DOI 10.33099/2618-1614-2025-28-1-36-46
УДК 355.4

В. В. Машталір,
доктор історичних наук, професор,
Національний університет оборони України,
Ю. А. Гусак,
доктор військових наук, професор,
Національний університет оборони України

Розвиток понятійного апарату з питань кібероборони та підходи до створення кіберсил в Україні

Проведений аналіз понятійного апарату з питань кібербезпеки та кібероборони, який застосовується в законодавчих та нормативних документах. На підставі основних положень воєнного мистецтва запропоновано систему понять у сфері кібероборони, зокрема таких, як агресія в кіберпросторі, кіберборотьба, кібернаступ та кібероборона, кібероперація, кіберудар тощо, та надано їхні визначення. Здійснений аналіз кіберсил провідних країн НАТО. Визначено, що кіберсили провідних країн НАТО можуть мати два варіанти організації: перший варіант передбачає входження кіберсил до складу національних збройних сил та взаємодію їх із цивільними кіберпідрозділами (США, Німеччина), а другий – об'єднання в окремій національній структурі військових та цивільних кіберпідрозділів (Велика Британія, Франція). Запропоновані напрями розвитку теоретичних засад створення системи кібероборони України, реалізація яких дасть можливість формувати кіберсили, подібні за складом, організацією, завданнями і функціями до кіберсил країн – членів НАТО, реалізувати єдину стратегію кібероборони в Міністерстві оборони України та Збройних Силах України, здійснювати управління силами кібероборони в умовах правового режиму воєнного стану (особливого періоду).

Ключові слова: кібероборона, кіберпростір, система кібероборони, суб'єкти кібероборони, кібервійська, кібербезпека, кіберзахист, кіберсистема, кібератака, кібернаступ, кібероперація.

Постановка проблеми. Розвиток сучасних кібертехнологій призвів до виникнення нових ризиків і загроз у сфері національної безпеки та оборони України, які здійснюються через та в кіберпросторі. Ці ризики та загрози створили виклики для України у сфері кібербезпеки (*рис. 1*) [1]. У зв'язку із цим відбувається трансформація поглядів на питання кібероборони та розробляються теоретичні засади кібероборони з урахуванням розвитку інформаційних технологій та прогнозуються можливі зміни у формах, способах і технологіях ведення війн.

Мілітаризація кіберпростору та розвиток кіберзброї ведуть до невпинного нарощування арсеналу кіберзброї наступального призначення та створюють кіберзагрози кібербезпеці України.

Загрози через кіберпростір впливають на всі базові сфери: політичну, воєнну, економічну, енергетичну, інфраструктурну тощо, та мають деструктивний вплив на національну безпеку та оборону загалом.

Загрозами кібербезпеці України є [1]: невпинне нарощування арсеналу кіберзброї наступального призначення; кіберзлочинність; кібершпигунство; кібертероризм (*рис. 2*).

Однією з найнебезпечніших кіберзагроз є застосування кіберзброї наступального призначення для проведення кібердиверсій або спеціальних інформаційних операцій.

У сучасному світі кібероборона як складова кібербезпеки має низку проблемних питань, які потребують негайного вирішення. У зв'язку із цим у розвинених країнах світу цьому питанню приділяють велику увагу. Ці питання розглядалися на таких важливих заходах НАТО, як [2]:

- саміт НАТО в Празі (2002) – уперше кіберзахист включений до політичного порядку денного Альянсу;
- саміт НАТО в Ризі (2006) – підтверджена необхідність додаткового захисту інформаційно-комунікаційних систем країн – членів НАТО;
- саміт НАТО в Лісабоні (2010) – прийнята Стратегічна концепція, в якій уперше було визнано, що кібератаки можуть загрожувати національній та євроатлантичній безпеці та стабільності;
- саміт НАТО в Чикаго (2012) – кіберзахист включений до процесу оборонного планування НАТО і визначені заходи централізованого захисту всіх мереж НАТО, для реалізації яких у липні 2012 р. у рамках реформи агенцій НАТО створене Агентство зв'язку та інформації НАТО;
- саміт НАТО у Вельсі (2014) – схвалена нова політика кіберзахисту, в якій кіберзахист визнаний частиною основного завдання НАТО щодо колективної оборони, що означає, що кібератака може бути підставою для застосування статті 5 установчого договору НАТО;

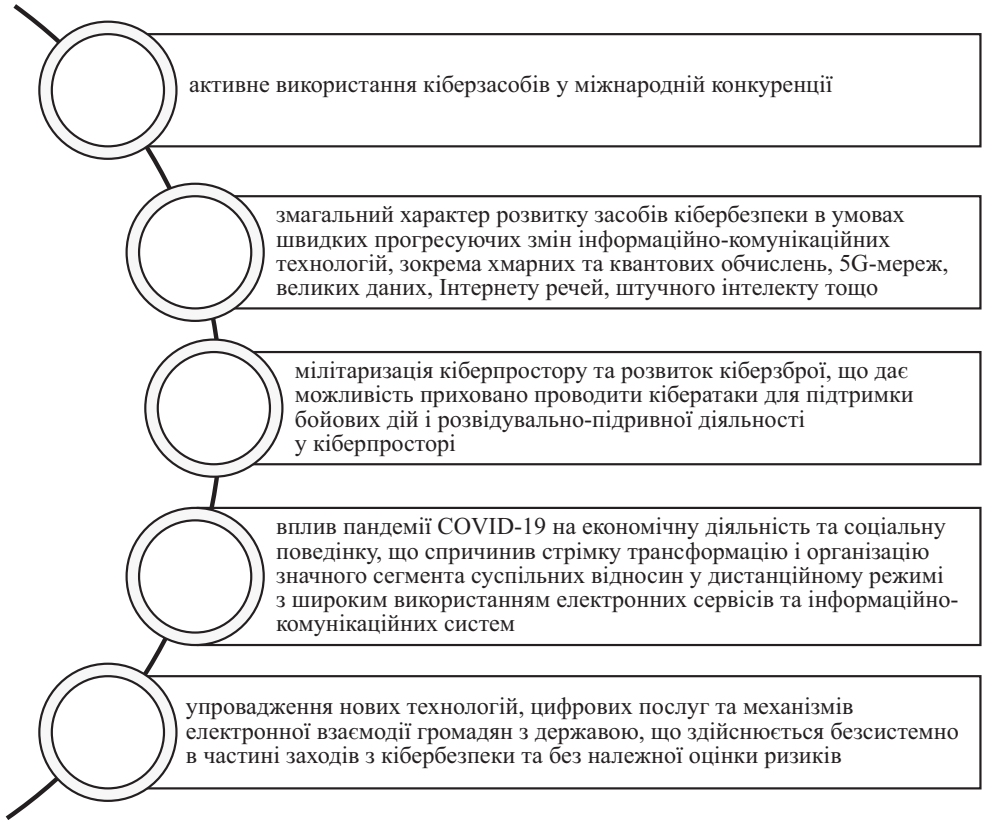

Рис. 1. Виклики для України у сфері кібербезпеки

Кіберзброя наступального призначення

- кібератаки на інформаційно-комунікаційні системи державних органів України та об'єкти критичної інформаційної інфраструктури з метою виведення їх з ладу (кібердиверсія);
- отримання прихованого доступу і контролю, здійснення розвідувальної та розвідувально-підривної діяльності;
- проведення спеціальних інформаційних операцій з метою маніпулятивного впливу на населення, втручання у виборчі процеси та дискредитації української державності

Кіберзлочинність

- використання кіберпростору для вчинення злочинів проти основ національної безпеки України;
- кримінальні правопорушення, пов'язані з легалізацією доходів, одержаних злочинним шляхом

Кібершпигунство

- викрадення в політичних, економічних або військових цілях чутливої інформації;
- здійсненням розвідувально-підривної діяльності

Кібертероризм

- використання терористичними організаціями кіберпростору для вчинення актів кібертероризму, фінансової та іншої підтримки терористичної діяльності

Рис. 2. Загрози кібербезпеці України

• саміт НАТО у Варшаві (2016) – кіберпростір визнаний сферою операцій, у якій НАТО має захищатися;

• саміт НАТО в Брюсселі (2018) – прийняте рішення про створення Оперативного центру в кіберпросторі, який має забезпечувати ситуаційну обізнаність і координувати оперативну діяльність НАТО в кіберпросторі та через нього;

• саміт НАТО в Брюсселі (2021) – схвалена Всеосяжна політика кіберзахисту для підтримки трьох основних завдань НАТО: активно стримувати, захищатися і протидіяти повному спектру кіберзагроз у будь-який час (у мирний час, під час криз та конфліктів) – на політичному, військовому і технічному рівнях;

• саміт НАТО у Вільнюсі (2023) – схвалена нова концепція посилення внеску кіберзахисту в загальну систему стримування та оборони НАТО для покращення спільної обізнаності НАТО про ситуацію та кіберстійкість;

• саміт НАТО у Вашингтоні (2024) – прийняте рішення про створення Центру інтегрованого кіберзахисту НАТО для посилення захисту мереж, ситуаційної обізнаності та використання кіберпростору для проведення кібероперацій.

На проведених заходах увага була зосереджена на необхідності своєчасного виявлення, запобігання, нейтралізації та ліквідації кіберзагроз, а також створення кібероборони.

Крім того, щорічно НАТО проводить низку значущих конференцій з питань кібербезпеки та оборони. Основними подіями стали:

1. Міжнародні конференції з кіберконфліктів (CyCon), які щорічно організовуються НАТО Cooperative Cyber Defence Centre of Excellence (CCDCOE) у Таллінні (Естонія). Теми CyCon охоплюють дослідження з технічних, стратегічних та правових аспектів кібероборони. Наприклад, на конференції CyCon у 2019 р. «Silent Battle» досліджувалися питання вразливостей, відповідальності та ситуаційної обізнаності в кіберпросторі, а на конференції CyCon у 2024 р. «Over the Horizon» були визначені перспективні виклики в кіберпросторі та заходи щодо реагування на них [3].

2. Щорічні навчання «Cyber Coalition», на яких відпрацьовуються форми та способи спільного реагування на кіберзагрози. Наприклад, у 2023 р. участь взяли 35 країн, включно з Україною [4].

3. Конференції з кібербезпеки в морській галузі, організовані НАТО Maritime Interdiction Operational Training Center (NMIOTC). На цих конференціях досліджуються питання захисту критичної морської інфраструктури та безпеки в цифровому середовищі. Наприклад, 8-ма Конференції з кібербезпеки в морській галузі відбулась у вересні 2024 р. [5].

4. Міжнародні навчання Locked Shields 2024 з кіберзахисту, в яких українські експерти співпрацювали з фахівцями з понад 40 країн для вдосконалення своїх навичок та посилення міжнародної кіберстійкості [6].

Ці заходи демонструють зусилля НАТО щодо вдосконалення колективної кібероборони та забезпечення безпеки своїх членів і партнерів у цифровому світі.

В Україні спільно з країнами НАТО активно проводяться дослідження з кібероборони, в яких беруть участь провідні науковці, організації та центри. Так, у роботі [7] опубліковане дослідження, проведене під егідою НАТО CCDCOE, щодо національного управління кібербезпекою в Україні. У звіті розглядається роль правової бази в розвитку кібербезпеки в Україні, що є основою для розробки міжнародних стратегій кібероборони.

У Національному кластері кібербезпеки України (NCSCC) активно вивчається та здійснюється обмін досвідом кіберзахисту та кібероборони в Україні з НАТО та ЄС [8].

Крім того, НАТО підтримує співпрацю українських дослідників через такі програми, які сприяють інноваціям у сфері кібербезпеки, як DIANA (Акселератор оборонних інновацій) та інвестиційний фонд НАТО. Це включає участь українських дослідників у спільних хакатонах і проєктах, таких як програма BRAVE1 у партнерстві з урядом України.

Ці зусилля свідчать про активну інтеграцію українських та міжнародних експертів для дослідження проблем реагування на виклики у сфері кібероборони, а також проблем розвитку правової бази та організаційних засад кібероборони. Разом з тим, проблемні питання, пов'язані з розвитком понятійного апарату та теоретичних засад кібероборони, системно не розглядалися. У зв'язку із цим актуальним є питання аналізу стану теоретичних засад кібероборони України та визначення перспектив їхнього розвитку.

Мета статті полягає в аналізі та розвитку понятійного апарату з питань кібероборони в Україні та формування пропозицій щодо створення кіберсил в Україні з урахуванням досвіду провідних країн НАТО.

Викладення основного матеріалу дослідження. Питання розроблення теоретичних засад кібероборони держави стало особливо актуальним у 2016 р., коли в березні була прийнята Стратегія кібербезпеки України [9] (далі – Стратегія-2016), у котрій дане поняття кібероборони, під якою розуміються заходи з підготовки держави до відбиття воєнної агресії в кіберпросторі, а Міністерство оборони України та Генеральний штаб Збройних Сил України визначені головними суб'єктами з кібероборони.

Подальший розвиток теоретичних засад кібероборони держави відбувся у 2017 р., коли в жовтні був прийнятий Закон України «Про основні засади забезпечення кібербезпеки України» [10] (далі – Закон про

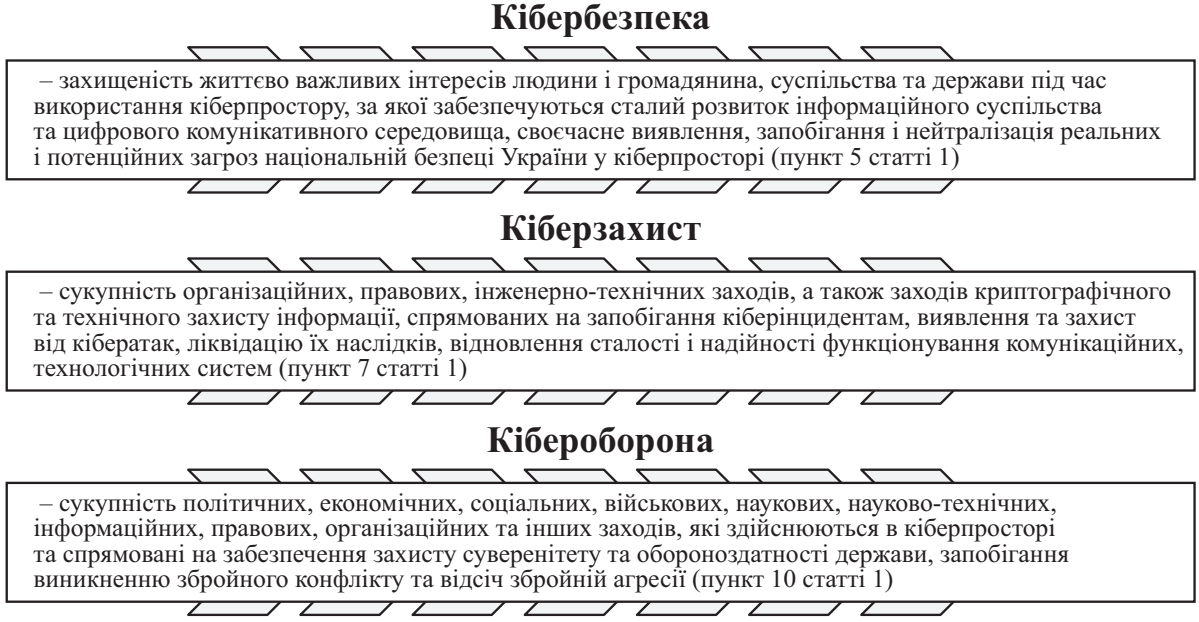

Рис. 3. Система нових понять у сфері кібербезпеки

кібербезпеку), у якому вперше законодавчо визначені такі терміни, як кібербезпека, кіберзахист та кібероборона (*рис. 3*).

Аналіз цих понять показує, що,

- по-перше, кібербезпека є властивістю держави захищати інтереси як людини (громадянина, суспільства), так і держави під час використання кіберпростору;
- по-друге, кіберзахист та кібероборона є сукупністю заходів у різних сферах інтересів людини (громадянина, суспільства) та держави, які здійснюються в кіберпросторі;
- по-третє, кібербезпека, кіберзахист та кібероборона тісно пов'язані між собою в кіберпросторі, при цьому кіберзахист і кібероборона – це сукупність різних заходів, спрямованих на забезпечення різних складових кібербезпеки;
- по-четверте, в понятті кібероборони розширено та деталізовано сукупність заходів з різних сфер людської діяльності, які здійснюються в кіберпросторі.

Принципово важливим є те, що статтю 3 Закону України «Про оборону України» доповнено новим абзацом про те, що підготовка держави до оборони має охоплювати кібероборону (активний кіберзахист) для захисту суверенітету держави, запобігання збройному конфлікту та відсічі збройній агресії [11].

Модель взаємозв'язків складових кібербезпеки, побудована за результатами стислого аналізу Стратегії-2016 та Закону про кібербезпеку, свідчить про те, що кібербезпека, кіберзахист і кібероборона є значною мірою різними за змістом, інтересами та заходами в кіберпросторі України (*рис. 4*).

З моделі взаємозв'язків складових кібербезпеки видно, що в широкому розумінні кібероборона здійснюється в інтересах держави шляхом виявлення, запобігання та нейтралізації реальних і прогнозованих загроз у кіберпросторі та спрямована на захист суверенітету та обороноздатності держави, запобігання виникненню збройного конфлікту та відсічі збройній агресії.

Указом Президента України № 447/2021 «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» від 26 серпня 2021 року була затверджена нова редакція Стратегії кібербезпеки України. Принципово важливим у цьому документі стало те, що першою стратегічною ціллю у формуванні потенціалу стримування визначено дієву кібероборону, для досягнення якої Україна має створити і забезпечити розвиток підрозділів з повноваженнями ведення збройного протиборства в кіберпросторі, сформувати модель функціонування та застосування кібервійськ, а також забезпечити ефективну взаємодію під час здійснення заходів з кібероборони [1].

У Стратегії кібербезпеки України система кібероборони держави є складовою національної системи кібербезпеки та має будуватися на засадах стримування, кіберстійкості та взаємодії. При цьому стратегічною ціллю створення нової національної системи кібербезпеки України є створення дієвої кібероборони (ціль С.1, Стратегія кібербезпеки України).

Ієрархія формування нової якості Національної системи кібербезпеки, яка охоплює виклики та загрози кібербезпеці України, стратегічні цілі та засади

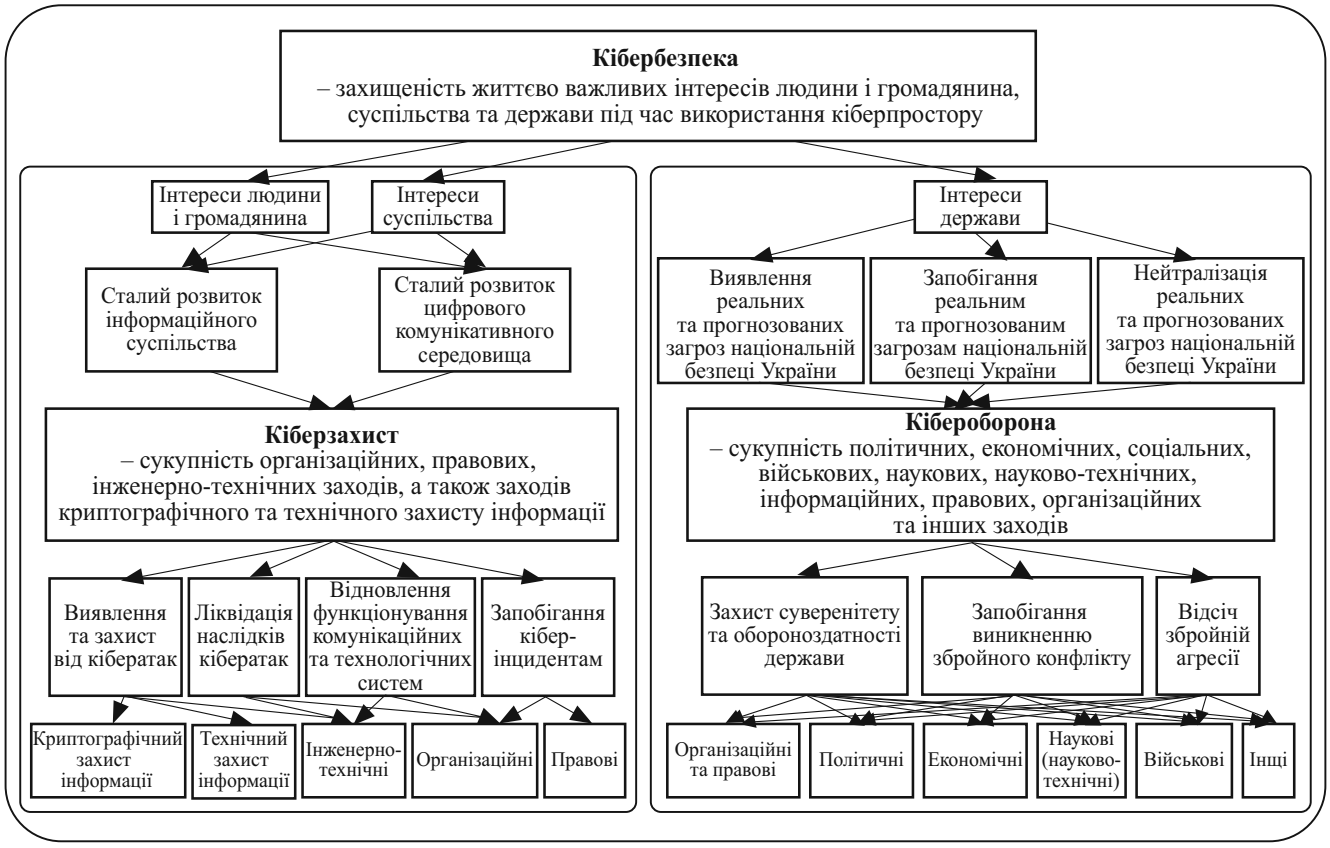

Рис. 4. Модель взаємозв'язків складових кібербезпеки

створення, а також суб'єкти забезпечення кібербезпеки наведена на *рисунку 5*. Аналіз рисунку показує, що в умовах мілітаризації кіберпростору та розвитку кіберзброї дієва кібероборона має передусім захищати від застосування кіберзброї, а також протидіяти кібершпигунству і кібертероризму. При цьому основними суб'єктами кібероборони є Міністерство оборони України, Генеральний штаб Збройних Сил України та Державна служба спеціального зв'язку та захисту інформації України.

Виходячи з основних положень воєнної науки, спираючись на визначення понять з кібероборони, наведені в законах України та нормативно-правових документах, дамо визначення основних категорій та понять з питань кібероборони.

Як відомо, кібероборона передбачає кібердії оборонного характеру, спрямовані на відсіч воєнній (збройній) агресії в кіберпросторі. Тому під агресією в кіберпросторі розумітимемо пряме або непряме застосування кіберпідрозділами іноземних держав кіберозброєння в кіберпросторі іншої держави. У результаті агресії в кіберпросторі між державами може виникнути таке явище, як війна у кіберпросторі, тобто кібервійна.

Специфічним змістом кібервійни є кіберборотьба, сутність якої полягає в організованому застосуванні кібервійськ та кіберпідрозділів розвідувальних і спеціальних служб у кіберпросторі для відсічі агресії в кіберпросторі. Оскільки агресія в кіберпросторі здійснюється приховано без оголошення загального стану війни між державами, то має місце конфлікт у кіберпросторі, або кіберконфлікт.

Кіберконфлікт є різновидом кіберборотьби, яка полягає в організованому застосуванні кібервійськ для досягнення визначених цілей у кіберпросторі. Характер, способи та масштаби кіберборотьби залежать від розвитку кіберозброєння та відбуваються відповідно до законів війни. Так, зміни у способах кіберборотьби відбуваються стрибками залежно від кількості нового кіберозброєння. Накопичення кількісних змін приводить до якісних змін. У процесі розвитку засобів та способів кіберборотьби виникають протиріччя між ними, оскільки засоби кіберозброєння розвиваються швидше, ніж способи та форми кіберборотьби. А це врешті-решт призводить до появи нових досконаліших форм і способів кіберборотьби.

Протиріччя, які виникають під час ведення дій у кіберпросторі, спричинені впливом різних засобів кіберозброєння, які застосовують сторіни кіберконфлікту (або кібервійни). Такі дії в кіберпросторі можуть призвести до порушення управління військами. Подолання

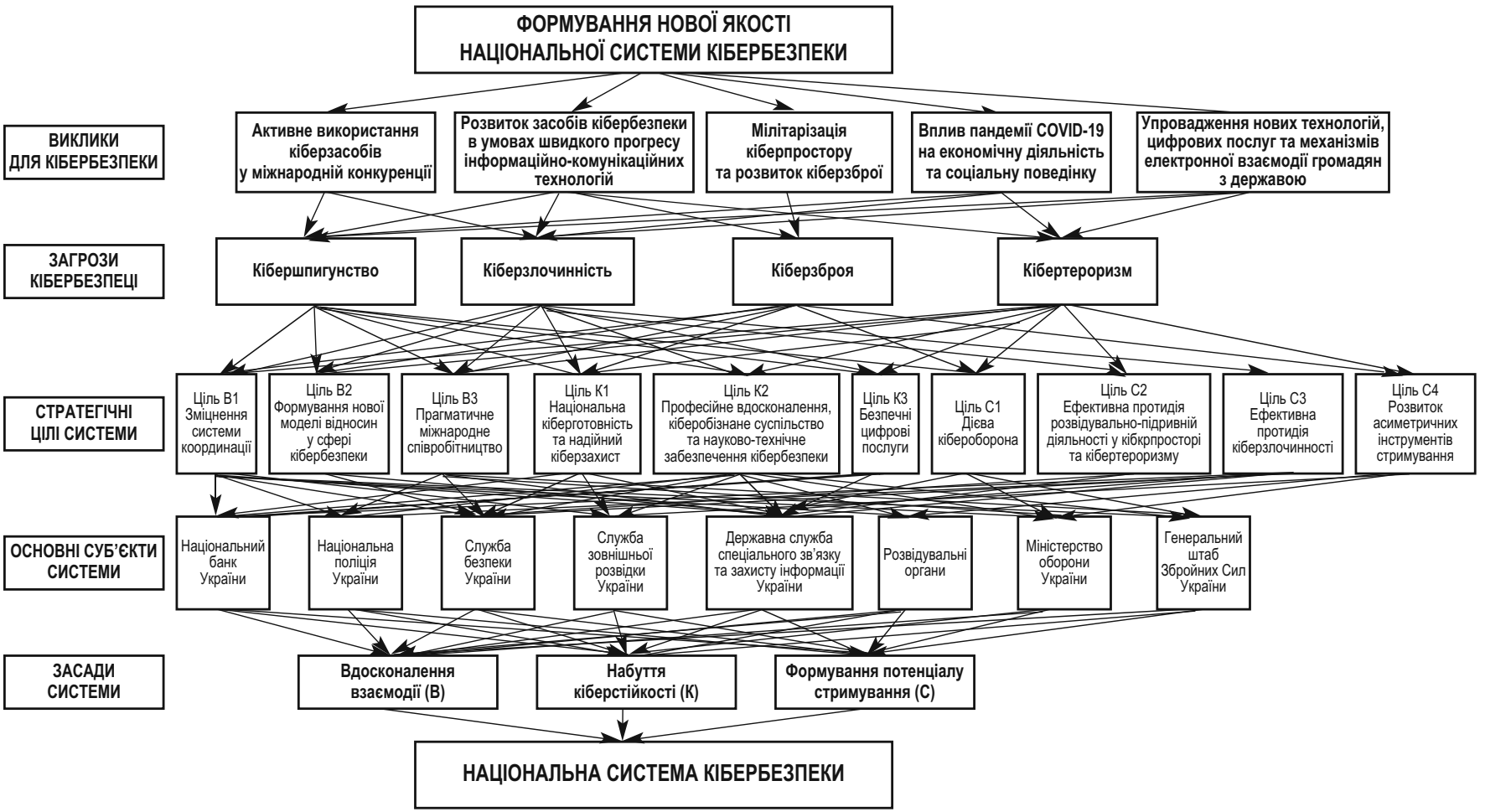

Рис. 5. Ієрархія формування Національної системи кібербезпеки

або зменшення негативних наслідків таких дій противника залежить від якості кіберозброєння та організації кіберборотьби, а також розвитку теоретичних засад кібероборони.

Бойові дії в кіберпросторі – це організоване застосування кіберсил та кіберзасобів з метою нанесення втрат і протидії противнику в кіберпросторі. При цьому під кіберсилами розуміють кіберпідрозділи військових формувань (кібервійська) та кіберпідрозділи розвідувальних і спеціальних служб, а під кіберзасобами – кіберозброєння.

Бойові дії в кіберпросторі можуть бути оборонними, наступальними чи агресивними. У разі агресивних дій у кіберпросторі ураженню піддаються також цивільні та невійськові об'єкти критичної інфраструктури.

На сучасному етапі основними формами дій у кіберпросторі є кібероперація та кіберудар, а способами дій у кіберпросторі – кібернаступ та кібероборона. Під кібернаступом розуміються наступальні дії в кіберпросторі, а під кібероборoною – оборонні дії в кіберпросторі.

Кібероперація – це сукупність узгоджених та взаємопов'язаних за ціллю, місцем та часом впливу кібератак, які проводяться за єдиним задумом та планом для вирішення завдань у кіберпросторі. Кіберудар – це короткочасний вплив на кіберпростір противника із застосуванням кіберозброєння. При цьому кібератака є вирішальним етапом кіберудару.

Кібернаступ проводиться з метою нанесення втрат противнику в кіберпросторі та здійснюється в рамках наступальних дій сил оборони у взаємодії з підрозділами розвідувальних і спеціальних служб. Кібернаступ може проводитися кібервійськами самостійно.

Кібернаступ має дві фази: підготовки та ведення.

Підготовка кібернаступу охоплює: прийняття рішення та планування кібернаступу; постановку завдань кібервійськам та організація взаємодії; групування кіберсил та кіберзасобів; усебічне забезпечення дій у кіберпросторі.

Ведення кібернаступу охоплює нанесення кібератак по об'єктах кіберпростору противника із застосуванням наявного кіберозброєння.

Кібероборона здійснюються кібервійськами з метою відбиття кібернаступу противника та захисту об'єктів кіберпростору. При цьому кібероборона має свою побудову, яка охоплює: угрупування кіберсил та кіберзасобів, систему кіберзахисту, систему нанесення кібератак.

Кібероборона, як і кібернаступ, має дві фази: підготовки та ведення.

Підготовка кібероборони охоплює: постановку завдань кібервійськам та планування кібероборони; побудову кібероборони; організація взаємодії; підготовку кібервійськ до дій та всебічне забезпечення оборонних дій у кіберпросторі.

Ведення кібероборони охоплює нанесення кібератак по об'єктах кіберпростору противника із застосуванням наявного кіберозброєння та відновлення об'єктів кіберпростору, які зазнали ураження.

У провідних країнах світу основою системи кібероборони є новий вид збройних сил – кіберсили (кібервійська) (*табл. 1*).

Кіберсили НАТО складаються з окремих ключових елементів, інтегрованих у загальну структуру оборони Альянсу. Основні складові кірерсил НАТО розкриті нижче.

1. Головним центром для координації зусиль у сфері кібербезпеки є Центр кібероперацій (Cyber Operations Center, CyOC), основна місія якого полягає в захисті цифрових мереж НАТО від кібератак, забезпеченні безперебійної роботи військових і цивільних функцій [12].

2. Центр передового досвіду у сфері кіберзахисту (CCDCOE) (м. Таллін, Естонія), який займається навчанням, дослідженнями та аналізом стратегій у сфері кіберзахисту. Центр організовує щорічні кібернавчання, такі як «Locked Shields» і «Crossed Swords», які є найбільшими у світі [13].

Кіберсили НАТО є комплексною мережею організацій, яка охоплює як військові структури, так і партнерства з приватними й академічними установами, спрямовані на забезпечення колективного кіберзахисту Альянсу та партнерів.

Кіберсили збройних сил країн НАТО об'єднують військових та цивільних фахівців з проведення наступальних чи оборонних дій у кіберпросторі. При цьому вони мають різні системи організації, управління, комплектування та підготовки. Коротко розгляньмо їх.

США. Кіберсили США [14] організовані під керівництвом U.S. Cyber Command (USCYBERCOM), який відповідає за оборону в кіберпросторі, підтримку військових операцій і національні інтереси в глобальній мережі, та кіберпідрозділ Cyber National Mission Force (CNMF), котрий проводить кібероперації як частину місій із захисту США, включно з міжнародними операціями «hunt forward» для протидії кіберзагрозам у країнах НАТО.

Основні складові кіберсил США містять п'ять ключових команд і 133 кіберпідрозділи. Команди входять до складу: 16-ї повітряної армії (16th Air Force) для кібероперацій у повітряній сфері; армійського кіберкомандування (Army Cyber Command) для підтримки сухопутних операцій; морського кіберкомандування (Fleet Cyber Command) для забезпечення кібероперацій на морі та морської кіберкоманди (Marine Corps Cyberspace Command) для забезпечення кіберзавдань корпусу морської піхоти.

Велика Британія (UK Cyber Forces). UK Cyber Forces складаються з декількох організацій і підрозділів, що працюють у взаємодії для захисту національних

Таблиця 1

Склад кіберсил провідних країн НАТО

Країна та рік утворення	Основний орган управління та основні складові кіберсил	Призначення складових кіберсил
Кіберсили США	1. U.S. Cyber Command (USCYBERCOM)	
	1.1. Cyber Mission Force (CMF) охоплює 133 кіберкоманди, зокрема:	• основна структура для проведення кібероперацій
	13 національних кіберкоманд (Cyber National Mission Teams)	• виконують незалежні операції для кіберзахисту США, ідентифікуючи кіберзагрози та захищаючи від кібератак
	27 бойових кіберкоманд (Cyber Combat Mission Teams)	• здійснюють підтримку бойових дій
	68 команд з кіберзахисту (Cyber Protection Teams)	• здійснюють захист мереж міністерства оборони США
	25 команд з кіберпідтримки (Cyber Support Teams)	• здійснюють інформаційно-аналітичне забезпечення інших підрозділів
	1.2. Cyber National Mission Force (CNMF)	• проводить кібероперації як частину місій із захисту США та протидії кіберзагрозам у країнах НАТО
Кіберсили Великої Британії (2020)	1. Національний центр кібербезпеки (National Cyber Security Centre, NCSC)	
	1.1. Міністерство оборони (MoD)	• забезпечує стратегічну підтримку операцій NCF; • інтегрує кібернетичні та електромагнітні операції з іншими військовими доменами
	1.2. Центр урядового зв'язку (GCHQ)	• фокусується на розвідувальній діяльності
Кіберсили Німеччини (2017)	1. Служба кібер- та інформаційного простору (Cyber- und Informationsraum, CIR)	
	1.1. Центральне командування CIR	• зосереджене на створенні єдиної оперативної команди для координації як внутрішніх, так і зовнішніх операцій Німеччини в кіберпросторі
	1.2. Підрозділи кіберзахисту (Cyber Defense Units)	• безпосередній захист ІТ-інфраструктури міністерства оборони, реагування на кіберзагрози та відновлення роботи після атак; • технічний моніторинг, виявлення та аналіз загроз
	1.3. Розвідувальні підрозділи (Cyber Intelligence)	• моніторинг кіберпростору, збирання розвідувальної інформації про загрози
	1.4. Центр військової ІТ-компетенції (Bundeswehr IT Center of Excellence)	• підготовка та навчання кадрів, дослідження нових технологій і підтримка впровадження сучасних ІТ-рішень у кіберзахисті
	1.5. Підрозділи інформаційних операцій	• інформаційна безпека та протидія дезінформації, особливо у військових контекстах; • підтримка операцій в інформаційному полі та розвиток стратегій інформаційного впливу
	1.6. Підрозділи інтеграції з НАТО з питань кібероборони	• активна співпраця з іншими країнами НАТО, зокрема в рамках Спільного центру передового досвіду з кібероборони (NATO CCDCOE) в Естонії
Кіберсили Франції	1. Командування COMCYBER (Cyber Defense Command)	• здійснення захисту інформаційних систем для запобігання, виявлення та протидії кібернападам; • захист військових інформаційних систем; • розробка, планування та проведення оборонних та наступальних військових операцій, операцій з впливу в кіберпросторі; • оперативна підготовка збройних сил у кіберпросторі через національні чи міжнародні тренування та навчання; • узгодженість моделі кіберзахисту та її загальна координація (кадрова політика, технічні потреби, розробка доктрини); • розвиток та управління резервом оперативного та цивільного кіберзахисту

Закінчення таблиці 1

Країна та рік утворення	Основний орган управління та основні складові кіберсил	Призначення складових кіберсил
	1.1. Штаб кіберзахисту (EM-CYBER)	• проведення операцій з кіберзахисту: командування кіберзахисту розробляє, планує та проводить військові операції з кіберзахисту і відповідає за оборону та захист інформаційних систем міністерства збройних сил, за винятком систем Генерального директорату зовнішньої безпеки (DGSE) і Директорату розвідки та оборонної безпеки (DRSD); • формує Стратегію кіберзахисту: командування кіберзахисту координує внески збройних сил і спільних організацій у національну та міжнародну політику кіберзахисту, зокрема для розробки та реалізації планів співпраці; це також забезпечує узгодженість моделі кіберзахисту міністерства та її загальну координацію; • розвиток спроможності: командування кіберзахисту сприяє розробці кадрової політики кіберзахисту, координації визначення конкретних технічних потреб кіберзахисту і розвитку та управління резервом кіберзахисту
	1.2. Армійська групи кіберзахисту (GCA)	• консолідація континууму між кіберзахистом та обороною шляхом сприяння синергії між цими сферами і передача досвіду між окремими підрозділами; • управління інформацією, людськими ресурсами (набір – цивільні, діючі військові та резервні, навчання, канцелярія) та кіберзахистом
	1.2.1. Центр аналізу кіберзагроз (CALID)	• координує військову кібероборону, відповідає за організацію як оборонних, так і наступальних операцій у кіберпросторі, забезпечуючи захист військових систем і підтримку стратегічних місій, технічний аналіз кіберзагроз, координацію оборонних заходів і впровадженням нових технологій
	1.2.2. Центр аудиту безпеки інформаційних систем (CASSI)	• національний центр, аудиторська місія якого охоплює дві сфери: безпеку інформаційних систем (ISS) і компрометацію паразитних сигналів (SPC)
	1.2.3. Об'єднаний головний узгоджувальний центр (CHPI)	• забезпечення безпеки інформаційних систем Міністерства Збройних Сил України протягом терміну їх експлуатації
	1.2.4. Центр оперативної підготовки кіберзахисту (C2PO)	• оперативна підготовка кібервинищувачів, спеціальне навчання кіберспеціалістів

інтересів у кіберпросторі, забезпечення обороноздатності та реалізації наступальних кібероперацій. Основними компонентами кіберсил є Національні кіберсили (National Cyber Force, NCF), створені 2020 р., які об'єднують підрозділи Міністерства оборони (MoD) та Центру урядового зв'язку (GCHQ) [15].

Національний центр кібербезпеки (National Cyber Security Centre, NCSC) орієнтований на захист критичної інфраструктури, підвищення стійкості до кіберзагроз та співпрацю з приватним сектором. Він забезпечує регіональну підтримку через надання стратегічних консультацій і допомогу у відбитті кібератак.

Німеччина. Кіберсили Німеччини є частиною Бундесверу та представлені Службою кібер- та інформаційного простору (Cyber- und Informationsraum, CIR), створеної 2017 р. для захисту цифрових інфраструктур, боротьби з кіберзагрозами, забезпечення інформаційної безпеки та управління розвідданими. Головним органом управління є Центральне управління CIR, зосереджене на єдиному оперативному управлінні як внутрішніми, так і зовнішніми операціями Німеччини в кіберпросторі.

Нині розглядається питання щодо трансформації кіберсил у новий четвертий вид збройних сил Німеччини, поряд із сухопутними військами, військово-морськими та військово-повітряними силами.

Франція. Кіберсили Франції складаються з декількох ключових компонентів, що діють під егідою збройних сил. Їхньою основною метою є захист національної безпеки в кіберпросторі, розробка наступальних та оборонних кіберзасобів, а також міжнародне співробітництво у сфері кібероборони. Кіберсили Франції

складаються з [16]: головного органу COMCYBER (Cyber Defense Command), який координує кібероборону та відповідає за організацію як оборонних, так і наступальних операцій у кіберпросторі, забезпечуючи захист військових систем і підтримку стратегічних місій. Для виконання своїх місій COMCYBER має дві структури:

- Штаб кіберзахисту (EM-CYBER);
- Армійську групу кіберзахисту (GCA).

EM-CYBER розробляє, планує та проводить військові операції кіберзахисту, формує стратегію кіберзахисту та розвиває спроможності з кібероборони та кіберзахисту.

GCA призначена для консолідацію континууму між кіберзахистом та обороною шляхом сприяння синергії між цими сферами і передачі досвіду. GCA об'єднує чотири технічні центри COMCYBER:

- центр аналізу оборонної комп'ютерної війни (CALID);
- центр аудиту безпеки інформаційних систем (CASSI);
- спільний головний центр акредитації (CHPI);
- центр підготовки до кібероперацій (C2PO).

COMCYBER взаємодіє з Національним агентством з безпеки інформаційних систем (ANSSI), яке здійснює захист критичної інфраструктури Франції, а також сприяє кібербезпеці в державному і приватному секторах. ANSSI також виконує роль консультанта для оборонних сил у сфері захисту інформаційних систем.

Аналіз *таблиці 1* показує, що кіберсили провідних країн НАТО мають два варіанти організації. Перший варіант передбачає входження кіберсил у склад національних збройних сил та взаємодію їх із цивільними кіберпідрозділами (США, Німеччина). Другий варіант – об'єднання в окремій національній структурі військових та цивільних кіберпідрозділів (Велика Британія, Франція). При цьому незалежно від варіанта організації кожна країна НАТО зберігає відповідальність за національний кіберзахист, але водночас здійснює обмін даними, координацію навчань і розробку спільних стратегій кібероборони.

Україна. Кіберсили України поки перебувають на етапі створення [17]. Відповідно до урядових планів, кіберсили України мають бути окремим родом військ у складі Збройних Сил України. До складу кіберсил мають входити як оперативні підрозділи для негайного реагування, так і аналітичні структури для розробки довгострокових стратегій кібероборони. Крім того, передбачається тісна співпраця з національними та міжнародними організаціями, що займаються питаннями кібербезпеки, зокрема в рамках НАТО. Їхніми основними завданнями стане забезпечення кіберзахисту військових інформаційних систем, відбиття кібератак, проведення наступальних кібероперацій та моніторинг кіберпростору. Це відповідає світовим тенденціям, де кіберсили стали важливим елементом військових структур багатьох країн, таких як США та Німеччина, які вже мають розвинені кіберкомандування для реалізації подібних функцій.

Висновки, пропозиції та рекомендації

Аналіз законів України, в яких викладені основні поняття з питань кібероборони, показує, що кібероборона є критично важливим елементом кібербезпеки та національної безпеки України загалом, оскільки розвиток сучасних кібертехнологій створює нові загрози для політичної, економічної та військової сфер. Основними загрозами є кіберзброя наступального призначення, кібершпигунство, кібертероризм та кіберзлочинність. При цьому модель кібероборони потребує більшого інтегрування з військовими та цивільними компонентами.

Аналіз досвіду країн НАТО у формуванні кіберсил показує, що існують два підходи: інтеграція кіберсил у збройні сили (США, Німеччина) або створення окремих національних структур, які об'єднують військові та цивільні кіберпідрозділи (Велика Британія, Франція). Тому, виходячи із цього досвіду, доцільно інтегрувати кібероборону в багаторівневу систему кібербезпеки України. При цьому розробка теоретичних засад і законодавчих актів має стати основою для створення дієвих кібервійськ. Для цього необхідно:

- сформувати окремий рід військ у складі Збройних Сил України, який міститиме оперативні та аналітичні підрозділи;
- розробити нові законодавчі акти або доповнити існуючі для регулювання діяльності кібероборони, враховуючи міжнародний досвід;
- посилити співпрацю з НАТО, зокрема в рамках програм, які підтримують обмін даними, навчання та спільну розробку кіберзасобів;
- розвивати програми підготовки кадрів з кібербезпеки та залучати новітні технології, зокрема штучний інтелект, для підвищення ефективності кібероборони;
- створити єдиний координаційний орган, який відповідатиме за управління всіма аспектами кібероборони;
- зосередити увагу на розробці форм та способів ведення кібероперацій, наприклад таких, як кібероборона, кіберудари, кібернаступ та управління конфліктами в кіберпросторі;
- забезпечити фінансування для розробки нових кіберзасобів і підтримки дослідницьких програм у сфері кібербезпеки;
- упровадити систему моніторингу та аналізу кіберзагроз у реальному часі для своєчасного реагування.

Перелік літератури

1. Стратегія кібербезпеки України [Електронний ресурс] : затверджена Указом Президента України № 447/2021 від 26 серпня 2021 р. // Верховна Рада України. Законодавство України. – Режим доступу : https://zakon.rada.gov.ua/laws/show/447/2021#n7.

2. Cyber defence [Електронний ресурс] // NATO. – Режим доступу : https://www.nato.int/cps/en/natohq/topics_78170.htm.

3. International Conference on Cyber Conflict – CyCon [Електронний ресурс] // CCDCOE. – Режим доступу : https://ccdcoe.org/cycon.

4. Cyber Coalition: NATO's Flagship Cyber Exercise [Електронний ресурс] // NATO Allied Command Transformation. – Режим доступу : https://www.act.nato.int/activities/cyber-coalition.

5. Cyber Security Conference [Електронний ресурс] // NMIOTC – NATO Maritime Interdiction Operational Training Centre – Greece. – Режим доступу : https://nmiotc.nato.int/transformation/conferences/cyber-security-conference.

6. Locked Shields 2024 Sets the Stage for Advancing Global Cyber Defence [Електронний ресурс] // CCDCOE. – Режим доступу : https://ccdcoe.org/news/2024/locked-shields-2024-sets-the-stage-for-advancing-global-cyber-defence.

7. New Report on National Cybersecurity Governance: Ukraine [Електронний ресурс] // CCDCOE. – Режим доступу : https://ccdcoe.org/news/2024/new-report-on-national-cybersecurity-governance-ukraine.

8. Зміцнюючи національну кібербезпеку [Електронний ресурс] // Національний кластер кібербезпеки. – Режим доступу : https://cybersecuritycluster.org.ua.

9. Стратегія кібербезпеки України [Електронний ресурс] : затверджена Указом Президента України № 96/2016 від 15 березня 2016 р. // Верховна Рада України. Законодавство України. – Режим доступу : https://zakon.rada.gov.ua/laws/show/96/2016/ed20160315#Text.

10. Про основні засади забезпечення кібербезпеки України [Електронний ресурс] : Закон України № 2163-VIII від 5 жовтня 2017 р. // Верховна Рада України. Законодавство України. – Режим доступу : https://zakon.rada.gov.ua/laws/show/2163-19#Text.

11. Про оборону України [Електронний ресурс] : Закон України № 1932-XII від 6 грудня 1991 р. // Верховна Рада України. Законодавство України. – Режим доступу : https://zakon.rada.gov.ua/laws/show/1932-12#Text.

12. NATO Cyber Operation Centre [Електронний ресурс] // NATO Rapid Deployable Corps Italy. – Режим доступу : https://nrdc-ita.nato.int/operations/allied-reaction-force/nato-cyber-operation-centre.

13. Exercises [Електронний ресурс] // CCDCOE. – Режим доступу : https://ccdcoe.org/exercises/.

14. *Lonergan E.* United States Cyber Force: A Defense Imperative [Електронний ресурс] / E. Lonergan, M. Montgomery // FDD. – Режим доступу : https://www.fdd.org/analysis/2024/03/25/united-states-cyber-force.

15. The National Cyber Force: Directions and Implications for UK – Analysis [Електронний ресурс] / D. Steed ; Elcano Royal Institute // Eurasia Review. – Режим доступу : https://www.eurasiareview.com/12022021-the-national-cyber-force-directions-and-implications-for-uk-analysis.

16. Le commandement de la cyberdéfense (COMCYBER) [Електронний ресурс] // Ministére des Armées. Commandement de la cyberdéfense. – Режим доступу : https://www.defense.gouv.fr/comcyber/commandement-cyberdefense-comcyber.

17. Проект Закону України про Кіберсили Збройних Сил України [Електронний ресурс] : № 12349 від 19 грудня 2024 р. // Верховна Рада України. Законопроекти. – Режим доступу : https://itd.rada.gov.ua/billinfo/Bills/Card/45453.