства, що є об'єктом нападу, та здійснені різноманітні відволікаючі маневри [6].

Основні завдання із забезпечення інформаційної безпеки критичної інфраструктури у формуванні енергетичної безпеки держави такі:

– нормативне, правове регулювання у сфері забезпечення безпеки інформації в критичній інфраструктурі держави;

– визначення загроз безпеки інформації та виявлення уразливостей у програмному та апаратному забезпеченні об'єктів критичної інфраструктури держави;

– оцінка реальної захищеності критичної інфраструктури держави;

– розроблення вимог щодо забезпечення безпеки інформації в критичній інфраструктурі держави;

– розроблення та реалізація заходів для убезпечення інформації в критичній інфраструктурі держави;

– підготовка фахівців із забезпечення безпеки інформації в критичній інфраструктурі держави;

– здійснення контролю і нагляду в галузі забезпечення безпеки інформації в критичній інфраструктурі держави;

– інформаційне, матеріально-технічне і науково-технічне забезпечення безпеки інформації в критичній інфраструктурі держави [7].

Як показує досвід розвинених країн, дослідження механізмів захисту інформації об'єктів критичної інфраструктури передбачає на перших кроках етап ідентифікації (визначення) елементів, які повинні розглядатися як об'єкти критичної інфраструктури. Разом з тим важливим напрямом забезпечення захисту інформації на об'єктах критичної інфраструктури є запровадження відповідного управлінського впливу, який передбачається здійснювати в декілька етапів, одним із головних мають стати моніторинг, спостереження та контроль [8].

Встановлюючи, за якими головними напрямами працює система, що забезпечує інформаційну безпеку критичної інфраструктури у формуванні енергетичної безпеки, можна зауважити, що передусім потрібно створити дієвий механізм, який координуватиме зусилля, докладені владними органами та підрозділами структур, що займаються забезпеченням інформаційної безпеки на відповідних об'єктах. Водночас необхідне впровадження суттєвих заходів державного, регіонального й галузевого рівнів, спрямованих на організаційне, нормативно-правове та науково-методичне забезпечення, зокрема потрібно:

– здійснювати загальне керівництво в царині, що забезпечує інформаційну безпеку критичної інфраструктури у формуванні енергетичної безпеки країни в цілому;

– на рівні законів регулювати відносини в галузі, що забезпечує інформаційну безпеку критичної інфраструктури у формуванні енергетичної безпеки країни;

– розробити Стратегію, завдяки якій буде гарантуватися інформаційна безпека державної критичної інфраструктури;

– розробити й реалізувати державні цільові програми, за допомогою яких забезпечується інформаційна безпека критичної інфраструктури у формуванні енергетичної безпеки;

– розробити й затвердити Державний реєстр об'єктів, які належать критичній інформаційній інфраструктурі;

– реалізувати загальнодержавні заходи, спрямовані на те, щоб об'єкти, які належать критичній інформаційній інфраструктурі, функціонували в сталому режимі;

– координувати й контролювати роботу, яку здійснюють органи державної влади, органи місцевого самоврядування, щоб об'єкти інформаційної безпеки, якими володіє критична інфраструктура, належно функціонували й були захищені;

– здійснювати державний контроль за тим, яким чином забезпечується інформаційна безпека критичної інфраструктури у формуванні енергетичної безпеки;

– здійснювати методичне керівництво, забезпечуючи критичній інформаційній інфраструктурі належне функціонування;

– здійснювати інформаційне, матеріально-технічне й науково-технічне забезпечення процесів, які відповідають за інформаційну безпеку об'єктів державної критичної інфраструктури.

Висновки. Отже, інформаційну безпеку критичної інфраструктури у формуванні енергетичної безпеки України розглядають як сукупність систем, задіяних у державному управлінні, мета яких – забезпечити обороноздатність об'єктів, у разі збою в роботі яких буде втрачене управління та незворотно зруйнується інфраструктура, якою володіє державна економіка, суб'єкт чи адміністративно-територіальна одиниця країни, а громадяни України довго не почуватимуться в безпеці. Щоб забезпечити інфор-

маційну безпеку критичної інфраструктури у формуванні енергетичної безпеки, необхідно цілеспрямовано вжити комплексні заходи, мета яких полягає в тому, щоб: розробити і вдосконалити головні положення, за допомогою яких відбувається ідентифікація кіберзлочинів, кібертероризму та інформаційних війн; створити взаємопов'язаний, систематизований набір, що містить моделі та сценарії, згідно з якими реалізуються комп'ютерні атаки на низку об'єктів, котрі характеризуються вразливістю з боку кіберзлочинної діяльності, та розробити й запровадити ефективні механізми, моделі та сценарії, завдяки комплексу яких можна буде боротися з подібними явищами; підготувати пропозиції, спрямовані на те, щоб реалізувати інформаційну безпеку допомагали механізми, вдосконалені на рівні законів, організації та операційних дій, та правові й нормативні документи, щоб ефективно протидіяти кіберзагрозам.

Список літератури:

1.Хаджийський М.О., Рибальченко Л. В. Інформаційна та економічна безпека під час військового стану. URL: https://dspace.lvduvs.edu.ua/bitstream/1234567890/6900/1/22_12_2023.pdf#page=162.

2.Нестерцова-Собокарь О. Забезпечення інформаційної безпеки критично важливих об'єктів інфраструктури України. URL: https://er.dduvs.edu.ua/bitstream/123456789/14215/1/144.pdf.

3.Іванова Є.І. Воєнно-інформаційна безпека України за умов ескалації конфлікту на сході України. URL: https://jarch.donnu.edu.ua/article/download/13389/13296.

4.Бубела Т.З., Мельник М.Я., Назаровець О.Б., Рудик Ю.І. Аналіз визначень та нормативних вимог системи захисту об'єкта критичної інфраструктури. *Вісник ЛДУБЖД.* 2024. Випуск 29. С. 119-127.

5.Войціховський А.В. Інформаційна безпека як складова системи національної безпеки (міжнародний і зарубіжний досвід). *Вісник Харківського національного університету імені ВН Каразіна.* 2020. № 29. С. 281-288.

6.Русецький А.А., Марков В.В. Аналіз стану загроз критичній інфраструктурі в Харківській області. *Актуальні проблеми вітчизняної юриспруденції.* 2017. № 1. С. 18-20.

7.Гончар С.Ф., Леоненко Г.П., Юдін О.Ю. Теоретико-методологічний аспект забезпечення інформаційної безпеки об'єктів критичної інфраструктури. *Вісник Національного університету Львівська політехніка. Комп'ютерні системи та мережі*. 2014. Випуск 806. С. 34-39.

8.Шевченко М.М. Методика системно-комплексного дослідження державного управління забезпеченням національної безпеки. *Вісник Національної академії оборони України.* 2010. № 4. С. 235-240.

Hornyk V.H., Simak S.V., Yevmieshkina O.L. INFORMATION SECURITY OF UKRAINE: NEW APPROACHES TO CRITICAL INFRASTRUCTURE PROTECTION IN THE FORMATION OF ENERGY SECURITY

The article is devoted to the disclosure of new approaches to information security to the protection of critical infrastructure in the formation of Ukraine's energy security. The relevance of the chosen topic of scientific research is due to the fact that the confrontation in the information sphere is becoming a fundamentally new area of rivalry between states. The rapid pace of development of information and communication technologies, the creation of a global information space has led to the emergence of many cyber threats in important areas of political, economic, social, and cultural life of society. Given the conditions of constant progressive changes in the project environment, taking into account the factors of martial law and constant uncertainty and instability, it becomes obvious that the risk of danger to the vital activity of territories and the population is increasing. First of all, this is reflected in the massive shelling of critical infrastructure facilities by the insidious enemy. It is worth noting that during the Russian full-scale aggression in eastern Ukraine, significant damage and losses have been caused to the infrastructure in recent years.

It was found that the information security of critical infrastructure in the formation of energy security of Ukraine is a set of state management systems aimed at ensuring the defense capability of objects, the disruption of which leads to the loss of control and irreversible destruction of the infrastructure of the country's economy, a subject or administrative-territorial unit of Ukraine, and a decrease in the security of the state's population for a long period. The main tasks of ensuring the information security of critical infrastructure in the formation of energy security are given. Measures that need to be implemented to ensure the information security of critical infrastructure in the formation of energy security are identified, which are aimed at: developing and improving the basic provisions identifying cybercrimes, cyberterrorism and information wars; creation of an interconnected, systematized set of models and scenarios for implementing computer attacks on objects potentially vulnerable to cybercrimes, as well as development and implementation of an effective set of mechanisms, models and scenarios for organizing counteraction to such phenomena.

Key words: *information security, critical infrastructure, energy, energy security, tasks.*