УДК 004.413.4

д.т.н., проф. **Даник Ю.Г.** (НУОУ)
Вдовенко С.Г. (НУОУ)

DOI: https://doi.org/10.17721/2519-481X/2020/66-08

ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ ЗАБЕЗПЕЧЕННЯ КІБЕРОБОРОНИ ДЕРЖАВИ

Зростання ролі і значення вирішення завдань кібербезпеки та кібероборони обумовлено інноваційним розвитком інформаційних, електронних та кібер- технологій, які стали рушієм ряду тенденцій у воєнній справі. Внаслідок формування та визнання штучного п'ятого простору – кіберпростору, окремою сферою боротьби між державами, включаючи збройне протиборство, питання кібербезпеки та кібероборони стали актуальними в забезпеченні національної безпеки і оборони розвинених держав, котрі особливу увагу приділяють формуванню та розвитку систем кібербезпеки та кібероборони, як головного фактору у досягненні воєнно-стратегічної переваги в забезпеченні національної безпеки і оборони в сучасних та перспективних умовах.

У статті здійснено аналіз загальних принципів побудови систем кібербезпеки і кібероборони провідних країн світу в контексті можливості та доцільності впровадження їх досвіду в Україні; аналіз передумов, існуючого стану та проблемних питань формування систем кібербезпеки та кібероборони в Україні. Зокрема, такими є: відсутність основних теоретичних та прикладних положень формування системи кібероборони; відсутність національного органу військового управління у сфері кібероборони; розпорошеність зусиль різних військово-організаційних структур щодо вирішення завдань кібербезпеки та відсутність сформульованих задач кібероборони.

Запропоновано найбільш раціональний варіант створення систем і структур кібербезпеки та кібероборони України з підсистемами освіти та науки, якій відповідно до сучасних тенденцій розвитку, з урахуванням військово-політичної обстановки, національних інтересів та законодавства, забезпечить інформаційну, кібернетичну та когнітивну перевагу над противником та буде сприяти практичній реалізації прийнятої в країнах членах НАТО концепції "смарт-оборони".

Ключові слова: кібербезпека, кібероборона, кіберпростір, система кібербезпеки, система кібероборони, кіберосвіта, кібератака, кібервплив, кіберзагроза, кібердія, кіберзахист, кібероперація, кіберрозвідка, кіберудар, суб'єкти кібербезпеки, суб'єкти кібероборони, об'єкти критичної інфраструктури.

Вступ та постановка проблеми. Стрімкий розвиток та масове впровадження досягнень електроніки, сучасних інформаційних та кібер- технологій призвело до формування нового спектру ризиків і загроз у сфері національної безпеки і оборони держави, які реалізуються у кіберпросторі та (або) через кіберпростір. Відбувається експоненціальне 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 та 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.

В сучасному світі питання кібербезпеки та кібероборони стали наріжними і найбільш проблемними та актуальними в забезпеченні національної безпеки і оборони практично всіх розвинених держав. На саміті НАТО в Варшаві (7-9.07.2016) на Кібер конференції з інформаційного забезпечення НАТО (NIAS) (6.12.2016), на конференції "Кібернетична оборона" (Париж, 15.05.2018), на засіданні Північноатлантичної ради (Брюссель 11-12.07.2018) та на саміті у Лондоні у листопаді 2019 року присвяченому 70-річчю створення альянсу НАТО було зосереджено увагу на важливості своєчасного виявлення, запобігання, нейтралізації і ліквідації загроз в кіберпросторі [1,2,3].

Зазначені проблеми в Україні і світі розглядаються перш за все на рівні термінологічного визначення [4-8], аналізу окремих питань кібербезпеки, здебільшого з точки зору

кіберзлочинності та кібертероризму і в деякій мірі на рівні аналізу особливостей впровадження систем кібербезпеки [9-20]. Концептуальні проблемні питання щодо загроз національній безпеці, зокрема у сфері інформаційної та кібербезпеки, окремі засади протидії кіберзлочинності та боротьби з кібертероризмом, 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, М.Яцишин та інші. Але, проблема створення системи кібероборони та особливостей її трансформації в умовах стрімкого розвитку науки, техніки та технологій системно і цілісно до цього часу не розглядалися, узагальнений аналіз особливостей формування та трансформації систем кібербезпеки і кібероборони під впливом різноманітних чинників та залежності їх ефективності від складу, організації, структурної побудови і систем управління ними у безпосередньому взаємозв'язку із нормативно-правовим, організаційним, науковим та кадровим забезпеченням у контексті визначення їх мети, завдань, функцій і шляхів досягнення необхідних спроможностей не проводився. Проблеми кібероборони, з точки зору воєнно-політичного та воєнно-стратегічного аналізу розглядаються здебільш іноземними фахівцями, публікуються в офіційних виданнях самітів НАТО, але не мають юридичної сили альянсу та є лише поглядами фахівців [21- 23].

Мета цієї роботи полягає в проведенні аналізу і узагальненні відомих результатів та дослідженні 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.

Викладення основних основного матеріалу дослідження. 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, науки кібернетики та впровадженням систем управління в усіх галузях і сферах людської діяльності, теорії зв'язку та інформації і стрімким розвитком інформаційних, кібернетичних та інформаційно-комунікаційних систем.

На цей час загальновизнано, що в результаті високотехнологічної та інформаційної діяльності людства додатково до природних: суходільного, морського повітряного та космічного, фактично сформувався штучний п'ятий простір – кіберпростір, який перетворився на окрему сферу боротьби між державами, включаючи збройне протиборство [1,24]. Перше офіційне визначення кіберпростору було дано військовими експертами США в настанові КНШ 2006 року "Інформаційні операції": "Кіберпростір – сфера, в якій застосовуються різні радіоелектронні засоби (зв'язку, радіолокації, розвідки, навігації, автоматизації, управління і наведення), що використовують широкий діапазон електромагнітного спектра частот для прийому, передачі, обробки, зберігання, перетворення і обміну інформацією, і пов'язана з ними інформаційна інфраструктура ЗС США". За поглядами провідних фахівців з кібербезпеки, кіберпростір визначається скоріше соціальними взаємодіями, а не його технічною реалізацією [11]. На їхню думку, обчислювальне середовище в кіберпросторі є доповненням каналу зв'язку між реальними людьми. Уряди провідних країн світу відносять взаємопов'язані інформаційні технології і взаємозалежну мережу інфраструктур інформаційних технологій кіберпростору до національної критичної інфраструктури.

Трансформація поглядів на питання кібербезпеки і кібероборони та, відповідно, розвиток їх структур в провідних країнах світу відбувається під впливом розвитку технологій, змін у безпековому середовищі, формах, способах та технологіях ведення війн і нових досягнень в цьому які очікуються.

На цей час в світі існує біля 40 ключових макротехнологій, які за думкою провідних експертів визначають рівень економіки та обороноздатності країн в сучасних умовах.

До високих технологій та технологій подвійного призначення (high technology, hi-tech - англ.) частіше за все відносять такі технології: штучний інтелект, космічні, робототехнічні, інформаційні та кібер- технології; нано-, квантові, нейронні, біотехнології, генну інженерію, інноваційні електромеханіку, електроніку, матеріалознавство, створення

нових напівпровідникових матеріалів, генерування, акумулювання та передача енергії, “чисті” (cleantech) та енергозберігаючі технології, телекомунікаційні, інфокомунікаційні технології та технології управління і автоматизації.

В цих сферах прогнозуються проривні досягнення перш за все у штучному інтелекті, хмарних технологіях, інтернеті речей, продуктивності та природі обчислювальних засобів, можливостях зберігання обробки та передачі великих масивів даних та інформації (Big Data), засобах і технологіях їх реалізації на кардинально нових принципах. Можливості і вразливості практично всіх сучасних інфокомунікаційних та кібернетичних систем все більше залежать, крім того, від зростання взаємозв’язків різноманітних інформаційних систем та систем управління між собою в багатопараметричному та багатовимірному кіберпросторі та їх інформаційно-кібернетичного взаємопроникнення, взаємодії і взаємозалежності тощо.

Проблемні питання і особливості створення та розвитку систем кібероборони.

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 в сучасних та перспективних умовах. Об’єктивність такого підходу обумовлена тим, що світ наразі перебуває на порозі нового стрибка технологій. У сфері оборони відбувається глобальний перехід на інтегровані системи управління військами та зброєю від стратегічного до тактичного рівня, та інноваційних систем озброєння, які до 80% побудовані з високотехнологічних складових.

Зростання ролі і значення вирішення завдань кібербезпеки та кібероборони також обумовлено інноваційним розвитком інформаційних, електронних та кібер- технологій, які стали рушієм ряду тенденцій у воєнній справі, зокрема таких, як:

1. глобальна інформатизація та початок роботизації військових формувань і створення високо інтегрованих систем управління, які, в свою чергу, стають об'єктами кібервпливу і вимагають розвитку форм і способів ведення кібер- протиборства;

2. зростання інтенсивності конфліктів в інформаційному та кіберпросторі, за участі спеціально створених для цього спеціалізованих структур та формувань. Ведення терористичних дій через інформаційний та кібер- простори та безпосередньо в них;

3. домінування більш розвинутих країн у веденні деструктивних дій саме через інформаційний та кібер- простори з одного боку, та з іншого - зростання уразливості держав при зростанні рівня їх високотехнологічного розвитку;

4. використання світових інформаційних мереж та електронних засобів масової інформації для маніпулювання свідомістю та досягнення когнітивних трансформацій як окремих спільнот і населення окремих країн так і світової громади;

5. виділення інформаційного та інформаційно-аналітичного забезпечення в самостійний вид забезпечення військ (сил) і формування відповідних структур для його здійснення;

6. постійне зростання кількості та можливостей комп’ютерних та електронних засобів, що задіяні в зберіганні, обміні і обробці інформації і під час прийняття управлінських рішень у тому числі на всіх етапах планування операцій та у ході бойових дій. Зростання ролі імітаційного моделювання при плануванні операцій і в процесі ведення бойових дій. Подальша інтеграція засобів штучного інтелекту в системи воєнного призначення;

7. інтеграція на основі продуктів високих технологій систем розвідки, управління та ураження від підрозділу (одиниці бойової техніки) до командування всіх ланок управління. Мініатюризація комп’ютерних та електронних засобів, їх використання практично у всі зразках озброєння та бойової техніки (від високоточної зброї до особистої зброї та спорядження).

Аналіз теорії, практики й досвіду побудови систем і забезпечення кібербезпеки та кібероборони провідних держав світу свідчить, що основною тенденцією при їх формуванні стало поєднання в єдиній структурі, яка відповідає за кібероборону, відповідно до мети, завдань, доцільних форм та способів забезпечення кібербезпеки у воєнній сфері, різних

напрямів діяльності (та відповідно, підрозділів, які її здійснюють) поєднаних їх відношенням до кіберпростору. Визначним чином на ці процеси вплинуло безпосередньо особливості формування та постійні розвиток і трансформація кіберпростору.

У провідних країнах світу при формуванні систем кібербезпеки та кібероборони основною тенденцією стало створення нового виду Збройних Сил – Кіберсил (Кібервійськ) з відповідними кіберкомандуваннями, шляхом об'єднання в єдиній структурі, що відповідає за кібероборону, органів військового управління, сил і засобів, які мають відношення до кіберпростору, з реформуванням, перерозподілом функцій, та перепідпорядкуванням військових частин, зі зміною, за необхідності, напрямків їх діяльності, корегування наукової та освітньої діяльності наукових центрів та закладів освіти, включно утворення нових структурних підрозділів, закладів освіти, військових частин та підрозділів різних напрямів діяльності для виконання спільних заходів кіберрозвідки, кіберзахисту, активних дій в кіберпросторі, відповідно до мети, завдань, доцільних форм та способів забезпечення кібербезпеки у воєнній сфері (таблиця 1).

Аналіз викладеного (таблиця 1) свідчить, що до складу Кіберсил (кібервійськ), як правило входять підрозділи радіоелектронної розвідки (РЕР), радіоелектронної боротьби (РЕБ), інформаційно-психологічних операцій (ІПсО), зв'язку та інформаційних систем, захисту інформації в ІТС, криптографічного забезпечення та криптологічної підтримки, геоінформаційного забезпечення тощо. Створені в провідних країнах світу системи кібероборони включають та об'єднують 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, проваджують діяльність у сфері технічних розвідок та здійснюють криптоаналіз, приймають участь у заходах введення в оману, здійснюють наукові дослідження в цих сферах та підготовку кадрів.

Наукове, науково-технічне, освітньо-тренувальне супроводження утворення Кіберсил здійснюється, як правило, багатофункціональними профільними військовими закладами. Держзамовлення на підготовку фахівців, включно науково-педагогічних працівників – збільшується. При відсутності профільних ВНЗ – вони утворюються. В провідних країнах світу (Великобританія, ФРН, Польща) ефективність вирішення зазначених проблем досягається шляхом формування та забезпечення функціонування інтегрованих навчально-наукових, дослідно-випробувальних університетів, які здійснюють на єдиній базі освітню і наукову діяльність за високотехнологічними напрямами. Наприклад, така інтеграція військової освіти і науки за високотехнологічними напрямами успішно реалізована у Військовому університеті технологій (Польща), де на одній базі зосереджені всі високотехнологічні напрями, спеціальності і спеціалізації підготовки військових фахівців (факультети: національної безпеки, електроніки та телекомунікацій, енергетики, технічної фізики, геодезії і картографії, інформатики, інженерії безпеки, інженерії матеріалів, криптології і кібербезпеки, авіації і космонавтики, механіки і машинобудування, мехатроніки, управління тощо) та наукових досліджень.

Законами України та іншими нормативно-правовими актами не визначено перелік вичерпних заходів щодо підготовки до відбиття та відбиття воєнної агресії у кіберпросторі. На думку авторів, завдання кібербезпеки та кібероборони в цілому можуть розглядатися в межах трьох три основних підсистем: кіберрозвідки, кіберзахисту, кібервпливу (активних дій). Питання забезпечення кібербезпеки можуть умовно розглядатися за:

напрямками – захист громадянина і суспільства, захист держави;

об'єктами кібервпливу – соціальні, технічні, соціотехнічні системи (рис. 1);

рівнями – державний (стратегічний), регіональний (оперативний), місцевий (тактичний);

завданнями – запобігання, стримування, протидії;

сферами – економіка (виробничий та невиробничий сектори, критична інфраструктура держави), сфери зовнішньої та внутрішньої політики, державного управління, освіта, наука, безпека і оборона (рис.2);

Зведені дані щодо кіберсил окремих держав світу. Таблиця 1

Показники (індикатори)	США	ФРН	Велика Британія	Франція	Польща	Угорщина	Ізраїль	РФ	Україна
Наявність національної Стратегії (доктрини) КО (КЗ). Рік видання діючої.	2018	2016	2018	2018	2018	2018	2015	2015	2016
Складові частини (функціональні елементи) Кіберсил	РЕР, РЕБ ІПсО зв'язок та ІС, крипто,	РЕР, РЕБ ІПсО зв'язок та ІС, крипто, гео-інформ забезп	РЕР РЕБ ІПсО зв'язок та ІС крипто	РЕР РЕБ ІПсО зв'язок та ІС, крипто	РЕБ, зв'язок та ІС, крипто	РЕБ, зв'язок та ІС, крипто	РЕР, РЕБ ІПсО зв'язок та ІС, крипто	ІПсО	-
Наявність сил КО, як окремого виду ЗС	+	+	+	+	+	+	+	+	-
Чисельність, тис/ % від чисельності ЗС	50/ 2,5%	13,5/ 6%	2/ 1,5%	4/ 1,5%	1/ 1%	1/ 0,4%	> 3/ 5,5%	1/ 0,1%	-
Наявність органу управління КО (кіберкомандування)	+	+	+	+	+	+	+	+	-
Роки формування,	2009-2019	2017-2021	2017-2021	2015-2019	2018-2021	2019-2022	2018-2021	2016 - …	-
Рік набуття спроможностей	2018	2021	2021	2018	2021	2020	2021	2015	?
Спосіб формування: на базі існуючих + нова структура -	+	+	+	+	+	+	+	-	-
Наявність системи наукової підтримки, освіти та підготовки системи КО (цив.*)	7	1	15*	2	2	1	3*	3	4 (неузгодж)

складовими частинами – кіберзахист (боротьба з кіберзлочинністю, кібершпигунством, кібертероризмом), кібероборона (дії в ІТ-мережах та програмно-комп'ютерні, дії в електромагнітному спектрі випромінювання, дії в соціокіберпросторі, кіберпросторі та через кіберпростір: інформаційні, психологічні, когнітивні) (рис. 3);

формами і способами кіберзахисту та активних кібердій (рис. 4);

суб'єктами, що здійснюють кіберзахист та кібероборону.

Процеси побудови, розвитку, та набуття спроможностей щодо бойового застосування систем кібероборони провідних країн світу супроводжувалися виявленням та вирішенням ряду проблем, основними з яких були:

протиріччя у відповідності теорії та практики забезпечення кібербезпеки та кібероборони в умовах формування та інтенсивного розвитку засад, форм, способів, засобів і технологій інформаційних та кібердій;

відсутність або недосконаліть дефініційно-термінологічного апарату, концепцій та стратегій створення і застосування кіберсил;

недостатня кількість або відсутність підготовлених кадрів, систем їх підготовки, науково-технічного супроводження;

відсутність або нераціональне вирішення питань державно-приватного партнерства;

відсутність необхідних та/або невідповідність практичній необхідності законів та нормативно-правових актів;

невідповідність визначеним завданням організаційно-штатних структур органів військового управління, підрозділів, які з інших видів збройних сил включалися до складу кіберкомандувань; невідповідність практичній потребі наявної штатної техніки та обладнання підрозділів кіберсил.

Рисунок 1 – Об'єкти кібервпливу

Разом з тим, формування систем кібербезпеки та кібероборони провідних країн світу відбуваються спираючись на загальні принципи, позитивні риси яких можуть та повинні бути використані при побудові системи кібероборони України, основні з них:

інтегрованість системи кібероборони в багаторівневу систему кібербезпеки держави (коаліції);

безперервність функціонування системи кібероборони;

відповідність рівня всебічного забезпечення кіберсил потребам оборони;

оптимальність (раціональність) побудови сил кібероборони;

керованість з єдиного координуючого органу з питань забезпечення кібербезпеки;

науково обґрунтовані законодавче, нормативно-правове, дефініційно-термінологічне супроводження;

державно-приватне та міжнародне партнерство;

узгодженість та взаємодія різних відомств у сфері забезпечення кібероборони держави;

інтегрованість закладів освіти до високотехнологічних навчально-наукових, дослідно-випробувальних комплексів, уніфікованість вимог щодо підготовки військового й цивільного персоналу кібербезпеки;

однозначність критеріїв (індикаторів) загроз у сфері кібероборони держави, рівня готовності систем КБ та КО, тощо.

Аналіз стану кібероборони в Україні. Оборона України, захист її суверенітету, територіальної цілісності і недоторканності, охорона повітряного та підводного простору держави покладаються на ЗС України [25-27]. З ухваленням у жовтні 2017 року Закону [28] на Міністерство оборони та Генеральний штаб Збройних Сил України покладено нове завдання щодо впровадження заходів із забезпечення кібероборони.

Законодавством також визначається обов'язковість здійснення заходів з підготовки держави до відбиття воєнної агресії у кіберпросторі, кібероборони для захисту суверенітету держави та забезпечення її обороноздатності, запобігання збройному конфлікту та відсічі збройній агресії, забезпечення кіберзахисту критичної інформаційної інфраструктури в умовах надзвичайного і воєнного стану, у тому числі – шляхом проведення спеціальних операцій (розвідувальних, інформаційних, психологічних, інформаційно-психологічних тощо) у кіберпросторі при підготовці до захисту та захисту України в разі збройної агресії. Розвідувальним органам України визначені завдання із здійснення розвідувальної діяльності щодо загроз національній безпеці України у кіберпросторі, інших подій і обставин, що стосуються сфери кібербезпеки. Значна увага приділяється військовій співпраці з НАТО та іншими суб'єктами оборонної сфери щодо забезпечення безпеки кіберпростору та спільного захисту від кіберзагроз [26-29].

Разом з тим, Законами України, або іншими нормативно-правовими актами не визначені:

кіберпростір, як середовище ведення оборонних дій для забезпечення захисту суверенітету держави;

перелік кіберзагроз державі в оборонній сфері;

перелік вичерпних заходів із підготовки до відбиття та відбиття воєнної агресії у кіберпросторі;

механізм координації діяльності суб'єктів кіберзахисту України при реалізації завдань щодо оборони України в кіберпросторі.

Пропозиції та рекомендації. Кібероборона – окрема, особлива, специфічна складова кібербезпеки держави, що має різнопланові повсякденні, поточні та бойові (спеціальні) завдання і функції. Тому, необхідно створювати єдину систему кібероборони під єдиним командуванням, всі складові якої діють узгоджено за єдиним замислом і планом. Відсутність зв'язків між розрізненими елементами знижує ефективність їх застосування. Натомість їх наявність – додає нові спроможності щодо ураження противника, ступінь якого може бути багатократно збільшена за рахунок ланцюгових ефектів кібердій [30].

Виходячи з викладеного, пропонується базис системи кібердій в інтересах кібероборони держави будувати на трьох основних поєднаних у єдине ціле складових підсистемах: кіберрозвідки, кіберзахисту, кібервпливу (рис. 3).

Для забезпечення створення та функціонування цілісної системи кіберорборони (СКО) з урахуванням національних вимог [24-29, 31] та рекомендацій експертів НАТО та країн-партнерів щодо уніфікації бойових командувань і процедур [1,23,31-33] необхідно здійснити низку взаємопов'язаних політичних, правових, організаційних, науково-технічних, безпосередньо військових та інших заходів.

Законами України та Стратегією воєнної безпеки України мають бути визначені нові функції і завдання МО України та ЗС України в СКО та відповідному кіберкомандуванню, зокрема такі як:

Рисунок 2 – Сфери економіки що підлягають кібероборони

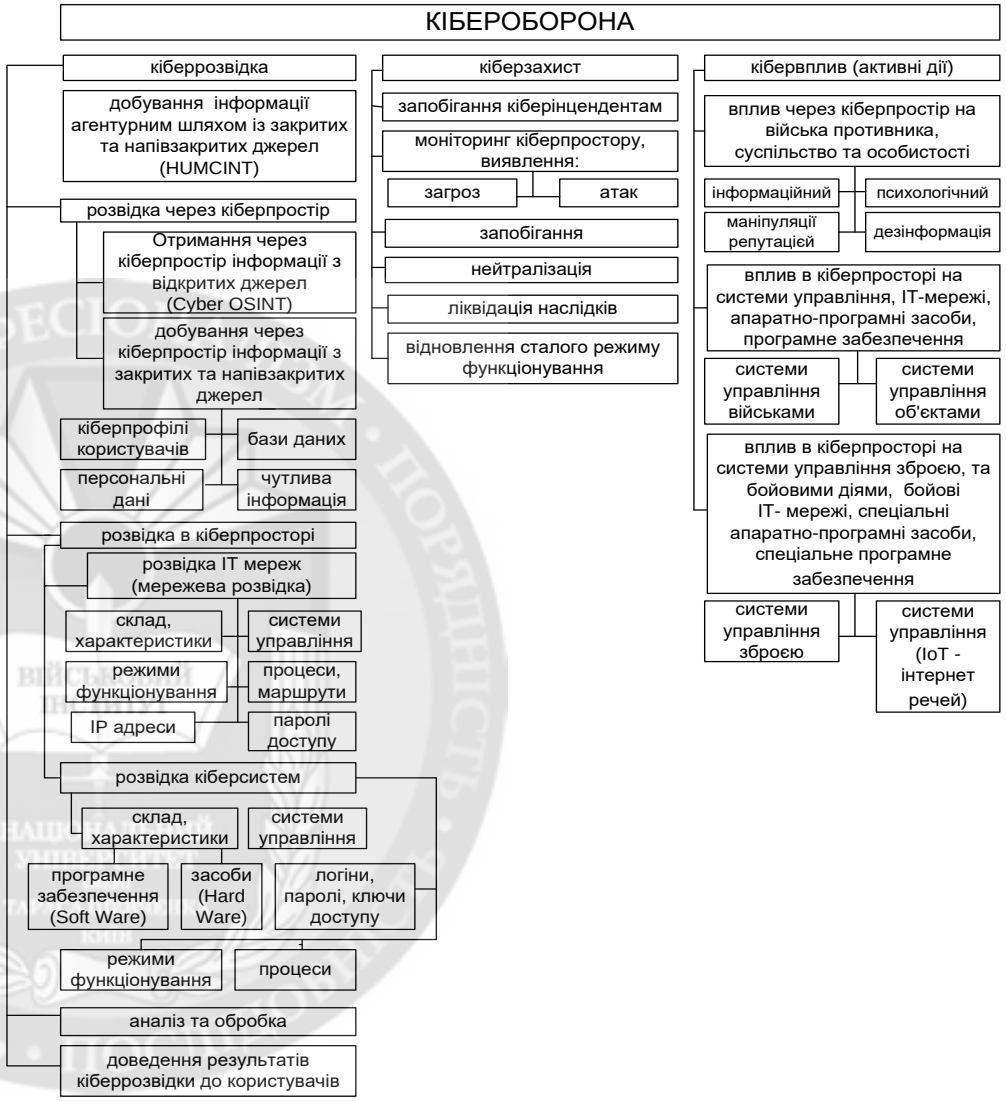

Рисунок 3 – Складові частини та завдання кібероборони

Рис.4. Активні кібердії за рівнями, формами, способами

розробка та реалізація засад державної політики у сфері кібероборони, визначення завдань, функцій та критеріїв військово-політичної, військової, військово-технічної, науково-технічної та розвідувальної діяльності суб'єктів кібероборони з питань планування кібероборони та дій у кіберпросторі і через кіберпростір на стратегічному рівні відповідно до Плану оборони держави;

участь в підготовці об'єктів критичної інформаційної інфраструктури держави щодо протидії кіберзагрозам та сталому їх функціонуванню в особливий період та в умовах воєнного стану;

розробка засад застосування ЗС України, інших військових та спеціальних формувань для виконання завдань кібероборони, включно питання асиметричних кібердій спрямованих на примушення противника до відмови або припинення воєнних (бойових) дій, кібердій під час підготовки і проведення спільних оборонних, наступальних, контр-наступальних операцій сил оборони, спеціальних операцій, коаліційних операцій, територіальної оборони, дій руху опору, ліквідації наслідків надзвичайних ситуацій, спричинених застосуванням зброї, та при захисті населення і територій від наслідків ведення воєнних дій;

формування стандартів підготовки та держзамовлення на підготовку фахівців з кібербезпеки та кіберобоони, розробка програм та планів оперативної і спеціальної підготовки, бойових статутів, стандартів і настанов ЗС України з питань кібероборони;

планування, організація та здійснення заходів з нейтралізації та активної протидії кіберзагрозам національним інтересам України у сфері оборони;

планування, координації дій, організації взаємодії та проведення заходів щодо підготовки держави до кібероборони зі структурними підрозділами інших центральних органів виконавчої влади та з міжнародними партнерами, узгоджене управління суб'єктами кібероборони.

втілення найсучасніших інформаційних технологій у сфері оборони, забезпечення розвитку і безпеки власної інформаційної та управлінської інфраструктури та ресурсів, захист їх від кіберзагроз.

Зазначене вимагає 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.

Цей орган управління відповідальний за організацію та здійснення заходів щодо забезпечення інформаційної та кібербезпеки в сфері оборони і кібероборони, має складатися зі структурних підрозділів, які умовно можна визначити виходячи з функціональних завдань, а саме: моніторингу кіберпростору, захисту кіберпростору, активних дій у кіберпросторі, та вирішувати такі основні задачі:

участь у формуванні та реалізації державної політики з питань інформаційної, кібер-безпеки та кібероборони;

формування та реалізація політики Міністерства оборони України та Збройних Сил України щодо дій у кіберпросторі;

участь у виконанні заходів зі створення та розвитку інформаційних систем та ресурсів у Збройних Силах України;

координації дій суб'єктів інформаційної, кібер- безпеки та кібероборони Міністерства оборони та Збройних Сил України;

участь у формуванні стандартів підготовки та держзамовлення на підготовку фахівців з інформаційної, кібер- безпеки та кібероборони;

організації взаємодії та проведення заходів (в т.ч. щодо підготовки держави до кібероборони) зі структурними підрозділами інших центральних органів виконавчої влади, в рамках державно-приватного партнерства та міжнародними партнерами з питань кібербезпеки і кібероборони;

підтримання взаємодії з системою відомчих команд реагування на комп'ютерні інциденти (CERT/CSIRT);

планування та узгоджене управління діяльністю суб'єктів у кіберпросторі за єдиним замислом і планом. Контроль та координація їх дій;

моніторинг та аналіз кіберінцидентів, деструктивних інформаційних та когнітивних дій у кіберпросторі та ефективності дій системи кібербезпеки, виявлення уразливостей в інформаційних та кібер системах своїх і противника;

планування, організацію та координацію розвідувальних (Cyber Warfare Intelligence), оборонних (Defensive Cyber Warfare) і наступальних (Offensive Cyber Warfare) операцій в кіберпросторі (Cyberspace Operation) через кіберпростір та кібероперацій (Cyber Operation);

організацію та координацію інформаційних дій у кіберпросторі (включаючи соціальні мережі).

Наявність ефективної системи управління силами і засобами які діють в кіберпросторі забезпечить інформаційну, кібернетичну та когнітивну 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, санкцій, переконання і застосування сили та інших впливів способом, який є найбільш рентабельним та має політичну і соціальну легітимність.

Висновки. На підставі аналізу еволюції напрямків кібербезпеки та кібероборони, тенденцій розвитку науки і техніки запропоновано найбільш раціональний варіант створення систем і структур кібербезпеки та кібероборони зі структурами освіти та науки, які б відповідали зазначеним тенденціям розвитку, з урахуванням реальних військово-політичної обстановки, національних інтересів та законодавства.

В Україні питання формування системи кібероборони знаходиться у стадії вирішення. Відповідно до чинного законодавства 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, структурні підрозділи різного підпорядкування, що призводить до зниження ефективності виконання цих задач.

Спираючись на вищеперераховані принципи, для створення і розвитку системи кібероборони України доцільно:

1. Утворення та розгортання системи кібероборони держави здійснити шляхом комплексного та докорінного реформування сектору безпеки та оборони з оптимальним перерозподілом функцій, завдань, сил і засобів, ресурсів, та позбавлення від невластивих задач і функцій. Використовуючи при цьому дані аналізу результатів аудиту нормативно-правового забезпечення, ефективності виконання визначених нормативно-правовими актами функцій з використанням досвіду, найкращих підходів, технологій, методик та моделей апробованих в інших держав та тих, які довели свою ефективність та раціональність**.** Відповідно до [2, 30, 32, 33- 35] використовуючи досвід інших держав, досягти оперативних та інших спроможностей щодо удосконалення систем інформаційної і кібербезпеки, кібероборони та кіберзахисту власної інформаційної інфраструктури, забезпечення безпеки кіберпростору і соціокіберпростору та спільного захисту від кіберзагроз визначають співпрацю з НАТО, ЄС, гармонізацію з ними законодавства у цій сфері. Для України більш доцільною та ефективною, одночасно менш затратною, могла б бути німецька модель утворення Кіберсил, як самостійного виду Збройних Сил, включно систему наукового супроводження та підготовки кадрів. З точки зору бойового застосування кіберсил, більш ефективною могла б бути американська модель.

2. Здійснити заходи реформування, удосконалення і розвитку системи військової освіти і науки, зокрема в частині, що стосується розвитку системи підготовки та підвищення кваліфікації фахівців у сфері кібербезпеки та кібероборони. Система кіберосвіти має забезпечити утворення, розгортання та ефективне функціонування системи кібероборони держави та включати: завчасне формування вимог професійних стандартів до фахівців кібероборони; визначення держзамовника та прогнозованих кількісних показників держзамовлення; формування (реформування) військових науково-навчальних закладів в інтегрований освітньо-науковий, дослідно-випробувальний міжвидовий та міжвідомчий військовий заклад вищої освіти – військовий університет технологій, який забезпечить здійснення на єдиній базі освітньої і наукової діяльності за високотехнологічними напрямами; забезпечення їх розвитку та матеріального стимулювання фахівців з числа науково-педагогічного складу, ад’юнктів, докторантів, слухачів тощо.

ЛІТЕРАТУРА:

1. 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 - Press Release (2016) 100 Issued on 09 Jul. 2016 Last updated: 29 Mar. 2017 10:55 режим доступу: https://www.nato.int/cps/en/natohq/official_texts_133169.htm

2. Speech by NATO Secretary General Jens Stoltenberg at the Cyber Defence Pledge Conference (Ecole militaire, Paris). Режим доступу: https://www.nato.int/cps/en/natohq/opinions_154462.htm

3. Statement on the implementation of the Joint Declaration signed by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization. Режим доступу: https://www.nato.int/cps/en/natohq/official_texts_138829.htm.

4. С.Вдовенко, Ю.Даник, С.Фараон, “Дефініційні проблеми термінології у сфері кібербезпеки і кібероборони та шляхи їх вирішення”. Електронний журнал політики відкритого доступу “Комп’ютерні науки та кібербезпека” Харківського національного університету імені В.Н.Каразіна. SSN 2519-2310 (Online) №1 (12) 2019. С.18-30. Режим доступу: https://periodicals.karazin.ua/cscs/issue/view/803

5. Alexander Kosenkov. Cyber Conflicts as a New Global Threat file: Режим доступу: https://www.researchgate.net/scientific-contributions/2115250763_Alexander_Kosenkov

6. О.А.Баранов, Про тлумачення та визначення поняття “кібербезпека” “Правова інформатика”, № 2(42)/2014. – С. 54-62.

7. В.Л. Бурячок Кібернетична безпека – головний фактор сталого розвитку сучасного інформаційного суспільства / А.Л. Бурячок // Сучасна спеціальна техніка : зб. наук. праць. – 2011. – № 3 (26). – С. 104-114.

8. В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа (2015). В. Б. Толубко (загальна редакція). Інформаційна на кіберберзпека: соціотехнічний аспект./ В. Л. Бурячок, . – К.: ДУТ, 2015. – 288 с.

9. В. Л. Бурячок Основи формування державної системи кібернетичної безпеки: монографія / В. Л. Бурячок. – К.: НАУ, 2013. – 432 с.

10. В. Л.Бурячок, Г. М. Гулак, В. О. Дорошко. Завдання, форми та способи ведення воєн у кібернетичному просторі. Наука і оборона, № 3 2011. С.35-42.

11.Ю.І. Грицюк. Кіберінтервенція та кібербезпека України: проблеми та перспективи їх подолання, Науковий вісник НЛТУ України. – 2016. – Вип. 26.8 Національний лісотехнічний університет України Режим доступу:. http://nltu.edu.ua/nv/Archive/2016/26_8/52.pdf

12.Р.В. Грищук , Ю.Г.Даник. Основи кібернетичної безпеки. Монографія. вид. трете перероблене Житомир. ЖНАЕУ, 2016. – 636 с.

13.Д.В.Дубов. Кібербезпека: світові тенденції та виклики для України / Д.В. Дубов, М.А. Ожеван. – К.: Вид-во НІСД, 2011. – 30 с.

14.Д.В. Дубов. Стратегічні аспекти кібербезпеки України / Д.В. Дубов // Стратегічні пріоритети : наук.-аналіт. щокварт. зб. / Нац. ін-т стратег. дослідж. – К.: Вид-во НІСД. – 2013. – № 4 (29). – С. 119-126.

15.Д. В. Дубов. Кіберпростір як новий вимір геополітичного суперництва: монографія /– К. : НІСД, 2014. – 328 с.. Режим доступу: http://www.niss.gov.ua/content/articles/files/Dubov_mon-89e8e.pdf

16.Р.В. Лук'янчук. Державна політика у сфері забезпечення кібернетичної безпеки в умовах проведення антитерористичної операції / Р.В. Лук'янчук // Вісник НАДУ: зб. наук. праць. – 2015. – Вип. 3. – С. 110-116.

17.Р. В. Лук’янчук. Деякі питання реформування системи державного управління у сфері забезпечення кібернетичної безпеки: сучасний погляд / Р.В. Лук'янчук // Вісник НАДУ : зб. наук. праць. – 2013. – Вип. 2. – С. 81 -92.

18.В.В. Петров. Щодо формування національної системи кібербезпеки України / В.В. Петров // Стратегічні пріоритети: наук.-аналіт. щокварт. зб. / Нац. ін-т стратег. дослідж. – К. : Вид-во НІСД. – 2013. – № 4 (29). – С. 127–130.

19.В.П. Шеломенцев. Правове забезпечення системи кібернетичної безпеки України та основні напрями її удосконалення / В.П. Шеломенцев // Боротьба з організованою злочинністю і корупцією (теорія і практика) : зб. наук. праць. – 2012. – № 1(27). – С. 312-320.

20.М. Ю. Яцишин. Міжнародно-правова протидія кібервійнам / Яцишин М. Ю.//, збірник праць Національного авіаційного університету – 2015 – № 1 – С. 67-71

21.Putin’s asymmetric assault on democracy in Russia and Europe: implications for U.S. National security a minority staff report prepared for the use of the committee on foreign relations United States Senate one hundred fifteenth congress second session January 10, 2018 Available: Режим доступу: http://www.gpoaccess.gov/congress/index.html

22. J. Andress Cyber warfare: Techniques, tactics and tools for security practitioners / Andress J., Winterfeld S., Rogers R. – Amsterdam : Syngress/Elsevier, 2011. – 289 p

23. The Tallinn Manual on the International Law Applicable to Cyber Warfare 2.0. Tallinn 2016. Режим доступу - http://csef.ru/media/articles/3990/3990.pdf

24. Стратегія національної безпеки України, затверджена Указом Президента України від 26.05.2015 № 287/2015.

25. Конституція України [Електронний ресурс] – Режим доступу: http://zakon0.rada.gov.ua/laws/show/254

26. 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.

27. 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.

28. 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

29. Стратегія кібербезпеки України, затверджена Указом Президента України від 15.03.2016 № 96 // Офіц. вісн. України. – 2016. – № 23.

30. Ю.Даник, С.Вдовенко, Ланцюгові ефекти в кібердіях, К., ВІКНУ імені Т.Шевченка, Зб. наукових праць випуск №64, 2019, С. 71-90.

31. Концепція розвитку сектору безпеки і оборони України, введена в дію Указом Президента України від 14.03.2016 №92/201632. DOD. Joint Publication 3-12, Cyberspace Operations, 8 June 2018 Режим доступу: https://fas.org/irp/doddir/dod/jp3_12.pdf.

33. Statement by lieutenant general Paul M. Nakasone Commander, United States Army Cyber Command before the Subcommittee. Режим доступу: https://www.armed-services.senate.gov/imo/media/doc/Nakasone_03-13-18.pdf.

REFERENCES:

1. 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 -Press Release (2016) 100 Issued on 09 Jul. 2016 Last updated: 29 Mar. 2017 10:55 режим доступу: https://www.nato.int/cps/en/natohq/official_texts_133169.htm

2. Speech by NATO Secretary General Jens Stoltenberg at the Cyber Defence Pledge Conference (Ecole militaire, Paris). Режим доступу - https://www.nato.int/cps/en/natohq/opinions_154462.htm

3. Statement on the implementation of the Joint Declaration signed by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization. Режим доступу - https://www.nato.int/cps/en/natohq/official_texts_138829.htm.

4. Vdovenko,S Danik,Y and Faraon, S (2019), "Дефініційні проблеми термінології у сфері кібербезпеки і кібероборони та шляхи їх вирішення." [Definitive problems of the Terms of the Sphere of Cyber security and Cyber Defense and the Ways of their solution], International electronic scientific journal Computer Science and Cybersecurity Issue 1(12) 2019 ISSN 2519-2310 (Online).p.p.18-30 – Available:https://periodicals.karazin.ua/cscs/issue/view/803

5. Kosenkov,A Cyber Conflicts as a New Global Threat file, Available: https://www.researchgate.net/scientific-contributions/2115250763_Alexander_Kosenkov

6. Baranov,A (2014) "Pro tlumachennya ta vyznachennya ponyattya kiberbezpeka", [On the interpretation and definition of cyber security], "Pravova informatyka", [Legal Informatics], No. 2 (42) / 2014 - p. 54-62.

7. Buryachok,V (2011) "Kibernetychna bezpeka – holovnyy faktor staloho rozvytku suchasnoho informatsiynoho suspilstva", [Cybernetic security - the main factor for the sustainable development of a modern information society],"Suchasna spetsialna tekhnika ",[Modern special technique] sciences works, No. 3 (26), p. 104-114.

8. Buryachok,V, Tolubko,V, Khoroshko,V and Tolyupa,S. (2015) "Informatsiyna na kiberberzpeka: sotsiotekhnichnyy aspekt",[Information on cyber-security: the sociotechnical aspect], Kyiv, DUT, 288 p.p.

9. Buryachok,V (2013) "Osnovy formuvannya derzhavnoyi systemy kibernetychnoyi bezpeky",[Fundamentals of the formation of the state system of cybernetic security], a monograph , Kyiv: NAU, 432 pp.

10. Buryachok,V, Gulak,G and Doroshko,V. (2011) "Zavdannya, formy ta sposoby vedennya voyen u kibernetychnomu prostori", [Tasks, forms and methods of conducting wars in cybernetic spacious], "Nauka i oborona", [Science and Defense], № 3, p. 35-42.

11. Grytsuk, Yu. (2016) "Kiberinterventsiya ta kiberbezpeka Ukrayiny: problemy ta perspektyvy yikh podolannya" [Ciber iintervention and cyber security of Ukraine: problems and prospects for their overcoming], Naukovyy visnyk NLTU Ukrayiny, [Scientific Bulletin of NLTU of Ukraine], vol. 26.8 National Forestry University of Ukraine http://nltu.edu.ua/nv/Archive/2016/26_8/52.pdf.

12. Grishchuk, R and. Danyk Yu. (2016) "Osnovy kibernetychnoyi bezpeky"[The basics of cybernetic security], Monograph., Zhytomyr. ZHNAEU, 636 pp.

13. Dubov, D and Ozhevan,M (2011) "Kiberbezpeka : svitovi tendentsiyi ta vyklyky dlya Ukrayiny", [Cybersecurity. World Trends and Challenges for Ukraine], Kyiv,View NISD, 2011, 30 p.p.

14. Dubov,D (2013) "Stratehichni aspekty kiberbezpeky Ukrayiny" [Strategic Aspects of Cyber security of Ukraine], "Stratehichni priorytety" [Strategic Priorities: Sciences], Kyiv,View NISD, № 4 (29), p. 119-126.

15. Dubov,D (2014) "Kiberprostir yak novyy vymir heopolitychnoho supernytstva", [Cyberspace as a new dimension of geopolitical rivalry], Monograph, Kyiv, View NISD, 328 p.p, Access Mode: http://www.niss.gov.ua/content/articles/files/Dubov_mon-89e8e.pdf.

16. Lukyanchuk,R. (2015) "Derzhavna polityka u sferi zabezpechennya kibernetychnoyi bezpeky v umovakh provedennya antyterorystychnoyi operatsiyi" [State policy in the field of providing cybernetic security in the context of anti-terrorist operation], "Visnyk NADU" zb. nauk. prats, [Bulletin NADU] sciences works p. 110-116.

17. Lukyanchuk, R (2013) "Deyaki pytannya reformuvannya systemy derzhavnoho upravlinnya u sferi zabezpechennya kibernetychnoyi bezpeky: suchasnyy pohlyad" [Some issues of reforming the system of public administration in the field of cybernetic security: modern view], "Visnyk NADU" zb. nauk. prats, [Visnyk NADU] sciences works, Issue 2. - p. 81 -92.

18. Petrov,V (2013) "Shchodo formuvannya natsionalnoyi systemy kiberbezpeky Ukrayiny" [Concerning the National Cybersecurity System of Ukraine], nauk.-analit. zb. "Stratehichni priorytety", [Strategic Priorities] Science-analyst. every quarter save, Kyiv, View of NISS, No. 4 (29), p. 127-130.

19. Shelomentsev,V (2012) "Pravove zabezpechennya systemy kibernetychnoyi bezpeky Ukrayiny ta osnovni napryamy yiyi udoskonalennya" [Legal support of the system of cybernetic security of Ukraine and the main directions of its improvement], "Borotba z orhanizovanoyu zlochynnistyu i koruptsiyeyu (teoriya i praktyka)" zb. nauk. prats, [Fighting organized crime and corruption (theory and practice)] sciences works save. No. 1 (27). - P. 312-320.

20. Yatsyshyn, M. (2015) "Mizhnarodno-pravova protydiya kiberviynam" [International legal counteraction to cyberwarfaces], zbirnyk prats Natsionalnoho aviatsiynoho universytetu [The National Aviation University publication collection] № 1, p. 67-71.

21. Putin's asymmetric assault on democracy in Russia and Europe: implications for U.S. National security a minority staff report prepared for the use of the committee on foreign relations United States Senate one hundred fifteenth congress second session January 10, 2018 Available: http://www.gpoaccess.gov/congress/index.html

22. Andress, J., Winterfeld,S. and Rogers,R. (2011) "Cyber warfare: Techniques, tactics and tools for security practitioners" , – Amsterdam: Syngress/Elsevier, 2011. – 289 p.

23. The Tallinn Manual on the International Law Applicable to Cyber Warfare 2.0. Tallinn 2016. Available: http://csef.ru/media/articles/3990/3990.pdf

24. The National Security Strategy of Ukraine. [Stratehiia natsionalnoi bezpeky Ukrainy], approved by the Decree of the President of Ukraine dated 05/26/2015 № 287/2015.

25. Konstytucija Ukrajiny [The constitution of Ukraine] – Available: http://zakon0.rada.gov.ua/laws/show/254.

26. Zakon Pro oboronu Ukrajiny: za stanom na 01.07.2018 r. / zatverdzhenyj VR Ukrajiny vid 06.12.1991, # 1932-XII. [Law on Defense of Ukraine: as of 01.07.2018 /, approved by the Verkhovna Rada of Ukraine dated 06.12.1991, № 1932-XII] – Available: http://zakon4.rada.gov.ua/laws/show/1932-12

27. Zakon Ukrajiny Pro Zbrojni Syly Ukrajiny vid 6 ghrudnja 1991 roku N 1934-XII (zi zminamy) [Law of Ukraine On the Armed Forces of Ukraine of December 6, 1991 N 1934-XII (as amended)]. Available: http://zakon3.rada.gov.ua/laws/show/1934-12

28. Zakon Ukrayiny "Pro osnovni zasady zabezpechennya kiberbezpeky Ukrayiny" № 2163-VIII 10/05/2017, [Law of Ukraine "On the Basic Principles of Cybersecurity of Ukraine] No. 2163-VIII of October 5, 2017. Available: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi.

29. Stratehiia kiberbezpeky Ukrainy [The strategy cyber security of Ukraine.], of was approved by the Decree of the President of Ukraine dated March 15, 2016, No. 96/2016.

30. Danyk. Ju., Vdovenko S., Lancjughovi efekty v kiberdijakh [Chain effects of cyberspace action], K., VIKNU imeni T.Shevchenka, Zb. naukovykh pracj vypusk #64, 2019, S. 71-90.

31. Kontseptsiia rozvytku sektoru bezpeky i oborony Ukrainy [Concept of development of the security and defense sector of Ukraine], put into effect by the Decree of the President of Ukraine dated March 14, 2016, No. 92/2016.

32. DOD. Joint Publication 3-12, Cyberspace Operations, 8 June 2018. Available: https://fas.org/irp/doddir/dod/jp3_12.pdf.

33. Statement by lieutenant general Paul M. Nakasone Commander, United States Army Cyber Command before the Subcommittee. Available: https://www.armed-services.senate.gov/imo/media/doc/Nakasone_03-13-18.pdf

д.т.н., проф. Даник Ю.Г., Вдовенко С.Г.

ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ ОБЕСПЕЧЕНИЯ КИБЕРОБОРОНЫ ГОСУДАРСТВА

Возрастание роли и значимости решения задач кибербезопасности и кибероборонывызвано инновационным развитием информационных, электронных и кибертехнологий, которые являются движителем ряда тенденций в военном деле. Вследствие формирования и признания искусственного пятого пространства – киберпространства, отдельной сферой борьбы между государствами, включая вооруженное противоборство, вопросы кибербезопасности и киберобороны стали актуальными в обеспечении национальной безопасности и обороны развитых государств, которые особенное внимание уделяют формированию и развитию систем кибербезопасности и киберобороны, как головного фактора достижения военно-стратегического превосходства в обеспечении национальной безопасности и обороны в современных и перспективных условиях.

В статье проведено анализобщих принципов построения систем кибербезопасности и киберобороны передовых государств мира в контексте возможности и целесообразности внедрения их опыта в Украине; анализ условий, текущего состояния и проблемных вопросов формирования систем кибербезопасности и киберобороны в Украине. В частности, отсутствие основных теоретических и прикладных положений формирования системы киберобороны; отсутствие национального органа военного управления в сфере кибеообороны; рассредоточение усилий различных военно-организационных структур в решении задач кибербезопасности и отсутствие сформулированных задач киберобороны.

Предложен наиболее рациональный вариант создания систем и структур кибербезопасности и киберобороны Украины с подсистемами образования и науки, который в соответствии с современными тенденциями развития, с учетом военно-политической обстановки, национальных интересов и законодательства, обеспечит информационное, кибернетическое и когнитивное превосходство над противником и будет способствовать практической реализации принятой в странах НАТО концепции “смарт-обороны”.

Ключевые слова: кибератака, кибербезопасность, кибервлияние, кибердействия, киберзащита, кибероборона киберопераци, киберпространство, киберразведка, киберугроза, кибердар, система кибербезопасности, система киберобороны, субъекты кибербезопасности, субъекты киберобороны, объекты критической информационной инфраструктуры.

prof. Y. Danyk, S.Vdovenko

PROBLEMS AND PROSPECTS OF ENSURING A STATE CYBER DEFENSE

The growing role and importance of solving the problems of cybersecurity and cyber defense is due to the innovative development of information, electronic and cyber technologies, which are the driving force behind a number of trends in military affairs. Due to the formation and recognition of the artificial fifth space - cyberspace, as a separate area of struggle between states, including armed confrontation, issues of cybersecurity and cyber defense have become urgent in ensuring national security and defense of developed states, which pay special attention to the formation and development of cybersecurity and cyber defense systems as the main factor achievements of military-strategic superiority in ensuring national security and defense in modern variables and future conditions.

The article analyzes the general principles of building cybersecurity and cyber defense systems of the advanced states of the world in the context of the possibility and expediency of introducing their experience in Ukraine; analysis of the conditions, current status and problematic issues of the formation of cybersecurity and cyber defense systems in Ukraine. In particular: the lack of basic theoretical and applied provisions for the formation of a cyber defense system; lack of a national military command and control agency in the field of cyber defense; the dispersed efforts of various military organizational structures in solving cybersecurity problems and the lack of formulated cyber defense tasks.

The most rational option of creating systems and structures of cybersecurity and cyber defense of Ukraine with subsystems of education and science is proposed, which, in accordance with modern development trends, taking into account the military-political situation, national interests and legislation, will provide informational, cybernetic and cognitive superiority over the enemy and will contribute to the practical implementation of the concept of “smart defense” adopted in NATO countries.

Keywords: cyber action, cyber attack, cyber defense, cyber intelligence, cyber security, cyberspace, cyber operation, cyber threat, cyber security information infrastructure entities, cyber security infrastructure subjects.

УДК 004.056.53

к.т.н., с.н.с. **Лаптєв О.А.** (ДУТ)
к.ф.-м.н., доц. **Собчук В.В.** (ДУТ)
д.т.н., проф. **Савченко В.А.** (ДУТ)

DOI: https://doi.org/10.17721/2519-481X/2020/66-09

МЕТОД ПІДВИЩЕННЯ ЗАВАДОСТІЙКОСТІ СИСТЕМИ ВИЯВЛЕННЯ, РОСПІЗНАВАННЯ І ЛОКАЛІЗАЦІЇ ЦИФРОВИХ СИГНАЛІВ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

В процесі виявлення, розпізнавання, та локалізації сингалу засобів негласного отримання інформації в інформаційних системах актуальним питанням є підвищення завадостійкості. В статті досліджено особливості використання фільтрів низької частоти з квадратичною та лінійною залежністю відгуку від вхідного сигналу. Показано, що принцип роботи фільтрів полягає у тому, що виконується процес підсумовування. При цьому, корисний сигнал підсумовується когерентно, а сигнал завади – некогерентно, тобто корисний сигнал збільшується, а сигнал завади зменшується. Під час впливу на вхід лінійного та квадратичного фільтрів прямокутного імпульсу, який імітує сигнал сучасних цифрових засобів негласного отримання інформації, визначені необхідні для подальшого використання параметри вхідних та вихідних сигналів: математичне сподівання, коефіцієнт кореляції, дисперсія, середньоквадратичне відхилення, відношення сигналів до завад у часовому та спектральному вигляді. Обчислено коефіцієнт виграшу, який показує ефективність використання фільтрів низької частоти.

Наведено графіки огинаючої напруги на виході ідеального смугового фільтру при впливі на вхід прямокутного імпульсу з різною тривалістю – сигналу засобів негласного отримання інформації. Проведено моделювання процесу фільтрації при різних коефіцієнтах кореляції. Це підтвердило можливість виділення сигналу засобів негласного отримання інформації методом визначення двомірної щільності ймовірності сигналу завади на фоні загального сигналу.

Досліджується процес підвищення завадостійкості системи у цілому. Доведено, що використання у процесі обробки сигналів вузько-смугових фільтрів низької частоти дозволяє досягти підвищення завадостійкості системи визначення, розпізнавання та локалізації засобів негласного отримання інформації на 23 %.

Ключові слова: завадостійкість, фільтр, математичне сподівання, дисперсія, моделювання.

Вступ. Під завадою радіосигналу в роботі розуміється будь-який вид електричних коливань, який, проникаючи в радіоприймальні пристрої із зовні або виникаючи всередині його, ускладнює визначення радіосигналу. Сигнал і завада, одночасно діють на вході приймача, відтворюються на виході останнього у вигляді випадкового коливального процесу. В результаті цього неможливо точно визначити параметри сигналу. Нормальне визначення сигналу можливо тільки при певному співвідношенні потужності сигналу і завади на виході приймача. Найменша потужність сигналу, при якій забезпечується задовільне визначення сигналу, залежить від рівня завад. Ця величина потужності характеризує чутливість приймача. Здатність радіоприймального пристрою приймати із заданою якістю сигнал при наявності завад називається завадостійкістю. Покращення завадостійкості радіоприймальних пристроїв – одна з основних і найскладніших проблем радіотехніки. Для успішного вирішення її необхідно вивчити властивості та характер впливу завад на сигнал, а потім визначити способи ослаблення їх впливу на якість визначення сигналу.