УДК 342.951

**ФЕДІЄНКО О.П.,** здобувач наукового ступеня.
ORCID: https://orcid.org/0009-0008-5383-3504.

# СУЧАСНІ ТЕНДЕНЦІЇ НОРМАТИВНОГО ЗАБЕЗПЕЧЕННЯ ІНСТИТУЦІЙНОГО ФОРМУВАННЯ КІБЕРВІЙСЬК (КІБЕРСИЛ): ДОСВІД ДЕЯКИХ КРАЇН НАТО

***Анотація.*** *Визначені загальні тенденції інституційного розвитку кібервійськ (кіберсил) у деяких кранах НАТО (Великобританія, США). Проаналізовано нормативні документи, присвячені створенню кібервійськ у вказаних країнах-членах НАТО. Розглянуто компетенцію, повноваження та функціональні завдання практичної діяльності кіберпідрозділів. Узагальнено особливості використання кібервійськ у рамках проведення оборонних та наступальних кібероперацій. Окреслено зміст та значення доктрини когнітивного ефекту та наслідків її використання. Деталізовано здобутки та приклади успішної діяльності кібервійськ Великобританії та США. На підставі узагальнення позитивного зарубіжного досвіду створення кібервійськ окреслено перспективи законодавчого забезпечення інституційного утворення кіберсил в Україні.*

***Ключові слова:*** *кіберстримування, кібероборона, кібероперація, кібердомен, кібервійська, кіберкомандування, кіберсили, НАТО, когнітивний ефект.*

***Summary.*** *The general trends of the institutional development of cybertroops (cyber forces) in certain NATO countries (Great Britain, the USA) are determined. Regulatory documents, devoted to the formation of cybertroops in these NATO member countries have been analyzed. The competence, powers and functional tasks of practical activities of cyber units are considered. The content and significance of the cognitive effect doctrine and the consequences of its use are outlined. The peculiarities of the use of cyber troops in the framework of conducting defensive and offensive cyber operations are summarized. The achievements and examples of successful activities of the cyber forces of Great Britain and the United States are detailed. On the basis of the generalization of positive foreign experience in the creation of cyber forces, the prospects of legislative support for the institutional formation of cyber forces in Ukraine are outlined.*

***Keywords:*** *cyber containment, cyber defense, cyber operation, cyber domain, cybertroops, cyber command, cyber forces, NATO, cognitive effect.*

**Постановка проблеми.** В умовах триваючої масштабної війни рф проти України саме кібердомен визнається світовою спільнотою одним із реальних театрів воєнних дій. Набирає сили світова тенденція щодо створення кібервійськ, до завдань яких належить не лише забезпечення кібероборони та захисту критичної інформаційної інфраструктури від кібератак, а й проведення превентивних наступальних операцій у кіберпросторі. Розуміючи необхідність та доцільність мілітаризації кіберпростору, у багатьох країнах світу останнім часом утворюються спеціальні підрозділи – кібервійська, які використовуються як для військових, так і розвідувальних цілей у кіберпросторі. Спеціалізовані підрозділи із кібербезпеки офіційно використовуються у десятках країн, а неофіційно – вже майже у сотні іноземних держав, оскільки важливою складовою забезпечення кібербезпеки є створення та розвиток кібервійськ. Відповідно до приписів НАТО, у 2016 році Альянс визнав кіберпростір полем проведення військових операцій нарівні з повітрям, сушею та морем. На теренах НАТО сформувалися системні підходи щодо посилення стійкості на основі розробки ефективних механізмів запобігання та

протидії кіберзагрозам. Високий рівень кіберстійкості забезпечується участю усіх суб`єктів системи кібербезпеки, формуванням надійних та ефективних інституцій, структур, агенцій та місій, що сприяють кібербезпеці та реагують на кібератаки [3, с. 78].

В сучасних умовах в Україні питання забезпечення безпеки кіберпростору гостро стоять перед політичним керівництвом нашої держави. Указом Президента України від 26 серпня 2021 року, яким було введено в дію рішення РНБО "Про невідкладні заходи з кібероборони держави" [1] анонсована необхідність створення у системі Міністерства оборони України кібервійськ з метою захисту суверенітету держави, забезпечення її обороноздатності, відсічі збройній агресії у кіберпросторі. План реалізації Стратегії кібербезпеки України, затверджений рішенням РНБО України від 30 грудня 2021 року та введений в дію Указом Президента України від 1 лютого 2022 року [2] чітко регламентує інституційні засади створення у системі Міністерства оборони України кібервійськ (кіберсил) протягом першого півріччя 2023 року. Хоча, попри нормативно встановлені терміни фактично кібервійська в Україні ще не створено, а формування кіберсил в умовах воєнного стану фактично залишається в стадії правової абстракції між різними військовими та невійськовими підрозділами. Тому висвітлення питань нормативного забезпечення інституційного створення кібервійськ, з урахуванням кращих практик та глобальних тенденцій, через призму зарубіжного досвіду є актуальним та своєчасним.

**Результати аналізу наукових публікацій.** Проблематику створення кібервійськ певним чином досліджували у своїх наукових працях: О. Горун [4], Р. Гула, І. Передерій та О. Вітринська [5], В. Чевардін та О. Мазулевський [6], В. Фіца [7], О. Терновий [8], Н. Ткачук [9]. На монографічному рівні питання створення та інституційного становлення кібервійськ частково висвітлювали: О. Задерейко, О. Троянський, Р. Чанишев, А. Дика [10], Ю. Даник, П. Воробієнко, В. Чернега [11]. Проте вказані автори предметно не розглядали особливості нормативного забезпечення інституційного формування кібервійськ (кіберсил) у провідних державах НАТО, таких як Великобританія та США. Висвітлення та узагальнення кращих практик зарубіжного досвіду законодавчого забезпечення створення кібервійськ надасть змогу імплементувати та адаптувати його до вітчизняних реалій, що є актуальним та своєчасним в умовах кібервійни.

**Метою статті** є визначення особливостей нормативного забезпечення інституційного створення кібервійськ (кіберсил) у провідних країнах НАТО (Великобританія, США) та розробка рекомендацій щодо прискорення інституційної розбудови кібервійськ (кіберсил) в Україні за власною моделлю, з урахуванням кращих практик передового зарубіжного досвіду.

**Виклад основного матеріалу.**

***Великобританія.*** Ця країна НАТО активно нарощує свій потенціал у кіберпросторі з метою протидії ймовірним супротивникам, особливо в умовах збройної військової агресії рф проти України. У 2016 році був створений Національний центр кібербезпеки з метою консультування уряду і громадськості про те, як знизити ризик реальних та потенційних кібератак. Саме у 2018 році Великобританія анонсувала про створення власних кібервійськ на базі Міністерства оборони країни з метою організації захисту власного кіберпростору, у першу чергу, від російської інформаційної експансії зі загальним штатом 2 тис. військовослужбовців та з бюджетним фінансуванням у розмірі понад 250 млн. фунтів. Головна мета – збільшення наступальної складової й кіберборотьба не лише проти окремих кіберзлочинців, але й недружніх країн чи транснаціональних кримінальних угрупувань: рф, іран, "ІДІЛ" тощо. При цьому, національні кіберсили Великобританії, включають у свій штат розвідників, представників міністерства оборони та профільних вчених, які територіально матимуть постійну базу

дислокації у Північній Англії, оскільки уряд цієї країни намагається стимулювати регіональний військовий розвиток за межами столиці – міста Лондона.

У 2020 році в цій країні було інституційно створено національні кіберсили “National Cyber Force” (далі – NCF) [12]. Кібервійська створені за ініціативи Міністерства оборони Великобританії і Центру урядового зв’язку, який відповідає за ведення радіоелектронної розвідки, а також забезпечує захист інформації уряду та британської армії. Причиною створення нового кібервійська стали зростаючі глобальні виклики та загрози світового масштабу, зокрема з боку рф. Кібервійська, у тому числі, орієнтовані, у першу чергу, на виконання наступальних кібероперацій.

Кібероперації (Cyberspace operations) – використання можливостей кіберпростору з метою досягнення стратегічних та тактичних військових цілей. Кібероперації націлені на технічні об’єкти, реалізуються приховано й здійснюють опосередкований психологічний вплив на осіб, що приймають рішення та фахівців ІТ-сфери, задіяних в управлінні об’єктами інформаційної інфраструктури. Усі кібероперації, які проводять NCF, здійснюються з дотриманням розроблених нормативів та правил етики відповідно до національного та міжнародного законодавства. Кібероперації базуються на глибокому розумінні сучасного кіберсередовища, що дозволяє NCF змістовно їх проектувати, визначати час і націлювати їх. Саме тому до складу британського кіберпідрозділу також увійшли фахівці Центру урядового зв’язку, а також досвідчені військовослужбовці.

У рамках функціональних завдань кібервійська захищають свої локації у кіберпросторі, які розміщені за кордоном; протидіють зовнішнім іноземним кампаніям у сфері дезінформації; проводять щоденний моніторинг кіберпростору, забезпечують кібероборону країни на перманентній основі, протидіють хакерським угрупуванням та світовим кіберзлочинцям, виробникам й розповсюджувачам дитячої порнографії тощо. Тобто NCF цієї країни націлені на припинення та блокування будь-яких кіберзагроз у режимі реального часу, включаючи іноземні системи ППО і мобільні телефони осіб, яких уряд вважає потенційними злочинцями або терористами. За оперативним задумом Кіберкомандування Великобританії, у найближчі роки планується збільшити штат цього спеціального підрозділу до 3 тис. співробітників та значно збільшити фінансування.

Центральне місце в діяльності кібервійськ Великобританії посідає “доктрина когнітивного ефекту”, яка включає методи, спрямовані на те, щоб посіяти паніку та недовіру, знизити бойовий дух й послабити здатність супротивника планувати та реалізовувати свою діяльність у кіберпросторі, через психологічний вплив навмисно провокувати ігнорування та невиконання наказів керівництва. Просте усунення комп’ютерних серверів або мереж може мати більш драматичний вплив у короткостроковій перспективі, але NCF вважають, що втрачене обладнання та устаткування можна легко замінити, тому перевагу надають довгостроковій психологічній стратегії впливу. Також NCF у межах компетенції та відповідно до функціональності можуть проводити наступальні кібероперації.

Сучасна військова доктрина Великобританії оприлюднена 22 березня 2021 року, і розрахована на період до 2030 року під назвою “Великобританія в епоху конкуренції” [13]. Особлива увага в цьому стратегічному документі приділяється у тому числі, саме питанням розбудови та оптимізації національних кібернетичних сил, їхньому динамічному розвиткові. У грудні 2021 року була опублікована оновлена Національна стратегія кібербезпеки Великобританії на 2022 – 2025 роки [14]. Окремі положення цього програмного документу присвячені питанням удосконалення перспективної діяльності кіберсил та розвитку їхніх бойових спроможностей, посилення стану кібероборони країни.

19 грудня 2022 року Уряд Великої Британії оприлюднив нову “Рамкову програму забезпечення національної стійкості” [15]. Цей документ розроблено відповідно до урядових зобов’язань, визначених у Звіті щодо Комплексного Огляду сектору безпеки, оборони, розвитку пріоритетів зовнішньої політики від 16 березня 2021 року з урахуванням масштабів поширення загрозливих тенденції та посилення невизначеності в глобальному безпековому середовищі та розраховано на період до 2030 року. Ця Рамкова програма містить оновлені концептуальні й методологічні підходи до управління ризиками та планування у цій сфері на всіх рівнях, передбачає посилення комплексної взаємодії, доповнює чинні стратегічні документи, зокрема у сферах енергетичної безпеки та кібербезпеки, переходу на екологічно чисту енергію, захисту об’єктів критичної інфраструктури тощо. Документ розкриває удосконалені підходи до оцінювання ризиків, розподілу обов’язків і сфер відповідальності, поліпшення звітування, посилення стратегічного партнерства, особливо у питаннях забезпечення кібербезпеки.

У доповіді уряду 2023 року “The National Cyber Force: Responsible Cyber Power in Practice” [16] розкриваються форми та методи ведення кібервійни національними кіберсилами Великої Британії, що включає, у тому числі, заходи психологічного впливу з метою створення параної серед ворогів, не даючи їм зрозуміти, що результати, з якими вони стикаються, є наслідком проведених успішних кібероперацій. Найбільший ефект досягається при впливі на інформаційні мережі ворога з часом, що викликає “непомітний нахил ігрового поля”. Так, наприклад, кібероперації проти терористичного угруповання “ІДІЛ” змусили його оперативників не довіряти відданим зверху наказам та мати сумнів щодо них. Розглядаючи цілі та завдання британських кібероперацій, можна констатувати основну мету таємних дій — викликати у ворогів параною та чинити масштабний психологічний тиск. Водночас, національні кіберсили Великої Британії ставлять на перше місце правдивість в кібервійні війні й прагнуть об’єднати свої зусилля з метою досягнення когнітивного ефекту. Виходячи із масштабів російської та іранської загроз у кібердомені, бюджет на фінансування кібервійськ Великобританії у 2023 році було збільшено до 400 млн. фунтів на рік. За результатами 3-річного успішного досвіду існування та функціонування національних кіберсил Великої Британії 4 квітня 2023 року Уряд Великобританії опублікував Керівництво під назвою: “Відповідальна кібервлада на практиці” [17]. Відповідно до його змісту основним фундаментальним документом, який визначає пріоритети діяльності кібервійськ є національна кіберпрограма, яка розробляється на планових засадах.

Стратегічна діяльність NCF полягає в тому, щоб ускладнити супротивнику використання кіберпростору та цифрових технологій для досягнення своїх амбітних цілей. NCF щодня проводить кібероперації, щоб захистити кібердомен Великобританії від кіберзагроз, розвивати та забезпечувати політику національної безпеки країни, підтримувати військові операції навколо світу та протидіяти сексуальній експлуатації та насильству над дітьми в мережі Інтернет. Кібероперації NCF проводяться як проти державних, так і недержавних загроз (наприклад, таких як тероризм). На практиці NCF розробляє та використовує кіберпотенціал для проведення своїх операцій, включаючи блокування та переривання можливості противника використовувати кіберпростір і цифрові технології, впливаючи на свідомість та психіку противника.

Виконання кібероперацій є досить складним та тривалим процесом. Сполучене Королівство, як відповідальна демократична кібердержава, діє в законний та відповідальний спосіб, узгоджений з етичними правилами. Проведення кібероперацій передбачає досягнення стратегічної мети – усунення здатності супротивника діяти у

кіберпросторі на випередження. Інші кібероперації спрямовані на більш широкий вплив та здатність супротивника реалізовувати свої протиправні наміри у кібердомені. Досягнути цього можливо різними способами, зокрема впливаючи на здатність супротивника здобувати, аналізувати та використовувати інформацію, необхідну для досягнення своїх цілей.

Виходячи із набутого операційного досвіду, кібервійська Великобританії можуть досягнути найбільшого когнітивного ефекту, впливаючи на функціональність і ефективність інформаційно-комунікаційних систем супротивника протягом певного періоду часу, а не заперечуючи їх повністю (оскільки в деяких випадках їх можна швидко замінити). Проте операції з руйнівним ефектом залишаються варіантом, де це є найбільш прийнятним та оптимальним рішенням. Щоб досягти оптимального ефекту, необхідний високий рівень планування, а в деяких випадках досить важливо правильно визначити час. Хоча миттєвий ефект від певної кібероперації може бути відносно короткочасним, когнітивний вплив, включаючи втрату довіри ворожого суб'єкта до своїх даних або технологій, може бути довготривалим. Об'єднання декількох операцій разом з іншими важелями впливу надає змогу досягнути сукупного ефекту та довгостроковість отриманих результатів. NCF інтегрує власні кібернетичні можливості з іншими військовими підрозділами Великобританії, щоб організувати ефективний та потужний кіберзахист.

NCF має повноваження здійснювати кібероперації в інтересах національної безпеки, забезпечення добробуту громадян Великобританії або для попередження злочинної діяльності у мережі Інтернет. Загалом існує три категорії кібероперацій, що проводяться NCF:

• протидія кіберзагрозам, які продукують та поширюють терористи, міжнародні злочинці і держави, які використовують глобальну всесвітню мережу для здійснення протиправних транскордонних операцій, кібератак, які можуть завдати суттєвої шкоди Великобританії або іншим державам НАТО;

• протидія кіберзагрозам, які підривають конфіденційність, цілісність і доступність інформації та даних, а також ефективне використання пошукових систем користувачами. Це може передбачати проведення кібероперацій, коли це необхідно, разом із низкою інших засобів пом'якшення, доступних для протидії загрозам кібербезпеці, включаючи покращену кіберстійкість, скоординовані дії з урядами союзників і плідну співпрацю з приватним ІТ-сектором;

• сприяння оборонним кіберопераціям Великобританії та допомога в реалізації військових програм зовнішньої політики держави. Кібероперації можуть підтримувати весь спектр оборонної діяльності та мати особливий внесок у підтримку ключових завдань зовнішньої політики та безпеки.

NCF регулярно проводить кібероперації з підтримки закордонних військових операцій, а також допомагає забезпечити безпечне виконання завдань закордонних військових місій. Це може включати використання спектру потенційних кіберможливостей, серед яких захист ланцюгів постачання та порушення роботи ворожого шкідливого програмного забезпечення тощо. Операції, які проводить NCF, здійснюються відповідно до усталеної правової бази, яка включає: Закон про розвідувальні служби 1994 року (ISA), Закон про слідчі повноваження 2016 року (IPA) і Закон про регулювання слідчих повноважень 2000 року (RIPA). Рішення про схвалення тієї чи іншої кібероперації приймаються на рівні вищого військового кіберкомандування за допомогою проведення юридичних консультацій щодо відповідності вимогам національного та міжнародного права. Крім того, важливе значення має етичний компонент під час операційного

планування діяльності NCF. Це робиться для того, щоб операції були чітко спланованими та відповідали чинному законодавству. Частково це гарантує, що операції відповідають британським та світовим демократичним цінностям і принципам відповідальної поведінки у кіберпросторі.

Діяльність NCF підлягає обов'язковому затвердженню міністром оборони, судовому нагляду та парламентському контролю, що робить режим управління кіберопераціями Великобританії одним із найбільш потужних у світі. Тобто проведення кібероперації має бути схвалено міністром, як правило, міністром закордонних справ або міністром оборони, залежно від характеру цілі та точних необхідних активів. NCF працює в рамках існуючого правового контролю та підлягатиме нагляду парламентського комітету з питань розвідки та безпеки. Ключовою частиною відповідальних кібероперацій є розробка та використання можливостей у спосіб, який є передбачуваним і контрольованим, і де ризики пропорційні необхідному результату. Кібероперації NCF потребують значної підготовки, щоб переконатися, що вони ефективні та можуть проводитися відповідально. Це включає відповідну технічну розвідку кіберопераційного середовища, щоб досягти найкращого можливого розуміння напередодні та під час будь-якої операції, що проводиться. Кібероперації ретельно розроблені таким чином, щоб зосередити увагу на конкретному результаті, якого потрібно досягти, і зважити пов'язані з цим можливі ризики. Загалом можна констатувати, що Великобританія залишається світовим лідером у проведенні наступальних кібероперацій, а NCF має трирічний досвід своєї успішної діяльності та є відносно новою структурою, яка поєднує в собі елементи як розвідувального співтовариства, так і збройних сил. При цьому, загальне керівництво кібероборoною здійснюється спільно міністерствами оборони та закордонних справ.

***Сполучені Штати Америки.*** Кібернетичне командування США (United States Cyber Command – USCYBERCOM) було створено 23 червня 2009 року у відповідності з наказом Міністра оборони США Роберта Гейтса у форматі 11-го військового об'єднаного командування США [18]. Кіберкомандування США створено на базі Агентства національної безпеки (штаб-квартира АНБ – Форт Джордж Мід, штат Меріленд) – ключової технічної розвідки країни. 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 [9, с. 70].

Кібернетичне командування – частина Збройних сил США, підпорядковане об'єднаному Стратегічному командуванню США (база ПС США Оффут, штат Небраска). Операції у кіберпросторі здійснюються через різні компоненти. До складу USCYBERCOM 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-та повітряна армія (AFCYBER) і Кіберкомандування берегової охорони (CGCYBER).

Бюджетний запит МО США на 2024 рік для фінансування заходів в кіберпросторі складає $13.5 млрд., з яких $332.6 млн. виділяються на функціонування штаб-квартири кіберкомандування, $129 млн. на закупівлі обладнання та устаткування, $1.1 млрд. на R&D. Станом на 2023 рік 133 команди Сил Національної Кібермісії складаються із загальної штатної чисельності 9 тис. осіб, з них 15 % складають цивільні та резервісти.

Основним завданням є планування та проведення глобальних кібероперацій з метою захисту та просування національних інтересів у співпраці з внутрішніми та міжнародними партнерами в повному спектрі наявної конкуренції та глобальних конфліктів.

Беззаперечно, найбільш потужну армію у кіберпросторі має США, а державне щорічне фінансування на її утримання складає понад $7 млрд. США. Комплектування цих підрозділів здійснюється переважно за рахунок хакерів, які поповнюють ряди кібервійськових. Надійний захист кіберпростору та домінування у світовому масштабі – стратегічне завдання уряду США, що не виключає військових дій у кіберпросторі з урахуванням площини національних інтересів. Політичний вектор, закладений у стратегічних наративах кібербезпеки США, аргументовано декларує систему кіберзагроз, настання яких провокує необхідність проведення спеціальних інформаційних операцій, спрямованих на запобігання їм та недопущення будь-яких кібератак з боку інших держав. Основними напрямками діяльності кібервійськ є шпигунство, у тому числі й промислове, проведення системних кібератак, спеціальних інформаційних операцій та навіть ведення війни у кіберпросторі. У військових структурах передових країн світу є навіть кіберкомандування та відокремлено персонал, який залучається для захисту інфраструктури військових кіберсистем. Девізом кіберпідрозділів США є перемога над супротивником у цифровій війні, що виступає найбільшим пріоритетом, аніж перемога у класичному військовому протистоянні.

Завданнями Кіберкомандування США виступають:

1) планування, проведення та координація кібероперацій з метою забезпечення і запобігання зовнішній агресії, забезпечення свободи дій оперативних і сухопутних (берегових, інших) формувань військ (сил) при досягненні переваги у кіберпросторі;

2) забезпечення технічної підтримки, надійності, безпеки та захисту каналів управління, включаючи комп’ютерні та космічні системи в секторі відповідальності;

3) керівництво діяльністю сил і засобів радіоелектронної боротьби, радіоелектронної розвідки та служби дешифрування;

4) досягнення можливостей включення військ (сил) в об’єднані командування збройних сил кібер-, інформаційних, криптологічних і космічних та інших операцій;

5) приведення глобальної комп’ютерної мережі військ (сил) у відповідність до загальних оперативних потреб кіберзахисту Збройних Сил країни.

Вирішення цих питань потребують ретельної комплексної підготовки військ (сил) та високої відповідальності, професійних якостей, навченості особового складу, надійності та ефективності роботи інформаційно-телекомунікаційної складової системи кібербезпеки країни. Для цього в США протягом десяти років створювалась потужна система кібербезпеки держави, яка має спроможності як бойового застосування, так і підготовки та розвитку військ, сил в мирний час. Система кібербезпеки США складається з різних фахівців, як військових, так і цивільних, які здатні виконувати складні завдання у сфері забезпечення захисту кіберпростору.

Наприклад, управління кіберзахисту (оборонних кібероперацій) ВМС США, яке базується на військово-морській базі Норфолка (штат Віргінія), відповідає за безперебійне функціонування мережі FORCENET, відбиття кібератак та ліквідацію наслідків після атак в межах військово-морського сегменту кіберпростору. Це розгалужена мережа з 700 тисяч комп’ютерів при чисельності командування у 200 військовослужбовців та цивільних співробітників. Умовно кажучи, за кількісною оцінкою, на кожного фахівця цього управління приходиться 3,5 тисячі компютерів.

Починаючи з 2011 року Кібернетичне командування США щорічно на регулярній основі проводить навчання “Cyber Flag” у взаємодії з іншими агентствами й відомствами

та разом з союзниками по Альянсу НАТО. У них беруть участь сотні фахівців з метою підвищення готовності до реагування на кібератаки, а також налагодження взаємодії між відомствами, а також союзниками та партнерами. Навчання "Cyber Flag" – це система колективної безпеки у кіберпросторі, створена задля поліпшення можливостей з виявлення, синхронізації та спільного реагування на змодельовані шкідливі дії в кіберпросторі, націлені на критично важливу інфраструктуру та ключові ресурси. Проект створений за ініціативи США із залученням міжнародних партнерів США: Канади, Великої Британії, Данії, Франції, Естонії тощо.

Діяльність кіберсил США спрямована на захист інформаційних систем Міністерства оборони від усіх можливих кібератак і вторгнень, передбачає посилення здатності країни протистояти кіберзагрозам і оперативно реагувати на них. Кіберкомандування 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. Американські кіберсили забезпечують здійснення повного спектра операцій (наступальних та оборонних) у кіберпросторі, щоб допомогти бойовим командирам і Об'єднаним силам у досягненні цілей їх місії в кіберпросторі та через нього. Кібероперації забезпечують надійний стан забезпечення безпеки мереж, даних і систем зброї навколо світу, надають можливість кібервійськам, під час використання своїх повноважень, нейтралізувати та нівелювати можливості злочинної діяльності хакерів та іноземних держав-супротивників. Першочергово USCYBERCOM створювалися як захисні сили та офіційно отримали наступальний мандат лише у 2018 році.

У 2018 році Президент США Д. Трамп надав дозвіл на проведення "підривної діяльності в кіберпросторі" на межі військових дій та на випередження дій потенційних ворогів (концепція превентивного удару). Підставою для цього став таємний указ Президента США (National Security Presidential Memoranda № 13) "Defend forward" ("захищатися на випередження"), "Hunt forward" ("полювати на випередження"), "Persistent engagement" ("постійне залучення"). Аналогічна норма продубльована у Стратегії кібероборони МО США 2018 року, відповідно до якої США захищатимуться на випередження, щоб зруйнувати джерело зловмисної кіберактивності, включаючи активність, яка є нижчою за рівень збройного конфлікту. Це означає, що якщо пристрій, мережа, організація чи держава-супротивник ідентифіковані як загроза мережам і установам США або активно атакують їх у кіберпросторі або через нього, вони можуть очікувати, що Сполучені Штати змусять їх за це "заплатити".

На виконання задекларованих завдань, 5 листопада 2018 року напередодні виборів у США, Кіберкомандування США на декілька днів заблокувало роботу російської фабрики тролів – Агентства Інтернет-досліджень, розташованого у м. санкт-петербурзі (рф) [19]. Підставою для цього стали здобуті розвідувальні дані щодо намірів втручання держави-агресора у президентські вибори в США. Це була перша наступальна кібероперація, яку офіційно санкціонувало та публічно визнало політичне керівництво країни. Таким чином, Кіберкомандування США отримало повноваження не лише проводити кібероперації для захисту своєї країни, але й для захисту країн-союзників, тобто надавати допомогу партнерам при одночасному забезпеченні національних інтересів США. Це була перша наступальна кібероперація, проведення та санкціонування якої відкрито визнало керівництво США, яка мала місце за часів президентства Д. Трампа, коли значно було 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 [20].

З 2018 року в Естонії, Литві, країнах Латинської Америки за сприяння США було створено Інтегрований кіберцентр та Об'єднаний центр операцій (загальний бюджет складає $500 млн.). Метою стало прагнення об'єднання військової та розвідувальної спільноти, інших федеральних агенцій, міжнародних партнерів (+ ФБР, МНБ та інші). 15 вересня 2021 року Австралія, Канада, Нова Зеландія, США та Великобританія утворити розвідувальний альянс "П'ять Очей" з метою оперативного обміну інформацією між собою, які мають передові у світі можливості для ведення кібервійни. Діяльність вказаних структур не просто передбачає обмін інформацією в реальному часі, а налагодження прямих каналів доступу до оперативної інформації партнерів між собою.

Президент США 2 березня 2023 року затвердив нову Стратегію національної кібербезпеки, яка замінила "Національну кіберстратегію", що була прийнята адміністрацією ще колишнього президента Д. Трампа у 2018 році. У Білому домі в межах нової національної стратегії кібербезпеки США планують використовувати всі доступні інструменти для протидії кіберзагрозам та активізувати міжнародну співпрацю з країнами, які раніше не брали участь у цьому питанні. Цей стратегічний документ чітко формулює завдання, вирішення яких надасть приватним особам, державним структурам та бізнесу можливість консолідовано діяти в цифровій сфері з мінімальними ризиками [21].

Перспективами розвитку цифрового технологічного прогресу вбачаються динамічні зміни та стимулювання розвитку американської IT-галузі на користь довгострокових інвестицій, дотримання балансу між захистом від нагальних загроз сьогодні та одночасним стратегічним плануванням й інвестуванням у стійке цифрове майбутнє. Стратегія спрямована на потужний захист інвестицій у відбудову американської критичної інфраструктури, розвиток сектору відновлюваної енергії та розвиток американських цифрових технологій та виробничої бази. США мають намір удосконалити власну цифрову екосистему, яка базується на таких ключових принципах, як: захищеність, стійкість, цінність діджиталізації. Стратегія побудована на п'яти основних засадах, серед яких пріоритетними є: захист критичної інфраструктури; ліквідація, запобігання та блокування будь-яких кіберзагроз; формування ринкових потужностей цифрової економіки, що гарантують кібербезпеку, інноваційний розвиток безпечних та стійких технологій й інфраструктури наступного покоління; розбудова міжнародного цифрового партнерства. Зауважимо, що Стратегія була розроблена після низки великих та потужних кібератак, включаючи напад на трубопровід "Colonial Pipeline" у 2021 році й кіберзлам федеральних установ протягом 2019 – 2020 років.

Таким чином, в США успішно функціонує Кіберкомандування USCYBERCOM як частина Збройних сил, що була створена ще у 2009 році й підпорядковується об'єднаному Стратегічному командуванню США. За часів президентства Д. Трампа було оголошено, що USCYBERCOM буде підвищений до статусу одного з Об'єднаних Командувань Збройних сил США / Unified Combatant Command, тобто до рівня одного із функціональних командувань, таких як, наприклад, Командування сил спеціальних операцій або Транспортне Командування. На переконання експертів Національної асоціації нинішніх та колишніх військової спеціалістів з цифрової безпеки (Military Cyber Professional Association), цього недостатньо і залежність Кіберкомандування від інших гілок Збройних сил США, які делегують USCYBERCOM свої ресурси та спеціалістів, створює несистемний та складний підхід до оцінки кіберзагроз й "непотрібний ризик" для національної безпеки США. Тому Асоціація закликає Конгрес

США створити окремий, сьомий рід військ – Кібервійська (U.S. Cyber Force), адже це питання все ще залишається відкритим та актуальним.

Загалом перевагами побудови кібервійськ за зразком США є те, що у кожного роду військ своя складова представлена в кіберпросторі, що надає можливості командувачам відповідних родів військ скоротити ланцюг в системі військового оперативного управління із забезпечення дій своїх сил (військ). Недоліком є розпорошеність сил кібервійськ і необхідність створення ще одного органу військового управління у вигляді "кіберкомандування" для управління наявними у всіх Збройних Силах кібервійськами, що потенційно призведе до додаткових фінансових витрат, спрямованих на утримання відповідних підрозділів.

19 грудня 2022 року Міністерство оборони США підвищило статус однієї із структур у складі Кіберкомандування, а саме оперативну групу "Cyber National Mission Force" (CNMF) [22], основними завданнями якої є централізоване проведення кібервійськових операцій та захист військових комп`ютерних мереж. Ця структура складається із 39 об'єднаних кіберкоманд та налічує штат понад 2 тис. військовослужбовців і цивільних осіб, які виконують, у тому числі, такі завдання, як: забезпечення безпеки електоральних процесів та виборів, боротьба з кібершпіонажем або програмами – вимагачами тощо.

У березні 2023 року Кіберкомандування США анонсувало про створення власного Центру розвідки, після того, як тривалий час відомство використовувало інші джерела збору інформації. Проект має на меті удосконалити процес збору даних та розширити спектр можливостей Кіберкомандування США у сфері діяльності іноземних держав в кіберсфері, яка постійно та динамічно змінюється й розширюється [23]. До кінця 2023 року в армії США планується створити офіс "Program Manager Cyber and Space", який в рамках компетенції та відповідно до функціональності займатиметься розробкою та реалізацією наступальних кібер- та космічними операцій. Наступальний кіберпортфель включає платформу спільного доступу та підготовку спеціальних програм. Необхідність створення нового офісу зумовлена збільшенням обсягів спільної роботи, яку армія виконує від імені Кіберкомандування США. Новий офіс продовжить роботу над удосконаленням тактичного кібеобладнання для забезпечення потреб армії США. Адже попри наявність кіберкомандування, загальне керівництво в сфері кібероборони здійснюється спільно Директором національної розвідки та Національною радою безпеки.

**Висновки.**

На підставі проведеного дослідження можна констатувати, що провідні країни НАТО (Великобританія, США) переймаються проблематикою розбудови кібервійськ як важливої компоненти у складі Збройних сил. Як правило, інституційне створення кібервійськ задекларовано у спеціальних нормативних актах, переважно військового спрямування (стратегіях, концепціях, доктринах) провідних держав світу. Основними питаннями, які потребують врегулювання, під час інституційного створення кібервійськ виступають: правові основи, штатна чисельність кіберпідрозділів, склад та структура кіберкомандування, компетенція та повноваження кібервійськ, стратегічні та функціональні завдання, обсяги щорічного фінансування, умови поповнення кадрового резерву тощо. До типових характеристик кіберсил на теренах НАТО відносяться: кіберсили у переважній більшості перебувають у складі збройних сил; грошове забезпечення на 20 – 30 % вище, аніж у військовослужбовців інших родів військ, віковий ценз та посилені вимоги до фізичної підготовки; відсутність універсальної структури або підпорядкування.

Так, наприклад, у Великобританії NCF – це співдружність та партнерство між обороною та розвідкою. Великобританія використовуватиме кібероперації як важливу частину своєї дипломатичної, економічної та військової політики. Відповідальність за результати діяльності NCF несуть спільно Державний секретар у справах закордонних справ, співдружності та розвитку та Державний секретар у справах оборони. Пріоритети діяльності кібервійськ визначаються у програмних документах, визначених Радою національної безпеки країни.

Перевагами створення та розбудови кібервійськ в США є широкомасштабний підхід, який було запроваджено під час формування Кіберкомандування (USCYBERCOM), яке є частиною Збройних сил, що підпорядковується об'єднаному Стратегічному командуванню США. Кожний рід військ – сухопутні війська, флот, повітряні сили та морська піхота мають власні кіберкоманди. В перспективі планується створення окремого, сьомого роду військ – кібервійська (U.S. Cyber Force). Попри наявність чітко структурованого Кіберкомандування на державному рівні загальне керівництво кібероборoною здійснюють спільно Директор національної розвідки (Director of National Intelligence, DNI) та Національна рада безпеки (United States National Security Council).

Сучасна тенденція кібервійськ (кіберсил) як у Великобританії, так і в США – проведення наступальних операцій у кібердомені, забезпечення потужної кібероборони, використання методів та практик інформаційно-психологічних операцій (впливу) на супротивника з метою його психічної дестабілізації та тривалого розладу психічного здоров'я (практичної реалізації доктрини когнітивного ефекту). Проаналізований зарубіжний досвід переконливо доводить, що національні кіберсили є ключовою компонентою в інтегрованому підході щодо посилення стану забезпечення національної безпеки. Таким чином, вивчення та адаптація кращих практик передових країн НАТО щодо інституційного створення кібервійськ надасть змогу прискорити запуск та подальшу розбудову в Україні власних кібервійськ (кіберсил) з метою кіберстримування збройної агресії та надання відсічі агресору у кібердомені. Прискорення створення спеціальних підрозділів кібервійськ в Україні є важливим та рішучим кроком, який спрямований на запровадження дієвих та ефективних механізмів стримування та відсічі російській агресії у кібердомені, особливо в умовах триваючої кібервійни. За таких умов доцільним є прискорення інституційного створення кібервійськ в Україні, що передбачатиме підготовку та схвалення на парламентському рівні законопроекту "Про Кіберсили Збройних Сил України" як дорожньої карти стратегічного планування та розвитку національних кібервійськ.

## 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 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

3. Демедюк С.В., Користін О.Є. Стійкість системи кібербезпеки та її забезпечення в НАТО. *Наука і правоохоронна.* 2023. № 1 (59). С. 77-85.

4. Горун О.Ю. Зарубіжний досвід правового забезпечення та особливостей створення кібервійськ на прикладі деяких держав НАТО. *Науковий вісник Міжнародного гуманітарного університету. Серія. Юриспруденція.* 2023. № 64. С. 33-37. URL: https://doi.org/10.32841/2307-1745.2023.64.7

5. Гула Р., Передерій І., Вітринська О. Концептуальні засади воєнної політики у кіберпросторі провідних держав світу та воєнно-політичних інституцій. *Вісник Книжкової палати.* – (Науково-практичний журнал). 2020. № 4. С. 22-26.

6. Чевардін В.Є., Мазулевський О.Є. Аналіз структур кіберкомандувань розвинутих країн. *Збірник наукових праць ВІТІ.* 2020. № 2. С. 121-128.

7. Фіца В.М. Інституційне забезпечення створення кібервійськ в Україні. *Інформація і право.* № 3(38)/2021. С. 109-114.

8. Терновий О., Шкуренко О., Міненко Л. Проблемні аспекти кібероборони: місце та роль кіберзахисту в Збройних силах України. *Сучасні інформаційні технології у сфері безпеки та оборони.* 2023. № 1. С. 23-31.

9. Ткачук Н.А. Досвід США зі створення та розбудови кіберкомандування: уроки для України. *Інтернаука. Серія: Юридичні науки.* – (Міжнародний науковий журнал). 2023. № 11 (69). С. 69-77. URL: https://doi.org/10.25313/2520-2308-2023-11-9428

10. Концептуальні основи захисту інформаційного суверенітету України: монографія / О.В. Задерейко, О.В. Троянський, Р.І. Чанишев, А.І. Дика. 2-ге вид., перероб. і доп. Одеса: Фенікс, 2022. 220 с.

11. Даник Ю.Г. Воробієнко П.П., Чернега В.М. Основи кібербезпеки та кібероборони: підручник. 2-ге вид., перероб. та доп. Одеса: ОНАЗ, 2019. 320 с. URL: https://metod.suitt.edu.ua/download/686

12. The National Cyber Force (NCF) is a partnership between defence and intelligence. URL: https://www.gov.uk/government/organisations/national-cyber-force/about

13. Global Britain in Competitive Age: The Integrated Review of Security, Defence, Development and Foreign Policy. URL: https://www.gov.uk/government/publications/global-britain-in-a-competitive-age-the-integrated-review-of-security-defence-development-and-foreign-policy

14. National Cyber Security Strategy 2022-2025 URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1180089/14.283_CO_National_Cyber_Strategy_Progress_Report_Web_v3.pdf

15. The UK Government Resilience Framework. URL: https://www.gov.uk/government/publications/the-uk-government-resilience-framework

16. The National Cyber Force: Responsible Cyber Power in Practice. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1148278/Responsible_Cyber_Power_in_Practice.pdf

17. Guidance Responsible Cyber Power in Practice URL: https://www.gov.uk/government/publications/responsible-cyber-power-in-practice/responsible-cyber-power-in-practice-html

18. United States Cyber Command – USCYBERCOM. URL: https://www.cybercom.mil

19. U.S. Cyber Command operation disrupted Internet access of Russian troll factory on day of 2018 midterms. URL: https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html

20. Sanger D. U.S. Escalates Online Attacks on Russia's Power Grid. The New York Times. 2019. URL: https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russiagrid.html

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

22. The Cyber National mission force is the newest military command. URL: https://mybaseguide.com/cyber-national-mission-force

23. US Army to launch offensive cyber capabilities office. URL: https://www.defensenews.com/electronic-warfare/2022/08/31/us-army-to-launch-offensive-cyber-capabilities-office

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