УДК 004.056.53:334.71-021.412.1](477) DOI: 10.31673/2412-4338.2025.048908

Гриців Ольга Петрівна
Національний Університет «Львівська Політехніка», Львів, Україна
ORDID ID: 0009-0009-1769-4823

Гарасимчук Олег Ігорович
Національний Університет «Львівська Політехніка», Львів, Україна
ORDID ID: 0000-0002-8742-8872

МЕХАНІЗМИ МІЖНАРОДНОЇ СПІВПРАЦІ У СФЕРІ КІБЕРЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В КОНТЕКСТІ МОЖЛИВОСТЕЙ ДЛЯ УКРАЇНИ

Анотація: *У сучасному світі, в умовах бурхливого розвитку технологій та масового використання онлайн-послуг як приватними особами, так і державними структурами, питання безпеки даних та конфіденційності користувачів набуває критичної актуальності. Зі зростанням обізнаності середньостатистичного громадянина та збільшенням частоти його присутності в цифровому просторі, паралельно зростає й кількість зловмисників та шахраїв, які активно шукають і використовують «прогалини» в захисті систем для отримання незаконної наживи. Саме тому всесвітніми організаціями на кшталт ООН і НАТО було створено різноманіття механізмів та ініціатив, орієнтованих на підтримку країн-партнерів цих організацій в сфері кіберзахисту. Метою цього дослідження є формулювання та подання низки конкретних, практичних рекомендацій, спрямованих на ефективне та стійке покращення ситуації в українському та світовому кіберпросторі. В даній роботі було проведено дослідження цих методів та висунуто низку рекомендацій щодо покращення цих методів для міжнародної співпраці у сфері кіберзахисту критичної інфраструктури, включаючи також можливості в цій співпраці для України. Показано, що комплексна модернізація системи захисту критичної інфраструктури та активна міжнародна співпраця зміцнюють цифровий суверенітет України та підвищують її роль як стратегічного партнера у сфері кібербезпеки. Акцентовано, що ефективне поєднання внутрішніх реформ та зовнішньої координації є визначальним чинником для забезпечення стійкої та адаптивної моделі кіберзахисту в умовах зростаючих глобальних загроз.*

Ключові слова: *Критична інфраструктура, міжнародна співпрацця, сфера кіберзахисту, кіберзахист інфраструктури, можливості для України, US-CERT, CCDCOE, Budapest Convention*

Olha Hrytsiv
Lviv Polytechnic National University, Lviv, Ukraine
ORDID ID: 0009-0009-1769-4823

Oleh Harasymchuk
Lviv Polytechnic National University, Lviv, Ukraine
ORDID ID: 0000-0002-8742-8872

MECHANISMS OF INTERNATIONAL COOPERATION IN THE FIELD OF CYBER PROTECTION OF CRITICAL INFRASTRUCTURE: OPPORTUNITIES FOR UKRAINE

In the modern world, in the conditions of rapid development of technologies and mass use of online services by both private individuals and government agencies, the issue of data security and user privacy is becoming critically important. With the growing awareness of the average citizen and the increasing frequency of his presence in the digital space, the number of attackers and fraudsters who actively seek and use "gaps" in the protection of systems to obtain illegal profits is also growing. That is why global organizations such as the UN and NATO have created a variety of mechanisms and initiatives aimed at supporting partner countries of these organizations in the field of cyber defense. The purpose of this study is to formulate and present a number of specific, practical recommendations aimed at effective and sustainable improvement of the situation in Ukrainian and global cyberspace. This paper examines these methods and makes a number of recommendations for improving these methods for international cooperation in the field of cyber protection of critical infrastructure, including the opportunities for Ukraine in this cooperation. It is shown that the comprehensive modernization of the critical infrastructure protection system and active international cooperation strengthen Ukraine's digital sovereignty and enhance its role as a strategic partner in the field of cybersecurity. It is emphasized that an effective combination of internal reforms and external coordination is a determining factor for ensuring a sustainable and adaptive model of cyber protection in the face of growing global threats.

Keywords: *critical infrastructure, international cooperation, cybersecurity sphere, infrastructure cyber protection, opportunities for Ukraine, US-CERT, CCDCOE, Budapest Convention*

Вступ

На даний час, станом на 2025 рік, в умовах воєнного стану в Україні спостерігається значний зріст кількості кіберзлочинів. Варто зазначити, що основною мішенню цих безперервних кібернападів, які становлять серйозну загрозу національній безпеці та економічній стабільності держави, стали банківські системи, системи управління державними сервісами, критична інфраструктура. Стрімке зростання кількості зафіксованих атак легко можна побачити, порівнюючи статистику з відкритих джерел (CERT Coordination Center (US-CERT), McAfee [1]) з започаткування відстеження кібератак 2010 року та з ситуацією зараз, в 2025 році [2-6].

Поява перших масованих кібератак такого типу впродовж минулого десятиліття стала тривожним дзвінком та суттєво сколихнула усю міжнародну спільноту фахівців з інформаційних технологій та кібербезпеки. Ці непоодинокі випадки спричинили активізацію наукових досліджень та інженерних розробок, що, в свою чергу, призвело до формування, появи та неухильного вдосконалення новітніх сервісів, протоколів та механізмів кіберзахисту.

Еволюція та зростання різноманітності методів, які використовувалися зловмисниками для здійснення нападів, прямо корелювали з поступовим, але динамічним розвитком сфери кібербезпеки, а безперервна гонка між атакою та захистом рішуче підкреслила її стратегічне значення в умовах глобального цифрового простору та сучасного високотехнологічного суспільства. З плином років, паралельно з розвитком кібератак, зросли й вимоги до організацій щодо захисту інфраструктури, що спричинило дослідження та розробку нормативних актів, директив, експертних груп, союзів захисту, центрів реагування та міжнародних організацій.

Однією з основних причин нерівномірного розвитку глобальної системи кіберзахисту є різниця у технологічній оснащеності, кадровому забезпеченні та зрілості механізмів у різних країнах, а серйозним каталізатором проблеми є напруга й недовіра у міжнародних відносинах, що ускладнює формування коаліцій та обмін критично важливою інформацією. Також помітною є розбіжність у підходах до визначення кібератаки та механізмів реагування на неї, зумовлена відмінностями у національних законодавствах держав.

На підставі всіх викладених вище фактів, включаючи різке зростання кіберзлочинів в сучасному цифровому просторі в умовах воєнного стану в Україні та фундаментальну проблему відсутності єдиного міжнародного правового режиму захисту, актуальним є ґрунтовний та всебічний аналіз наявних методів та механізмів кіберзахисту.

Метою роботи є формулювання та подання низки конкретних, практичних рекомендацій, спрямованих на ефективне та стійке покращення ситуації в українському та світовому кіберпросторі.

Динаміка (статистика) частот кібератак в Україні станом на 2011 та 2025 роки

Кіберзлочинність є однією з ключових проблем сучасної правоохоронної сфери, а занепокоєння розвинутих держав спричинене широким поширенням таких правопорушень. У світі, де цифрові технології стали невід'ємною частиною життя людей та організацій, зростає кількість кібератак, онлайн-шахрайств та викрадень персональних даних, що створює серйозні ризики для державної безпеки, економіки та приватних осіб і ускладнює їх запобігання. Тому ефективна протидія кіберзлочинності потребує вдосконалення правових механізмів, розвитку технічних засобів та підвищення кваліфікації фахівців.

У період з 2011 по 2025 рік в Україні спостерігалося поступове зростання кількості та складності кібератак, а також розвиток національної системи кіберзахисту.[6]:

– У 2011-2013 роках кількість інцидентів залишалася на відносно низькому рівні, але поступово з'являлися складніші типи атак, зокрема на державні ресурси та стратегічні об'єкти.

– В 2014 році під час дочасних Президентських виборів та подій Революції Гідності відбулися масштабні кібератаки на державні системи, які успішно нейтралізувалися командою CERT-UA, що було одним із перших підтверджень існування системного реагування на кіберзагрози в країні.

– З 2015 по 2019 роки активізувались атаки на урядові сайти, енергетичний сектор, фінансові установи, а також на підприємства критичної інфраструктури, що відбивало зростаючу зацікавленість у дестабілізації критичних систем.

– У 2020-2021 роках значна увага була зосереджена на захисті від фішингових атак, шкідливого ПЗ, кібершпигунства та кібершаботажу, а також впровадженні нових технологій та процедур у системі CERT-UA, що підсилювало здатність протидіяти комплексним загрозам.

– Особливо інтенсивними стали кібернапади у 2022 році, коли лише за січень було зафіксовано понад 120 кібератак на понад 70 державних сайтів, включно з атаками на "Дії", Кабмін, МВС, МОЗ та інші ключові відомства. Загалом у 2022 році CERT-UA обробила понад 2100 кіберінцидентів, з яких близько 1500 сталися після початку повномасштабного вторгнення росії.

У 2023 році було зафіксовано понад 2500 кіберінцидентів, що означає подальше зростання порівняно з 2022 роком; основними цілями стали держоргани, сектор безпеки й оборони, енергетика.

Впродовж 2024 року кількість кібератак зросла приблизно до 4300 інцидентів, причому основними цілями стали критична інфраструктура та державні реєстри, а вже у 2025 році в середньому фіксується близько 15 кіберінцидентів на добу та понад 150 активних кластерів загроз, що свідчить про перехід CERT-UA до режиму безперервної, інтегрованої з міжнародними партнерами кібероборони.

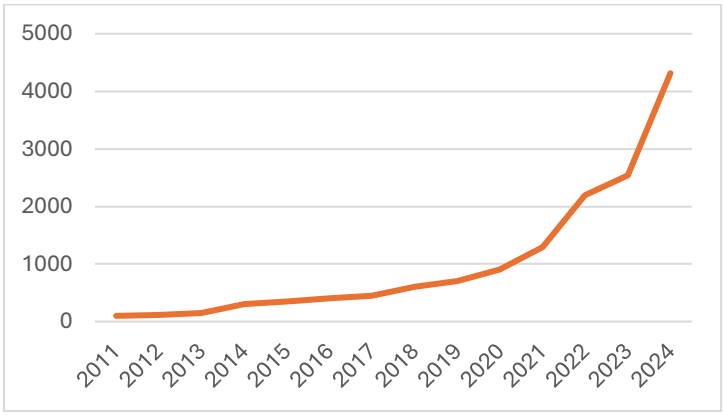

Рисунок 1. Графік частот кібератак в Україні станом на 2011 та 2025 роки

Різноманіття механізмів міжнародної співпраці та створені ініціативи

Оскільки кіберзлочинці не зважають на державні кордони, а атаки часто спрямовані на конкретні об’єкти, різні організації ініціювали власні заходи протидії. Так було створено NATO CCDCOE [10], яке забезпечує підтримку та захист держав-партнерів і об’єднує як членів НАТО, так і країни поза Альянсом.

Нижче в таблиці 1 наведено приклади ключових механізмів та ініціатив у сфері кібербезпеки, які спрямовані на посилення співпраці між державами, обмін досвідом та координацію дій у протидії загрозам:

Таблиця 1.

Міжнародно-правові механізми координації

Назва механізму	Опис механізму
Будапештська конвенція про кіберзлочинність (2001 р.) [8]	Перший міжнародний договір, що встановив стандарти криміналізації кіберзлочинів і механізми співпраці держав у розслідуванні та переслідуванні кіберзлочинців. Україна приєдналася до неї у 2006 році.
Директива NIS (Network and Information Security Directive, 2016; оновлена NIS2 у 2023 р.) [11]	Нормативна основа ЄС, що вимагає від держав-членів створення національних стратегій кібербезпеки, визначення операторів критичної інфраструкутури (КІ) та впровадження механізмів звітування про інциденти
Механізми НАТО [13]	Через програму Cyber Defence Pledge [15] та створення Центру передового досвіду з кібероборони у Таллінні, Альянс формує єдині стандарти реагування на кіберзагрози для військової та цивільної критичної інфраструктури.
Програми ООН та ОБСЄ [14]	Спрямовані на розвиток довіри між державами, обмін інформацією та формування глобальної культури кібербезпеки.

Європейська модель кіберзахисту критичної інфраструктури

Європейська модель кіберзахисту критичної інфраструктури базується на комплексному поєднанні правових, інституційних, технічних та координаційних механізмів. Її головна мета — забезпечити спільний цифровий простір довіри та підвищити стійкість ключових секторів до кіберзагроз шляхом узгодженого реагування між державами ЄС.

Таблиця 2.

Ключові елементи європейської моделі

Назва механізму	Опис та основні функції
Директиви NIS та NIS2 [11]	Директива NIS (2016) заклала правову основу кіберзахисту операторів критичних послуг у ЄС. Вона зобов'язала країни створити національні стратегії кібербезпеки, компетентні органи, CSIRT-команди та системи обміну інформацією. Оновлена NIS2 (2023) суттєво розширила перелік секторів КІ, встановила єдину систему звітності про кіберінциденти і передбачила фінансову відповідальність операторів за невиконання вимог безпеки.
ENISA та мережева координація [10]	Європейське агентство з кібербезпеки (ENISA) координує політику ЄС щодо кіберзахисту КІ, здійснює навчання, підтримує роботу CSIRT Network і розробляє технічні стандарти. ENISA виконує роль «інформаційного хаба» між державами, бізнесом і секторальними операторами КІ.
Європейська програма EPCIP [12]	European Programme for Critical Infrastructure Protection (EPCIP) забезпечує механізм ідентифікації об'єктів КІ, оцінки ризиків і планування заходів безперервності діяльності. EPCIP інтегрується з NIS2, формуючи єдиний нормативний контур для захисту фізичних і цифрових елементів КІ.

Для кращого розуміння того, як ці механізми працюють на практиці та як вони структуровані на рівні ЄС, розглянемо ключові елементи європейської моделі, згруповані за їхнім функціональним призначенням (див. Табл. 2).

Ці ключові механізми європейської моделі формують цілісний стандарт кібербезпеки. Для України їхнє вивчення та імплементація є стратегічно важливими кроками у процесі євроінтеграції. Гармонізація національного законодавства з NIS2 та інтеграція в мережі ENISA забезпечують не лише підвищення стійкості критичної інфраструктури, але й повну сумісність української системи кіберзахисту з європейською. Це зміцнює позиції України як надійного партнера у спільному цифровому просторі та є необхідною передумовою для повноцінної участі в системі колективної кібероборони ЄС.

Оборонно-політичні та кооперaційні механізми

Оборонно-політичні та кооперaційні механізми відіграють ключову роль у формуванні стійкої міжнародної системи кіберзахисту, забезпечуючи узгодженість дій держав, збройних сил, міжнародних організацій та приватного сектору. У сучасному безпековому середовищі кіберпростір визнаний повноцінним операційним доменом нарівні з повітряним, морським, сухопутним і космічним, що кардинально змінює підходи до оборони та вимагає координації не лише технічних інструментів, а й політичних рішень та військових можливостей. Ці механізми стають критично важливими для створення спільних доктрин, інтеграції кіберрозвідки у систему стратегічного попередження та розробки регламентів колективного реагування на кібератаки, прирівняні до збройного нападу, перетворюючи кіберзахист із технологічного питання на фундаментальну складову міжнародної та національної безпеки.

НАТО та колективна кібероборона

НАТО розглядає кіберпростір як п'ятий операційний домен і розвиває комплекс заходів для колективного захисту. Для демонстрації колективної кібероборони НАТО, нижче представлено ключові механізми Альянсу, їхню суть та функціональне призначення:

Таблиця 3

Ключові механізми НАТО

Назва механізму	Опис та основні функції
Cyber Defence Pledge (2016) [15]	Зобов'язання союзників посилено зміцнювати національні системи кіберзахисту, особливо критичної інфраструктури, та інвестувати у відповідні можливості.
Центр передового досвіду з кібероборони в Таллінні (CCDCOE) [13]	Платформа для досліджень, інновацій та навчань, включаючи організацію найбільших у світі багатонаціональних навчань із кібероборони (*Locked Shields*).
Cyber Rapid Reaction Teams (CRRTs) [16]	Мобільні, висококваліфіковані групи швидкого реагування, які можуть бути розгорнуті на запит союзника для надання допомоги у протидії масштабним та складним кібератакам.

Україна активно залучається до програм НАТО, використовуючи отриманий досвід для зміцнення потенціалу CERT-UA та участі в багатонаціональних навчаннях. Така співпраця прискорює сумісність українських оборонних структур із силами Альянсу та формує Україну як стратегічного партнера, здатного посилювати колективну кібероборону євроатлантичного простору.

ОБСЄ, ITU та регіональні ініціативи

ОБСЄ відіграє важливу роль у запобіганні конфліктам у кіберпросторі, запровадивши добровільні заходи довіри для попередження інцидентів між державами. Це доповнюється діяльністю інших міжнародних організацій і регіональних платформ, що спрямовані на розбудову потенціалу та обмін досвідом. Нижче представлено сутність і завдання цих ініціатив на глобальному та регіональному рівнях:

Таблиця 4

Міжнародні та регіональні ініціативи

Назва механізму	Опис та основні функції
Міжнародний союз електрозв'язку (ITU)	Реалізує Global Cybersecurity Agenda, спрямовану на підтримку національних CERT-центрів.
Meridian Process	Здійснює обмін найкращими практиками між державними органами, відповідальними за захист КІ.

Як видно з таблиці, діяльність ОБСЄ, ITU та Meridian Process підкреслює необхідність багатостороннього підходу, що включає три рівні: політичну довіру, розбудову національного потенціалу, та обмін найкращими практиками у сфері захисту КІ. Ці ініціативи формують інституційну основу для глобальної координації та є важливими для України як для посилення міжнародної легітимності своїх дій, так і для систематичної інтеграції у світову систему обміну знаннями.

Технічні та інформаційні механізми координації

Критично важливу роль у колективній обороні відіграють технічні та інформаційні механізми, які забезпечують оперативний обмін даними та спільні тренування. Вони дозволяють негайно перетворювати політичні рішення на практичні дії у сфері реагування на інциденти. Суть цих механізмів наведена в таблиці 5.

Ці механізми є технологічним фундаментом колективного аналізу та реагування. Вони забезпечують не просто обмін інформацією, а оперативну інтероперабельність між різними національними та міжнародними структурами. Саме завдяки MISP та мережам, як FIRST і EU-CSIRT, досягається швидке виявлення атак, спільний аналіз шкідливих кампаній і координована реакція на загрози, перетворюючи абстрактне поняття "колективної оборони" на дієву, технічно реалізовану систему.

Таблиця 5

Інструменти технічної та інформаційної координації

Назва Технічного Механізму / Мережі	Опис та основні функції
FIRST (Forum of Incident Response and Security Teams) [17]	Глобальна мережа для оперативного обміну даними та координації дій між командами реагування на кіберінциденти.
MISP (Malware Information Sharing Platform) [18]	Спеціалізована платформа для обміну технічними індикаторами компрометації та інформацією про шкідливі кампанії.
EU-CSIRT Network [19]	Структура, що забезпечує оперативне реагування та співпрацю між урядовими та секторальними командами реагування в межах Європейського Союзу.
Cyber Europe Exercises [20]	Спільні, широкомасштабні тренування для перевірки готовності операторів КІ та урядових агентств до реагування на комплексні кіберкризи.

Оцінка ефективності та виклики міжнародної співпраці

Зосередимо наш подальший аналіз на ключових міжнародних ініціативах і правових інструментах, що визначають рамки співпраці у сфері кібербезпеки:

1. Будапештська конвенція про кіберзлочинність (2001 р.).

Ефективність:

– Створила перші міжнародні стандарти криміналізації кіберзлочинів.

– Сприяє обміну доказами, взаємній правовій допомозі й гармонізації національних законів.

– Дозволяє країнам-партнерам, зокрема Україні, координувати слідчі дії через мережу 24/7 contact points.

Виклики / недоліки:

– Не всі держави світу є учасниками (Китай, росія, багато країн Азії та Африки), що обмежує глобальність дії конвенції.

– Різні правові системи створюють бар'єри для швидкого обміну інформацією.

– Відсутність єдиного механізму примусу до співпраці – держави діють добровільно.

– Питання захисту персональних даних може створювати конфлікт між державами-партнерами при обміні цифровими доказами.

2. Директиви NIS (2016) та NIS2 (2023).

Ефективність:

– Встановили єдині стандарти кіберзахисту критичної інфраструктури в ЄС.

– Забезпечили чітку систему звітності про інциденти та відповідальність операторів.

– Посилюють взаємодію між приватним сектором і державними структурами.

Виклики / недоліки:

– Різний рівень цифрової зрілості держав-членів ускладнює гармонізацію стандартів.

– Невисока готовність малих операторів до дотримання вимог NIS2 через фінансові та кадрові обмеження.

– Механізми звітності створюють додаткове адміністративне навантаження.

– Країни-партнери ЄС (зокрема Україна) не завжди мають повний доступ до внутрішніх координаційних платформ через правовий статус «не члена».

3. Механізми НАТО.

Ефективність:

– Розроблені єдині стандарти кібероборони серед союзників.

– NATO CCDCOE у Таллінні став провідним центром практичних навчань і досліджень (зокрема, Locked Shields).

– Cyber Defence Pledge стимулює держави інвестувати у власні системи кіберзахисту.

– Механізм колективної оборони поширюється і на кіберпростір (ст. 5 Вашингтонського договору).

Виклики / недоліки:

– Різний рівень готовності держав-членів до спільних кібероперацій.

– Питання обміну розвідувальними даними часто обмежене національною безпекою.

– Партнери, що не є членами Альянсу (як Україна), залучені до навчань і програм, але не мають повного доступу до секретних аналітичних систем.

– Високий рівень залежності від США у питаннях технічних і кадрових ресурсів.

4. Програми ООН та ОБСЄ.

Ефективність:

– Підвищують рівень довіри між державами, формують культуру мирного використання кіберпростору.

– Сприяють діалогу між державами, що не мають прямих двосторонніх угод.

– Формують основу для глобальних правил поведінки у кіберсфері.

Виклики / недоліки:

– Добровільний характер зобов'язань – відсутність механізму примусу.

– Політичні розбіжності між державами (наприклад, різні тлумачення "кіберагресії").

– Низький рівень технічної підтримки з боку міжнародних органів для країн, що розвиваються.

– Повільність ухвалення рішень у межах консенсусних процедур ООН.

5. Технічні та інформаційні мережі (FIRST, MISP, EU-CSIRT).

Ефективність:

– Забезпечують швидкий обмін технічними індикаторами загроз (IoC, TTPs).

– Дозволяють спільно аналізувати кампанії атак і розробляти контрзаходи.

– Сприяють стандартизації форматів кіберінформації (STIX/TAXII).

Виклики / недоліки:

– Висока залежність від довіри між учасниками — не всі держави готові ділитися чутливою інформацією.

– Проблеми з уніфікацією форматів даних між національними CERT-командами.

– Обмежений доступ до деяких платформ для країн поза межами ЄС або НАТО.

Місце України в міжнародній системі кіберзахисту

Україна посилює свою роль у міжнародній системі кіберзахисту, здійснюючи системну інтеграцію у європейський та трансатлантичний простір кібербезпеки. Зокрема, країна активно залучена до ключових регіональних ініціатив, таких як EU4Digital [22], спрямованої на розвиток цифрової економіки в Європі, програма CyberEast [23], що підтримує посилення кібербезпеки в країнах Східного партнерства, а також діяльність Центру передового досвіду з кібероборони НАТО (NATO CCDCOE), який забезпечує підвищення спроможностей у сфері кіберзахисту. Одночасно Україна проводить комплексну адаптацію національного законодавства, аби відповідати вимогам оновленої Директиви ЄС NIS2 [10], яка встановлює нові стандарти кібербезпеки для критичних секторів економіки та державного управління, підвищуючи таким чином рівень захищеності національної інфраструктури.

Важливою складовою зовнішньої співпраці є тісна взаємодія з Європейською агенцією з кібербезпеки (ENISA) [10] та міжнародною організацією FIRST [17], що об'єднує команди реагування на комп'ютерні інциденти. Український національний центр реагування на кіберінциденти CERT-UA виступає ключовим партнером у цих форматах, що дозволяє оперативно обмінюватися інформацією про кіберзагрози, посилювати координацію дій та підвищувати стійкість до сучасних кібератак.

Кібератаки на українську енергетику, фінанси й урядові системи у 2015–2022 роках стали каталізатором посилення міжнародної взаємодії. Повномасштабна агресія проти України також супроводжується безпрецедентним зростанням кількості та складності кібератак, спрямованих на підрив роботи державних сервісів і критичної інфраструктури. Саме тому Україна фактично є полігоном для тестування міжнародних механізмів кіберстійкості, що робить її важливим партнером у глобальній системі кібербезпеки. Для України участь у цих механізмах є стратегічною умовою забезпечення стійкості національної критичної інфраструктури та інтеграції до єдиного європейського безпекового простору.

Розробка рекомендацій з покращення механізмів захисту критичної інфраструктури у національному та міжнародному контексті

Зміцнення системи кіберзахисту критичної інфраструктури потребує поєднання національних стратегічних дій із використанням міжнародних механізмів співпраці. Україна вже бере участь у низці європейських та трансатлантичних ініціатив, однак ефективність цих процесів залежить від глибини інтеграції у спільні системи реагування, стандарти безпеки та обмін інформацією в реальному часі. Нижче (табл. 6) наведено комплекс рекомендацій, які поєднують внутрішні реформи та міжнародну кооперацію. Як видно з таблиці, ефективна кібероборона базується на технологічній інтероперабельності.

Таблиця 6

Технічна модернізація та підвищення кіберстійкості.

Напрямок	Ключові Заходи та Стандарти
Архітектура та захист КІ	Впровадження Zero Trust (сегментація, MFA, централізоване управління ідентичностями). Захист промислових систем (OT/ICS)
Оперативний Моніторинг	Встановлення систем SIEM/XDR для цілодобового збору даних. CERT-UA має стати національним центром (*SOC Hub*), інтегрованим із мережами FIRST і MISP.
Оцінка Безпеки	Регулярне тестування на проникнення та аудит безпеки із залученням незалежних сертифікованих експертів (CREST, ISO 27001, OSCP).
Міжнародна Сумісність	Узгодження технічних вимог із рекомендаціями ENISA та стандартами ISO/IEC 27001.

Впровадження архітектури Zero Trust і захист OT/ICS створюють необхідну фізичну та цифрову стійкість критичної інфраструктури. Паралельно, інтеграція CERT-UA з FIRST і MISP гарантує оперативне реагування та спільний аналіз загроз, що є ключовим для переходу до проактивної моделі захисту.

Таблиця 7

Кадровий розвиток та підвищення компетенцій.

Напрямок	Заходи Розвитку та Механізми Контролю
Кадровий Потенціал	Національна програма підготовки фахівців КІ у співпраці з ENISA, NATO CCDCOE та CyberEast. Включення міжнародних сертифікацій (CISSP, CEH, GIAC).
Навчання та Тренування	Підтримка університетських лабораторій (наприклад, через EU4Digital Academy). Регулярні спільні кіберсимуляції між CERT-UA, операторами КІ та партнерами НАТО/ЄС.
Регулярні спільні навчання та кіберсимуляції	Проведення регулярних спільних навчань і кіберсимуляцій за участі CERT-UA, операторів критичної інфраструктури, а також партнерів з НАТО та ЄС сприяє підвищенню координації дій, обміну досвідом і готовності до ефективного реагування на масштабні кіберінциденти.

Таблиця 8

Фінансування, аудит і контроль ефективності.

Напрямок	Заходи
Фінансова Стійкість	Створення Державного фонду кіберзахисту критичної інфраструктури. Фонд має акумулювати кошти держави, донорів ЄС, НАТО та приватних компаній, спрямовані на модернізацію обладнання (SIEM), навчання персоналу та сертифікацію продуктів.
Запровадження механізму кіберстрахування для операторів КІ.	Запровадження механізму кіберстрахування для операторів КІ. Страхові поліси мають виступати стимулом для обов'язкового дотримання міжнародних стандартів безпеки та підвищення відповідальності.
Якісний аудит	Регулярний аудит кіберзахисту операторів КІ. Оцінювання повинно проводитися за визнаними моделями, такими як NIST Cybersecurity Framework та ISO/IEC 27001..
Визначення ключових показників ефективності (KPI):	Чітке визначення та моніторинг KPI для оцінки результативності: середній час виявлення (MTTD) і реагування (MTTR); рівень виконання рекомендацій NIS2; кількість сертифікованих фахівців; кількість інцидентів, успішно локалізованих завдяки міжнародній координації.

Отже, стійкість системи визначається не лише технологіями, а й людським ресурсом і фінансовою прозорістю. Спільні кіберсимуляції з партнерами НАТО/ЄС та міжнародні освітні програми формують необхідну експертизу, а створення Державного фонду, кіберстрахування та аудит за KPI/NIS2 забезпечують стабільне фінансування й контроль відповідності стандартам.

Технічна модернізація, кадровий розвиток та фінансовий аудит (див. Табл. 8) є взаємопов'язаними стовпами, які формують цілісну та адаптивну систему кіберзахисту України. Комплексна реалізація усіх заходів, дозволить Україні не лише відповідати міжнародним стандартам, але й перейти до проактивної моделі оборони, зміцнивши свою роль як надійного та високостійкого учасника глобальної системи колективної кібербезпеки.

Реалізація цих стратегічних заходів дозволить укріпити позиції України у європейському кіберпросторі, посприяє глибинній інтеграції до європейських та трансатлантичних структур безпеки, а також забезпечить безперервність і стійкість функціонування національної критичної інфраструктури в умовах зростаючих кібератак та гібридних загроз.

Перспективи України у міжнародній системі співпраці:

В умовах зростання глобальних кіберзагроз Україна переходить від ролі споживача безпекових рішень до активного партнера міжнародної кіберспільноти, спираючись на свій досвід протидії масштабним гібридним атакам. Розвиток кібербезпеки відбувається у тісній інтеграції з європейськими та трансатлантичними структурами, що підсилює партнерство й визнає українську експертизу. Співпраця з FIRST, ENISA та CSIRT Network забезпечує оперативний обмін даними, участь у спільних розслідуваннях, впровадження вимог NIS2, а гармонізація нормативів створює основу для довіри та координації з ЄС.

Активна участь у стратегічних навчаннях та аналітичній роботі НАТО CCDCOE у Таллінні не є ізольованим процесом, а логічно продовжує розпочату співпрацю, дозволяючи налагоджувати комплексний обмін знаннями, опановувати сучасні методики реагування та впроваджувати нові стандарти у підготовці кадрів.

Підтримка ЄС через програми EU4Digital і CyberEast створює нові професійні можливості та інтегрує українські напрацювання в європейську систему кіберзахисту. Обмін інформацією, сертифікація продуктів, підвищення кваліфікації та співпраця між командами набувають практичного змісту й посилюють визнання України в європейському цифровому просторі.

Демонстрація спроможності протидіяти масштабним атакам на критичні сектори держави стає важливим аргументом для їхнього вивчення та впровадження у міжнародних стратегіях. Досвід кіберконфліктів – таких як NotPetya, Industroyer, WhisperGate, Sandworm – використовується західними аналітичними центрами для оновлення захисту інфраструктур, а українські фахівці стають лідерами у розробці інноваційних рішень із кібербезпеки.

Така багаторівнева кооперація та поєднання сучасних технологій із міжнародними практиками створюють сталу основу для формування нових стратегій і методологій. Це дозволяє державі не лише захищати власні інтереси, а й робити вагомий внесок у глобальну цифрову безпеку, встановлюючи нові стандарти реагування на кіберзагрози.

Інституційна інтеграція з ключовими європейськими структурами відкриває Україні доступ до обміну технічними індикаторами, спільних досліджень та фінансування ЄС: асоційоване членство в CSIRT Network ENISA та Європейському центрі кібербезпеки поглиблює співпрацю й підвищує експертизу. Паралельна участь у програмах НАТО, зокрема Cyber Defence Pledge [15] і потенційне долучення до NATO Cyber Rapid Reaction Teams [16], забезпечує можливість участі в колективних операціях та доступ до аналітичних платформ Альянсу, що зміцнює кіберстійкість держави. Накопичений український досвід може стати основою для створення регіонального кіберцентру в Східній Європі з функціями моніторингу, реагування та моделювання гібридних загроз.

Ключові виклики та обмеження

Попри успіхи в інтеграції національної системи кібербезпеки з міжнародними структурами, існують об'єктивні виклики:

– Обмежений статус партнера НАТО не дає повного доступу до стратегічних даних та платформ Альянсу, ускладнюючи швидке реагування на загрози та участь у спільному стратегічному плануванні.

– Гармонізація законодавства з директивою NIS2 проходить нерівномірно через відсутність єдиного закону про захист критичної інфраструктури, що ускладнює управління ризиками та аудит [25].

– Недостатнє фінансування та обмежений кадровий потенціал стримують модернізацію ключових секторів, створення SOC та впровадження технологій SIEM і XDR, особливо в умовах воєнного стану та економічних обмежень.

Зростання кібероперацій з боку ворожих держав проти України та її союзників створює серйозну загрозу. Це потребує не лише технічного вдосконалення, а й посилення стратегічної співпраці для ефективних систем раннього попередження та обміну аналітикою в реальному часі. Відсутність єдиної архітектури обміну даними між цивільним і військовим сегментами та міжнародними партнерами ускладнює реагування на кіберінциденти. Необхідно впровадити інтегровані протоколи взаємодії за стандартами, як NATO Federated Mission Networking [26], для підвищення ефективності дій на національному рівні.

Перспективні напрями розвитку

Для забезпечення сталості та зміцнення міжнародного фронту боротьби з кіберзагрозами важливе поглиблення співпраці з ENISA. Підписані меморандуми передбачають обмін даними про нові атаки, спільні навчання, розробку рекомендацій щодо технічних стандартів та участь у програмах взаємної підтримки під час інцидентів. Це дозволяє українським командам інтегруватися в європейські та глобальні платформи обміну інформацією, знижуючи ризики масштабних атак.

Інтеграція сприяє економічному розвитку: участь у створенні єдиної європейської системи сертифікації кіберпродуктів за Cybersecurity Act [27] дає українським розробникам доступ до спрощених процедур оцінки відповідності, що підвищує конкурентоспроможність продукції на ринках ЄС. Паралельно інтеграція з політико-безпековими механізмами НАТО передбачає обмін інформацією з CCDCOE та аналітичними групами країн Альянсу, участь у спільних тренінгах, розробці регламентів реагування на масові атаки та формуванні доктрини колективної кібероборони.

Висновки

Ефективна протидія сучасним кіберзагрозам потребує інтеграції в глобальну систему колективної кібероборони. Через транскордонний характер атак необхідні узгодження політик, уніфікація стандартів та безперервний обмін інформацією між державами для підвищення стійкості цифрового простору. Для України міжнародна співпраця забезпечує доступ до передових технологій та експертного потенціалу для зміцнення кіберстійкості. Розвиток системи захисту критичної інфраструктури передбачає модернізацію: від гармонізації законодавства з NIS2 до впровадження архітектури Zero Trust та підготовки фахівців. Ці заходи забезпечують завчасне виявлення загроз, ефективне управління ризиками, зміцнення цифрового суверенітету та безперервність критично важливих систем, сприяючи інтеграції України в європейський та євроатлантичний безпековий простір і формуючи надійну, адаптивну систему кіберзахисту.

Список використаної літератури:

1. CERT-UA. Офіційний сайт Національного центру реагування на комп'ютерні інциденти України, [Online]. Available: https://cert.gov.ua.

2. CIP. Офіційна сторінка Державної служби спеціального зв'язку та захисту інформації України, [Online]. Available: https://cip.gov.ua.

3. Річний аналітичний огляд жовтень 2023- вересень 2024, [Online]. Available: https://www.rnbo.gov.ua/files/2024/NATIONAL_CYBER_SCC/20250109/Year%20in%20review_UKR_upd.pdf.

4. The Evolving Shadow War: A Decade of Global Cyber Attacks (2015–2025) and the Urgent Need for Resilience, [Online]. Available: https://ytcventures.com/2025/09/22/the-evolving-shadow-war-a-decade-of-global-cyber-attacks-2015-2025-and-the-urgent-need-for-resilience/.

5. MS.detector.media. Український ринок кібербезпеки за останні вісім років збільшився в чотири рази і продовжує зростати, — дослідження, [Online]. Available: https://ms.detector.media/kiberbezpeka/post/37152/2025-01-07-ukrainskyy-rynok-kiberbezpeky-za-ostanni-visim-rokiv-zbilshyvsya-v-chotyry-razy-i-prodovzhuie-zrostaty-doslidzhennya/.

6. Welt.de. Wie die Ukraine zum Testfeld für den Cyberwar wurde, [Online]. Available: https://www.welt.de/wirtschaft/webwelt/article206911377/Cyberwar-Wie-die-Ukraine-zum-Testfeld-fuer-den-digitalen-Krieg-wurde.html.

7. SCPC. Державний центр кіберзахисту України. Статистичні звіти, аналітичні матеріали, [Online]. Available: https://scpc.gov.ua.

8. Council of Europe. Budapest Convention on Cybercrime, [Online]. Available: https://www.coe.int/en/web/cybercrime.

9. The European Cyber Defence Policy, [Online]. Available: https://www.european-cyber-defence-policy.com/.

10. ENISA. European Union Agency for Cybersecurity. Офіційна аналітика, нормативи NIS/NIS2, CSIRT Network, [Online]. Available: https://www.enisa.europa.eu.

11. European Commission. New rules to boost cybersecurity of EU's critical entities and networks, [Online]. Available: https://ec.europa.eu/commission/presscorner/detail/en/ip_24_5342.

12. European Programme for Critical Infrastructure Protection, [Online]. Available: https://eur-lex.europa.eu/EN/legal-content/summary/european-programme-for-critical-infrastructure-protection.html.

13. CCDCOE. NATO Cooperative Cyber Defence Centre of Excellence. Навчання, практичні кейси, дослідження Locked Shields, [Online]. Available: https://ccdcoe.org.

14. The OSCE's Pioneering Work on Cyber Security, [Online]. Available: https://www.shrmonitor.org/osces-pioneering-work-cyber-security/.

15. NATO. Cyber Defence Pledge, [Online]. Available: https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2016/07/08/cyber-defence-pledge.

16. Cyber Rapid Response Teams and Mutual Assistance in Cyber Security (CRRTs), [Online]. Available: https://crrts.eu/.

17. FIRST. Forum of Incident Response and Security Teams. Глобальний обмін даними про кіберінциденти, best practices, [Online]. Available: https://first.org.

18. MISP Project. Malware Information Sharing Platform. Технічна платформа для обміну індикаторами компрометації, [Online]. Available: https://www.misp-project.org.

19. EU-CSIRT Network, [Online]. Available: https://csirtsnetwork.eu/.

20. ENISA. Cyber Europe, [Online]. Available: https://www.enisa.europa.eu/topics/skills-and-competences-for-companies/cyber-europe.

21. Council of Europe. Budapest Convention on Cybercrime. Міжнародний правовий механізм співпраці, [Online]. Available: https://www.coe.int/en/web/cybercrime.

22. EU4Digital Initiative. Програма ЄС підтримки цифрової трансформації та кібербезпеки у Східному партнерстві, [Online]. Available: https://eu4digital.eu.

23. CyberEast, [Online]. Available: https://www.coe.int/en/web/cybercrime/cybereast.

24. Forbes.ua, Delo.ua, MS.detector.media, Texty.org.ua, Dou.ua. Профільна аналітика, новини, коментарі експертів, [Online]. Available: https://forbes.ua, https://delo.ua, https://ms.detector.media, https://texty.org.ua, https://dou.ua.

25. Довгань О.Д. Правові аспекти забезпечення кібербезпеки об'єктів критичної інфраструктури // Інформаційне право. — 2024, [Online]. Available: https://il.ippi.org.ua.

26. NATO ACT. Federated Mission Networking, [Online]. Available: https://www.act.nato.int/activities/federated-mission-networking/.

27. European Commission. EU Cybersecurity Act, [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act.