Філософія, методологія, теорія та історія
основ національної безпеки держави

УДК 657

Котух Євген Володимирович
доктор наук з державного управління, кандидат технічних наук,
доцент, професор кафедри кібербезпеки
Національний технічний університет «Дніпровська політехніка»
Kotukh Yevgen
Doctor of Science in Public Administration, Candidate of Technical Sciences,
Associate Professor, Professor of Cybersecurity
Dnipro University of Technology
ORCID: 0000-0003-4997-620X

СВІТОВИЙ ДОСВІД ОРГАНІЗАЦІЇ КІБЕРРОЗВІДКИ ТА РОЗВІДКИ З КІБЕРЗАГРОЗ: ПРАКТИКА ТА ВИСНОВКИ ДЛЯ УКРАЇНИ
GLOBAL EXPERIENCE OF CYBER INTELLIGENCE ORGANIZATION AND INTELLIGENCE WITH CYBER THREATS: PRACTICE AND CONCLUSIONS FOR UKRAINE

Анотація. *Стаття присвячена дослідженню міжнародних норм і правил, що регулюють діяльність у сфері кіберрозвідки загроз інформаційній безпеці, структури кіберрозвідки країн-членів НАТО, США з метою імплементації в Україні кращих міжнародних практик для підвищення рівня кібербезпеки та захисту національних інтересів. Проаналізовано етапи розвитку кіберрозвідки загроз та наукові підходи вітчизняних та зарубіжних вчених щодо її дослідження. Аналіз міжнародного досвіду дозволив виявити взаємозв'язок між кібербезпекою і розвідкою кіберзагроз, оскільки кіберрозвідка загроз є невід'ємною частиною загальної стратегії забезпечення кібербезпеки враховуючи її*

розвідувальні та контррозвідувальні аспекти. Досліджено особливості структури систем кіберрозвідки США, НАТО та України, а також нормативні документи, які формують політику, стратегію та визначають повноваження державних органів у сфері кібербезпеки та кіберрозвідки. Проаналізовано динаміку змін національного індексу кібербезпеки (усереднений показник) країн-членів НАТО, США та України, оскільки за цим комплексним показником оцінюють загальний рівень кібербезпеки в країнах. На основі узагальнення результатів дослідження запропоновано впровадження низки заходів, спрямованих на підвищення ефективності взаємодії між суб'єктами національної системи кібербезпеки в контексті задач кіберрозвідки.

Вступ. В умовах інтеграції суспільства з цифровими технологіями кібербезпека є одним із пріоритетів у системі національної безпеки держави. Динамічний розвиток інформаційних технологій та їх конвергенція з технологіями штучного інтелекту впливають на зростання питомої ваги кіберзагроз інформаційній безпеці у сегменті загроз національній безпеці країн. Зростання такого впливу на функціонування структур управління як національних, так і міжнародних, формує абсолютно нову безпекову ситуацію з викликами нового технологічного рівня, з дедалі складнішим ландшафтом кіберрозвідки.

В той же час між світовими центрами сили відбувається боротьба за поділ сфер випливу та посилення своїх геополітичних позицій у кіберпросторі. Прогнозується зростання інтенсивності міждержавного протиборства і розвідувально-підривної діяльності у кіберпросторі; це знайде своє відображення у збільшенні кількості держав, які прагнутимуть створити і швидко розвинути власну кіберрозвідку та проактивно використовувати сучасні технології розвідувально-підривної діяльності у кіберпросторі. Війна росії проти України демонструє важливу роль інноваційних технологій та цифровізації процесів під час бойових дій.

Більшої актуальності набуває відокремлення сутностей кіберрозвідки та розвідки кіберзагроз (Cyber Threat Intelligence). Таким чином, тема дослідження є актуальною в контексті дослідження ролі та засобів кіберрозвідки, нормативно-регуляторного забезпечення кіберрозвідки та напрямів вдосконалення засобів та можливостей відповідальних державних органів, а також відокремлення сутностей кіберрозвідки та розвідки кіберзагроз в методологічному та практичному базисах застосування.

Мета. Мета дослідження полягає у вивченні міжнародних норм та правил, що регулюють діяльність у сфері кіберрозвідки, структури кіберрозвідки країн-членів НАТО, США для удосконалення існуючої структури в Україні та підвищення рівня кібербезпеки, захисту національних інтересів та забезпечення стабільності у цифровому світі.

Матеріали і методи. Матеріалами дослідження є: 1) нормативно-правове забезпечення щодо регулювання діяльності в сфері кібербезпеки та кіберрозвідки України, США та країн НАТО; 2) праці вітчизняних та зарубіжних авторів, що провадять свої науково-практичні дослідження у царині кібербезпеки в публічному просторі, забезпечення діяльності з кіберрозвідки, розвідки кіберзагроз та розвідки по відкритих джерелах.

В процесі здійснення дослідження було використано наступні наукові методи: теоретичного узагальнення та групування (для характеристики структури кіберрозвідки України, США та країн НАТО, складових взаємозв'язку кібербезпеки та розвідки кіберзагроз); формалізації, аналізу та синтезу (для побудови структурних схем державних органів з забезпечення функцій кіберрозвідки та формування інформації щодо витрати на забезпечення діяльності з кіберрозвідки в провідних країнах світу); логічного узагальнення результатів (формулювання висновків).

Результати. У науковій статті досліджено міжнародні норми і правила, що регулюють діяльність у сфері кіберрозвідки загроз

інформаційній безпеці, структури кіберрозвідки країн-членів НАТО, США з метою імплементації в Україні кращих міжнародних практик для підвищення рівня кібербезпеки та захисту національних інтересів у кіберпросторі. розкрито питання нормативно-регуляторного забезпечення органів кіберрозвідки на прикладі США. Визначено складові структури органів кіберрозвідки в Україні, США та країнах НАТО. З'ясовано місце витрат на кібербезпеку в національних бюджетах провідних країн світу. Виявлено взаємозв'язок між кібербезпекою та розвідкою кіберзагроз, оскільки розвідка кіберзагроз є невід'ємною частиною загальної стратегії забезпечення кібербезпеки враховуючи її розвідувальні та контррозвідувальні аспекти.

Перспективи. В подальших наукових дослідженнях пропонується зосередити увагу на пропозиціях щодо гармонізації законодавства з провідними країнами світу членами НАТО, імплементації досвіду, розробки та впровадженню методологічного забезпечення, що сприятиме підвищенню рівня кібербезпеки в Україні та захисту національних інтересів у цифровому світі. Варто зазначити, що з огляду на широке застосування поняття кіберрозвідка в контексті кібербезпеки актуальним науковим завданням залишається розгляд цього питання в контексті діяльності розвідувальних органів України.

Ключові слова: *розвідка кіберзагроз, кібербезпека, кіберрозвідка, індекс кібербезпеки, структура кіберрозвідки, кіберпростір.*

Summary. *Paper is dedicated to the study of international norms and rules regulating activities in the field of cyber intelligence of threats to information security, the structure of cyber intelligence of NATO member countries, the USA with the aim of implementing the best international practices in Ukraine to increase the level of cyber security and protect national interests. The stages of the development of cyber threat intelligence and the scientific approaches of*

domestic and foreign scientists to its research are analyzed. The analysis of international experience made it possible to reveal the relationship between cyber security and cyber threat intelligence, since cyber threat intelligence is an integral part of the overall strategy of ensuring cyber security, taking into account its intelligence and counter-intelligence aspects. The peculiarities of the structure of the cyber intelligence systems of the USA, NATO, and Ukraine, as well as regulatory documents that form policy, strategy, and determine the powers of state bodies in the field of cyber security and cyber intelligence, have been studied. The dynamics of changes in the national cyber security index (average indicator) of NATO member states, the USA and Ukraine were analyzed, since the overall level of cyber security in the countries is evaluated by this comprehensive indicator. Based on the generalization of the research results, it is proposed to implement a number of measures aimed at increasing the effectiveness of interaction between the subjects of the national cyber security system in the context of cyber intelligence tasks.

Introduction. In the context of the integration of society with digital technologies, cyber security is one of the priorities in the state's national security system. The dynamic development of information technologies and their convergence with artificial intelligence technologies affect the growth of the specific weight of cyber threats to information security in the segment of threats to the national security of countries. The growth of such influence on the functioning of both national and international governance structures creates a completely new security situation with challenges of a new technological level, with an increasingly complex cyber intelligence landscape.

At the same time, there is a struggle between the world's power centers to divide spheres of influence and strengthen their geopolitical positions in cyberspace. An increase in the intensity of interstate confrontation and intelligence-subversive activities in cyberspace is predicted; this will be reflected in an increase in the number of states that will seek to create and quickly develop

their own cyber intelligence and proactively use modern technologies of intelligence and subversive activities in cyberspace. Russia's war against Ukraine demonstrates the important role of innovative technologies and digitalization of processes during hostilities. The separation of the essences of cyber intelligence and cyber threat intelligence (Cyber Threat Intelligence) is becoming more relevant. Thus, the research topic is relevant in the context of researching the role and means of cyber intelligence, normative and regulatory support for cyber intelligence and directions for improving the means and capabilities of responsible state bodies, as well as separating the essences of cyber intelligence and cyber threat intelligence in the methodological and practical bases of application.

Purpose. The purpose of the study is to study the international norms and rules governing activities in the field of cyber intelligence, the structure of cyber intelligence of NATO member countries, the USA to improve the existing structure in Ukraine and increase the level of cyber security, protect national interests and ensure stability in the digital world.

Materials and methods. The materials of the study are: 1) regulatory and legal support for the regulation of activities in the field of cyber security and cyber intelligence of Ukraine, the USA and NATO countries; 2) works of domestic and foreign authors conducting scientific and practical research in the field of cyber security in the public space, providing cyber intelligence, cyber threat intelligence and open-source intelligence.

In the process of carrying out the research, the following scientific methods were used: theoretical generalization and grouping (to characterize the structure of cyber intelligence of Ukraine, the USA and NATO countries, components of the interconnection of cyber security and cyber threat intelligence); formalization, analysis and synthesis (for the construction of structural schemes of state bodies for the provision of cyber intelligence functions and the formation of information

on the costs of ensuring cyber intelligence activities in the leading countries of the world); logical generalization of results (formulation of conclusions).

Results. The scientific article examines the international norms and rules governing activities in the field of cyber-intelligence of threats to information security, the structure of cyber-intelligence of NATO member countries, the USA with the aim of implementing the best international practices in Ukraine to increase the level of cyber security and protect national interests in cyberspace. the issue of normative-regulatory support of cyber-intelligence bodies on the example of the USA is revealed. The constituent structures of cyber intelligence agencies in Ukraine, the USA and NATO countries have been determined. The place of spending on cyber security in the national budgets of the world's leading countries has been clarified. The relationship between cyber security and cyber threat intelligence has been revealed, as cyber threat intelligence is an integral part of the overall cyber security strategy, taking into account its intelligence and counter-intelligence aspects.

Discussion. In further scientific research, it is proposed to focus attention on proposals for the harmonization of legislation with the leading countries of the world by NATO members, implementation of experience, development and implementation of methodological support, which will contribute to increasing the level of cyber security in Ukraine and protecting national interests in the digital world. It is worth noting that considering the wide application of the concept of cyber intelligence in the context of cyber security, consideration of this issue in the context of the activities of the intelligence agencies of Ukraine remains an urgent scientific task.

Key words: *cyber threat intelligence, cyber security, cyber intelligence, cyber security index; structure of cyber intelligence, cyberspace.*

Постановка проблеми. В умовах інтеграції суспільства з цифровими технологіями кібербезпека є одним із пріоритетів у системі

національної безпеки держави. Динамічний розвиток інформаційних технологій та їх конвергенція з технологіями штучного інтелекту впливають на зростання питомої ваги кіберзагроз інформаційній безпеці у сегменті загроз національній безпеці країн. Зростання такого впливу на функціонування структур управління як національних, так і міжнародних, формує абсолютно нову безпекову ситуацію з викликами нового технологічного рівня, з дедалі складнішим ландшафтом кіберрозвідки.

В той же час між світовими центрами сили відбувається боротьба за поділ сфер випливу та посилення своїх геополітичних позицій у кіберпросторі. Прогнозується зростання інтенсивності міждержавного протиборства і розвідувально-підривної діяльності у кіберпросторі; це знайде своє відображення у збільшенні кількості держав, які прагнутимуть створити і швидко розвинути власну кіберрозвідку та проактивно використовувати сучасні технології розвідувально-підривної діяльності у кіберпросторі. Війна росії проти України демонструє важливу роль інноваційних технологій та цифровізації процесів під час бойових дій. Більшої актуальності набуває відокремлення сутностей кіберрозвідки та розвідки кіберзагроз (Cyber Threat Intelligence). Таким чином, тема дослідження є актуальною в контексті дослідження ролі та засобів кіберрозвідки, нормативно-регуляторного забезпечення кіберрозвідки та напрямів вдосконалення засобів та можливостей відповідальних державних органів, а також відокремлення сутностей кіберрозвідки та розвідки кіберзагроз в методологічному та практичному базисах застосування.

Аналіз останніх досліджень і публікацій. Перші наукові праці, які використовували термін "кіберрозвідка", з'явилися на початку 2000-х років. Вони були присвячені питанням збору та аналізу даних про кіберзагрози, методам виявлення атак та стратегії захисту. Зарубіжні дослідники розглядали дану проблематику переважно з позиції інструментів і методів розвідки з відкритих джерел (OSINT), тобто збір, оцінка, аналіз і

розповсюдження інформації з загальнодоступних джерел, таких як медіа (засоби масової інформації), соціальні мережі, форуми та блоги, для використання в цілях розвідки або як доказ для допомоги у внутрішніх розслідуваннях. Серед таких досліджень можна виділити праці С. Адамс (S. Adams) [1], С. Д. Гібсон (S.D. Gibson) [2], Н.А. Хасан (N.A. Hassan), & Р. Хіжазі (R. Hijazi) [3], Дж. Селянко (J. Selianko) [4], Х. Дж. Уільямс (H.J. Williams), & Блюм (Blum) [5].

Українські вчені досліджують кіберрозвідку переважно через призму кібербезпеки та кіберзахист у контексті національної безпеки. С. Петров [6] дослідив сучасні проблеми розбудови національної системи кібербезпеки України та обґрунтував посилення міжнародної співпраці і необхідність вдосконалення чинного законодавства в умовах зростання кількості й складності кіберзлочинів. Дослідження В. Шемчука [7] свідчать, що кібербезпека є пріоритетом не лише держав, а і їх регіональних об'єднань та світової спільноти в цілому. О. Козицька [8] дослідила кіберрозвідку на основі відкритих джерел як метод отримання криміналістично значимої інформації задля виконання завдань, спрямованих на виявлення, розкриття та розслідування кримінальних правопорушень, встановлення місцезнаходження розшукуваних осіб. Г. Піскорська та Н. Яковенко акцентують увагу на напрямах міжнародної взаємодії у кіберпросторі [9]. І. Доронін [10] наголошує на недосконалості термінологічної бази та необхідності законодавчого встановлення вимог до порядку звітування суб'єктів кібербезпеки. Праці І. Забара [11] присвячені напрямам міжнародно-правового регулювання інформаційної безпеки та кібербезпеки. Питання аудиту кібербезпеки в державних установах, кібербезпеки в публічному секторі, впливу кіберзлочинності, існуючі проблеми протидії та формування систем кібербезпеки в органах публічної влади присвячені роботи [12; 13; 14; 15; 16]. Разом з тим слід зазначити, що комплексного дослідження кіберрозвідки та визначення складових її

підсистем (Cyber Threat Intelligence, OSINT та інші), їх інституціонального складу та зв'язків між ними не проводилося.

Мета статті полягає у вивченні міжнародних норм та правил, що регулюють діяльність у сфері кіберрозвідки, структури кіберрозвідки країн-членів НАТО, США для удосконалення існуючої структури в Україні та підвищення рівня кібербезпеки, захисту національних інтересів та забезпечення стабільності у цифровому світі.

Матеріали і методи. Під час проведення дослідження використані загальнонаукові і спеціальні методи пізнання, а для з`ясування місця і ролі кіберрозвідки в системі кіберзахисту – метод структурно-функціонального аналізу. Історико-правовий метод використовувався для вивчення наукових праць, присвячених кіберрозвідці. Застосування методів аналізу та синтезу сприяло ефективному розробленню рекомендацій щодо організації взаємодії кіберрозвідки із суб'єктами національної системи кібербезпеки.

Виклад основного матеріалу. Кіберрозвідка загроз (Cyber Threat Intelligence) є важливим інструментом для захисту від сучасних кіберзагроз, допомагаючи державам бути більш проактивними в своєму підході до кібербезпеки загроз [17; 18]. Історія розвитку кіберрозвідки загроз є відносно новою порівняно з іншими видами розвідки, проте вона має свої важливі етапи та події (рис. 1).

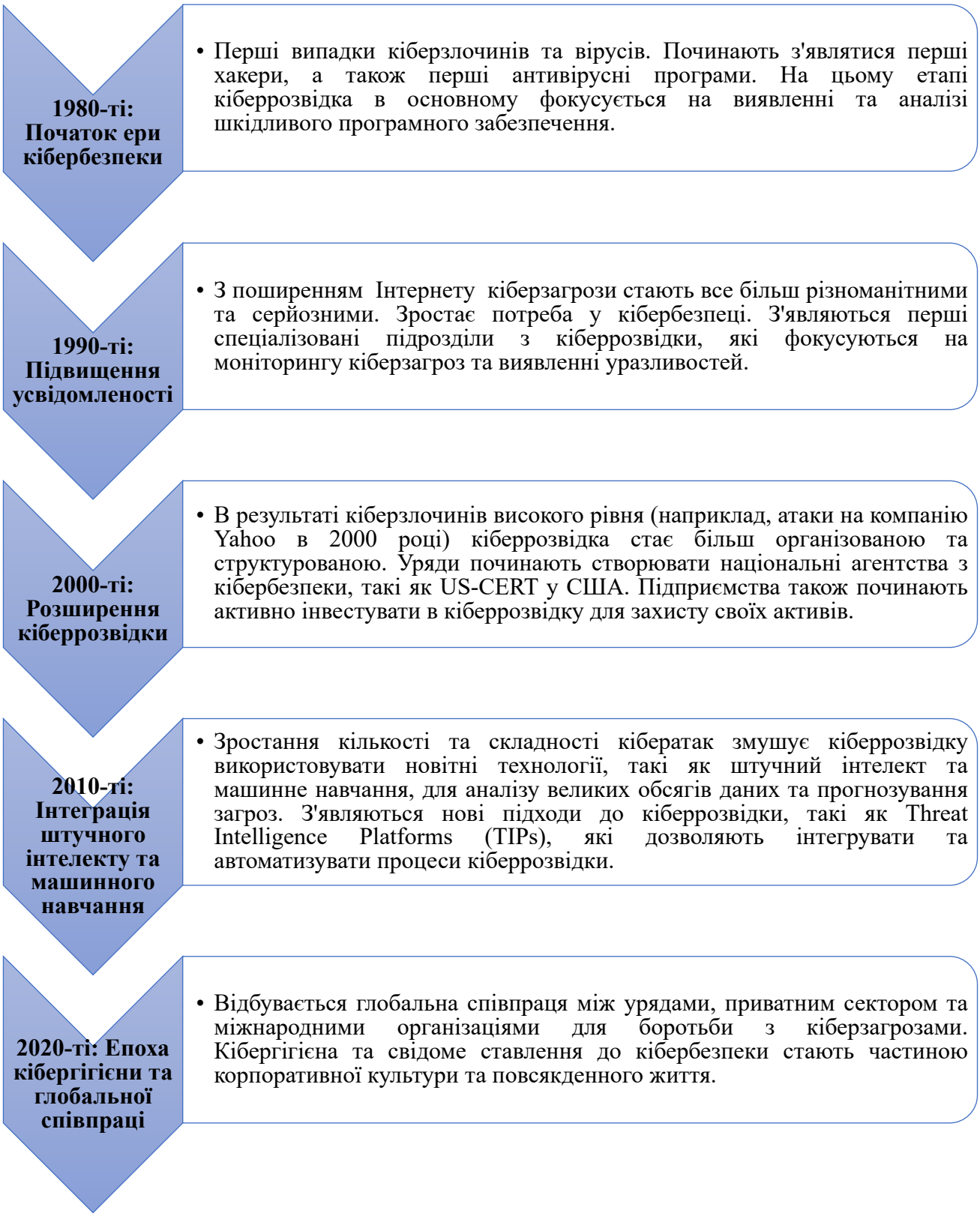

Рис. 1. Етапи розвитку кіберрозвідки загроз

Джерело: ілюстративна наукова пропозиція автора

Кіберрозвідка продовжує розвиватися, пристосовуючись до нових викликів та технологій. Вона стає важливим інструментом для запобігання, виявлення та реагування на кіберзагрози в сучасному цифровому світі на регіональному та національному рівнях та є елементом кібербезпеки [19; 20; 21]. Згідно з Законом України «Про основні засади забезпечення кібербезпеки України» [22] під кібербезпекою розуміють захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі, а кіберрозвідка визначається як діяльність, що здійснюється розвідувальними органами у кіберпросторі або з його використанням.

Для виявлення взаємозв'язку між цими сутностями Фондом академії електронного врядування Естонії розроблено і реалізується Національний індекс кібербезпеки (NCSI), а Глобальний індекс кібербезпеки (GCI) укладає Міжнародний союз електрозв'язку (МСЕ), він є ініціативою для зацікавлених сторін, спрямованою на підвищення обізнаності щодо кібербезпеки та вимірювання прихильності країн до кібербезпеки та її широкого застосування в різних галузях і секторах. Рівень розвитку кібербезпеки кожної країни аналізується за п'ятьма категоріями: правові заходи, технічні заходи, організаційні заходи, розбудова потенціалу та співробітництво. Зазначені індекси є комплексними показниками, що оцінюють рівень кібербезпеки країн і є тісно пов'язаними з розвідкою кіберзагроз, оскільки кіберрозвідка є невід'ємною частиною загальної стратегії забезпечення кібербезпеки.

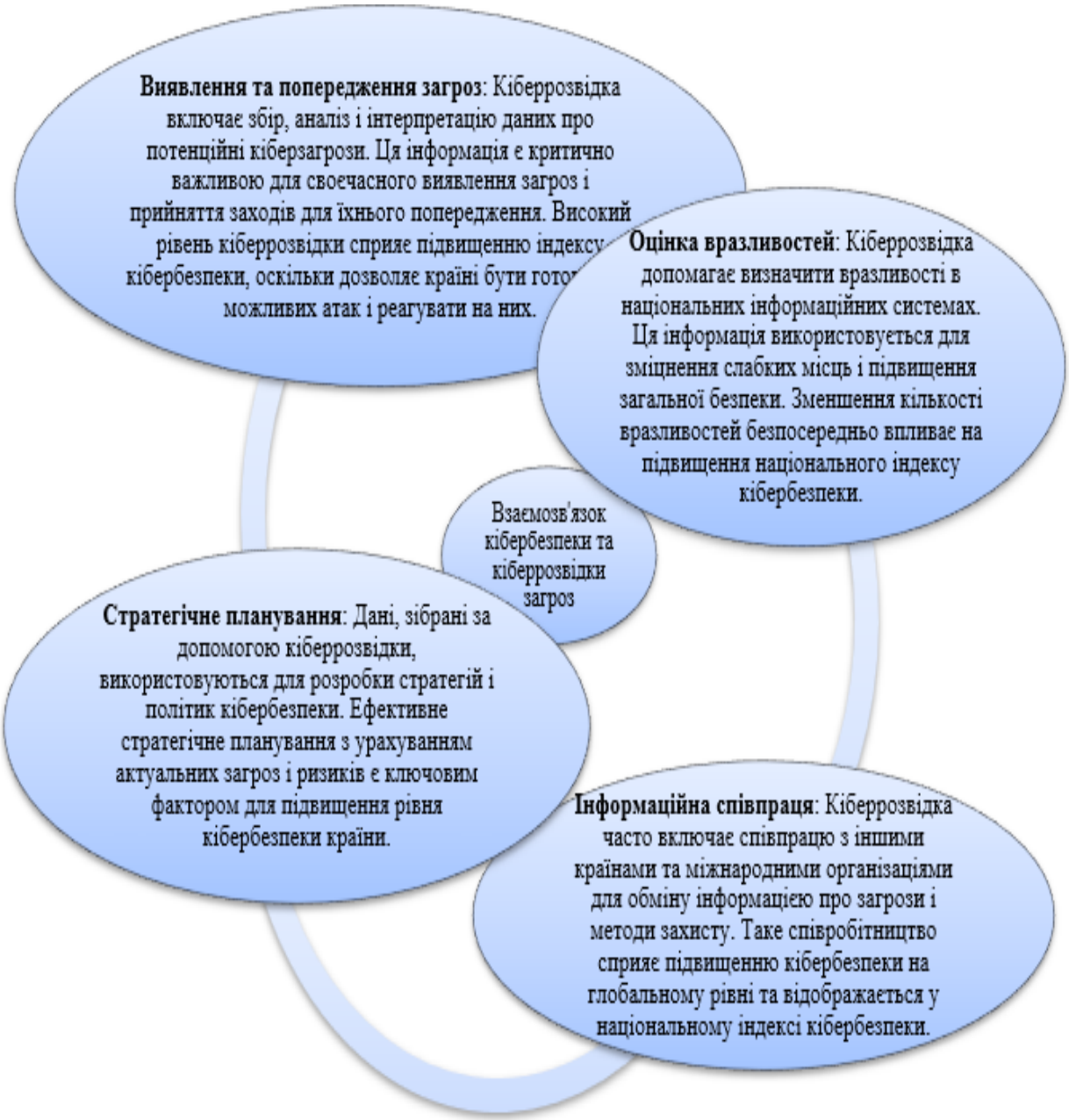

Рис. 2. Взаємозв'язок між кібербезпекою і кіберрозвідкою

Джерело: власна пропозиція автора

Взаємозв'язок між кібербезпекою і розвідкою кіберзагроз наведено на рис. 2.

На рис. 3 наведено динаміку національного індексу кібербезпеки (середній показник) по країнах-членах НАТО, США, Україні. США демонструють постійне покращення свого індексу кібербезпеки, що відображає посилені заходи та політику протидії кіберзагрозам. Ця

тенденція вказує на тверду прихильність підтримці та вдосконаленню національної системи кібербезпеки, в тому числі її інфраструктури. Показник країн НАТО демонструє зростання.

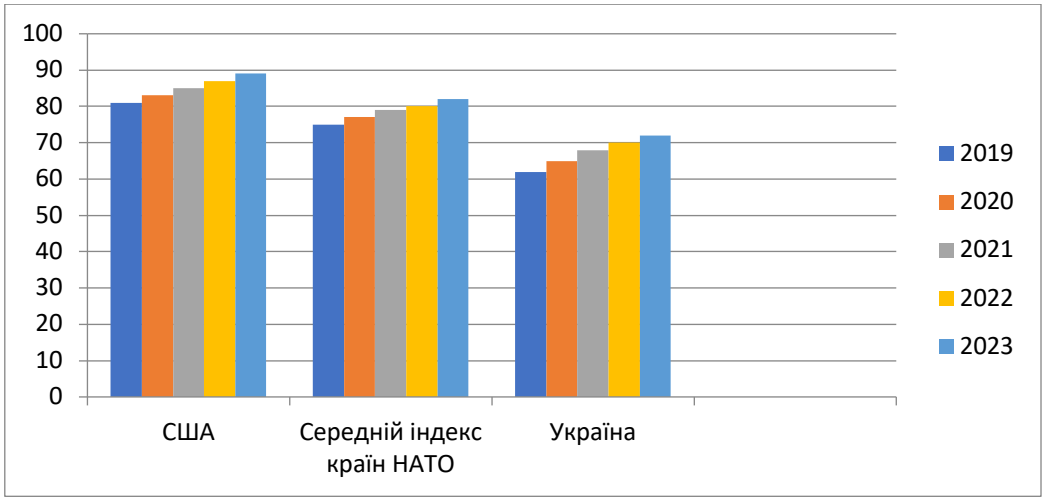

Рис. 3. Динаміка національного індексу кібербезпеки (середній показник)

Джерело: систематизовано автором на основі [23]

Зазначене свідчить про спільні зусилля держав-членів для зміцнення їх кіберзахисту, обміну найкращими практиками та посилення співпраці з метою ефективної протидії кіберзагрозам. Індекс України продемонстрував значне покращення функціонування національної системи кібербезпеки, що свідчить про стале впровадження нових заходів кібербезпеки та міжнародну підтримку, зокрема з боку НАТО, для посилення її кіберспроможності [24; 25].

Слід зазначити, що для забезпечення ефективності кіберрозвідки необхідне стабільне та достатнє фінансування, оскільки така діяльність потребує відповідного апаратного забезпечення, спеціалізованого програмного забезпечення, підтримки та постійного удосконалення системи моніторингу та аналізу даних, залучення та мотивації висококваліфікованих фахівців з кібербезпеки, аналітиків даних та інженерів програмного забезпечення тощо. Постійний розвиток технологій вимагає від фахівців з кіберрозвідки постійного професійного навчання та підвищення

кваліфікації. Також, відповідного фінансування вимагає проведення операцій з кіберрозвідки, включаючи витрати на зв'язок, ліцензії, підписки на інформаційні ресурси, інвестування у нові технології та методи захисту та атаки, що є необхідним для випередження кіберзлочинців.

Таблиця 1

Витрати на оборону для країн НАТО, США та України,

млрд. дол. США [26-29]

Країна	2019 р.	2020 р.	2021 р.	2022 р.	2023 р.
Сполучені Штати	721	738	755	801	860
Німеччина	52	55	59	64	68
Об'єднане Королівство	55	58	60	63	65
Франція	48	50	52	54	56
Україна	4.7	5.2	6.0	7.5	10

Джерело: систематизовано автором на основі [26-29]

Відомості щодо витрат на кіберрозвідку складно виокремити, водночас певні тенденції можна прослідкувати шляхом аналізу витрат на оборону для країн НАТО, США та України (табл. 1).

Країни НАТО зобов'язалися витрачати щонайменше 2 % свого ВВП на оборону, при цьому багато країн блоку збільшують свої бюджети у відповідь на геополітичну напруженість, потреби безпеки та зростання кількості та якості загроз у кіберпросторі. США збільшили витрати із 721 мільярда доларів у 2019 р. до 860 мільярдів доларів у 2023 р. Німеччина – з 52 мільярдів доларів у 2019 р. до 68 мільярдів доларів у 2023 р. Велика Британія – від 55 мільярдів доларів у 2019 р. до 65 мільярдів доларів у 2023 р. Франція – з 48 мільярдів доларів у 2019 р. до 56 мільярдів доларів у 2023 р.

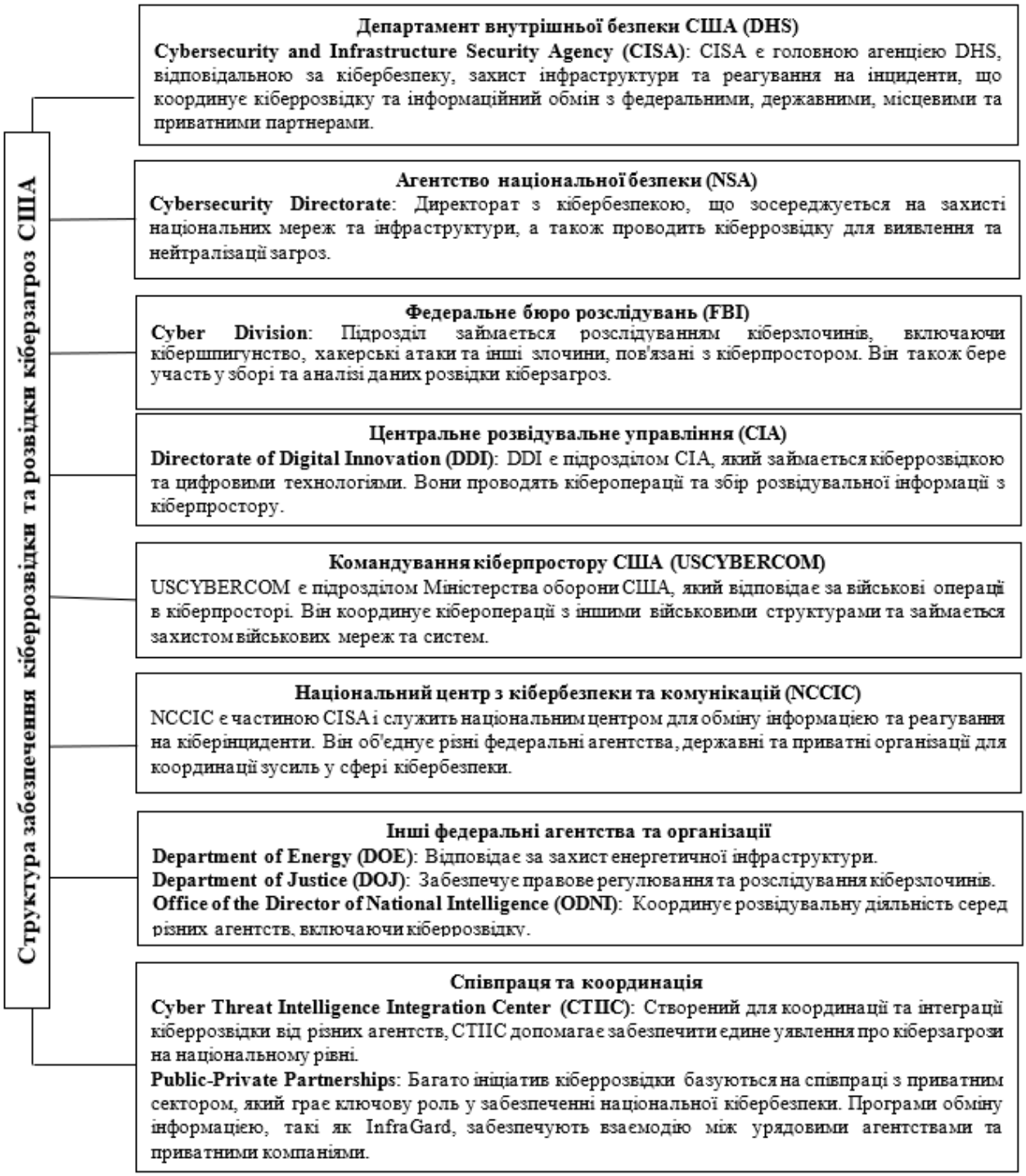

Рис. 4. Структура кіберрозвідки США

Джерело: ілюстративна наукова пропозиція автора

Витрати на оборону України через війну зросли з приблизно удвічі – з 4,7 мільярда доларів у 2019 р. до близько 10 мільярдів доларів США у 2023 р. [26-29].

Світові лідери вже сформували загальнодержавні системи кібербезпеки як найбільш оптимальні організаційні структури, які здатні в короткий проміжок часу акумулювати сили та засоби компетентних органів для протидії кіберзагрозам та проведення активних заходів щодо потенційних загроз в кіберрозвідки та розвідки з кіберзагроз США, країн-членів НАТО та України.

Таблиця 2

Нормативні документи, що регламентують кіберрозвідку США

Назва документу	Зміст
Homeland Security Act (2002)	Цей закон створив Департамент внутрішньої безпеки США (DHS) та надав йому широкі повноваження у сфері захисту національної інфраструктури, включаючи кібербезпеку. Закон також передбачає створення Національного центру з кібербезпеки та комунікацій (NCCIC).
Federal Information Security Management Act (FISMA) (2002, оновлений у 2014)	Закон встановлює вимоги до захисту інформаційних систем федеральних агентств, включаючи вимоги до управління ризиками та забезпечення безпеки інформаційних систем.
Cybersecurity Information Sharing Act (CISA) (2015)	Закон сприяє обміну інформацією про кіберзагрози між приватним сектором і урядом, створюючи правову основу для захисту компаній, що надають таку інформацію, від юридичної відповідальності.
National Defense Authorization Act (NDAA)	Щорічний закон про оборонний бюджет часто включає положення щодо кібербезпеки та кібероперацій, надаючи Міністерству оборони США (DoD) та іншим агентствам конкретні повноваження у сфері кіберзахисту та кіберрозвідки.
Executive Order 13636 "Improving Critical Infrastructure Cybersecurity" (2013)	Указ президента США, який встановлює політику щодо захисту критичної інфраструктури від кіберзагроз та покладає на федеральні агентства завдання з розробки та впровадження стандартів кібербезпеки.
Executive Order 13800 "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure" (2017)	Указ спрямований на підвищення кібербезпеки федеральних мереж та критичної інфраструктури, включаючи вимоги до оцінки ризиків та покращення механізмів обміну інформацією.
National Cyber Strategy (2018)	Стратегія визначає національні пріоритети та напрямки політики США у сфері кібербезпеки, включаючи захист критичної інфраструктури, зміцнення кібервідповідальності та розвиток міжнародного співробітництва.
Department of Defense Cyber Strategy (2018)	Стратегія Міністерства оборони США щодо кібероперацій та кіберзахисту, включаючи оборону національних мереж, розробку кіберздатностей та підготовку до кіберконфліктів.
NIST Cybersecurity Framework	Рамкова методика кібербезпеки, розроблена Національним інститутом стандартів і технологій (NIST). Вона включає стандарти, керівні принципи та кращі практики для управління ризиками кібербезпеки.
Federal Risk and Authorization Management Program (FedRAMP)	Програма стандартизує підхід до забезпечення безпеки хмарних сервісів, що використовуються федеральними агентствами, забезпечуючи спільні вимоги до кібербезпеки та процедури авторизації.
National Institute of Standards and Technology (NIST) Special Publications (SP)	Серія публікацій, які надають рекомендації та стандарти щодо різних аспектів кібербезпеки, включаючи управління ризиками, захист інформаційних систем.

Джерело: складено автором, ілюстративна наукова пропозиція автора

Рис. 5. Структура кіберрозвідки та розвідки з кіберзагроз країн-членів НАТО

Джерело: ілюстративна наукова пропозиція автора

У Сполучених Штатах кіберрозвідка регламентується низкою нормативних документів, які визначають політику, стратегію та обов'язки різних державних органів у сфері кібербезпеки та кіберрозвідки (табл. 2).

Так, структура кіберрозвідки та розвідки з кіберзагроз США є багаторівневою та охоплює кілька ключових організацій та агентств, які співпрацюють для забезпечення національної кібербезпеки. На Рис. 4 наведено основні компоненти цієї багаторівневої структури, що дозволяє США ефективно виявляти, аналізувати та реагувати на кіберзагрози, забезпечуючи захист національних інтересів та інфраструктури.

Ці нормативні документи забезпечують комплексний підхід до регулювання кіберрозвідки та кібербезпеки в США, встановлюючи правові та процедурні рамки для захисту національних інтересів у кіберпросторі.

Структура кіберрозвідки країн-членів НАТО є складною та багаторівневою, оскільки кожна країна має власні організації та підрозділи, відповідальні за кібербезпеку та кіберрозвідку. Проте, існують загальні риси та спільні структури, які забезпечують координацію між країнами-членами. Основні компоненти кіберрозвідки країн НАТО включають національні кіберрозвідувальні агентства, військові підрозділи, а також міжнародні організації НАТО, які сприяють співпраці та обміну інформацією (рис. 5).

Структура кіберрозвідки та розвідки з кіберзагроз країн-членів НАТО є гнучкою та децентралізованою, що дозволяє кожній країні розробляти власні підходи до кібербезпеки, одночасно співпрацюючи в рамках НАТО для забезпечення загального захисту від кіберзагроз.

Структура кіберрозвідки та розвідки з кіберзагроз в Україні складається з кількох ключових організацій та відомств, які співпрацюють для забезпечення кібербезпеки країни, та зв'язків між ними. Основні компоненти цієї структури включають державні органи, військові підрозділи та спеціалізовані агентства. Нижче наведено основні елементи структури кіберрозвідки в Україні (рис. 6).

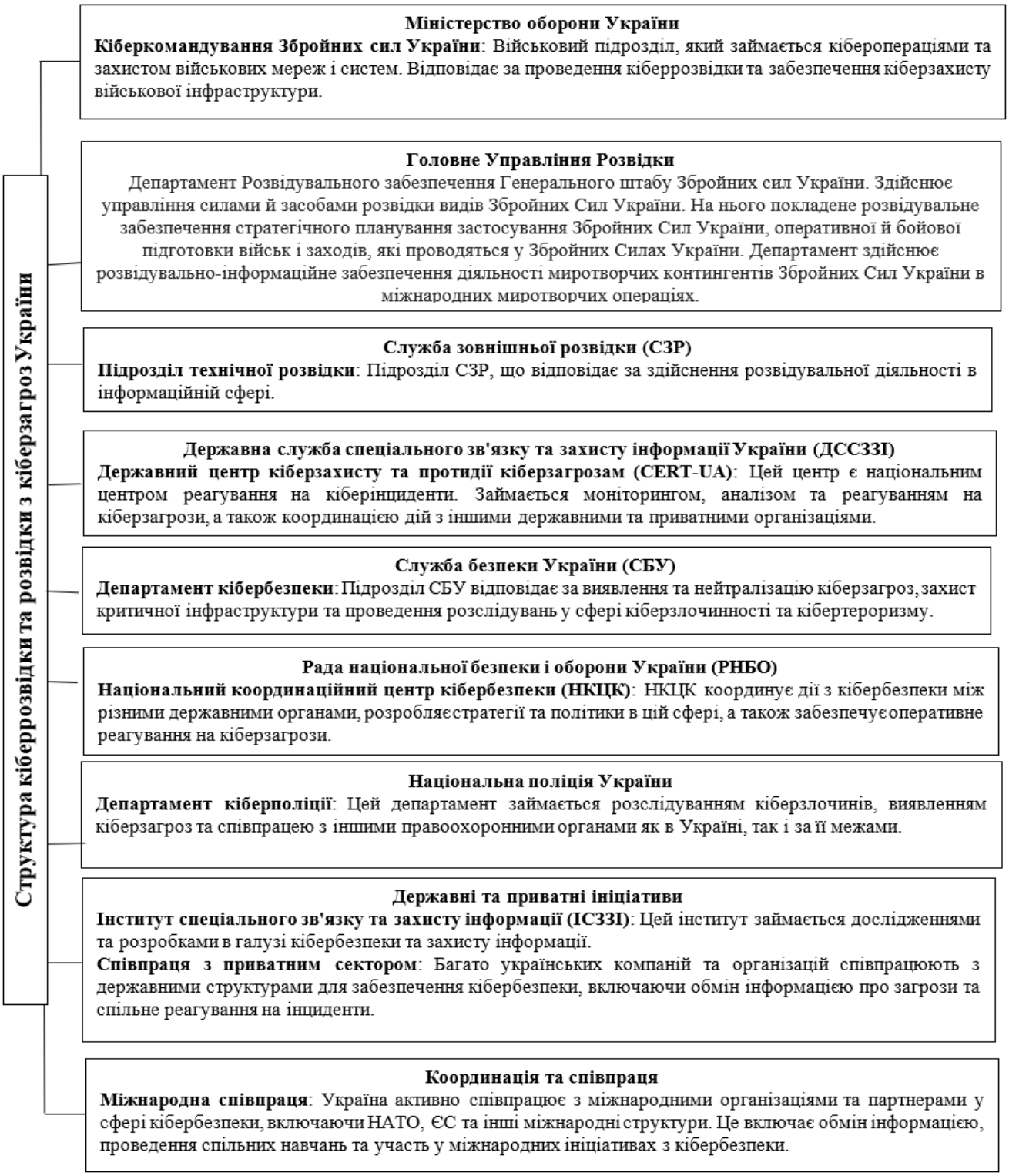

Рис. 6. Структури кіберрозвідки та розвідки з кіберзагроз в Україні

Джерело: ілюстративна наукова пропозиція автора

Ця структура є важливою складовою функціонування національної система кібербезпеки, яка включає сукупність суб'єктів забезпечення кібербезпеки та взаємопов'язаних заходів політичного, науково-технічного, інформаційного, освітнього характеру, організаційних, правових, оперативно-розшукових, розвідувальних, контррозвідувальних, оборонних, інженерно-технічних заходів, а також заходів криптографічного і технічного захисту національних інформаційних ресурсів, кіберзахисту об'єктів критичної інформаційної інфраструктури.

Висновки і перспективи подальших досліджень. На підставі проведеного дослідження слід зазначити, що розвиток сучасних інформаційних технологій зумовлює необхідність постійного удосконалення функціонування кіберрозвідки та розвідки з кіберзагроз. Відокремлення цих двох сутностей в США та інших країнах НАТО зумовлено структурою та нормативно-законодавчим забезпеченням. З огляду на завдання приведення структури та методів роботи у відповідність до стандартів НАТО, впровадження сучасних технологій, гармонізація підходів до збору, аналізу та захисту інформації, виявлення загроз в кіберпросторі, посилення технічних видів розвідки та розширення можливостей кіберрозвідки, що зумовлені геополітичною ситуацією, вимогами до членства НАТО, глобальними викликами, досвідом повномасштабної агресії російської федерації та внутрішніми реформами розвідувальних органів такий підхід відображає сучасний стан та напрями подальшого вдосконалення органів відповідальних за заходи з кіберрозвідки та розвідки кіберзагроз одночасно. Війна росії проти України вимагає якнайшвидше поглибити співпрацю з міжнародними організаціями, такими як НАТО та ЄС, для обміну передовими практиками та інформацією, активізувати спільні навчання та тренінги з міжнародними партнерами. У цьому контексті особливої уваги слід надати кадровому забезпеченню, а саме – створити освітні програми у співпраці з провідними світовими

університетами та навчальними закладами з цього напрямку. Забезпечити фахівців сучасним програмним та апаратним забезпеченням для збору, аналізу та моніторингу кіберзагроз, що вимагає залучення інвестицій в розробку та впровадження нових технологій для випередження кіберзлочинців, а також включити витрати на кіберрозвідку у національний бюджет з чітким виділенням коштів, враховуючи досвід США та країн-членів НАТО.

Необхідним є розвиток національної системи обміну інформацією про кіберзагрози між державними органами, приватним сектором та міжнародними партнерами. Україні також доцільно використовувати індекси кібербезпеки для аналізу прогресу та коригування стратегії у разі необхідності.

Впровадження цих пропозицій сприятиме підвищенню рівня кібербезпеки в Україні та захисту національних інтересів у цифровому світі. Варто зазначити, що з огляду на широке застосування поняття кіберрозвідка в контексті кібербезпеки актуальним науковим завданням залишається розгляд цього питання в контексті діяльності розвідувальних органів України.

Література

1. Adams S. An introduction to OSINT and III. 2020. URL: https://www.intelligencewithsteve.com/post/an-introduction-to-osint-and-iii (дата звернення: 28.06.2024).

2. Gibson S.D. Open Source Intelligence (OSINT): a contemporary intelligence lifeline: *PhD Tesis.* Cranfield University. 2007. URL: https://www.scribd.com/document/552940969/2007-OPEN-SOURCE-INTELLIGENCE-a-Contemporary-Intelligence-Lifeline (дата звернення: 28.06.2024).

3. Hassan N.A., Hijazi R. Open Source Intelligence Methods and Tools. 2018. doi: https://doi.org/10.1007/978-1-4842-3213-2_1.

4. Selianko J. NATO Open Source Intelligence Handbook. 2001. URL: https://archive.org/details/NATOOSINTHandbookV1.2/mode/2up (дата звернення: 28.06.2024).

5. Williams H.J., Blum I. Defning Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise. 2018. doi: https://doi.org/10.7249/RR1964.

6. Петров С. Розбудова національної системи кібербезпеки України як необхідний елемент розвитку інформаційного суспільства. *Вісник ХНУВС.* 2021. № 4 (95). С. 146-156.

7. Шемчук В. В. Основні напрямки міжнародного співробітництва у сфері кібербезпеки. *Вчені записки. Серія : Юридичні науки. Кримінальне право та кримінологія ; кримінально-виконавче право.* 2018. Т. 29(68), № 2. С. 125-129.

8. Козицька О. Загальна характеристика кіберрозвідки на основі відкритих джерел як методу отримання криміналістично значущої інформації. *Baltic Journal of Legal and Social Sciences.* 2021. № 3. С. 91-98.

9. Піскорська Г. А., Яковенко Н. Л. Сучасні виклики і загрози в кіберпросторі: формування механізму міжнародної інформаційної безпеки. *International relations, part «Political science».* 2018. № 18-19(2). URL: https://cutt.ly/GQCBYfV (дата звернення: 28.06.2024).

10. Доронін І. М. Організація звітування суб'єктів кібербезпеки. *Актуальні проблеми управління інформаційною безпекою держави : зб. тез наук. доп. наук.-практ. конф.* Київ : Нац. акад. СБУ, 2019. URL: https://cutt.ly/5QCBPIq (дата звернення: 28.06.2024).

11. Забара І. М. Кібернетична безпека держави в умовах розвитку штучного інтелекту: до питання визначення напрямків міжнародно-правового регулювання. *Актуальні проблеми управління інформаційною*

безпекою держави : зб. тез наук. доп. наук.-практ. конф. Київ : Нац. акад. СБУ, 2019. URL: http://academy.ssu.gov.ua/upload/file/konf_04_04_2019.pdf (дата звернення: 28.06.2024).

12. Аудит інформаційної безпеки як необхідна складова управління в державних установах. URL: http://db.kh.ua/index.php/db/article/view/1176 (дата звернення: 28.06.2024).

13. Котух Є.В. Кібербезпека у публічному секторі : монографія. Харків : Колегіум, 2021. 271 с.

14. Kotukh Y. V., Kislov D. V., Yarovoi T. S., Kotsiuba R. O., Bondarenko O. H. Cybercrime and subculture of cybercriminals. *Linguistics and Culture Review*. 2021. *5*(S4). P. 858-869. doi: https://doi.org/10.21744/lingcure.v5nS4.1769.

15. Котух Є. Кіберзброя: проблеми та перспективи протидії кіберзлочинності. *ЗС: зовнішні справи.* 2012. URL: http://www.uaforeignaffairs.com/en/expert-opinion/view/article/kiberzbroja-problemi-ta-perspektivi-protidiji-kiberzlo (дата звернення: 28.06.2024).

16. Котух Є. В. Формування систем кібербезпеки в органах публічної влади. *Державне управління: удосконалення та розвиток.* 2020. № 3.

17. Котух Є.В. Основні виклики врядування у сфері кібербезпеки. *Теорія та практика державного управління.* 2020. № 4 (71). С. 38-46.

18. Котух Є.В. Теоретико-методологічна модель розробки національної стратегії кібербезпеки. *Наукові перспективи.* 2021. № 6 (12). С. 39-52.

19. Котух Є.В. Особливості національної та регіональної політики у сфері кібербезпеки. *Теорія та практика державного управління.* 2019. № 4(67). С. 40-47.

20. Котух Є.В. Проблеми кібербезпеки в сучасному світі. *Актуальні проблеми державного управління.* 2019. № 2(56). С. 33-38.

21. Котух Є.В. Особливості забезпечення кібербезпеки в публічному секторі в умовах глобалізації. *Державне будівництво.* 2019. № 2. URL: http://db.journal.kharkiv.ua/index.php/db/article/view/65/60 (дата звернення: 28.06.2024).

22. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 28.06.2024).

23. National Cyber Security Index. URL: https://ncsi.ega.ee/ncsi-index/; https://www.itu.int/pub/D-STR-GCI.01 (дата звернення: 28.06.2024).

24. NATO's role in cyberspace. URL: https://www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.html (дата звернення: 28.06.2024).

25. Statement of the NATO-Ukraine Commission. URL: https://www.nato.int/cps/en/natohq/official_texts_170408.htm (дата звернення: 28.06.2024).

26. Defence Expenditures of NATO Countries (2014-2022). URL: https://www.nato.int/cps/en/natohq/news_197050.htm (дата звернення: 28.06.2024).

27. NATO Spending by Country 2024. URL: https://worldpopulationreview.com/country-rankings/nato-spending-by-country (дата звернення: 28.06.2024).

28. Defence Expenditure of NATO Countries (2014-2021). URL: https://www.nato.int/cps/en/natohq/news_184844.htm (дата звернення: 28.06.2024).

29. Defence expenditures and NATO's 2 % guideline. URL: https://www.nato.int/cps/en/natohq/topics_49198.htm?selectedLocale=tk (дата звернення: 28.06.2024).

References

1. Adams, S. (2020). An introduction to OSINT and III. Retrieved from https://www.intelligencewithsteve.com/post/an-introduction-to-osint-and-iii.

2. Gibson, S.D. (2007). Open Source Intelligence (OSINT): a contemporary intelligence lifeline: *PhD Thesis.* Cranfield University. Retrieved from https://www.scribd.com/document/552940969/2007-OPEN-SOURCE-INTELLIGENCE-a-Contemporary-Intelligence-Lifeline.

3. Hassan, N.A., & Hijazi, R. (2018). Open Source Intelligence Methods and Tools. doi: https://doi.org/10.1007/978-1-4842-3213-2_1.

4. Selianko, J. (2001). NATO Open Source Intelligence Handbook. Retrieved from https://archive.org/details/NATOOSINTHandbookV1.2/mode/2up.

5. Williams, H.J., & Blum, I. (2018). Defning Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise. doi: https://doi.org/10.7249/RR1964.

6. Petrov, S. (2021). Development of the national cyber security system of Ukraine as a necessary element of the development of the information society. *Visnyk KhNUVS – Bulletin of KhNUIA.* No. 4 (95). P. 146-156 [in Ukrainian].

7. Shemchuk, V. V. (2018). Main directions of international cooperation in the field of cyber security. *Scientific notes. Series: Legal sciences. Criminal law and criminology; criminal executive law.* Vol. 29(68), No. 2. P. 125-129 [in Ukrainian].

8. Kozytska, O. (2021). General characteristics of cyber intelligence based on open sources as a method of obtaining forensically significant information. *Baltic Journal of Legal and Social Sciences.* No. 3. P. 91-98 [in Ukrainian].

9. Piskorska, G. A., & Yakovenko, N. L. (2018). Modern challenges and threats in cyberspace: formation of the mechanism of international information security. *International relations, part "Political science".* No. 18–19(2). URL: https://cutt.ly/GQCBYfV [in Ukrainian].

10. Doronin, I. M. (2019). Organization of reporting of cyber security subjects. *Actual problems of state information security management: Coll. theses of sciences add. science and practice conf.* Kyiv: National. Acad. SBU. URL: https://cutt.ly/5QCBPIq [in Ukrainian].

11. Zabara, I. M. (2019). Cybernetic security of the state in the conditions of the development of artificial intelligence: to the issue of determining the directions of international legal regulation. *Actual problems of state information security management: coll. theses of sciences add. science and practice conf.* Kyiv: National. Acad. SBU. URL: http://academy.ssu.gov.ua/upload/file/konf_04_04_2019.pdf [in Ukrainian].

12. Audit of information security as a necessary component of management in state institutions. URL: http://db.kh.ua/index.php/db/article/view/1176.

13. Kotukh, E.V. (2021). Cyber security in the public sector: monograph. Kharkiv: Collegium [in Ukrainian].

14. Kotukh, Y.V., Kislov, D.V., Yarovoi, T.S., Kotsiuba, R.O., & Bondarenko, O.H. (2021). Cybercrime and subculture of cybercriminals. *Linguistics and Culture Review.* No. 5 (S4). P. 858-869. doi: https://doi.org/10.21744/lingcure.v5nS4.1769.

15. Kotukh, Y. (2012). Cyber weapons: problems and prospects of countering cybercrime. *Ministry of Foreign Affairs: foreign affairs.* URL: https://uaforeignaffairs.com/en/journal-item/23 [in Ukrainian].

16. Kotukh, Y.V. (2020). Formation of cyber security systems in public authorities." *Public Administration: Improvement and Development.* No. 3 [in Ukrainian].

17. Kotukh, Y.V. (2020). The main challenges of governance in the field of cyber security. *Theory and practice of public administration.* No. 4 (71). P. 38-46 [in Ukrainian].

18. Kotukh, Y.V. (2021). Theoretical and methodological development model of the national cyber security strategy. *Scientific prospects.* No. 6 (12). P. 39-52 [in Ukrainian].

19. Kotukh, Y.V. (2019). Peculiarities of national and regional policy in the field of cyber security. *Theory and practice of public administration.* No. 4(67). P. 40-47.

20. Kotukh, Y.V. (2019). Problems of cyber security in the modern world. *Actual problems of public administration.* No. 2(56). P. 33-38 [in Ukrainian].

21. Kotukh, Y.V. (2019). Peculiarities of ensuring cyber security in the public sector in the conditions of globalization. *State construction*. No. 2 [in Ukrainian].

22. On the main principles of ensuring cyber security of Ukraine: Law of Ukraine dated 05.10.2017 No. 2163. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text [in Ukrainian].

23. National Cyber Security Index. URL: https://ncsi.ega.ee/ncsi-index/; https://www.itu.int/pub/D-STR-GCI.01.

24. NATO's role in cyberspace. URL: https://www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.html (date of access: 28.06.2024).

25. Statement of the NATO-Ukraine Commission. URL: https://www.nato.int/cps/en/natohq/official_texts_170408.htm.

26. Defense Expenditures of NATO Countries (2014-2022). URL: https://www.nato.int/cps/en/natohq/news_197050.htm.

27. NATO Spending by Country 2024. URL: https://worldpopulationreview.com/country-rankings/nato-spending-by-country.

28. Defense Expenditure of NATO Countries (2014-2021). URL: https://www.nato.int/cps/en/natohq/news_184844.htm.

29. Defense expenditures and NATO's 2% guideline. URL:

https://www.nato.int/cps/en/natohq/topics_49198.htm?selectedLocale=tk.