http://doi.org/10.26565/1727-6667-2024-1-11
УДК 355.3

Живило Євген Олександрович,
кандидат наук з державного управління, докторант кафедри публічної політики
Навчально-наукового інституту «Інститут державного управління»
Харківського національного університету імені В.Н. Каразіна
майдан Свободи, 4, м. Харків, 61022, Україна
ORCID ID: https://orcid.org/0000-0003-4077-7853
e-mail: zhivilka@i.ua

Докіль Валентин Миколайович,
ад'юнкт наукового відділу організації підготовки та атестації
науково-педагогічних кадрів науково-методичного центру організації
наукової та науково-технічної діяльності Національного університету оборони України,
проспект Повітряних Сил, 28, 03049, Київ, Україна
ORCID ID: https://orcid.org/0000-0002-6321-0940
e-mail: v.dokil@ukr.net

НОРМАТИВНО-ПРАВОВІ ШЛЯХИ ВИРІШЕННЯ ІСНУЮЧИХ КОЛІЗІЙ У СФЕРІ КІБЕРБЕЗПЕКИ В УМОВАХ СТВОРЕННЯ КІБЕРСИЛ ЗБРОЙНИХ СИЛ УКРАЇНИ

Анотація. Існуюче поширення та комерціалізація інструментів проведення кібератак змінили баланс сил у кіберпросторі та дозволили широкому колу суб'єктів використовувати кіберінструменти для геополітичного впливу та економічної вигоди. Застосовуємі інструменти, якими можна вільно користуватись, надають безпрецедентні можливості для шпигунства, шахрайства та хакерства, застосування яких має на меті фінансовий зиск, порушення сталого функціонування об'єктів критичної інфраструктури та різних форм власності електронно-комунікаційних систем і мереж.

Динаміка поточної ситуації щодо можливості купувати готові апаратно-програмні рішення та створювати індивідуальні кіберінструменти продовжує "кидати виклик" національній безпеці, комерційному сектору та цивільному населенню.

Розширюючи можливості придбання кіберінструментів на комерційній основі, як державні, так і недержавні суб'єкти можуть швидко переходити від нових загроз до існуючих, тому цей стрибок розглядається як ключовий фактор в ситуації з кіберзахистом. В подальшому це може привести до високого рівня геополітичної нестабільності в конфліктах, які буде складніше передбачити, ніж традиційні військові зміни в балансі сил.

За цих умов вагомим завданням для України є створення умов для захисту суверенітету та забезпечення обороноздатності держави у кіберпросторі шляхом підтримки спроможностей сил оборони здійснювати активний кіберзахист власної інформаційної інфра-

структури і підготовку держави до відбиття воєнної агресії в кіберпросторі як у мирний час так і воєнний стан (особливий період).

З огляду на вищезазначене, у цій роботі проаналізовано чинні нормативно-правові акти держави щодо питань виконання суб'єктами забезпечення кібербезпеки відповідних завдань в рамках виконання заходів з кібероборони держави та національного кіберзахисту з метою розмежування повноважень, встановлення відповідальності за конкретними напрямами діяльності та реалізації пріоритетних завдань у цій сфері.

Ключові слова: *інформаційно-комунікаційні технології, система захисту інформації та кібербезпеки, інформаційні технології, інформаційна безпека, кібербезпека, кібервплив, активні кібердії.*

Як цитувати: Живило Є. О., Докіль В. М. Нормативно-правові шляхи вирішення існуючих колізій у сфері кібербезпеки в умовах створення кіберсил Збройних Сил України. *Теорія та практика державного управління*. 2024. Вип. 1 (78). С. 183–196. http://doi.org/10.26565/1727-6667-2024-1-11

Вступ. З моменту свого створення інформаційно-комунікаційні технології (далі – ІКТ) перетворилися на основу сучасного бізнесу, критично важливих послуг та інфраструктури, соціальних мереж і глобальної економіки в цілому.

Як наслідок, національні лідери почали впроваджувати цифрові стратегії та фінансувати проекти, спрямовані на розширення доступу до Інтернету та використання переваг, що випливають з використання ІКТ, для стимулювання економічного зростання, підвищення продуктивності та ефективності, покращення надання послуг та розширення можливостей, забезпечення доступу до бізнесу та інформації, уможливлення електронного навчання, підвищення кваліфікації робочої сили та сприяння належному врядуванню. Країни не можуть ігнорувати можливості, пов'язані з підключенням та участю в інтернет-економіці.

Хоча залежність наших суспільств від цифрової інфраструктури зростає, технології залишаються вразливими за своєю суттю. Конфіденційності, цілісності та доступності інфраструктури ІКТ загрожують ризики, що швидко розвиваються, зокрема, електронне шахрайство, крадіжка інтелектуальної власності та персональної інформації, перебої в наданні послуг, пошкодження або знищення майна, а також заподіяння шкоди національній безпеці. Трансформаційна сила ІКТ та Інтернету як каталізаторів економічного зростання та соціального розвитку досягла критичної межі, коли довіра громадян та держави до використання ІКТ підривається кібербезпекою (далі – КБ).

При цьому, більшість експертів галузі захисту інформації та КБ з впевненістю зазначають, що розширення вільного "кіберринку" та стабільна розгалуженість платформ кіберінструментів з відкритим кодом наддасть принципіальні привілеї щодо досягнення асиметричної переваги недержавним і державним суб'єктам [1].

Сьогодні Україна має унікальний досвід успішного протистояння у кібервійні. Підтвердженням цього є великий кадровий ресурс ІТ-фахівців, які брали і продовжують брати участь в заходах кібероборони (далі – КО) національного сегменту кіберпростору (далі – КП) на тлі збройної агресії. В свою чергу зазна-

чене вище вимагає від держави розвитку обізнаного в цифровому відношенні суспільства, що є найважливішою сферою її внутрішньої політики. Це підкреслює незаперечний факт, що попит на фахівців з КБ буде постійно зростати з розвитком високотехнологічного суспільства [2].

За цих умов, слід зазначити, що унікальний досвід успішного протистояння в кібервійні включає кілька ключових аспектів:

1. Розвиток кіберінфраструктури, а саме використання сучасних технологій та обладнання, для зміцнення кіберзахисту критичних інфраструктур.

2. Підготовка фахівців, що здійснюється шляхом проведення регулярних тренінгів та навчання кіберфахівців, дозволить оперативно реагувати на нові загрози та адаптуватися до змін у КП.

3. Співпраця з міжнародними партнерами, через обмін інформацією та досвідом, участь у спільних кібероперацiях та залучення до навчань чи тренувань.

4. Інноваційні методи захисту. Використання новітніх методів і технологій для виявлення та нейтралізації кіберзагроз, таких як штучний інтелект, машинне навчання та блокчейн [3].

5. Прозорість та відкритість. Проведення активного інформування громадськості та співпраця з приватним сектором для підвищення обізнаності та підготовки до можливих кіберзагроз.

6. Законодавче регулювання, а саме прийняття та впровадження законів і нормативних актів, які регулюють КБ та захист інформації на державному рівні.

Цей досвід є цінним не тільки для України, але й для всього світу, адже він демонструє, як ефективно протистояти кібератакам і забезпечувати безпеку в умовах сучасних загроз.

Огляд літератури. За результатами аналізу друкованих відкритих джерел, засобів масової інформації та висвітлених інтерв'ю з науковими експертами, суб'єктами КБ та захисту інформації, власниками об'єктів критичної інфраструктури та об'єктів критичної інформаційної інфраструктури було визначено три підходи на яких зосереджена зазначена спільнота. Це пост експлуатація, набуття та нарощення індивідуальних кіберспроможностей. При цьому головним напрямком є створення власного кіберпотенціалу, придбання його із зовнішніх джерел та використання "партнерства як мосту".

Виходячи з цього зазначені підходи, ймовірніше за все залишаться життєздатними в довгостроковій перспективі і, збережуть тенденцію збільшення доступу до різноманітних кіберінструментів або кіберзброї, які можна поєднувати для проведення упереджувальних та деструктивних операцій у КП, спрямованих на збирання, злочинну фінансову вигоду або цифрове стеження.

Так, ще у 2021 році Президент України Володимир Зеленський порушив питання про створення нового окремого роду військ – кіберсил Збройних Сил України, але наразі вони все ще не мають юридичного оформлення. Це може змінитися у 2024 році, оскільки відповідний законопроєкт вже знаходиться на завершальних стадіях.

Як повідомляє популярний український онлайн-журнал про ІТ-бізнес, стартапи, технології та підприємництво AIN, законопроєкт "Про кіберсили Збройних

Сил України" вже на стадії погодження із зацікавленими сторонами як у системі Міністерства оборони, так і зацікавлених суб'єктів Сил оборони та безпеки. Це є фінальним етапом перед винесенням його на розгляд Верховної Ради [4].

За словами керівника служби з питань інформаційної безпеки та кібербезпеки Апарату Ради національної безпеки і оборони України Наталії Ткачук, кіберсили Збройних Сил України матимуть такі функції [5]:

– захисна функція та наступальні кібероперації;

– додаткові функції розвідки або інтеграція з одним з органів розвідки для отримання інформації в інтересах ефективного проведення кібероперацій;

– координація проведення кібероперацій основними суб'єктами національної системи КБ;

– координація взаємодії з міжнародними партнерами та приватним сектором, зокрема шляхом формування кіберрезерву та залучення кіберволонтерів;

– формування кадрового потенціалу української КО в стратегічній і довгостроковій перспективі з урахуванням кон'юнктури оплати праці на світовому ринку ІТ-фахівців.

Отже враховуючи зазначене можна зробити висновок що в найближчому майбутньому рівень обороноздатності держави буде визначатися рівнем готовності Сил оборони та безпеки забезпечувати відбиття воєнної агресії у КП (КО).

Метою статті є розробка та впровадження комплексної правової бази щодо виконання суб'єктами завдань із забезпечення КБ, охоплюючи низку ключових законів та регламентів з визначенням обов'язків та повноважень суб'єктів, а також механізмів функціонування та взаємодії органів і установ у цій сфері.

Методологія дослідження Методологія дослідження нормативно-правових актів держави у сфері КБ передбачає комплексний підхід, яка включає об'єкт дослідження як систему нормативно-правових актів, що регулюють діяльність суб'єктів забезпечення КБ та предмет дослідження, а саме зміст, структура, та взаємозв'язок цих актів; систематизацію актуальних нормативно-правових документів за хронологічним та тематичним принципами; оцінку правової бази з точки зору її відповідності сучасним вимогам КБ, вивчення змісту актів, їх положень та норм, визначення правового статусу суб'єктів забезпечення КБ та їх повноважень; аналіз досвіду інших країн у розробці та впровадженні нормативно-правової бази КБ та порівняння нормативно-правових актів України з міжнародними стандартами та практиками у сфері КБ; формулювання рекомендацій щодо вдосконалення нормативно-правової бази у сфері КБ, з визначенням необхідних змін та доповнень до чинних актів; оприлюднення результатів дослідження у наукових та професійних виданнях, на конференціях та семінарах.

Саме такий методологічний підхід забезпечує систематичне та всебічне дослідження нормативно-правових актів держави щодо питань виконання суб'єктами завдань із забезпечення КБ, що сприятиме вдосконаленню правової бази у цій важливій сфері.

Виклад основного матеріалу та результати дослідження. Наразі КБ в Україні займаються такі державні органи як CERT-UA (урядова команда з реагування на комп'ютерні надзвичайні події, що працює в складі Державної служби

спеціального зв'язку та захисту інформації України) та Національний координаційний центр кібербезпеки при Раді національної безпеки і оборони України [6], який опікується координацією та контролем за діяльністю суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку, гарантування КБ, виявлення кіберзагроз, участь у розробці пропозицій щодо забезпечення кіберзахисту об'єктів критичної інфраструктури тощо.

При цьому формування та реалізацію державної політики у сфері КБ, захист прав і свобод людини і громадянина, національних інтересів України у КП, боротьбу з кіберзлочинністю здійснює Кабінет Міністрів України.

Безпосереднє здійснення заходів щодо запобігання використанню КП у воєнних, розвідувально-підривних, терористичних та інших протиправних і злочинних цілях, а також виявлення і реагування на кіберінциденти та кібератаки, усунення їх наслідків, у межах своєї компетенції, покладено на правоохоронні, розвідувальні, контррозвідувальні органи, суб'єкти оперативно-розшукової діяльності ЗС України та ІВФ.

У цьому контексті вимоги до мінімально необхідного пакету зі створення, впровадження, технічної підтримки та вдосконалення системи менеджменту ІБ і кіберзахисту об'єктів критичної інформаційної інфраструктури фінансового сектору здійснюється Національним банком України [7].

Окремі завдання з КБ, відповідно до нормативно-правових актів України покладені на суб'єкти господарювання, громадян України та об'єднання громадян, які провадять діяльність та/або надають послуги, пов'язані з національними інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом [8].

Проаналізувавши чинну нормативну базу України щодо виконання суб'єктами забезпечення КБ відповідних завдань в рамках КО держави необхідно зазначити, що суб'єкти забезпечення КБ в Україні діють саме в рамках існуючої нормативної площини. Саме національними нормативно-правовими актами визначено їх повноваження, обов'язки та механізми взаємодії у сфері КО держави.

Слід зазначити що Україна активно працює над створенням комплексної системи забезпечення КБ. Так було впроваджено низку законів, які визначають правові та організаційні основи КБ, а саме [8] та [9]. Інформаційна безпека та захист державної таємниці аргументована такими законодавчими актами, як [10] та [11], що забезпечує захист критичної інформації та державної таємниці.

Указом Президента України [12] визначено довгострокові цілі та напрямки розвитку КБ. Постановою Кабінету Міністрів України [13] визначено порядок реагування на кіберзагрози.

Активна співпраця з міжнародними партнерами у сфері КБ щодо уніфікації нормативно-правової бази України з питань кіберзахисту національних інформаційних ресурсів призвела до гармонізації численних існуючих керівних принципів та стандартів відповідно до норм міжнародного права, галузевих стандартів та директив ЄС і НАТО, що зафіксовано у Законах та нормативно-правовій базі України [14].

Проведений аналіз свідчить про системний підхід до забезпечення КБ в Україні, який охоплює різні аспекти від правового регулювання до практичного реагування на загрози.

Деталізуючи зазначене вище необхідно зауважити, що в рамках чинних нормативно-правових актів України суб'єктам забезпечення КБ, в умовах КО держави визначено/встановлено:

– правові основи інформаційної діяльності;
– правові та організаційні основи забезпечення КБ;
– повноваження органів державної влади у сфері КБ;
– завдання для суб'єктів забезпечення КБ;
– механізми взаємодії між суб'єктами забезпечення КБ;
– дії суб'єктів з забезпечення КБ під час кіберінцидентів;
– доступ до інформації та її захист;
– вимоги до забезпечення безпеки інформаційних систем та засобів захисту;
– порядок захисту інформації в інформаційно-комунікаційних системах [15];
– порядок захисту державної таємниці;
– обмеження доступу до інформації, що становить державну таємницю;
– основні напрямки політики у сфері КБ;
– порядок реагування на кіберінциденти та кіберзагрози;
– порядок оновлення стратегії КБ з урахуванням сучасних загроз [16];
– завдання для подальшого розвитку системи КБ України.

Таким чином, враховуючи перевантаження повноважень та виконання невластивих завдань відповідними суб'єктами КБ, в майбутньому, при формуванні кіберсил Збройних Сил України стануть одним із потенційних недоліків, що можуть спричинити наступні проблеми [17]:

1. Розмитість відповідальності. Наявність численних суб'єктів з перекритими повноваженнями може спричинити неясність у визначенні відповідальних за конкретні завдання та реагування на інциденти [18].

2. Уповільнення процесу прийняття рішень. Через необхідність координації між багатьма суб'єктами можуть виникати затримки у прийнятті оперативних рішень та реагуванні на кіберзагрози.

3. Конфлікти повноважень. Можливі конфлікти та непорозуміння між різними суб'єктами КБ щодо сфер їхньої відповідальності та дій.

4. Неефективне використання ресурсів. Дублювання функцій та завдань може призвести до нераціонального використання людських та матеріальних ресурсів.

5. Складність координації. Велика кількість суб'єктів із різними повноваженнями ускладнює процес координації та узгодженості дій під час реалізації заходів з КО.

6. Недостатня узгодженість нормативно-правової бази. Можливі неузгодженості у законодавстві, що регулює діяльність різних суб'єктів КБ, можуть створювати додаткові труднощі в їхній роботі.

Отже зазначені проблематики вказують на необхідність перегляду та оптимізації повноважень відповідних суб'єктів КБ для підвищення ефективності їхньої діяльності та покращення координації дій у сфері КО держави під час формування кіберсил Збройних Сил України та планування на їх застосування.

Тому за результатами проведеної роботи було встановлено та пропонується наступне:

1. В Законі України [8]:

– в частині безпосереднього розроблення і реалізації превентивних заходів суб'єктами забезпечення КБ у межах своєї компетенції визначити головного виконавця, який буде здійснювати координацію та контроль за виконанням суб'єктами забезпечення КБ визначених завдань;

– необхідно визначити головного виконавця, який буде здійснювати координацію та контроль виконаних завдань/заходів з підготовки держави до відбиття воєнної агресії у КП (КО); здійснювати військову співпрацю з НАТО, міжнародними організаціями та іншими суб'єктами оборонної сфери щодо забезпечення безпеки КП та спільного захисту від кіберзагроз в Міністерстві оборони України та Генеральному штабі Збройних Сил України відповідно;

– визначити головного виконавця щодо здійснення розвідувальної діяльність стосовно загроз національній безпеці України у КП, інших подій і обставин, що стосуються сфери КБ серед Служби зовнішньої розвідки України, розвідувального органу Міністерства оборони України та розвідувального органу центрального органу виконавчої влади, що реалізує державну політику у сфері охорони державного кордону.

2. В Указі Президента України [19] одним з пріоритетних завдань правоохоронних, спеціальних, розвідувальних та інших державних органів відповідно до їх компетенції визначена активна та ефективна протидія розвідувально-підривній діяльності, спеціальним інформаційним операціям та кібератакам, російській та іншій підривній пропаганді. За цих умов важливо визначити головного виконавця, який буде здійснювати координацію та контроль за виконанням зазначеного завдання.

3. В Указі Президента України [20]:

– щодо ведення силами оборони узгоджених воєнних (бойових) дій у повітрі, на суші, на морі, в інформаційному просторі, КП як складовій інформаційного простору та з використанням результатів космічної діяльності в інтересах оборони держави також необхідно визначити головного виконавця (ів) за виконанням зазначеного (их) завдання (нь);

– розглядаючи завдання по розвитку спроможностей з ведення протиборства в інформаційному просторі (включаючи КП) Збройними Силами України та іншими складовими сил оборони теж слід визначити головного виконавця, який буде здійснювати координацію та контроль за виконанням зазначеного завдання;

– вивчаючи питання щодо спроможності з ведення протиборства в інформаційному просторі та КП, а саме критерій спроможності – "Створення системи КО для ведення протиборства в інформаційному просторі (включаючи КП)" відповідно покладено на Державну спеціальну службу транспорту Міністерства оборони України, Збройні Сили України, Національну гвардію України, Державну прикордонну службу України, Службу безпеки України, Державну службу спеціального зв'язку та захисту інформації України, Служба зовнішньої розвідки України. Вважається за необхідне доповнити зазначений критерій спромож-

ності Головним управлінням розвідки Міністерства оборони України, як розвідувальний орган України що здійснює розвідувальну діяльність щодо загроз національній безпеці України у КП. При цьому, включити Міністерство оборони України, а Державну спеціальну службу транспорту Міністерства оборони України виключити. Визначити головного виконавця, який буде здійснювати координацію та контроль за виконанням зазначеного завдання;

– розбираючи критерій спроможності "Здатність до забезпечення ефективного кіберзахисту власної інформаційної інфраструктури (критичної інформаційної інфраструктури), проведення превентивних дій щодо виявлення, реагування на кібератаки та інциденти КБ, усунення їх наслідків в умовах ведення противником кіберрозвідки та інтенсивного кібервпливу (кібератак)" який покладено на Головне управлінням розвідки Міністерства оборони України, Державну спеціальну службу транспорту Міністерства оборони України, Збройні Сили України, Національну гвардію України, Державну прикордонну службу України, Службу безпеки України, Державну службу спеціального зв'язку та захисту інформації України, Службу зовнішньої розвідки України вважається за необхідне включити Міністерство оборони України, а Державну спеціальну службу транспорту Міністерства оборони України виключити. Визначити головного виконавця, який буде здійснювати координацію та контроль за виконанням зазначеного завдання;

– в критерії спроможності "Здатність до 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, її призначення, місцезнаходження, технологічні процеси, уразливість, встановлення прихованого контролю, перехоплення та дешифрування керуючих і ресурсних даних та інформації" за напрямком "Спроможності з ведення протиборства в інформаційному просторі та КП" необхідно визначити головного виконавця, який буде здійснювати координацію та контроль за виконанням зазначеного завдання;

– вивчаючи розділ "Спроможності з ведення протиборства в інформаційному просторі та КП" щодо критерію спроможності "Здатність до підготовки та проведення скоординованих демонстраційних кібердій (кібервпливу) у КП щодо запобігання виникненню воєнних конфліктів, стримування та відсічі воєнній агресії в КП" вважається за необхідне доповнити зазначений критерій спроможності Головним управлінням розвідки Міністерства оборони України, Державною прикордонною службою України. Визначити головного виконавця, який буде здійснювати координацію та контроль за виконанням зазначеного завдання;

– розглядаючи критерій спроможності "Здатність організовувати підготовку та проводити кібердії (кібервпливи, кібератаки) із застосуванням усіх видів кіберзброї або захоплення (виведення з ладу, отримання контролю), заподіяння шкоди (каскадний ефект), порушення функціонування об'єктів критичної та інформаційної інфраструктури противника з одночасним приховування слідів своєї діяльності в КП" розділу "Спроможності з ведення протиборства в інфор-

маційному просторі та КП" вважається за необхідне доповнити зазначений критерій спроможності Головним управлінням розвідки Міністерства оборони України та Державною прикордонною службою України. Визначити головного виконавця, який буде здійснювати координацію та контроль за виконанням зазначеного завдання;

– досліджуючи розділ "Спроможності з ведення протиборства в інформаційному просторі та КП", а саме критерій спроможності "Застосування апаратно-програмних комплексів КБ, засобів з кіберзахисту, кіберзброї для вирішення завдань кіберборотьби", що покладено на Державну спеціальну службу транспорту Міністерства оборони України, Збройні Сили України, Національну гвардію України, Державну прикордонну службу України, Службу безпеки України, Державну службу спеціального зв'язку та захисту інформації України, Службу зовнішньої розвідки України вважається за необхідне Державну спеціальну службу транспорту Міністерства оборони України виключити. При цьому пропонується ввести Міністерство оборони України та Головне управлінням розвідки Міністерства оборони України. Визначити головного виконавця, який буде здійснювати координацію та контроль за виконанням зазначеного завдання.

4. Внести відповідні зміни в чинні нормативно-правові акти держави в частині відведення головної ролі у забезпеченні КО у мирний час, в умовах кризових ситуацій, воєнного стану та в особливий період Збройним Силам України, при цьому Генеральному штабу Збройних Сил України, як головному органу із забезпечення КО держави визначити/доручити – формування та реалізацію державної політики щодо забезпечення КО держави; стратегічне планування застосування та координацію діяльності суб'єктів забезпечення КО; прогнозування тенденцій розвитку форм і способів ведення воєнних дій у КП та пов'язаних з ним засобів збройної боротьби; формування вимог до порядку забезпечення КО; організацію впровадження правових, воєнних, організаційно-технічних та інших заходів щодо обмеження доступу або руйнації ресурсів, які використовуються для порушення обороноздатності держави в КП; здійснення міжнародного співробітництва; розробку та видання наказів, директив і оперативних завдань суб'єктам забезпечення КО.

5. Внести зміни у закони України, які регламентують діяльність основних суб'єктів національної системи КБ, виконання завдань з КБ (КО) в межах їхніх компетенцій.

Отже, в цілому перегляд та оптимізація повноважень відповідних суб'єктів КБ є вкрай важливим та необхідним заходом в ході утворення кіберсил як окремого роду військ. В подальшому зазначена організаційна структура забезпечить розбудову, розвиток і набуття нових бойових спроможностей для дій у домені КО держави як складової національної системи КБ; підвищить рівень координованості складових сил оборони, вдосконалить механізм їх консолідованого розвитку та посилення відповідних оперативних спроможностей для забезпечення КО; посилить спроможності сил оборони в ефективній боротьбі з кіберзагрозами воєнного характеру, підвищить готовність до відбиття воєнної агресії у КП та поглибить міжнародне співробітництво у цій сфері.

Висновки та перспективи подальших досліджень. Існуюче поширення та комерціалізація інструментів проведення кібератак змінили баланс сил у КП та дозволили широкому колу суб'єктів використовувати їх для геополітичного впливу та економічної вигоди.

Україна дедалі більше уваги приділяє розвитку й захисту власних інформаційних ресурсів, проводяться заходи розбудови національної системи КБ, створюються або реформуються відповідні державні органи та структури. При цьому зазначене відбувається на тлі повномасштабного вторгнення Російської Федерації на територію України.

Отже, сьогодні закріплення організаційно-правового статусу кіберсил Збройних Сил України відбувається в умовах трансформації системи управління складових сил оборони та безпеки. При цьому залишаються невирішеними питання в нормативно-правовому полі щодо виконання суб'єктами забезпечення КБ відповідних завдань в рамках виконання заходів з КО держави, які унеможливлюють формалізацію безпекової політики в КП.

В цілому, з огляду на зазначене, в статті проаналізовано чинні нормативно-правові акти держави щодо забезпечення КБ. Запропоновано розмежування повноважень основних суб'єктів національної системи КБ, встановлено відповідальність за конкретні напрямами діяльності та реалізації пріоритетних завдань у цій сфері.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Живило Є.О. Геостратегічні гравці сучасного кіберпростору. Загрози, виклики, наслідки. Монографія. Moderní aspekty vědy: XLV. Díl mezinárodní kolektivní monografie / Mezinárodní Ekonomický Institut s.r.o.. Česká republika: Mezinárodní Ekonomický Institut s.r.o., 2024. pp. 29 – 63. URL: http://perspectives.pp.ua/public/site/mono/mono-45.pdf (дата звернення: 29.04.2024).

2. Живило Є. Пошук та засвоєння сучасних кадрових компетентностей сфери кібербезпеки в умовах цифрової трансформації держави. *Актуальні проблеми державного управління*, 2023. № *2*(63), С. 111-127. DOI: https://doi.org/10.26565/1684-8489-2023-2-08 (дата звернення: 29.04.2024);

3. Коваль М., Сова О., Орлов О., Шишацький А., Артабаєв Ю., Шкнай О., Веретнов А., Кошлан О., Живило Є., Живило, І. Удосконалення комплексного управління ресурсами систем зв'язку спеціального призначення. Eastern-European Journal of Enterprise Technologies, 2022. № 5 (9 (119)), С. 34–44. DOI: https://doi.org/10.15587/1729-4061.2022.266009 (дата звернення: 29.04.2024);

4. Законопроєкт про Кіберсили ЗСУ вже обговорюють у МО та Силах оборони. Ми дізнались більше про майбутній рід військ. URL: https://ain.ua/2024/05/08/cyberforce/ (дата звернення: 29.04.2024).

5. Олександр Кузьменко, Законопроєкт про оформлення Кіберсил ЗСУ як окремого роду військ вже на стадії погодження в Міноборони та Силах Оборони. Що відомо. URL: https://dev.ua/news/zakonoproiekt-pro-kibersyly-zsu-1715175332 (дата звернення: 29.04.2024).

6. Живило Є.О., Орлов О.В. Сутність кібербезпеки національного сегменту кіберпростору держави в умовах кризового управління. Публічне управління XXI століття в умовах гібридних загроз*:* зб. наук. матеріалів XXII Міжнародного наукового конгресу, 27 квітня 2022 р. Харків: ХНУ ім. В.Н. Каразіна, 2022. С. 248-254.

7. Onyshchenko S., Zhyvylo Y., Cherviak, A., Bilko S. Determining the patterns of using information protection systems at financial institutions in order to improve the level of financial security. *Eastern-European Journal of Enterprise Technologies*, 2023. № 5 (13 (125)), С. 65–76. DOI: https://doi.org/10.15587/1729-4061.2023.288175 (дата звернення: 29.04.2024).

8. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2469-VIII. Дата оновлення: 28.07.2022. URL:https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 29.04.2024).

9. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.07.1994 р. № 80/94-ВР. Дата оновлення: 28.06.2024. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text (дата звернення: 29.04.2024).

10. Про державну таємницю: Закон України від 21.01.1994 р. № 3855-XII. Дата оновлення: 01.01.2024. https://zakon.rada.gov.ua/laws/show/3855-12#Text (дата звернення: 29.04.2024).

11. Про інформацію: Закон України від 02.10.1992 р. № 2657-XII. Дата оновлення: 27.07.2023. https://zakon.rada.gov.ua/laws/show/3855-12#Text (дата звернення: 29.04.2024);

12. Про рішення Ради національної безпеки і оборони України від 14.05.2021 р. "Про Стратегію кібербезпеки України" : Указ Президента України від 26.08.2021 р. № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення: 29.04.2024).

13. Порядок реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі: Постанова Кабінету Міністрів України від 04.04.2023 р. № 299. Дата оновлення: 04.04.2023. https://zakon.rada.gov.ua/laws/show/299-2023-%D0%BF#n12 (дата звернення: 29.04.2024).

14. О. Данілов: Кіберзахист державних інформаційних ресурсів – важлива складова у процесі цифрової трансформації країни, 2020 [Електронний ресурс]. – Режим доступу: URL: https://www.rnbo.gov.ua/ua/Diialnist/4606.html (дата звернення: 29.04.2024).

15. Kumar V (2020) Cybersecurity challenges and solutions in the telecom industry. Industry wired. URL: https://industrywired.com/cybersecurity-challenges-and-solutions-in-the-telecom-industry/ (дата звернення: 29.04.2024).

16. OAGOV (2020) Cyber security threats against global governments increase exponentially. Open access government. URL: https://www.openaccessgovernment.org/cyber-security-threats-global-governments-increasing/96789/ (дата звернення: 29.04.2024).

17. Живило Є.О., Докіль В.М. Модель методики оцінювання спроможностей військ зв'язку та кібербезпеки Збройних Сил України щодо виконання завдань з відбиття воєнної агресії в кіберпросторі. Сучасні інформаційні технології у сфері безпеки та оборони. К.: Національний університет оборони України імені Івана Черняховсько, 2023. №1 (46). С. 32-41.

18. Deloitte (2021) Global cyber executive briefing: high technology. Case studies,DeloitteDevelopment LLC. URL: https://www2.deloitte.com/ba/en/pages/risk/articles/High-Technology-Sector (дата звернення: 29.04.2024);

19. Про рішення Ради національної безпеки і оборони України від 14.09.2020 р. "Про Стратегію національної безпеки України" : Указ Президента України від 14.09.2020 р. № 392/2020. URL: https://https://www.president.gov.ua/documents/3922020-35037#Text (дата звернення: 29.04.2024);

20. Про рішення Ради національної безпеки і оборони України від 20.08.2021 р. "Про Стратегічний оборонний бюлетень України" : Указ Президента України від 17.09.2021 р. № 473/2021. URL: https://zakon.rada.gov.ua/laws/show/n0063525-21#Text (дата звернення: 29.04.2024).

Стаття надійшла до редакції 30.04.2024
Стаття рекомендована до друку 20.05.2024

Yevhen Zhyvylo, Ph.D. in the field of Public Management and Administration,
Doctoral candidate of the Department of Economic Policy and Management,
Educational and Scientific Institute «Institute of Public Administration»,
V. N. Karazin Kharkiv National University, 4 Svobody Sq., Kharkiv, 61022, Ukraine
ORCID ID: http://orcid.org/0000-0003-4077-7853 e-mail: zhivilka@i.ua

Valentyn Dokil, Adjunct of the scientific department of the organization of training and certification of scientific and pedagogical personnel of the scientific and methodological center of the organization of scientific and scientific and technical activities,
National Defense University of Ukraine, prosp. Povtryanyi Sil, 28, Kyiv, 03049, Ukraine
ORCID ID: http://orcid.org/0000-0002-6321-0940 e-mail: v.dokil@ukr.net

REGULATORY AND LEGAL WAYS TO RESOLVE EXISTING CONFLICTS IN THE FIELD OF CYBER SECURITY IN THE CONTEXT OF THE CREATION OF CYBER FORCES OF THE ARMED FORCES OF UKRAINE

Abstract: The current proliferation and commercialization of cyber attack tools has changed the balance of power in cyberspace and allowed a wide range of actors to use cyber tools for geopolitical influence and economic gain. The applicable tools, which can be freely used, provide unprecedented opportunities for espionage, fraud and hacking, the use of which is aimed at financial gain, disruption of the sustainable functioning of critical infrastructure facilities and various forms of ownership of electronic communication systems and networks.

The dynamics of the current situation regarding the ability to buy ready-made hardware and software solutions and create individual cyber tools continues to "challenge" national security, the commercial sector and the civilian population.

By increasing the ability to acquire cyber tools on a commercial basis, both state and non-state actors can quickly move from new threats to existing ones, so this leap is seen as a key factor in the cyber defense landscape. In the future, this can lead to a high level of geopolitical instability in conflicts that will be more difficult to predict than traditional military changes in the balance of power.Under these conditions, an important task for Ukraine is to create conditions for protecting sovereignty and ensuring the defense capability of the state in cyberspace by supporting the capabilities of the defense forces to carry out active cyber protection of its own information infrastructure and preparing the state to repel military aggression in cyberspace both in peacetime and in a state of war (a special period).

In view of the above, this paper analyzes the current regulatory legal acts of the state regarding the implementation of relevant tasks by cyber security entities within the framework of state cyber defense and national cyber defense measures with the aim of delimiting powers, establishing responsibility for specific areas of activity and implementing priority tasks in this field.

Keywords: *information and communication technologies, information protection system and cyber security, information technologies, information security, cyber security, cyber influence, active cyber actions.*

In cites: Zhyvylo, Ye. O., & Dokil, V. M. (2024). Regulatory and Legal Ways to Resolve Existing Conflicts in the Field of Cyber Security in the Context of the Creation of Cyber Forces of the Armed Forces of Ukraine. *Theory and Practice of Public Administration*, 1 (78), 182–196. http://doi.org/10.26565/1727-6667-2024-1-11 [in Ukrainian].

REFERENCES:

1. Zhyvylo, Y. O. (2024). Geostrategic players of modern cyberspace: Threats, challenges, consequences. In C91 Modern aspects of science: XLV. International collective monograph (pp. 29–63). International Ekonomický Institut s.r.o. (in Czech Republic) URL: http://perspectives.pp.ua/public/site/mono/mono-45.pdf [in Ukrainian] (accessed 29.04.2024).

2. Zhyvylo, Y. (2023). Exploring and acquiring modern human resource competencies in cybersecurity amidst state digital transformation. *Pressing Problems of Public Administration*, 2(63), 111–127. DOI: https://doi.org/10.26565/1684-8489-2023-2-08 [in Ukrainian] (accessed 29.04.2024).

3. Koval, M., Sova, O., Orlov, O., Shyshatskyi, A., Artabaiev, Yu., Shknai, O., Veretnov, A., Koshlan, O., Zhyvylo, Ye., & Zhyvylo, I. (2022). Udoskonalennia kompleksnoho upravlinnia resursamy system zviazku spetsialnoho pryznachennia. *Eastern-European Journal of Enterprise Technologies*, 5(9(119)), 34–44. DOI: https://doi.org/10.15587/1729-4061.2022.266009 [in English] (accessed 29.04.2024).

4. The draft law on Cyber Forces of the Armed Forces is already being discussed in the Ministry of Defense and the Defense Forces. We learned more about the future type of troops. URL: https://ain.ua/2024/05/08/cyberforce/ [in Ukrainian] (accessed 29.04.2024).

5. Kuzmenko, O. (2024). The Draft Law on the Designation of the Cyber Forces of the Armed Forces of Ukraine as a separate type of military is already at the stage of approval by the Ministry of Defense and the Defense Forces. What is known. URL: https://dev.ua/news/zakonoproiekt-pro-kibersyly-zsu-1715175332 [in Ukrainian] (accessed 29.04.2024).

6. Zhyvylo, Y. O., & Orlov, O. V. (2022). The essence of cyber security of the national segment of the state's cyberspace in the context of crisis management. *Public Administration of the XXI Century in the Conditions of Hybrid Threats:* collection of Scientific Materials of the XXII International Scientific Congress, 248–254 [in Ukrainian] (accessed 29.04.2024).

7. Onyshchenko, S., Zhyvylo, Y., Cherviak, A., & Bilko, S. (2023). Determining the patterns of using information protection systems at financial institutions in order to improve the level of financial security. *Eastern-European Journal of Enterprise Technologies*, 5(13(125)), 65–76. DOI: https://doi.org/10.15587/1729-4061.2023.288175 [in Ukrainian] (accessed 29.04.2024).

8. On the main principles of ensuring cyber security of Ukraine: Law of Ukraine dated October 5, 2017 No. 2469-VIII. Date of update: 07/28/2022. https://zakon.rada.gov.ua/laws/show/2163-19#Text [in Ukrainian] (accessed 29.04.2024).

9. On the protection of information in information and communication systems: Law of Ukraine dated July 5, 1994 No. 80/94-VR. Date of update: 06/28/2024. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text [in Ukrainian] (accessed 29.04.2024).

10. On state secrets: Law of Ukraine dated January 21, 1994 No. 3855-XII. Date of update: 01.01.2024. URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text [in Ukrainian] (accessed 23 June 2024).

11. About information: Law of Ukraine dated October 2, 1992 No. 2657-XII. Date of update: 07/27/2023. URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text [in Ukrainian] (accessed 29.04.2024).

12. On the decision of the National Security and Defense Council of Ukraine dated May 14, 2021 "On the Cybersecurity Strategy of Ukraine": Decree of the President of Ukraine dated August 26, 2021 No. 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text [in Ukrainian] (accessed 29.04.2024).

13. Procedure for response by cyber security entities to various types of events in cyberspace: Resolution of the Cabinet of Ministers of Ukraine dated April 4, 2023 No. 299. Date of update: 04.04.2023. URL: https://zakon.rada.gov.ua/laws/show/299-2023-%D0%BF#n12 [in Ukraine] (accessed 29.04. 2024).

14. Danilov, O. (2020). Cyber protection of state information resources is an important component in the process of digital transformation of the country. https://www.rnbo.gov.ua/ua/Diialnist/4606.html [in Ukrainian] (accessed 29.04.2024).

15. Kumar, V. (2020). Cybersecurity challenges and solutions in the telecom industry. Industry Wired. URL: https://industrywired.com/cybersecurity-challenges-and-solutions-in-the-telecom-industry/ [in English] (accessed 29.04.2024).

16. OAGOV. (2020). Cyber security threats against global governments increase exponentially. Open Access Government. https://www.openaccessgovernment.org/cyber-security-threats-global-governments-increasing/96789/ [in English] (accessed 29.04.2024).

17. Zhyvylo, Y. O., & Dokil, V. M. (2023). Model of assessment of military communication and cyber security capabilities of the armed forces of Ukraine for performing tasks of reflecting military aggression in cyber space. *Scientific Journal "Modern Information Technologies in the Sphere of Security and Defence*, 1(46), 32–41. National University of Defense of Ukraine named after Ivan Chernyakhovsko [in Ukrainian] (accessed 29.04.2024).

18. Deloitte. (2021). Global cyber executive briefing: High technology. *Case studies. Deloitte Development LLC*. URL: https://www2.deloitte.com/ba/en/pages/risk/articles/High-Technology-Sector [in English] (accessed 29.04.e 2024).

19. On the decision of the National Security and Defense Council of Ukraine dated September 14, 2020 "On the National Security Strategy of Ukraine": Decree of the President of Ukraine dated September 14, 2020 No. 392/2020. URL: https://www.president.gov.ua/documents/3922020-35037#Text [in Ukrainian] (accessed 29.04.2024).

20. On the decision of the National Security and Defense Council of Ukraine dated August 20, 2021 "On the Strategic Defense Bulletin of Ukraine": Decree of the President of Ukraine dated September 17, 2021 No. 473/2021. URL: https://zakon.rada.gov.ua/laws/show/n0063525-21#Text [in Ukrainian] (accessed 29.04. 2024).

The article was received by the editors 30.04.2024
The article is recommended for printing 20.05.2024