АКТУАЛЬНІ ПИТАННЯ ЕКОНОМІЧНИХ НАУК

Менеджмент

351:65.012.8:33

DOI https://doi.org/**10.5281/zenodo.15578447**

Інформаційна сталість об'єктів критичної інфраструктури регіонів: міжнародний досвід та українські реалії

Бабічев Анатолій Валерійович

кандидат наук з державного управління, доцент,

доцент кафедри управління та адміністрування,

Харківський національний університет імені В.Н. Каразіна,

Майдан Свободи, 4, Харків, 61022, Україна,

babichev@karazin.ua,

ORCID https://orcid.org/0000-0002-7587-4824

Прийнято: 19.05.2025 | Опубліковано: 29.05.2025

Анотація. *Складні реальні загрози, які впливають на сталість об'єктів критичної інфраструктури регіонів, потребують системного вивчення та осмислення, оцінки і адекватного реагування. Це дослідження зосереджено більшою мірою на вивченні міжнародного досвіду для посилення ефективності забезпечення інформаційної сталості об'єктів критичної інфраструктури регіонів через покращення системи управління, планування та реагування. Метою статті є розробка рекомендацій щодо подальшого розширення контуру можливостей адаптації практик забезпечення інформаційної сталості об'єктів критичної інфраструктури регіонів України з урахуванням міжнародного досвіду. Для обґрунтування отриманих результатів використані: міждисциплінарний підхід (при встановленні зав'язків у положеннях філософії, менеджменту, права, дотичних до завдань цього дослідження), порівняльний*

аналіз та синтез (для оцінки управлінських підходів щодо забезпечення інформаційної сталості об'єктів критичної інфраструктури в провідних країнах світу), компаративний метод (для окреслення кращих міжнародних практик), метод аналогій (при розробці практичних рекомендацій), метод дедукції (при формулюванні висновків). В ході дослідження: 1) оцінені перспективи та обсяги інновацій для забезпечення інформаційної сталості об'єктів критичної інфраструктури регіонів у світі, 2) проаналізований міжнародний досвід в контексті можливостей адаптації в українську практику, 3) визначені цілі, реалізація яких забезпечує посилення ефективності системи інформаційної об'єктів критичної інфраструктури в галузево-регіональному контексті. Результатами дослідження є такі: 1) підтверджене поступове нарощення інвестицій кінцевими користувачами на забезпечення інформаційної сталості об'єктів критичної інфраструктури 2) систематизовані практики з міжнародного досвіду щодо теми дослідження в контексті можливостей адаптації в українську практику, 3) запропоновані рекомендації щодо підвищення ефективності системи інформаційної сталості об'єктів критичної інфраструктури в галузево-регіональному контексті з урахуванням міжнародного досвіду.

Ключові слова: *критична інфраструктура регіонів, інформаційна сталість, управлінські підходи, загрози інформаційній сталості, об'єкти критичної інфраструктури*

 ISSN 3041-2129

АКТУАЛЬНІ ПИТАННЯ ЕКОНОМІЧНИХ НАУК

Information sustainability of critical infrastructure facilities in regions: international experience and Ukrainian realities

Babichev Anatoliy
Candidate of Sciences in Public Administration, Associate Professor, Associate Professor of the Department of Management and Administration,
V. N. Karazin Kharkiv National University,
4 Svobody Square, Kharkiv, 61022, Ukraine,
babichev@karazin.ua,
ORCID. https://orcid.org/0000-0002-7587-4824

Abstract. *Complex real threats that affect the sustainability of critical infrastructure facilities in regions require systematic study and understanding, assessment and adequate response. This study focuses more on the study of international experience to enhance the effectiveness of ensuring information sustainability of critical infrastructure facilities in regions through improving the management, planning and response system. The purpose of the article is to develop recommendations for further expanding the scope of opportunities for adapting practices for ensuring information sustainability of critical infrastructure facilities in regions of Ukraine, taking into account international experience. To substantiate the results obtained, the following methods were used: an interdisciplinary approach (when establishing links in the provisions of philosophy, management, law, relevant to the tasks of this study), comparative analysis and synthesis (for assessing management approaches to ensuring information sustainability of critical infrastructure facilities in leading countries of the world), a comparative method (for outlining the best international practices), the method of analogies (when developing practical recommendations), and the method of deduction (when formulating conclusions). During the study: 1) the prospects and scope of innovations for ensuring information sustainability of critical infrastructure facilities in regions around the world were*

assessed, 2) international experience was analyzed in the context of adaptation possibilities to Ukrainian practice, 3) goals were defined, the implementation of which ensures the strengthening of the effectiveness of the information system of critical infrastructure facilities in the sectoral and regional context. The results of the study are as follows: 1) confirmed gradual increase in investments by end users in ensuring information sustainability of critical infrastructure facilities 2) systematized practices from international experience on the topic of the study in the context of adaptation possibilities to Ukrainian practice, 3) recommendations were proposed for increasing the effectiveness of the information sustainability system of critical infrastructure facilities in the sectoral and regional context, taking into account international experience.

Keywords: *critical infrastructure of regions, information sustainability, management approaches, threats to information sustainability, critical infrastructure facilities*

Постановка проблеми. Тенденції в глобальному просторі вказують на зростання вірогідності гібридних загроз, як то поширення терористичних злочинів, руйнування інфраструктури внаслідок збройних конфліктів та стихійних лих, активізація кіберзлочинності у напрямку збільшення частоти та складності кібератак. Цифрова трансформація, як одна з глобальних тенденцій, сприяла зростанню обсягу і швидкості обміну інформацією і розширенню спектру способів її збору, обробки, презентації. При цьому кіберзагрози постійно еволюціонують, шкідливе програмне забезпечення створюється набагато швидше, ніж відповідні інструменти захисту, і розрив між ними постійно збільшується. Пошук шляхів забезпечення інформаційної сталості об'єктів критичної інфраструктури (ОКІ) регіонально-галузевого характеру є актуальною та далекою від остаточного вирішення, що обумовлено складністю таких об’єктів та різноманітністю самих загроз.

Аналіз останніх досліджень і публікацій. Регіонально-галузеві ОКІ часто мають обмежені ресурси для забезпечення надійного захисту, що вказує на їх вразливість до загроз. Тому розширення ландшафту методів забезпечення інформаційної сталості (ІС) об'єктів критичної інфраструктури регіонів є предметом досліджень науково-практичного характеру широко кола вітчизняних та зарубіжних фахівців. Зокрема, у фокусі наукових напрацювань Бобра Д. Г. – пошук шляхів щодо удосконалення підходів до оцінки рівня критичності об'єктів інфраструктури [1], системи захисту критичної інфраструктури для підвищення її стійкості в контексті загроз досліджують Верголяс О., Кондратов С., Гобулін В. та ін. [2, 3]. Домарацький М. Б., Бірюков Д. ґрунтовно досліджують методи державного та адміністративно-правового регулювання функціонування ОКІ України [4, 5]. Єрменчук О.П., Пальчик М.Л., Мартинюк В.В. та ін. проводять аналіз для пошуку вирішення проблемних аспектів правового забезпечення кібербезпеки критичної інфраструктури регіонів України [6, 7]. Тафазолли М. удосконалює механізми підтримки сталого розвитку ОКІ через безперервний збір даних, перевірку та вимірювання впливу на навколишнє середовище [8]. Т. Палеії досліджує вплив ОКІ на економічне зростання та глобальну конкурентоспроможність [9]. Проте проблемні питання щодо об'єктів критичної інфраструктури потребують подальшого дослідження з метою прийняття обґрунтованих оперативних і стратегічних рішень по забезпеченню безпеки та сталості їх функціонування в режимі реального часу, що підкреслює актуальність обраної тематики цієї статті.

Виділення невирішених раніше частин загальної проблеми. Проблематика забезпечення сталості та безпеки критичної інфраструктури регіонів зростає динамічними темпами, що обумовлено збільшенням загроз та їх ускладненням, вразливістю ОКІ. Тому, це дослідження спрямовано на подальше вивчення та адаптацію міжнародного досвіду до українських реалій щодо забезпечення інформаційної сталості об'єктів критичної інфраструктури у регіональному контексті.

Формулювання цілей статті (постановка завдання). Метою статті є розробка рекомендацій щодо подальшого розширення контуру можливостей адаптації практик забезпечення інформаційної сталості об'єктів критичної інфраструктури регіонів України з урахуванням міжнародного досвіду. Для досягнення поставленої мети було сформовано та вирішено такі завдання:

– оцінити перспективи та обсяги інновацій для забезпечення інформаційної сталості секторів економіки у світовому масштабі,

– проаналізувати міжнародний досвід забезпечення інформаційної сталості об'єктів критичної інфраструктури в контексті можливостей адаптації в українську практику,

– запропонувати рекомендації щодо підвищення ефективності системи інформаційної сталості об'єктів критичної інфраструктури в галузево-регіональному контексті.

Методологічна основа дослідження: міждисциплінарний підхід, що охоплює положення філософії, менеджменту, права, дотичних до завдань цього дослідження. Порівняльний аналіз та синтез використані при оцінці підходів до забезпечення інформаційної сталості ОКІ в провідних країнах світу. Для аналізу міжнародного досвіду застосовано компаративний метод. Метод аналогій використаний при розробці практичних рекомендацій. Для формулювання висновків використаний метод дедукції.

Виклад основного матеріалу дослідження. Критична інфраструктура формує основу функціональності та стійкості регіонів держави. В умовах інтенсифікації розвитку інфраструктури збільшується перелік її критичних об'єктів, виведення з ладу яких здатне призвести до надзвичайних ситуацій, пов'язаних з екологічною катастрофою, заподіянням значних матеріальних та економічних збитків. Більшість таких об'єктів так чи інакше залежать від комп'ютерних мереж, їх систем управління, а також цифрових технологій. І це обумовлює їхню вразливість до кіберзагроз та важливість забезпечення їх інформаційної сталості (ІС). Така ситуація є характерною для ОКІ більшості

країн світу. Звернемось до аналітики. Протягом останніх десятиліть серйозні інциденти, що впливають на критично важливу інфраструктуру, мали значний негативний вплив на багато секторів промисловості у всьому світі. За прогнозами експертів, для 2025 р. буде характерним різке збільшення ресурсів для забезпечення інформаційної сталості (табл. 1).

Таблиця 1.

Витрати кінцевих користувачів на інформаційну безпеку за сегментами, у всьому світі, 2023–2025 (млн. дол. США)

Сегмент оцінки	2023 рік		2024 рік		2025 рік (прогноз)	
	Витрати	Темп приросту, %	Витрати	Темп приросту, %	Витрати	Темп приросту, %
Програмне забезпечення безпеки	76574	13,6	87481	14,2	100692	15,1
Служби безпеки	65556	13,6	74478	13,6	86073	15,6
Безпека мережі	19985	6,2	21912	9,6	24787	13,1
Всього	162115	12,7	183872	13,4	211552	15,1

Джерело: [10]

Згідно прогнозам компанії Gartner, витрати кінцевих користувачів на забезпечення інформаційної сталості у світі становитимуть 212 млрд. $. у 2025 р., що на 15,1 % більше, ніж у 2024 р., коли витрати становили 183,9 млрд. $. «Посилення загроз, що продовжується, розвиток хмарних технологій і брак кадрів змушують керівників служб інформаційної безпеки (CISO) підвищувати витрати на забезпечення безпеки та сталості», – доводить Shailendra Upadhyay, старший директор із досліджень компанії Gartner [8]. За цим прогнозом, для здійснення масштабних атак соціальної інженерії 17% від загальної кількості кібератак/витоків даних будуть пов'язані з генеративним ШІ. В таких умовах, є об’єктивна ймовірність порушення інформаційної сталості об’єктів критичної інфраструктури, що змушує розглядати стійкість ОКІ в умовах впливу на них загроз інформаційній безпеці. На рівні вітчизняної практики рівень захищеності

ОКІ в регіонах є недостатнім, що обумовлено: 1) відсутністю системного фінансування заходів ІБ на місцях, недостатністю системного моніторингу інцидентів; 3) нестачею кваліфікованих кадрів у сфері кібербезпеки на рівні регіонів; 4) слабкою координацією між державними та приватними структурами, 5) залежністю від централізованих рішень та ін. Низька автономність регіонів у питаннях модернізації чи захисту інфраструктури є причиною того, що рішення часто спускаються зверху, без урахування локальної специфіки регіону.

Захист цілісності та конфіденційності ОКІ для забезпечення соціального, економічного розвитку регіонів може бути посилений завдяки міжнародного досвіду (рис. 1).

Аналіз міжнародного досвіду забезпечення ІС ОКІ доводить ефективність: 1) централізованого управління, 2) чіткого законодавчого регулювання, 3) публічно-приватної взаємодії. Ці три складові є взаємопов’язаними. Незалежно від суб’єкта управління ОКІ (державний чи приватний сектор, або їх поєднання) управління має здійснюватися під наглядом державних органів з зазначенням чітких розмежувань в обов'язках та зобов'язаннях між приватним сектором та державними органами та основі чіткого законодавчого регулювання. Забезпеченню інформаційної сталості ОКІ сприяють чіткі: вертикальні ролі та відповідальність, горизонтальні ролі та обов'язки.

 ISSN 3041-2129

Рис. 1. Аналіз міжнародного досвіду забезпечення ІС ОКІ для оцінки можливостей провадження в Україні на рівні регіонів

Джерело : складено автором на основі [10-13]

В міжнародній практиці державні органи функціонують як наглядові органи [10-13]. Їх функція - контроль загального напрямку забезпечення інформаційної сталості та розробка дій в надзвичайній ситуації під час кіберінцидентів. Підприємства, які є об'єктами критичної інфраструктури мають відповідальність за щоденну підтримку їх ІС. Тому, чіткість в розподілі ролей та відповідальності здатне підсилити довіру та забезпечити ефективне партнерство (рис. 2). Так, підвищенню ефективності співробітництва між державним та приватним сектором для підвищення інформаційної захищеності сприяють взаємна довіра, узгодженість механізмів взаємодії, використання гнучких, адаптивних підходів до управління. В той же час, взаємна довіра та прозорість забезпечують швидкість обміну інформацією між сторонами (державні та приватні структури) про ризики та загрози, що допомагає своєчасно реагувати на проблеми, що виникають.

За практикою, яка діє у США, обмін інформацією йде через систему CISA, це надає можливість приватним компаніям повідомити про можливі або поточні ризики в обмін на підтримку та/або координацію з боку державних органів. Протидія новим загрозам для ОКІ буде більш ефективна за умов забезпечення гнучкості та адаптивності. Кращими практиками в цьому контексті є стандарти безпеки, впровадження передових технологій захисту. Так, за Центр кібербезпеки (NCSC, Велика Британія) регулярно оновлює рекомендації та інформує про кращі практики щодо протидії новим видам загроз [15].

Ефективною міжнародною практикою є практика постійного розвитку компетенцій фахівців та співробітників у приватному та державному секторах через спільне навчання, тренінги, курси підвищення кваліфікації та симуляції кібератак. Це допомагає сформувати та підтримувати єдину культуру безпеки та підвищувати постійно професійний рівень кадрів. Участь України у міжнародних форумах, таких як Глобальний форум з кібербезпеки або Європейський форум з критичної інфраструктури, дозволяє обмінюватись досвідом та впроваджувати міжнародні стандарти у національну практику.

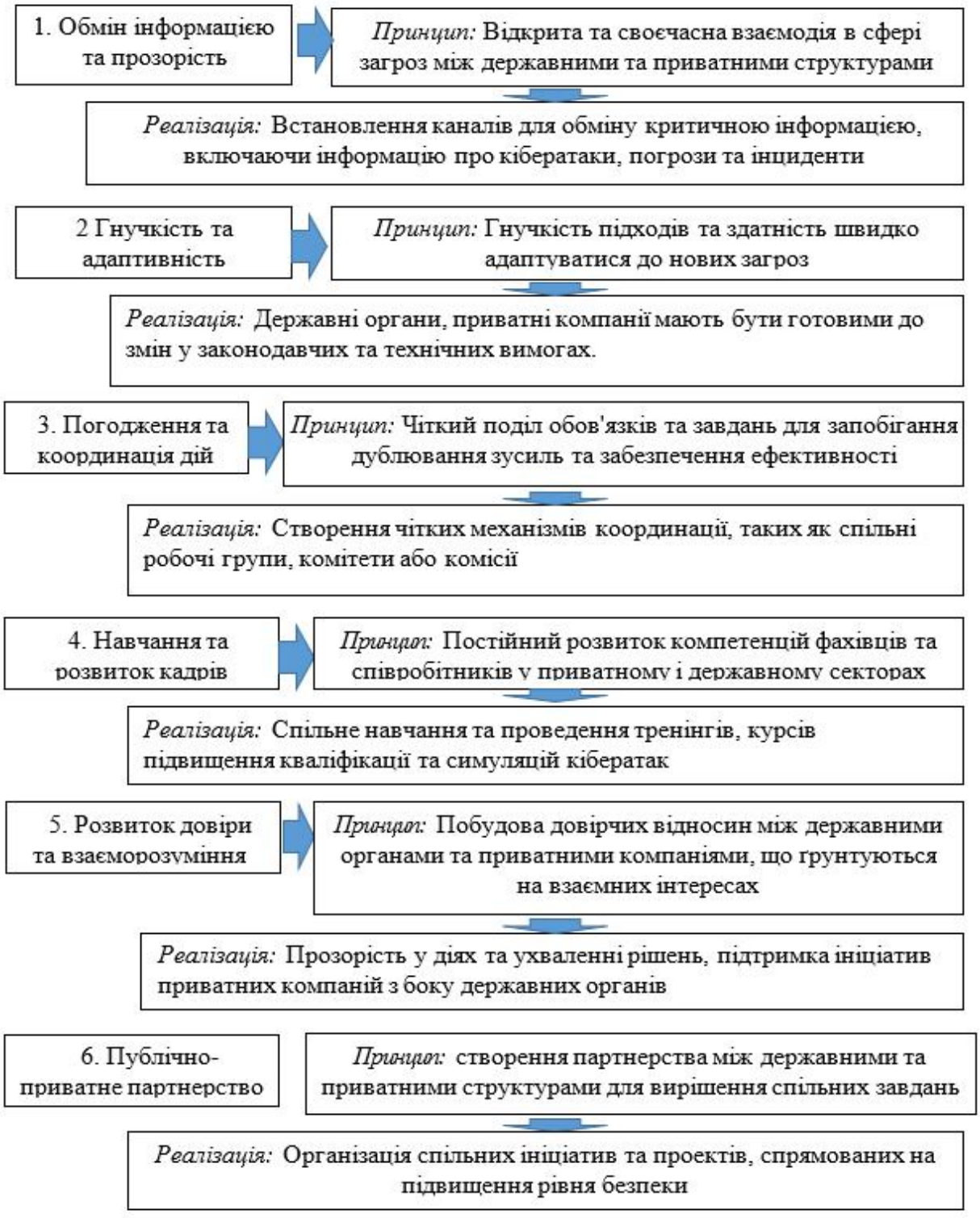

Рис. 2 Напрямки співпраці між державним та приватним сектором: аналіз міжнародного досвіду з метою імплементації на рівні регіонів України для підвищення ефективності управлінських дій щодо інформаційної сталості ОКІ

Джерело : складено автором на основі [12-14]

Спираючись на NIST США SP 800-3931 [16], ІС ОКІ є здатністю ОКІ до продовження функціонування в несприятливих умовах або під тиском, навіть якщо ОКІ перебуває у зруйнованому чи ослабленому стані, при збереженні основних експлуатаційних можливостей і відновлюватися до ефективного робочого стану терміни, що відповідають цільовим потребам. В такому ключі, ключовим поняттям стійкості функціонування ОКІ є прийняття можливості реалізації загрози ІБ як ймовірної події. Забезпечення стійкості ОКІ регіонів є циклічним процесом, який ґрунтується на постійному вдосконаленні систем запобігання, відновлення та адаптації інформаційним загрозам. Цьому активно сприяють ефективні практики співробітництва, спільні ініціативи та проекти, як то спільні платформи для обміну даними про кіберзагрози, розробка та участь у спільних програмах навчання та сертифікації. Так, у Європі та США існують ініціативи, де приватні компанії надають дані про інформаційні загрози в обмін на підтримку з боку державних органів у сфері захисту інфраструктури [13-15].

Міжнародні організації (НАТО, ЄС, ООН) активно підтримують Україну у зміцненні інформаційної захищеності на рівні країни та окремих регіонів, що має прояв у фінансуванні програм, навчанні кадрів, обміні досвідом щодо створення спеціалізованих центрів для обміну інформацією та реагування на інциденти. Ця співпраця допомагає Україні впроваджувати сучасні методи управління, а також сприяє створенню ефективніших механізмів координації між різними секторами на рівні регіонів. Проте є певні труднощі, які пов’язані, в тому числі, з тим, що: 1) деякі ОКІ регіонів покладаються на застарілі інформаційні технології, які вже не підгримуються, що збільшує загрозу їх вразливості кібератаками, оскільки забезпечення сталості може бути недоступною; 2) значна кількість ОКІ регіонів мають обмежені ресурси та бюджети для забезпечення інформаційної сталості. Впровадження системи моніторингу та реагування на кібератаки в Україні з використанням технологій, таких як ШІ та автоматизовані платформи стало можливим завдяки партнерству з приватними компаніями та міжнародними

організаціями, такими як Європейська мережа центрів реагування на інциденти (CSIRT).

Актуалізація питань забезпечення ІС ОКІ регіонів пов’язана також з тим, що високий рівень їх взаємопов'язаності та взаємозалежності здатний привезти до того, що «перебої» в одному секторі можуть мати каскадний наслідок для інших секторів регіону. Тому, доцільною для розгляду щодо впровадження є практика Великої Британії щодо регулярного аудиту та оцінки стану інформаційної захищеності у приватному та державному секторах. Це є елементом постійного моніторингу ризиків та загроз, що сприяє оперативному виявленню вразливостей та реагуванню на зміни у ситуації.

В контексті цього дослідження, результативним в контексті забезпечення ІС ОКІ розвиток нормативно-правової бази у сфері безпеки в Україні з урахуванням міжнародного досвіду. Україна за останні роки здійснила низку кроків у напрямі зміцнення інформаційної безпеки. Ретроспективний аналіз доводить про такі дії в правовому полі держави Україна:

– ухвалення Закону України «Про основні засади забезпечення кібербезпеки України» (2016 р.), який частково запозичив найкращі практики із законодавства ЄС (наприклад, з Директиви NIS2) та США. Ці міжнародні підходи регламентують взаємодію приватного та державного секторів, а також визначають стандарти захисту для критичної інфраструктури;

– прийняття Постанови КМУ «Деякі питання об’єктів критичної інфраструктури (2020 р.);

– ухвалення Стратегії кібербезпеки (2021 р.);

– ухвалення Закону України «Про критичну інфраструктуру (2021 р.),

– прийняття низки нормативно-правових актів, як-то «Про затвердження Методичних рекомендацій щодо категоризації ОКІ (2021 р.) та ін.

У 2022 р. Постановою КМУ (від 12.07.2022 № 787) визначено Уповноважений орган у сфері ЗКІ, яким є Державна служба захисту критичної інфраструктури та забезпечення національної системи стійкості України (ДЗКІ).

Аналіз міжнародної практики дозволив сформулювати низку пропозицій для забезпечення інформаційної сталості ОКІ регіонів.

1. Посилення інституційного забезпечення. Це є актуальним у двох аспектах: розробки та використання стандартів забезпечення ІС з урахуванням галузевого аспекту ОКІ, а також посилення результативності регіональних підрозділів з питань ОКІ в структурі регіональних адміністрацій для координації заходів безпеки.

2. Підготовка та реалізація навчальної практики для опрацювання сценаріїв реагування на загрози ІС, формування алгоритмів дій у разі кібератак на ОКІ, системні спільні навчання суб'єктів: органи влади, оператори критичної інфраструктури, правоохоронні органи.

3. Посилення публічно-приватного партнерства шляхом створення регіональної екосистеми, що передбачає залучення ІТ-компаній, фахівців, представники підрозділів з питань ОКІ та наукових установ на рівні регіону для реалізації спільних платформ для обміну даними про кіберзагрози або запуску спільних програм навчання та сертифікації.

Реалізація запропонованих заходів здатна посилити ефективність забезпечення ІБ ОКІ регіонів через покращення системи управління, планування та реагування, з опорою на місцеві ресурси та аналіз та оцінку міжнародних практик.

Висновки. Підтримка сталого розвитку ОКІ на рівні регіонів це безперервний процес протягом усього терміну служби об'єктів такого типу. Інфраструктури. Інформаційна захищеність є основоположною для економічної безпеки ОКІ регіонів в умовах геополітичної нестабільності, змін у світовому порядку, посилення частоти та збільшення типів кібератаки. Аналіз та оцінка діючої практики забезпечення ІС ОКІ в провідних країнах світу дозволив систематизувати основі напрямки, які можуть перспективу для імплементації у вітчизняну практику. У рамках цього дослідження 1) зосереджена увага на аналізі напрямків співпраці між державним та приватним сектором в контексті

забезпечення ІС ОКІ, 2) систематизовані труднощі, що є перешкодою в швидкому реагування на інциденти в рамках регіонів, 3) розглянуті практики удосконалення нормативно-правової бази у сфері безпеки на основі міжнародного досвіду. Реалізація запропонованих практичних заходів на основі вивчення та аналізу міжнародного досвіду здатна посилити інформаційну сталість ОКІ через покращення системи управління, планування та реагування, з опорою на ресурси регіонів.

Список використаних джерел

1. Бобро Д. Г. Методологія оцінки рівня критичності об'єктів інфраструктури. *Стратегічні пріоритети*. 2016. № 3 (40). С. 77–86. URL: http://www.niss.gov.ua/public/File/Str_prioritetu/SP_3_40_16.pdf.

2. Верголяс О. Реформування системи захисту та підвищення стійкості критичної інфраструктури України в розрізі актуальних загроз – Електронний ресурс. URL: https://coolyanews.info/reformuvannyasistemi-zahistu-ta-piidvischennyastiijkostii-kritichnoyi-iinfrastrukturi-ukrayinii-v-rozriiziiaktual.html

3. Developing The Critical Infrastructure Protection System in Ukraine : monograph / [S. Kondratov, D. Bobro, V. Horbulin et al.] ; general editor O. Sukhodolia. Kyiv : NISS, 2017. 184 p.

4. Домарацький М. Б. Специфіка державного регулювання критичної інфраструктури в Україні. *Публічне управління та митне адміністрування.* 2020. № 2(25). С. 24–46.

5. Бірюков Д. Концепція захисту критичної інфраструктури як елемент загальноєвропейської безпекової політики. *Наукові записки.* 2013. № 6 (68). С. 106−115. https://ipiend.gov.ua/wp-content/uploads/2018/07/birukov_kontseptsia.pdf

6. Єрменчук О.П., Пальчик М.Л. Проблемні аспекти правового регулювання державно-приватного партнерства у сфері захисту критичної інфраструктури. *Інформаційна безпека людини, суспільства, держави.* 2019. № 2 (26). С. 40-49.

7. Мартинюк В.В., Паламарчук Н.А., Паламарчук С.А., Сівоха О.М. Задачі вдосконалення інформаційної та кібернетичної безпеки об'єктів критичної інфраструктури. *Збірник наукових праць ВІТІ*. 2020. №2. С. 54-63. – URL: http://www.viti.edu.ua/files/zbk/2020/6_2_2020.pdf

8. Tafazzoli, Mohammadsoroush. Maintaining the Sustainability of Critical Infrastructure. 2019. DOI:10.5772/intechopen.85915

9. Palei T. Assessing the impact of infrastructure on economic growth and global competitiveness. *Procedia Economics and Finance*. 2015. Vol. 23. H. 168-175/

10. Gartner Forecasts Global Information, August 2024. URL: https://www.gartner.com/en/newsroom/press-releases/2024-08-28-gartner-forecasts-global-information-security-spending-to-grow-15-percent-in-2025

11. International Analytical Center IDC. URL: https://www.idc.com/events

12. European Programme for Critical Infrastructure Protection (EPCIP). URL: https://home-affairs.ec.europa.eu/e-library/glos%20sary/european-programme-critical_en

13. Council Directive 2008/114/E Cof 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. URL: https://eur-lex.europa.eu/legal-con tent/EN/TXT/?uri=uriserv%3AOJ.L_.2008.345.01.0075.01.ENG

14. Commission of the European Communities. Communication from the commission on a European Programme for Critical Infrastructure Protection. 100 Brussels, 12.12.2006. URL: https://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:EN:PDF

15. The National Cyber Security Centre. URL: https://www.ncsc.gov.uk/

16. NIST Special Publication 800-30 Revision 1 Спеціальна публікація Національного інституту Стандартів та Технологій США. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.