УДК 343.326:004]:351.86:004.056(4-6ЄС)
DOI https://doi.org/10.32782/2663-6170/2024.39.15

ЄВРОПЕЙСЬКІ РЕГІОНАЛЬНІ ЗАСОБИ ПРОТИДІЇ КІБЕРТЕРОРИЗМУ

EUROPEAN REGIONAL MEANS OF COUNTERING CYBERTERRORISM

Зінченко О.І.,
аспірантка кафедри політології
Харківського національного університету імені В.Н. Каразіна

У роботі досліджуються європейські регіональні засоби протидії кібертероризму, зокрема правові, інституційні та операційні механізми, розроблені в межах Європейського Союзу для забезпечення кібербезпеки. Кібертероризм, як новітня форма тероризму, представляє серйозну загрозу не лише національній безпеці, а й стабільності міжнародних відносин. Використання технологій для здійснення терористичних актів та маніпулювання інформацією в глобальному просторі вимагає комплексного підходу до запобігання, виявлення та нейтралізації кіберзагроз.

Аналізуються основні правові акти та стратегії, що регулюють кібербезпеку в Європейському Союзі, зокрема Регламент (ЄС) 2019/881 (Cybersecurity Act), Директива (ЄС) 2022/2555 (NIS 2), а також рішення Ради ЄС щодо боротьби з кібертероризмом. Окрему увагу приділено діяльності Європейського агентства з кібербезпеки (ENISA) та механізмам міжнародної співпраці, зокрема в рамках Будапештської конвенції та з іншими регіональними організаціями, такими як НАТО та ООН.

Робота також розглядає співпрацю між державними та приватними структурами у сфері кібербезпеки, роль технологій (штучного інтелекту, великих даних, блокчейну) у боротьбі з кібертероризмом, а також виклики, що виникають внаслідок правових, технічних і політичних обмежень у цій сфері. Особливу увагу звернуто на потребу вдосконалення національних і міжнародних механізмів реагування на кіберзагрози, включаючи розвиток кадрового потенціалу та підвищення рівня обміну інформацією серед країн ЄС.

Завданням роботи є також визначення ключових проблем, що виникають у процесі реалізації європейських ініціатив у сфері кібербезпеки, та надання рекомендацій щодо покращення регіональних і глобальних засобів протидії кібертероризму, враховуючи постійно змінювані технологічні та геополітичні умови. Робота підкреслює важливість інтегрованих і скоординованих зусиль для забезпечення ефективної протидії кібертероризму в Європі.

Ключові слова: кібертероризм, Європейський Союз, кібербезпека, міжнародна співпраця, правове регулювання, публічно-приватне партнерство.

This paper examines European regional measures for countering cyberterrorism, focusing on the legal, institutional, and operational mechanisms developed within the European Union to ensure cybersecurity. Cyberterrorism, as a modern form of terrorism, represents a serious threat not only to national security but also to the stability of international relations. The use of technology for conducting terrorist acts and manipulating information in the global space requires a comprehensive approach to the prevention, detection, and neutralization of cyber threats.

The paper analyzes key legal acts and strategies regulating cybersecurity in the European Union, particularly Regulation (EU) 2019/881 (Cybersecurity Act), Directive (EU) 2022/2555 (NIS 2), and the EU Council's decisions on combating cyberterrorism. Special attention is given to the activities of the European Union Agency for Cybersecurity (ENISA) and mechanisms for international cooperation, notably under the Budapest Convention and with other regional organizations such as NATO and the UN.

The study also addresses the collaboration between public and private entities in cybersecurity, the role of technologies (artificial intelligence, big data, blockchain) in countering cyberterrorism, as well as the challenges arising from legal, technical, and political constraints in this area. Particular emphasis is placed on the need to improve national and international response mechanisms to cyber threats, including the development of human resources and enhanced information sharing among EU member states.

The objective of this paper is also to identify key issues arising in the implementation of European cybersecurity initiatives and provide recommendations for improving regional and global measures to counter cyberterrorism, considering constantly evolving technological and geopolitical conditions. The paper underscores the importance of integrated and coordinated efforts for effective counteraction to cyberterrorism in Europe.

Key words: cyberterrorism, European Union, cybersecurity, international cooperation, legal regulation, public-private partnership.

Постановка проблеми. У сучасному світі кібертероризм стає одним із ключових викликів міжнародній безпеці. Використання кіберпростору терористичними групами для здійснення атак на критичну інфраструктуру, крадіжки даних, маніпуляції громадською думкою та інші форми дестабілізації створює серйозні загрози для національної та міжнародної стабільності. Європейський Союз (ЄС), як один із провідних глобальних регіонів, зіткнувся з необхідністю розробки ефективних інструментів протидії цим загрозам.

Проблема посилюється стрімким розвитком технологій, які одночасно забезпечують нові можливості для захисту та розширюють потенціал для кібертерористичної діяльності. Нерівномірний рівень технологічного розвитку країн-членів ЄС, відмінності у правових системах та обмеженість ресурсів у деяких регіонах ускладнюють ство-

рення єдиної стратегії. Крім того, кіберзагрози є транскордонними за своєю природою, що вимагає тісної міжнародної співпраці, гармонізації законодавства та інтеграції зусиль держав, приватного сектору та громадянського суспільства.

Сучасна нормативно-правова база ЄС, яка включає Регламент (ЄС) 2019/881, Директиву (ЄС) 2022/2555 та Рамкове рішення 2002/475/ЈНА, створює основу для боротьби з кібертероризмом. Однак виникають виклики у їхній практичній реалізації через розбіжності у підходах країн-членів, недостатній рівень довіри між суб'єктами кіберзахисту та брак узгоджених механізмів реагування на надзвичайні ситуації.

Таким чином, актуальність дослідження європейських регіональних засобів протидії кібертероризму визначається необхідністю аналізу наявних підходів, виявлення їхніх сильних сторін і недоліків, а також розробки рекомендацій для підвищення ефективності боротьби з кібертерористичними загрозами як у межах ЄС, так і на глобальному рівні.

Аналіз останніх досліджень та публікацій. Аналіз останніх досліджень з протидії кібертероризму в ЄС показує різноманіття підходів: від нормативно-правових до технологічних і організаційних аспектів. Baker-Beall і Mott [1] аналізують сприйняття кібертероризму в ЄС, Christou [2] досліджує колективну безпеку кіберпростору, а Al Asyari [3] порівнює стратегії ЄС та АСЕАН. Oleksiewicz [4] оцінює ефективність правової політики ЄС у боротьбі з кібертероризмом. Trofymenko і Mishanchuk [5] аналізують філософські та правові аспекти кібертероризму. Однак, існують недосконалості в деталях взаємодії між країнами ЄС у контексті кібертероризму та недостатнє дослідження конкретних інструментів для моніторингу кібертерористичних загроз на регіональному рівні.

Метою роботи є дослідження європейських регіональних механізмів і заходів протидії кібертероризму, аналіз ефективності наявних правових та інституційних інструментів, а також вивчення ролі міжнародної співпраці в забезпеченні кібербезпеки в межах Європейського Союзу.

Виклад основного матеріалу. Кібертероризм є серйозною загрозою для міжнародної безпеки, що ускладнює стабільність регіонів, зокрема Європейського Союзу (ЄС). Зростання кібертерористичних атак, які використовують сучасні технології, створює виклики для окремих держав і регіонів. Це вимагає активнішої співпраці між урядами та міжнародними організаціями для розробки ефективних механізмів протидії [6].

ЄС застосовує системний підхід до боротьби з кібертероризмом, включаючи правове регулювання, створення інституцій і співпрацю з іншими регіонами. Регламент (ЄС) 2019/881 і Директива (ЄС) 2022/2555 підвищують кіберстійкість країн-членів і зміцнюють роль Європейського агентства з кібербезпеки (ENISA). Публічно-приватні партнерства стають важливим елементом цієї боротьби [7; 8].

Будапештська конвенція є основою для міжнародного співробітництва у боротьбі з кіберзлочинами, а її вплив поширюється за межі ЄС. Однак існує потреба в адаптації правових механізмів до нових викликів цифрової епохи.

Європа активно використовує сучасні технології, як-от штучний інтелект, великі дані та платформи обміну інформацією, для зменшення ризиків і підвищення ефективності боротьби з кібертероризмом. Колективне управління ризиками та стійкість кіберпростору залишаються ключовими пріоритетами.

Попри успіхи, ЄС стикається з викликами, такими як координація між державами-членами, узгодження законодавства, підготовка кадрів і фінансування ініціатив. Регламент (ЄС) 2019/881 (Cybersecurity Act) забезпечує ENISA розширеними повноваженнями та створює базу для сертифікації ІКТ, посилюючи кібербезпеку в ЄС [7].

ENISA, створене у 2004 році, до прийняття Cybersecurity Act діяло як дорадчий орган, зосереджуючись переважно на рекомендаціях та розробці стратегій кібербезпеки. Проте, Регламент (ЄС) 2019/881 значно посилив повноваження агентства. Як зазначає OLEKSIEWICZ та CIVELEK (2023), ENISA отримало мандат на постійну діяльність, що дозволяє агентству ефективніше координувати заходи у сфері кібербезпеки на рівні ЄС.

Одним з основних нововведень Регламенту є розробка єдиної системи сертифікації кібербезпеки. ENISA, за даними European Union (2019), стало ключовим органом у створенні та впровадженні схем сертифікації для забезпечення безпеки інформаційно-комунікаційних технологій. Ця система спрямована на підвищення довіри до цифрових рішень, які використовуються як урядовими установами, так і приватним сектором.

Регламент 2019/881 забезпечує важливий правовий інструмент у боротьбі з кібертероризмом. Christou (2019) наголошує, що колективна безпека кіберпростору залежить від скоординованих зусиль між державами-членами. У цьому контексті ENISA виступає як ключовий координатор, забезпечуючи взаємодію між державними установами, приватним сектором та міжнародними партнерами [7].

ENISA також відіграє важливу роль у підвищенні обізнаності про кіберзагрози. Як зазначає Baldassarre [9], інформаційні кампанії агентства спрямовані на підвищення обізнаності серед громадян та організацій щодо ризиків кібертероризму. Це дозволяє зменшити ймовірність успішних атак через необізнаність або людські помилки.

Попри численні переваги, експерти підкреслюють обмеження Cybersecurity Act. Зокрема, Bossong [10] зазначає, що ENISA стикається з викликами через різнорівневу підготовку держав-членів до кіберзагроз. Відсутність гармонізації національних підходів може створювати проблеми для реалізації єдиної стратегії кібербезпеки на рівні ЄС.

Іншим критичним аспектом є недостатність фінансування ENISA. Як зазначає Biscop [11], бюджет агентства є недостатнім для реалізації всіх поставлених завдань, особливо в умовах зростання кількості кібертерористичних атак. Цей аспект потребує подальшого аналізу та розробки механізмів фінансування.

Регламент 2019/881 заклав основу для створення сучасної системи кібербезпеки у Європейському Союзі. Проте, подальший розвиток цього законодавчого акту є необхідним для забезпечення більш ефективної боротьби з кібертероризмом. Як зазначає Oleksiewicz I. та Civelek M. [12], одним із можливих шляхів удосконалення є інтеграція новітніх технологій, таких як штучний інтелект та машинне навчання, у процеси виявлення та реагування на кіберзагрози.

ENISA може також розширити свою діяльність у сфері міжнародного співробітництва. Al Asyari [3] підкреслює важливість співпраці ЄС з іншими регіонами, такими як АСЕАН, у боротьбі з кібертероризмом. Впровадження кращих практик та обмін досвідом можуть значно підвищити ефективність боротьби з кіберзагрозами на глобальному рівні.

Регламент (ЄС) 2019/881 (Cybersecurity Act) є важливим інструментом у забезпеченні кібербезпеки Європейського Союзу. ENISA відіграє ключову роль у реалізації стратегій протидії кібертероризму, забезпечуючи взаємодію між різними зацікавленими сторонами. Проте, для подолання наявних викликів необхідні додаткові заходи, спрямовані на гармонізацію національних підходів, збільшення фінансування та впровадження новітніх технологій. Це дозволить Європейському Союзу зміцнити свою позицію як лідера у сфері кібербезпеки [7].

Директива (ЄС) 2022/2555, відома як NIS 2, є ключовим нормативно-правовим актом, що запроваджує нові стандарти кібербезпеки для держав-членів Європейського Союзу. Ця директива замінила попередню NIS Directive (2016/1148), пропонуючи більш розширений і структурований підхід до забезпечення кіберстійкості. Вона спрямована на гармонізацію кібербезпекової політики серед країн-членів ЄС, підвищення рівня захисту критично важливої інфраструктури та зміцнення загальної безпеки кіберпростору [13].

NIS 2 суттєво розширює сферу дії порівняно з її попередником. Як зазначає Radoniewicz [14], директива зобов'язує ширший спектр організацій – від постачальників критичних послуг до цифрових платформ – дотримуватися високих стандартів кібербезпеки. Директива також вводить жорсткіші вимоги до управління кіберризиками, що включають регулярний моніторинг, виявлення вразливостей та швидке реагування на інциденти.

Суттєвим нововведенням є створення єдиного механізму управління інцидентами. Згідно з положеннями NIS 2, держави-члени повинні запровадити чітку структуру відповідальних органів, таких як компетентні національні органи та CSIRT (команди реагування на кіберінциденти). Як зазначає Skoczylas [15], це дозволяє покращити координацію дій між країнами та зменшити час реагування на кіберзагрози.

NIS 2 має значний потенціал у боротьбі з кібертероризмом, забезпечуючи проактивний підхід до управління ризиками. Як зазначає Baldassarre [9], посилені вимоги до захисту критично важливої інфраструктури, такої як енергетика, транспорт і телекомунікації, знижують ймовірність успішних атак кібертерористів. Крім того, директива вимагає впровадження механізмів обміну інформацією між організаціями та державами, що підвищує їх здатність ідентифікувати та запобігати загрозам.

Radoniewicz [14] наголошує, що директива робить особливий акцент на міжнародній співпраці. Це включає обмін інформацією з третіми країнами та використання кращих практик, розроблених на основі глобального досвіду. У випадках кібертероризму цей підхід дозволяє створити ефективні механізми раннього попередження про загрози.

Попри численні переваги, деякі дослідники вказують на недоліки директиви. Як зазначає Trofymenko & Mishanchuk [5], значна різниця у рівні кіберготовності серед держав-членів створює труднощі для гармонізації політики. Деякі країни можуть стикпоставати перед труднощами у впровадженні нових стандартів через обмежені фінансові та технічні ресурси.

Іншим викликом є забезпечення виконання вимог директиви. Як зазначає Olesen [16], ефективне впровадження NIS 2 залежить від здатності національних органів контролювати дотримання стандартів, що вимагає значних адміністративних ресурсів. Крім того, ризик кіберзагроз постійно еволюціонує, що потребує регулярного оновлення підходів до управління ризиками.

Для ефективності NIS 2 важливо впровадити новітні технології, такі як штучний інтелект, та збільшити фінансування програм кібербезпеки. Тісніша міжнародна співпраця з організаціями, як НАТО та АСЕАН, та проведення навчань підвищать готовність держав-членів до нових викликів.

NIS 2 зміцнює кіберстійкість ЄС, підвищує захист критично важливої інфраструктури та зміц-

нює міжнародну співпрацю. Її вдосконалення є пріоритетом для ЄС у боротьбі з кібертероризмом [17].

Рамкове рішення 2002/475/ЈНА стало основою для боротьби з тероризмом у ЄС, і після еволюції кіберзагроз було розширене для врахування кібертероризму. Воно визначає тероризм як дії, що шкодять державам або міжнародним організаціям, зокрема атаки на критичну інфраструктуру, характерні для кібертероризму [8].

Рамкове рішення спрямоване на боротьбу з різними формами терористичних загроз, у тому числі кіберзагрозами, які мають такі характеристики:

1. Атаки на критичну інфраструктуру: Olesen [16] зазначає, що кібертерористи часто націлюються на енергетичні, транспортні та комунікаційні системи.

2. Використання інтернету для вербування та пропаганди: Laytouss [18] підкреслює роль кіберпростору у поширенні екстремістських ідеологій та вербуванні членів терористичних груп.

3. Фінансування тероризму через кіберпростір: Зростання використання криптовалют та цифрових фінансових інструментів створює нові можливості для фінансування терористичних актів, що відповідає загрозам, визначеним у Рамковому рішенні.

Попри адаптацію до нових загроз, Рамкове рішення стикається з низкою викликів. Trofymenko та Mishanchuk [5] вказують на розбіжності у правових системах держав-членів, що ускладнює ефективну боротьбу з кіберзлочинністю. Зростання складності кіберзагроз також потребує використання передових технологій для їх виявлення та нейтралізації. Інший виклик – це забезпечення балансу між безпекою та захистом прав людини. Oliynyk та ін. [19] відзначають, що розширення правових повноважень у боротьбі з тероризмом може створити ризики для конфіденційності та інших основних прав громадян.

Для підвищення ефективності Рамкового рішення в контексті кіберзагроз необхідно врахувати кілька аспектів:

1. Гармонізація законодавства: Olesen [16] пропонує уніфікацію правових норм серед держав-членів для покращення координації в боротьбі з кіберзлочинністю.

2. Інтеграція технологій: Використання штучного інтелекту, машинного навчання та великих даних може значно підвищити здатність держав виявляти кіберзагрози.

3. Поглиблення міжнародної співпраці: Al Asyari [3] підкреслює важливість обміну інформацією між ЄС та іншими регіонами для створення глобальної системи протидії кібертероризму.

4. Навчання та підготовка фахівців: Baldassarre [9] вказує на необхідність створення освітніх програм для підвищення кваліфікації фахівців у сфері кібербезпеки.

Рамкове рішення ЄС 2002/475/ЈНА залишається важливим інструментом у боротьбі з тероризмом, включаючи кібертероризм. Воно встановлює правові основи для криміналізації терористичної діяльності, що охоплює кіберпростір. Однак, для ефективного розв'язання проблем, пов'язаних із новими формами кіберзагроз, необхідні подальші вдосконалення, зокрема у сфері технологій, міжнародного співробітництва та гармонізації законодавства. Ці заходи сприятимуть підвищенню стійкості ЄС до кібертерористичних загроз та забезпеченню безпеки в умовах цифрової епохи [8].

Розвиток інституційних механізмів відіграє вирішальну роль у реалізації стратегій кібербезпеки, оскільки саме вони забезпечують координацію зусиль, впровадження стандартів і реагування на нові виклики. У цьому контексті Європейський Союз пропонує багаторівневий підхід, де ключову роль відіграють спеціалізовані органи, такі як Європейське агентство з кібербезпеки (ENISA), а також співпраця з іншими міжнародними організаціями, зокрема Радою Європи.

ENISA стало центральним інститутом у забезпеченні кібербезпеки в Європейському Союзі. Його роль значно змінилася з ухваленням Регламенту (ЄС) 2019/881, відомого як Cybersecurity Act [7]. Як зазначає Oleksiewicz та Civelek [12], завдяки розширенню мандату агентство набуло статусу постійного координатора заходів у сфері кібербезпеки, що дозволило ЄС перейти до більш системного підходу.

Аналізуючи вплив діяльності ENISA, Christou [2] підкреслює, що агентство стало рушійною силою гармонізації стандартів кібербезпеки в ЄС. Однак автор критикує ENISA за недостатню оперативність у впровадженні нових схем сертифікації, що затримує їхнє впровадження на рівні держав-членів. Крім того, Bossong [10] наголошує, що через різний рівень готовності країн до кіберзагроз ENISA змушене адаптувати свої рекомендації, що знижує їх ефективність.

Ще одним аспектом критики є недостатнє фінансування. Biscop [11] звертає увагу на обмежених ресурсах ENISA, які не відповідають масштабам його завдань, особливо в умовах зростання кількості та складності кіберзагроз. Автори наголошують, що підвищення фінансування могло б сприяти реалізації більш амбітних програм.

Попри ці виклики, Oleksiewicz [12] позитивно оцінює діяльність ENISA у сфері підвищення обізнаності щодо кіберзагроз. Зокрема, інформаційні кампанії агентства допомагають зменшити ризики людських помилок, які часто стають причиною успішних атак.

Будапештська конвенція (2001), яку координує Рада Європи, залишається головним міжнародним правовим документом у боротьбі з кіберзлочинністю. Як зазначає Denning [20], ця конвенція

забезпечує єдиний підхід до криміналізації кіберзлочинів, включаючи ті, що пов'язані з кібертероризмом. Її положення слугують основою для правового регулювання у багатьох країнах світу.

Однак Christou [2] критикує конвенцію за її обмежений вплив на глобальну боротьбу з кіберзлочинами. Хоча більшість країн ЄС є її сторонами, недостатня кількість підписантів серед країн, що не входять до ЄС, ускладнює її реалізацію. Цей недолік посилюється відсутністю механізмів примусового виконання.

Radoniewicz [14] підкреслює роль Будапештської конвенції у формуванні міжнародного співробітництва. Проте автор наголошує, що у сфері кібертероризму цей документ часто поступається місцем новішим ініціативам ЄС, таким як NIS 2.

Однак, Olesen [16] акцентує на ефективності партнерств Ради Європи з приватним сектором. Це сприяє впровадженню практичних інструментів для виявлення та реагування на кіберзагрози.

Співпраця з приватним сектором є ключовим елементом у боротьбі з кіберзагрозами. Bossong [10] класифікує моделі взаємодії в ЄС, виділяючи публічно-приватні партнерства як найбільш ефективний формат. Однак автор також звертає увагу на складність координації між учасниками через різницю у пріоритетах.

Як зазначає Baldassarre [9], приватний сектор часто відіграє важливу роль у впровадженні технологій для моніторингу та попередження кіберзагроз. Проте недостатній рівень довіри між державними установами та бізнесом може ускладнювати обмін інформацією.

Trofymenko & Mishanchuk [5] наголошують на необхідності створення загальноєвропейської платформи для обміну даними між приватним та державним секторами. Така платформа могла б значно покращити координацію та підвищити швидкість реагування на кібертерористичні атаки.

Christou [2] підкреслює, що приватний сектор часто демонструє вищу гнучкість у впровадженні інноваційних рішень. Проте автор звертає увагу на ризики, пов'язані з комерційними інтересами, які можуть суперечити завданням забезпечення безпеки.

Інституційні механізми Європейського Союзу демонструють значний прогрес у боротьбі з кібертероризмом. ENISA відіграє центральну роль у гармонізації стандартів кібербезпеки, Рада Європи забезпечує міжнародну співпрацю через Будапештську конвенцію, а приватний сектор стає важливим партнером у впровадженні новітніх технологій. Попри це, існує низка викликів, включаючи недостатнє фінансування, брак гармонізації та низький рівень довіри між державними й приватними структурами. Подолання цих перешкод є ключовим для підвищення ефективності інституційних механізмів у боротьбі з кіберзагрозами.

Колективна безпека кіберпростору стала одним із ключових напрямів політики Європейського Союзу, що дозволяє забезпечити стійкість та ефективне реагування на кіберзагрози. У сучасному цифровому середовищі кібербезпека не може бути досягнута зусиллями лише окремих держав чи організацій. Як зазначає Christou [2], колективна безпека передбачає інтеграцію державних, приватних та міжнародних зусиль, а також використання новітніх технологій для протидії кіберзагрозам.

Christou [2] пропонує концепцію колективної кібербезпеки в ЄС, засновану на спільній відповідальності, інтеграції ресурсів та адаптивності. Автор підкреслює важливість загальноєвропейської стійкості та координації, зокрема через CSIRT Network, хоча різний рівень підготовки держав ускладнює співпрацю [10].

Christou також зазначає, що недостатня інтеграція приватного сектору у механізми безпеки обмежує використання передових технологій і даних, необхідних для прогнозування загроз. Відсутність довіри між державними й приватними структурами залишається ключовою перешкодою.

Публічно-приватне партнерство (PPP) є важливим елементом у забезпеченні кібербезпеки, зокрема в боротьбі з кібертероризмом. Bossong [10] класифікує партнерства на горизонтальні (між державними структурами) та вертикальні (між державними й приватними суб'єктами). У контексті кібертероризму PPP включає:

1. Обмін інформацією: Приватний сектор надає державним органам дані про кіберзагрози, а державні структури забезпечують регулювання [9].

2. Розробку технологічних рішень: Комерційні компанії створюють інструменти моніторингу та прогнозування атак [18].

Проте, PPP стикається з викликами, такими як комерційна конфіденційність і ризики витоку даних [10]. Відсутність єдиної платформи для взаємодії ускладнює обмін інформацією. Radoniewicz [14] наголошує на необхідності прозорості у співпраці та впровадженні стандартів обміну даними.

Технології відіграють важливу роль у попередженні кіберзагроз. Christou [2] акцентує на використанні великих даних, ШІ та автоматизації для виявлення загроз. Baldassarre [9] виділяє ключові технології, такі як:

1. Штучний інтелект (ШІ): Для аналізу поведінки користувачів і виявлення аномалій.

2. Блокчейн: Для забезпечення безпеки даних.

3. Хмарні технології: Для зберігання і доступу до великих обсягів даних.

Ferrag et al. [21] вказують на важливість державного фінансування для підвищення потенціалу приватних технологій. Christou [2] також підкреслює значення платформ для обміну інформацією, таких як MISP, хоча Olesen [16] зазначає проблеми з конфіденційністю та безпекою цих платформ.

Колективна кібербезпека ЄС спирається на співпрацю держав, приватного сектору та міжнародних партнерів, впровадження інновацій, публічно-приватне партнерство та платформи обміну інформацією. Головними викликами залишаються брак довіри, нерівність готовності держав і обмежені ресурси. Їхнє подолання є ключем до стійкості кібербезпеки.

У глобалізованому світі кіберзагрози потребують міжнародної координації. ЄС активно співпрацює з ініціативами, як-от АСЕАН, аналізуючи та порівнюючи підходи до кібербезпеки в різних регіонах.

АСЕАН є важливим партнером ЄС у сфері кібербезпеки, враховуючи зростання кіберзагроз у Південно-Східній Азії та їхній вплив на глобальну кібербезпеку. Al Asyari [3] підкреслює, що співпраця між ЄС та АСЕАН базується на обміні кращими практиками, технологіями та досвідом у сфері кібертероризму. Одним із ключових інструментів цього партнерства є діалог високого рівня між представниками ЄС та АСЕАН, який сприяє розробці спільних стратегій.

Основні напрямки співпраці:

1. Обмін інформацією про кіберзагрози: Платформи обміну між ЄС та АСЕАН дозволяють швидко виявляти загрози та розробляти спільні механізми реагування [3].

2. Навчання та підвищення кваліфікації: ЄС підтримує освітні програми в АСЕАН для підготовки спеціалістів з кібербезпеки [9].

3. Спільні навчання: Спільні кібернавчання підвищують готовність до складних атак, включаючи кібертероризм [3].

Виклики:

- Різні стандарти регулювання у країнах ЄС та АСЕАН ускладнюють реалізацію ініціатив [16].

- Різний рівень кіберготовності в країнах АСЕАН.

Пропозиції для розвитку співпраці включають створення спільних платформ та розширення навчальних програм [3], а також підтримку гармонізації стандартів кібербезпеки в країнах АСЕАН. ЄС і НАТО мають спільні принципи колективної безпеки, але ЄС більше фокусується на цивільній кібербезпеці, а НАТО – на військовій [14].

Спільні навчання НАТО та ЄС демонструють ефективність інтеграції військових і цивільних підходів. Ferrag et al. [21] підкреслюють, що подібна взаємодія сприяє виявленню вразливостей у системах кібербезпеки та розробці нових стандартів.

Проте, як зазначає Oleksiewicz [12], основним викликом для співпраці залишається розбіжність у пріоритетах. НАТО фокусується на безпосередній обороні, тоді як ЄС займається довгостроковою побудовою кіберстійкості.

ОАД є провідною організацією у Західній півкулі, яка активно працює над розвитком кібербезпеки. Laytouss [18] вказує на подібності між підходами ОАД і ЄС, зокрема у питаннях підготовки кадрів та обміну інформацією. Проте ОАД має менший вплив на гармонізацію законодавства через відсутність єдиної правової системи в регіоні.

Досвід ЄС у створенні спільних правових стандартів, таких як NIS 2, міг би стати корисним для ОАД. Водночас як зазначає Baldassarre [14], обмеженість фінансування в країнах Латинської Америки може ускладнювати впровадження європейських підходів.

Співпраця ЄС та Африканського Союзу у сфері кібербезпеки є на етапі становлення. Як зазначає Biscop [11], основними напрямками є технічна допомога та навчання фахівців. Водночас через відсутність регіональної кіберстратегії, Африканський Союз значно поступається ЄС у структурованості підходів.

Radoniewicz [14] наголошує, що ЄС може сприяти створенню правової бази для боротьби з кібертероризмом в Африці. Це передбачає впровадження інструментів, схожих на Будапештську конвенцію.

Висновки та перспективи дослідження. Взаємодія ЄС з іншими регіональними ініціативами демонструє прагнення до створення глобальної системи кібербезпеки. Співпраця з АСЕАН, НАТО, ОАД та Африканським Союзом дає змогу обмінюватися кращими практиками та підвищувати рівень готовності до кіберзагроз. Однак існують суттєві виклики, такі як різні рівні розвитку, обмеженість ресурсів та відсутність гармонізації законодавства. Для подолання цих проблем необхідні довгострокові ініціативи, спрямовані на зміцнення міжнародної взаємодії та обмін досвідом.

Аналіз європейських підходів до протидії кібертероризму показав, що Європейський Союз (ЄС) створив комплексну систему правових, інституційних та технологічних механізмів. У межах цієї системи було розглянуто основні аспекти, які охоплюють нормативно-правову базу (Регламент (ЄС) 2019/881, Директива (ЄС) 2022/2555, Рамкове рішення 2002/475/ЈНА), діяльність ключових інституцій (ENISA, Рада Європи), розвиток публічно-приватного партнерства та співпрацю з іншими регіональними ініціативами.

Результати дослідження підтвердили важливість комплексного підходу до протидії кібертероризму. Використання європейського досвіду може бути корисним для інших регіонів, які прагнуть розвивати власні системи кібербезпеки. Особливо актуальними є дослідження Christou та Baldassarre, які окреслюють перспективи колективної безпеки кіберпростору та роль інноваційних технологій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Baker-Beall C., Mott G. Understanding the european union's perception of the threat of cyberterrorism: a discursive analysis. JCMS: journal of common market studies. 2021. URL: https://doi.org/10.1111/jcms.13300

2. Christou G. The collective securitisation of cyberspace in the European Union. West european politics. 2018. Vol. 42, no. 2. P. 278–301. URL: https://doi.org/10.1080/01402382.2018.1510195

3. Al Asyari H. The evolution of cyberterrorism: perspectives and progress from the european union and association of southeast asian nation. Jurnal hukum ius quia iustum. 2022. Vol. 29, no. 1. P. 1–23. URL: https://doi.org/10.20885/iustum.vol29.iss1.art1

4. Oleksiewicz I. A legal assessement of management of the european union cyberterrorism policy. Modern management review. 2017. URL: https://doi.org/10.7862/rz.2017.mmr.32

5. Trofymenko V., Mishanchuk A. Cyberterrorism: an attempt of philosophical and legal understanding. The Bulletin of Yaroslav Mudryi National Law University. Series:philosophy, philosophies of law, political science, sociology. 2021. Vol. 2, no. 49. URL: https://doi.org/10.21564/2663-5704.49.229782

6. Council of the European Union (2021) Parties/Observers to the Budapest Convention and Observer Organisations to the T-CY. URL: https://www.coe.int/en/web/cybercrime/parties-observers.

7. European Union. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). 2019. URL: https://eur-lex.europa.eu/eli/reg/2019/881/oj/eng

8. EU Framework Decision on Combating Terrorism (2002/475/JHA), 2002. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32002F0475

9. Baldassarre S. Cyberterrorism and religious fundamentalism: new challenges for europe in the age of universal internet access. Religions. 2023. Vol. 14, no. 4. P. 458. URL: https://doi.org/10.3390/rel14040458

10. Bossong, R. A Typology of Cybersecurity and Public – Private Partnerships in the Context of the European Union [In:] Bures, O., Carrapico, H., ed., Security Privatization. How Non-security-related Private Businesses Shape Security Governance. Warszawa. 2018. URL: https://www.researchgate.net/publication/309170004_A_typology_of_cybersecurity_and_public-private_partnerships_in_the_context_of_the_EU

11. Biscop, S. The EU Global Strategy 2020 ("Security Policy Brief" No. 108). Brussels: EGMONT – Royal Institute for International Relations. 2019. URL: http://www.egmontinstitute.be/content/uploads/2019/03/SPB108.pdf?type=pdf.

12. Oleksiewicz I., Civelek M. E. Where are the changes in eu cybersecurity legislation leading? Humanities and social sciences quarterly. 2023. Vol. 30, no. 4 - part I. P. 183–197. URL: https://doi.org/10.7862/rz.2023.hss.50

13. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (O.J.L. 333, 27.12.2022). URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng

14. Radoniewicz F. Cybersecurity in the european union law. Cybersecurity in poland. Cham, 2021. P. 73–92. URL: https://doi.org/10.1007/978-3-030-78551-2_6

15. Skoczylas D. ICT Development in Eastern European Countries in the Context of Cybersecurity. Threats and Cyberspace Protection – Selected Issues. Prawo i Wiez, 2022. №41. P. 328–344. URL: https://doi.org/10.36128/priw.vi41.220

16. Olesen N. European public-private partnerships on cybersecurity - An instrument to support the fight against cybercrime and cyberterrorism. In Advanced Sciences and Technologies for Security Applications. 2016. pp. 259–278. URL: https://doi.org/10.1007/978-3-319-38930-1_14

17. European Commission, Cybersecurity Policies. Shaping Europe's digital future. URL: https://ec.europa.eu/digital-single-market/en/cyber-security

18. Laytouss B. New Terrorism and the Use of Electronic Jihad, Brussels International Center. 2021. URL: www.bic-rhr.com/sites/default/files/inline-files/New%20Terrorism%20and%20the%20Use%20of%20Electronic%20Jihad_1.pdf

19. Oliynyk, O. B., Romanova, A. S., Koval, I. M., Chornobai, O. L., & Poliarush-Safronenko, S. O. Protection of Personal Data in the Context of Human Rights: Experience and Relevance of ECtHR Decisions. Revista Juridica Portucalense, 2023. №33, Pp. 234–249. https://doi.org/10.34625/issn.2183-2705(33)2023.ic-10

20. Denning, D. Cyberterrorism, Prepared for Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives. 2023. URL: http://www.cs.georgetown.edu/~denning/infosec/cvberterror.html.

21. Ferrag, M. A., Kantzavelou, I., Maglaras, L., & Janicke, H. Hybrid Threats, Cyberterrorism and Cyberwarfare. Hybrid Threats, Cyberterrorism and Cyberwarfare. CRC Press. 2023. URL: https://doi.org/10.1201/9781003314721