№ 11(25) 2023
НАУКА і ТЕХНІКА СЬОГОДНІ
серії: право, економіка, педагогіка, техніка, фізико-математичні науки

УДК [001.8/.816/.817] + 001.92 + [371.315.5/.315.6/.335] +655.52

https://doi.org/10.52058/2786-6025-2023-11(25)-678-689

Козубцов Ігор Миколайович доктор педагогічних наук, кандидат технічних наук, старший науковий співробітник, професор кафедри Бойового застосування підрозділів зв'язку, Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, вул. Князів Острозьких, 45/1, м. Київ, 01011, тел.: (063)404-84-41https://orcid.org/0000-0002-7309-4365

Ткач Володимир Олександрович старший науковий співробітник науково-дослідного відділу (комплексних систем захисту інформації в інформаційно-телекомунікаційних системах) науково-дослідного управління (проблем захисту інформації) Наукового центру зв'язку та інформатизації, Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, вул. Князів Острозьких, 45/1, м. Київ, 01011, тел.: (098) 395-38-98, https://orcid.org/0000-0003-0013-7368

Глобін Андрій Вікторович науковий співробітник науково-дослідного відділу (технічного забезпечення засобів зв'язку та автоматизації) науково-дослідного управління (розвитку військ зв'язку) Наукового центру зв'язку та інформатизації, Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, вул. Князів Острозьких, 45/1, м. Київ, 01011, тел.: (095) 160-99-10, https://orcid.org/0000-0001-5335-6869

Фомкін Денис Валентинович молодший науковий співробітник науково-дослідного відділу (комплексних систем захисту інформації в інформаційно-телекомунікаційних системах) науково-дослідного управління (проблем захисту інформації) Наукового центру зв'язку та інформатизації, Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, вул. Князів Острозьких, 45/1, м. Київ, 01011, тел.: (050) 330-38-33, https://orcid.org/0000-0003-0128-9355

УПОВНОВАЖЕННЯ ОРГАНІВ СЕКТОРУ БЕЗПЕКИ ТА ОБОРОНИ НА ОРГАНІЗАЦІЮ ТА ПРОВЕДЕННЯ ЗАХОДІВ З КІБЕРДОРОЗВІДКИ

Анотація. У гібридній війні перемагає та сторона, яка першою створює умови, необхідні для порушення цільових функцій кібербезпеки систем захисту інформації та критичної інформаційної інфраструктури. Створення передумов для порушення цільової функції потребує попереднього виявлення вразливостей у системах захисту інформації та кібербезпеки об'єктів критичної

інформаційної інфраструктури противника. Це завдання виконується під час проведення кібердорозвідки. Тривалий час поняття кібердорозвідки було відсутнє в науковому середовищі, але така діяльність вже здійснювалася в контексті кіберрозвідки. Лише у 2021 році на законодавчому рівні кібердорозвідку було визначено як діяльність, спрямовану на виявлення вразливостей у програмному забезпеченні, телекомунікаційному обладнанні, автоматизованих системах управління військами, зброєю та/або технічними процесами конкретного об'єкта (об'єктів кіберінфраструктури). Предметом дослідження у науковій статті є обґрунтування адміністративно-правових засад організації кібердорозвідки. Метою цієї статті є висвітлення адміністративно-правової бази, що дозволяє органам сектору безпеки та оборони організовувати діяльність з кібердорозвідки в умовах гібридної війни. Для досягнення поставленої мети і завдань використано такі теоретичні методи дослідження: узагальнення наукової літератури, структурно-генетичний аналіз для визначення предмета та об'єкта дослідження, аналітичний та порівняльний аналіз для оцінки новизни результатів дослідження, узагальнення для формулювання висновків і рекомендацій. Наукова новизна результатів дослідження полягає в узагальненні інформації про нові види діяльності з кібердорозвідки, схематичному описі процесу діяльності та визначено найбільш ймовірні уповноважені органи (суб'єкти) на її реалізацію. Запропоновано складові кібердорозвідки та етапи проведення кібердорозвідки. Дослідження не охоплює всіх аспектів проблеми. Теоретичні результати, отримані в ході наукового дослідження, створюють основу для подальшої верифікації формалізованого формату кібернетичної розвідки.

Ключові слова: адміністративно-правові засади; організація; реалізація; заходи; кібердорозвідка; кіберрозвідка; збір інформації; кіберпростір; сектор безпеки та оборони.

Kozubtsov Igor Mykolaiovych Doctor of Pedagogical Sciences, Candidate of Technical Sciences, Senior researcher, Professor of the Department of combat use of communication units, Military Institute of telecommunications and informatization named after Heroes of Krut, Knyaziv Ostrozkyh St., 45/1, Kiev, 01011, tel.: (063) 404-84-41, https://orcid.org/0000-0002-7309-4365

Tkach Volodymyr Oleksandrovych senior researcher of the research department (integrated information security systems in information and telecommunications systems) of the research department (problems of Information Protection) of the Scientific Center for communications and informatization, Military Institute of telecommunications and informatization named after Heroes of Krut, Knyaziv Ostrozkyh St., 45/1, Kiev, 01011, tel.: (098) 395-38-98, https://orcid.org/0000-0003-0013-7368

Hlobin Andrii Viktorovych researcher of the Research Department (Technical support of communication and automation equipment) of the Research Department (Development of communication forces) of the Scientific Center for Communication and Informatization, Military Institute of telecommunications and informatization named after Heroes of Krut, Knyaziv Ostrozkyh St., 45/1, Kiev, 01011, tel.: (095) 160-99-10, https://orcid.org/0000-0001-5335-6869

Fomkin Denys Valentynovych junior researcher of the research department (integrated information security systems in information and telecommunications systems) of the research department (problems of Information Protection) of the Scientific Center for communications and informatization, Military Institute of telecommunications and informatization named after Heroes of Krut, Knyaziv Ostrozkyh St., 45/1, Kiev, 01011, tel.: (050) 330-38-33, https://orcid.org/0000-0003-0128-9355

AUTHORIZATION OF SECURITY AND DEFENSE SECTOR BODIES TO ORGANIZE AND CONDUCT CYBER INTELLIGENCE EVENTS

Abstract. In a hybrid war, the winner is the party that first creates the conditions necessary to violate the target cybersecurity functions of information security systems and critical information infrastructure. Creating prerequisites for violating the target function requires preliminary identification of vulnerabilities in information security and cybersecurity systems of enemy critical information infrastructure facilities. This task is performed during Cyber Intelligence. For a long time, the concept of cyber intelligence was absent in the scientific community, but such activities were already carried out in the context of cyber intelligence. Only in 2021, at the legislative level, cyber intelligence was defined as an activity aimed at identifying vulnerabilities in software, telecommunications equipment, automated control systems for troops, weapons and/or technical processes of a specific object (cyber infrastructure objects). The subject of research in the scientific article is the justification of the administrative and legal foundations of the organization of cyber intelligence. The purpose of this article is to highlight the administrative and legal framework that allows security and defense sector bodies to organize cyber intelligence activities in a hybrid war. To achieve this goal and objectives, the following theoretical research methods were used: generalization of scientific literature, structural and genetic analysis to determine the subject and object of research, analytical and comparative analysis to assess the novelty of research results, generalization to formulate conclusions and recommendations. The scientific novelty of the research results consists in summarizing information about

new types of cyber intelligence activities, schematically describing the process of activity, and identifying the most likely authorized bodies (subjects) for its implementation. The components of cyber intelligence and stages of cyber intelligence are proposed. The study does not cover all aspects of the problem. The theoretical results obtained in the course of scientific research create the basis for further verification of the formalized format of cyber intelligence.

Keywords: administrative and legal bases; organization; implementation; activities; cyber intelligence; cyber intelligence; information collection; cyberspace; security and defense sector.

Постановка проблеми. З початком широкомасштабного військового вторгнення Російської Федерації в Україну було організовано вогневе ураженням об'єктів критичної інфраструктури (ОКІ) нанесено кібератаки на об'єктів критичної інформаційної інфраструктури (ОКІІ). Завдяки вмілій та своєчасній підготовці українського сегменту Інтернету до кібероборони, більшість ОКІ продовжували працювати в штатному режимі, не постраждавши від DDoS-атак.

Не очікуваним для Російської Федерації став факт небайдужості фахівців ІТ-сфери з числа цивільного населення, яке синергетично згуртувалося і створило передумови до проведення активних заходів у кіберпросторі.

Незважаючи на війну, Україна продовжує дотримуватися міжнародних норм ведення війни, в тому числі і в кіберпросторі. Однак приклади позитивного ставлення цивільного населення до необхідності застосування активних форм дій у кіберпросторі підтверджують тезу про необхідність домінування над супротивником - Російською Федерацією, а також важливу роль України в усуненні адміністративно-правових прогалин у правовій системі України.

Аналіз останніх досліджень і публікацій. Найбільш активну позицію зайняли такі науковці, як В. Бурячок, Ю. Даник, С. Вдовенко, Є. Войтко, Діордіца, В. Кива, В. Куцаєв, Є. Судніков, О. Чорноног, В. Чернега, Ю. Хлапонін. У зв'язку з обраною темою дослідження цікавим є вивчення та розвиток теоретичних засад кібердорозвідки. На основі досвіду розбудови систем кібербезпеки та кібероборони провідних країн світу авторами роботи [1] узагальнюють питання організації та здійснення діяльності з кібердорозвідки (збору розвідувальної інформації в кіберпросторі), що і є предметом даного дослідження.

У роботах [2; 3] під розвідкою інформаційно-телекомунікаційної системи (ІТС) тлумачать як комплекс заходів, спрямованих на систематичний і цілеспрямований пошук та добування з ІТС інформації стосовно протиборчої сторони (конкурента), її вивчення та оброблення, а також формування на цій

підставі уявлення про реальні та/або потенційно можливі джерела деструктивного впливу на власний кіберпростір.

Розвідка ІТС відрізняється від інших видів розвідки головним чином своїми механізмами (методами і способами), а також силами і засобами, що залучаються для отримання розвідувальної інформації Основними методами розвідки ІТС є телекомунікаційна розвідка, мережева розвідка і кібернетична розвідка. телекомунікаційна розвідка, мережева розвідка та кіберрозвідка.

У роботі [4] підтверджується, що кіберрозвідка, яка в першу чергу здійснює пошук і збір розвідувальної інформації в Інтернеті, залишається ефективним засобом розвідки ІТС, і що найбільш дієвим методом є соціальна інженерія, призначена для організації доступу до найбільш захищених розвідувальних інформаційних ресурсів.

Кібервплив стає все більш ефективним інструментом для досягнення мети невійськового контролю і управління як об'єктами ОКІ, так і окремими громадянами і об'єднаннями, які можуть зазнати такого впливу. Спираючись на міжнародний досвід, можна стверджувати, що процес забезпечення кібербезпеки насамперед передбачає протидію деструктивним впливам у цій сфері. Це вимагає створення та організації потужної підсистеми кіберзахисту. Не менш важливим елементом системи кібербезпеки є підсистема кіберрозвідки та кібервпливу [5, с. 7].

Отже, розвиток методів розвідки ІТС породжує потребу розбудовувати систему кібероборони як систему протидії кібервтручанням. У зв’язку з проблемою пошуку підходів протидії найпоширенішим кібернетичним втручанням в інформаційно–комунікаційні мережі (ІКМ) привертають увагу автори статті [6]. Хоча аналіз методів та інструментів показав їхню придатність для виявлення кібератак, не існує єдиного універсального методу захисту від усіх типів атак в ІКМ.

У науковій статті “Методи розвідки кіберпростору” [7] описано важливість забезпечення національної безпеки в кіберпросторі. Автори розкривають не тільки доцільність, але й необхідність проведення розвідувальних операцій у кіберпросторі противника. Описано етапи, складові та методи ведення кібернетичної розвідки в кібернетичному просторі, а також критичні дані, які необхідно отримати під час розвідувальних операцій для забезпечення командування інформацією про противника. Визначено основні переваги та недоліки активних і пасивних методів збору розвідувальної інформації, а також запропоновано комплексний підхід, який використовує переваги кожного методу для підвищення ефективності кібернетичної розвідки в ІКМ.

Здобуття інформації у кіберпросторі про ІКМ противника є процесом розвідувально-інформаційної діяльності (РІД) в умовах невизначеності [8].

Одержані результати цікаві для даного дослідження, якщо, кібердорозідку розглядати як новий напрямок РІД, яка має вирішувати коло інтелектуальних за змістом завдань: відбір і формування розвідувальних ознак; розпізнавання та ідентифікація об'єктів розвідки при неповній і нечіткій інформації в умовах значної невизначеності вихідних даних.

Виділення аспектів, що недостатньо вивчені. Однак питання застосування активних засобів (кібердорозвідки) у кіберпросторі потенційних супротивників недостатньо досліджено в літературі [1–8], але потреба в цьому є нагальною.

Формулювання мети статті. Метою цієї статті є висвітлення адміністративно-правової бази, що дозволяє органам сектору безпеки та оборони організовувати діяльність з кібердорозвідки в умовах гібридної війни.

Виклад основного матеріалу.

Законодавча база з кібердорозвідки. Адміністративно-правовою основою для регулювання активних і пасивних заходів у кіберпросторі можна вважати подію 2016 року, коли Президент України затвердив "Стратегію кібербезпеки України". Ця стратегія вперше ввела в термінологію дефініцію поняття "кібероборона" [9].

Пізніше була запропонована в проекті Указу Президента України [10] дефініцію "кібердорозвідка" – збір інформації щодо вразливостей програмного забезпечення, телекомунікаційного обладнання, автоматизованих систем управління силами, зброєю та/або технологічними процесами визначеної цілі. Проте, слід зазначити, що в затвердженому Указі Президента України [11] під кібердорозвідкою прийнято розуміти діяльність щодо виявлення вразливостей програмного забезпечення, телекомунікаційного обладнання, автоматизованих систем управління силами, зброєю та/або технологічними процесами визначеної цілі (об'єкта кіберінфраструктури).

Іншими словами, визначення кібердорозвідки (збір інформації в кіберпросторі) розуміється наступним чином діяльність щодо виявлення вразливостей програмного забезпечення, телекомунікаційного обладнання, автоматизованих систем управління силами, зброєю та/або технологічними процесами визначеної цілі (об'єкта кіберінфраструктури) з точки зору адміністративно-правових норм як вид діяльності визначено.

Механізми реалізації заходів кібердорозвідки. Однією зі складових кіберрозвідки (рис. 1) є комп'ютерна розвідка, де збір розвідувальних даних полягає в отриманні даних та інформації, що циркулюють в засобах електронно-обчислювальної техніки, локальних і глобальних комп'ютерних мережах, в тому числі з несанкціонованим доступом, і доповнюється кібердорозвідкою.

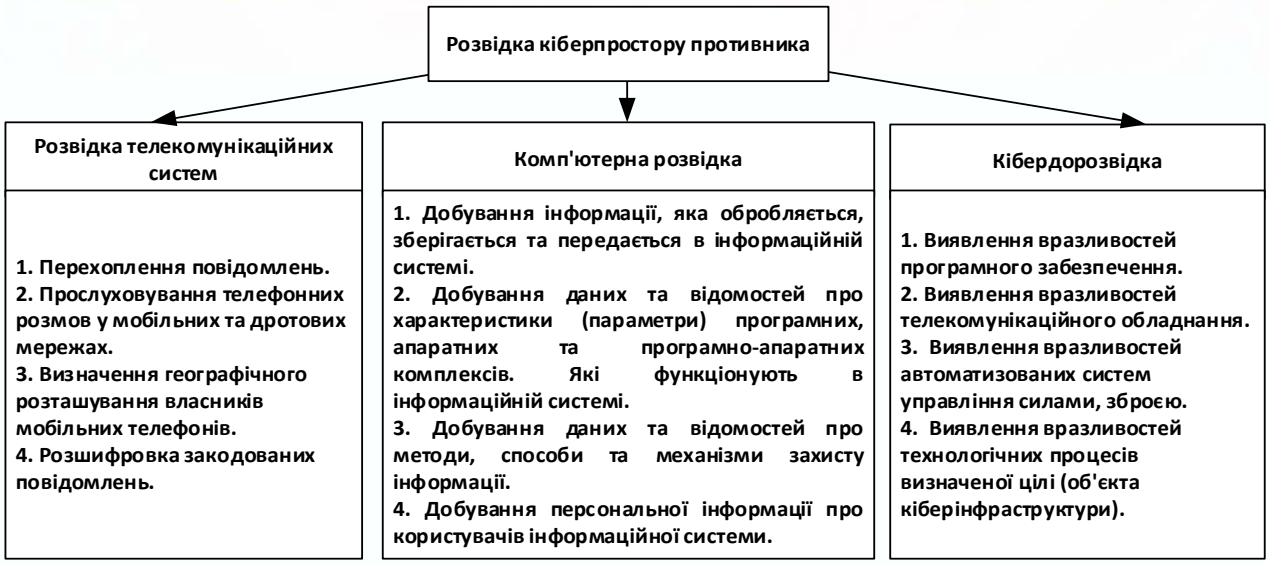

Рис. 1. *Складові кіберрозвідки*

Способи реалізація розвідки ІТС детально описана в [4] тому, її опис ми опускає, але слід зазначити, що вона логічно може бути використана для кібердорозвідки ІТС (див. рис. 2).

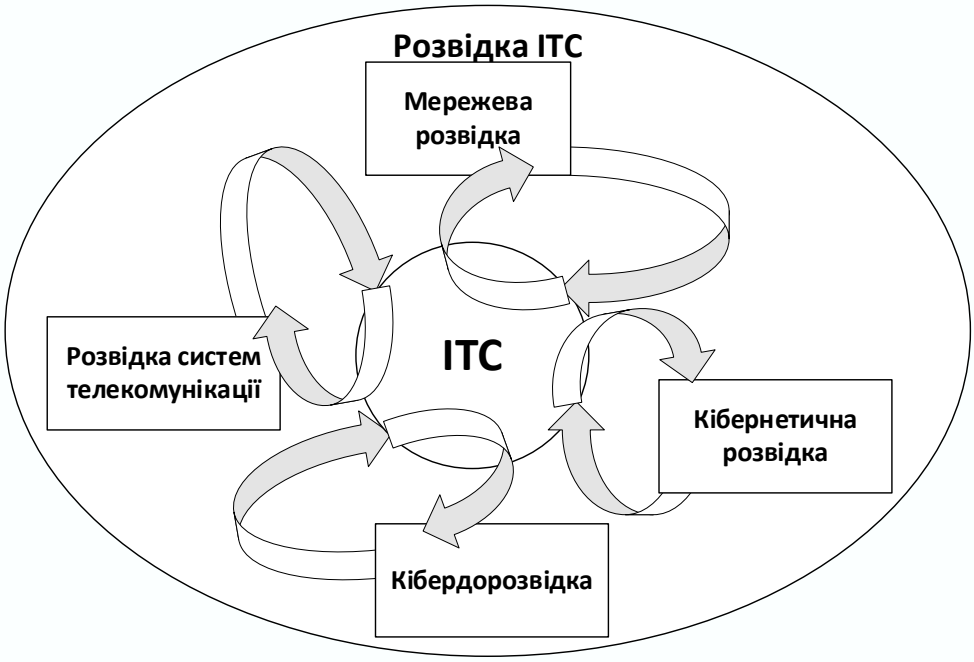

Рис. 2. *Способи реалізації кібердорозвідки ІТС*

Враховуючи досвід [4], можна спрогнозувати, що кібердорозвідка використовуватиме технічні та програмні методи і прийоми соціальної інженерії у поєднанні з відкритим і відносно відкритим стеженням за електронними джерелами та активними провокаціями (рис. 3).

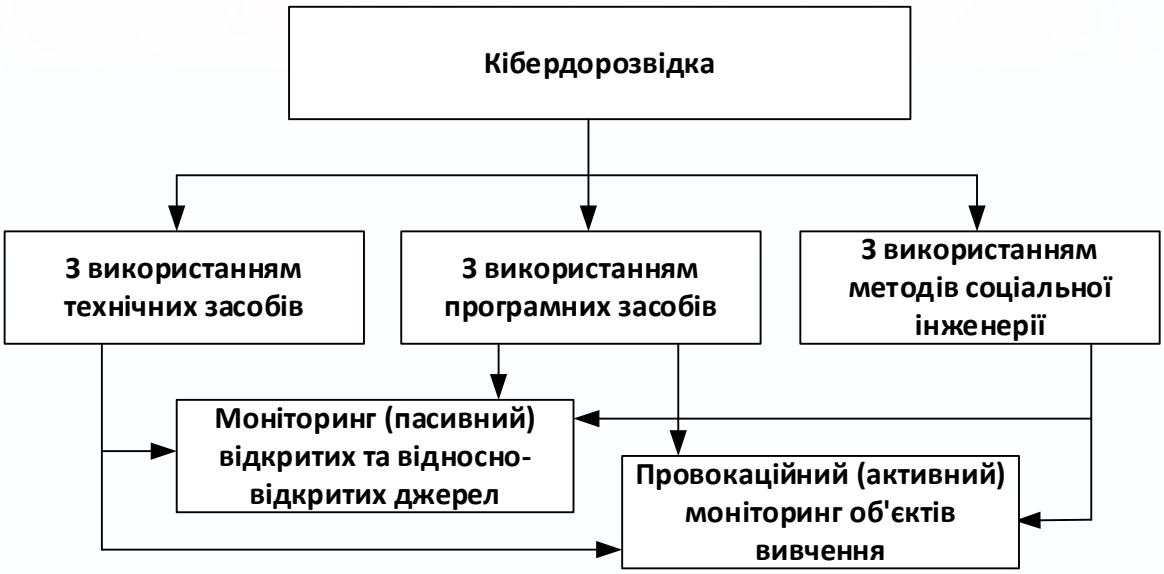

Рис. 3. *Складові кібердорозвідки*

Зібрана інформація також може бути використана для побудови моделі системи нападу противника, що полегшить проникнення та кібервпливу на цю систему в майбутньому.

Діяльність компетентних органів, на здійснення кібердорозвідки об'єктів противника, відбувається за класичною схемою, етапи якої проілюстровані на рис. 4.

Рис. 4. *Етапи проведення кібердорозвідки*

Кожен з етапів кібердорозвідки, перерахованих на схемі, має свої завдання і цілі, що в кінцевому підсумку дозволяє проводити розвідувальні операції і отримувати очікувану або необхідну інформацію про об'єкти противника.

Відповідно до Додатку 3 [11], за реалізацію здатності ведення кіберрозвідки та кібердорозвідки в інформаційно-телекомунікаційних мережах та системах державного, приватного і військового призначення (об’єктів критичної інфраструктури) противника для здобуття інформації про кіберінфраструктуру противника, їх призначення, місцезнаходження,

технологічних процесів, уразливості, встановлення прихованого контролю, перехоплення та дешифрування керуючих і ресурсних даних та інформації відповідають покладаються наступні органи: Головне управління розвідки Міністерства оборони України, Збройні Сили України та Державну прикордонну службу України.

Враховуючи сферу застосування кібероборони, окреслену в [1, с.44], можна створити систему органів (суб'єктів) сектору безпеки і оборони, які уповноважені здійснювати кібердорозвідку (рис. 5). Зазначимо, що метою їх діяльності є забезпечення кібероборони держави.

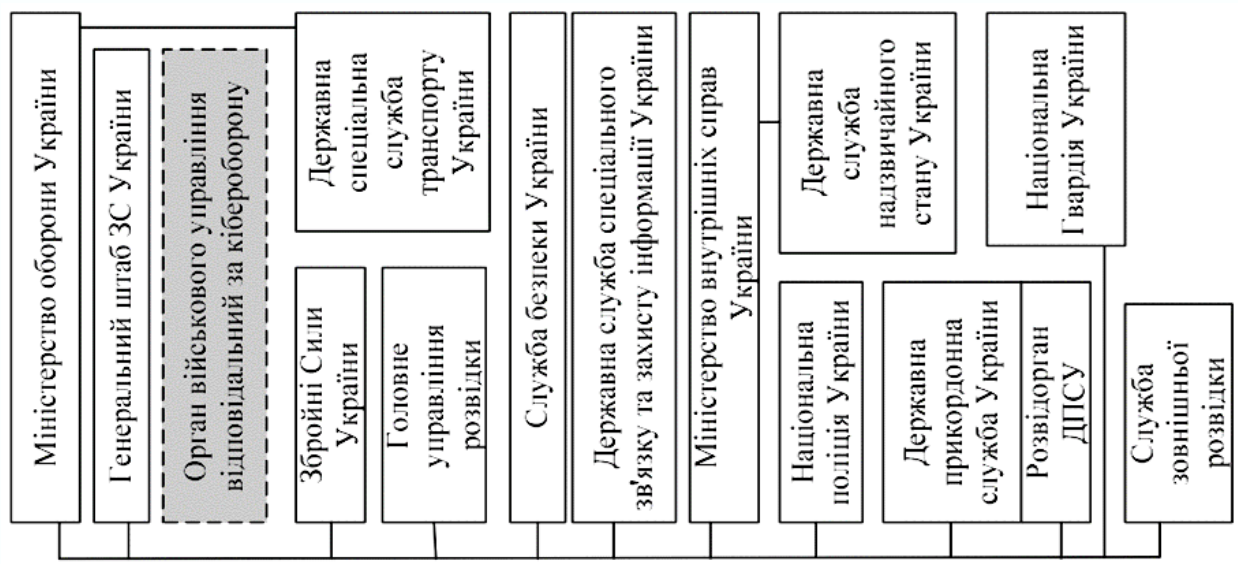

Рис.5. *Ймовірні уповноважені органи (суб'єкти) здійснювати кібердорозвідку*

Кібердорозвідка - це складова РІД, являє собою постійний управлінський процес, що здійснюється розвідувальними органами і включає комплекс заходів з організації та проведення розвідувально-інформаційної роботи з метою задоволення потреб споживачів розвідувальної інформації [12].

Обговорення попередніх результатів. Таким чином, можна офіційно вважати, що з моменту прийняття Указу Президента України [11] органи влади отримали достатні повноваження для проведення операцій з кібердорозвідки в кіберпросторі як суб'єкт кібероборони. Як показала практика, самоорганізовані ІТ-спеціалісти з груп "білих хакерів" надають потужну превентивну підтримку в проведенні операцій з кібердорозвідки. Їхній приклад підтверджує обґрунтованість припущення про необхідність створення гібридних підрозділів цивільно-військового співробітництва [13].

Відсутність централізованого управління призвело до децентралізованого створення телеграм каналів, до прикладу КіберАрмія та інші, які станом дня

25.02.2022 р. нараховували понад 250 тисяч учасників [14]. Прогностичність дій вбачають за необхідність у пошуку та виявлення вразливостей програмного забезпечення, телекомунікаційного обладнання, автоматизованих систем управління силами, зброєю та/або технологічними процесами визначеної цілі (об'єкта кіберінфраструктури).

Відсутність централізованого управління призвела до децентралізованого створення телеграм-каналів, наприклад, “Кіберармії”, яка станом на 25 лютого 2022 року налічувала понад 250 000 учасників [14]. Прогностичні дії розглядаються як необхідність пошуку та виявлення вразливостей у програмному забезпеченні, телекомунікаційному обладнанні, автоматизованих системах управління військами, зброєю та/або технологічними процесами визначеної цілі (об'єкта кіберінфраструктури).

Висновки. Відтак, з 2021 року законодавчим органом затверджено поняття кібердорозвідка. Кіберрозвідка – це діяльність, спрямована на виявлення вразливостей у програмному забезпеченні, засобах зв'язку, автоматизованих системах управління військами, зброєю та/або технічними процесами конкретного об'єкта (об'єкта кіберінфраструктури). Однак той факт, що до цього часу в секторі безпеки і оборони не визначено жодного уповноваженого органу чи підрозділу для здійснення діяльності з кібердорозвідки, створює плутанину та безвідповідальність.

Вперше узагальнено інформацію щодо нового виду діяльності з кібердорозвідки, подано схематичний опис процесу діяльності та визначено найбільш ймовірні уповноважені органи (суб’єкти) на її реалізацію. Запропоновано складові кіберрозвідки та етапи проведення кібердорозвідки.

Теоретичні результати, отримані в ході наукового дослідження, є основою для подальшого обґрунтування формалізованого формату здійснення кібердорозвідки.

Література:

1. Вдовенко, С.Г., Даник, Ю.Г., Пермяков, О.Ю. Досвід розвитку систем кібербезпеки та кібероборони провідних країн світу. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2020. Том. 1. №(37). С. 31–48.

2. Бурячок, В.Л., Гулак, Г.М., Хорошко, В.О. До питання організації та проведення розвідки у кібернетичному просторі. *Наука і оборона*. 2011. № 2. С. 19–23.

3. Бурячок, В.Л., Ільяшов, О.А., Гулак, Г.М. Поняття кібервійни та розвідки інформаційно-телекомунікаційних систем у контексті захисту держави від стороннього кібернетичного впливу. Збірник матеріалів круглого столу “Актуальні питання підготовки фахівців із розслідування кіберзлочинів”. Київ: НА СБ України, 2011. С. 27–32.

4. Бурячок, В.Л., Корченко, О.Г., Бурячок, Л.В. Соціальна інженерія як метод розвідки інформаційно-телекомунікаційних систем. *Журнал «Захист інформації»*. 2012. 14, 4 (57). С. 5–11.

5. Даник, Ю.Г., Воробієнко, П.П., Чернега, В.М. Основи кібербезпеки та кібероборони: підручник. Одеса: ОНАЗ ім. О.С. Попова. 2019.

6. Чередниченко, О.Ю., Фесьоха, В.В., Процюк, Ю.О., Бондаренко, Т.В. Аналіз існуючих підходів протидії найпоширенішим кібернетичним втручанням в інформаційно–телекомунікаційні мережі. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2018. №2(32). С. 13–16.

7. Кива, В.Ю., Судніков, Є.О., Войтко, О.В. Методи розвідки кіберпростору. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2018. №3 (33). С. 45–52.

8. Гаценко, С.С., Ліщенко, О.М., Сотніченко, А.І., Жарков, Я.А. Математична модель процесу розвідувально-інформаційної діяльності в умовах невизначеності. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2020. №1 (37). С. 77–84.

9. Указ Президента України. Стратегія кібербезпеки України, 96, https://zakon.rada.gov.ua/laws/show/96/2016/ed20160315.

10. Проект Указу Президента України. "Про рішення Ради національної безпеки і оборони України", "Про Стратегічний оборонний бюлетень України", https://www.mil.gov.ua/content/pdf/up_rrnb.pdf.

11. Указ Президента України. "Про рішення Ради національної безпеки і оборони України від 20 серпня 2021 року" 473/2021, "Про Стратегічний оборонний бюлетень України", https://zakon.rada.gov.ua/laws/show/473/2021.

12. Військовий стандарт ВСТ 01.101.004 – 2019 (03). Воєнна розвідка. Інформаційно-аналітична діяльність. Терміни та визначення.

13. Пономарьов О.А., Пивоварчук С.А., Козубцова Л.М., Козубцов І.М., Бондаренко Т.В., Терещенко Т.П. Гібридна побудова системи кібербезпеки: адміністративно-правові засади військово-цивільного співробітництва. *Кібербезпека: освіта, наука, техніка*. 2023. Том 3. № 19. С. 109 – 121.

14. Мальцева, І., Черниш, Ю., Штонда, Р. Аналіз деяких кіберзагроз в умовах війни. Кібербезпека: освіта, наука, техніка. 2022. Том 4. №16. С. 37–44.

References:

1. Vdovenko, S.H., Danyk, Yu.H., Permiakov, O.Yu. (2020). Dosvid rozvytku system kiberbezpeky ta kiberoborony providnykh krain svitu [Experience in the development of cybersecurity and cyber defense systems in the leading countries of the world]. *Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony – Modern information technologies in the field of security and defense*, 1,(37), 31–48. [in Ukrainian].

2. Buriachok, V.L., Hulak, H.M., Khoroshko, V.O. (2011). Do pytannia orhanizatsii ta provedennia rozvidky u kibernetychnomu prostori [On the issue of organizing and conducting intelligence in cybernetic space]. *Nauka i oborona – Science and defense*, 2, 19–23. [in Ukrainian].

3. Buriachok, V.L., Iliashov, O.A., Hulak, H.M. (2011). Poniattia kiberviiny ta rozvidky informatsiino-telekomunikatsiinykh system u konteksti zakhystu derzhavy vid storonnoho kibernetychnoho vplyvu [The concept of cyber warfare and intelligence of information and telecommunications systems in the context of state protection from extraneous cybernetic influence]. *Zbirnyk materialiv kruhloho stolu "Aktualni pytannia pidhotovky fakhivtsiv iz rozsliduvannia kiberzlochyniv" – Collection of materials of the round table "topical issues of training specialists in the investigation of cybercrime"*, (pp. 27–32). Kyiv: NA SB Ukrainy [in Ukrainian].

4. Buriachok, V.L., Korchenko, O.H., Buriachok, L.V. (2012). Sotsialna inzheneriia yak metod rozvidky informatsiino-telekomunikatsiinykh system [Social engineering as a method of intelligence of information and telecommunications systems]. *Zhurnal «Zakhyst informatsii» – Journal "Information Protection"*, 14, 4 (57), 5–11. [in Ukrainian].

5. Danyk, Yu.H., Vorobiienko, P.P., Cherneha, V.M. (2019). Osnovy kiberbezpeky ta kiberoborony [Fundamentals of cybersecurity and cyber defense]: pidruchnyk. Odesa: ONAZ im. O.S. Popova. [in Ukrainian].

6. Cherednychenko, O.Yu., Fesokha, V.V., Protsiuk, Yu.O., Bondarenko, T.V. (2018). Analiz isnuiuchykh pidkhodiv protydii naiposhyrenishym kibernetychnym vtruchanniam v informatsiino–telekomunikatsiini merezhi [Analysis of existing approaches to countering the most common cyber interference in information and telecommunications networks]. *Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony – Modern information technologies in the field of security and defense*, 2(32), 13–16. [in Ukrainian].

7. Kyva, V.Yu., Sudnikov, Ye.O., Voitko, O.V. (2018). Metody rozvidky kiberprostoru [Methods of cyberspace intelligence]. *Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony – Modern information technologies in the field of security and defense*, 3 (33), 45–52. [in Ukrainian].

8. Hatsenko, S.S., Lishchenko, O.M., Sotnichenko, A.I., Zharkov, Ya.A. (2020). Matematychna model protsesu rozviduvalno-informatsiinoi diialnosti v umovakh nevyznachenosti [Mathematical model of the process of intelligence and information activity in conditions of uncertainty]. *Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony – Modern information technologies in the field of security and defense*, 1 (37), 77–84. [in Ukrainian].

9. Ukaz Prezydenta Ukrainy (2016). Stratehiia kiberbezpeky Ukrainy [Cybersecurity strategy of Ukraine]. https://zakon.rada.gov.ua/laws/show/96/2016/ed20160315. [in Ukrainian].

10. Proekt Ukazu Prezydenta Ukrainy (2021). “Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy”, “Pro Stratehichnyi oboronnyi biuleten Ukrainy” ["On the decision of the National Security and Defense Council of Ukraine”, “On the Strategic Defense Bulletin of Ukraine”], https://www.mil.gov.ua/content/pdf/up_rrnb.pdf. [in Ukrainian].

11. Ukaz Prezydenta Ukrainy (2021). “Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy, “Pro Stratehichnyi oboronnyi biuleten Ukrainy” ["On the decision of the National Security and Defense Council of Ukraine,” On the Strategic Defense Bulletin of Ukraine"], https://zakon.rada.gov.ua/laws/show/473/2021. [in Ukrainian].

12. Viiskovyi standart VST 01.101.004 – 2019 (03). Voienna rozvidka. Informatsiino-analitychna diialnist. Terminy ta vyznachennia [Military intelligence. Information and analytical activities. Terms and definitions]. [in Ukrainian].

13. Ponomarov O.A., Pyvovarchuk S.A., Kozubtsova L.M., Kozubtsov I.M., Bondarenko T.V., Tereshchenko T.P. (2023). Hibrydna pobudova systemy kiberbezpeky: administratyvno-pravovi zasady viiskovo-tsyvilnoho spivrobitnytstva [Hybrid construction of the cybersecurity system: administrative and legal bases of military-civil cooperation]. *Kiberbezpeka: osvita, nauka, tekhnika –Cybersecurity: education, science, and technology*, 3, 19, 109 – 121. [in Ukrainian].

14. Maltseva, I., Chernysh, Yu., Shtonda, R. (2022). Analiz deiakykh kiberzahroz v umovakh viiny [Analysis of some cyber threats in war conditions]. *Kiberbezpeka: osvita, nauka, tekhnika – Cybersecurity: education, science, and technology*, 4, 16, 37–44. [in Ukrainian].