Інформаційна і національна безпека

УДК 342.951

ТКАЧУК Н.А., *кандидат юридичних наук*

ДОСВІД США ЗІ СТВОРЕННЯ ТА РОЗБУДОВИ КІБЕРКОМАНДУВАННЯ: УРОКИ ДЛЯ УКРАЇНИ

Анотація. *У статті досліджено досвід США як країни, яка має найпотужніші кіберспроможності у світі зі створення, забезпечення функціонування та розвитку Кіберкомандування, у контексті можливості використання зазначеного досвіду Україною під час розбудови власних кіберсил.*

Ключові слова: *Кіберкомандування США, кіберсили України, кібервійська, кібероборона, кібероперації.*

Summary. *The article examines the experience of the United States, as a country with the most powerful cyber capabilities in the world, in creating, ensuring the operation and development of the Cyber Command, in the context of possibility of using this experience by Ukraine during the development of its own Cyber Forces.*

Keywords: *US Cyber Command, Cyber Forces of Ukraine, Cyber Defense, Cyber Operations.*

Постановка проблеми. Вже більше року Україна мужньо протистоїть повномасштабному військовому вторгненню рф, одним із компонентів якого є агресія в кіберпросторі. Ця агресія розпочалася ще у 2014 році та зумовила розбудову кібербезпекових спроможностей України для забезпечення захисту та дієвої протидії. Держава продемонструвала стійкість Національної системи кібербезпеки та ефективність кіберзахисту, злагоджену роботу основних суб'єктів забезпечення кібербезпеки, високий рівень державно-приватного партнерства та залучення громадянського суспільства в умовах воєнного стану. Водночас слід визнати, що питання системної розбудови організаційно-правових засад та спроможностей кібероборони на стратегічному та тактичному рівнях у розрізі діяльності Збройних сил України залишається невирішеним.

14 травня 2021 року було прийняте рішення Ради національної безпеки і оборони України "Про невідкладні заходи з кібероборони держави", введене в дію Указом Президента України 26 серпня 2021 року № 446, спрямоване на невідкладне створення у системі Міністерства оборони України кібервійськ та набуття ними відповідних спроможностей [1]. Зазначене завдання було закріплене в новій Стратегії кібербезпеки України [2] як стратегічна ціль номер один, а також деталізоване у Плані її реалізації [3].

Натомість ще й досі не завершена робота над формуванням відповідної законодавчої бази для створення та діяльності кібервійськ (кіберсил), як окремого роду військ (сил), а також вироблення стратегічної концепції їх функціонування.

У цьому контексті є важливим вивчення досвіду провідних країн світу, насамперед ЄС та НАТО, які вже пройшли цей шлях, для врахування такого досвіду у розбудові вітчизняних кіберсил. Безумовно, досвід будь-якої країни не може бути скалькований нашою державою без урахування особливостей функціонування вітчизняної системи національної безпеки та кібербезпеки зокрема, правового поля та безпекового середовища.

Водночас потребує обов'язкового дослідження досвід Сполучених Штатів Америки – однієї із небагатьох кібер-наддержав у світі, яка одна із перших розбудувала власні спроможності із кібероборони та ще у 2009 році створила Кіберкомандування (USCYBERCOM) – об'єднане бойове командування збройних сил США, яке на сьогодні вже набуло повної оперативної готовності.

Результати аналізу наукових публікацій. Дослідження функціонування Кіберкомандування США розглядалося у роботах іноземних та вітчизняних науковців: Д. Дубова [4], М. Сміта [5; 6], Е. Ракс [7], Дж. Пейн [8], Деппа К. [9] та інших. Водночас, на сьогодні практично відсутні наукові публікації вітчизняних авторів, присвячені аналізу досвіду США зі створення та функціонування Кіберкомандування у контексті визначення кращих практик, які варто врахувати Україні в процесі розбудови власних спроможностей з кібероборони.

Метою статті є визначення концептуальних засад діяльності, а також розбудови Кіберкомандування США, для врахування досвіду Сполучених Штатів у ході створення українських кіберсил.

Виклад основного матеріалу. USCYBERCOM було створено у 2009 році як відповідь на кібератаки рф. Восени 2008 хакери рф проникли у внутрішню таємну мережу Пентагону SIPRNet, в той час Міністерство оборони США навіть не мало спроможностей оцінити масштаби загрози, кількість скомпрометованих пристроїв, об'єми інформації, що була викрадена зловмисниками, а також куди ця інформація витекла. Операція з ліквідації наслідків (під кодовою назвою Buckshot Yankee) зайняла у США більше року [10].

Ця безпрецедентна кібератака та неготовність до протидії спричинили кардинальну зміну підходів до кібербезпеки в системі МО США – із питання, що було суто у компетенції системних адміністраторів МО, воно стало пріоритетом стратегічного рівня [11].

Кіберкомандування США було створено на базі Агентства національної безпеки (штаб-квартира АНБ – Форт Джордж Мід (штат Меріленд) – ключової технічної розвідки країни. Ці дві структури розташовані в одній будівлі, використовують спільний технічний і кадровий ресурс та мають спільного керівника, який очолює ці дві структури [12].

Статус USCYBERCOM було підвищено у 2017 році до рівня Об'єднаного бойового командування шляхом виключення зі складу Об'єднаного стратегічного командування ЗС США [13].

Незважаючи на те, що Кіберкомандування США створювалося суто як структура із захисним мандатом – його основне завдання полягало у захисті військових систем США від ворожих дій в кіберпросторі – діяльність Кіберкомандування почала включати і наступальні операції, спрямовані на забезпечення національних інтересів.

Прикладом такої операції, інформація про яку наявна у відкритих джерелах (відбулася вже після загальновідомої операції STUXNET, у ході якої було виведено з ладу технологічні потужності зі збагачення урану ядерної програми Ірану), є операція "Nitro Zeus" під керівництвом генерала Пола Накасоне, який пізніше очолив Кіберкомандування.

Ця операція полягала у забезпеченні можливості знищити протиповітряну систему захисту Ірану, системи зв'язку та енергозабезпечення за допомогою кіберспроможностей. Для цього США глибоко проникло в іранські мережі і навіть системи управління терористичної організації – Корпусу вартових Ісламської революції.

Це була надзвичайно масштабна кібероперація із залученням сотень військових і цивільних. Але день "Х" так і не настав – дипломатичні заходи дозволили уникнути ескалації конфлікту шляхом підписання у 2015 році ядерної угоди Ірану [14].

На думку автора, проведення наступальних операцій на кшталт згаданої вище – отримання прихованого контролю над військовими системами противника із можливістю їх знешкодження у разі ескалації загрози національній безпеці та обороні, а також знешкодження технічних спроможностей, які потенційно можуть використовуватися зловмисними акторами проти національних інтересів має стати одним із завдань кіберсил України.

Саме таку операцію зі знешкодження технічних спроможностей противника було у 2018 році санкціоновано Президентом США Д. Трампом. 5 листопада 2018 року, напередодні виборів у США, USCYBERCOM, діючи на основі наявних розвідданих щодо можливого втручання рф у виборчий процес, на кілька днів повністю заблокувало роботу фабрики рф-тролів – Агентства Інтернет-досліджень, розташованого у санкт-петербурзі [15]. Крім цього, за словами очільника Кіберкомандування США П. Накасоне, демонстрація наступальних спроможностей з боку США стала важелем стримування для супротивників. Так, у наступні роки рівень атак та спроб протиправного впливу на США під час виборчого процесу став набагато меншим [16].

Слід зазначити, що це була перша наступальна кібероперація, проведення та санкціонування якої відкрито визнало керівництвом країни. Саме за часів президентства Д. Трампа було значно розширено мандат USCYBERCOM на проведення наступальних кібероперацій. Так, у 2018 році Трамп фактично легалізував та розширив повноваження Кіберкомандування щодо наступальних кібероперацій, надавши дозвіл на проведення підривної діяльності в кіберпросторі на межі військових дій та на випередження дій потенційних ворогів [17].

Саме впровадження принципів захисту на випередження та постійного залучення дозволило змінити позицію Міністерства оборони США та USCYBERCOM у кіберпросторі з реактивної на проактивну.

Принцип "захищатися на випередження" (defense forward) полягає в наступному – Сполучені Штати захищатимуться, щоб припиняти зловмисну кіберактивність у її джерелі, включно з діяльністю, яка є нижчою за рівень збройного конфлікту. Це означає, що якщо пристрій, мережа, організація чи держава-супротивник визначені як загроза мережам і установам США чи активно атакують їх у кіберпросторі або через нього, вони можуть очікувати, що Сполучені Штати змусять їх за це заплатити [18].

Другий ключовий принцип діяльності Кіберкомандування США це "постійне залучення" (persistent engagement). Відповідно до нього кіберфахівці постійно працюють над виявленням і припиненням кіберзагроз, погіршенням можливостей і мереж противників, безперервним посиленням кібербезпеки інформаційної мережі Міністерства оборони США, яка також підтримує відповідні місії [19].

Керівництво Кіберкомандування проілюструвало застосування цього принципу в ході проведення наступальної операції проти "фабрики тролів" рф [16]. Цій операції передувала ретельна підготовка заздалегідь, наступним етапом був безпосередній вплив на мережі супротивника у визначений час і блокування їх роботи, після досягнення визначеної мети було вжито також інший компонент заходів заключного етапу та аналіз впливу операції на дії супротивника у подальшому. Тобто дії Кіберкомандування були системними та безперервними, складалися із різних етапів та були підпорядковані єдиному стратегічному задуму.

Ще одним із напрямів діяльності Кіберкомандування є операції "полювання на випередження" (hunt forward) – це суто захисні операції за кордоном, які проводяться на запит партнерської країни, що приймає. Метою таких операцій є виявлення ворожої активності в мережах країни – партнера у взаємодії із місцевими кібербезпековими органами. Така допомога є корисною і для США, адже аналітика кіберзагроз, що збирається фахівцями Кіберкомандування, зокрема нові методи, тактика та інструментарій ворожих акторів, враховується у заходах із посилення кібербезпеки США [20].

Починаючи з 2018 року Кіберкомандування провело кілька десятків подібних операцій, спільно з такими країнами як Естонія, Литва [21], країни Латинської Америки [22] тощо. Одна з найбільших команд Хант Форвад була розгорнута в Україні, починаючи з 2021 року і до моменту повномасштабного військового вторгнення рф. Спільно із українськими кіберіфахівцями вживалися заходи із виявлення ворожої активності в українських системах та протидії масованим кібератакам з боку рф, зокрема тим, які відбулися у середині січня 2022 року та передували вторгненню [23].

Враховуючи набутий Україною досвід у протистоянні кіберагресії рф як елементу повномасштабного військового вторгнення, автор вважає, що проведення аналогічних кібероперацій українськими кіберсилами із надання підтримки дружнім країнам могло б стати суттєвим внеском у систему колективної кібербезпеки демократичного світу, а також сприяти ситуаційній обізнаності вітчизняних сил щодо новітніх загроз та механізмів їх реалізації. Базовою основою для взаємодії у цьому напрямі діяльності може слугувати приєднання у 2022 році України до Об'єднаного центру передових технологій з кібероборони НАТО та підписання відповідної Технічної угоди про співпрацю [24].

На сьогодні основними завданнями Кіберкомандування США є такі [25]:

1. Захист інформаційних систем Міністерства оборони від усіх кібератак і вторгнень.

2. Посилення здатності країни протистояти кібератакам і реагувати на них. Командування надає варіанти для політиків та використовує свої міжвідомчі та міжнародні зв'язки для виявлення та припинення зловмисної кіберактивності, перш ніж вона загрожуватиме критичній інфраструктурі та ключовим ресурсам країни.

3. Здійснення повного спектра операцій у кіберпросторі, щоб допомогти бойовим командирам і Об'єднаним силам у досягненні цілей їх місії в кіберпросторі та через нього. Кібероперації забезпечують безпеку мереж, даних і систем зброї по всьому світу, використовуючи свої повноваження, щоб погіршити, нейтралізувати та знищити можливості зловмисних кіберакторів та іноземних держав-супротивників.

Кібероперації здійснюються через різні компоненти USCYBERCOM. До них входять 133 команди Сил Національної Кібермісії (CMF), Штаб об'єднаних сил (JFHQ-DODIN), Сили Національної Кібермісії (CNMF), Об'єднана оперативна група Ares та відповідні кіберкомпоненти видів збройних сил – Армійського кіберкомандування (ARCYBER), Кіберкомандування Корпусу морської піхоти (MARFORCYBER), Кіберкомандування флоту/Десятий флот (FCC/10F), Кіберкомандування ВПС/16-тої повітряної армії (AFCYBER) і Кіберкомандування берегової охорони (CGCYBER).

Команди Сил Національної Кібермісії є основою Кіберкомандування США, що залучене до проведення наступальних та оборонних операцій, їх загальна чисельність становить приблизно 5800 осіб. У 2024 році заплановане збільшення кількості команд до 147 [26].

Слід зазначити, що в США відсутній окремий закон, яким регулюється діяльність та організаційно-правові засади функціонування Кіберкомандування. Натомість у своїй діяльності Кіберкомандування керується: Національною кіберстратегією США [27] та Кіберстратегією Міністерства оборони США [28], іншими нормативно-правовими актами, а також актами Президента США та відомчими підзаконними нормативно-правовими актами Міноборони США, зокрема закритого характеру. Проведення Кіберкомандуванням наступальних кібероперацій, що матимуть значний ефект та вплив на супротивника, має бути погоджене із керівництвом Міноборони та президентом країни [29].

Ще однією особливістю діяльності USCYBERCOM є специфічний підхід до розуміння суверенітету у кіберпросторі. Фактично США вважає, що у разі загрози національним інтересам, Кіберкомандування може проводити операції в мережах (кіберпросторі) інших (третіх) країн, які використовуються зловмисними акторами для проведення кібератак на США. Водночас ці країни можуть бути сповіщенні американською стороною про такі заходи з боку USCYBERCOMMAND, а можуть і ні. Також, США фактично не доєдналося до підходів, закріплених в Талліннській настанові щодо застосування норм міжнародного гуманітарного права до проведення кібероперацій в умовах воєнного та мирного часу. Така позиція надає США більшої маневреності у захисті власних інтересів у кіберпросторі.

Характерним у діяльності USCYBERCOM є повна інтеграція спроможностей із АНБ – працівники Кіберкомандування та АНБ працюють разом в одному приміщенні та використовують єдину технічну інфраструктуру, що належить АНБ [30].

Цікаво, що ще з моменту створення Кіберкомандування неодноразово порушувалося питання розділення цих організацій, зокрема припинення їх перебування під керівництвом однієї й тієї ж військової особи. Основні аргументи були такі: ці дві посади передбачають дуже велику відповідальність, щоб з нею могла впоратися одна людина, Кіберкомандування США потребує власного лідера, щоб стати повноцінною бойовою силою, а також ці дві організації мають принципово різні завдання та місії.

Так, місія Кіберкомандування полягає у виведенні з ладу та руйнуванні мереж противника, коли це необхідно, захист країни від кіберзагроз критично важливим системам, а також кіберзахист військових систем.

Незважаючи на те, що АНБ виконує теж окремі функції із кіберзахисту, зокрема систем, де циркулює інформація з обмеженим доступом, основна місія АНБ полягає у проведенні технічної (електронної) розвідки щодо закордонних цілей з метою збору розвідувальної інформації про ворога та іноземні держави [31].

Зокрема за впровадження таких змін активно взявся Б. Обама під час свого президенства. Він наголошував, що незважаючи на те, що колись подвійна посада була доцільна, щоб дати можливість новонародженому Кіберкомандуванню використовувати розширені можливості та досвід АНБ, зараз Кіберкомандування вже дозріло до такого рівня, коли йому потрібен власний лідер.

У 2013 році ця ініціатива щодо розділення посад була практично реалізована Обамою, але його відмовила від неї група високопосадовців на чолі із тодішнім керівником АНБ Александром Кітом, які наголошували, що ці дві структури повинні мати спільного керівника, щоб забезпечувати можливість використання Кіберкомандуванням ресурсів АНБ. Тож це питання було відкладене і мова почала йти про поступовий перехід, який би не завадив ефективності Кіберкомандування.

У серпні 2018 року новий керівник Кіберкомандування генерал Пол Накасоне також подав на розгляд президентові свої рекомендації щодо збереження наявної

“подвійної” посади, наголошуючи, що Кіберкомандування все ще потребує розвідувальної підтримки з боку АНБ, адже для проведення кібероперацій Кіберкомандування спирається саме на розвідувальну інформацію, отриману від АНБ. Для розвитку власних розвідувальних спроможностей Накасоне створив у структурі Кібркомандування підрозділ, який займається криптографією [32].

У 2022 році знову повернулися до перегляду цього питання на рівні вищого керівництва країни і було прийняте практично однозначне рішення, що розподіл посад є непотрібним, адже забезпечує ефективну роботу і Кіберкомандування і АНБ, зокрема у спільній роботі щодо протидії рф у кіберпросторі.

Як до того наголошував П. Накасоне, це дає швидкість, спритність та злагодженість дій, а рішення, яке буде прийняте, має бути найкращим не для Кіберкомандування, не для АНБ чи розвідувальної спільноти, а для країни [33].

20 липня 2023 року під час виступу в Сенаті кандидат на посаду нового очільника Кіберкомандування та АНБ генерал повітряних сил США Тімоті Хоф, також наголосив на необхідності збереження єдиного керівництва для цих двох відомств, аргументуючи, що це дозволяє ще на початку планування кібероперацій розуміти як захистити джерела розвідданих і при цьому отримати той результат, який є необхідним [34].

Для забезпечення ще більшої координації та взаємодії у сфері кібероборони та проведення кібероперацій між Кіберкомандуванням та АНБ у травні 2023 року було створено Інтегрований кіберцентр, а також Об’єднаний центр операцій, на що було витрачено 500 мільйонів доларів [35].

Він став платформою, яка об’єднала військову та розвідувальну спільноту, інші федеральні агенції, а також міжнародних партнерів з метою кращої синхронізації, координації та деконфліктації кібероперацій. До цього і у АНБ і у Кіберкомандування були свої відомчі центри проведення кібероперацій, фактично “розділені дверима”, але як зазначали фахівці цих відомств “насправді між ними був цілий світ”. Раніше навіть фізично було неможливо розмістити разом фахівців усіх відомств через обмеження наявних приміщень. Але кібербезпека та проведення кібероперацій це виключно “командна гра”, і саме цей принцип відображає створення Об’єднаного кіберцентру, наголошував Чарльз Мур, колишній заступник Командувача кіберсил, який єдиний мав унікальний досвід керувати процесами і у старій, і в новій парадигмі на рівні J3 Кіберкомандування. “В епоху цифрової конвергенції ми зрозуміли, що всі державні структури мають працювати разом, спільно з нашими друзями та союзниками, а також приватним сектором, щоб ефективно боротися з багатьма зловмисниками, які загрожують країні”, – зазначив він у інтерв’ю виданню DefenseScoop у травні 2023 року [36].

До роботи в об’єднаному центрі залучені представники ФБР, МВБ, країн, які є учасниками розвідувального союзу “5 очей” [37]. “Ці партнери не просто бачать інформацію Кіберкомандування та АНБ, вони мають прямі канали доступу до інформації, що надходить із їхніх систем, з їхніх організацій та країн. Це дозволяє обмінюватися даними в реальному часі та формує загальну єдність зусиль, що усуває велику кількість потенційної плутанини, дублювання зусиль, допомагає встановити чіткі ролі та обов’язки, а також дозволяє нам працювати швидко та гнучко”, – зазначив Мур. Також, перевагою створення Центру стала можливість застосувати інструменти, які дозволяють бачити дружні сили в кіберпросторі та їхню готовність, що значно оптимізує деконфліктацію в ході проведення кібероперацій.

За оцінкою фахівців, без переваг, властивих Інтегрованому кіберцентру, тобто дієвої координації всіх державних гравців, проведення спільних кібероперацій та

безперешкодною взаємодії та обміну даними як між ними, так і міжнародними партнерами, Кіберкомандування США просто не змогло б на такому рівні проводити всі кібероперації, здійснені протягом останніх 5 років [36].

Висновки.

Отже, за останні 14 років США вдалося створити та забезпечити ефективний розвиток структури, яка є ключовою у питанні кібероборони країни – USCYBERCOM, що пройшла трансформацію від виконання суто захисних функцій до проведення масштабних наступальних кібероперацій стратегічного рівня та надання допомоги (експортування свого досвіду та можливостей) іншим країнам, забезпечивши США статус кібер-наддержави.

Україна також має необхідний потенціал стати надпотужною кібердержавою шляхом створення кіберсил у структурі ЗСУ, які зможуть проводити наступальні кібероперації на кшталт США. Перевага України в унікальному досвіді, який ми вже маємо із протидії кіберагресії рф.

Створення кіберсил, розбудова їх спроможностей та інтеграція кіберкомпонента у проведення військових операцій потенційно зможе стати альтернативою ядерного стримування, збільшить ефективність ЗСУ та підвищить авторитет України на міжнародній арені. Враховуючи розвиток кібертехнологій та штучного інтелекту, а також того, що кіберагресія з боку рф триватиме у гібридному форматі навіть після припинення повномасштабного військового вторгнення, держава не повинна зволікати із розбудовою національних кібероборонних спроможностей.

У цьому контексті, серед основних висновків та уроків для України щодо аналізу досвіду США, можна виділити наступні:

1. *Ключова перевага Кіберкомандування США полягає у забезпеченні можливості проводити не лише захисні, але й наступальні кібероперації, для чого було створене відповідне нормативно-правове поле, технічні та кадрові спроможності.* Наступальні дії американського Кіберкомандування слугували демонстрацією сили та певною мірою є важелем стримування супротивників щодо кіберагресії проти США (наприклад, повне блокування Кіберкомандуванням США роботи “фабрики тролів” рф для унеможливлення втручання в американські вибори).

Враховуючи, що кіберагресія рф проти України триватиме і після завершення прямих воєнних дій на території України та реалізовуватиметься у формі гібридних операцій нижче порогу реагування з урахуванням норм міжнародного гуманітарного права – ключовим завданням для України є забезпечення власних наступальних спроможностей на випередження для протидії потенційним загрозам та захисту національних інтересів. Тому окрім захисної функції під час створення Кіберкомандування в складі ЗСУ повинен обов’язково передбачатися компонент здійснення наступальних кібероперацій (заходів активної кібероборони).

2. *Без інтеграції розвідувального компонента неможливо забезпечити ефективність кіберсил у частині проведення операцій.* Не зважаючи на те, що США не стали створювати орган, який би мав широкі повноваження проводити як наступальні/оборонні кібероперації, так і здійснювати розвідувальну діяльність – організаційно-правові засади Кіберкомандування сформовані таким чином, що забезпечують повною мірою інтеграцію Кіберкомандування та потужного органу технічної розвідки – Агенства національної безпеки США. Зокрема, ці дві структури мають єдиного керівника, територіально розташовані в одному приміщенні. Кіберкомандування при плануванні та проведенні кібероперацій повною мірою використовує технічні та кадрові спроможності АНБ, як однієї із найпотужніших у світі

електронних розвідок. І, незважаючи на тривалі дебати, щодо розділення цих структур, у результаті – розділення було визнане недоцільним, як таке, що значно знизить ефективність проведення США кібероперацій.

Таким чином, без отримання додаткових розвідувальних функцій (за прикладом Сил спеціальних операцій ЗС України) або інтеграції з одним із розвідувальних органів (наприклад, ГУР МО України), яка забезпечуватиме безперешкодну взаємодію як на стратегічному, так і тактичному рівнях, ефективність проведення кібероперацій українськими кіберсилами буде недостатньою.

3. *Важливим завданням, яке має забезпечити Кіберкомандування, є координація кібероперацій на міжвідомчому рівні, а також з міжнародними партнерами.* Зокрема, в Кіберкомандуванні США для цього було створено Об'єднаний центр кібероперацій, до якого увійшли представники як державних структур (ФБР, МВБ тощо), так і міжнародних партнерів (країни розвідувального союзу "5 очей"). Водночас досвід США довів, що для забезпечення ефективності така координація має здійснюватися не лише формально, а шляхом створення спільного робочого простору (об'єднання фахівців відповідних органів у єдиному приміщенні) та забезпечення спільного доступу до закритих мереж та інформації один одного, зокрема з використанням технічних можливостей бачити спроможності та рівень готовності інших.

4. *Одним із основних завдань українського Кіберкомандування (органа управління кіберсил) має обов'язково стати забезпечення координації проведення кібероперацій.* Основними суб'єктами національної системи кібербезпеки (відповідно до їх компетенції), а також координації взаємодії із міжнародними партнерами та приватним сектором (зокрема, шляхом формування кіберрезерву та залучення кіберволонтерів на законних підставах). Це значно підвищить ефективність кібероперацій, сприятиме економії ресурсів, сил та засобів, а також забезпеченню законності, відповідальності та підзвітності щодо їх проведення.

5. *В США не має окремого закону, який би визначав організаційно-правові засади створення та функціонування Кіберкомандування*. Зокрема у своїй діяльності Кіберкомандування керується законодавством у сфері безпеки і оборони, а також підзаконними нормативно-правовими актами. Цей досвід вважаємо за доцільне врахувати у формуванні правового поля щодо кіберсил України. Автор вважає що немає потреби у розробці окремого детального закону, присвяченого функціонуванню кіберсил, адже більшість практичних питань повинно врегульовуватися підзаконними НПА, зокрема із закритим доступом. Натомість на законодавчому рівні достатньо внести точкові зміни у законодавство (закони України "Про Збройні сили України", "Про оборону України", "Про розвідку", "Про основні засади забезпечення кібербезпеки України" тощо) для забезпечення основних правових засад функціонування кіберсил.

Слід враховувати, що правова система США значно відрізняється від української, а також, що створення кіберсил, які матимуть змогу проводити наступальні кібероперації, потребуватиме з боку України прозорості, відповідальної поведінки, суворого дотримання вимог не лише національного, але й міжнародного права, впровадження дієвого демократичного цивільного контролю (насамперед парламентського), а головне – визначення чіткого бачення цього процесу. *Тому пропонується розробити та у подальшому затвердити Указом Президента України Концепцію створення кіберсил України, яка визначатиме основні етапи, цілі, завдання, принципи створення, функціонування, підзвітності й взаємодії кіберсил як окремого роду сил Збройних сил України, результати, які має досягнути України шляхом їх створення, а також*

визначатиме загальні засади щодо формування кіберрезерву та проведення кібероперацій.

6. *Кіберкомандування США здійснює не лише наступальні кібероперації (або операції активної кібероборони), але й виконує функції кіберзахисту систем МО США.* Більше того, наступальні функції Кіберкомандування поступово трансформувалися з виконання саме захисних завдань. Навіть операції hunt forward, у ході яких Кіберкомандування надає підтримку партнерським країнам із виявлення зловмисників у мережі та локалізації кібератак – вважаються також суто захисними кібероперaціями. У цьому контексті виникає потреба чіткого концептуального визначення: чи буде компонент кіберзахисту, зокрема кіберзахисту ЗСУ, який зараз забезпечують війська зв'язку та кібербезпеки ЗСУ, входити до повноважень кіберсил як окремого роду сил ЗС України. У такому випадку існує потреба у переформатуванні також структури і функціональних завдань зазначеного роду військ. На нашу думку, це потребує додаткової наукової та експертної дискусії.

7. *Кіберкомандування США має більш гнучку кадрову політику у порівнянні з іншими структурами ЗС США*. По-перше, це стосується інших вимог до кандидатів на роботу до Кіберкомандування (фізична підготовка та стан здоров'я), по-друге – дозволена значна частина цивільного персоналу, і по- третє – впроваджено особливий механізм нарахування заробітної плати та інші бонуси для стимулювання роботи висококваліфікованих фахівців у сфері кібербезпеки та ІТ-технологій [38 – 40]. Як показала практика та досвід України, без забезпечення цих елементів кадрової політики (і в першу чергу – це конкурентноспроможна заробітна плата) втримати гідного спеціаліста у державному секторі кібербезпеки, зокрема кібероборони, неможливо. Звичайно, воєнний стан змінив цю ситуацію шляхом застосування можливостей мобілізації кращих фахівців приватного сектору, але таке рішення може розглядатися лише як тимчасове. Формування кадрового потенціалу української кібероборони у стратегічній та довгостроковій перспективі має враховувати кон'юнктуру оплати праці на світовому ринку ІТ-фахівців.

Використана література

1. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про невідкладні заходи з кібероборони держави": Указ Президента України від 26.08.21 р. № 446/2021. URL: **https://www.president.gov.ua/documents/4462021-40009**

2. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про стратегію кібербезпеки України": Указ Президента України від 26.08.21 р. № 447/2021. URL: https://www.president.gov.ua/documents/4472021-40013

3. Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року "Про План реалізації Стратегії кібербезпеки України": Указ Президента України від 01.02.22 р. № 37/2022. URL: https://www.president.gov.ua/documents/372022-41289

4. Дубов Д.В. Кіберпростір як новий вимір геополітичного суперництва: монографія. URL: https://niss.gov.ua/sites/default/files/2015-02/Dubov_mon-89e8e.pdf

5. Smeets Max "No shortcuts". URL: https://global.oup.com/academic/product/no-shortcuts-978 0197661628?cc=us&lang=en&

6. Smeets, Max "An Outcome-Based Analysis of U.S. Cyber Strategy of Persistence and Defend Forward". URL: https://www.lawfaremedia.org/article/outcome-based-analysis-us-cyber-strategy-per sis tence-defend-forward

7. Ruckes, Amy "The Development of the U.S. Cyber Command". URL: https://www.resear chgate.net/publication/370303871_Working_Paper_The_Development_of_the_US_Cyber_Command

8. Pane, James. “Cyber Warfare and U.S. Cyber Command”. URL: https://www.heritage.org/military-strength/assessment-us-military-power/cyber-warfare-and-us-cyber-command

9. Deppa, Catherine S. “U.S. Cyber Command: An Overview”. *American Intelligence Journal*. 34, no. 1 (2017): 12-15. URL: https://www.jstor.org/stable/26497111

10. Jason Healey, A Fierce Domain: Conflict in Cyberspace, 1986 to 2012 (Vienna: Atlantic Council, 2013), 1750, Kindle.

11. Insiders Doubt 2008 Pentagon Hack Was Foreign Spy Attack (Updated). URL: https://www.wired.com/2010/08/insiders-doubt-2008-pentagon-hack-was-foreign-spy-attack

12. URL: https://www.heritage.org/defense/report/should-cyber-command-and-the-nsa-have-separate-leadership-how-decide

13. URL: https://www.cybercom.mil/About/History

14. URL: https://www.nytimes.com/2018/06/17/us/politics/cyber-command-trump.html

15. URL: https://www.nytimes.com/2020/07/11/us/politics/trump-russia-cyber-attack.html

16. URL: https://therecord.media/cyber-command-conducted-offensive-operations-to-protect-mid term-elections

17. URL: https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html

18. URL: https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_S UM MARY_FINAL.PDF

19. URL: https://www.cybercom.mil/Media/News/Article/3198878/cyber-101-defend-forward-and-persistent-engagement/

20. URL: https://www.cybercom.mil/Media/News/Article/3218642/cyber-101-hunt-forward-operations/#:~:text=Hunt%20Forward%20Operations%20(HFOs)%20are,the%20request%20of %20partner%20nations

21. URL: https://taskandpurpose.com/news/cyber-command-security-hunt-forward

22. URL: https://governmentciomedia.com/cyber-command-finishes-its-first-hunt-forward-operation-latin-america

23. URL: https://www.cybercom.mil/Media/News/Article/3229136/before-the-invasion-hunt-forward-operations-in-ukraine/

24. URL: https://www.unian.ua/politics/ukrajina-oficiyno-priyednalasya-do-centru-kiberoboroni-nato-12258807.html

25. URL: https://www.cybercom.mil/Media/News/Article/3192016/cyber-101-us-cyber-comm and -mission

26. URL: https://therecord.media/cyber-command-reshuffles-cyber-mission-force-due-to-navy-readiness-woes

27. URL: https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

28. URL: https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strat egy _Summary.PDF

29. URL: https://www.lawfaremedia.org/article/president-bidens-policy-changes-offensive-cyber-operations

30. URL: https://defensescoop.com/2022/11/17/two-key-lawmakers-in-favor-of-keeping-dual-hat-arrangement-between-cybercom-and-nsa

31. URL: https://www.washingtonpost.com/world/national-security/obama-moves-to-split-cyber warfare-command-from-the-nsa/2016/12/23/a7707fc4-c95b-11e6-8bee-54e800ef2a63_story.html

32. URL: https://www.washingtonpost.com/world/national-security/trump-gives-the-military-more -latitude-to-use-offensive-cyber-tools-against-adversaries/2018/08/16/75f7a100-a160-11e8-8e87-c869fe 70a721_story.html

33. URL: https://www.washingtonpost.com/politics/2022/12/22/nsa-cyber-command-should-continue-share-leader-key-review-suggests

34. URL: https://www.airandspaceforces.com/air-force-nominee-nsa-and-cybercom-share-leader

35. URL: https://www.c4isrnet.com/dod/cybercom/2018/05/07/cyber-command-nsa-open-new-500-million-operations-center

36. URL: https://defensescoop.com/2023/05/31/five-years-in-a-look-at-how-cybercom-and-nsas-integrated-cyber-center-improved-coordination-of-operations

37. URL: https://www.scmagazine.com/brief/improved-cyber-coordination-from-cyber-command-nsas-integrated-center-detailed

38. URL: https://pshra.org/u-s-military-offers-special-pay-to-retain-top-cyber-talent

39. URL: https://www.arcyber.army.mil/Portals/34/Fact%20Sheets/CEAD%20Fact%20Sheets/Benefits%20_Incentives%20-%20DoD%20Scholars%20as%20Federal%20Employees.pdf?ver=HdE-uWd2vR7e-DXvb6FJxg%3D%3D

40. URL: https://www.cybercom.mil/Employment-Opportunities

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~