DOI: 10.18372/2225-5036.31.20636

КОНЦЕПЦІЯ АКТИВНОГО КІБЕРЗАХИСТУ В КОНТЕКСТІ ТЕХНОЛОГІЧНИХ СПРОМОЖНОСТЕЙ ПРОТИДІЇ КІБЕРЗАГРОЗАМ

Микола Коваль

Державний університет «Київський авіаційний інститут»,
Державна служба спеціального зв'язку та захисту інформації України

КОВАЛЬ Микола Васильович
Рік та місце народження: 1988, м. Київ
Освіта: ІСЗЗІ НТУУ "КПІ", 2010
Посада: аспірант Державного університету «Київський авіаційний інститут», фахівець Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України.
Наукові інтереси: кібербезпека, інформаційна безпека, технічний захист інформації, реагування на кіберінциденти, комп'ютерно-технічні дослідження, кіберрозвідка
Публікації: -
E-mail: uac.3333@gmail.com
Orcid ID: 0009-0004-9699-6849

Анотація. *Забезпечення кібербезпеки визначено одним із ключових пріоритетів у системі національної безпеки України, а кіберпростір розглядається як один з можливих театрів воєнних дій. Еволюція ландшафту кіберзагроз та вдосконалення програмних засобів їх реалізації на тлі стрімкої цифровізації зумовили суттєве зростання швидкості здійснення кібератак і, відповідно, скорочення часу, допустимого для ефективного реагування. Це актуалізує потребу у впровадженні проактивних заходів кіберзахисту, при цьому виключно в межах дій ненаступального характеру.*

У статті здійснено огляд кіберстратегій окремих європейських та азіатських країн з акцентом на підходах до розвитку активного кіберзахисту та використання відповідних технологічних спроможностей. Такий аналіз дозволяє окреслити тенденції міжнародної практики й можливості їх адаптації в національному контексті.

Особливу увагу приділено підходам до активної протидії кіберзагрозам, заснованим на унеможливленні інформаційного обміну між суб'єктом та об'єктом мережевої взаємодії на рівнях IP та DNS. Розглянуто питання масштабованості таких рішень, контекстуалізації даних та технічної спроможності до оперативної генерації сповіщень про кіберзагрози.

Ключові слова*: кіберзахист, активний кіберзахист, протидія кіберзагрозам, стратегія кібербезпеки, threat intelligence, active cyber protection, NIS2.*

Постановка проблеми

Стратегією кібербезпеки України, що затверджена Указом Президента України від 26.08.2021 №447/2021 (далі – Кіберстратегія) [1], забезпечення кібербезпеки визначено одним із пріоритетів у системі національної безпеки України, а кіберпростір – одним з можливих театрів воєнних дій.

Так, протягом останнього десятиліття, захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору була неодноразово порушена внаслідок проведення цільових деструктивних кібератак.

Водночас Кіберстратегією для створення нової якості національної системи кібербезпеки окреслено основні напрямки розвитку, серед яких формування потенціалу стримування (С) та набуття кіберстійкості (К). При цьому, для досягнення стратегічної цілі С.2 "Ефективна протидія розвідувально-підривній діяльності у кіберпросторі та кібертероризму", передбачено *створення технологічних можливостей для автоматичного виявлення кібератак у режимі реального часу в потоках даних загальнодержавних інформаційно-комунікаційних систем та на окремих об'єктах критичної інфраструктури, їх блокування та визначення пріоритетності*. Крім того, досягнення стратегічної цілі К.1 "Національна кіберготовність та надійний кіберзахист" планується здійснити шляхом *забезпечення постійного моніторингу національних електронних комунікаційних мереж та інформаційних ресурсів, аналізу вторгнень щодо цих мереж і ресурсів, а також виявлення в режимі реального часу аномалій їх функціонування*.

Крім того, абзацем 57 та пунктом "j" статті 7 директиви Європейського парламенту 2022/2555 від 14.12.2022 (далі - NIS2) [2] наголошено, що стратегія захисту, в широкому розумінні, повинна передбачати розвиток *активного кіберзахисту* (англ. - "active cyber protection"), що є сукупністю активних засобів та заходів для протидії, виявлення, моніторингу, аналізу, запобігання кібератак у формі безкоштовних послуг та інструментів, включаючи самостійну перевірку, засоби виявлення та блокування, розгорнутих, в тому числі, за межами комп'ютерних мереж об'єктів кібератаки. При цьому, можливість швидкого автоматичного розповсюдження індикаторів кіберзагроз, коректна інтерпретація кіберінцидентів та кібератак (контекстуалізація, зокрема, атрибуція), оперативні інформування, - так звані ранні сповіщення (англ. "early warning") та

застосування контрзаходів є критичними для успішного виявлення, запобігання та блокування кібератак, спрямованих на комп'ютерні мережі та інформаційні системи. В той же час, активний кіберзахист повинен виключати наступальні дії.

Президентом України 27.03.2025 було підписано Закон України №4336-IX "Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури" [3], відповідно до якого, серед іншого, введено поняття "національна система реагування на кіберінциденти, кібератаки, кіберзагрози" та "національна система обміну інформацією про кіберінциденти, кібератаки, кіберзагрози".

З огляду на викладене набирає актуальності питання вивчення та розвитку національних технологічних спроможностей для моніторингу, виявлення, аналізу, пріоритизації, блокування кібератак в загальнодержавних інформаційно-комунікаційних системах (ІКС), які можна було б застосовувати в режимі реального часу в рамках існуючого правового поля, виключаючи наступальну природу таких дій.

Аналіз останніх досліджень і публікацій

Поняття Active Cyber Defence (укр. "активна кібероборона"), зокрема в дослідженнях Дороті Е. Деннінг [4], часто розглядається разом із Passive Cyber Defence (укр. "пасивна кібероборона"). У цьому контексті англійське defence перекладають як "оборона", а "активна" складова інтерпретується автором як така, що включає заходи наступального характеру. Схожу позицію висловлює Р. Девар [5], наводячи приклади заходів, що іноді відносять до Active Cyber Defence, - наприклад, hack-back (укр. "злам у відповідь") або honeypots (укр. "мережеві пастки").

Водночас директива NIS2 [2] вводить термін Active cyber protection (укр. "активний кіберзахист"), підкреслюючи як ключову характеристику non-offensive (укр. "ненаступальну") природу відповідних засобів і заходів. У цьому контексті protection доречно перекладати як "захист", що відокремлює його семантику від поняття "оборона" з бойовим/військовим забарвленням.

В той же час, у законодавстві України існує певна невизначеність. Наприклад, у Законі "Про основні засади забезпечення кібербезпеки України" [6] надаються визначення поняттям "кібероборона" та "кіберзахист", натомість у Законі "Про оборону України" [7] поряд із формулюванням "заходи з кібероборони" в дужках зазначено "активного кіберзахисту": "здійснення заходів з кібероборони (активного кіберзахисту) для захисту суверенітету держави та забезпечення її обороноздатності, запобігання збройному конфлікту та відсічі збройній агресії;". Таке формулювання нормативно зближує або навіть ототожнює ці поняття.

Зазначене створює методологічну і термінологічну суперечність, яка ускладнює адаптацію міжнародних концепцій (зокрема Active cyber protection, визначеного в NIS2 [2] як сукупність ненаступальних превентивних заходів) до національної нормативної бази.

З огляду на викладене в цій статті "активний кіберзахист" пропонується розглядати як поняття, тотожне Active cyber protection (включно з наголосом на ненаступальний характер заходів і засобів), тоді як "активна кібероборона" трактуватиметься як поняття, пов'язане з державною/військовою діяльністю у кіберпросторі, що потенційно здатне включати операції для безпосереднього впливу на інфраструктуру атакуючих.

Мета та постановка завдання

Метою статті є дослідження концепції активного кіберзахисту як ненаступального інструменту протидії кібератакам на загальнодержавному рівні, з акцентом на застосування технологічних спроможностей у режимі реального часу в умовах динамічного ландшафту кіберзагроз.

Досягнення цієї мети передбачає насамперед аналіз наявних підходів до визначення й інтерпретації понять "активний кіберзахист" та "активна кібероборона" у міжнародному та національному правових і наукових контекстах.

Важливим завданням є формування теоретичного підґрунтя для розробки технологічних можливостей активного кіберзахисту з урахуванням його ненаступального характеру.

Окремої уваги потребує окреслення практичних напрямів застосування таких технологічних спроможностей для моніторингу, виявлення, аналізу, пріоритизації та блокування кібератак у масштабах загальнодержавних інформаційно-комунікаційних систем.

Крім того, необхідно визначити, яким чином активний кіберзахист може сприяти досягненню стратегічних цілей, визначених Кіберстратегією України, та узгоджуватися з вимогами й рекомендаціями європейського законодавства, зокрема директиви NIS2.

Виклад основного матеріалу дослідження

Уряд Австралії 22.11.2023 затвердив Стратегію кібербезпеки Австралії на 2023-2030 роки [8], згідно з якою для досягнення країною лідерства у сфері до 2030 року визначено шість ключових напрямків розвитку ("щитів") та три фази ("горизонти") їх імплементації. Так, щит №3 передбачає створення мережі для обміну інформацією про кіберзагрози ("threat intelligence"), а також розробку й масштабування спроможностей "нового покоління" для автоматичного блокування кібератак в режимі реального часу в масштабах країни із залученням операторів та провайдерів телекомунікацій на основі

вивіреної та контекстуалізованої інформації щодо кіберзагроз.

Стратегія кібербезпеки Республіки Латвія на 2023 - 2026 роки [9], візія якої полягає у створенні захищеного, безпечного, вільного, довіреного кіберпростору, визначає три основні пріоритети її імплементації: захист, стримування та розвиток. Разом з тим, незважаючи на те, що було зазначено необхідність розробки засобів активного кіберзахисту як частини заходів стримування, детальної інформації щодо реалізації цього задуму не наведено.

Стратегія національної безпеки Японії 2022 року [10], в частині удосконалення спроможностей щодо реагування у сфері кібербезпеки, визначає пріоритетним розвиток "активного кіберзахисту", спрямованого на завчасну (проактивну) ліквідацію можливостей (передумов) для здійснення кібератак. Передбачається, що такий підхід включатиме: 1) покращення обміну інформацією з приватним сектором та об'єктами критичної інфраструктури, 2) виявлення серверів, що використовуються для здійснення кібератак, у взаємодії з вітчизняними провайдерами телекомунікацій, 3) нейтралізацію згаданих серверів, в тому числі шляхом завчасного отримання доступу до останніх.

У 2016 році у Великобританії почав роботу Національний центр кібербезпеки (NCSC). Водночас, в Національній стратегії кібербезпеки на 2016 - 2021 роки [11], візія якої визначала Великобританію захищеною та стійкою до кіберзагроз, процвітаючою та впевненою у цифровому світі, одна з трьох основних цілей - ЗАХИСТ ("DEFEND") - передбачала створення спроможностей для захисту країни від кіберзагроз та ефективного реагування на кіберінциденти, на виконання чого першим пунктом розділу 5 Стратегії визначено "активний кіберзахист", як концептуальний принцип та сукупність заходів для проактивного захисту, формалізованих у вигляді програми "Active Cyber Defence" (ACD).

В Національній кіберстратегії 2022 року [12] вжиття безпосередніх заходів, спрямованих на зменшення негативного впливу кібератак на Великобританію, передбачається здійснювати, в тому числі, із застосуванням ACD, а NCSC, у взаємодії з Національними кіберсилами (NCF), офіційно визначено відповідальною установою за реалізацію таких заходів.

Стратегія кібербезпеки Бельгії на 2021 - 2025 роки [13], у п.3.4, окрім моніторингу та ідентифікації кіберзагроз, передбачає заходи, спрямовані на нейтралізацію інфраструктури зловмисників та захист державних і приватних комунікацій від неї. Водночас, Центром кібербезпеки Бельгії ССВ велася робота в напрямку розробки проактивних заходів кіберзахисту, концепція яких мала назву "Активна кібербезпека" ("Active Cybersecurity"). З прийняттям NIS2 на національному рівні згаданий підхід отримав назву "Active Cyber Protection" ACP та був описаний у відповідному документі [14]. При цьому, основними властивостями ACP визначено проактивність, релевантність (для споживача), партиципативність та автоматизованість, а проекти цієї програми згруповано навколо шістьох "стовпів" ("pillars"), серед яких ідентифікація та нейтралізація інфраструктур, що використовуються для здійснення кібератак, а також оперативні сповіщення про кіберзагрози.

Таким чином концепція активного кіберзахисту розглядається та імплементується багатьма країнами на стратегічному рівні як один із підходів до проактивної боротьби з кіберзагрозами в національних масштабах в режимі реального часу, заснований на поєднанні вивірених даних щодо кіберзагроз ("threat intelligence") та певних технологічних спроможностей.

Глосарій [15] Комітету національних систем безпеки США CNSS (функціонує у складі Агентства національної безпеки США NSA) містить таке визначення терміну "active cyber defense (ACD)": "*Synchronized, real-time capability to discover, detect, analyze, and mitigate threats and vulnerabilities*" (укр. "Синхронізована в реальному часі здатність виявляти, ідентифікувати, аналізувати та зменшувати вплив загроз і вразливостей").

В абзаці 57 директиви Європейського парламенту 2022/2555 від 14.12.2022 [2] термін "active cyber protection" розкривається як "*prevention, detection, monitoring, analysis and mitigation of network security breaches in an active manner, combined with the use of capabilities deployed within and outside the victim network*" (укр. "Запобігання, виявлення, моніторинг, аналіз та зменшення впливу наслідків порушень безпеки мережі активним способом, у поєднанні з використанням можливостей/засобів, розгорнутих як всередині, так і поза мережею об'єкта").

Водночас, в Законі України "Про основні засади забезпечення кібербезпеки України" надано такі визначення термінам "активна протидія агресії у кіберпросторі" та "система активної протидії агресії у кіберпросторі":

22) система активної протидії агресії у кіберпросторі - сукупність організаційних, правових, наукових та технічних заходів, спрямованих на підвищення рівня кіберзахисту держави шляхом здійснення впливу на інформаційні (автоматизовані), електронно-комунікаційні, інформаційно-комунікаційні системи держави-агресора, ***джерела походження*** *кіберзагроз та кібератак;*

23) активна протидія агресії у кіберпросторі - дії, спрямовані на підвищення рівня кіберзахисту шляхом ***нейтралізації кібератак*** *держави-агресора, його систем і мереж, а також* ***джерел походження*** *кіберзагроз та кібератак, які використовуються для завдання шкоди національній безпеці України;*".

Таким чином, термін "активний кіберзахист" або "активна протидія кіберзагрозам" потребує визначення, для чого доцільно більш детально розкрити його сутність та розробити (обґрунтувати) певні критерії.

Попри природну обмеженість публічної інформації щодо засобів і заходів забезпечення національної безпеки в кіберпросторі, доцільним є аналіз підходів різних країн до впровадження активного кіберзахисту. Такий досвід дозволяє більш повно окреслити критерії цього явища та запропонувати його визначення.

Програма "Active Cyber Defence" (ACD), що розвивається у Великобританії з 2017 року, покликана "*захистити більшість людей від більшості можливих негативних наслідків, що можуть бути спричинені більшістю кібератак протягом переважної більшості часу*". При цьому, ACD складається з трьох категорій безкоштовних безпекових сервісів, кожен з яких містить певний набір заходів та засобів:

1. Сервіси для самоперевірки (англ. "Self service checks")
    a. Перевірка стану кібербезпеки
        i. E-mail (DMARC)
        ii. IP-адреса
        iii. Веббраузер
    b. Перевірка DNS (англ. "DNS Check")
    c. Раннє інформування (англ. "Early Warning")
    d. Навчальні сценарії (англ. "Exercise in a Box")
    e. Перевірка поштової підсистеми (англ. "Mail Check")
    f. Перевірка вебресурсів (англ. "Web Check")
2. Засоби виявлення
    a. Програмний засіб для кінцевих точок (англ. "Host Based Capability")
    b. Сервіс DNS з функцією захисту (англ. "Protective DNS")
    c. Розкриття вразливостей (англ. "Vulnerability Disclosure")
3. Засоби запобігання та захисту
    a. Інформування про підозрілі електронні листи (англ. "Suspicious Email Reporting Service")
    b. Блокування шкідливих вебресурсів (англ. "Takedown Service")
    c. Поширення індикаторів кіберзагроз (англ. "Share and Defend Capability").

Слід зауважити, що частина сервісів інтегрована в платформу "MyNCSC" [17], яка є єдиною точкою входу для конфігурування та користування ними. Крім того, за період з 2018 по 2023 роки NSCS було опубліковано шість детальних звітів щодо результатів програми за кожним із сервісів та напрямів [18-23].

За результатами вивчення щорічних звітів, а також особливостей кожного з сервісів, очевидно, що захисні функції, в контексті протидії кіберзагрозам в режимі реального часу, щонайменше, притаманні технологічним спроможностям, які реалізують сервіс "Protective DNS" (функціонує на основі механізму RPZ [24]). Крім того, описаний функціонал сервісу раннього інформування забезпечує зворотній зв'язок користувачеві, надаючи контекстуалізовану інформацію про кіберзагрози, співставляючи IP-адресу(-и) ІКС споживача (яка, за умовами підключення, повинна бути статичною) та IP-адреси і доменні імена, класифіковані системою як індикатори кіберзагроз. Відтак, функціонування певних засобів захисту здійснюється на рівні DNS та TCP/IP.

Бельгійський підхід до "Active Cyber Protection" ACP також включає низку проектів, зокрема:

1. Бельгійський антифішинговий щит (англ "Belgian Anti-Phishing Shield, BAPS")
2. Проект для підвищення обізнаності Safeonweb
    a. BePhish
    b. Розширення для Інтернет-браузерів
3. Система раннього попередження (англ. "Early Warning System, EWS")
4. Набір контролів (англ. "CyberFundamentals").

Проект BAPS, серед іншого, передбачає реалізацію захисних функцій на рівні національного DNS в режимі реального часу та за участі провайдерів послуг інтернету (детально технологія не розкривається).

Інформування щодо безпекових подій та фактів виявлення кіберзагроз здійснюється за допомогою EWS, яка, у свою чергу, потребує реєстрації (автентифікація користувача здійснюється на основі eID "ItsMe") та ідентифікації активів організації: IP-адрес та доменних імен.

Стратегія кібербезпеки Фінляндії на 2024 - 2035 роки [16] висуває вимогу щодо національної готовності до активного кіберзахисту, можливості атрибуції та контрзаходів. Один із стовпів кіберстратегії, "Співпраця", передбачає розвиток та надання централізованих сервісів кібербезпеки державним сектором у партнерстві з приватним. Серед таких сервісів виділено HAVARO - децентралізовану систему для виявлення кіберзагроз та раннього інформування, функціонал якої, зокрема, реалізується технічними засобами класу IDS, та HYÖKY - сервіс для управління поверхнею атаки. Слід підкреслити, що HAVARO передбачає використання сенсорів у співпраці з приватними центрами управління безпекою (SOC), при чому апаратне забезпечення суб'єкт взаємодії повинен придбати самостійно. Водночас, інша інформація щодо технологічних спроможностей саме активної протидії кіберзагрозам в публічному доступі відсутня.

Отже, на підставі наведеної у статті інформації, а також враховуючи пункт 57 директиви NIS2, можна виділити такі властивості концепції "активного кіберзахисту":

- Базується на оборонній стратегії, має активний характер але виключає наступальні дії.
- Область дії виходить за межі ІКС конкретно взятої організації.
- Є сукупністю сервісів, що забезпечуються певними технологічними спроможностями.

– У відношенні кіберзагроз повинна забезпечувати:
  - ✓ моніторинг
  - ✓ виявлення
  - ✓ аналіз (контекстуалізація, зокрема – атрибуція)
  - ✓ запобігання (блокування)
  - ✓ поширення сповіщень (зворотній зв'язок).

Відповідно до законодавства України, кіберзагроза – *це "наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об'єктів"*, а для її виявлення (та реагування) використовуються показники (технічні дані) - індикатори кіберзагроз.

В класичному представлені для реалізації задуму зловмисник, з використанням технічних засобів та каналів зв'язку, так чи інакше взаємодіє з елементами ІКС об'єкта атаки на мережевому рівні. Крім того, у випадку застосування програмних засобів (в тому числі шкідливих), управління останніми також передбачає мережеву взаємодію відповідно до рівнів стеку протоколів TCP/IP. Таким чином, у контексті взаємодії технічних засобів суб'єкту та об'єкту кібератаки, для останнього джерело походження загрози може бути формалізовано у вигляді показників (технічних даних) відповідного інформаційного обміну, зокрема IP-адреси (і мережевого порта) та доменного імені. Відтак, вплив на джерела походження кіберзагроз з метою їх нейтралізації може полягати у запобіганні мережевій взаємодії (інформаційному обміну) між суб'єктом та об'єктом атаки на рівні протоколів IP та DNS, при цьому не передбачаючи впливу ні на фізичну особу (зловмисника), ні на використовуваний ним технічний засіб, виключаючи, в такий спосіб, будь-які наступальні дії.

Як відомо з попереднього аналізу досвіду інших країн, на рівні DNS таке запобігання мережевій взаємодії реалізується технологічними спроможностями у вигляді DNS-серверів з функцією захисту, як правило, на основі технології RPZ (Response Policy Zone). Таке технічне рішення є яскравим прикладом засобу активного кіберзахисту, що може бути застосований в національних масштабах.

Слід додати, що з метою створення передумов для раннього адресного інформування про кіберзагрози, виявлені та заблоковані в один з описаних способів, попередньо доцільно здійснити ідентифікацію ІКС організації-споживача сервісу (співставити IP-адреси та ідентифікатор організації), а індикатори кіберзагроз - контекстуалізувати, зазначивши, серед іншого, атрибуцію.

Висновки

Розвиток незалежного, вільного й процвітаючого суспільства неминуче зумовлюватиме подальшу цифровізацію світових економік та трансформацію способу життя населення.

Забезпечення стійкості інформаційних систем і телекомунікацій до негативного впливу, а також захист інтересів людини і громадянина в кіберпросторі вже сьогодні формують основу пріоритетів національної безпеки як України, так і міжнародної спільноти загалом.

У статті проаналізовано стратегії кібербезпеки Великобританії, Австралії, Японії, Латвії, Бельгії, Фінляндії та детально досліджено підходи згаданих країн до розвитку та впровадження національних засобів та способів протидії кіберзагрозам .

Визначено, що постійна еволюція програмних засобів реалізації кіберзагроз, а також удосконалення тактик, технік і процедур зловмисників у мирний та воєнний час зумовлюють не тільки очевидну необхідність регулярного перегляду ландшафту кіберзагроз, а й розвиток технологічних спроможностей для активної протидії, що формують фундамент активного кіберзахисту - концепцію, розвиток якої доцільно визначити однією з пріоритетних цілей стратегії кібербезпеки України на 2026 - 2031 роки.

На основі дослідження можна дійти висновку, що згадані технологічні спроможності мають становити комплекс заходів і засобів, здатних функціонувати у масштабах загальнодержавних інформаційно-комунікаційних систем у режимі реального часу, щонайменше, на рівні протоколів DNS та TCP/IP, інтегруючись із національними та регіональними телекомунікаційними мережами, водночас уникаючи створення єдиних точок відмови й надмірного навантаження на обладнання та канали зв'язку. При цьому, вхідними параметрами такої інформаційної системи є вивірені, контекстуалізовані технічні дані щодо кіберзагроз у вигляді індикаторів (зокрема, IP-адрес та доменних імен), що отримуються в процесі дослідження (розвідки) кіберзагроз (англ. "threat intelligence") [25].

Водночас, розвиток концепції активного кіберзахисту має ґрунтуватися на виключенні застосування наступальних дій, що забезпечує недопущення ескалації конфліктів, дотримання норм міжнародного законодавства, узгодженість із національними доктринами та збереження миру.

Список літератури

[1]. Указ Президента України "Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України" [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/447/2021.

[2]. 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) [Електронний ресурс]. Режим доступу: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng.

[3]. Закон України "Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури" [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/4336-20.

[4]. Denning, D.E. (2014) Framework and Principles for Active Cyber Defense. Computers & Security. 40, 108–113. doi:10.1016/j.cose.2013.11.004.

[5]. Dewar, Robert S (2017). Active Cyber Defense, Cyber Defense Trend Analysis, Center for Security Studies (CSS), ETH Zürich.

[6]. Закон України "Про основні засади забезпечення кібербезпеки України" [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19.

[7]. Закон України "Про оборону України" [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/1932-12.

[8]. 2023-2030 Australian Cyber Security Strategy [Електронний ресурс]. Режим доступу: https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy.pdf.

[9]. The Cybersecurity strategy of Latvia 2023-2026 [Електронний ресурс]. Режим доступу: https://www.mod.gov.lv/sites/mod/files/document/Kiberdrosibas%20strategija%202023%20ENG.pdf.

[10]. National Security Strategy of Japan (Provisional Translation) [Електронний ресурс]. Режим доступу: https://www.cas.go.jp/jp/siryou/221216anzenhoshou/nss-e.pdf.

[11]. National Cyber Security Strategy 2016-2021 [Електронний ресурс]. Режим доступу: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.

[12]. National Cyber Strategy 2022 [Електронний ресурс]. Режим доступу: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1053023/national-cyber-strategy-amend.pdf.

[13]. Cybersecurity Strategy Belgium 2.0 2021-2025 [Електронний ресурс]. Режим доступу: https://ccb.belgium.be/sites/default/files/2024-10/CCB_Strategie%202.0_UK_WEB.pdf.

[14]. Active Cyber Protection (ACP). Policy document [Електронний ресурс]. Режим доступу: https://ccb.belgium.be/sites/default/files/2024-10/ACP_Policy_Document_EN.pdf.

[15]. Committee on National Security Systems (CNSS) Glossary (CNSSI 4009) [Електронний ресурс]. Режим доступу: https://www.cnss.gov/CNSS/issuances/Instructions.cfm.

[16]. Finland's Cyber Security Strategy 2024-2035 [Електронний ресурс]. Режим доступу: https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/165893/VNK_2024_13.pdf.

[17]. MyNCSC [Електронний ресурс]. Режим доступу: https://www.ncsc.gov.uk/information/myncsc

[18]. Active Cyber Defence - One Year On [Електронний ресурс]. Режим доступу: https://web.archive.org/web/20180804004353/https://www.ncsc.gov.uk/content/files/protected_files/article_files/ACD%20-%20one%20year%20on_0.pdf.

[19]. Active Cyber Defence - The Second Year [Електронний ресурс]. Режим доступу: https://www.ncsc.gov.uk/files/Active%20Cyber%20Defence-The%20Second%20Year%20(2).pdf.

[20]. Active Cyber Defence: The Third Year [Електронний ресурс]. Режим доступу: https://www.ncsc.gov.uk/files/Active_Cyber_Defence_-_The_Third_Year.pdf.

[21]. Active Cyber Defence: The Fourth Year [Електронний ресурс]. Режим доступу: https://www.ncsc.gov.uk/files/Active-Cyber-Defence-ACD-The-Fourth-Year.pdf.

[22]. Active Cyber Defence – The Fifth Year [Електронний ресурс]. Режим доступу: https://www.ncsc.gov.uk/files/ACD-The-Fifth-Year-full-report.pdf.

[23]. Active Cyber Defence – The Sixth Year [Електронний ресурс]. Режим доступу: https://www.ncsc.gov.uk/files/ACD6-full-report.pdf.

[24]. DNS Response Policy Zones (RPZ) [Електронний ресурс]. Режим доступу: https://datatracker.ietf.org/doc/html/draft-vixie-dnsop-dns-rpz.

[25]. А. Жилін, Б. Ніколаєнко, О. Бакалинський, "Підвищення захищеності державних інформаційних ресурсів за рахунок застосування платформи Threat intelligence", Захист інформації, том 23, №3, липень-вересень 2021, 2021. - С. 136-146

УДК 004.738

Koval M. Active cyber protection concept in context of technical capabilities for cyber threats mitigation

Abstract. *Ensuring cybersecurity has been identified as one of the key priorities within the national security system of Ukraine, while cyberspace is regarded as a potential theater of warfare. The evolution of the cyber threat landscape and the advancement of tools used for their implementation, against the backdrop of rapid digitalization, have led to a significant increase in the speed of cyberattacks and, consequently, a reduction of the time permissible for effective response. This highlights the need for the implementation of proactive cybersecurity measures, limited strictly to non-offensive actions.*

The article provides an overview of the cybersecurity strategies of selected European and Asian countries, with a focus on their approaches to the development of active cyber protection and the application of related technological capabilities. Such an analysis makes it possible to identify international trends and explore the potential for their adaptation in the national context.

Special attention is given to approaches aimed at active counteraction to cyber threats based on preventing network communication between victim's device and attacker's infrastructure at the IP and DNS levels. The study also considers the scalability of such solutions, real-time reaction, contextualization of data, and the technical feasibility of generating cyber threat alerts (early warning messages).

Коваль Микола Васильович, фахівець Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України.

Koval Mykola, specialist at the State Cyber Security Center of the State Service for Special Communications and Information Protection of Ukraine.