КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (21), 2023
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2023.21.616
УДК 007.2+ 004.942 + 004.05 +004.056.5

Пономарьов Олександр Анатолійович
начальник факультету
Військовий інститут телекомунікацій і інформатизації імені Героїв Крут, Київ, Україна
ORCID 0009-0008-2320-1549
aleksan_bimer3@ukr.net

Козубцова Леся Михайлівна
кандидат технічних наук
завідувач кафедри
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна
ORCID 0000-0002-7866-8575
lesia.kozubtsova@viti.edu.ua

Козубцов Ігор Миколайович
доктор педагогічних наук, кандидат технічних наук, старший науковий співробітник
професор кафедри
Військовий інститут телекомунікацій і інформатизації імені Героїв Крут, Київ, Україна
ORCID ID 0000-0002-7309-4365
kozubtsov@gmail.com

Ткач Володимир Олександрович
старший науковий співробітник науково-дослідного відділу
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна
ORCID ID 0000-0003-0013-7368
tkachwolodymyr@gmail.com

АДМІНІСТРАТИВНО-ПРАВОВІ ЗАСАДИ УПОВНОВАЖЕННЯ ОРГАНІВ СЕКТОРУ БЕЗПЕКИ ТА ОБОРОНИ ЩОДО ОРГАНІЗАЦІЇ ЗАХОДІВ КІБЕРДОРОЗВІДКИ

Анотація. В умовах гібридної війни перемагає та сторона, яка першою створить умови до порушення цільової функції працездатності системи захисту інформації та кібербезпеки об'єктів критичної інформаційної інфраструктури. Для створення передумов до порушення цільової функції необхідно завчасно виявити вразливі місця у системи захисту інформації та кібербезпеки об'єктів критичної інформаційної інфраструктури противника. Це завдання виконується в ході кібердорозвідки. Тривалий час було відсутнє у науковому обізі поняття кібердорозвідки однак діяльність як така вже виконувалась у контексті кіберрозвідки. Лише у 2021 року на законодавчому рівні прийнято під кібердорозвідкою розуміти діяльність щодо виявлення вразливостей програмного забезпечення, телекомунікаційного обладнання, автоматизованих систем управління силами, зброєю та/або технологічними процесами визначеної цілі (об'єкта кіберінфраструктури). Предметом дослідження у науковій статті є обґрунтування адміністративно-правових засад організації кібердорозвідки. Для досягнення мети та поставленого завдання використовувались теоретичні методи дослідження: узагальнення наукової літератури; структурно-генетичного аналізу при уточненні об'єкту та предмету дослідження; аналітично-порівняльного аналізу при оцінюванні новизни результатів дослідження; узагальнення – для формулювання висновків і рекомендацій. У дослідженні отримано результати, наукова новизна яких полягає в узагальнені інформації 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. Перспективи подальших досліджень у даному напрямку. Представлене дослідження не вичерпує всіх аспектів зазначеної проблеми. Теоретичні результати, що одержані в процесі наукового пошуку, становлять підґрунтя для подальшого обґрунтування формалізованого бланку на

проведення кібердорзвідки.

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

ВСТУП

Ефективність системи – це властивість системи, що характеризує її здатність виконувати свою цільову функцію. Під «ефективністю системи захисту інформації і кібербезпеки» будемо розуміти ступінь відповідності досягнутих результатів поставленим цілям щодо захисту інформації [1]. Встановлено, що нині відсутнє єдине бачення щодо методології протидії війнам за гібридною формою. В умовах гібридної війни перемагає та сторона, яка першою створить умови до порушення цільової функції працездатності системи захисту інформації та кібербезпеки об'єктів критичної інформаційної інфраструктури (ОКІІ). Відсутність методології протидії вимагає перегляду існуючих підходів до гарантування та підтримки державної безпеки та пошуку нестандартних рішень.

Постановка проблеми. З початку повномасштабної військової агресії Російської Федерації проти України одночасно з вогневим ураженням об'єктів критичної інфраструктури нанесено кібератаки на ОКІІ. Завдяки вмілій і своєчасній підготовці українського сегменту Інтернету до кібероборони, було досягнуто успіху в тому, що більша частина ОКІІ продовжила функціонувати в штатному режимі не зазнаючи втручання та наслідків від DDoS-атак. Зважаючи на то, що Україна не планувала і не здійснила акту вторгнення на територію Російської Федерації, вона була вимушена застосувати весь потенціал кібероборони. Однак приємним для нас і 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. Україна, незважаючи на війну, продовжує дотримуватися міжнародних норм ведення війни в тому числі у кіберпросторі. Однак, приклад активної громадянської позиції щодо необхідності застосування активних форм дій в кіберпросторі підтверджує тезу про вирішальну роль у необхідності у домінуванні над супротивником, Російською Федерацією, та одночасно у вирішені адміністративно-правових прогалин законодавства України.

Аналіз останніх досліджень і публікацій. До вивчення аспектів під різними кутами зору адміністративно-правових засад забезпечення кібероборони присвячено досить багато наукових робіт. Найбільш активну позицію проявили науковці: В.Л. Бурячок, Ю.Г. Даник, С.Г. Вдовенко, І.В. Діордіца, Є.О. Живило, В.В. Куцаєв, О.О. Черноног та ін. Стосовно обраного предмету дослідження цікавим є наукові пошуки та розробки теоретичних основ кібердорозвідки. Ґрунтуючись на досвіді розвитку систем кібербезпеки та кібероборони провідних країн світу авторами [2] узагальнено організацію та реалізацію заходів кібердорозвідки (збору інформації в кіберпросторі), які цікаві для нашого дослідження.

У колективних роботах [3; 4] 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. Від інших видів розвідка ІТС відрізняється перш за все механізмами

(способами і методами), а також силами і засобами, що задіяні в добуванні розвідувальної інформації. Головними способами ведення розвідки ІТС є розвідка систем телекомунікацій, мережева розвідка і кіберрозвідка.

У статті [5] авторами констатовано, що найбільш дієвим і потужним способом розвідки ІТС на найближчу перспективу залишатиметься кіберрозвідка, призначена для пошуку та збору розвідувальної інформації передусім у Internet, а найбільш результативним – метод соціальної інженерії, призначений для організації доступу до будь-яких найбільш захищених інформаційних ресурсів.

Кібервпливи все частіше стають ефективним інструментом для досягнення мети щодо несилового контролю та управління, як об'єктами з критичною інформаційною інфраструктурою держави, що може піддатися такому впливу, так і окремо взятими громадянами, їх об'єднаннями. Спираючись на світовий досвід можна стверджувати, що процес забезпечення кібербезпеки, перш за все, передбачає протидію деструктивним впливам у цій сфері. Для цього потребує створення й організації потужна підсистема кіберзахисту. Не менш важливими складовими системи забезпечення кібербезпеки мають виступати і підсистеми кіберрозвідки та кібервпливу [6, 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–телекомунікаційні мережі (ІТМ) привертають увагу автори статті [7]. Аналіз методів та засобів показав доцільність їх застосування до виявлення кібератак однак не існує єдиного універсального методу захисту від всіх видів атак в ІТМ.

У науковій статті "Методи розвідки кіберпростору" [8] описується важливість забезпечення національної безпеки держави у кіберпросторі. Авторами обґрунтовано не лише актуальність, а в більшій мірі необхідність проведення розвідувальних заходів у кіберпросторі противника. Визначено етапи, складові та методи кібернетичної розвідки у кіберпросторі, а також критичні дані, які необхідно добути у ході проведення розвідувальних заходів для забезпечення командування інформацією про противника. Визначено основні переваги та недоліки активного та пасивного методу добування розвідувальних даних та запропоновано комплексний підхід використання переваг кожного методу, що дасть можливість підвищити ефективність проведення кібернетичної розвідки у інформаційно-телекомунікаційних мережах.

Здобуття інформації у кіберпросторі про ІТМ противника є процесом розвідувально-інформаційної діяльності (РІД) в умовах невизначеності [9]. 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.

Однак, з погляду зазначеної проблеми застосування активних заходів (кібердорозвідки) в кіберпросторі потенційного ворога на цей час у публікаціях [2–9] вивчено не достатньо, проте враховуючи отриманий досвід у ході відбиття зовнішньої агресії Російської Федерації проти України, є в такому нагальна необхідність.

Мета статті. Метою статті полягає висвітлити адміністративно-правові засади уповноваження органів сектору безпеки та оборони на організацію заходів кібердорозвідки в умовах гібридної війни.

ISSN 2663 - 4023

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Аналіз законодавчої бази та керівних (нормативних) документів щодо кібердорозвідки. Адміністративно-правовою основою, для організації активних та пасивних заходів в кіберпросторі, можна вже вважати подію 2016 р. затвердження Президентом України "Стратегії кібербезпеки України". Саме цією стратегією вперше було введено в термінологію дефініцію поняття "кібероборона" [10].

Згодом у проекті Указу Президента України від 2021 р. "Про рішення Ради національної безпеки і оборони України'', "Про Стратегічний оборонний бюлетень України", з яким можна ознайомитися за посиланням [11] запропоновано доповнити термінологію поняттям "кібердорозвідка" – збір інформації щодо вразливостей програмного забезпечення, телекомунікаційного обладнання, автоматизованих систем управління силами, зброєю та/або технологічними процесами визначеної цілі. Однак вже у затвердженому Указі Президента України від 17.09.2021 №473/2021 [12] 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).

У додатку 3. "Матриця основних спроможностей сил оборони" до Стратегічного оборонного бюлетеня України систематизовані інституційні спроможності центральних органів виконавчої влади та інших державних органів, які здійснюють керівництво, спрямовують та координують діяльність військових формувань, що входять або виділяють відповідні сили і засоби до складу сил оборони, та оперативні, бойові і спеціальні спроможності сил оборони [12]. Так, згідно з якими 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 покладаються на: Головне управління розвідки Міноборони, Збройні Сили України, Державна прикордонна служба України.

Отже, поняття кібердорозвідки (збору інформації в кіберпросторі) – це 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. Складовою кіберрозвідки (рис. 1) є комп'ютерна розвідка, при якій добування розвідувальних відомостей полягає в отриманні даних та інформації, що циркулює в засобах електронно-обчислювальної техніки, локальних та глобальних обчислювальних мережах, в тому числі із використанням несанкціонованого доступу та доповнимо її кібердорозвідкою.

ISSN 2663 - 4023

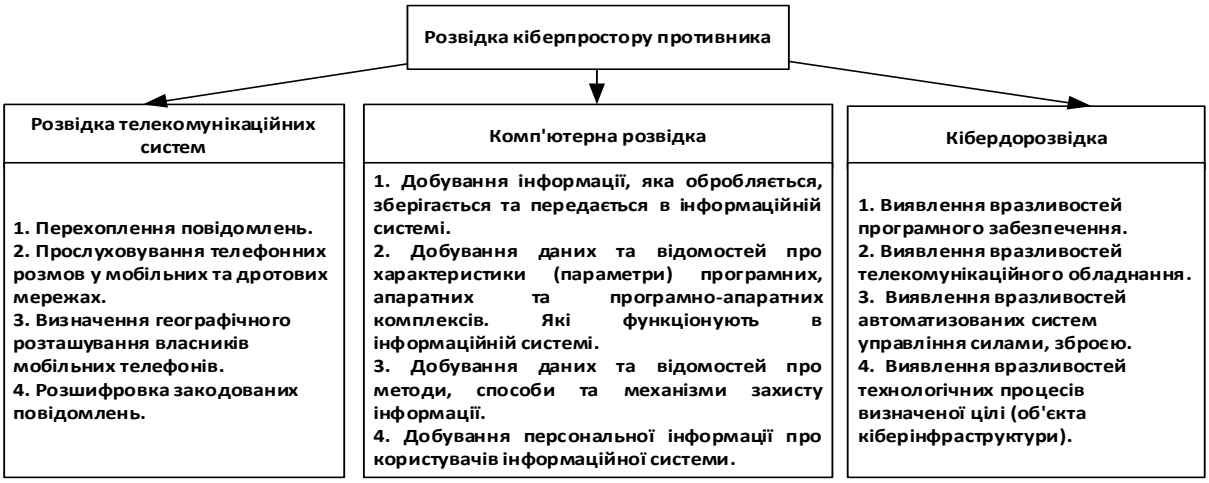

Рис. 1. Складові кіберрозвідки

Слід відзначити, що відомості про спосіб ведення розвідки ІТС нам відомі з публікації [5] вони за очевидною логікою можуть бути використані і для ведення кібердорозвідки ІТС (див. рис. 2).

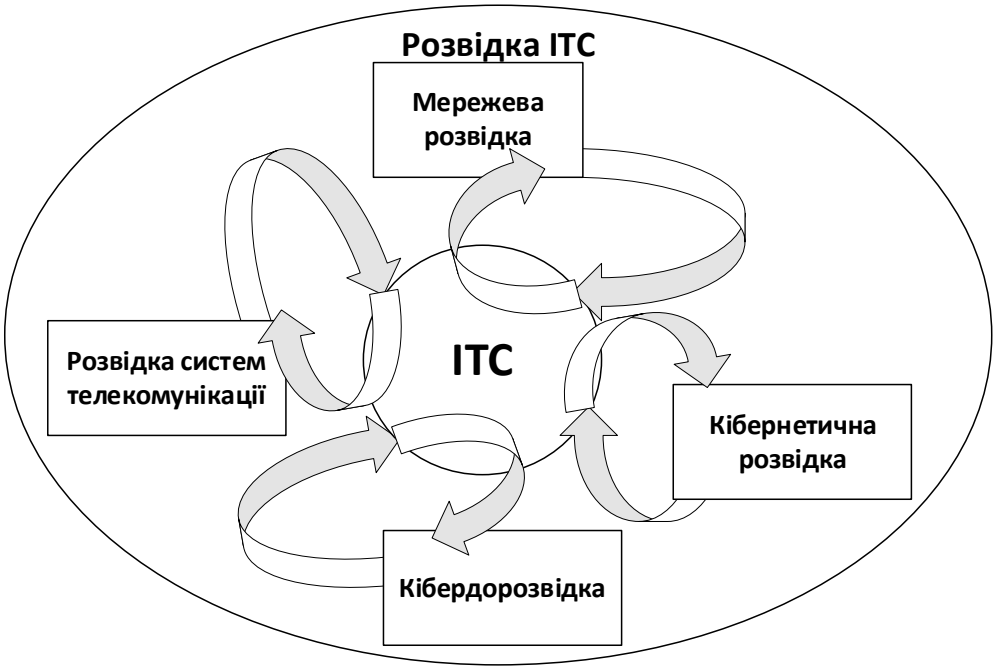

Рис. 2. Способи ведення розвідки ІТС

Враховуючи попередній досвід [5], можемо прогнозувати, що для пошуку і збору інформації про ІТС, кіберрозвідка застосовуватиме технічний і програмний методи її ведення, а також методи соціальної інженерії, в комбінацією з моніторингом відкритих і відносно відкритих електронних джерел, а також, активні заходи провокаційного характеру (рис. 3).

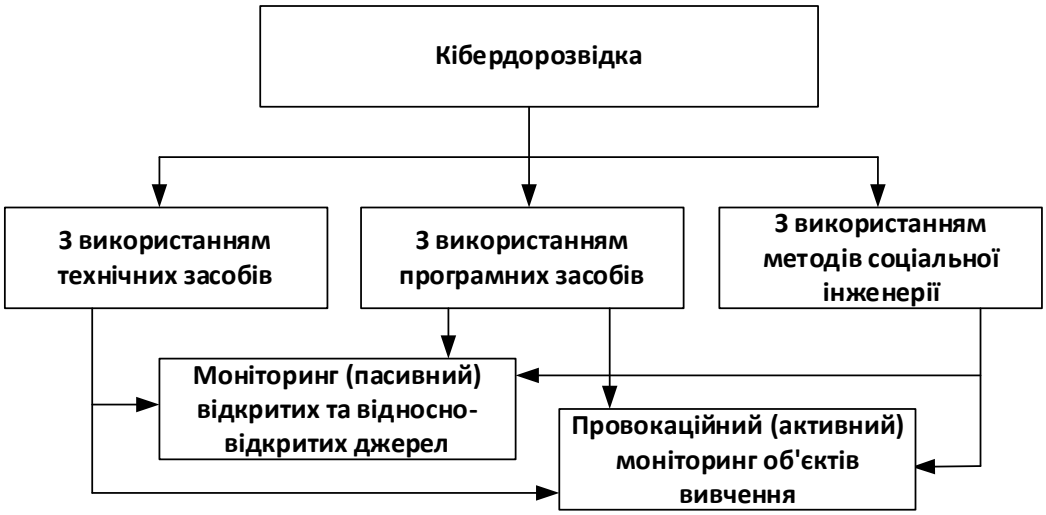

Рис. 3. Складові кібердорозвідки

Здобута інформація може бути використана для побудови моделі атакуючої системи для полегшення в майбутньому спроби проникнення до неї задля реалізації кібервпливу.

Метод активного добування розвідувальних даних полягає у безпосередньому контактуванні з піддослідним об’єктом розвідки із використанням методів прихованого сканування, що дає можливість бути непомітним при здійсненні впливу на противника. На відміну від пасивного методу добування даних при активному добуванні ймовірність помилкової ідентифікації віддаленого об’єкта зменшується врази, що підвищує точність розвідувальної інформації та ефективність подальшого формування кібервпливу на основі добутих розвідувальних даних про об’єкт дослідження.

Діяльність кібердорозвідки об’єкту противника включає наступні етапи (рис. 4).

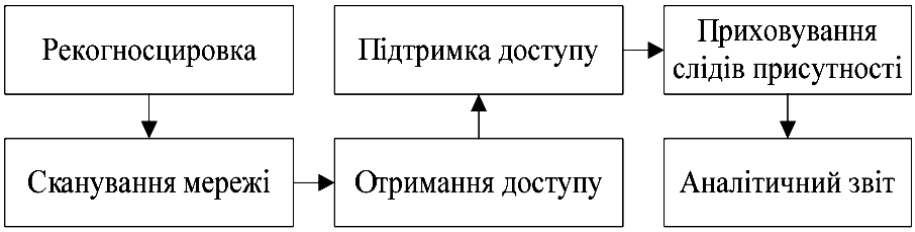

Рис. 4. Етапи проведення кібердорозвідки

Рекогносцировка є підготовчим етапом, де суб’єкт кібердорозвідки прагне добути попередню інформацію про можливі вразливості програмного забезпечення, телекомунікаційного обладнання, автоматизованих систем управління силами, зброєю та/або технологічними процесами визначеної цілі (об'єкта кіберінфраструктури). В залежності від факторів які впливають на добування розвідданих про противника рекогносцировка може бути двох видів:

активна рекогносцировка – включає активну взаємодію з об’єктом атаки з безпосереднім використанням будь-яких засобів, наприклад телефонні дзвінки в службу підтримки певного органу для отримання певної інформації;

пасивна рекогносцировка – включає отримання інформації без безпосередньої

ISSN 2663 - 4023

взаємодії з об'єктом кібернетичного впливу, наприклад пошук інформації на викинутих документах, записках, накопичуваних пристроях, комп'ютерах.

Сканування мережі відноситься до етапу попереднього збору інформації про інформаційну інфраструктуру противника. Задля цього орган уповноважений на реалізацію заходів кібердорозвідки сканує мережу, та отримує певну інформації про вразливості одержаної за результатами проведеної в ході рекогносцировки. Сканування може включати в себе сканування портів, IP-адрес, топології мережі, сервісів, вразливостей та визначення типу операційної системи.

Отримання доступу відноситься до точки входу в систему, де коли орган уповноважений на реалізацію заходів кібердорозвідки отримує доступ до операційної системи або додатків на комп'ютері або інших елементах інформаційної інфраструктури.

Орган уповноважений на реалізацію заходів кібердорозвідки може підвищити привілеї, щоб отримати повний контроль над системою, що дає можливість у подальшому приєднатися до проміжних систем, які підключені до неї. Може отримати доступ на рівні операційної системи, рівні додатків або мережевому рівні, прикладом може бути злом паролів, переповнення буфера, відмова у обслуговуванні.

Підтримка доступу відноситься до етапу, коли уповноважений орган на реалізацію заходів кібердорозвідки намагається зберегти доступ до системи. Для цього може використати вразливості нульового дня (0-day) з використанням Backdoor, Trojan, RootKit.

Орган уповноважений на реалізацію заходів кібердорозвідки може завантажувати, вивантажувати або маніпулювати даними додатків або конфігурацією над атакуючою системою, а також використовувати систему для запуску нових кібератак.

Приховування слідів присутності відноситься до етапу, коли орган уповноважений на реалізацію заходів кібердорозвідки намагається здійснити атаку не замiченою та не перехопленою, видаливши докази котрі могли б привести його до кримінального переслідування.

Всі добуті розвідувальні дані про вразливості аналізуються та формуються певні пропозиції та висновки, щодо реалізації кібернетичного впливу на противника. Аналітичний звіт являє собою опис ретельного дослідження противника, а також описує результативні показники та підсумки у кількісному та якісному вимірі, які є пріоритетними в оцінці ефективності проведення розвідувальних заходів під час добування інформації про противника.

Кожен з вище зазначених етапів кібернетичної розвідки має свою ціль та мету, яка в кінцевому результаті виконання розвідувальних заходів дає можливість добути бажану інформацію про противника.

Враховуючи масштаб забезпечення кібероборони [2, с. 44], вибудуємо систему із найбільш ймовірних уповноважених органів (суб'єктів) здійснювати кібердорозвідку із складу сектору безпеки та оборони, метою діяльності яких є забезпечення кібероборони (рис.5).

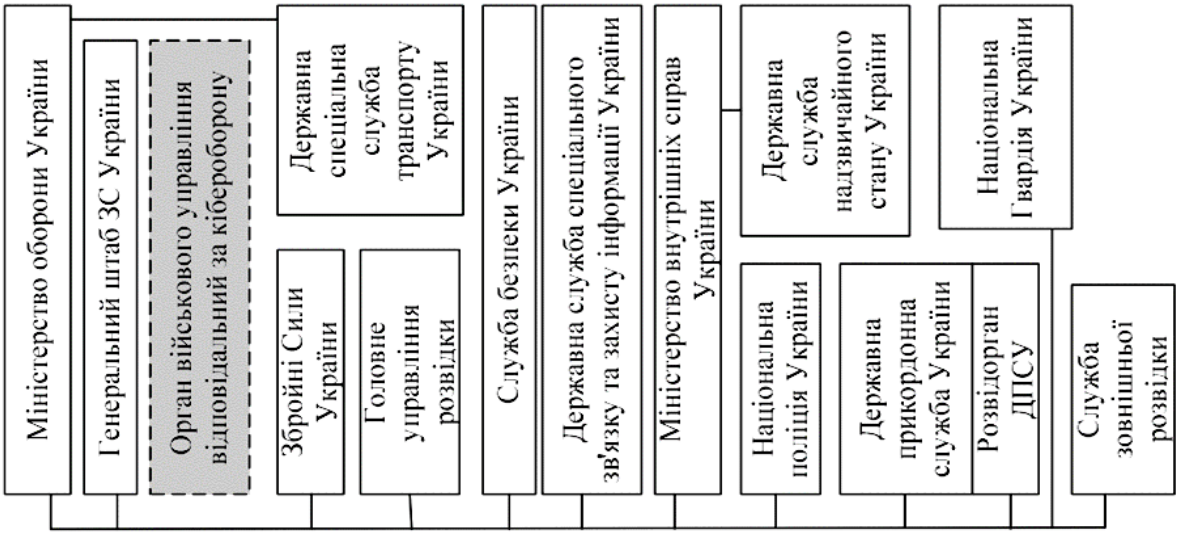

Рис.5. Ймовірні уповноважені органи (суб'єкти) здійснювати кібердорозвідку

Діяльність кібердорозвідки об'єкту противника – це є складовою РІД, являє собою безперервний у часі процес управління розвідувальними органами та містить комплекс заходів з організації та ведення розвідувально-інформаційної роботи для задоволення інформаційних потреб споживачів розвідувальної інформації [13], огляд якого не є предметом нашого дослідження.

Обговорення попередніх результатів. Таким чином, із затвердженням Указу Президента України від 17.09.2021 №473/2021 "Про рішення Ради національної безпеки і оборони України від 20 серпня 2021 року" ознаменувало узаконення адміністративно-правових норм майбутньої кібердорозвідки, як діяльності в кіберпросторі суб'єкта кібероборони. Однак з початком повномасштабної військової агресії Російської Федерації проти України Державні органи та організаційні структури, які є носіями спроможностей [12] виявились в теорії спроможними. Потужну і превентивну допомогу в реалізації кібердорозвідки, як показала практика, надали самоорганізовані не байдужі ІТ-фахівці, які в певній мірі підтвердили раціональність ранішого припущення, щодо необхідності створення гібридних підрозділів військово-цивільного співробітництва.

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).

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Таким чином, за результатами проведеного дослідження можна сформулювати наступні висновки:

1. Лише в 2021 році на законодавчому рівні визначено поняття кібердорозвідка, як діяльність щодо виявлення вразливостей програмного забезпечення, телекомунікаційного обладнання, автоматизованих систем управління силами, зброєю та/або технологічними процесами визначеної цілі (об'єкта кіберінфраструктури).

2. Відсутність чіткого покладання обов'язків виконання діяльності на певний уповноважений орган або сектор безпеки та оборони породжує хаотичність та безвідповідальність. Тому, з початком повномасштабної військової агресії значних успіхів в одержанні відомостей про кібервразливості противника мали самоорганізовані групи ''білих хакерів''.

3. 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.

Перспективи подальших досліджень у даному напрямку. Представлене дослідження не вичерпує всіх аспектів зазначеної проблеми. Теоретичні результати, що одержані в процесі наукового пошуку, становлять підґрунтя для подальшого обґрунтування формалізованого бланку на проведення кібердорзвідки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 Хлапонін, Ю.І., Козубцова, Л.М., Козубцов, І.М., Штонда, Р.М. (2022). Функції системи захисту інформації і кібербезпеки критичної інформаційної інфраструктури. *Кібербезпека освіта, наука, техніка*, 3, 15, 124–134.

2 Вдовенко, С.Г., Даник, Ю.Г., Пермяков, О.Ю. (2020). Досвід розвитку систем кібербезпеки та кібероборони провідних країн світу. *Сучасні інформаційні технології у сфері безпеки та оборони*, 1 (37), 31–48.

3 Бурячок, В.Л., Гулак, Г.М., Хорошко, В.О. (2011). До питання організації та проведення розвідки у кібернетичному просторі. *Наука і оборона*, 2, 19–23.

4 Бурячок, В.Л., Ільяшов, О.А., Гулак, Г.М. (2011). 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*", (pp. 27–32). Київ: НА СБ України.

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

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

7 Чередниченко, О.Ю., Фесьоха, В.В., Процюк, Ю.О., Бондаренко, Т.В. (2018). Аналіз існуючих підходів протидії найпоширенішим кібернетичним втручанням в інформаційно–телекомунікаційні мережі. *Сучасні інформаційні технології у сфері безпеки та оборони*, 2(32), 13–16.

8 Кива, В.Ю., Судніков, Є.О., Войтко, О.В. (2018). Методи розвідки кіберпростору. *Сучасні інформаційні технології у сфері безпеки та оборони,* 3 (33), 45–52.

9 Гаценко, С.С., Ліщенко, О.М., Сотніченко, А.І., Жарков, Я.А. (2020). Математична модель процесу розвідувально-інформаційної діяльності в умовах невизначеності. *Сучасні інформаційні технології у сфері безпеки та оборони*, 1 (37), 77–84.

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

11 Проект Указу Президента України (2021). "Про рішення Ради національної безпеки і оборони України", "Про Стратегічний оборонний бюлетень України", https://www.mil.gov.ua/content/pdf/up_rrnb.pdf.

12 Указ Президента України (2021). "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.

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

14 Мальцева, І., Черниш, Ю., Штонда, Р. (2022). Аналіз деяких кіберзагроз в умовах війни. *Кібербезпека: освіта, наука, техніка*, 4(16), 37–44.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (21), 2023
ISSN 2663 - 4023

Oleksandr A. Ponomarov
head of the Faculty
Military Institute of telecommunications and informatization named after Heroes of Krut, Kiev, Ukraine
ORCID 0009-0008-2320-1549
aleksan_bimer3@ukr.net

Lesya M. Kozubtsova
candidate of Technical Sciences
head of the Department
Military Institute of telecommunications and informatization named after Heroes of Krut, Kiev, Ukraine
ORCID 0000-0002-7866-8575
lesia.kozubtsova@viti.edu.ua

Igor M. Kozubtsov
Doctor of Pedagogical Sciences, Candidate of Technical Sciences, Senior researcher
professor of the Department
Military Institute of telecommunications and informatization named after Heroes of Krut, Kiev, Ukraine
ORCID ID 0000-0002-7309-4365
kozubtsov@gmail.com

Volodymyr O. Tkach
senior researcher at the research department
Military Institute of telecommunications and informatization named after Heroes of Krut, Kiev, Ukraine
ORCID ID 0000-0003-0013-7368
tkachwolodymyr@gmail.com

ADMINISTRATIVE AND LEGAL BASIS FOR AUTHORIZING SECURITY AND DEFENSE SECTOR BODIES TO ORGANIZE CYBER TO INTELLIGENCE ACTIVITIES

Abstract. In a hybrid war, the winner is the party that first creates conditions for violating the target function of the operability of the information security system and cybersecurity of critical information infrastructure facilities. To create prerequisites for a violation of the target function, it is necessary to identify vulnerabilities in the information security system and cybersecurity of enemy critical information infrastructure facilities in advance. This task is performed during Cyber to Intelligence. For a long time, the concept of cyber to intelligence was absent from scientific research, but the activity as such was already carried out in the context of cyber intelligence. Only in 2021, at the legislative level, it was adopted to understand cyber to intelligence as activities aimed at identifying vulnerabilities in software, telecommunications equipment, automated control systems for forces, weapons and/or technological processes of a certain target (cyber infrastructure object). The subject of research in the scientific article is the justification of the administrative and legal foundations of the organization of cyber to intelligence. To achieve the goal and the set task, theoretical research methods were used: generalization of scientific literature; structural and genetic analysis when clarifying the object and subject of research; analytical and comparative analysis when evaluating the novelty of research results; generalization-for formulating conclusions and recommendations. The research results are obtained, the scientific novelty of which consists in summarizing information about a new type of cyber to intelligence activity, a schematic description of the activity process is presented, and the most likely authorized bodies (subjects) for its implementation are identified. The components of cyber intelligence and stages of cyber intelligence are proposed. Prospects for further research in this area. The presented study does not exhaust all aspects of this problem. The theoretical results obtained in the course of scientific research form the basis for further justification of the formalized form for conducting cyber to intelligence.

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

REFERENCES (TRANSLATED AND TRANSLITERATED)

1 Khlaponin, Yu.I., Kozubtsova, L.M., Kozubtsov, I.M., Shtonda, R.M. (2022). Funktsii systemy zakhystu informatsii i kiberbezpeky krytychnoi informatsiinoi infrastruktury. *Kiberbezpeka osvita, nauka, tekhnika*, 3, 15, 124–134.

2 Vdovenko, S.H., Danyk, Yu.H., Permiakov, O.Yu. (2020). Dosvid rozvytku system kiberbezpeky ta kiberoborony providnykh krain svitu. *Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony*, 1 (37), 31–48.

3 Buriachok, V.L., Hulak, H.M., Khoroshko, V.O. (2011). Do pytannia orhanizatsii ta provedennia rozvidky u kibernetychnomu prostori. *Nauka i oborona*, 2, 19–23.

4 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. Zbirnyk materialiv kruhloho stolu "*Aktualni pytannia pidhotovky fakhivtsiv iz rozsliduvannia kiberzlochyniv*", (rr. 27–32). Kyiv: NA SB Ukrainy.

5 Buriachok, V.L., Korchenko, O.H., Buriachok, L.V. (2012). Sotsialna inzheneriia yak metod rozvidky informatsiino-telekomunikatsiinykh system. *Zhurnal «Zakhyst informatsii»*, 14, 4 (57), 5–11.

6 Danyk, Yu.H., Vorobiienko, P.P., Cherneha, V.M. (2019). Osnovy kiberbezpeky ta kiberoborony: pidruchnyk. Odesa: ONAZ im. O.S. Popova.

7 Cherednychenko, O.Yu., Fesokha, V.V., Protsiuk, Yu.O., Bondarenko, T.V. (2018). Analiz isnuiuchykh pidkhodiv protydii naiposhyrenishym kibernetychnym vtruchanniam v informatsiino–telekomunikatsiini merezhi. *Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony*, 2(32), 13–16.

8 Kyva, V.Yu., Sudnikov, Ye.O., Voitko, O.V. (2018). Metody rozvidky kiberprostoru. Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony, 3 (33), 45–52.

9 Hatsenko, S.S., Lishchenko, O.M., Sotnichenko, A.I., Zharkov, Ya.A. (2020). Matematychna model protsesu rozviduvalno-informatsiinoi diialnosti v umovakh nevyznachenosti. *Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony*, 1 (37), 77–84.

10 Ukaz Prezydenta Ukrainy (2016). Stratehiia kiberbezpeky Ukrainy, 96, https://zakon.rada.gov.ua/laws/show/96/2016/ed20160315.

11 Proekt Ukazu Prezydenta Ukrainy (2021). "Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy", "Pro Stratehichnyi oboronnyi biuleten Ukrainy", https://www.mil.gov.ua/content/pdf/up_rrnb.pdf.

12 Ukaz Prezydenta Ukrainy (2021). "Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 20 serpnia 2021 roku" 473/2021, "Pro Stratehichnyi oboronnyi biuleten Ukrainy", https://zakon.rada.gov.ua/laws/show/473/2021.

13 Viiskovyi standart VST 01.101.004 – 2019 (03). Voienna rozvidka. Informatsiino-analitychna diialnist. Terminy ta vyznachennia.

14 Maltseva I., Chernysh Yu., Shtonda R. (2022). Analiz deiakykh kiberzahroz v umovakh viiny. *Kiberbezpeka: osvita, nauka, tekhnika*, 4(16), 37–44.