УДК 004.4: 004.056.5 DOI: 10.26565/2519-2310-2019-1-02

ДЕФІНІЦІЙНІ ПРОБЛЕМИ ТЕРМІНОЛОГІЇ У СФЕРІ КІБЕРБЕЗПЕКИ І КІБЕРОБОРОНИ ТА ШЛЯХИ ЇХ ВИРІШЕННЯ

Сергій Вдовенко, Юрій Даник, Сергій Фараон

Національний університет оборони України імені Івана Черняховського, пр-т Повітрофлотський, 28, Київ, 03049, Україна
vsg64@ukr.net, zhvinau@ukr.net, faraon34@ukr.net

Рецензент: Олександр Кузнецов, д.т.н., проф., академік Академії наук прикладної радіоелектроніки, Харківський національний університет імені В.Н. Каразіна, майдан Свободи 6, Харків, 61022, Україна
kuznetsov@karazin.ua

Надійшло в лютому 2019

Анотація: *На підставі аналізу термінології сфери кібербезпеки та кібероборони, національних інтересів України в кіберпросторі та з урахуванням досвіду провідних країн світу, у статті розглянуті концептуальні підходи щодо врегулювання нормативно-правового поля і термінологічних систем національного сектору кібербезпеки та кібероборони держави.*

Ключові слова: *кібератака; кібербезпека; кібервплив; кіберконфлікт; кіберпростір; кіберзахист; кіберзагроза; кіберзброя.*

1 Вступ

Результатом стрімкого науково-технічного прогресу у сфері інформаційних технологій стало значне посилення ролі складних автоматизованих систем управління, які застосовуються у багатьох галузях діяльності людини, зокрема у військовій сфері, в тому числі – для управління військовими операціями та зброєю. Процеси функціонування таких систем відбуваються у сформованому новому віртуальному просторі – кіберпросторі, який доповнив існуючи: сухопутний, морський, повітряний, космічний, та став сферою конфліктів і можливих бойових дій [1,2]. При цьому відбувається зміна традиційних форм і способів ведення протиборства. Більше того, майбутня війна може бути спровокована в кіберпросторі.

Відомо, що війна та військовий конфлікт не є кінцевою метою, а лише силовим інструментом, за умов неможливості досягнення визначених політичних та/чи економічних цілей іншими способами.

У 2010 році 1-й командувач Кіберкомандування Сполучених Штатів Америки (США) генерал К. Александер відмічав: «Домінування в кіберпросторі, на відміну від, наприклад повітряного не розглядалося при військовому плануванні. доки нові технології не надали таку змогу» [3]. Розвиток сучасних технологій надає змогу досягти перемоги навіть без безпосереднього зіткнення бойових компонентів. Перенесення збройного протиборства в інформаційно-інтелектуальну й інформаційно-технічну сфери суттєво підвищує роль і значення кібероборони.

Концептуальні проблемні питання щодо загроз національній безпеці, зокрема у сфері інформаційної безпеки, окремі організаційно-правові засади протидії кіберзлочинності та боротьби з кібертероризмом досліджували О.А. Баранов [4], В.Л. Бурячок [5,6,7,8], Ю.І. Грицюк [9], Р.В. Грищук [10], Ю.Г. Даник. [10], Д.В. Дубов [11,12,13], Р.В. Лук'янчук [14,15], В.В. Петров [16], В.П. Шеломенцев [17], М.Ю. Яцишин [18] та інші.

Деякі технічні та правові аспекти проблем захисту військової інфраструктури від деструктивних, в тому числі кібервпливів, розглядалися іноземними та вітчизняними фахівцями. [4, 9,19,20].

Соціальні аспекти кіберконфліктів досліджувалися, зокрема, О. Косенковим, якій відмітив, що засоби кібервпливу це перші в історії людства засоби боротьби, які реально існують та застосовуються, але без повного розуміння і контролю. За його думкою слід відрізняти

соціальні аспекти кіберконфліктів від інформаційної війни в кіберпротсторі, а кіберконфлікти слід вважати найважливішим компонентом війни [21].

Проблеми кібероборони, з точки зору воєнно-політичного та воєнно-стратегічного аналізу розглядаються здебільш іноземними фахівцями, публікуються в офіційних виданнях саммітів НАТО (*North Atlantic Treaty Organisation* - Організація Північноатлантичного договору), але не мають юридичної сили та є лише поглядами відповідних фахівців [22,23].

Всі поточні дослідження не розглядають цілісний підхід до проблем кібероборони.

Сучасна геополітика вимагає цілеспрямованої активної діяльності держав, щодо пошуку ефективної моделі оперативного управління кібербезпекою та підвищення ролі і значення державних інституцій щодо створення ефективної системи кібероборони, та реалізації заходів з її забезпечення. Особливо актуально це в умовах ведення гібридних війн, кризових ситуацій, надзвичайного або воєнного стану.

2 Основна частина

В Україні для досягнення необхідних оперативних спроможностей сектору безпеки і оборони між іншими, визначені завдання щодо: удосконалення систем інформаційної і кібербезпеки, систем захисту інформації та безпеки інформаційних ресурсів; забезпечення інформаційної і кібербезпеки; посилення спроможностей зміцнення інституціональних та технічних можливостей суб'єктів сектору безпеки та оборони для ефективної боротьби із кіберзагрозами воєнного характеру, кібершпигунством, кібертероризмом та кіберзлочинністю; поглиблення міжнародного співробітництва у цій сфері; формування підрозділів забезпечення кібербезпеки та кіберзахисту Збройних Сил України (ЗСУ); здійснення міжвідомчої координації та взаємодії з цих питань в інтересах забезпечення обороноздатності держави; створення необхідних матеріально-технічних ресурсів для забезпечення здатності протидіяти іноземним технічним розвідкам, інформаційним, кібернетичним атакам, спецопераціям противника; створення ефективних сучасних зразків кіберзброї; розвиток мережі реагування на комп'ютерні надзвичайні події (CERT) [24,25].

Стратегія кібербезпеки України [26] пріоритетними заходами у сфері забезпечення кібербезпеки сектору безпеки і оборони визначає:

- здійснення воєнно-політичних, військово-технічних та інших заходів для розширення можливостей Воєнної організації держави, сектору безпеки і оборони у кіберпросторі;
- створення, розвиток сил, засобів та інструментів можливої відповіді на агресію у кіберпросторі, яка може застосовуватись як засіб стримування військових конфліктів та загроз у кіберпросторі (*активний кіберзахист*);
- створення єдиного підрозділу із забезпечення кібербезпеки та кіберзахисту ЗСУ на стратегічному, оперативному та тактичному рівнях;
- розвиток підрозділів кібербезпеки та кіберзахисту ЗСУ;
- розвиток науково-виробничого потенціалу та системи підготовки спеціалістів кібербезпеки та кібероборони для потреб органів сектору безпеки і оборони України.

Разом з тим, довгостроковими та середньостроковими планами України [27,28] передбачається здійснити удосконалення та розвиток системи кібербезпеки та захисту інформації шляхом створення в Міністерстві оборони України (МОУ), інших складових сектору оборони підрозділів з кіберзахисту, протидії технічним розвідкам, впровадження заходів із захисту інформації відповідно до вимог нормативно-правових актів України та з урахуванням стандартів НАТО і ISO/IEC, причому у ЗСУ переважно за рахунок реформування Головного управління зв’язку та інформаційних систем Генерального штабу ЗСУ. Притому, ряд заходів передбачених Планом [28] суперечить нормативно-правовому полю держави. Це в деякій мірі звужує спектр визначених Указами Президента України [24-26] завдань та не сприяє створенню системи кібероборони.

Виходячи з цього, необхідність побудови ефективної кібероборони слід розглядати через призму ризиків та загроз, що притаманні світові та насамперед для України у першій чверті XXI століття.

В січні 2018 року в Сенаті США здійснено доповідь [29], в якій відзначається, що з 2014 року кіберпростір України використовується в якості театру кібердій та полігону для випробовування кіберзброї, а кібератаки, як головний інструмент гібридної війни, направлені на всі сектори суспільства та економіки, зокрема такі як медіа, фінанси, транспорт, політика, енергетика і військова справа. Визнається необхідність використання такої ситуації для розуміння тактики й практики дій, прогнозування типів майбутніх кіберударів та відпрацювання ефективних заходів захисту від них, з одночасним наданням допомоги Україні в побудові оборонних сил. Співпраця з Україною щодо протидії цим загрозам вважається критично важливим елементом створення кібероборони США [29].

При цьому відверто заявлено, що США та їх європейські союзники залишаються вразливими до кібератак, які здійснюються переважно з застосуванням гібридної асиметричної зброї та це є загрозою для всіх держав. За наявності загроз кібератак для урядових та неурядових структур міжнародне співтовариство не розробило правил, які могли б встановити норми керівництва кібероборoною у довгостроковій перспективі. Держави НАТО не визначили критерії класифікації кібератак в контексті можливості застосування для колективного захисту статті 5 Північно-Атлантичного договору.

Констатовано, що уряд США не має інституцій, здатних активно залучати сили й допомагати неурядовим організаціям щодо протидії загрозам кібератак, крім обговорення можливостей щодо здійснення киберзагроз на стратегічному рівні. Визначено, що Уряд (США), спільно з державами-членами НАТО, повинен переглянути масштаби наслідків кібератак, не тільки як кримінальних загроз, але й як загроз національній безпеці, має збільшити обмін інформацією між їх розвідувальними та правоохоронними органами й розробити офіційні керівні принципи стосовно того, яким саме чином Альянс буде розглядати такі напади, у контексті статті 5 Північно-Атлантичного договору [29]. Слід зазначити, що необхідність вжиття перерахованих заходів була декларована США в липні 2016 року у підсумковому документі Варшавського саміту НАТО [1].

В вересні 2018 року президентом США Д. Трампом підписана Національна кіберстратегія США (*National Cyber Strategy of the United States of America*), на підставі якої, а також на підставі Стратегії національної безпеки США, в цьому ж місяці анонсована Кіберстратегія МО США (*Department of Defense Cyber Strategy*), що замінює Кіберстратегію 2015 року. Ця Стратегія має обмеження доступу, відомі лише її загальні цілі та задачі. На відміну від попередніх Стратегій, остання ґрунтується на взаємопов'язаних завданнях: зі створення більш руйнівної кіберсили, здатної конкурувати з противником та стримувати його дії в кіберпросторі; з реформування системи управління Кіберсилами; з розширення співробітництва в межах альянсу та з партнерами; з підтримки та розвитку талантів у кіберсфері. Згідно доповіді командувача Кіберкомандування США генерал-лейтенанта П. Накасоне перед підкомітетом з кіберзахисту Сенату, Кіберстратегія МО США визначає наступні пріоритети: підготовка простору операцій; висока готовність; ресурсне забезпечення; підготовка; партнерство. Всі вищезазначені Стратегії у своїй структурі мають глосарій, якій містить скорочення, абревіатури, терміни та визначення [30,31]. Включення або не включення дефініцій до глосаріїв Стратегій є підставою внесення або виключення їх до/зі Словника МО США *(DOD Dictionary of Military and Associated Terms)* [32], якій є затвердженою термінологією для застосування всіма суб'єктами МО США та має юридичну силу стандарту.

В розвиток доповіді [29] у лютому 2018 року Палата представників Конгресу США схвалила проект «Закону про співпрацю з Україною з питань кібербезпеки», що спрямований на просування активнішої взаємодії між Україною і США у сфері кібербезпеки в умовах протидії загрозам у всесвітній мережі Інтернет.

Стратегія [26] передбачає гармонізацію нормативних документів України у сфері кібербезпеки відповідно до міжнародних стандартів і стандартів ЄС та НАТО. При цьому дуже важливим індикатором готовності систем кібербезпеки та кібероборони держав-партнерів є досягнення визначеного рівня їх інтероперабельності.

Аналіз існуючих Законів України і інших нормативно-правових актів України та провід-

них країн світу, зокрема США, свідчить про дефініційну, термінологічну та нормативно-правову невизначеність або/та розбіжність об'єктно-предметної області декількох десятків понять, що складають базовий термінологічний набір терміносистеми сфери кібербезпеки та кібероборони, зокрема таких як: *– кібербезпека; – кіберзахист; – кіберзброя; – кібероборона; – кіберпростір; – кібертероризм* тощо.

Семантичне навантаження дефініції визначається описом об'єкту, предмету, їх ознак та взаємозв'язків між ними. Гармонізація термінології сфери кібербезпеки та кібероборони вимагає однакового тлумачення суті об'єкту та предмету.

Крім того, недостатньо з'ясовано масштаб та наслідки можливого застосування кібертероризму, а також сил кібербезпеки (кібервійськ, кіберсил) провідних країн, що формуються та набувають оперативних спроможностей на протязі останніх років, їх функції, завдання, зміст діяльності, склад, порядок підготовки підрозділів, військових і цивільних фахівців у цій сфері [33]. У цьому контексті можна стверджувати, що аналіз проблем нормативно-правового, науково-технічного, організаційного і кадрового забезпечення розвитку кіберсил є актуальним для створення в Україні національної системи кібербезпеки та кібероборони.

Для досягнення зазначеної мети слід оперувати чітко визначеними поняттями та критеріями оцінки небезпеки (загрозами), Розглянемо деякі з них.

Кіберпростір. Поняття "кіберпростір" (*cyberspace*) вперше використано у 1984 р. американським письменником Уільямом Гібсоном ("Нейромант") для позначення всієї сукупності інформації, що міститься у комп'ютерних мережах. Доктрина інформаційних операцій ЗС США 2006 р. (*JP 3-13 Information Operations Doctrine*) це підтверджувала: "Кіберпростір – віртуальна обстановка, в якій цифрова інформація циркулює в комп'ютерних мережах".

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".

З розвитком цифрових технологій поняття в англомовній сфері та у деяких російських виданнях розширилось до позначення сукупності всіх електронних систем.

Так, згідно [34] *кіберпростір* – сукупність користувачів, мереж, пристроїв, програмного забезпечення, процесів, збереженої або транзитної інформації, додатків, послуг та систем, які можуть бути прямо чи опосередковано під'єднані до мереж. Словник [32] визначає кіберпростір, як глобальний домен в інформаційному середовищі, що складається з взаємозалежних мереж інфраструктури, інформаційних технологій і резидентних даних, включаючи Інтернет, телекомунікаційні мережі, комп'ютерні системи та вбудовані процесори та контролери.

Натомість, Законом України [35] визначено, що кіберпростір - це середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних.

Тобто за кордоном кіберпростір розглядається як сфера діяльності складних технічних систем, а в Україні – складних соціотехнічних систем.

За поглядами окремих військових фахівців США домінування у кіберпросторі також виходить за рамки телекомунікаційних та інформаційних технологій і потребує переваги в усіх його складових: соціальній, технічній, телекомунікаційній, інформаційній, мережекомпьютерній тощо та по всьому електромагнітному спектру – "від постійного струму до денного світла, включаючи радіохвилі, інфрачервоне і рентгенівське випромінювання, спрямовану енергію, а також області, про які ще не почали навіть замислюватись, для забезпечення глобального командування і управління, глобального доступу і глобальної могутності"[36]. Тому, складовими кіберпростору слід вважати: інформаційний простір, комунікаційний простір, віртуальний комп'ютерно-мережний простір та соціотехнічний простір.

Розглядаючи сферу оборони (військовий аспект), визначимо, що кіберпростір – це єдиний простір сформований з інформаційного, комунікаційного, віртуального комп'ютерно-мережного та соціотехнічного просторів та об'єднаний системою зв'язків, в якому відбувається створення, зберігання, модифікація та передача інформації, управління об'єктами (системами) та зброєю, вплив на об'єкти (системи) протидіючої сторони, захист власних об'єктів (систем) в існуючих фізичних полях та середовищах.

Кібербезпека. Виходячи з дефініції "кібернетична безпека", єдиною і об'єднуючою ознакою в усі епохи розвитку людської цивілізації, яка однозначно характеризує явища та факти пов'язані з проблематикою її забезпечення, є безумовно ознака, яка визначає наявність систем та процесів управління. Виокремлення кібербезпеки в окремий вид безпеки сталося порівняно недавно. Вперше в світі в 1996 р. у військовій доктрині США "Concept Force XXI" на законодавчому рівні визнано необхідність захисту кіберпростору.

Так як проблема кібербезпеки носить глобальний характер, важливою є позиція міжнародних організацій. Так, Міжнародний союз електрозв'язку (ITU) [34,37] визначає що кібербезпека - це набір засобів, стратегії, принципи забезпечення безпеки, гарантії безпеки, керівні принципи, підходи до управління ризиками, дії, професійна підготовка, практичний досвід, страхування і технології, які можуть бути використані для захисту кіберсередовища, ресурсів організації та користувача. Загальні завдання безпеки у кіберсередовищі включають забезпечення ***доступності, цілісності, конфіденційності*** інформації. Глобальна програма [37] включає 5 стратегічних напрямів та 7 стратегічних цілей, що їх слід враховувати при створенні системи кібероборони, причому вимога щодо уніфікації глобального законодавства у сфері кібербезпеки розглядається як головна стратегічна ціль (див. Табл. 1).

За поглядами американських військових фахівців [38] до цього часу кібербезпека США розглядалася як комплекс заходів, спрямованих на захист комп'ютерів, електронних даних і мереж їх передачі від несанкціонованого доступу (конфіденційність), та інших дій, пов'язаних з маніпулюванням або крадіжкою, блокуванням (доступність), псуванням (спотворення), руйнуванням і знищенням (цілісність) умисного і випадкового характеру. Згідно Словника [32] виданого в січні 2019 року кібербезпека (безпека кіберпростору) - це дії, вжиті в захищеному кіберпросторі для запобігання несанкціонованому доступу, експлуатації або пошкодженню комп'ютерів, електронних систем зв'язку та інших інформаційних технологій, включаючи інформаційні технології платформи, а також інформацію, що міститься в ній, для забезпечення її доступності, цілісності, аутентифікації, конфіденційності і неспростовності. Зазначений приклад наведений з метою підтвердження зміни за останні три роки базового термінологічного апарату МО США в сфері кібербезпеки на 25-30%, що свідчить про гнучкість термінологічної системи сфери кібербезпеки США. Українське ж законодавство [39] комплекс цих заходів однозначно визначає як - ***технічний захист інформації*** (ТЗІ).

В Україні термін "кібербезпека" вперше використано у 2007 році [40], але лише в контексті необхідності "розробки та впровадження національних стандартів та технічних регламентів застосування інформаційно-комунікаційних технологій, гармонізованих з відповідними європейськими стандартами, у тому числі згідно з вимогами ратифікованої Верховною Радою України Конвенції про кіберзлочинність". З 2016 році кібербезпека України визначається як стан захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі [26]. Відповідно до Закону України [35], кібербезпека - захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі.

Тобто, іноземні фахівці розглядають кібербезпеку як комплекс заходів та засобів захисту складних технічних систем, у той час як в Україні кібербезпека визначається як стан захищеності людини, громадянина, а також складних соціотехнічних систем.

На погляд авторів, основними критеріями ефективності заходів щодо забезпечення кібербезпеки повинні бути критерії, що базуються на оцінці якості функціонування саме складних

соціотехнічних систем. Оскільки, якщо реалізація кіберзагроз навіть і призводить до порушення роботи комп'ютерних систем, але це майже не позначається на якості функціонування відповідної соціотехнічної системи, то гострота проблеми забезпечення кібербезпеки різко знижується.

Таблиця 1 – Стратегічні напрямки і цілі міжнародної програми кібербезпеки ITU

Стратегічні цілі \ Стратегічні напрямки		Стратегічні напрямки				
		Правові заходи	Технічні та процедурні заходи	Організаційні структури	Створення потенціалу	Міжнародне співробітництво
Стратегічні цілі	Розробка стратегій формування уніфікованого глобального законодавства сумісного з діючими національними та регіональними нормами законодавства.	+			+	+
	Розробка глобальних стратегій утворення національних й регіональних організаційних структур та політики боротьби з кіберзлочинністю.		+	+	+	+
	Розробка глобальних стратегій вироблення критеріїв безпеки та вимог щодо санкціонування використання апаратних засобів, програмних засобів та систем.		+		+	+
	Розробка стратегій міжнародної координації діяльності щодо утворення глобальних структур спостереження, оповіщення, реагування на інциденти		+	+	+	+
	Розробка глобальних стратегій щодо утворення та затвердження універсальної системи цифрової ідентифікації, а також організаційних структур для забезпечення визнання цифрових посвідчень особи без урахування географічних кордонів.	+	+	+	+	+
	Розробка глобальної стратегії сприяння утворенню людського та інституційного потенціалу для збільшення знань та ноу-хау стосовно всіх цілей та напрямків.	+	+	+	+	+
	Підготовка пропозицій щодо засад глобальної стратегій участі всіх зацікавлених сторін задля міжнародного співробітництва, діалогу та координації діяльності стосовно всіх цілей та напрямків.	+	+	+	+	+

Кіберзагроза. Загрози - будь-які обставини або події, що виникають у зовнішньому середовищі та можуть призвести до небезпеки. Історичний досвід розвитку людської цивілізації показує, що невід'ємною ознакою існування останньої є ризики та потенційні загрози, які існують навіть тоді, коли про них нічого невідомо.

Кіберзагрози, носять глобальний характер. Межі кіберпростору не визначаються державними кордонами, або іншими географічними бар'єрами. Географічні, кліматичні, часові характеристики, місцезнаходження, державна (коаліційна) належність, форма власності об'єктів тощо, не є стримуючими факторами для здійснення кібервпливу чи кібератак. Кіберзагрози можуть бути реалізовані будь-де та в будь-який час та за незначний проміжок часу нанести величезні збитки. Потенційно вразливими до кіберзагроз є життєво важливі сектори економіки (енергетика, транспорт), критично важливі об'єкти інфраструктури, об'єкти критичної інформаційної інфраструктури, національна телекомунікаційна мережа, національні

електронні інформаційні ресурси, системи: банківсько-фінансова та охорони здоров'я, сфера оборони тощо. Правових і технічних заходів на національному та регіональному рівнях недостатньо для того, щоб подолати ці глобальні загрози.

Стандарт ITU та Європейського союзу ISO/IEC 27000 визначає загрозу (*threat*) як потенційну причину небажаного інциденту, що може призвести до збитків системі або/та організації [41]. Законодавство України [35] визначає кіберзагрози як наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об'єктів.

В Україні визнано [25], що у середньостроковій перспективі намагання реалізації іноземними державами, міжнародними злочинними угрупованнями кіберзагроз щодо автоматизованих систем державного та військового управління, об'єктів критичної інформаційної інфраструктури залишаються серед найбільш актуальних. Серед чинників, що вливають на результати протидії кіберзагрозам воєнного, кримінального, терористичного та іншого характеру відмічається недостатня ефективність діяльності суб'єктів сектору безпеки і оборони України у цій сфері. Крім того, кіберзагрози в оборонній сфері законодавчо або підзаконними актами в Україні не визначені.

Проблема оцінки стану кібербезпеки повинна передусім розглядатися в нерозривному зв'язку з оцінкою можливих чи завданих збитків соціальним або соціотехнічним системам відповідно до потенційних або/та реалізованих загроз. Найбільш небезпечні виклики та загрози національній безпеці України в сфері кібербезпеки визначені в [42].

Ряд системних та управлінських проблем слід розглянути окремо, як такі, що не забезпечують належний рівень (*індекс*) кібербезпеки:

- відсутність системності ведення кібердій, теорії застосування сил та засобів кібероборони, взаємодії різних відомств у сфері забезпечення кібероборони держави;
- відсутність в секторі оборони єдиного координуючого органу з питань забезпечення кібербезпеки та системи підготовки військового й цивільного персоналу;
- проблеми кадрового забезпечення відповідних структурних підрозділів та відтік за кордон кваліфікованих спеціалістів;
- зниження рівня наукового потенціалу, відсутність наукових шкіл, складнощі із методичним, науковим і технічним забезпеченням відтік за кордон кваліфікованих наукових кадрів.

Вирішення вище перерахованих проблем неможливе без гармонізації та унормування термінологічних систем сфер кібербезпеки та кібероборони. На фоні не вирішення таких проблем, потенційні кіберзагрози можуть реалізуватися в успішні кібератаки на складні соціотехнічні системи держави, які призведуть до виникнення критичних ситуацій (у тому числі техногенних аварій та катастроф. Зокрема, це можуть бути:

- порушення управління державою та її інституціями шляхом здійснення деструктивних впливів на соціум (населення та політиків і керівників різного рівня з метою усунення та дискредитація осіб, які приймають рішення, формування негативної громадської думки про дії влади, спонукання населення до деструктивних дій тощо);
- використання глобальних інформаційних мереж терористичними та екстремістськими організаціями з метою організації терористичних актів, а також вербування нових бойовиків;
- несанкціоноване втручання в комп'ютерні мережі та системи управління органів державного та військового управління, стратегічно важливих об'єктів критичної інфраструктури, національних підприємств, управління військами та зброєю з метою отримання доступу до службової, конфіденційної або комерційної інформації, її викрадення, спотворення чи знищення, або/та взяття таких систем під контроль чи виведення їх з ладу.

Терміни ***кібератака, кіберзахист, кіберрозвідка, кібертероризм, кібершпигунство*** – розглядаються, як це визначено в Законі [35]. Ряд дефініцій, які відсутні або некоректні в нормативно-правовому полі України можуть, на погляд авторів, бути визначними так:

*Кібероборона***.** Дефініція виразу кібероборона вимагає розуміння, що ключовим словом є оборона, а кібер - це зазначення простору, де відбуваються дії сил протиборчих сторін.

Класичне військове мистецтво розглядає оборону як вид воєнних (бойових) дій військ (сил), в основі яких є захисні дії ЗС, їх об'єднань, частин та підрозділів.

За масштабом оборона може бути стратегічною, оперативною і тактичною. За типом організації – вимушеною або навмисною. За показниками активності – активною або пасивною.

Досвід всіх воєн та військових конфліктів свідчить, що успішною може бути тільки активна оборона з елементами наступальних та інших видів дій військ (сил). Активність оборони характеризується масовою часткою таких дій. За класифікацією простору ведення воєнних дій – наземна оборона, оборона морського узбережжя та морських комунікацій, протиповітряна, протикосмічна тощо. Відповідно до організації збройних сил та ступеню інтеграції управління можуть розглядатися і інші види оборони.

Враховуючи визнання кіберпростору п'ятою сферою ведення воєнних (бойових) дій кібероборона розглядається як сукупність політичних, економічних, соціальних, військових, наукових, науково-технічних, інформаційних, правових, організаційних та інших заходів, які здійснюються в кіберпросторі та спрямовані на забезпечення захисту суверенітету та обороноздатності держави, запобігання виникненню збройного конфлікту та відсіч збройній агресії [1,2,35]. На погляд авторів, законодавчо визначена дефініція потребує корегування. Цілком зрозуміло, що політичні, економічні, соціальні, правові, організаційні заходи, які спрямовані на досягнення мети кібероборони, здійснюються не в кіберпросторі. Доцільно запропонувати наступне визначення: Кібероборона – сукупність політичних, економічних, соціальних, військових, наукових, науково-технічних, інформаційних, правових, організаційних та інших заходів, які здійснюються в Державі та кіберпросторі й спрямовані на забезпечення захисту її суверенітету та обороноздатності, запобігання виникненню збройного конфлікту та відсіч збройній агресії.

За висновками американської компанії *Communications and Electronics Association* у книзі «The First Information War», виданої у 1992 році, застосування комп'ютерних мереж та високих технологій для управління логістикою в операції "Буря в пустелі" забезпечувало майже миттєвий обмін інформацією та змінило війну.

Кібервійна (війна у кіберпросторі) – складне суспільно-політичне явище, що відбивається в протиборстві непримиренних сторін в кіберпросторі з використанням кіберзброї, засобів кіберрозвідки, захисту або впливу для завдання матеріальних втрат (збитків) супротивнику і мінімізації особистих втрат (збитків) в економічній, військовій, політичній та ідеологічних сферах.

Кібервплив – сукупність реалізованих підрозділами кібероборони за єдиним замислом та під єдиним керівництвом одночасних або послідовних взаємопов'язаних за метою і завданнями кібератак та/або кіберударів, спрямованих на визначені елементи кіберпростору противника з метою порушення їх функціонування (стану), або - на елементи управління через кіберпростір з метою порушення процесів управління. Його складові: програмно-комп'ютерний вплив; фізичний вплив на органи і системи управління; радіоелектронне подавлення (ураження); інформаційно-психологічний вплив тощо.

Кіберзброя – сукупність технічних, програмних та інших засобів, призначених для здійснення деструктивних впливів на визначені елементи кіберпростору противника з метою виведення їх з ладу, або - на елементи управління через кіберпростір з метою порушення процесів управління.

Кібероперація – сукупність спланованих і реалізованих визначеними силами та засобами за єдиним замислом та під єдиним керівництвом одночасних або послідовних взаємопов'язаних за метою і завданнями кібератак та/або кіберударів, спрямованих на визначені елементи кіберпростору противника, або - на елементи управління через кіберпростір, з одночасним захистом власного кіберпростору від таких дій з боку противника.

Кіберудар – форма воєнних (спеціальних) дій підрозділів кібероборони спрямованих на реалізацію деструктивних (руйнівних) впливів на визначені елементи кіберпростору противника з метою їх блокування, знищення елементів інфраструктури, об'єктів, техніки та озброєння, руйнації циркулюючих в них даних і інформації, як в реальному так і в розподіленому

масштабі часу. За масштабами може бути стратегічного або оперативного рівня. За ступенем концентрації зусиль – поодинокий, масований. За вибором цілі – цільовий, груповий.

З 2011 року Положення Міжнародної стратегії кібербезпеки [38] розглядають кібератаки на критично важливу інфраструктуру як "акт війни", що підпадає під статтю 5 Північноатлантичного договору та дає юридичні підстави для удару у відповідь будь-якими засобами відповідно до ситуації, включно традиційними військовими. Словник [32] визначає кібероборону (оборону кіберпростору) як заходи, вжиті в захищеному кіберпросторі для подолання конкретних загроз, які порушили або загрожують порушенням заходів безпеки в кіберпросторі, і включають заходи щодо виявлення, визначення типів та характеристик загроз (включно шкідливе програмне забезпечення або несанкціоновані дії користувачів), протидії їм та мінімізації їх наслідків, приведення систем до безпечної конфігурації.

З урахуванням широкого застосування сучасних інформаційних технологій у секторі безпеки і оборони, створення єдиної автоматизованої системи управління ЗСУ оборона держави стає більш уразливою до кіберзагроз [2].

Згідно Законів [43,44] оборона України, захист її суверенітету, територіальної цілісності і недоторканності, охорона повітряного простору та підводного простору держави покладаються на ЗС України. Однак жодним Законом України кіберпростір не визначений, як середовище ведення оборонних дій для забезпечення захисту суверенітету держави. Натомість Закон України [35] встановлює, що національна система кібербезпеки включає в тому числі й оборонні заходи, а також визначає МО України та Генеральному штабу ЗС України завдання щодо підготовки держави до відбиття воєнної агресії у кіберпросторі (кібероборони); військової співпраці з НАТО та іншими суб'єктами оборонної сфери щодо забезпечення безпеки кіберпростору та спільного захисту від кіберзагроз, забезпечення кіберзахисту критичної інформаційної інфраструктури в умовах надзвичайного і воєнного стану.

Стратегія [26] визначає МО України, Генеральному штабу ЗС України завдання щодо здійснення заходів з підготовки держави до відбиття воєнної агресії у кіберпросторі (кібероборони) та кіберзахисту власної інформаційної інфраструктури. Закон України (зі змінами) [45] визначає обов'язковість здійснення заходів з кібероборони (активного кіберзахисту) для захисту суверенітету держави та забезпечення її обороноздатності, запобігання збройному конфлікту та відсічі збройній агресії, у тому числі - проведення спеціальних операцій (розвідувальних, інформаційно-психологічних тощо) у кіберпросторі при підготовці до захисту та захисту України в разі збройної агресії.

А ні законами України, а ні іншими нормативно-правовими актами не визначено перелік вичерпних заходів щодо підготовки до відбиття та відбиття воєнної агресії у кіберпросторі. Тому, для досягнення мети та безпосереднього виконання заходів у сфері забезпечення кібербезпеки сектору безпеки і оборони, визначених в [24, 25, 26, 32, 35, 45] необхідно стандартизувати та гармонізувати в нормативно-правовому полі України дефініції термінологічних систем сфери кібербезпеки та кібероборони.

Операція формування значення для терміну, дефініція (лат. *definitio* - визначення), є важливим засобом описів та міркувань у наукових теоріях та галузях знань, чим виконує важливу функцію у науково-освітній та практичній діяльності [46].

В термінології, як розділі лексикології, аксіомою є, що визначення будь якого терміну (дефінієндума) та зміст і значення визначаючого поняття (дефінієнса) мають бути тотожними, вичерпувати один одного і мати один і той же зміст (денотат). До науково-технічних термінів висуваються додаткові вимоги: системність, вмотивованість, однозначність, точність, відсутність синонімів [47].

З певних історичних, воєнно-наукових, зовнішньополітичних та інших причин в термінологічній системі галузі кібербезпеки та кібероборони України, склалося протиріччя, що вимагають відповідного наукового розв'язання. Воно полягає в недотриманні в термінографії сфери кібербезпеки принципів однозначності, точності та відсутності синонімів. А саме, у терміносистемі сфери кібербезпеки одночасно існує й паралельно застосовується низка дефініцій, в яких одному дефінієндуму (Dfd) ставиться у відповідність декілька дефінієнсів (Dfn),

або навпаки, один дефінієнс розкриває значення різних дефінієндумів. Термінологічна сфера кібероборони в Україні ще не сформована, тим не менш, процесу її формування притаманні ті ж самі помилки. Ускладнення цього протиріччя в площині практичного застосування термінологічного апарату сфери кібербезпеки та кібероборони відбувається за рахунок невідповідності термінологічних систем сфер кібербезпеки міжнародного співтовариства, зокрема ЄС та НАТО й України.

Вирішення протиріччя полягає у формуванні за правилами науково-технічної лексикографії множини семантичних аналітичних та синтетичних визначень термінологічної системи сфери кібербезпеки та кібероборони. Автори вважають за можливе організацію та виконання даної роботи здійснити за наступним алгоритмом:

1. Вибір термінів та їх дефініцій з множини ключового набору термінів термінологічних систем сфер кібербезпеки та кібероборони

2. Збір максимальної кількості вживаних конкретних дефініцій кожного терміну терміносистеми, включно з іноземних офіційних джерел міжнародних організації та країн-партнерів

3. Аналіз кожної дефініції:

- на системність – то б то належність терміна до певної термінологічної системи; за результатом – виключення зайвих термінів;
- на відсутність синонімів; за результатом – виключення зайвих термінів, що в межах одній терміносистеми, забезпечує запобігання взаємному непорозумінню фахівців;
- на однозначність, тобто на тотожність тільки одного наукового або технічного терміну Dfd та відповідного йому поняття Dfn; за результатом – виключення зайвих термінів;
- на точність – при чому слід з’ясувати чому виникло занадто широке значення змісту (надлишковість) або занадто вузьке визначення;
- на вмотивованість, то б то спроможність передати змістовне навантаження без додаткового застосування термінологічного словника.

4. Декомпозиція обраних для подальшої роботи термінів.

5. Композиція однозначних нових дефініцій термінів. При чому, дефініція кожного нового словосполучення (складного терміну) має містити дефініційні ознаки кожного слова складного терміну, які мають формувати дефініцію складного терміну. При цьому складний термін має формувати нові властивості притаманні тільки йому.

6. Аналіз нової дефініції терміну на вмотивованість, точність, однозначність, відсутність синонімів, системність.

7. Порівняльний аналіз на точність та вмотивованість синтезованої дефініції терміну з аналогом міжнародної терміносистеми в даній сфері

8. Формування пропозицій щодо включення термінів до фахових термінологічних словників.

9. Формування пропозицій щодо гармонізації нормативних документів України у сфері кібербезпеки та кібероборони відповідно до міжнародних стандартів і стандартів ЄС та НАТО.

3. Висновки

У роботі проведений аналіз термінології сфери кібербезпеки і кібероборони та розглянуті концептуальні підходи щодо врегулювання нормативно-правового поля та термінологічних систем національного сектору кібербезпеки, та кібероборони держави.

Запропоновано алгоритм формування множини семантичних аналітичних і синтетичних визначень термінологічної системи сфери кібербезпеки та кібероборони, що враховує правила науково-технічної лексикографії.

Сформульовані рекомендації щодо усунення визначених невідповідностей шляхом нормативно-правового й дефініційного врегулювання понятійного апарату у сфері кібербезпеки та кібероборони.

Визначені напрями подальших досліджень, що пов'язані з формуванням остаточного переліку функцій та завдань суб'єктів кібероборони, систем управління, їх взаємозв'язків, критеріїв (індикаторів) загроз у сфері кібероборони держави.

Посилання

[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. URL: https://www.nato.int/cps/en/natohq/official_texts_133169.htm

[2] Стратегія національної безпеки України, затверджена Указом Президента України від 26.05.2015 № 287/2015. URL: https://zakon.rada.gov.ua/laws/show/287/2015

[3] Keith A. Statement for the Record, Commander, US Cyber Command: House Armed Services Committee Statement. (Washington, DC. 23 September 2010). URL: https://www.govinfo.gov/content/pkg/CHRG-111hhrg62397/pdf/CHRG-111hhrg62397.pdf

[4] Баранов О.А. Про тлумачення та визначення поняття "кібербезпека". *Правова інформатика.* 2014. № 2(42). С. 54 – 62.

[5] Бурячок В. Л. Основи формування державної системи кібернетичної безпеки: монографія. Київ: НАУ, 2013. 432 с.

[6] Бурячок В.Л. Кібернетична безпека – головний фактор сталого розвитку сучасного інформаційного суспільства. *Сучасна спеціальна техніка* : зб. наук. праць. 2011. № 3 (26). С. 104 – 114.

[7] Інформаційна на кіберберзпека: соціотехнічний аспект / Бурячок В. Л., Толубко В. Б., Хорошко В. О., Толюпа С. В. Київ: ДУТ, 2015. 288 с.

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

[9] Грицюк Ю.І. Кіберінтервенція та кібербезпека України: проблеми та перспективи їх подолання. *Науковий вісник НЛТУ України*. 2016. Вип. 26.8. URL: http://nltu.edu.ua/nv/Archive/2016/26_8/52.pdf

[10] Грищук Р.В., Даник Ю.Г. Основи кібернетичної безпеки: монографія. Житомир: ЖНАЕУ, 2016. 636 с.

[11] Дубов Д.В., Ожеван М.А. Кібербезпека: світові тенденції та виклики для України. Київ: Вид-во НІСД, 2011. 30 с.

[12] Дубов Д.В. Стратегічні аспекти кібербезпеки України. *Стратегічні пріоритети*: наук.-аналіт. щокварт. збірник Нац. ін-т стратег. дослідж. 2013. № 4 (29). С. 119–126.

[13] Дубов Д. В. Кіберпростір як новий вимір геополітичного суперництва: монографія. Київ: НІСД, 2014. 328 с. URL: http://www.niss.gov.ua/content/articles/files/Dubov_mon-89e8e.pdf

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

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

[16] Петров В.В. Щодо формування національної системи кібербезпеки України. *Стратегічні пріоритети*: наук.-аналіт. щокварт. збірник Нац. ін-т стратег. дослідж. 2013. № 4 (29). С. 127–130.

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

[18] Яцишин М. Ю. Міжнародно-правова протидія кібервійнам. *Збірник праць Національного авіаційного університету*. 2015. № 1. С. 67 – 71.

[19] Вдовенко С.Г., Даник Ю.Г. Концептуальні напрями комплексного вирішення проблеми захисту інформації в системі скритого управління Збройних сил. *Сучасні інформаційні технології у сфері безпеки та оборони.* 2017. № 2(29). С. 98 – 106.

[20] Вдовенко С.Г., Даник Ю.Г. Концептуальні напрямки комплексного вирішення проблеми захисту від несанкціонованого доступу в складних системах спеціального призначення. URL: http://epsi.vntu.edu.ua/uploads/2017/61-f1s0m4m1jhvk8ix2vjd81nyxuzb1i3q9.pdf

[21] Kosenkov A. Cyber Conflicts as a New Global Threat file. URL: futureinternet-08-00045.pdf

[22] Andress J., Winterfeld S., Rogers R. 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. URL: http://csef.ru/media/articles/3990/3990.pdf

[24] Стратегія національної безпеки України, затверджена Указом Президента України від 26.05.2015 № 287/2015. *Урядовий кур'єр*. 2015. № 95. URL: http://zakon.rada.gov.ua/287/2015

[25] Концепція розвитку сектору безпеки і оборони України, затверджена Указом Президента України від 14.03.2016 №92/2016. URL: https://zakon.rada.gov.ua/laws/show/92/2016

[26] Стратегія кібербезпеки України, затверджена Указом Президента України від 15.03.2016 № 96. *Офіційний вісник України*. 2016. № 23.

[27] Стратегічний оборонний бюлетень України, введений в дію Указом Президента України від 06.06.2016 № 240/2016 URL: https://www.president.gov.ua/documents/2402016-20137

[28] План дій щодо впровадження оборонної реформи у 2016 - 2020 роках (дорожня карта оборонної реформи), затверджений Міністром оборони України 15.08.2016. URL: http://www.mil.gov.ua/diyalnist/reformi-ta-planuvannya-u-sferi-oboroni/22082016-04.html; http://www.mil.gov.ua/content/tenders/Plan_2208.pdf

[29] 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 . URL: http://www.gpoaccess.gov/congress/index.html

[30] DOD. Joint Publication 3-12, Cyberspace Operations, 8 June 2018. URL: 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. URL: https://www.armed-services.senate.gov/imo/media/doc/Nakasone_05-23-17.pdf

[32] DOD Dictionary of Military and Associated Terms. As of January 2019. URL: https://www.jcs.mil/Portals/36/Documents/ Doctrine/pubs/dictionary.pdf

[33] Мазулевський О.В., Вдовенко С.Г. Огляд підходів дій кібернетичних сил держав світу. *Перспективи розвитку озброєння і техніки сухопутних військ*: збірник тез доповідей Міжнародної науково-технічної конференції. Львів: НАСВ, 2018.С.220. URL: http://repositsc.nuczu.edu.ua/bitstream/123456789/7088/1/17-18-05-2018_zb_tez_dop.pdf

[34] Рекомендация МСЭ-Т X.1205. Обзор кибербезопасности. Женева: МСЕ, 2010. С. 55. URL: www.itu.int/ITU-T/recommendations/rec.aspx?rec=9136&lang=ru

[35] Закон України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII від 5 жовтня 2017 року. URL: https://zakon.rada.gov.ua/laws/show/2163-19

[36] Secretary of State Hillary Rodham Clinton On the Release of President Obama Administration's International Strategy for Cyberspace. May 16, 2011. URL: http://www.state. gov/secretary/rm/2011/05/163523.htm

[37] ITU Global Cybersecurity Agenda (GCA) A Framework for International Cooperation in Cybersecurity. URL: https://www.intgovforum.org/Substantive_2nd_IGF/ITU_GCA_E.pdf

[38] International Strategy For Cyberspace: Prosperity, Security and Openness in a Networked World. Washington DC: The White House, May 2011. URL: http://www.whitehouse.gov/sites/default/files/rss_viewer/internationalstrategy_ cyberspace.pdf.

[39] Про захист інформації в інформаційно-телекомунікаційних системах: Закон України. URL: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi

[40] Стратегія національної безпеки України, затверджена Указом Президента України від 12.02.2007 № 105/2007 в редакції Указу Президента України від 8.06.2012 року № 389/2012 . URL: https://zakon.rada.gov.ua/laws/show/105/2007

[41] Рекомендації міжнародного союзу електрозв'язку. МСЕ-Т.Сер.Х.1208. Мережі передачі даних, взаємозв'язок відкритих мереж та безпека. Безпека кіберпростору – кібербезпека. 2014 р. ISO/IEC 27000. URL: https://www.itu.int/itu-t/recommendations/rec.aspx?rec=11950&lang=ru

[42] Кібербезпека: українські реалії. URL: http://timeua.info/post/oborona-i-bezopasnost/k-berbezpeka-ukra-ns-k--real--07454.html

[43] Конституція України. URL: http://zakon0.rada.gov.ua/laws/show/254

[44] Про Збройні Сили України: Закон України від 6 грудня 1991 року N 1934-XII (зі змінами). URL: http://zakon3.rada.gov.ua/laws/show/1934-12

[45] Про оборону України: Закон України станом на 01.07.2018 р., затверджений ВР України від 06.12.1991, № 1932-XII . URL: http://zakon4.rada.gov.ua/laws/show/1932-12

[46] Новейший философский словарь. URL:https://www.google.com/search?q=chrome.69i57.9536j0j8&sourceid=chrome&ie=UTF-8

[47] Васенко Л.А., Дубічинський В.В., Кримець О.М. Фахова українська мова: Навч. посібник. Київ: Центр навчальної літератури, 2008. 272 с. URL: http://uchebniks.com/book/277-faxova-ukrayinska-mova-navchalnij-posibnik-vasenko-la/23-vimogi-do-terminiv.html

Reviewer: Alexandr Kuznetsov, Doctor of Technical Sciences, Prof., Academician of the Academy of Sciences of Applied Radio Electronics, V. N. Karazin Kharkiv National University, 6 Svobody Sq., Kharkiv, 61022, Ukraine.
E-mail: kuznetsov@karazin.ua

Received: February 2019.

Authors:

Serhii Vdovenko, Colonel, Associate Professor of the Department of Communication and Automated Control Systems of the Institute of Information Technologies of the National University of Defense named after Ivan Chernyakhovsky, Kyiv, Ukraine.
E-mail: vsg64@ukr.net

Yury Danik, Major general, Doctor of Sciences (Eng.), Full Prof., Head of the Institute of Information Technologies of the National University of Defense named after Ivan Chernyakhovsky, Kyiv, Ukraine.
E-mail: zhvinau@ukr.net

Serhii Faraon, Colonel, Adjunct of the Scientific Department of the Organization of Training and Attestation of Scientific and Pedagogical Staff of the Scientific and Methodological Center for the Organization of Scientific and Scientific-Technical Activity of the National University of Defense of Ukraine named after Ivan Chernyakhovsky, Kyiv, Ukraine.
E-mail: faraon34@ukr.net

Definitive problems of the Terms of the Sphere of Cyber security and Cyber Defense and the Ways of their solution.

Abstract. Based on cybersecurity terminology analysis and cyber defense, national interests of Ukraine in cyberspace and taking into account the experience of leading countries of the world, the article discusses conceptual approaches to resolving the regulatory and definitive field in the state cyberdefense sector.

Keywords: Cyberattack; Cybersecurity; Cyberimpact; Cyberconflict; Cyberdefense; Cyberspace; Cyberthreat; Cyberweapons.

Рецензент: Александр Кузнецов, д.т.н., проф., академик Академии наук прикладной радиоэлектроники, Харьковский национальный университет имени В. Н. Каразина, пл. Свободы 6, Харьков, 61022, Украина.
E-mail: kuznetsov@karazin.ua

Поступила: Февраль 2019.

Авторы:

Сергей Вдовенко, полковник, доцент кафедры связи и автоматизированных систем управления Института информационных технологий Национального университета обороны Украины имени Ивана Черняховского, Киев, Украина.
E-mail: vsg64@ukr.net

Юрий Даник, генерал-майор, доктор технических наук, профессор, начальник института информационных технологий Национального университета обороны Украины имени Ивана Черняховского, Киев, Украина.
E-mail: zhvinau@ukr.net

Сергей Фараон, полковник, адъюнкт научного отдела организации подготовки и аттестации научно-педагогичных кадров научно-методического центра организации научной и научно-технической деятельности Национального университета обороны Украины имени Ивана Черняховского, Киев, Украина.
E-mail: faraon34@ukr.net.

Дефинитивные проблемы терминологии в сфере кибербезопасности и кибероборонь и пути их решения.

Аннотация. На основании анализа терминологии сферы кибербезопасности и кибероборонь, национальных интересов Украины в киберпространстве и с учетом опыта ведущих стран мира, в статье рассмотрены концептуальные подходы по урегулированию нормативно-правового и дефинитивного поля сектора кибероборонь государства.

Ключевые слова: кибератака; кибербезопасность, кибервлияние; киберконфликт; киберпространство; киберзащита; киберугроза; кибероружие.