DOI:**10.33099/2311-7249/2020-37-1-31-48**

УДК: 004.413.4

Сергій Григорович Вдовенко
Юрій Григорович Даник *(доктор технічних наук, професор)*
Олександр Юрійович Пермяков *(доктор технічних наук, професор)*

Національний університет оборони України імені Івана Черняховського, Київ, Україна

ДОСВІД РОЗВИТКУ СИСТЕМ КІБЕРБЕЗПЕКИ ТА КІБЕРОБОРОНИ ПРОВІДНИХ КРАЇН СВІТУ

Стрімкий розвиток та масове впровадження досягнень електроніки, сучасних інформаційних та кібер- технологій призвели до формування нового спектру ризиків та загроз у сфері національної безпеки і оборони держави, які реалізуються у кіберпросторі та (або) через кіберпростір. Відбувається стрімке зростання інформатизації та автоматизації всіх сфер людської діяльності, кількості інформації що зберігається, обробляється і передається, швидкості її передачі і обробки, ускладнення систем управління, взаємодії між ними і зв'язків між процесами управління. Кіберзагрози охоплюють всі базові сфери суспільної діяльності (політичну, воєнну, правову, економічну, енергетичну, інфраструктурну, соціальну, духовну, технологічну тощо), деструктивно впливаючи на національну безпеку в цілому.

Більше 60 країн світу, міжнародні (ЄС) та військово-політичні союзи (НАТО), міжнародні безпекові організації (ОБСЄ) зосереджують значні зусилля щодо забезпечення спроможностей зі своєчасного виявлення, запобігання, нейтралізації і ліквідації загроз в кіберпросторі, зокрема у сфері оборони.

В статті представлені результати: здійснення аналізу існуючих систем кібербезпеки і кібероборони провідних країн світу в контексті можливості та доцільності впровадження їх досвіду в Україні; здійснення аналізу передумов, існуючого стану та проблемних питань формування систем кібербезпеки та кібероборони в Україні, а також потрібного рівня їх всебічного забезпечення; здійснення розробки основних теоретичних та прикладних положень формування систем кібербезпеки та кібероборони в Україні.

Ключові слова: *кібербезпека; кібероборона; кіберпростір; система кібербезпеки; система кібероборони; кіберзагроза; кіберзахист; суб'єкти кібербезпеки; суб'єкти кібероборони; об'єкти критичної інфраструктури.*

Вступ

Постановка проблеми. В сучасному світі питання кібербезпеки та кібероборони стали найбільш актуальними й разом з тим найбільш проблемними в забезпеченні національної безпеки і оборони практично для всіх держав світу. На даний час інформаційні та кібер- фактори стають системоутворюючими у сучасних воєнних (гібридних, проксі- та інших) кофліктах та збройній боротьбі у всіх її проявах. Але, комплексних та системних досліджень з цих питань проведено недостатньо. І це особливо проявляється в умовах криз (як, наприклад, при проведенні АТО (ООС), сьогоднішньої пандемії COVID-19 тощо), коли кількість кібератак та кіберінцидентів значно зростає.

Аналіз останніх досліджень і публікацій. Концептуальні проблемні питання щодо загроз національній безпеці, зокрема у сфері інформаційної та кібербезпеки, окремі засади протидії кіберзлочинності та боротьби з кібертероризмом, управління кібербезпекою, а також загальної теорії кібербезпеки досліджували О.Баранов, В.Бурячок, Ю.Грицюк, Р.Грищук, Ю.Даник, Д.Дубов, Р.Лук'янчук, С.Мельник, В.Шеломенцев, В.Шпачук, М.Яцишин та інші. У вітчизняних фахових виданнях проблемам кібероборони, порівняно з провідними країнами світу, приділяється вкрай незначна увага та лише окремими дослідниками [1-3].

Мета цієї роботи полягає в проведенні аналізу і узагальненні відомих результатів, дослідженні і удосконаленні загальної методології та практики формування і розвитку систем кібербезпеки і кібероборони провідних країн світу та, виходячи з цього, розробці найбільш раціонального варіанту вирішення цієї задачі в Україні.

Виклад основного матеріалу дослідження

Поняття "кібернетика" (κυβερνητική – грец.) з'явилося в стародавній Греції, як похідне від слова "кюбернетес" (*κυβερνήτη* – грец.), що означає "керманич". З цим словом пов'язана етимологія інших слів, що широко вживаються у багатьох мовах світу. Так, давні римляни перетворили його на "губернатор" (*gubernator*), англійці – на "уряд" (*government*), в сучасній українській мові це - "керівник".

В давнину під кібернетикою розуміли "мистецтво управління". Древньогрецький

філософ Платон у своїх творах кібернетику визначає, як мистецтво управління кораблем, або колісницею, а також як мистецтво правити людьми. Відомий французький вчений-фізик А.Ампер (André-Marie Ampère) в першій частині своєї праці "Досвід про філософію наук, або Аналітичний виклад природної класифікації всіх людських знань" у 1834 р. зазначив кібернетику як політичну науку про управління державою (народом), яка допомагає урядові вирішувати конкретні завдання з управління державою і забезпечує досягнення при цьому миру для держави та процвітання для народу. У другій частині роботи, опублікованої після його смерті в 1843 р., він визначив кібернетику як мистецтво управління взагалі, управління відносинами між народами зокрема. Роль кібернетики в політиці порівняна ним зі значенням стратегії в військовому мистецтві, з тією відмінністю, що перша націлена на збереження миру між народами.

Початок розвитку сучасної кібернетики, як самостійного наукового напрямку, відносять до 1948 р., коли Норберт Вінер (Norbert Wiener) опублікував роботу "Кібернетика, або управління і зв'язок у тварині і машині", в якій узагальнив закономірності, притаманні системам управління різної природи (біологічних, технічних, соціальних) та визначив, що кібернетика це наука про загальні закономірності процесів управління і передачі інформації в живих організмах, суспільстві та машинах. Пізніше, у 1954 р., у книзі "Кібернетика й суспільство" питання управління в соціальних системах ним були розглянуті більш докладно.

У цей же період, у 1945 р., Клод Шеннон (Claude Elwood Shannon) виступає в Конгресі США із секретною доповіддю "Теорія зв'язку в секретних системах", яка стала точкою відліку для самостійної науки – криптологія. Доповідь була розсекречена у 1949 р. та видана у вигляді монографії разом з роботою "Математична теорія зв'язку", в якій була доведена теорема відліків, або теорема Віттакера – Найквиста – Шеннона – Котельникова. Теорема незалежно була доведена ще у 1933 р. радянським вченим В.Котельниковим у роботі "Щодо перепускної спроможності етеру та дроту в електрозв'язку", яка тоді ж була представлена Генеральному штабу РСЧА у вигляді секретної доповіді.

У грудні 1949 р. Джон фон Нейман (John von Neumann) читає в Іллінойському університеті серію лекцій "Теорія і організація складних автоматів", матеріали яких та ряду інших лекцій стали основою теорії самовідтворення автоматів.

У 1955 р. опублікована стаття С.Соболева, А.Кітова, О.Ляпунова "Основні риси кібернетики". В той же час публікуються дослідження В.Глушкова, які разом склали основи методології сучасної кібернетики, а надалі й кібербезпеки, як галузі знань про забезпечення захищеності процесів управління в усіх сферах (технічній, соціальній, соціотехнічній, економічній тощо) від різноманітних кіберзагроз різної природи та для забезпечення їх ефективності.

Опублікована у 1975 р. робота У.Діффі, (W. Diffie) та Э. Хеллмена (A.Hellman) "Захищеність та імітостійкість. Введення у криптографію" відкрила еру відкритої криптографії та змінило інформаційну структуру суспільства. З'явилася реальна можливість перенести у кіберпростір ряд соціально значущих, в тому числі і соціоуправлінських функцій, заощаджуючи час та кошти, а також мінімізуючи корупційну складову.

У 2016 р. українськими вченими І.Горбенко, О.Замулою та Є.Семенко запропоновано визначення криптографічного дискретного сигналу (КДС), сформульовано в загальному вигляді і вирішено задачу синтезу й аналізу КДС [4,5]. Це значною мірою може вплинути на забезпечення захисту військових кіберфізичних систем (КФС).

Питання та передумови виникнення напрямів кібербезпеки та кібероборони в тому чи іншому контексті пов'язані із появою та розвитком радіотехніки і радіоелектроніки, електронної техніки і технічних засобів шифрування та криптоаналізу, обчислювальної техніки і інформатики, кібернетики, теорії зв'язку та інформації, стрімким розвитком кібернетичних, інформаційно-телекомунікаційних систем та їх впровадженням в усі галузі й сфери людської діяльності [6,7].

Однією з перших країн, яка на державному рівні означила кібернетичну безпеку як окремий вид безпеки, були США. У лютому 2003 р. у США була оприлюднена "Національна стратегія щодо забезпечення безпеки кіберпростору" (National Strategy to Secure Cyberspace), в якій були визначені об'єкти критичної кібернетичної інфраструктури, що підлягають кіберзахисту, а саме: державні та приватні установи різних галузей господарства, промисловості, уряду, оборонного комплексу, телекомунікацій, енергетики, транспорту, банківської справи та фінансового сектору, хімічної промисловості та виробництва небезпечних речовин, судноплавства тощо (рис. 1).

Зокрема, у стратегії було відмічено, що усі вони об'єднані у рамках одного простору - кібернетичного, якій складається із сотень тисяч об'єднаних між собою комп'ютерів, серверів, маршрутизаторів, комутаторів, волоконно-оптичних кабелів, інших електронних систем і пристроїв, які забезпечують роботу об'єктів критичної кібернетичної інфраструктури. Задачею кібербезпеки у рамках цієї стратегії було визначено забезпечення безпеки кіберпростору за рахунок координації цілеспрямованих зусиль уряду та громадян.

Вперше у міжнародний обіг термін кібербезпека офіційно було введено на засіданні підготовчого комітету Всесвітньої зустрічі на вищому рівні з питань побудови інформаційного

суспільства у лютому 2003 р. у Женеві. У першому наближенні під кібербезпекою розумілися питання, пов'язані з проблемами забезпечення безпеки даних та захисту інформації в інформаційному суспільстві, а також проблема недоторканості приватного життя. Але, до того часу вже стали реаліями життя дії в електромагнітному спектрі випромінювання з метою передачі та отримання інформації і протидії цим процесам, соціокібернетичні дії в кіберпросторі та через кіберпростір.

Рис.1. Сфери життєдіяльності що підлягають кіберзахисту та кібероборони.

Для формування науково обґрунтованого підходу щодо визначення напрямків розвитку воєнної, воєнно-технічної, воєнно-наукової, воєнно-економічної, воєнно-дипломатичної політики держави у сфері кібероборони, стратегії кібероборони тощо, слід згадати декілька етапів розвитку окремих питань управління у воєнній сфері, та деяких інших аспектів, що з точки зору воєнно-історичного аналізу впливають на досягнення мети статті.

В усіх без виключення війнах та військових конфліктах була, є і буде присутньою інформаційна складова. З метою приховування своїх намірів та дій, а також для взяття під контроль процесів управління населенням та силами протиборчої сторони використовувалися притаманні для свого часу методи, комунікації та засоби. Питання досягнення успіху за рахунок інформаційних дій свого часу розглядалися на теоретичному рівні Сунь-Цзи, Карлом фон Клаузевіцем (Carl Philipp Gottlieb von Clausewitz), Лідделлом Гартом (Sir Basil Henry Liddell Hart), який в своїй роботі [8] аналізує досвід попередніх поколінь в досягненні мети війни та робить висновок, що дійсною метою війни є створення вигідної стратегічної обстановки яка забезпечить перемогу. У 1996 р. у військовій доктрині США "Concept Force XXI" вперше в світі на законодавчому рівні було визнано необхідність захисту кіберпростору. До цього моменту де-юре мова йшла лише щодо інформаційної безпеки. Але, де-факто, на практиці такі питання фрагментарно та ситуативно вирішувалися від початку практичного застосування радіохвиль, а щодо криптографії – значно раніше.

Історію розвитку та еволюції поглядів людства на кіберінформаційні аспекти управління військами, бойовими діями та війною умовно можна поділити на декілька етапів.

І етап: Початок – перша третина XX сторіччя. Використання електронних засобів для передачі інформації та здійснення інформаційних впливів на широкі маси населення стало можливим з винаходом радіо (1896, 1897 р.р., Олександр Попов, Гульєльмо Марконі (Guglielmo Marconi)). Початок застосування електронних засобів для порушення роботи засобів зв'язку та отримання інформації про противника, зафіксовано невдовзі після винаходу радіо (1904-1905. Російсько-Японська війна), що надало поштовх розвитку напрямків радіорозвідки, радіоподавлення (РЕР, РЕБ) та заборони застосування засобів радіовипромінювання без кріптозахисту інформації, якою обмінювалися. Необхідність дотримання скритності управління військами при масовому використанні засобів зв'язку (1914-18-ий роки, І світова війна та 1920-30-ті роки), призвела до стрімкого розвитку криптографії та криптоаналізу, що згодом поєдналися в єдину науку – криптологія.

З врахуванням висновків з теорії Джуліо Дуе (Giulio Douhet), щодо панування в повітрі, та розвитку засобів повітряного, нападу, формуються військово-повітряні та протиповітряні сили держав, як окремі види збройних сил, військово-повітряні та протиповітряні компоненти видів збройних сил, як роди військ, з відповідними командуваннями, системами управління та забезпечення бойового функціонування. Для їх ефективних дій формуються системи повітряного спостереження, оповіщення та зв'язку – прообраз сучасних систем $C^NX…X$ (наприклад, C4ISR – Command, Control, Communication, Computers, Intelligence, Surveillance, Reconnaissance).

ІІ етап: Друга третина XX сторіччя. В ході та після ІІ Світової війни, що мала характер "війни моторів", на озброєння приймаються атомна зброя, засоби масового ураження, високотехнологічні засоби їх доставки (літаки, гелікоптери, ракети, атомні підводні човни). З'являється можливість масового застосування радіо та телебачення для пропаганди (масовий вплив) А для розвідувальних операцій й управління військами держав та коаліцій – радіозасобів, засобів радіолокації, радіорозвідки, дезінформації, електромеханічних та електронних пристроїв для криптографічного захисту інформації та криптоаналізу (прообраз сучасних комп'ютерів). Виникли та отримали

розвиток нові напрямки науки: теорія зв'язку та інформації, криптологія, кібернетика.

Для боротьби з засобами військово-повітряного, а далі і ракетно-ядерного нападу, які набули стратегічного значення, формується протиповітряна оборона держав, як окремий вид збройних сил, або складова частина ВПС (в деяких державах), компоненти ППО інших видів збройних сил, а далі і війська ракетно-космічної оборони (РКО) з компонентами попередження про ракетний напад та протиракетної оборони, контролю космічного простору та протикосмічної оборони з відповідними командуваннями, системами управління військами і зброєю та забезпечення їх бойового функціонування системами з високим рівнем автоматизації. В них вперше в збройних силах комплексно впроваджуються складні системи автоматизації (автоматизовані системи управління - АСУ), технічні (електронні) системи і комплекси розвідки, наземного, повітряного та космічного базування, об'єднані в єдину систему, системи передачі даних та обміну інформацією, кіберінформаційні (кібернетичні) системи та системи підтримки прийняття рішень. Утворюються та розвиваються стратегічні ядерні сили, у вигляді ядерної тріади з відповідними командуваннями, системами управління та забезпечення бойового функціонування. Ступень автоматизації та інтеграції автоматизованих систем управління ядерними силами РВСП, ВПС, ВМС, РКО на наступному III етапі буде досягнута рівня майже 100%.

III етап: кінець 60-их середина 90-тих років XX сторіччя. Стрімкий розвиток електроніки, комп'ютеризація, інтеграція систем управління до моделей C2 та C3I (Comand, Control, Comunication, Intelegence), виконання космічних програм призвели до:

появи космічних систем суто воєнного призначення та застосування їх з метою моніторингу земної поверхні, ведення розвідки, телекомунікації, геоінформаційного та навігаційного забезпечення, управління високоточною зброєю;

формування концепції мережецентричних війн (дій), проксі та "заколот" війн, так званих 4GW війн (за західною класифікацією, 1989 рік);

визнання можливості застосування інформаційної, психологічної та когнітивної зброї.

Особливістю цього етапу стало масове використання реалізованих передових військових технологій для забезпечення потреб суспільства. Як приклад, можна привести Інтернет, мобільний зв'язок, космічні та інформаційні технології. В свою чергу, це підвищило можливості розвідки (OSINT) за рахунок багатократного збільшення відкритих джерел та засобів їх аналізу.

Космос де-факто визнано четвертою сферою ведення бойових дій, хоча міжнародна правова заборона на мілітаризацію космосу продовжує діяти. В окремих державах (США, колишньому СРСР), вже де-юре формуються та розвиваються військово-космічні сили з відповідними командуваннями, системами управління та забезпечення бойового функціонування з повною інтеграцією їх систем управління. В інших державах світу, наприклад КНР, це відбулося пізніше, умовно на IV етапі.

IV етап: Кінець XX сторіччя. Потужності і можливості кіберінформаційних (кібер-) систем стрімко зросли, відбувся якісний стрибок у швидкодії і продуктивності електронних засобів та обсягів інформації, що обробляється, зберігається та передається. Що, одночасно створило безліч нових вразливостей в системах управління (в тому числі і в оборонній сфері), тобто, кібервразливостей, і дозволило практично розглядати перехід до принципу функціонального ураження, як безпекової і оборонної складових держави так і їх окремих елементів. В той же час, технічні засоби отримання (розвідки), обробки та передачі інформації, управління і наведення засобів впливу, забезпечили ефективне застосування сил та засобів збройної боротьби відповідно до задачі не лише на стратегічному та оперативному рівнях, але й на тактичному [9].

Можливості таких систем, в наслідок посилення науково-технічних, виробничо-технологічних та фінансових спроможностей держав дозволяють створювати бойові підрозділи нового типу, які призначені для нанесення ураження противнику не лише в кінетичний (вогневого ураження) спосіб, але й в енергетичний (електронний) та інформаційно-когнитивний та широкого застосування, в тому числі групового і комплексного, робототехнічних засобів повітряного, наземного та морського (надводного і підводного) базування.

Проникнення інформаційних технологій в усі сфери життя людини та суспільства дозволило розглядати інформаційну зброю, як зброю першого удару. Згідно концепції Уордена-Бойда (John Ashley Warden III, John Boyd) в "операціях на основі ефектів" (EBO – Effect-based-Operations), що ставили за мету системні порушення управління та функціонування держав противника до кризового рівня (рис.2), в якості цілей для ураження або взяття під контроль стали розглядатися не лише збройні сили, їх системи управління, інфраструктура та комунікації, але й об'єкти економіки, населення і керівництво держав протиборчої сторони (рис.1) [10,11]. Формується функціональна модель бойового управління силами та засобами, що мають нові бойові спроможності. Це обумовило необхідність захисту вищезазначених об'єктів (рис.1) на новому рівні, складність та масштабність завдань якого дозволить розпочати його виконання лише на наступному **V** етапі.

V етап. Початок XXI сторіччя. Нове неймовірно стрімке зростання у розвитку можливостей IT-технологій в цілому та особливо кіберсистем щодо обробки великих обсягів даних

та швидкодії, глобальна комп'ютерізація всіх областей існування та функціонування людини та суспільства призвели до створення інтернету речей (IoT), теле та кібермедицини, а у воєнній сфері високо інтегрованих мережецентрічних систем управління воєнними діями (Network-centric Warfare, NCW), або C5ISR (Command, Control, Communication, Computers, Combat System, Intelligence, Surveillance, Reconnaissance) [12,13], кіберзброї, когнітивної та консцієнтальної (руйнуючої свідомість) зброї.

Відбулося визнання кіберпростору п'ятою сферою ведення бойових дій [14,15].

У більш ніж 60 країнах світу формуються кібервійська (кіберсили) з відповідними командуваннями, системами управління та забезпечення бойового функціонування. Базою та технічною основою цих систем є безпосередньо кіберсистеми. Сфера їх бойового застосування – кіберпростір. Подальший розвиток кіберсистем пов'язаний із технологіями збору і обробки великих масивів даних та обміну ними, IoT, глобальною роботизацією та штучним інтелектом.

Суттєво розширюється комплексне застосування різноманітної кіберзброї проти кіберфізичних та інших вразливих до неї систем, сферою діяльності яких є кіберпростір, поєднаний з іншими чотирма природними фізичними просторами.

Кіберфізична система (КФС – Cyber Physical system, CPS) – система, яка інтегрує обчислювальні, комунікаційні та керуючі технології для регулювання діяльності фізичних об'єктів під контролем фізичних осіб. До КФС відносять, наприклад, системи управління різного призначення, зокрема енергетикою, транспортом, робототехнічні системи, самокеровані літальні апарати, безпілотні автомобільні системи, бойові кораблі та підводні човни, Інтернет речей тощо [16].

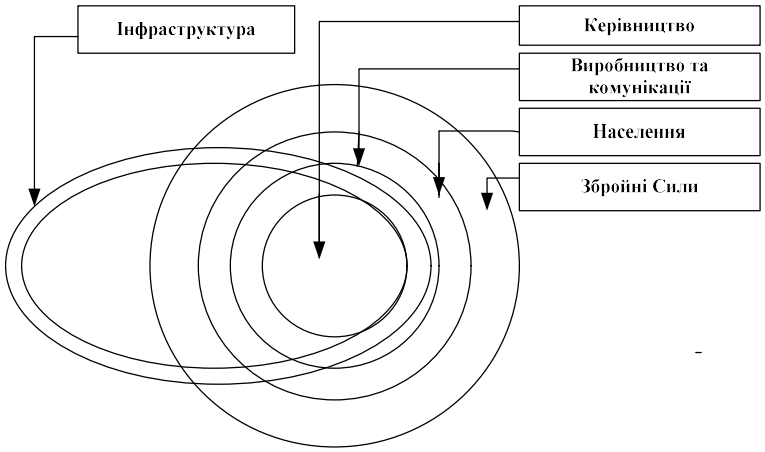

Рис. 2. Модифіковані кільця Уордена (Цілі ЕВО – атак)

Нездатність захистити ці системи від деструктивних впливів, зокрема кібератак, може мати катастрофічні наслідки [17,18]. З метою підвищення рівня захищеності своїх кіберфізичних систем, а також збільшення рівня ефективності впливу на кіберфізичні системи противника, провідні країни світу створюють науково-дослідні установи, як то Лабораторія кіберфізичних систем Академії ВМС США [19].

Особливістю кібероборони є необхідність захисту кіберсистем об'єктів критичної інфраструктури свого сектору національної безпеки та оборони, військового управління, комплексів озброєння та військової техніки, а також досягнення необхідних спроможностей деструктивного впливу на кіберфізичні та кіберсистеми противника (порушення функціонування, взяття під свій контроль та управління, фізичне знищення тощо). Особливого значення в цьому контексті набувають питання застосування робототехнічних комплексів. Можливість порушення функціонування кіберсистем робототехнічних комплексів (РТК) потребує розвитку засобів і способів їх надійного захисту від подібних впливів, а також засобів і способів моніторингу та впливу на РТК противника та боротьби з ними шляхом некінетичного (ЕМ, енергетичного, програмного тощо) впливу на Hard and Soft Wear їх кіберсистем.

Нижченаведені приклади свідчать про об'єктивність, перспективність та незворотність зазначеного.

У кінці березня 2020 р. Космічні сили США прийняли на озброєння систему спостереження за супутниками Space Fence («Космічний паркан»). Для боротьби з ворожими безпілотниками США розміщують на закордонних базах лазерні системи боротьби з БПЛА HELWS (High-Energy Laser Weapon System) з багато спектральними системами наведення, електромагнітні системи THOR та імпульсні системи PHASER. HELWS може робити кілька десятків пострілів на одному заряді та відрізняється підвищеною точністю. PHASER здатна виводити з ладу дрони за одну мікросекунду та дозволяє атакувати кілька цілей одночасно. Завдання електромагнітної системи THOR — знищення груп безпілотників. Системи

пройдуть випробування в бойових умовах на базах в Іраку і Сирії, після чого будуть розміщені на базах у США [19].

В США ведуться роботи над створенням технології виробництва великих безпілотників-носіїв, які зможуть запускати групу невеликих розвідувальних або бойових дронів. У 2017 р. успішно відбулися випробування прообразу такої системи, в ході яких з літака-носія F-18 було випущено рій зі 103 нано-дронів "Perdix" [35, 36]. В цьому ж році, на фестивалі в Гуанчжоу Китайська компанія "Ehang" продемонструвала управління з одного пульту роєм з 1000 дронів та виконання ним 6 різних тактичних завдань [19].

Для підвищення бойової ефективності піхотних підрозділів на тактичному рівні Збройні сили Великої Британії формують роботизовані взводи. На озброєнні взводу перебувають чотири вантажні роботизовані машини Mission Master-Cargo, які можуть бути як вантажними, так і бойовими й легко адаптуються під різні завдання (захист, розвідка, спостереження, вогнева підтримка, медична евакуація, зв'язок) [19].

Міністерство оборони Франції для потреб сухопутних військ закуповує багатоцільові мікророботи NERVA, які мають три модифікації. Вони здатні в будь-яких умовах вести розвідку та приховане стеження в автономному режимі, а також можуть бути використані для розмінування. Керуються за допомогою будь-якого стандартного комп'ютера, планшета чи смартфона [19].

У 2014 р. Управління військово-морських досліджень США продемонструвало можливість супроводження бойового корабля невеличким роєм безпілотних човнів. А вже у 2019 р. Військово-морський флот США замовив чотири роботизованих кораблі. В Корпусі морської піхоти будуть розформовані ряд частин авіації та вертолітних ескадрилій, зняті з озброєння танки M1 "Abrams " та більшість ствольної артилерії. Натомість на озброєння надійдуть робототехнічні засоби і реактивні системи залпового вогню [19].

Поява результатів фундаментальних та прикладних досліджень у галузях нанотехнологій, насамперед матеріалознавства, прогнозує закінчення дієвості закону Мура (Moore's law) щодо експоненціального зростання обсягів виробництва та якісних змін електронних пристроїв й систем внаслідок розвитку технологій та здешевлення виробництва. Цей емпіричний закон був сформульований Гордоном Муром (Moore, Gordon) ще у 1965 р., та їм же ж, виходячи з атомарної природи речовин та постійної величини швидкості світла у вакуумі, у 2003-2007 р.р. спростований та уточнений [20-22]. У 2016 р. дослідники Массачусетського технологічного інституту (Massachusetts Institute of Technology), під керівництвом Джеффрі Біча (Beach, Geoffrey), зробили відкриття щодо існування скірміонів (skyrmions) [23], віртуальних часток, електромагнітні властивості яких, дозволили створити та призведуть до масового використання в найближчому майбутньому квантових комп'ютерів, роботизованих систем нового покоління, подальшого розвитку штучного інтелекту та постквантової криптографії. Це вже впливає та й надалі все більше буде впливати на формування політики держав у сферах кібербезпеки та кібероборони.

Основними світовими трендами розвитку інформаційних, електронних та кібер- технологій, що безпосередньо здійснюють вплив на розвиток суспільства, суспільно-політичних та суспільно-економічних відносин, можуть бути наступні:

лавиноподібне зростання кількості інформації, що обробляється, зберігається і передається;

зміна форм представлення інформації, необхідної для прийняття управлінських рішень;

ускладнення систем управління та нелінійних зв'язків і процесуальної взаємодії між складовими різнорідних процесів управління та задіяних елементів.

Сучасні високі технології змінюють процеси організації бойових дій (операцій) та методи управління ними, і тому вимагають розробки та впровадження нових концепцій та стратегій оборони, розвитку існуючих та розробки нових, які враховують досягнення інноваційних технологій, форм, способів, методів і технологій збройної боротьби в сучасних і особливо перспективних умовах, а також підготовки та перепідготовки фахівців сектору безпеки та оборони, здатних їх впроваджувати та ефективно використовувати. У сфері оборони відбувається глобальний перехід на інтегровані системи управління військами та зброєю від стратегічного до тактичного рівня, та інноваційні системи озброєння, які до 80% побудовані з високотехнологічних складових [7,24].

Це швидко веде до набуття передовими арміями світу можливості ведення мережевих війн, в тому числі на тактичному рівні. В США реалізують нову версію платформи NCW у версії C6ISR, до якої додається ще одна компонента – Cyber [25]. Для ведення кібердій платформа NCW може бути розгорнута до моделі C5IEWS&IM (Command, Control, Communications, Computers, Cyber, Intelligence, Electronic Warfare, Sensors and Information Management) [7, 26].

З іншого боку інноваційний розвиток інформаційних та кібер- технологій та їх доступність у рази посилює можливість ведення не лише військовими або розвідувальними службами, але й незаконними формуваннями, злочинними та терористичними організаціями шпигунських й терористичних дій через інформаційний та кібер-простори та безпосередньо в них. Кібератаки стали більш організованими та руйнівними для державних установ, підприємств, економіки, транспорту, електроенергетики, об'єктів критичної інфраструктури. Вони можуть досягти критичного рівня, який загрожує національному і євроатлантичному процвітанню, безпеці і стабільності [6,18,27]. Нові вразливості

національної критичної інфраструктури, які проявляються паралельно з бурхливим розвитком технологій, породжують нові небезпеки, загрози й ризики в інформаційному та кібер- просторах та вимагають вирішення питань щодо їх запобігання, стримування та нейтралізації. Це питання існування і майбутнього держав у сучасному світі, що перебуває напередодні нового етапу розвитку суспільства – постінформаційного.

Виходячи з цього, у держав виникає необхідність утворення ефективної системи кібербезпеки та кібероборони з функціональною спроможністю не нижче гранично необхідного рівня, не залежно від рівня їх економічного розвитку і стану та науково-технічного прогресу країни, але адекватно до рівня загроз, що притаманні світові у першій чверті XXI століття, а у стратегічній перспективі – до середини століття [6,28].

Аналіз теорії, практики й досвіду побудови систем і забезпечення кібербезпеки та кібероборони провідних країн світу свідчить про їх адекватність загрозам, як відомим так і прогнозованим. Кіберсили розглядаються в якості сил стримування. Державне та військове керівництво армій розвинених країн світу у відповідності до нових підходів щодо будівництва збройних сил особливу увагу приділяє формуванню та розвитку систем кібербезпеки та кібероборони, як головного фактору у досягненні воєнно-стратегічної переваги в забезпеченні національної безпеки і оборони у сучасних умовах та у перспективі.

Концепція колективної оборони НАТО передбачає розвиток та застосування всіх політичних та військових можливостей щодо запобігання, виявлення, захисту і відновлення порушень внаслідок кібератак. Йде вдосконалення процесу планування НАТО та формування Кіберкомандування Альянсу, завданням якого будуть: охоплення усіх органів НАТО централізованим кіберзахистом; вдосконалення та координація національних можливостей з кіберзахисту; інтеграція національних систем в єдину систему попередження і реагування НАТО на кіберзагрози. Це стосується також країн - партнерів [14].

Світовий досвід свідчить, що ефективне вирішення будь-якими військами задач за призначенням та забезпечення максимально повного використання потенціалу озброєння та військової техніки можливе лише за умов їх об'єднання у єдиній військово-організаційній структурі (відповідно до фізичного простору де вони діють, або озброєння, яке вони застосовують) та наявності раціональної системи управління на усіх рівнях від стратегічного до тактичного. Як приклад – на початку XX століття масова поява авіації, танків та засобів протиповітряної оборони гостро поставила питання щодо створення відповідних органів управління підрозділами, з'єднаннями, об'єднаннями, оснащеними цими засобами, а також їх підготовки і всебічного забезпечення. Відомо, що до того, доки не були створені раціональні системи управління, ефективність застосування зазначених сил та засобів була вкрай низькою.

Кіберсили створюються й розвиваються в залежності від розвитку сучасної науки та технологій під впливом процесу розвитку і трансформації кіберпростору, який на відміну від природних просторів (сухопутного, морського, повітряного, космічного) не є незмінним у своїй фізичній суті. Це відбувається за рахунок поєднання в єдиній структурі, яка відповідає за кібероборону, всіх необхідних складових, відповідно до мети, завдань, доцільних форм та способів їх застосування для забезпечення кібербезпеки у воєнній сфері та реалізації різних функцій та напрямів діяльності поєднаних їх відношенням до кіберпростору. Створені в провідних країнах світу системи кібероборони включають та об'єднують військово-організаційні структури, які відповідають за: дії в комп'ютерних мережах, електромагнітному спектрі випромінювання, інформаційні та психологічні операції, організацію та застосування технічних видів розвідки, забезпечують зв'язок та криптографічний захист інформації, приймають участь у заходах введення в оману, здійснюють наукові дослідження і випробування в цих сферах та підготовку кадрів. (Рис. 3) [6,7].

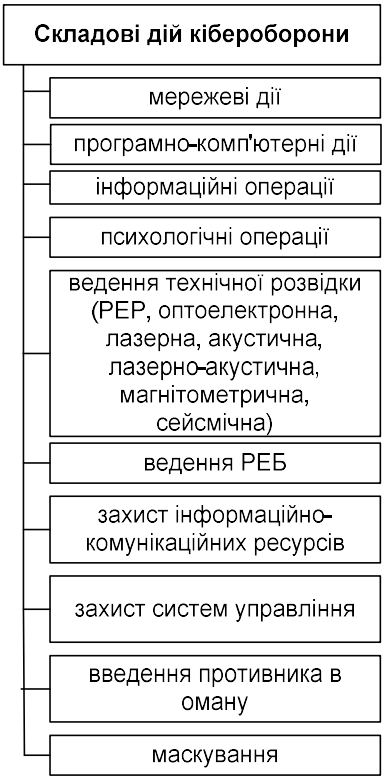

Рис. 3. Складові дій кібероборони

США. Система кібербезпеки США є трирівневою та ґрунтується на функціональній взаємодії державних інституцій та суб'єктів

національної економіки та приватно-державному партнерстві.

Перший, стратегічний рівень, включає:

Міністерство оборони, з підпорядкованим йому Агентством Національної Безпеки (АНБ – National Security Agency, NSA). Останнє виконує завдання в інтересах оборони, відповідає за збір та аналіз розвідувальної інформації та за захист інформаційних систем і комп'ютерних мереж, налічує близько 120000 співробітників та має річний бюджет за різними оцінками $3,5 – 13 млрд. [19];

Міністерство внутрішньої безпеки, до складу якого входить Національне управління кібербезпеки США з річним бюджетом $400 млн., виконує завдання із захисту національної критичної інфраструктури;

Міністерство юстиції, до складу якого входить ФБР, що займається розслідуванням кіберзлочинів в США.

На другому рівні, серед інших інституцій, Кіберкомандування США (United States Cyber Command – USCYBERCOM) та розвідувальне співтовариство.

На третьому – регіональні та локальні підрозділи кіберзахисту.

З 2018 р. в Законом про національну оборону (“National Defense Authorization Act”) для міністерства оборони США визначено завдання централізації керівництва всіма силами та засобами, які відповідають за кіберзахист, активні заходи дій в кіберпросторі та інші операції в комп’ютерних мережах, електромагнітному спектрі випромінювання, інформаційні та психологічні операції, дії в космічному просторі, дії відповідних технічних видів розвідки тощо. З 2019 р. кібербезпека (безпека кіберпростору) у США розглядається як дії, вжиті в захищеному кіберпросторі для запобігання несанкціонованому доступу, експлуатації або пошкодженню комп’ютерів, електронних систем зв'язку та інших інформаційних технологій, включаючи інформаційні технологічні платформи, а також інформацію, що міститься у них [29].

Кіберстратегія МО США визначає наступні пріоритети: підготовка простору операцій; висока готовність; ресурсне забезпечення; підготовка; партнерство. Кібервійська повинні бути спроможними контролювати ескалацію конфліктів і впливати на розвиток подій на всіх етапах конфліктів. Їх фінансування складає до $7 млрд. на рік. [19, 30, 31].

США з 2009 р. для захисту від кіберзагроз військової інфраструктури, реалізації програм та засобів, що спроможні контролювати ескалацію конфліктів та впливати на розвиток подій на всіх етапах конфліктів, першими у світі почали формування сил кібероборони, як окремого виду збройних сил [32,33]. Кіберкомандування США було утворено на базі та фондах АНБ й управління інформаційної безпеки Повітряних Сил (Air Forc Information Security Agency), шляхом об’єднання сил і засобів (підрозділів) за ознакою їх віднесення до кіберпростору (електромагнітного спектру), перепрофілювання або створення установ (підрозділів) науки та підготовки персоналу, створення системи кіберрозвідки з підсистемою управління, силами та засобами. У 2015 р. його повноваження були значно розширені Кіберстратегією 2.0, яка з метою підвищення рівня кіберзахисту та кібероборони США передбачала створення кіберсил, підпорядкованих окремому командуванню [34]. На сьогодні Кіберкомандування та АНБ одночасно очолює одна особа. З 2018 р. Кіберкомандування виведено з підпорядкування Стратегічного командування (STRATCOM) в самостійне бойове командування з наступним його відділенням від АНБ.

Причина майбутнього розділення полягає в тому, що відповідно до законодавства США, АНБ, як розвідувальний орган спеціального призначення, має право проводити за межами держави лише розвідувальні операції, право ведення бойових (воєнних) дій, в тому числі поза межами США – належить тільки військовим. Для забезпечення автономності ведення бойових дій проводяться заходи щодо створення спеціального Розвідувального центру кібероперацій (Cyber Warfare Intelligence Center) [19, 35,36].

Станом на кінець 2019 р. в підпорядкуванні Кіберкомандування **США** перебувають та виконують завдання кібероборони органи управління та військові підрозділи трьох видів Збройних Сил та одного роду військ, що налічують майже **50000** військовослужбовців та працівників **(**2,5% від загальної чисельності ЗС США). Діяльність Кіберкомандування США забезпечується потужною освітньо-науковою базою. Дослідження з питань кібербезпеки та кібероборони та підготовка персоналу здійснюються в 5 науково-дослідних установах та 2 навчально-тренувальних центрах [19].

Кіберкомандування Армії США (Army Cyber Units), або Командування 2 Армії – **19000** осіб. Йому підпорядковані військово-організаційні структури із завданнями:

1) Командування технологічних мереж Армії США (United States Army Network Enterprise Technology Command - NETCOM), або 9 командування зв’язку Армії США (командувань зв’язку територіальних – 3, бригад зв’язку територіальних - 7; бригада кіберзахисту) – веде глобальні операції в кіберпросторі та здійснює активну кібероборону від дій противника. Розгортає Центр управління інформаційних операцій Армії (AIOC), який забезпечує єдину оперативну підтримку планування інформаційних операцій Армії, розвідувальний аналіз та технічну допомогу розгорнутим командам інформаційних операцій (Information Operations Command, IO CMD), іншим військово-організаційним структурам, установам та відомствам, які потребують підтримки. Жодна інша структура

Армії не здійснює подібних завдань в кібер-інформаційному середовищі.

2) 1-ше Командування інформаційних операцій (1st Information Operations Command (Land) - 1st IO CMD) (штаб, штабні елементи, бригада військової розвідки (кібер) – 1, бригада кіберзахсту – 1, 1-й та 2-й окремі батальйони) – здійснює спеціальну підготовку фахівців та підрозділів кібербезпеки, розгортає різноманітні команди для виконання визначених завдань при підготовці та проведення інформаційних операцій та операцій у кіберпросторі, зокрема:

команди польової підтримки інформаційних операцій (IO Field Support Teams – FST), які забезпечують узгодження та досягнення максимальної ефективності завдань інформаційних операцій та операцій в кіберпросторі при плануванні та проведенні операцій угрупованнями Армії або спільними угрупованнями;

команди оцінки вразливості (IO Vulnerability Assessment Teams – VAT), які допомагають підрозділам визначати уразливості військ та систем від впливу противника в повному спектрі інформаційних операцій та надають командуванню пропозиції щодо покращення захисту включно операційну безпеку (OPSEC), фізичну безпеку, соціальну інженерію, безпеку радіозв'язку і захищених телефонного зв'язку та електронної пошти (COMSEC), а також безпеки операції у кіберпросторі;

елемент підтримки операційної безпеки (Operations Security Support Element - OSSE), якій здійснює підготовку керівників програм та посадових осіб до управління підрозділами системи підтримки операційної безпеки, надає допомогу керівництву та командирам підрозділів системи з усіх напрямків діяльності, несе відповідальність за планування, навчання, проведення оцінок та інтеграцію системи підтримки операційної безпеки в усій Армії;

навчально-тренувальні імітаційні центри інформаційних та кібер- операцій (Information Warfare/Cyber Opposing Force – IW/Cyber OPFOR) - призначені для забезпечення імітації реалістичних, реальних, віртуальних рутинних та деструктивних масованих дій кіберсил збройних сил інших держав, насильницьких екстремістських та кримінальних кібератак та кібервпливів під час навчань й тренувань підрозділів кібербезпеки в пунктах постійної дислокації, центрах бойової підготовки та під час командно-штабних навчань;

3) Центр управління інформаційних операцій Армії (The Army Information Operations Center – AIOC) – забезпечує єдину оперативну підтримку планування інформаційних операцій Армії, розвідувальний аналіз та технічну допомогу розгорнутим командам IO CMD та іншим військовим частинам, підрозділам, установам та відомствам, які вимагають підтримки. Жодна інша організація в Армії не надає цього критичного, унікального способу, орієнтованого на інформаційне середовище.

4) система навчальних курсів інформаційних операцій (Specialized IO training – SIOT) – курси у Форт Бельвоар, штат Вірджинія, і мобільні навчальні команди (MTT) по всьому світу. Кожен з курсів фокусується на інтеграції інформаційних можливостей (IRCs). Навчальні курси включають: Навчальний курс IO, програми та планування (IOCAP); Фундаментальний курс інформаційних операцій (IOFC); Військовий курс підготовки планувальників введення противника в оману (MDPC); Інтегрований курс радіоелектронної боротьби (EWIC); та курс інтеграції операцій з військової інформаційної підтримки (MISOIC);

підрозділи підготовки (Mission Readiness Exercise - MRX) активної та резервної компоненти команд системи польової підтримки інформаційних операцій (IO FST), зокрема:

1 батальйон 1-го Командування IO відповідає за підготовку активної та резервної компонент бойових команд та розгортання декількох глобальних експедиційних інформаційних операцій (IO), синхронізацію інформаційних можливостей для підтримки Армії, спільних оперативних сил і окремих бойових підрозділів й команд. Він здійснює аналіз соціальних мереж та планування залучення їх можливостей для потреб Армії та об'єднаних сил, використовуючи загальнодоступну інформацію забезпечує операційну безпеку розгорнутого угруповання;

2-й батальйон 1-го Командування IO розгортає багатофункціональні команди інформаційних операцій (IO) у всьому світі, зберігаючи при цьому безпосередній і віддалений доступ до мережі та використовуючи всі можливості IO для підвищення готовності та здатності військових сил США щодо дій в інформаційному середовищі [19].

Кіберкомандування Повітряних Сил США (Air Forces Cyber), або 24 Повітряна Армія – понад 14000 військовослужбовців та працівників, що розміщені на 6 авіабазах в США та ФРН, здійснює кіберзахист мереж управління ПС, забезпечує підтримку бойових операцій ПС, приймає участь в об'єднаних (спільних) кіберопераціях. Складається з 11 органів управління (Центра операцій – 1, оперативної групи дій в кіберпросторі – 1, бойових груп мережевих операцій – 2, груп бойових комунікацій – 2, групи операцій у кіберпросторі – 1, інженерної групи забезпечення кіберпростору – 1, крила інформаційних операцій в комп'ютерних мережах – 1, крила бойового застосування кіберсистем – 1, крила зв'язку (бойових комунікацій) – 1) та 36 ескадрилей (мережевих операцій – 10, бойового зв'язку - 10, операцій в кіберпросторі – 2, інформаційних операцій – 2, розвідувальної підтримки – 1, оперативної підтримки – 1, підтримки операцій – 1, операційної підтримки - 2, підтримки бойового зв'язку – 2, інженерних – 2, підрядників – 1, випробувальної – 1, підготовки до дій в

кіберпросторі – 1), назви яких відображають сутність їх завдань [19].

Кіберкомандування ВМС (U.S. Fleet Cyber), або 10 Флот США – понад 16000 військовослужбовців і працівників дійсної служби та резерву, організованих у 27 активних та 27 резервних командувань, розміщених на 11 військово-морських базах (аеродромах) США, що формують 40 кіберкоманд, діючих по всьому світу (зокрема, Бахрейн – 2, Італія - 2, Японія – 3, Маріанські острови, Великобританія – по одній). Здійснює кіберзахист мереж управління ВМС, забезпечує підтримку бойових операцій ВМС, приймає участь в об'єднаних (спільних) кібероперація̈х. Складається з:

Командування комп'ютерних мереж ВМС (Naval Network Warfare Command – NNWC) - 1, тактичних кібергруп (Cyber tactic group, CTG) – 3;

Командування кіберзахисту ВМС (Navy Cyber Defense Operations Command – NCDOC) - 1, CTG – 2**;**

Командування інформаційних операцій ВМС на ТВД (Navy Information Operations Command, NIOC) – 5;

6-та бойова група криптологічного забезпечення (Cryptologic Warfare Group – CWG6) у складі: 61морський підрозділ криптологічних дій (Cryptologic Warfare Maritime Activity – CWMA); 63 підрозділ криптологічного забезпечення кібер-ударів (Cyber Strike Activity – CSA); 64 підрозділ криптографічного забезпечення кіберзахисту (Cyber Defense Activity – CDA). Група розгортає бойові підрозділи криптологічної підтримки операції по всьому світові – 10;

Група розробок інформаційних операцій, досліджень, розробок, випробувань та оцінок (Research and development).

Об'єднані спеціальні підрозділи (Joint Base San Antonio) [19].

Кіберкомандування Корпусу Морської Піхоти (U.S. Marine Corps Forces Cyberspace Command – MARFORCYBER) - біля 800 осіб особового складу, здійснює кіберзахист мереж управління МП, забезпечує підтримку бойових операцій МП, приймає участь в об'єднаних (спільних) кібероперація̈х. Складається з Командного центру комп'ютерної безпеки корпусу МП (Network Operations Security Center) та батальйону криптографічної служби (Marine Corps Cryptologic Support Battalion). Розгортає:

оперативну кібергрупу корпусу МП (The Marine Corps Cyber Operations Group), яка здійснює збір та аналіз розвідувальної інформації, необхідної для планування виконання завдань за призначенням, збір та обмін інформацією щодо стану інцидентів в мережах, керівництво захистом мереж, реагування на загрози, вразливості та інциденти, технічне керівництво та втілення нових технологій;

бойову кібергрупу корпусу МП (The Marine Corps Cyber Warfare Group) [19].

Завданням USCYBERCOM є планування, координація, об'єднання, синхронізація і проведення заходів щодо керівництва операціями і захисту комп'ютерних мереж міністерства оборони; підготовка і здійснення повного спектру військових операцій в кіберпросторі, забезпечення свободи дій США та їх союзників в кіберпросторі та перешкоджання аналогічних дій противника. Спектр операцій Кіберкомандування США показаний на рис. 4.

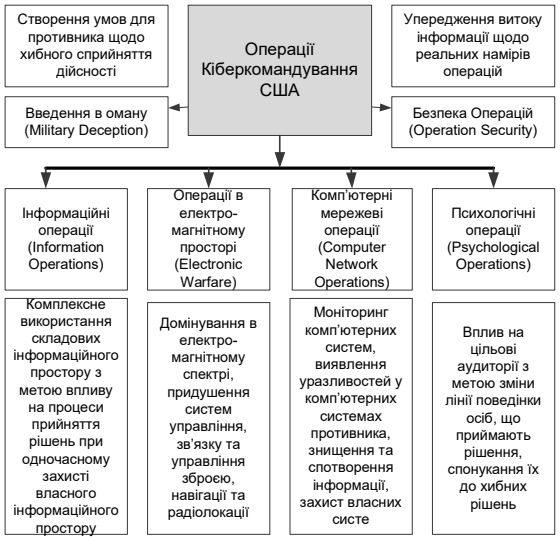

Рис. 4. Операції Кіберкомандування США.

У 2019 р. США провели ряд бойових кібероперацій, зокрема проти Ірану та Росії. [19]. Активні сили складаються з майже 6200 осіб військового й цивільного персоналу (включно персонал запасних компонентів), організованих в 133 бойові команди, які досягли оперативної спроможності та активно проводять операції [19], а саме:

команди національної місії (National Mission Teams) захисту США та критичної інфраструктури від кібератак – 13 (використовують цивільних фахівців);

команди захисту пріоритетних мереж та систем (Cyber Protection Teams) - 68;

команди створення інтегрованих ефектів кіберпростору (Combat Mission Teams) для підтримки оперативних планів, операцій та бойових дій на випадок непередбачених обставин – 27;

команди (Support Teams) аналітичної та планової підтримки команд національної місії та бойової місії – 25.

Таким чином, США мають раціональну систему управління та необхідні сили і засоби об'єднані в єдину структуру відповідно до цілей, завдань і функцій для ведення всіх видів кібердій в кіберпросторі та через кіберпростір.

ФРН. Командування кібер- та інформаційного простору (далі ККІП), створено у 2017 році, має статус окремого виду збройних сил (ЗС). Чисельність 13700 військовослужбовців і 1500 тисячі цивільних осіб (6% від загальної

чисельності ЗС ФРН). Повна операційна готовність ККІП буде досягнута до кінця 2021 року.

ККІП організаційно складається з двох командувань ланки дивізії, кожне з яких має у своєму розпорядженні близько десяти структурних підрозділів нижчого рівня, та Центру геоінформації. Перше – реорганізоване Командування сил розвідки (КСР) відповідає за ведення РЕР і РЕБ та здійснення інформаційного і радіоелектронного впливу на противника. Друге – Командування інформаційно-технічних засобів (реорганізоване командування управління та зв'язку) відповідає за утримання і функціонування системи бойового управління та зв'язку, а також за захист інформаційних мереж від кібернетичних атак противника. Центр геоінформації бундесверу призначений для забезпечення всіх користувачів актуальними даними широкого спектру, включно: матеріали фотограмметрії, дистанційного зондування Землі, геофізичні, геодезичні, гідрологічні, гідрографічні, океанографічні, метеорологічні,та картографічні матеріали тощо.

Створення ККІП здійснено за рахунок передачі в його розпорядження існуючих структурних підрозділів інших видів ЗС і не призвело до збільшення загальної чисельності Бундесверу. Зокрема, із Командування базових сил Бундесверу до складу ККІП передані у повному обсязі Командування стратегічної розвідки (близько 5500 осіб), Командування управління і зв'язку (понад 6000 осіб) та Центр інформаційно-психологічних операцій (близько 1000). Крім того, до складу ККІП включено частину підрозділів Федерального агентства озброєння, інформаційної техніки та експлуатації Бундесверу. Найменший підрозділ, якій відповідає за атаки, налічує лише 60 військовослужбовців. Структура ККІП ФРН показана на рис. 5.

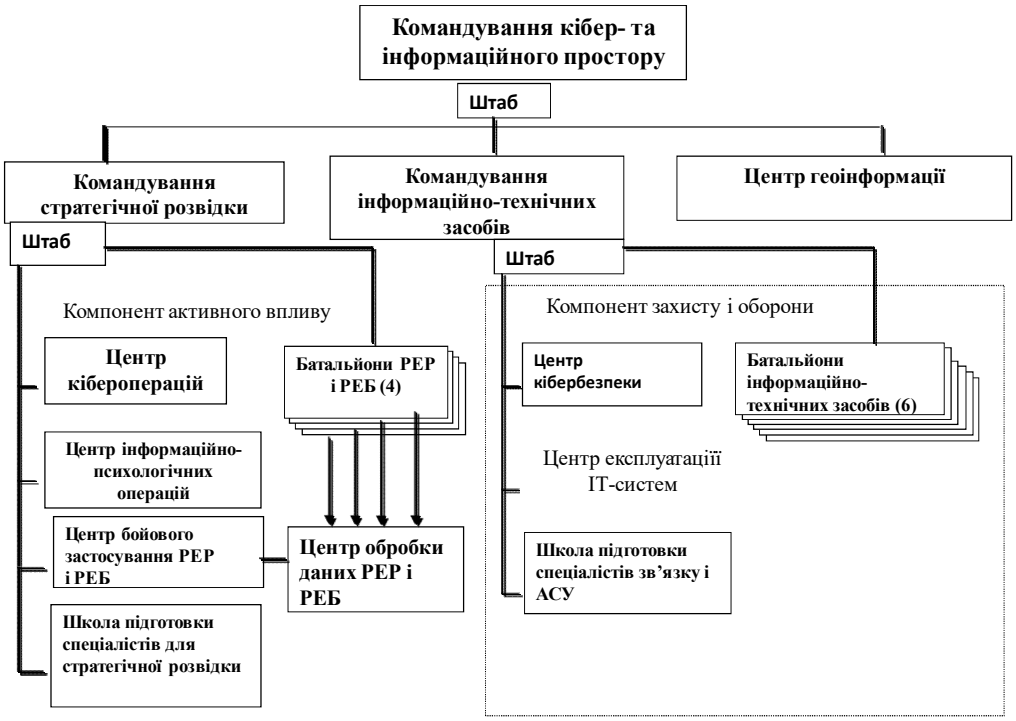

Рис. 5. Структура Командування кібер- та інформаційного простору ФРН

В університеті бундесверу в Мюнхені 11 кафедр пов'язані з обороною кіберпростору. Бюджет Дослідницького центру університету на 2019-2021 р.р. двадцять мільйонів євро [37].

Великобританія. Розгортання британських кібервійськ проходить згідно з ініціативи Міністерства оборони Великої Британії і Центру урядового зв'язку (GCHQ). Великобританія спланувала на розвиток кібербезпеки у 2016–2021 роках витрати у розмірі понад 3 мільярди фунтів. З них 22 млн. фунтів стерлінгів ($27,8 млн.) - на створення Центру активних кібероперацій, який буде спільно використовуватися МО та GCHQ й забезпечувати та посилювати діяльність 77-ої бригади кібероперацій. До 2021 року кібервійська нараховуватимуть 2000 осіб, а фінансування, становитиме понад 250 мільйонів фунтів на рік. Національний центр кібербезпеки Великої Британії щороку проводить найбільші у світі кібернавчання Locked Shields для експертів у сфері кіберзахисту [38].

Республіка Польща. Гарантоване безпечне функціонування в кіберпросторі визнано однією з основних стратегічних цілей безпеки держави. Військова контррозвідка (Sluzba Kontrwywiadu Wojskowego, SKW), яка підпорядкована Міністру національної оборони здійснює не тільки контррозвідувальні заходи, але й забезпечує кібербезпеку для Збройних Сил Республіки Польща. Військова розвідка (Sluzba wywiadu Wojskowego, SWW) здійснює в інтересах оборони електронну розвідку та криптоаналіз. Активно

здійснюються заходи правового, організаційного та технічного характеру щодо вдосконалення національної системи кібербезпеки та кібероборони, розробки нормативно-правової бази активної оборони в кіберпросторі.

На створення кіберсил Польща виділила 2 млрд. злотих (близько 465 млн євро). З 2019 р. розпочато формування Військ оборони кіберпростору, які у продовж кількох років мають нараховувати 1000 військовослужбовців. На основі Національного центру криптології (військово-організаційна структура підпорядкована Генеральному штабу) та Командування ІТ-мереж (структура МО) сформовано безпосередньо підпорядкований Міністерству Національної оборони РП Національний Центр кіберзахисту, до складу якого включений Інспекторат інформатики. Йому підпорядковані: Центр інформаційної підтримки Збройних Сил, Регіональні центри інформаційної підтримки – 4, до складу яких входять відділи кібербезпеки та захисту інформації; Центр інформаційної підтримки Повітряних Сил, райони інформаційної підтримки ПС – 4; Центр управління інформаційними мережами; Центр проектування інформаційних систем; група реагування інфраструктури – 4; військове бюро з регулювання й вимірювання радіочастот [39,40].

Угорщина створює у складі Збройних Сил Центр (Командування) кібербезпеки з підпорядкуванням йому існуючих підрозділів: Центру кібербезпеки Служби національної безпеки Угорщини, Головного центру кібербезпеки Будапештської гарнізонної бригади, Центру забезпечення захисту інформації та підтримки управління 43 полку зв'язку, а також створює для підготовки військових та цивільних фахівців силових структур країни Академію кіберзахисту, яка складається з 5 кафедр та 3 лабораторій. Центр кібербезпеки підпорядкований директорату технологій, кібер- та ІТ-захисту. В свою чергу, Директорат є військово-організаційною структурою, що входить до складу Воєнної служби національної безпеки. Чисельність Центру кібербезпеки може нараховувати до 1000 військовослужбовців [41,42].

Естонія відіграє провідну роль у зміцненні європейського кіберзахисту. З 2008 року у Таллінні діє Об'єднаний центр передових технологій з кібероборони НАТО (NATO Cooperative Cyber Defence Centre of Excellence), який сьогодні є флагманом європейської кібербезпеки. Центр має акредитацію НАТО. Центр налічує 20 учасників – 17 членів НАТО та 3 країни-партнери. Унікальність центру полягає в тому, що там разом працюють військові, цивільні, представники уряду. Робота центру сфокусована на трьох основних напрямках: дослідження, тренування та навчання. З 2018 р. Естонія розпочала формування кібервійськ, кількість яких складатиме 300 осіб. Набуття спроможностей визначено на 2023 р. [43].

РФ. Воєнна доктрина (2014) та Доктрина інформаційної безпеки (2016) визначають можливість застосування сил інформаційних операцій (дії в кіберпросторі не відокремлюються) в інформаційній війні з метою створення системи неядерного стримування та запобігання конфліктам, для оборони, а також з метою нападу. Основну частину активних дій покладено на "добровольців", "хактивістів" та інші "підконтрольні" умовно невійськові сили та засоби.

Війська інформаційних операцій МО РФ створені на підставі указу президента РФ у лютому 2014 року та налічують близько 1000 військовослужбовців, їх фінансування – на рівні 18 млрд руб. ($300 млн.). Кіберкомандування ГШ ЗС РФ створено у січні 2014 року на підставі наказу МО РФ. Його основними завданням є: управління та захист воєнних комп'ютерних мереж та систем управління і зв'язку від кібертероризму та дій імовірного противника [44]. Крім військових закладів вищої освіти, підготовка висококваліфікованого військового та науково-технічного персоналу для кібер командування та військ ІО здійснюється в наукових ротах, зокрема: 6 нр Восьмого управління ГШ ЗС РФ (м. Краснодар), 3 нр Військ повітряно-космічної оборони (м. Красногорськ), нр Військово-повітряної академії ім. Жуковського та Гагаріна (м. Воронеж). Особливістю останніх є те що до них відбираються найбільш талановиті випускники, або студенти останнього року навчання профільних цивільних закладів вищої освіти, які після призову, протягом 2 років проходять дійсну строкову військову службу та одночасно здійснюють наукову діяльність. З присвоєнням першого офіцерського звання, випускники наукових рот отримують призначення у військові або оборонні науково-дослідні установи, або в конструкторські бюро оборонного призначення [45].

Ізраїль. На виконання п'ятирічного Плану розвитку сил оборони Ізраїлю, прийнятого у 2015 році, якій передбачає активізацію діяльності щодо відбиття кібератак та інших асиметричних загроз від недержавних та терористичних організацій регіону, для захисту життєво важливих об'єктів інфраструктури Ізраїлю створена Національна цільова кібернетична група (НЦКГ) рівня дивізії, яка є відповідальною за кібероборону. НЦКГ була утворена шляхом об'єднання в єдину організаційну структуру Національного кібернетичного штабу, що існував з 2012 р. та Національного управління з кібернетики, що діяло з 2015 р. НЦКГ очолив колишній керівник Центру шифрування та захисту інформації, що забезпечує криптографічний захист мереж ЦАХАЛу, служби внутрішньої безпеки ШАБАК, розвідки МОССАД, а також національних корпорацій. Розглядається можливість розгортання в подальшому НЦКГ у

Кіберкорпус, який стане відповідальним за оборону країни, як і інші існуючи Армійській, Військово-морській та Військово-повітряний корпуси. У 2019 р. на це реформування було виділено $150 млн. У разі створення, Кіберкорпус має виконувати інтегровані функції електронної розвідки, протидії та захисту, які наразі виконуються органами військової розвідки трьох існуючих корпусів та командою 8200 військової розвідки, а також Управлінням командування, управління, зв'язку, інформаційних систем та розвідки (C4I) в частині, що стосується захисту від кібератак та криптографічного захисту інформації мереж воєнного призначення, а також мереж стратегічних військових концернів, таких як Ізраїльська електрична компанія, національна водна монополія "Мекорот" і телефонна компанія "Безек". Кібервійська будуть відповідати за забезпечення належного рівня оборони Ізраїлю та координацію розробок нового програмного забезпечення для Збройних Сил та ізраїльських компаній сектору високих технологій. Чисельність, яка планується – 1000 осіб [46].

Аналіз стану кібероборони в Україні. В Україні питання формування системи кібероборони знаходиться у стадії вирішення. Відповідно до чинного законодавства та окремих нормативно-правових актів підготовка держави до відбиття агресії у кіберпросторі (кібероборона) є одним із головних завдань, які покладаються на Міністерство оборони та Збройні Сили України. За виконання пов'язаних за змістом та простором завдань кібероборони на цей час відповідають різноманітні, різнопідпорядковані структурні підрозділи, що призводить до зростання витратності та зниження ефективності виконання цих задач. (рис. 5, 6) [47-54]. Щоб правильно визначити цілі і задачі стратегії кібероборони, необхідно спираючись на визначені функції та завдання, на основі структурно-системного підходу, здійснити чітку структуризацію та визначення зон відповідальності кожній складовій сектору безпеки і оборони стосовно кібербезпеки та кіберорборони.

"Індекс кібер-готовності 2.0", опублікований у 2015 р. Потомакським Інститутом політичних досліджень [36] рекомендує для оцінки дієвості системи кібероборони держави та здатності Національного органу кібероборони та Збройних Сил держави щодо захисту від загроз, що йдуть від кіберпростору, використовувати наступну модель перевірки, що складається з 7 груп:

1. Наявність національної стратегії кібербезпеки.
2. Наявність структур відповідальних за інциденти, здатність їх до реагування на них.
3. Наявність правоохоронної кібер-структури та стан правоохоронної практики
4. Наявність системи обміну інформацією.
5. Наявність системи підготовки персоналу, досліджень та випробовувань.
6. Дипломатія та торгівля.
7. Оборона та наявність структур, що реагують на кризові ситуації.

Країни, зацікавлені у функціонуванні дієвої системи кібероборони, здійснюють заходи щодо створення в рамках Збройних Сил профільних кіберкомандувань, та кібервійськ (сил) з підрозділами кібербезпеки та активної кібероборони, а також забезпечення високого рівня їх забезпеченості та готовності.

У разі невідповідності вимогам, плануються та виконуються заходи щодо утворення інституцій та систем, які б відповідали цим вимогам. Зокрема, в рамках 7-ї групи, мають бути здійснені заходи щодо:

утворення Національного органу у складі Збройних Сил, на який покладено основне завдання щодо кібероборони;

формування його політичних та функціональних повноважень та стратегій реагування на кіберзагрози;

оприлюднення в рамках національного законодавства його пріоритетів та повноважень щодо кібероборони, як на території суверенної держави, так й поза її межами.

Національним центральним органом виконавчої влади у сфері кібероборони, в окремих суверенних державах може бути також Національна поліція або органи безпеки, чи розвідки. Але, обов'язковою умовою також є відповідність сучасним вимогам та готовність Збройних Сил до дій в кіберпросторі у разі збройного конфлікту. Законодавство України [101 - 104] однозначно покладає це завдання на Міністерство оборони та Збройні Сили України.

Для забезпечення створення та функціонування цілісної системи кіберорборони (СКО) з урахуванням національних вимог [47-56] та рекомендацій провідних науково-дослідних центрів та країн-партнерів щодо уніфікації бойових командувань і процедур [36] необхідно здійснити низку взаємопов'язаних політичних, правових, організаційних, науково-технічних, безпосередньо військових та інших заходів спрямованих на формування такої системи кібербезпеки та кібероборони, яка забезпечить скоординоване управління всіма її складовими.

Така система потребує наявності відповідного єдиного органу управління, подібного за структурою, завданнями і функціями до аналогічних органів управління в цій сфері країн-членів НАТО, призначеного для реалізації єдиної політики та стратегії дій Міністерства оборони України та Збройних Сил України в інформаційному та кіберпросторі; організації та координації заходів щодо кібербезпеки та захисту критичної інформаційної інфраструктури держави; управління силами кібербезпеки та кібероборони під час кризових ситуацій, в умовах особливого періоду та правового режиму воєнного стану (рис. 6, 7) [6,7].

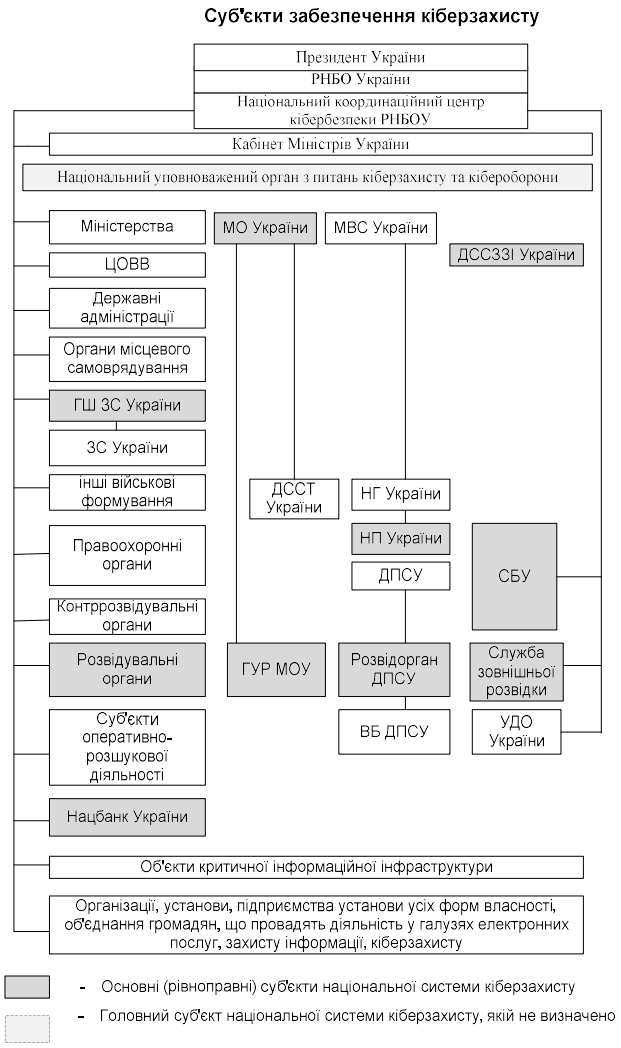

Рис.6. Суб’єкти забезпечення кіберзахтисту

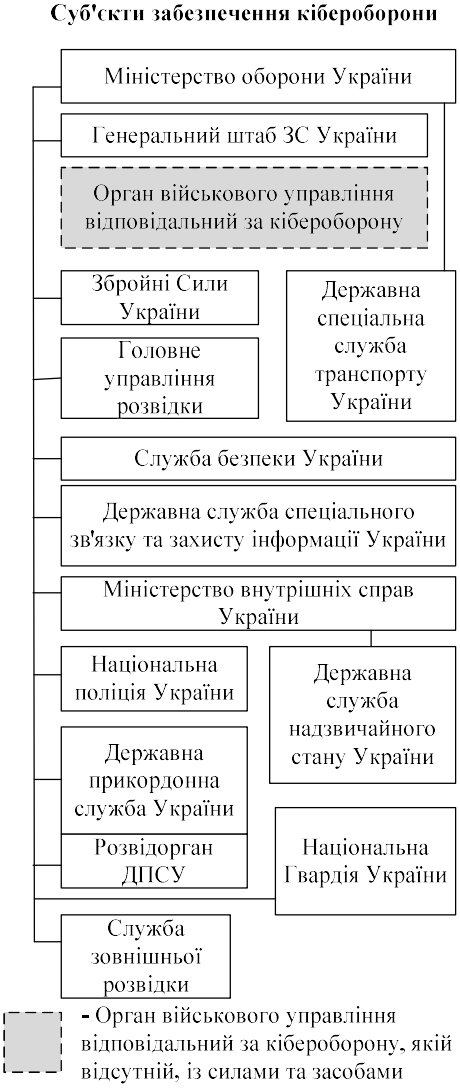

Рис.7. Суб’єкти забезпечення кібероборони

Висновки й перспективи подальших досліджень

На думку авторів, утворення та розгортання системи кібероборони держави доцільно здійснювати шляхом комплексного узгодження напрямів діяльності складових сектору безпеки та оборони, які задіяні в вирішенні питань кібербезпеки з чітким розподілом функцій за їх належністю до вирішення питань кібероборони. Далі, повинна бути здійснена інтеграція всіх сил та засобів, які на цей час вирішують питання, що мають відношення до кібероборони, за досвідом країн НАТО, в єдину структуру, подібну до кіберсил (кібервійськ) країн НАТО. Для них повинні бути чітко визначені цілі, функції і завдання, які вони повинні вирішувати в інтересах забезпечення кібероборони держави та здійснене відповідне кадрове, наукове і ресурсне забезпечення. Необхідно спланувати та провести заходи щодо утворення дієздатної національної системи кібероборони з урахуванням вимог законів та нормативно-правових актів України [47-49,51,52,54,55] та досвіду провідних країн світу, особливо країн-членів НАТО.

Створення, з урахуванням досвіду країн-членів НАТО та наявність ефективної системи управління силами і засобами які діють в кіберпросторі забезпечить їх найбільш раціональне функціонування та застосування, інформаційну і кібер перевагу над противником та буде сприяти практичній реалізації прийнятої в країнах членах НАТО концепції “смарт-оборони”, ключовими елементами якої є високотехнологічна підготовка персоналу та збалансоване поєднання найбільш ефективних аспектів стратегій “жорсткої сили” та “м’якої сили”, шляхом зваженого і узгодженого використання інструментарію стратегічних комунікацій, інформаційних та кібер-дій, санкцій, переконання і раціональне застосування сили та інших впливів способом, який є найбільш рентабельним та має політичну і соціальну легітимність

Література

1. В.Бурячок, Г.Гулак, В.Хорошко**,** Завдання, форми та способи ведення війн у кібернетичному просторі – К.: Наука і оборона №3 - 2011, с.35-42. **2.** Є.Живило О., О.Черноног**.** Стратегія кібероборони України – К.: ВІТІ № 4 – 2017, с. 30-37 3. В. Ліпкан, І. Діордіца. Національна система кібербезпеки як складова частина системи забезпечення національної безпеки України – К.: Підприємництво, господарство і право №5– 2017, с. 174-180. **4.** I.Gorbenko, A.Zamula, Ye.Semenko. Ensemble and correlation properties of cryptographic signals for telecommunication system and network applications - Kharkiv/ Telecommunications and Radio Engineering. – 2016. – Vol. 75. – Issue 2. – P. 169–178. **5.** І.Горбенко, О.Замула. Моделі та методи синтезу криптографічних сигналів та їх оптимізація за критерієм часової складності – Харків - Математичне та комп'ютерне моделювання. Серія: Фізико-математичні науки - 2017. Випуск 15. с.43-49 - [Електронний ресурс]. Режим доступу:http://nbuv.gov.ua/UJRN/Mtkm_fiz_mat_2017_15_10 **6.** Ю.Даник, С.Вдовенко. Проблеми та перспективи забезпечення кібероборони держави К.:ВІКНУ, випуск 66, 2020 - С. 56-72. **7.** Ю.Даник. Високотехнологічні аспекти забезпечення національної безпеки й оборони. К.: Военная связь. Телеком. Жовтень 2018. с. 58-69 **8.** Г. Лиддел. Стратегия непрямых действий — М.: ИЛ - 1957. **9.** DoD C4ISR Cooperative Research Program Assistant Secretary of Defense (C3I) Mr. Arthur L. Money Special Assistant to the ASD (C3I). [Електронний ресурс]. Режим доступу: http://dodccrp.org/files/Alberts NCW.pdf **10.** Warden, John A. III (September 1995), Chapter 4: Air theory for the 21st century, Battlefield of the Future: 21st Century Warfare Issues. **11.** Bryant D.J. Critique, Explore, Compare and Adapt (CECA): A New Model for Command Decisionmaking. Defence R&D Toronto Technical Report, DFDC, Toronto TR, 2003. 63 p. **12.** DoD C4ISR Cooperative Research Program Assistant Secretary of Defense (C3I) Mr. Arthur L. Money Special Assistant to the ASD(C3I). [Електронний ресурс]. Режим доступу http://dodccrp.org/files/Alberts_NCW.pdf **13.** Л.Поліщук, С.Богуцький М. Сучасні тенденції розвитку систем управління збройних сил провідних країн світу - ВІТІ - 2014, с.42-46 **14.** Warsaw Summit Communiqué. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016 09 Jul. 2016 – 2016, 100 **15.** Стратегія національної безпеки України, затверджена Указом Президента України від 26.05.2015 № 287/2015. **16.** S.Neema. Symbiotic Design for Cyber Physical Systems. Defense Advanced Research Projects Agency Program Information. [Електронний ресурс]. Режим доступу: https://www.darpa.mil/program/symbiotic-design-for-cyber-physical-systems. **17**. С.Вдовенко, Ю.Даник. Концептуальні напрямки комплексного вирішення проблеми захисту від несанкціонованого доступу в складних системах спеціального призначення. Вінниця, ВНПУ - 2017, с. 61 – 64. **18**. Ю.Даник, С.Вдовенко. Ланцюгові ефекти в кібердіях. Збірник наукових праць військового інституту Київського Національного університету імені Тараса Шевченка, випуск 64 - 2019 - С. 56-71. **19**. [Електронний ресурс]. Режим доступу: https://www.usna.edu/wrc/cpsl/index.php, https://thebabel.com.ua/news/41889-ssha-rozgortayut-protidronovi-lazerni-sistemi-na-zarubizhnih-bazah, https://defence-ua.com/index.php/statti/2245-vyprobuvannya-bpla-6-ho-pokolinnya-ssha-pokazaly-mistse-rosiyi, http://www.nanonewsnet.ru/news/2017/kitaitsy-obedinili-v-stayu-tysyachu-dronov**,** https://lb.ua/world/2015/11/17/321192_britaniya_sozdast_spetsialnie.html, http://www.lefigaro.fr/international/l-armee-se-dote-de-56-microrobots-de-reconnaissance**,** https://www.linkedin.com/company/national-security-agency?trk=similar-pages_result-card_full-click, https://www.cybercom.mil/About/Mission-and-Vision/ https://www.cybercom.mil/, https://www.cybercom.mil/About/Leadership/Bio-Display/Article/1512978/commander-uscybercom/, https://en.wikipedia.org/wiki/United_States_Cyber_Command, https://military.wikia.org/wiki/Second_United_States_Army https://www.globalsecurity.org/military/agency/usaf/afcyber htm, https://www.public.navy.mil/fcc-c10f/Pages/home.aspx, https://www.navy.mil/local/fccc10f/ https://www.armed-services.senate.gov/imo/media/doc/Gilday_05-23-17.pdf, https://www.candp.marines.mil/Organization/Operating-Forces/US-Marine-Corps-Forces-Cyberspace-Command/ https://www.epravda.com.ua/news/2018/10/23/641908/ https://www.rbc.ua/rus/news/ssha-proveli-kiberataku-iranskie-raketnye-1561260168.html https://lexinform.com.ua/v-sviti/ssha-pochaly-kiberoperatsiyu-proty-rosiyi/ https://www.arcyber.army.mil/, https://www.fifthdomain.com/dod/cybercom/2019/07/25/what-the-future-holds-for-cyber-command/ **20.** Moore, Gordon E. (1965). Cramming more components onto integrated circuits, Electronics Magazine. с. 4 [Електронний ресурс]. Режим доступу: https://newsroom.intel.com/wp-content/uploads/sites/11/2018/05/moores-law-electronics.pdf **21.** Moore, Gordon E. No Exponential is Forever: But "Forever" Can Be Delayed!, International Solid-State Circuits Conference 2003 / SESSION 1 / PLENARY / 1.1 -2003. [Електронний ресурс]. Режим доступу: https://ieeexplore.ieee.org/document/1234194 **22.** Kurzweil, Ray -2005. The Singularity Is Near. When Humans Transcend Biology. Penguin Books [Електронний ресурс]. Режим доступу: http://stargate.inf.elte.hu/~seci/fun/Kurzweil/ Ray_Singularity_Near_The_hardbac_ed_Bv1._D.pdf **23.** Recently discovered phenomenon could provide a way to bypass the limits to Moore's Law. [Електронний ресурс]. Режим доступу: https://phys.org/news/2017-10-phenomenon-bypass-limits-law.html **24.** В. Бегма**,** В. Шемаєв. Розвиток технологій у провідних країнах світу. Уроки для України. [Електронний ресурс]. Режим доступу: https://defence-ua.com/index.php/statti/publikatsiji-partneriv/8982-rozvytok-tekhnolohiy-u-providnykh-krayinakh-svitu-uroky-dlya-ukrayiny **25.** Network Centric Warfare Market by Platform (Land, Air, Naval, Unmanned), Application (ISR, Communication, Computer, Cyber, Combat, Control & Command), Mission Type, Communication Network, Architecture, and Region - Global Forecast to 2021. [Електронний ресурс]. Режим доступу: https://www.marketresearch.com/MarketsandMarkets-v3719/Network-Centric-Warfare-Platform-Land-10188278/ **26.** BMC4ISR means Battle Management/Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance. [Електронний ресурс]. Режим доступу: http://acronymsandslang.com/definition/24656/BMC4ISR-meaning.html **27.** Summit Meeting of NATO Heads of State and Government - Lisbon, Portugal, 19-20 Nov 2010. [Електронний ресурс]. Режим доступу: https://www.nato.int/cps/en/natolive/events_66529.htm **28.** С.Вдовенко, Ю.Даник, С.Фараон. Дефініційні проблеми термінології у сфері кібербезпеки і кібероборони та шляхи їх вирішення. – Харків: ХНУ ім. В.Н.Каразіна – 2019, №1(12). [Електронний ресурс]. Режим доступу: https://doi.org/10.26565/2519-2310-2019-1-02 **29.** DOD Dictionary of Military and Associated Terms As of January 2020. Електронний ресурс. Режим доступу: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdfhttps://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf **30.** DOD. Joint Publication 3-12, Cyberspace Operations, 8 June 2018/. Електронний ресурс. Режим доступу: https://fas.org/irp/doddir/dod/jp3_12.pdf **31.** Statement by lieutenant general Paul M. Nakasone Commander, United States Army Cyber Command before the Subcommittee on Cybersecurity Committee on Armed Services United States Senate second session, 115th congress May 23, 2017. Електронний ресурс. Режим доступу: https://www.armed-

services.senate.gov/imo/media/doc/Nakasone_05-23-17.pdf. **32.** International Strategy For Cyberspace: Prosperity, Security and Openness in a Networked World. Washington DC: The White House, May 2011. Електронний ресурс. Режим доступу: http://www.whitehouse.gov/sites/default/files/rss_viewer/internationalstrategy cyberspace.pdf **33.** Secretary of State Hillary Rodham Clinton On the Release of President Obama Administration's International Strategy for Cyberspace. May 16, 2011. Електронний ресурс. Режим доступу: http://www.state.gov/secretary/rm/2011/05/163523.htm **34.** Department of Defense. The Department of Defense Cyber Strategy - April 2015 National Cyber Strategy of the United States of America. September 2018. Електронний ресурс. Режим досупу: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf **35.** Summary Department of Defense Cyber Strategy - 2018. Електронний ресурс. Режим доступу: https://media.defense.gov/2018/sep/18/2002041658/-1/-1/1/cyber_strategy_summary_final.pdf **36.** Cyber Readiness Index 2.0 A Plan for Cyber Readiness: a baseline and an index. Potomac Institute for Policy Studies 901 N. Stuart St, Suite 1200 Arlington, VA, 22203, Електронний ресурс. Режим доступу: https://www.potomacinstitute.org/images/CRIndex2.0.pdf **37.** [Електронний ресурс] – Режим доступу: https://www.dw.com/uk / ukr-rss-MetaUA-ukr-V_Mire-3051-xml-mrss, https://espreso.tv/news/2015/03/23/u_nimechchyni_vyrishyly_vstanovyty_pravyla_dlya_kiberviyn **38.** [Електронний ресурс] – Режим доступу: https://intvua.com/news/society/1537605491-velika-britaniya-priynyala-rishennya-pro-stvorennya-kiberviysk.html, https://dt.ua/WORLD/britaniya-pochala-zbilshuvati-svoyi-kiberviyska-zmi-289016_.html, https://www.unian.ua/world/1112130-velikobritaniya-zbilshue-finansuvannya-kiberviyn-u-10-raziv.html **39.** White book on National Security of the Republic of Poland. Published by National Security Bureau, Warsaw Poland, 2013. P.263. **40.** [Електронний ресурс] – Режим доступу: https://www.unn.com.ua/uk/news/1766148-polscha-stvorit-viyska-kiberoboroni **41.** Disinformation as a Cyber Threat in the V4: Capabilities and Reactions to Russian Campaigns. [Електронний ресурс] – Режим доступу: https://stratpol.sk/wp-content/uploads/2018/08/Infographic-Cyber-V4- - STRATPOL.pdf **42.** Cyber defense academy in Budapest.: [Електронний ресурс] – Режим доступу:https://dailynewshungary.com/cyber-defense-academy-budapest/https://dailynewshungary.com/cyber-defense-academy-budapest/ **43.** [Електронний ресурс] – Режим доступу: https://en.wikipedia.org/wiki/Cooperative_Cyber_Defence_Centre_of_Excellence, https://www.eurointegration.com.ua/articles/2017/12/1/7074473/, http://www.eurointegration.com.ua/news/2017/11/8/7073389/ **44.** Доктрина информационной безопасности Российской Федерации (Указ Президента Российской Федерации от 05.12.2016 № 646). [Електронний ресурс] – Режим доступу: http://kremlin.ru/acts/bank/41460 **45.** Електронний ресурс. Режим доступу: http://recrut.mil.ru/for_recruits/research_company/companies.htm, https://www.nstu.ru/studies/army_research **46.** М.Гребенюк, Б.Леонов, Р.Лук'янчук. Досвід Ізраїлю у сфері забезпечення кібербезпеки // К,: Інформація і право – 2018,№ 2(25). **47** Конституція України [Електронний ресурс] – Режим доступу: http://zakon0.rada.gov.ua/laws/show/254 **48.** Закон України Про основні засади забезпечення кібербезпеки України № 2163-VIII від 5 жовтня 2017 року.[Електронний ресурс] — Режим доступу:http://zakon.rada.gov.ua/laws/show/2163-19 **49.** Закон Про оборону України: за станом на 01.07.2018 р./, затверджений ВР України від 06.12.1991, № 1932-XII — [Електронний ресурс] — Режим доступу: http://zakon4.rada.gov.ua/laws/show/1932-12 **50.** Закон України Про Збройні Сили України від 6 грудня 1991 року N 1934-XII (зі змінами), [Електронний ресурс] – Режим доступу: http://zakon3.rada.gov.ua/laws/show/1934-12 **51.** Стратегія кібербезпеки України, затверд жена Указом Президента України від 15.03.2016 № 96 // Офіц. вісн. України. — 2016. — № 23. **52.** Концепція розвитку сектору безпеки і оборони України, введена в дію Указом Президента України від 14.03.2016 №92/2016 **53.** Стратегічний оборонний бюлетень України, введений в дію Указом Президента України від 6.06.2016 № 240/2016 **54.** Візія Генерального штабу ЗС України щодо розвитку Збройних Сил України на найближчі 10 років. Електронний ресурс. Режим доступу: http://www.mil.gov.ua/news/2020/01/11/viziya-generalnogo-shtabu-zs-ukraini-shhodo-rozvitku-zbrojnih-sil-ukraini-na-najblizhchi-10-rokiv/ **55.** Стратегія національної безпеки України, затверджена Указом Президента України від 26.05.2015 № 287/2015.

ОПЫТ РАЗВИТИЯ СИСТЕМ КИБЕРБЕЗОПАСНОСТИ И КИБЕРОБОРОНИ ИНОСТРАННЫХ ГОСУДАРСТВ

Сергей Григорьевич Вдовенко
Юрий Григорьевич Даник *(доктор технических наук, профессор)*
Александр Юрьевич Пермяков *(доктор технических наук, профессор)*

Национальный университет обороны Украины имени Ивана Черняховского, Киев, Украина

Стремительное развитие и массовое внедрение достижений электроники, современных информационных и кибер технологий привели к формированию нового спектра рисков и угроз в сфере национальной безопасности и обороны государства, реализуемых в киберпространстве и (или) через киберпространство. Происходит стремительный рост информатизации и автоматизации всех сфер человеческой деятельности, количества хранящейся, обрабатываемой и передаваемой информации, скорости ее передачи и обработки, усложнение систем управления, взаимодействия между ними и связей между процессами управления. Киберугрозы охватывают все базовые сферы общественной деятельности (политическую, военную, правовую, экономическую, энергетическую, инфраструктурную, социальную, духовную, технологическую и т.п.), деструктивно влияя на национальную безопасность в целом.

Более 60 стран мира, международные (ЕС) и военно-политические союзы (НАТО), международные организации безопасности (ОБСЕ) сосредотачивают значительные усилия по обеспечению возможностей по своевременному выявлению, предупреждению, нейтрализации и ликвидации угроз в киберпространстве, в частности в сфере обороны.

В статье представлены следующие результаты: анализ организации и задач существующих систем кибербезопасности и кибероборони ведущих стран мира в контексте возможности и целесообразности внедрения их опыта в Украине; анализ предпосылок, существующего состояния и

проблемных вопросов формирования систем кибербезопасности и кибероборонь в Украине, а также нужного уровня их всестороннего обеспечения; пути разработки основных теоретических и прикладных положений формирования систем кибербезопасности и кибероборонь в Украине.

Ключевые слова: *кибербезопасность; кибероборона; киберпространство; система кибербезопасности; киберзащита; киберугрозы; система кибероборонь; объекты критической инфраструктуры; субъекты кибербезопасности; субъекты кибероборонь.*

EXPERIENCE OF DEVELOPMENT OF CYBER SECURITY SYSTEMS AND CYBER DEFENSE FOREIGN STATES

Serhii Vdovenko
Yurii Danyk *(Doctor of Technical Science, Professor)*
Oleksandr Permiakov *(Doctor of technical sciences, Professor)*

National Defence University of Ukraine named after Ivan Cherniakhovsky, Kyiv, Ukraine

The rapid development and widespread adoption of electronics, modern information and cyber technologies have led to the emergence of a new range of national security and defense risks and threats that are being implemented in cyberspace and (or) across cyberspace. There is a rapid growth of information and automation of all spheres of human activity, the amount of information stored, processed and transmitted, the speed of its transmission and processing, the complexity of control systems, the interaction between them and the links between management processes. Cyber threats cover all basic spheres of public activity (political, military, legal, economic, energy, infrastructure, social, spiritual, technological, etc.), destructively affecting national security as a whole.

More than 60 countries, international (EU) and military-political alliances (NATO), international security organizations (OSCE) are focusing considerable efforts on providing capabilities to detect, prevent, neutralize and eliminate cyberspace threats in a timely manner, in particular in the field of defense.

The results of the article are presented: analysis of the existing cyber security and cyber defense systems of the leading countries in the context of the possibility and expediency of implementing their experience in Ukraine; analysis of the prerequisites, current status and problems of the formation of cyber security and cyber defense systems in Ukraine, as well as the required level of their comprehensive provision; development of basic theoretical and applied provisions for the formation of cyber security and cyber defense systems in Ukraine.

Keywords: *Critical Infrastructure; Cyberspace; Cyber Defense; Cyber Defense System; Cyber Security; Cyber Defense Entities; Cyber Security Entities; Cybersecurity System; Cyberthreat.*

References

1. V. Buryachok, G. Hulak, V. Khoroshko. Tasks, Forms and Methods of War in Cybernetic Space - K .: Science and Defense №3 - 2011, p.35-42. **2. E. Zhivilo O., O.Chernohog**. Cyber Defense Strategy of Ukraine - K .: VITI № 4 - 2017, p. 30-37 **3. V. Lipkan, I. Diordica.** The National Cyber Security System as an Integral Part of the National Security System of Ukraine - K.: Business, Economy and Law №5– 2017, p. 174-180. **4. I.Gorbenko, A.Zamula, Ye.Semenko.** Ensemble and correlation properties of cryptographic signals for telecommunication system and network applications - Kharkiv/ Telecommunications and Radio Engineering. – 2016. – Vol. 75. – Issue 2. – P. 169–178. 5. **I.Gorbenko, O.Zamula.** Models and methods of synthesis of cryptographic signals and their optimization by the criterion of time complexity - Kharkiv - Mathematical and computer simulation. Series: Physical and Mathematical Sciences - 2017. Issue 15. p.43-49 - [Electronic resource]. Access mode: http://nbuv.gov.ua/UJRN/Mtkm_fiz_mat_2017_15_10 **6. Yu.Danik, S.Vdovenko.** Problems and Prospects of Providing Cyber Defense to the State of K.: MIKNU, Issue 66, 2020 - P. 56-72. **7. Yu. Danik.** High-tech aspects of national security and defense. K.: Military Communications. Telecom. October 2018 p. 58-69 **8. G. Liddell.** Indirect Action Strategy - M .: IL - 1957. **9.** DoD C4ISR Cooperative Research Program Assistant Secretary of Defense (C3I) Mr. Arthur L. Money Special Assistant to the ASD (C3I). [Electronic resource]. Access mode:: http://dodccrp.org/files/Alberts_NCW.pdf **10.** Warden, John A. III (September 1995), Chapter 4: Air theory for the 21st century, Battlefield of the Future: 21st Century Warfare Issues. **11. Bryant D.J.** Critique, Explore, Compare and Adapt (CECA): A New Model for Command Decisionmaking. Defence R&D Toronto Technical Report, DFDC, Toronto TR, 2003. 63 p. **12.** DoD C4ISR Cooperative Research Program Assistant Secretary of Defense (C3I) Mr. Arthur L. Money Special Assistant to the ASD(C3I). [Electronic resource]. Access mode: http://dodccrp.org/files/Alberts_NCW.pdf **13.** L.Polishchuk, S.Bogutsky M. Current Trends in the Development of Armed Forces Management Systems in Leading Countries of the World - VITI - 2014, p.42-46 **14.** Warsaw Summit Communiqué. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016 09 Jul. 2016 – 2016, 100 **15.** National Security Strategy of Ukraine, approved by Presidential Decree No 287/2015 of May 26, 2015.**16.** S.Neema. Symbiotic Design for Cyber Physical Systems. Defense Advanced Research Projects Agency Program Information. [Electronic resource]. Access mode: https://www.darpa.mil/program/symbiotic-design-for-cyber-physical-systems. **17. S.Vodovenko, Y.Danik.** Conceptual directions of complex solution of the problem of protection against unauthorized access in complex systems of special purpose. Vinnitsa, VNPU - 2017, p. 61 - 64.**18. Yu.Danik, S.Vdovenko.** Chain effects in cyberdias. Proceedings of the Military Institute of the Taras Shevchenko National University of Kyiv, issue 64 - 2019 - P. 56-71. **19.** [Electronic resource]. Access mode: https://www.usna.edu/wrc/cpsl/index.php, https://thebabel.com.ua/news/41889-ssha-rozgortayut-protidronovi-lazerni-sistemi-na-zarubizhnih-bazah, https://defence-ua.com/index.php/statti/2245-vyprobuvannya-bpla-6-ho-pokolinnya-ssha-pokazaly-mistse-rosiyi, http://www.nanonewsnet.ru/news/2017/kitaitsy-obedinili-v-stayu-tysyachu-dronov, https://lb.ua/world/2015/11/17/321192_britaniya_sozdast_spetsialnie.html, http://www.lefigaro.fr/international/l-armee-se-dote-de-56-microrobots-de-reconnaissance, https://www.linkedin.com/company/national-security-agency?trk=similar-pages_result-card_full-click, https://www.cybercom.mil/About/Mission-and-Vision/ https://www.cybercom.mil/, https://www.cybercom.mil/About/Leadership/Bio-Display/Article/1512978/commander-uscybercom/,

https://en.wikipedia.org/wiki/United_States_Cyber_Command, https://military.wikia.org/wiki/Second_United_States_Armyhttps://www.globalsecurity.org/military/agency/usaf/afcyber htm, https://www.public.navy.mil/fcc-c10f/Pages/home.aspx, https://www.navy.mil/local/fccc10f/ https://www.armed-services.senate.gov/imo/media/doc/Gilday_05-23-17.pdf, https://www.candp.marines.mil/Organization/Operating-Forces/US-Marine-Corps-Forces-Cyberspace-Command/ https://www.epravda.com.ua/news/2018/10/23/641908/ https://www.rbc.ua/rus/news/ssha-proveli-kiberataku-iranskie-raketnye-1561260168.html https://lexinform.com.ua/v-sviti/ssha-pochaly-kiberoperatsiyu-proty-rosiyi/ https://www.arcyber.army.mil/, https://www.fifthdomain.com/dod/cybercom/2019/07/25/what-the-future-holds-for-cyber-command/ **20.** Moore, Gordon E. (1965). Cramming more components onto integrated circuits, Electronics Magazine. c. 4 [Electronic resource]. Access mode: https://newsroom.intel.com/wp-content/uploads/sites/11/2018/05/moores-law-electronics.pdf **21.** Moore, Gordon E. No Exponential is Forever: But "Forever" Can Be Delayed!, International Solid-State Circuits Conference 2003 / SESSION 1 / PLENARY / 1.1 -2003. [Electronic resource]. Access mode: https://ieeexplore.ieee.org/document/1234194 **22.** Kurzweil, Ray -2005. The Singularity Is Near. When Humans Transcend Biology. Penguin Books [Electronic resource]. Access mode: http://stargate.inf.elte.hu/~seci/fun/Kurzweil/ Ray_Singularity_Near_The_hardbac_ed_Bv1._D.pdf **23.** Recently discovered phenomenon could provide a way to bypass the limits to Moore's Law. [Electronic resource]. Access mode: https://phys.org/news/2017-10-phenomenon-bypass-limits-law.html **24. V. Begma, V. Shemaev.** Technology development in the world's leading countries. Lessons for Ukraine. [Electronic resource]. Access mode: https://defence-ua.com/index.php/statti/publikatsiji-partneriv/8982-rozvytok-tekhnolohiy-u-providnykh-krayinakh-svitu-uroky-dlya-ukrayiny **25.** Network Centric Warfare Market by Platform (Land, Air, Naval, Unmanned), Application (ISR, Communication, Computer, Cyber, Combat, Control & Command), Mission Type, Communication Network, Architecture, and Region - Global Forecast to 2021. [Electronic resource]. Access mode: https://www.marketresearch.com/MarketsandMarkets-v3719/Network-Centric-Warfare-Platform-Land-10188278/ **26.** BMC4ISR means Battle Management/Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance. [Electronic resource]. Access mode: http://acronymsandslang.com/definition/24656/BMC4ISR-meaning.html **27.** Summit Meeting of NATO Heads of State and Government - Lisbon, Portugal, 19-20 Nov 2010. [Electronic resource]. Access mode: https://www.nato.int/cps/en/natolive/events_66529.htm **28. S.Vodovenko, Y. Danik, S. Pharaoh.** Definitional problems of terminology in cybersecurity and cyber defense and ways of solving them. - Kharkiv: KhNU. VN Karazin - 2019, No.1 (12). [Electronic resource]. Access mode: https://doi.org/10.26565/2519-2310-2019-1-02 **29.** DOD Dictionary of Military and Associated Terms As of January 2020. [Electronic resource]. Access mode: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdfhttps://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf **30.** DOD. Joint Publication 3-12, Cyberspace Operations, 8 June 2018/. [Electronic resource]. Access mode: https://fas.org/irp/doddir/dod/jp3_12.pdf **31.** Statement by lieutenant general Paul M. Nakasone Commander, United States Army Cyber Command before the Subcommittee on Cybersecurity Committee on Armed Services United States Senate second session, 115th congress May 23, 2017. [Electronic resource]. Access mode: https://www.armed-services.senate.gov/imo/media/doc/Nakasone_05-23-17.pdf. **32.** International Strategy For Cyberspace: Prosperity, Security and Openness in a Networked World. Washington DC: The White House, May 2011. [Electronic resource]. Access mode: http://www.whitehouse.gov/sites/default/files/rss_viewer/internationalstrategy cyberspace.pdf **33.** Secretary of State Hillary Rodham Clinton On the Release of President Obama Administration's International Strategy for Cyberspace. May 16, 2011. [Electronic resource]. Access mode: http://www.state.gov/secretary/rm/2011/05/163523.htm **34.** Department of Defense. The Department of Defense Cyber Strategy - April 2015 National Cyber Strategy of the United States of America. September 2018. [Electronic resource]. Access mode: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf **35.** Summary Department of Defense Cyber Strategy - 2018. [Electronic resource]. Access mode: https://media.defense.gov/2018/sep/18/2002041658/-1/-1/1/cyber_strategy_summary_final.pdf **36.** Cyber Readiness Index 2.0 A Plan for Cyber Readiness: a baseline and an index. Potomac Institute for Policy Studies 901 N. Stuart St, Suite 1200 Arlington, VA, 22203, [Electronic resource]. Access mode: https://www.potomacinstitute.org/images/CRIndex2.0.pdf **37.** [Electronic resource]. Access mode: https://www.dw.com/uk / ukr-rss-MetaUA-ukr-V Mire-3051-xml-mrss, https://espreso.tv/news/2015/03/23/u nimechchyni vyrishyly vst anovyty pravyla dlya kiberviyn **38.** [Electronic resource]. Access mode: https://intvua.com/news/society/1537605491-velika-britaniya-priynyala-rishennya-pro-stvorennya-kiberviysk.html, https://dt.ua/WORLD/britaniya-pochala-zbilshuvati-svoyi-kiberviyska-zmi-289016 .html, https://www.unian.ua/world/1112130-velikobritaniya-zbilshue-finansuvannya-kiberviyn-u-10-raziv.html **39.** White book on National Security of the Republic of Poland. Published by National Security Bureau, Warsaw Poland, 2013. P.263. **40.** [Electronic resource]. Access mode: https://www.unn.com.ua/uk/news/1766148-polscha-stvorit-viyska-kiberoboroni **41.** Disinformation as a Cyber Threat in the V4: Capabilities and Reactions to Russian Campaigns [Electronic resource]. Access mode: https://stratpol.sk/wp-content/uploads/2018/08/Infographic-Cyber-V4- - STRATPOL.pdf **42.** Cyber defense academy in Budapest. [Electronic resource]. Access mode: https://dailynewshungary.com/cyber-defense-academy-budapest/https://dailynewshungary.com/cyber-defense-academy-budapest/ **43.** [Electronic resource]. Access mode: https://en.wikipedia.org/wiki/Cooperative_Cyber_Defence_Centre_of_Excellence, https://www.eurointegration.com.ua/articles/2017/12/1/7074473/, http://www.eurointegration.com.ua/news/2017/11/8/7073389/ **44.** Doctrine of Information Security of the Russian Federation (Decree of the President of the Russian Federation of 05.12.2016 No. 646). [Electronic resource]. Access mode: http://kremlin.ru/acts/bank/41460 **45.** [Electronic resource]. Access mode: http://recrut.mil.ru/for_recruits/research_company/companies.htm , https://www.nstu.ru/studies/army research **46.** M. Grebenyuk, B. Leonov, R. Lukyanchuk. Israel's experience in cybersecurity // K,: Information and Law - 2018, No. 2 (25). **47** Constitution of Ukraine [Electronic resource]. Access mode: http://zakon0.rada.gov.ua/laws/show/254 **48.** Law of Ukraine On the Fundamental Principles of Cyber Security of Ukraine No. 2163-VIII of October 5, 2017. [Electronic resource]. Access mode: http://zakon.rada.gov.ua/laws/show/2163-19 **49.** Law on Defense of Ukraine, approved by the Verkhovna Rada of Ukraine dated 06.12.1991, No. 1932-XII — [Electronic resource]. Access mode: http://zakon4.rada.gov.ua/laws/show/1932-12 **50.** Law of Ukraine On the Armed Forces of Ukraine of December 6, 1991 N 1934-XII, [Electronic resource]. Access mode: http://zakon3.rada.gov.ua/laws/show/1934-12 **51.** Ukraine's cybersecurity strategy, approved by Presidential Decree No. 96 of March 15, 2016 // Official. hanging Of Ukraine. - 2016. - № 23. **52.** The Concept of Development of the Security and Defense Sector of Ukraine, Implemented by the Decree of the President of Ukraine of 14.03.2016 # 92/2016 **53.** Strategic Defense Bulletin of Ukraine, Enacted by Presidential Decree of June 6, 2016 No. 240/2016 **54.** Vision of the General Staff of the Armed Forces of Ukraine on the development of the Armed Forces of Ukraine for the next 10 years. [Electronic resource]. Access mode: http://www.mil.gov.ua/news/2020/01/11/viziya-generalnogo-shtabu-zs-ukraini-shhodo-rozvitku-zbrojnih-sil-ukraini-na-najblizhchi-10-rokiv/ **55.** National Security Strategy of Ukraine, approved by Presidential Decree No 287/2015 of May 26, 2015.