ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

УДК 006.013

Вдовенко С.Г. (НУОУ)
к.н.держ.упр. **Живило Є.О.** (НУОУ)
Черноног О.О. (МОУ)
Докіль В.М. (НУОУ)

DOI: https://doi.org/10.17721/2519-481X/2022/74-06

АНАЛІЗ ОСОБЛИВОСТЕЙ ФУНКЦІОНУВАННЯ СИСТЕМИ КІБЕРОБОРОНИ. НОРМАТИВНО-ПРАВОВІ АСПЕКТИ

Актуальність данної роботи обумовлена одним із пріоритетів системи національної безпеки України по виконанню функцій і завдань сил оборони України в умовах деструктивної активності на кібербезпекове середовище держави.

Сучасний розвиток інформаційних і кібертехнологій та глобальна інформатизація у світі призвели до того, що інформаційна та кіберсфери стали об'єктом різноманітних деструктивних впливів на усі сфери діяльності суспільства через кіберпростір, який доповнив існуючі, а саме сухопутний, морський, повітряний, космічний, та став сферою конфліктів і можливих бойових дій.

Держави, в залежності від ступеню їх розвитку, по різному будують системи (моделі) захисту своїх інформаційних, телекомунікаційних інфрастуктур, визначають порядок використання технологічних процесів, які циркулюють в зазначених системах та здійснюють захист об'єктів критичної інфраструктури від кіберзагроз, визначають функції, напрями та способи дій у кіберпросторі. На сьогодні в світі більш ніж 60 держав відкрито або/та приховано провадять діяльність щодо підвищення рівня функціональності національних систем кібербезпеки та кібероборони. Йде створення національних та коаліційних кіберсил, визначаються їх функції, завдання, формуються зміст та порядок діяльності, склад, алгоритми підготовки підрозділів, військових і цивільних фахівців, розробляються стратегії, вдосконалюється нормативно-правова база, апаратно-програмні комплекси, спеціальне-програмне забезпечення для кібероборони та тактики їх застосування.

В цілому, розвиток та широке впровадження систем і комплексів зв'язку з використанням інноваційних інформаційних та телекомунікаційних технологій в системах військового призначення відбувається у відповідності до міжнародних правил ведення кібервійн на зразок Женевської конвенції. При цьому основними принципами формування систем кібербезпеки і кібероборони провідних країн світу є науково обґрунтовано законодавче, нормативно-правове, дефініційно-термінологічне супроводження. За цих умов трансформування нормативно-правової бази відбувається з врахуванням постійної мілітарізації національних сегментів кіберпростору з врахуванням критеріїв (індикаторів) загроз у сфері кібербезпеки та кібероборони провідних держав, рівня готовності систем та набуття відповідних спроможностей, тощо.

Для вирішення завдань, щодо врегулювання та імплементації норм та правил міжнародних організацій сфери кібербезпеки та кібероборони пропонується провести аналіз чинних положень (аксіоматик) існуючої законодавчої, державної та відомчої нормативно-правової бази, а також нормативно-правового поля міжнародних організацій (Європейский Союз, НАТО, ITU) щодо забезпечення кібербезпеки.

Ключові слова: кіберпростір, кібербезпека, кібероборона, закон України, нормативно – правова база, нормативно-правовий акт, об'єкт критичної інформаційної інфраструктури.

Вступ та постановка задачі. Вимогами рішення Ради національної безпеки і оборони України від 14 травня 2021 р. "Про невідкладні заходи з кібероборони держави", введеного в дію Указом Президента України від 26 серпня 2021 р. № 446 та у відповідності до вимог схваленого на засіданні Кабінету Міністрів України Плану організації виконання рішення Ради національної безпеки і оборони України від 14 травня 2021 р. "Про невідкладні заходи з кібероборони держави", введеного в дію Указом Президента України від 26 серпня 2021 р. №

446 передбачено нормативне визначення та включення до системи операцій Збройних Сил України (далі – ЗС України) сучасних форм і способів дій військ (сил) у кіберпросторі та через кіберпростір, ведення ними кібероборони.

У цьому контексті вбачається, що система кібероборони буде орієнтована на набуття необхідних спроможностей суб'єктами підготовки та здійснення заходів кібероборони, створення і розвиток сил, засобів та інструментів протиборства в кіберпросторі та через кіберпростір, які забезпечать створення необхідного потенціалу сил оборони для відбиття воєнної агресії в кіберпросторі.

За цих умов постає доволі суттєва проблема, щодо вдосконалення державних механізмів регулювання проведення узгоджених дій силами оборони зі здійснення цифрової трансформації, впровадження сучасних технологій автоматизації управління військами та зброєю, моніторингу, аналізу інформації, моделювання, експертних систем, спеціального програмного забезпечення та інформаційних систем.

Також, доволі змістовним питанням постає розробка нового, трансформація та вдосконалення існуючого нормативно-правового поля щодо формування та використання єдиного інформаційного середовища сил оборони шляхом застосування єдиних стандартів, протоколів, архітектур (проектних рішень), надання необхідних сервісів та повноцінного використання інформаційних ресурсів, спрямованих на ефективне застосування сил оборони під час проведення операцій сил оборони (операцій об'єднаних сил).

Запровадження системної, нормативно врегульованої взаємодії складових сил оборони в подальшому надасть їм змоги досягти військових критеріїв сумісності, необхідних для інтеграції України в євроатлантичні та європейські безпекові структури, здійснити взаємодію та співробітництво зі збройними силами держав - членів НАТО та держав - партнерів НАТО.

Отже, удосконалення існуючої нормативно-правової бази (далі – НПБ), підготовка проектів нормативно-правових актів (далі – НПА), нормативне врегулювання питань з реалізації заходів, що забезпечують якісне проведення розрахунків потреб з обсягу матеріально-технічних та фінансових ресурсів, необхідних для створення і забезпечення належного функціонування кібервійськ, комплектування особовим складом кібервійськ з урахуванням оптимального співвідношення військовослужбовців, працівників Міністерства оборони України (далі – МО України), а також зарахованих у запас, резервістів та інших категорій осіб є важливим практичним та науковим завданням.

Аналіз останніх досліджень. Аналіз існуючої НПБ щодо створення та функціонування системи кібербезпеки та кібероборони (далі – КБ та КО) в інформаційно-телекомунікаційних системах військового призначення (далі – ІТС ВП) свідчить про те, що Національна система кібербезпеки, одним із трьох завдань якої є кіберзахист державного інформаційного ресурсу**,** створюється і розвивається відповідно до Конституції України, законів України (далі – ЗУ) та інших НПА, що регулюють суспільні відносини у сфері національної безпеки, оборони, інформаційної та кібербезпеки і захисту інформації. Виходячи з цього, системи кіберзахисту в ІТС ВП також створюються та функціонують відповідно до вимог законів та НПА України, а саме:

Законів України: "Про національну безпеку України" [4]; "Про основні засади забезпечення кібербезпеки України" [5]; "Про захист інформації в інформаційно-телекомунікаційних системах" [6]; "Про розвідку" [7]; "Про електронні довірчі послуги" [8]; "Про Національну програму інформатизації" [9]; "Про ратифікацію Конвенції про кіберзлочинність" [10]; "Про Державну службу спеціального зв'язку та захисту інформації України" [11]; "Про державну таємницю" [12]; "Про доступ до публічної інформації" [13]; "Про захист персональних даних" [14]; "Про оборону України" [15]; "Про інформацію" [16]; "Про Збройні Сили України" [17].

Документів довгострокового та оборонного планування України: Стратегія національної безпеки України [18]; Стратегія кібербезпеки України [2]; Стратегія воєнної безпеки України [19]; Стратегічний оборонний бюлетень України (далі – СОБ) [20]; Питання

Апарату Ради національної безпеки і оборони України, Про Національний координаційний центр кібербезпеки [21]; Стратегія інформаційної безпеки України [22].

Нормативних документів міжнародних організацій, згода на використання яких надана Верховною Радою України. Зокрема, рекомендації Міжнародного союзу електрозв'язку (далі – ITU), міжнародні стандарти з інформаційної безпеки ISO/IEC 27000 та інші [25-29]. З урахуванням того, що проблема кібербезпеки носить глобальний характер, позиція міжнародних організацій є важливою. Глобальна програма програми кібербезпеки Міжнародного союзу електрозв'язку [29] включає п'ять стратегічних напрямів та сім стратегічних цілей, що їх слід враховувати при створенні систем кіберобезпеки ІТС, в т.ч. військового призначення. Причому вимога щодо уніфікації глобального законодавства у сфері кібербезпеки, сумісного з діючими національними та регіональними нормами законодавства, розглядається як головна стратегічна ціль [29, 30, 42].

Аналіз існуючих ЗУ та інших НПА України, ЄС, НАТО, провідних 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 КБ та КО, зокрема таких як: "кібербезпека", "кіберзахист", "кіберзброя" "кібероборона", "кіберпростір", "кібертероризм" тощо [42].

Так, ITU [27, 28] 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. Українське ж законодавство [6] комплекс цих заходів однозначно визначає як – технічний захист інформації [30, 42].

Нормативно-правових актів МО України та ЗС України, більшість з яких має обмеження доступу, видаються відповідно до вимог ЗУ, підзаконних актів державних органів, уповноважених у сферах телекомунікації, інформатизації, захисту інформації тощо, частина з яких також не є відкритою інформацією відповідно до вимог ЗУ [12, 13, 16]. Разом з тим, спираючись на [13, 16], є можливим й доцільним цитування в частині кіберзахисту ІТС військового призначення, окремих положень та завдань з НПА МО України і ЗС України, які не є інформацією з обмеженим доступом. Так, визначено, що функціональна складова кіберзахисту включає системи на [54]:

запобігання (англійською мовою – "Prevention") – заходи щодо завчасного виявлення, уникнення, стримування, запобігання можливих (потенційних) кіберзагроз чи кібератак, припинення підготовки до них;

захисту (англійською мовою – "Protection") – заходи щодо забезпечення випереджувального захисту від можливих кібератак (кібервпливу) противника, в першу чергу в інтересах всебічного та стійкого забезпечення у кіберпросторі процесів управління власними військами;

попередження (англійською мовою – "Mitigation") – заходи щодо безпосереднього виявлення, відвернення загрози, зменшення можливих втрат (збитків, пошкоджень) у разі безпосередньої загрози проведення кібератак;

реагування (англійською мовою – "Response") – заходи комплексного реагування на вплив противника, у тому числі заходи захисту власної інфраструктури, особового складу, ресурсів тощо від впливу противника;

відновлення (англійською мовою – "Recovery") – заходи, направлені на відновлення інформаційної та іншої інфраструктури, яка стала об'єктом кібератак противника, стабілізацію ситуації та ліквідації інших негативних наслідків.

Відповідним органом військового управління (далі – ОВУ), що керує військовими організаційними структурами, які уповноважені на виконання вищезазначених функцій, визначені завдання щодо:

співпраці (реалізації спільних проектів та заходів, підтримання взаємодії) у межах повноважень з суб'єктами забезпечення воєнної безпеки та кібербезпеки держави, а також з НАТО, Європейським Союзом, державами-партнерами в частині спільного виконання завдань кібероборони;

реагування (практичного виконання необхідних заходів) на поточні загрози кібербезпеці у воєнній сфері шляхом їх попередження, завчасного виявлення, випереджувального реагування на них, усунення (мінімізації, ліквідації наслідків) їх впливу;

здійснення кіберзахисту власної інформаційної інфраструктури (засобів рухомого зв'язку як апаратної, так і контентної складових, додатків та сервісів зв'язку, інших інформаційно-комунікаційних систем та об'єктів інформаційної діяльності суб'єктів оборони держави) від кібератак та кібервпливу противника, що забезпечує необхідний рівень інформаційного забезпечення управління військами та зброєю, інші дії в кіберпросторі тощо.

Виклад основного матеріалу. Формування НПБ в сфері КБ та КО останніми роками здійснювалося та здійснюється під впливом певних історичних, воєнно-наукових, зовнішньо-політичних та інших причин та обставин з елементами жорсткої нормативно-правової легітимізації дефініцій (термінів), що запропоновані та втілені в обіг на рівні емоційних та емпіричних логічних операцій окремих виконавців (авторів), без необхідного наукового супроводження [30]. Так, наприклад, на формування НПБ системи нормативних документів системи технічного захисту інформації значною мірою вплинули, та й досі впливають норми й правила, у т.ч. з обмеженням доступу, започатковані та встановлені Державною технічною комісією СРСР (Гостехкомиссия СССР). Разом з тим, слід відмітити, що цей процес є результатом всесвітньо визнаних наукових робіт С.Соболева, А.Кітова, О.Ляпунова, В.Глушкова, зокрема [31, 32], які разом склали основи методології сучасної кібернетики, а надалі й кібербезпеки, як галузі знань про забезпечення захищеності процесів управління в усіх сферах (технічній, соціальній, соціотехнічній, економічній тощо) від різноманітних кіберзагроз різної природи та для забезпечення його ефективності.

Формування сучасної НПБ системи КБ та КО відбувається з урахуванням норм міжнародного права, стандартів та директив ЄС та НАТО, що зафіковано у Законах та НПБ України [2, 5, 10, 20].

З огляду перманентності законодавчого, нормативно-правового, дефініційно-термінологічного супроводження системи КБ та КО України вважається за доцільне надати коротку історичну довідку щодо законодавчого забезпечення дій у кіберпросторі.

До 2007 року в Україні, в т.ч. стосовно кримінальної відповідальності законодавчо розглядалися лише питання пов'язані з терміном комп'ютерні загрози. Вперше, у 2003 р. в ЗУ "Про основи національної безпеки України" [37] одними з потенційних загроз національній безпеці України визнані комп'ютерна злочинність та комп'ютерний тероризм, але зазначені дефініції не розкриті.

Вперше термін кібербезпека використано в 2007 р. у Стратегії національної безпеки України [34] визнаючи за пріоритетне завдання створення національної системи кібербезпеки, 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. Конвенцію ратифіковано ЗУ [10] із застереженнями і заявами. Конвенція наголошує на необхідності зупинення дій, спрямованих проти конфіденційності, цілісності і доступності комп'ютерних систем, мереж і комп'ютерних даних, а також зловживання такими системами, мережами і даними, шляхом встановлення кримінальної відповідальності за таку поведінку, як це описано у Конвенції, надання повноважень, достатніх для ефективної боротьби з такими кримінальними правопорушеннями шляхом сприяння їхньому виявленню, розслідуванню та переслідуванню, як на внутрішньодержавному, так і на міжнародному рівнях, і укладання домовленостей щодо швидкого і надійного міжнародного співробітництва.

До 2012 р. в Україні використовували термін кібербезпека без розкриття його змісту [35].

У 2013 р. законопроєкт № 2483 [36], що був відкликаний 27.02.2014, передбачав з порушенням принципів однозначності, точності та відсутності синонімів, визначення дефініцій з подвійним дефінієндумом: кібернетична безпека (кібербезпека), кібернетичний простір (кіберпростір). Це започаткувало безсистемність вжитку цих та інших термінів не лише у наукових працях, але й в ЗУ [5] та НПБ державного та відомчого рівнів. Що призводить до викривлень у становленні теорії предмету кібербезпеки, неадекватності НПБ цієї галузі, і, як наслідок, до хаотичності у практичних діях.

У 2015 р. на державному рівні [37, 38] наголошено на уразливості об'єктів критичної інфраструктури, державних інформаційних ресурсів та визначено шляхи досягнення необхідних оперативних та інших спроможностей складових сектору безпеки і оборони, зокрема щодо систем забезпечення інформаційної і кібербезпеки, систем захисту інформації та безпеки державних інформаційних ресурсів, технічного і криптографічного захисту інформації з урахуванням практики держав - членів НАТО та ЄС.

У 2016 р. введена в дію Стратегія кібербезпеки України [39], яка системно базувалася на положеннях Конвенції про кіберзлочинність, законодавства України щодо основ національної безпеки, засад внутрішньої та зовнішньої політики, електронних комунікацій, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом та спрямована на реалізацію до 2020 року Стратегії національної безпеки України [40] та стала першим офіційнм документом, який визначив дефініцію кібербезпека як стан захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі, що досягається комплексним застосуванням сукупності правових, організаційних, інформаційних заходів. Стратегія [39] визначила МО України та ГШ ЗС України завдання щодо здійснення заходів з підготовки держави до відбиття воєнної агресії у кіберпросторі (кібероборони) та кіберзахисту власної інформаційної інфраструктури. Вона передбачала гармонізацію нормативних документів України у сфері кібербезпеки відповідно до міжнародних стандартів і стандартів ЄС та НАТО. За результатами експертних оцінок, стан реалізації Стратегії за визначеними показниками не перевищує 40 %, а саме:

не розроблені індикатори виконання Стратегії кібербезпеки України;
не вирішені питання оперативного обміну інформацією про кіберзагрози;
не сформовано перелік об'єктів критичної інформаційної інфраструктури;
недостатніми є організація і проведення наукових досліджень у сфері кібербезпеки;
не створена ефективна система підготовки кадрів;
не створено дієву модель державно-приватного партнерства;
кібернавчання проводились епізодично.

У 2017 р. Указом Президента України [41] було визначено завдання щодо невідкладного забезпечення підготовки законодавчих пропозицій стосовно визначення вимог щодо кіберзахисту об'єктів критичної інформаційної інфраструктури, прав і обов'язків основних суб'єктів забезпечення кібербезпеки та вкотре, з 2005 р., наголошено на необхідності імплементації в Україні положень Конвенції про кіберзлочинність. Еволюцію НПА України стосовно підходів щодо дій в кіберпросторі наведено в таблиці.

У цьому ж 2017 р. ЗУ "Про основні засади забезпечення кібербезпеки України" [5] було визначено правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки.

Законом [5] також визначені базові терміни у сфері кібербезпекі, зокрема такі, що впливають на виконання завдання щодо формалізації опису стану кібербезпеки та процесів кіберзахисту в ІТС ВП: індикатори кіберзагроз; інформація про інцидент кібербезпеки; інцидент кібербезпеки (кіберінцидент); кібератака; кібербезпека; кіберзагроза; кіберзахист; кіберзлочин (комп'ютерний злочин); кіберзлочинність; кібероборона; кіберпростір; кіберрозвідка; кібертероризм; кібершпигунство; критична інформаційна інфраструктура;

критично важливі об’єкти інфраструктури (об’єкти критичної інфраструктури); національна телекомунікаційна мережа; національні електронні інформаційні ресурси (національні інформаційні ресурси); об’єкт критичної інформаційної інфраструктури; система управління технологічними процесами (технологічна система); системи електронних комунікацій (комунікаційні системи).

Таблиця 1

Еволюція НПА України стосовно підходів щодо дій в кіберпросторі

Термін	Закон, нормативно-правовий акт	Короткий зміст, особливості
19.06.2003	Закон України “Про основи національної безпеки України” № 964-IV від 19.06.2003	Одними з потенційних загроз національній безпеці України визнані комп’ютерна злочинність та комп’ютерний тероризм
07.09.2005	Закон України “Про ратифікацію Конвенції про кіберзлочинність” від 07.09.2005 № 2824-IV	Ратифіковано із застереженнями і заявами
12.02.2007	Стратегія національної безпеки України від 12 лютого 2007 № 105/2007	Вперше використано термін кібербезпека. Наголошено про необхідність гармонізації національних стандартів та технічних регламентів згідно з Конвенцією про кіберзлочинність
2013	Проект Закону України “Про внесення змін до Закону України про основи національної безпеки України щодо кібернетичної безпеки України” (№ 2483 від 07.03.2013)	Запропоновані визначення: кібербезпека (кібернетична безпека), кіберпростір (кібернетичний простір). Проект відкликано 27.02.2014
26.05.2015	Стратегія національної безпеки України, Указ Президента України від 26 травня 2015 року № 287 “Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року “Про Стратегію національної безпеки України”	1. Наголошено на уразливості об’єктів критичної інфраструктури, державних інформаційних ресурсів; 2. Визначено завдання щодо удосконалення систем забезпечення інформаційної і кібербезпеки, захисту інформації та безпеки інформаційних ресурсів
14.03.2016	Концепція розвитку сектору безпеки і оборони України, Указ Президента України від 14.03.2016 № 92/2016	Визначено завдання щодо удосконалення систем забезпечення інформаційної і кібербезпеки, систем захисту інформації та безпеки інформаційних ресурсів
15.03.2016	Стратегія кібербезпеки України. Указ Президента України 15 березня 2016 року № 96/2016 Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року “Про Стратегію кібербезпеки України”	1. Наведено визначення кібербезпека України; 2. Кіберпростір визнано сферою ведення бойових дій; 3. МО України, ГШ ЗС України визначено завдання щодо здійснення заходів з підготовки держави до відбиття воєнної агресії у кіберпросторі (кібероборони) та кіберзахисту власної інформаційної інфраструктури; 4. Визначено пріоритетні заходи у сфері забезпечення кібербезпеки сектору безпеки і оборони:

Термін	Закон, нормативно-правовий акт	Короткий зміст, особливості
		а) 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); б) розвиток підрозділів кібербезпеки та кіберзахисту ЗС України
13.02.2017	Указ Президента України від 13 лютого 2017 року №32/2017 Про затвердження Рішення Ради національної безпеки і оборони України від 29 грудня 2016 року "Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації"	Визначено конкретні завдання щодо: невідкладної підготовки законодавчих пропозицій стосовно: а) імплементації положень Конвенції про кіберзлочинність, ратифікованої Законом України від 7 вересни 2005 року № 2824-IV; б) визначення вимог щодо кіберзахисту об'єктів критичної інформаційної інфраструктури, прав і обов'язків основних суб'єктів забезпечення кібербезпеки та власників (розпорядників) об'єктів критичної інформаційної інфраструктури, механізму взаємодії між ними під час виявлення, попередження, припинення кібератак та кіберінцидентів, усунення їх наслідків, запровадження відповідальності за порушення вимог щодо кіберзахисту

Термінологічну базу Закону [5] необхідно визнати принципово недосконалою, що перешкоджає змістовно розглядати практично значну кількість його положень. Жорстка нормативно-правова легітимізація наведених термінів та їх дефініцій за умов недотримання в термінографії сфери кібербезпеки принципів однозначності, точності та відсутності синонімів закладає перше протиріччя, що вимагає наукового та правового розв'язання задачі щодо стандартизації та гармонізаціїї в нормативно-правовому полі України дефініцій термінологічних систем сфери КБ та КО. Шляхи її вирішення запропоновані в НДР "Дефініція" [42].

Встановлено, що національна система кібербезпеки включає в тому числі й оборонні заходи, також визначено МО України та ГШ ЗС України завдання щодо підготовки держави до відбиття воєнної агресії у кіберпросторі (кібероборони); передбачено військову співпрацю з НАТО та іншими суб'єктами оборонної сфери щодо забезпечення безпеки кіберпростору та спільного захисту від кіберзагроз, зазначено про забезпечення кіберзахисту критичної інформаційної інфраструктури в умовах надзвичайного і воєнного стану. Розвідувальним органам України визначені завдання із здійснення розвідувальної діяльності щодо загроз національній безпеці України у кіберпросторі, інші події і обставини, що стосуються сфери кібербезпеки [3].

З огляду на актуальність цієї проблематики стосовно обґрунтування пропозицій щодо формалізації процесів кіберзахисту в ІТС ВП, між Законами [5] та [6, 15] закладено друге протиріччя, що підлягає розв'язанню. Воно полягає в штучному звуженні спектру завдань, що вирішуються ІТС військового призначення за рахунок виключення зі сфери діяльності Закону

[5] комунікаційних та технологічних систем, призначених для оброблення інформації, що містить державну таємницю.

Так, ЗУ [5] визначаючи МО України, ЗС України та розвідувальним органам завдання щодо кібероборони та кіберрозвідки зазначає, що його дія не поширюється на:

1) відносини та послуги, пов'язані із змістом інформації, що обробляється (передається, зберігається) в комунікаційних та/або в технологічних системах;

2) діяльність, пов'язану із захистом інформації, що становить державну таємницю, комунікаційні та технологічні системи, призначені для її оброблення;

Разом з тим, ЗУ [6] встановлює умови та обмеження щодо поводження з державними інформаційними ресурсами або інформацією з обмеженим доступом, вимога щодо захисту якої встановлена законом, зокрема ЗУ "Про державну таємницю" [12], яким визначається, що інформація у сфері оборони визначеним порядком та за відповідними процедурами може бути віднесена до державної таємниці. ЗУ [15, 17] встановлюють норму, щодо дотримання вимог законодавства України [12] в ході вирішення завдань підготовки держави до оборони та виконання завдань передбачених ст. 17 Конституції України.

У 2018 р. ЗУ "Про національну безпеку України" [4] кібербезпека України віднесена до сфери національної безпеки і оборони, визначена роль Стратегії національної безпеки України, Стратегії кібербезпеки України, Стратегії воєнної безпеки України, Національної розвідувальної програми у формуванні засад національній безпеки України. Так, Стратегія кібербезпеки [39] визначається як основа для підготовки державних програм та нормативно-правових актів, що стосуються забезпечення кібербезпеки України. ЗУ [4] огляд стану кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури, що є основою для розроблення Стратегії кібербезпеки, включено до питань Комплексного огляду сектору безпеки і оборони.

Кабінету Міністрів України встановлено завдання щодо визначення порядку проведення:

огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом – Державною службою спеціального зв'язку та захисту інформації України;

оборонного огляду, що є основою для розроблення Стратегії воєнної безпеки – МО України. Стратегіія воєнної безпеки, в свою чергу, є основою для розроблення Стратегічного оборонного бюлетеня України [4].

Крім того, Законом [4] покладені завдання щодо:

формування та реалізації державної політики у сферах кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом – на Державну службу спеціального зв'язку та захисту інформації України;

забезпечення контррозвідувального захисту кібербезпеки – на Службу безпеки України.

Чим закладено третє протиріччя між ЗУ [4] та ЗУ "Про контррозвідувальну діяльність" [43], яке не визначає завдання щодо ведення контррозвідувальної діяльності в кіберпросторі. Розв'язання протиріччя є можливим у ході реформування Служби безпеки України з прийняттям Стратегії забезпечення державної безпеки України, відповідного Закону та подальшим внормуванням контррозвідувальної діяльності.

У 2019 р. Постановою Кабінету Міністрів України [24] затверджені загальні вимоги до кіберзахисту об'єктів критичної інфраструктури, обов'язок та відповідальність за впровадження якого покладається на керівника об'єкту критичної інфраструктури (далі – ОКІ) на всіх стадіях життєвого циклу об'єкта критичної інформаційної інфраструктури (далі – ОКІІ) ОКІ. Визначено, що кібербезпека ОКІ забезпечується шляхом впровадження на ОКІ ОКІІ кіберзахисту або системи інформаційної безпеки з підтвердженою відповідністю. Наведена дефініція Система інформаційної безпеки – сукупність організаційних та технічних заходів, а також засобів і методів захисту інформації, які впроваджуються на ОКІ ОКІІ з метою

запобігання кіберінцидентам, виявлення та захисту від кібератак, порушення конфіденційності, цілісності та доступності інформаційних ресурсів.

Постанова [24] визначає організаційно-методологічні, технічні та технологічні умови кіберзахисту ОКІ, які впроваджуються на ОКІ ОКІІ та повинні забезпечувати:

формування на ОКІ загальної політики інформаційної безпеки;

управління доступом користувачів та адміністраторів до об'єктів захисту ОКІІ ОКІ;

ідентифікацію та автентифікацію користувачів та адміністраторів ОКІІ ОКІ;

реєстрацію подій компонентами ОКІІ ОКІ та їх періодичний аудит;

мережевий захист компонентів та інформаційних ресурсів ОКІІ ОКІ;

доступність та відмовостійкість компонентів та інформаційних ресурсів ОКІІ ОКІ;

визначення умов використання змінних (зовнішніх) пристроїв та носіїв інформації на ОКІІ ОКІ;

визначення умов використання програмного та апаратного забезпечення ОКІІ ОКІ;

визначення умов розміщення компонентів ОКІІ ОКІ.

Постановою [24] визначені базові функції захисту, які повинні бути впроваджені під час створення комплексної системи захисту інформації (системи інформаційної безпеки) ОКІІ ОКІ, зокрема такі:

захист від атак "нульового дня" (вразливості програмного забезпечення, які ще невідомі користувачам чи розробникам програмного забезпечення та проти яких ще не розроблені механізми захисту), виявлення зловмисного коду та шкідливого програмного забезпечення;

фільтрація трафіку та розмежування доступу між мережею об'єкта критичної інфраструктури та зовнішніми мережами за критеріями дозволених та заборонених служб, протоколів, портів, мережевих адрес, мережевих з'єднань, небажаних веб-сайтів тощо. блокування трафіку та з'єднань, які не відповідають визначеним критеріям;

фільтрація та аналіз трафіку за визначеними відповідно до політики інформаційної безпеки критеріями;

моніторинг трафіку на наявність зловмисного коду, вірусів зловмисного програмного забезпечення та за іншими визначеними відповідно до політики інформаційної безпеки критеріями;

виявлення та запобігання атакам та вторгненням, спрямованим на програмні та апаратні компоненти та інформацію об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури;

захист від атак типу "відмова в обслуговуванні";

захист від несанкціонованого доступу через Інтернет;

балансування навантаження;

маскування структури і мережевих адрес мережі;

завершення з'єднання з вузлом уразі атаки;

здійснення реєстрації збереження в електронних журналах та захист від модифікації інформації про події, що мають відношення до безпеки.

До останніх віднесено наступні події:

доступ та дії з інформацією, яка зберігається та обробляється на ОКІІ ОКІ, а також з налаштуваннями програмного та апаратного забезпечення ОКІІ ОКІ, журналами реєстрації подій тощо (читання, модифікація, створення, видалення тощо);

реєстрація подій, пов'язаних із встановленням та зміною прав доступу до служб (функцій), інформації та компонентів об'єкта;

вхід/вихід користувачів та адміністраторів в/із компонентів об'єкта;

невдалі спроби входу користувачів та адміністраторів на ОКІІ ОКІ та перевищення граничної кількості спроб введення пароля;

реєстрація, видалення (блокування) облікових записів користувачів та адміністраторів у компонентах об'єкта;

зміна пароля користувача в компонентах об'єкта;

реєстрація подій, пов'язаних із зміною конфігураційних налаштувань компонентів об'єкта;

спроби здійснення несанкціонованого доступу до ресурсів ОКІІ ОКІ;

негативні результати перевірок цілісності даних та програмного і апаратного забезпечення ОКІІ ОКІ;

всі дії адміністратора з журналами реєстрації подій компонентів об'єкта та налаштування ним параметрів реєстрації.

Четверте протиріччя закладено між ЗУ "Про основні засади забезпечення кібербезпеки України" [5] та іншими НПА внаслідок вищезгаданих причин, та полягає у тому, що ОВУ, військові частини, установи, організації МО України та ЗС України, а також угруповання військ до ОКІ не віднесені. Так, в Україні дефініція критична інфраструктура законодавчо не визначена. ЗУ [5] визначає синонімічно, що критично важливі об'єкти інфраструктури (об'єкти критичної інфраструктури) – підприємства, установи та організації незалежно від форми власності, діяльність яких безпосередньо пов'язана з технологічними процесами та/або наданням послуг, що мають велике значення для економіки та промисловості, функціонування суспільства та безпеки населення, виведення з ладу або порушення функціонування яких може справити негативний вплив на стан національної безпеки і оборони України, навколишнього природного середовища, заподіяти майнову шкоду та/або становити загрозу для життя і здоров'я людей. Також визначається, що об'єкт критичної інформаційної інфраструктури є об'єктом кіберзахисту (запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідація їх наслідків, відновлення функціонування).

Це протиріччя може бути частково вирішене з прийняттям Закону на основі проекту ЗУ "Про критичну інфраструктуру та її захист" [44], робота над яким триває з 2019 р. Проєкт розглядає критичну інфраструктуру, як сукупність об'єктів, які є стратегічно важливими для економіки і національної безпеки, порушення функціонування яких може завдати шкоди життєво важливим національним інтересам; та об'єкт критичної інфраструктури, як визначений у встановленому законодавством порядку складовий елемент критичної інфраструктури, функціональність, безперервність, цілісність і стійкість якого забезпечують реалізацію життєво важливих національних інтересів. Законопроєкт [44] пропонує визначити суб'єктність питань захисту КІ та критерії віднесення підприємств, установ та організацій незалежно від форми власності до ОКІ, які дещо відмінні від [5]. Так, до суб'єктів державної системи захисту критичної інфраструктури пропонується віднести також ЗС України, інші військові формування, утворені відповідно до ЗУ, правоохоронні та розвідувальні органи. До ОКІ, відповідно до визначених критеріїв, арсенали, бази та склади та інші об'єкти ЗС України, де знаходяться або зберігаються озброєння, військова техніка, матеріально-технічні засоби, здійснюється підготовка і застосування військ (сил).

Завдання покладені на МО України щодо вирішення деяких з цих питань визначені законопроектом [44]. До прийняття встановленим порядком Закону на основі законопроекту [44], відповідно до нормативно-правових актів [45] важливі об'єкти ЗС України можуть розглядатися лише як військові об'єкти, що є цілями для нападу, об'єктами терористичних посягань. Це може вплинути на повноту та об'єктивність формального опису стану кібербезпеки та процесів кіберзахисту в ІТС ВП, оскільки є нормативно-правовою підставою для формування моделі загроз та моделі порушника для ІТС та її підсистем.

У 2020 р. відповідно до вимог ЗУ "Про національну безпеку України" [4] прийнята Стратегія національної безпеки України [18], яка є основою для розроблення ряду документів щодо планування у сферах національної безпеки і оборони, що визначатимуть шляхи та інструменти її реалізації, зокрема таких, що на сьогодні діють, або розробляються: Стратегія кібербезпеки України [2]; Стратегія воєнної безпеки України [19]; Стратегія інформаційної безпеки; Стратегія забезпечення державної безпеки; Національна розвідувальна програма.

Для системного захисту України від загроз національній безпеці Стратегія [18] акцентує увагу на необхідності розвитку сектору безпеки і оборони зі стратегічною метою завершення

створення національної системи кібербезпеки, формування сучасних спроможностей суб'єктів забезпечення кібербезпеки і кібероборони та зміцнення системи їх координації.

Отже, враховуючи зазначене вище слід відмітити, що НПБ сфери КБ та КО в Україні ще не сформована. Враховуючи ієрархію існуючої НПБ на рисунку нижче наведено модель формування НПБ України, МО України та ЗС України сфери КБ та КО станом на 2021 рік.

Рисунок 1 – Модель формування нормативно правової бази України, МО України та ЗС України сфери КБ та КО

У 2021 р. прийнято низку логічно взаємопов'язаних (рис. 1) документів оборонного та довгостроковго планування, зокрема, Стратегія воєнної безпеки [19] та Національну розвідувальну програму, які поряд зі Стратегією кібербезпеки [2] мають бути основою для відпрацювання Стратегічного оборонного бюлетеня (далі – СОБ) [46]. Разом з тим, Стратегією [19] цілі та приорітети у сфері КБ та КО не визначені. Натомість, у СОБ [46] кіберзагрози воєнного характеру розглядаються як реальні та потенційні кіберзагрози національним інтересам у воєнній сфері та визначено стратегічні цілі щодо кібероборони, зокрема щодо захисту інформації та кіберзахисту інформаційної інфраструктури.

Із затвердженям у 2021р. Стратегії кібербезпеки України [2] втратила чинність Стратегя кібербезпеки 2016 р. [39]. Ряд її засад, стратегічних цілей та завдань, з урахуванням значного відсотка її не виконання, враховано в новій Стратегії [2], яка на відміну від попередньої, забезпечення кібербезпеки визначає одним із пріоритетів у системі національної безпеки України. Стратегія [2] враховує попередній досвід і проблеми, стан кібербезпекового середовища на національному та міжнародному рівні, а також положення Стратегії кібербезпеки ЄС на цифрове десятиліття, стратегії кібербезпеки окремих держав-членів ЄС та держав-членів НАТО, зокрема в черговий раз окреслює завдання щодо завершення імплементації в законодавство України положень Конвенції про кіберзлочинність.

Вона визначає загрози кібербезпеці України, серед яких:

гібридна агресія Російської Федерації проти України у кіберпросторі із застосуванням кіберзброї;

організовані та спонсоровані урядами інших держав кібератаки;

використання терористичними організаціями кіберпростору для вчинення актів кібертероризму.

Серед передумов загрозам кібербезпеці України, що можуть вплинути на хід та результати обґрунтування пропозицій щодо формалізації процесів кіберзахисту в ІТС ВП розглядаються:

висока технологічна залежність України від іноземних виробників продукції інформаційно-комунікаційних технологій, що підвищує ступінь уразливості інформаційної інфраструктури та звужує спроможності протидії кіберзагрозам;

недосконаліть НПБ у сфері кібербезпеки, а також її застарілість у сфері захисту інформації, повільна імплементація положень європейського законодавства;

невідповідність вимогам законодавства стану захисту інформаційно-комунікаційних систем державних органів, в яких обробляється значна частина інформації з обмеженим доступом;

відсутність системи незалежного аудиту інформаційної безпеки та механізмів розкриття інформації про вразливості в умовах динамічної цифровізації всіх сфер державного управління та життєдіяльності держави;

недостатня захищеність від кібератак державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури;

незавершеність заходів з упровадження організаційно-технічної моделі кіберзахисту;

відсутність дієвої системи інформаційно-аналітичного забезпечення кібербезпеки;

відсутність належного контролю за кіберзахистом;

низький рівень правової відповідальності за порушення вимог законодавства у сфері кібербезпеки.

Серед стратегічних цілей необхідним для формування потенціалу стримування кіберзагроз та набуття кіберстійкості в Стратегії [2] визначені:

формування належної правової, організаційної, технологічної моделі функціонування та застосування підрозділів з повноваженнями ведення збройного протиборства в кіберпросторі;

формування системи ефективної протидії розвідувально-підривній діяльності у кіберпросторі, кібертероризму та кіберзлочинності;

забезпечення кіберстійкості шляхом створення національної системи управління кіберінцидентами та забезпечення постійної готовності до реальних та потенційних кіберзагроз, здатності виявленя та усуненя передумов до їх виникнення;

спрямування відносин з міжнародними партнерами на обмін інформацією про кібератаки та кіберінциденти, проведення спільних кібероперацій та розслідування міжнародних кіберзлочинів, регулярні кібернавчання та тренінги, обмін досвідом та найкращими практиками;

координація спільних дій заінтересованих сторін під час попередження, відбиття та нейтралізації наслідків кібератак та кіберінцидентів та подолання надзвичайних (кризових) ситуацій у кіберпросторі,

створення умов для ефективної взаємодії суб'єктів забезпечення кібербезпеки в процесі розбудови та функціонування національної системи кібербезпеки.

Відповідно ЗУ [5] національна система кібербезпеки є сукупністю суб'єктів забезпечення кібербезпеки та взаємопов'язаних заходів розвідувальних, оборонних, інженерно-технічних заходів, а також заходів криптографічного і технічного захисту національних інформаційних ресурсів, кіберзахисту об'єктів критичної інформаційної інфраструктури. Серед основних суб'єктів національної системи кібербезпеки визначені МО України та ГШ ЗС України, розвідувальні органи.

СОБ прийнятий у 2021 р. [46] на підставі Стратегії кібербезпеки [37] формує стратегічні цілі розвитку сил оборони на період до 2025 року, спрямовує діяльність державних органів й сил безпеки і оборони на досягнення такого рівня оперативних, бойових і спеціальних спроможностей, які забезпечать здатність ведення узгодженого протиборства в усіх сферах ведення бойових дій, у т.ч. - в кіберпросторі, зосереджуючи увагу на досягненні визначеного

рівня спроможностей в інформаційних технологіях, у т. ч. електронних комунікаціях, визначає завдання та заходи для їх досягнення.

Це вкотре підкреслює існування п'ятого протиріччя, яке полягає у відмінностях термінологічних систем сфер КБ та КО міжнародного співтовариства, зокрема ЄС та НАТО й України, має історичні та науково-термінологічні коріння та є невирішеним протягом десятиліть.

Відмінності еволюційно сформувалися внаслідок особливостей розвитку науки і техніки в умовах геополітичних подій XX століття та суттєво ускладненюють практичне застосування термінів сфери КБ та КО щодо спільних заходів із забезпечення безпеки кіберпростору та дій у кіберпросторі.

Зокрема, суттєвою відмінністю є, наприклад те, що за кордоном кіберпростір розглядається як сфера діяльності складних технічних систем, а в Україні – складних соціотехнічних систем [30, 42, 47]. Інша відмінність полягає в підходах щодо формування критеріїв віднесення об'єктів до критичної інфраструктури в Україні та ЄС і державах-членах НАТО. На відміну від ЗУ [5] ЄС та США визначають ОКІ як системи, їх частини або об'єкти розташовані в державах-членах, які мають важливе значення для підтримки життєво важливих соціальних функцій. Пошкодження, руйнування або порушення яких в результаті стихійних лих, тероризму, злочинної діяльності або зловмисної поведінки, може істотно негативно вплинути на безпеку ЄС, здоров'я і захищеність економічного та соціального добробуту населення держави-члена, через неспроможність такої інфраструктури підтримувати згадані функції. Загальна методологія із захисту ОКІ рекомендує посилити увагу на технологічних й інформаційних елементах захисту об'єктів КІ, припинення функціонування яких матиме транскордонний вплив. [48 - 50].

Дане, п'яте , протиріччя не можливо вирішити директивним шляхом, як то визначено в Законі [5] щодо вищого пріоритету міжнародних договорів в сфері КБ та КО над НПБ України. Шляхи його вирішення мають бути вирішені в ході науково обґрунтованої імплементації (адаптації) нормативно-правових вимог та термінологічних систем ITU, ЄС, НАТО до НПБ України, як то передбачено, наприклад у законопроекті [42].

СОБ [46] пропонує до вжитку ряд нових дефініцій, зокрема таких, як: воєнна агресія в кіберпросторі, дії в кіберпросторі, єдине розвідувально-інформаційне середовище, кіберзагрози воєнного характеру, кібероборотьба, кібердії, кібердорозвідка, кіберзброя, кіберінфраструктура, оперативне обладнання території. Зазначене також має безпосереднє відношення до п'ятого протиріччя, оскільки в СОБ [46] визначено захід 5.6.9. Розширення військової співпраці з НАТО щодо забезпечення безпеки кіберпростору та спільних дій у кіберпросторі, що неможливо вирішити без гармонізації термінологічних баз систем КБ та КО України та НАТО.

Окремо слід розглянути положення законів України, що встановлюють відповідальність за злочини та правопорушення у кіберпросторі, не врахування яких може вплинути на повноту та об'єктивність формального опису стану кібербезпеки та процесів кіберзахисту в ІТС військового призначення, оскільки такі є нормативно-правовою підставою для формулювання опису окремих ситуацій, пов'язаних з ліквідацією наслідків порушення сталої роботи ІТС в результаті кібервпливу на них.

Чинний Кримінальний кодекс (далі - КК) України [51] встановлює (відповідно до Розділу (XVI) відповідальність за злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (статті 361-363). розділ XVI "Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку" Особливої частини КК містить шість статей:

1. ст. 361 КК - несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку;

2. ст. 361[1] КК - створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут;

3. ст. 361² КК - несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації;

4. ст. 362 - несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї;

5. ст. 363 КК - порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється;

6. ст. 363¹ КК - перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку.

Кодексом України про адміністративні правопорушення (далі - КУпАП) [52] (ст. 212-6) передбачена адміністративна відповідальність за здійснення незаконного доступу до інформації в інформаційних (автоматизованих) системах, незаконне виготовлення чи розповсюдження копій баз даних інформаційних (автоматизованих) систем. Визначається відповідальність за такі правопорушення:

здійснення незаконного доступу до інформації, яка зберігається, обробляється чи передається в інформаційних (автоматизованих) системах;

здійснення незаконного доступу до інформації, яка зберігається, обробляється чи передається в інформаційних (автоматизованих) системах, призначених для зберігання та обробки інформації з обмеженим доступом;

незаконне копіювання інформації, яка зберігається в інформаційних (автоматизованих) системах, у паперовій чи електронній формі;

безоплатне незаконне розповсюдження інформації, яка зберігається в інформаційних (автоматизованих) системах, у паперовій чи електронній формі;

незаконний збут інформації, яка зберігається в інформаційних (автоматизованих) системах, у паперовій чи електронній формі.

КК та КУпАП України не встановлюють відповідальності за діяльність, неналежну діяльність або бездіяльність, яка класифікується як кіберзлочини, кібершпигунство, кібертероризм, кібердиверсії, кіберпроступки, а також призвела до шкідливих наслідків різного ступеню, пов'язаних із порушенням сталої роботи ІТС, комп'ютерних систем, цілісності, конфіденційності, доступності інформації внаслідок кібердій.

У 2017 р. Указом Президента України [42] було визначено завдання щодо забезпечення підготовки законодавчих пропозицій щодо посилення відповідальності за невиконання вимог законодавства стосовно захисту інформації в ІТС. Мета не досягнута.

На думку колективу авторів, доцільно розглядати і військові злочини у кіберпросторі, оскільки, кіберпростір визнано сферою ведення бойових дій [1, 2].

Висновки. Виходячи з викладеного, можливо зробити наступні висновки:

1. Сучасна НПБ України сфери КБ та КО перебуває в стадії формування та становлення. При цьому вона має низку протиріч, які умовно можна об'єднати в три групи, а саме:

1.1. Дефініційно-термінологічні розбіжності НПБ України сфери КБ та КО.

1.2. Нормативно-правові розбіжності НПБ України сфери КБ та КО.

1.3. Законодавчі, нормативно-правові, дефініційно-термінологічні розбіжності між НПБ сфери КБ та КО України та міжнародного співтовариства.

В умовах глобалізації світу окрема держава практично не може протистояти можливим кіберзагрозам сучасності без інформаційного обміну з іншими. НПБ України [2, 5, 15, 17] значна увага приділяється співпраці з ЄС, НАТО іншими міжнародними суб'єктами щодо забезпечення безпеки кіберпростору та спільного захисту від кіберзагроз, в т.ч. у військовій та оборонній сферах. Дуже важливим індикатором готовності систем кібербезпеки та кібероборони держав-партнерів є досягнення визначеного рівня їх інтероперабельності. Але, в ході проведення чисельних консультації, практичних навчань, науково-практичних

конференцій, семінарів та тренінгів, що займають значне місце серед різноманітних заходів програм взаємодії між Україною і НАТО та США у сфері кібербезпеки, були виявлені протиріччя базового термінологічного апарату, що як мінімум знижує ефективність заходів та не дозволить в майбутньому ефективно виконувати завдання передбачені [2, 5, 46] та рядом інших домовленостей. Аналіз існуючих законів України та інших нормативно-правових актів України [2, 5, 46], ЄС, НАТО, провідних 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 КБ та КО, зокрема таких як: "кібербезпека", "кіберзахист", "кіберзброя", "кібероборона", "кібертероризм", "кіберпростір", тощо [45]. Так, США, ITU, ENISA розглядають кіберпростір як сферу діяльності складних технічних систем, а в Україні – складних соціотехнічних систем [30, 42, 47, 53].

2. З метою вирішення вищезазначених протиріч Законодавча та НПБ України потребує суттєвих змін, зокрема таких як:

2.1. Розроблення та ухвалення нових ЗУ:

"Про кібербезпеку" з метою вдосконалення системи державного управління, чіткого розмежування функцій та завдань КБ та КО між органами влади, самоврядування, ОВУ, іншими суб'єктами КБ та КО, а також усунення ряду протиріч дефініційно-термінологічного походження;

"Про критичну інфраструктуру України" з метою визнання ОКІ України суб'єктами кібербезпеки (кіберзахисту), визначення їм завдань, обов'язків та прав;

"Про ДССЗЗІУ" з метою впорядкування та розмежування регуляторних, наглядових, адміністративних, управлінських і правоохоронних функцій.

2.2. Внесення на підставі цього змін до ЗУ [13, 15, 16, 17, 43, 51, 52], з урахуванням вимог розроблених та ухвалених інших ЗУ, зокрема "Про СБУ", "Про безпеку класифікованої інформації".

2.3. Приведення НПБ України сфери КБ та КО, в т.ч. МО України та ЗС України, у відповідність до вимог нових Законів.

2.4. Врахування у законотворчій діяльності сфери КБ та КО необхідності реальної імплементації міжнародних стандартів ISO/IEC 27k, NIS Directive, NIST CS Framework, зокрема щодо запровадження базового рівня відповідності вимогам з кібербезпеки, оцінювання ризиків, реагування на кіберінциденти і врегулювання інцидентів, відновлення сталого функціонування ІТС, розвитку мережі CERT/CSIRT.

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 Issue don 09 Jul. 2016 Last updated: 29 Mar. 2017 10:55 [Електронний ресурс] – Режим доступу: https://www.nato.int/cps/en/natohq/official_texts_133169.htm.

2. Стратегія кібербезпеки України, введена в дію Указом Президента України від 26 серпня 2021 року № 447/2021, – Режим доступу https://www.president.gov.ua/documents/4472021-40013.

3. Живило Є.О., Черноног О.О. Стратегія кібероборони України // Збірник наукових праць ВІТІ № 4 – 2017 [Електронний ресурс] – Режим доступу: //http://www.viti.edu.ua/files/zbk/2017/4/4_4_2017.pdf.

4. Закон України "Про національну безпеку України" від 21.06.2018 р. № 2469-VIII // Законодавство України [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/2469-19#Text.

5. Закон України "Про основні засади забезпечення кібербезпеки України" від 05.10.2017 р. № 2163-VIII // Законодавство України [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

6. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text.

7. Закон України “Про розвідку” від17.09.2020 № 912-IX [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/912-20#Text.

8. Закон України “Про електронні довірчі послуги” від 5 жовтня 2017 № 2155-VIII [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/2155-19#Text.

9. Закон України “Про Національну програму інформатизації” від 04.02.1998 р. № 74/98-ВР // Законодавство України [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80#Text.

10. Закон України “Про ратифікацію Конвенції про кіберзлочинність” від 10.03.2006 р. № 2163-VIII // Законодавство України [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/2824-15#Text.

11. Про Державну службу спеціального зв’язку та захисту інформації : Закон України від 23.02.2006 р. [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/3475-15#Text.

12. Закон України “Про державну таємницю”від 21 січня 1994 № 3855-XII(зі змінами) [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/3855-12#Text.

13. Закон України “Про доступ до публічної інформації” від 13 січня 2011 р. № 2939-VI. [Електронний ресурс] – Режим доступу : https://zakon.rada.gov.ua/laws/show/2939-17#Text.

14. Закон України “Про захист персональних даних” від 01.06.2010 р. № 2297-VI [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/2297-17#Text.

15. Закон України “Про оборону України” від 06.12.1991 р. № 1932-XII // Законодавство України [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/1932-12#Text.

16. Закон України України “Про інформацію” № 2938-VI. [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/2657-12#Text.

17. Закон України “Про Збройні Сили України” від 6 грудня 1991 року № 1934-XII (зі змінами) // Законодавство України [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/1934-12#Text.

18. Стратегія національної безпеки України, введена в дію Указом Президента України від 14 вересня 2020 року № 392/2020 Про рішення Ради національної безпеки і оборони України], від 14 вересня 2020 року Про Стратегію національної безпеки України [Електронний ресурс] – Режим доступу: https://www.president.gov.ua/documents/3922020-35037.

19. Стратегія воєнної безпеки України, введена в дію Указом Президента України від 25 березня 2021 року № 121/2021 Про рішення Ради національної безпеки і оборони України від 25 березня 2021 року Про Стратегію воєнної безпеки України [Електронний ресурс] – Режим доступу: https://www.president.gov.ua/documents/1212021-37661.

20. Указ Президента України №473/2021 від 17 вересня 2021 року №473/2021 Про рішення Ради національної безпеки і оборони України від 20 серпня 2021 року “Про Стратегічний оборонний бюлетень України” [Електронний ресурс] – Режим доступу: https://www.president.gov.ua/documents/4732021-40121.

21. Указ Президента України №27/2020 28 січня 2020 року Про внесення змін до Указів Президента України від 27 січня 2015 року № 37 та від 7 червня 2016 року № 242 [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/27/2020#Text.

22. Стратегія інформаційної безпеки України, введена в дію Указом Президента України від 28 грудня 2021 року № 685/2021 Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року Про Стратегію інформаційної безпеки України [Електронний ресурс] – Режим доступу: https://www.president.gov.ua/documents/6852021-41069.

23. Постанова Кабінету Міністрів України від 29 березня 2006 р. № 373 Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах (Офіційний вісник України, 2006 р., № 13, ст. 878) [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF#Text.

24. Постанова Кабінет міністрів України від 19 червня 2019 р. № 518 Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text.

25. Recommendation concerning the Promotion and Use of Multilingualism and Universal Access to Cyberspace. Annex. 32 sessio General Assebly UNESCO, 2003. [Електронний ресурс] – Режим доступу: https://unesdoc.unesco.org/ark:/48223/pf0000133171.

26. ДСТУ ISO/IEC 27000:2019 (ISO/IEC 27000:2018, IDT). Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Огляд і словник термінів. Набув чинності відповідно до наказу Державного підприємства “Український науково-дослідний і навчальний центр

проблем стандартизації, сертифікації та якості" від 16.10.2019 № 312 Про прийняття та скасування національних стандартів, прийняття поправок до національних стандартів [Електронний ресурс] – Режим доступу: http://online.budstandart.com/ua/catalog/doc-page?id_doc=85639.

27. Рекомендация МСЭ¬Т X.1205. Обзор кибербезопасности. – Женева:МСЕ, 2010. – С. 55. [Електронний ресурс] – Режим доступу: www.itu.int/ITU-T/recommendations/rec.aspx?rec=9136&lang=ru.\.

28. Рекомендації міжнародного союзу електрозв'язку. Мережі передачі даних, взаємозв'язок відкритих мереж та безпека. Безпека кіберпростору – кібербезпека. МСЕ-Х.1208 2014 р. ISO/IEC 27000.

29. ITU Global Cybersecurity Agenda (GCA) A Framework for International Cooperation in Cybersecurity. [Електронний ресурс] – Режим доступу: https://www.intgovforum.org/Substantive_2nd_IGF/ITU_GCA_E.pdf

30. Вдовенко С. Дефініційні проблеми термінології у сфері кібербезпеки і кібероборони та шляхи їх вирішення / С. Вдовенко, Ю. Даник, С. Фараон // Електронний журнал політики відкритого доступу "Комп'ютерні науки та кібербезпека" Харківського національного університету імені В.Н. Каразіна. – SSN2519-2310 (Online) № 1 (12) 2019 [Електронний ресурс] – Режим доступу: https://periodicals.karazin.ua/cscs/article/view/13080.

31. С.Соболев, А.Китов, О.Ляпунов. Основные черты кибернетики – М.: Вопросы философии - 1955, №4. [Електронний ресурс] – Режим доступу: https://www.computer-museum.ru/books/cybernetics.htm.

32. Енциклопедія кібернетики: [у 2 т.] / редкол.: В. М. Глушков (відп. ред) [та ін.]; АН Української РСР. – К. Голов. ред. Укр, рад. енцикл. 1973.

33. Закон України "Про основи національної безпеки України" N 964-IV від 19.06.2003 [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/964-15#Text.

34. Стратегія національної безпеки України (в редакції від 12 лютого 2007 року № 105/2007) // Офіційний вісник України від 23.02.2007 — 2007 р., № 11, стор. 7, стаття 389, код акту 38751/2007 [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/105/2007#Text.

35. Стратегія національної безпеки (в редакції Указу Президента № 389/2012 від 08.06.2012) [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/389/2012#Text.

36. Законопроект № 2483 від 07.03.2013 "Про внесення змін до Закону України Про основи національної безпеки України щодо кібернетичної безпеки України", [Електронний ресурс] – Режим доступу: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_2?id=&pf3516=2483&skl=8.

37. Стратегія національної безпеки України, затвердженою Указом Президента України від 26.05.2015 № 287/2015 [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/287/2015#Text.

38. Концепція розвитку сектору безпеки і оборони України, введеною в дію Указом Президента України від 14.03.2016 №92/2016 [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/92/2016#Text.

39. Стратегія кібербезпеки України Указ Президента України15.03.2016 № 96/2016 Про рішення Ради національної безпеки і оборони України від 27.01.2016 року "Про Стратегію кібербезпеки України" [Електронний ресурс] – Режим доступу: https://www.president.gov.ua/documents/962016-19836.

40. Стратегія національної безпеки України, затвердженої Указом Президента України від 26.05.2015 року № 287 "Про рішення Ради національної безпеки і оборони України від 06.05.2015 року "Про Стратегію національної безпеки України" [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/287/2015#Text.

41. Указ Президента України від 13.02. 2017 №32/2017 про затвердження Рішення Ради національної безпеки і оборони України від 29.12. 2016 "Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації" [Електронний ресурс] – Режим доступу: https://www.president.gov.ua/documents/322017-21282.

42. Звіт про науково-дослідну роботу удосконалення понятійно-категорійного апарату у сфері кібероборони шифр "Дефініція" (заключний) № держреєстрації 0120U103696 8.06.5.035, К.2020, 203 с.

43. Закон України "Про контррозвідувальну діяльність" від 26.12.2002 р. № 374-IV// Законодавство України [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/374-15#Text.

44. Проект Закону України від 27.05.2019 N 10328 "Про критичну інфраструктуру та її захист" [Електронний ресурс] – Режим доступу:http://search.ligazakon.ua/l_doc2.nsf/link1/JH7YW00A.html.

45. Концепція боротьби з тероризмом в Україні, затверджена Указом Президента України від 5 березня 2019 року № 53/2019. [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/53/2019#Text.

46. Указ Президента України № 473/2021 від 17 вересня 2021 року Про рішення Ради національної безпеки і оборони України від 20 серпня 2021 року "Про Стратегічний оборонний бюлетень України" [Електронний ресурс] – Режим доступу: https://www.president.gov.ua/documents/4732021-40121.

47. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / В.Л. Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа; за заг. ред. В.Б. Толубка. – К.: ДУТ, 2015. – 288 с.

48. European Program for Critical Infrastructure Protection (EPCIP). [Електронний ресурс] – Режим доступу: https://ec.europa.eu/home-affairs/e-library/glossary/critical-infrastructure_en.

49. European Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve the protection [Електронний ресурс] – Режим доступу: http://eurlex.europa.eu/legal-content/EN/NOT/?uri=CELEX:32008L0114.

50. European Critical Infrastructure Warning Information Network, CIWIN COM(2008) 676 [Електронний ресурс] – Режим доступу: – https://www.eumonitor.eu/9353000/1/j9vvik7m1c3gyxp/viampa6xdqyw.

51. Кримінальний кодекс України [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/2341-14#Text.

52. Кодекс України про адміністративні правопорушення [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/80731-10#Text.

53. Трофименко О.Г. Аналіз дефініцій різновидів інформаційних війн: [Електронний ресурс] – Режим доступу: http://conf.inf.od.ua/doklady-konferentsii/150-trofimenko.

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 Issue don 09 Jul. 2016 Last updated: 29 Mar. 2017 10:55 [Elektronny`j resurs] – Rezhy`m dostupu https://www.nato.int/cps/en/natohq/official_texts_133169.htm.

2. Strategiya kiberbezpeky` Ukrayiny`, vvedena v diyu Ukazom Prezy`denta Ukrayiny` vid 26 serpnya 2021 roku # 447/2021, – Rezhy`m dostupu https://www.president.gov.ua/documents/4472021-40013.

3. Zhy`vy`lo Ye.O., Chernonog O.O. Strategiya kiberoborony` Ukrayiny` // Zbirny`k naukovy`x pracz` VITI # 4 – 2017 [Elektronny`j resurs] – Rezhy`m dostupu: //http://www.viti.edu.ua/files/zbk/2017/4/4_4_2017.pdf.

4. Zakon Ukrayiny` "Pro nacional`nu bezpeku Ukrayiny`" vid 21.06.2018 r. # 2469-VIII // Zakonodavstvo Ukrayiny` [Elektronny`j resurs] – Rezhy`m dostupu: https://zakon.rada.gov.ua/laws/show/2469-19#Text.

5. Zakon Ukrayiny` "Pro osnovni zasady` zabezpechennya kiberbezpeky` Ukrayiny`" vid 05.10.2017 r. # 2163-VIII // Zakonodavstvo Ukrayiny` [Elektronny`j resurs] – Rezhy`m dostupu: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

6. Zakon Ukrayiny` "Pro zaxy`st informaciyi v informacijno-telekomunikacijny`x sy`stemax" [Elektronny`j resurs] – Rezhy`m dostupu: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text.

7. Zakon Ukrayiny` "Pro rozvidku" vid17.09.2020 # 912-IX [Elektronny`j resurs] – Rezhy`m dostupu: https://zakon.rada.gov.ua/laws/show/912-20#Text.

8. Zakon Ukrayiny` "Pro elektronni dovirchi poslugy`" vid 5 zhovtnya 2017 # 2155-VIII [Elektronny`j resurs] – Rezhy`m dostupu: https://zakon.rada.gov.ua/laws/show/2155-19#Text.

9. Zakon Ukrayiny` "Pro Nacional`nu programu informaty`zaciyi" vid 04.02.1998 r. # 74/98-VR // Zakonodavstvo Ukrayiny` [Elektronny`j resurs] – Rezhy`m dostupu: https://zakon.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80#Text.

10. Zakon Ukrayiny` "Pro raty`fikaciyu Konvenciyi pro kiberzlochy`nnist`" vid 10.03.2006 r. # 2163-VIII // Zakonodavstvo Ukrayiny` [Elektronny`j resurs] – Rezhy`m dostupu: https://zakon.rada.gov.ua/laws/show/2824-15#Text.

11. Pro Derzhavnu sluzhbu special`nogo zv'yazku ta zaxy`stu informaciyi : Zakon Ukrayiny` vid 23.02.2006 r. [Elektronny`j resurs]. – Rezhy`m dostupu: https://zakon.rada.gov.ua/laws/show/3475-15#Text.

12. Zakon Ukrayiny` "Pro derzhavnu tayemny`cyu"vid 21 sichnya 1994 # 3855-XII (zi zminamy`) [Elektronny`j resurs]. – Rezhy`m dostupu: https://zakon.rada.gov.ua/laws/show/3855-12#Text.

13. Zakon Ukrayiny` “Pro dostup do publichnoyi informaciyi” vid 13 sichnya 2011 r. # 2939-VI. [Elektronny`j resurs] – Rezhy`m dostupu : https://zakon.rada.gov.ua/laws/show/2939-17#Text.

14. Zakon Ukrayiny` “Pro zaxy`st personal`ny`x dany`x” vid 01.06.2010 r. # 2297-VI [Elektronny`j resurs] – Rezhy`m dostupu: https://zakon.rada.gov.ua/laws/show/2297-17#Text.

15. Zakon Ukrayiny` “Pro oboronu Ukrayiny`” vid 06.12.1991 r. # 1932-XII // Zakonodavstvo Ukrayiny` [Elektronny`j resurs] – Rezhy`m dostupu: https://zakon.rada.gov.ua/laws/show/1932-12#Text.

16. Zakon Ukrayiny` Ukrayiny` “Pro informaciyu” # 2938-VI. [Elektronny`j resurs] – Rezhy`m dostupu: https://zakon.rada.gov.ua/laws/show/2657-12#Text.

17. Zakon Ukrayiny` “Pro Zbrojni Sy`ly` Ukrayiny`” vid 6 grudnya 1991 roku # 1934-XII (zi zminamy`) // Zakonodavstvo Ukrayiny` [Elektronny`j resurs] – Rezhy`m dostupu: https://zakon.rada.gov.ua/laws/show/1934-12#Text.

18. Strategiya nacional`noyi bezpeky` Ukrayiny`, vvedena v diyu Ukazom Prezy`denta Ukrayiny` vid 14 veresnya 2020 roku # 392/2020 Pro rishennya Rady` nacional`noyi bezpeky` i oborony` Ukrayiny`], vid 14 veresnya 2020 roku Pro Strategiyu nacional`noyi bezpeky` Ukrayiny` [Elektronny`j resurs] – Rezhy`m dostupu: https://www.president.gov.ua/documents/3922020-35037.

19. Strategiya voyennoyi bezpeky` Ukrayiny`, vvedena v diyu Ukazom Prezy`denta Ukrayiny` vid 25 bereznya 2021 roku # 121/2021 Pro rishennya Rady` nacional`noyi bezpeky` i oborony` Ukrayiny` vid 25 bereznya 2021 roku Pro Strategiyu voyennoyi bezpeky` Ukrayiny` [Elektronny`j resurs] – Rezhy`m dostupu: https://www.president.gov.ua/documents/1212021-37661.

20. Ukaz Prezy`denta Ukrayiny` #473/2021 vid 17 veresnya 2021 roku #473/2021 Pro rishennya Rady` nacional`noyi bezpeky` i oborony` Ukrayiny` vid 20 serpnya 2021 roku “Pro Strategichny`j oboronny`j byuleten` Ukrayiny`” [Elektronny`j resurs] – Rezhy`m dostupu: https://www.president.gov.ua/documents/4732021-40121.

21. Ukaz Prezy`denta Ukrayiny` #27/2020 28 sichnya 2020 roku Pro vnesennya zmin do Ukaziv Prezy`denta Ukrayiny` vid 27 sichnya 2015 roku # 37 ta vid 7 chervnya 2016 roku # 242 [Elektronny`j resurs] – Rezhy`m dostupu: https://zakon.rada.gov.ua/laws/show/27/2020#Text.

22. Strategiya informacijnoyi bezpeky` Ukrayiny`, vvedena v diyu Ukazom Prezy`denta Ukrayiny` vid 28 grudnya 2021 roku # 685/2021 Pro rishennya Rady` nacional`noyi bezpeky` i oborony` Ukrayiny` vid 15 zhovtnya 2021 roku Pro Strategiyu informacijnoyi bezpeky` Ukrayiny` [Elektronny`j resurs] – Rezhy`m dostupu: https://www.president.gov.ua/documents/6852021-41069.

23. Postanova Kabinetu Ministriv Ukrayiny` vid 29 bereznya 2006 r. # 373 Pro zatverdzhennya Pravy`l zabezpechennya zaxy`stu informaciyi v informacijny`x, telekomunikacijny`x ta informacijno-telekomunikacijny`x sy`stemax (Oficijny`j visny`k Ukrayiny`, 2006 p., # 13, st. 878) [Elektronny`j resurs] – Rezhy`m dostupu: https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF#Text.

24. Postanova Kabinet ministriv Ukrayiny` vid 19 chervnya 2019 r. # 518 Pro zatverdzhennya Zagal`ny`x vy`mog do kiberzaxy`stu ob'yektiv kry`ty`chnoyi infrastruktury` [Elektronny`j resurs] – Rezhy`m dostupu: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text.

25. Recommendation concerning the Promotion and Use of Multilingualism and Universal Access to Cyberspace. Annex. 32 sessio General Assebly UNESCO, 2003. [Elektronny`j resurs] – Rezhy`m dostupu: https://unesdoc.unesco.org/ark:/48223/pf0000133171.

26. DSTU ISO/IEC 27000:2019 (ISO/IEC 27000:2018, IDT). Informacijni texnologiyi. Metody` zaxy`stu. Sy`stemy` keruvannya informacijnoyu bezpekoyu. Oglyad i slovny`k terminiv. Nabuv chy`nnosti vidpovidno do nakazu Derzhavnogo pidpry`yemstva "Ukrayins`ky`j naukovo-doslidny`j i navchal`ny`j centr problem standarty`zaciyi, serty`fikaciyi ta yakosti" vid 16.10.2019 # 312 Pro pry`jnyattya ta skasuvannya nacional`ny`x standartiv, pry`jnyattya popravok do nacional`ny`x standartiv [Elektronny`j resurs] – Rezhy`m dostupu: http://online.budstandart.com/ua/catalog/doc-page?id_doc=85639.

27. Rekomendacy`ya MSЭ¬T X.1205. Obzor ky`berbezopasnosty`. – Zheneva:MSE, 2010. – S. 55. [Elektronny`j resurs] – Rezhy`m dostupu: www.itu.int/ITU-T/recommendations/rec.aspx?rec=9136&lang=ru.\.

28. Rekomendaciyi mizhnarodnogo soyuzu elektrozv'yazku. Merezhi peredachi dany`x, vzayemozv'yazok vidkry`ty`x merezh ta bezpeka. Bezpeka kiberprostoru – kiberbezpeka. MSE-X.1208 2014 r. ISO/IEC 27000.

29. ITU Global Cybersecurity Agenda (GCA) A Framework for International Cooperation in Cybersecurity. [Elektronny`j resurs] – Rezhy`m dostupu: https://www.intgovforum.org/Substantive_2nd_IGF/ITU_GCA_E.pdf.

30. Vdovenko S. Definicijni problemy` terminologiyi u sferi kiberbezpeky` i kiberoborony` ta shlyaxy` yix vy`rishennya / S. Vdovenko, Yu. Dany`k, S. Faraon // Elektronny`j zhurnal polity`ky` vidkry`togo dostupu

“Komp'yuterni nauky` ta kiberbezpeka” Xarkivs`kogo nacional`nogo universy`tetu imeni V.N. Karazina. – SSN2519-2310 (Online) # 1 (12) 2019 [Elektronny`j resurs] – Rezhy`m dostupu: https://periodicals.karazin.ua/cscs/article/view/13080.

31. S.Sobolev, A.Ky`tov, O.Lyapunov. Osnovnыe chertы ky`bernety`ky` – M.: Voprosы fy`losofy`y` - 1955, #4. [Elektronny`j resurs] – Rezhy`m dostupu: https://www.computer-museum.ru/books/cybernetics.htm.

32. Ency`klopediya kibernety`ky`: [u 2 t.] / redkol.: V. M. Glushkov (vidp. red) [ta in.]; AN Ukrayins`koyi RSR. – K. Golov. red. Ukr, rad. ency`kl. —1973.

33. Zakon Ukrayiny` “Pro osnovy` nacional`noyi bezpeky` Ukrayiny`” N 964-IV vid 19.06.2003 [Elektronny`j resurs] – Rezhy`m dostupu: https://zakon.rada.gov.ua/laws/show/964-15#Text.

34. Strategiya nacional`noyi bezpeky` Ukrayiny` (v redakciyi vid 12 lyutogo 2007 roku # 105/2007) // Oficijny`j visny`k Ukrayiny` vid 23.02.2007 — 2007 r., # 11, stor. 7, stattya 389, kod aktu 38751/2007 [Elektronny`j resurs] – Rezhy`m dostupu: https://zakon.rada.gov.ua/laws/show/105/2007#Text.

35. Strategiya nacional`noyi bezpeky` (v redakciyi Ukazu Prezy`denta # 389/2012 vid 08.06.2012) [Elektronny`j resurs] – Rezhy`m dostupu: https://zakon.rada.gov.ua/laws/show/389/2012#Text.

36. Zakonoproekt # 2483 vid 07.03.2013 Pro vnesennya zmin do Zakonu Ukrayiny` Pro osnovy` nacional`noyi bezpeky` Ukrayiny` shhodo kibernety`chnoyi bezpeky` Ukrayiny`, [Elektronny`j resurs] – Rezhy`m dostupu: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_2?id=&pf3516=2483&skl=8.

37. Strategiya nacional`noyi bezpeky` Ukrayiny`, zatverdzhenoyu Ukazom Prezy`denta Ukrayiny` vid 26.05.2015 # 287/2015 [Elektronny`j resurs] – Rezhy`m dostupu: https://zakon.rada.gov.ua/laws/show/287/2015#Text.

38. Koncepciya rozvy`tku sektoru bezpeky` i oborony` Ukrayiny`, vvedenoyu v diyu Ukazom Prezy`denta Ukrayiny` vid 14.03.2016 #92/2016 [Elektronny`j resurs] – Rezhy`m dostupu: https://zakon.rada.gov.ua/laws/show/92/2016#Text.

39. Strategiya kiberbezpeky` Ukrayiny` Ukaz Prezy`denta Ukrayiny`15.03.2016 # 96/2016 Pro rishennya Rady` nacional`noyi bezpeky` i oborony` Ukrayiny` vid 27.01.2016 roku "Pro Strategiyu kiberbezpeky` Ukrayiny`" [Elektronny`j resurs] – Rezhy`m dostupu: https://www.president.gov.ua/documents/962016-19836.

40. Strategiya nacional`noyi bezpeky` Ukrayiny`, zatverdzhenoyi Ukazom Prezy`denta Ukrayiny` vid 26.05.2015 roku # 287 "Pro rishennya Rady` nacional`noyi bezpeky` i oborony` Ukrayiny` vid 06.05.2015 roku "Pro Strategiyu nacional`noyi bezpeky` Ukrayiny`" [Elektronny`j resurs] – Rezhy`m dostupu: https://zakon.rada.gov.ua/laws/show/287/2015#Text.

41. Ukaz Prezy`denta Ukrayiny` vid 13.02. 2017 #32/2017 pro zatverdzhennya Rishennya Rady` nacional`noyi bezpeky` i oborony` Ukrayiny` vid 29.12. 2016 Pro zagrozy` kiberbezpeci derzhavy` ta nevidkladni zaxody` z yix nejtralizaciyi [Elektronny`j resurs] – Rezhy`m dostupu: https://www.president.gov.ua/documents/322017-21282.

42. Zvit pro naukovo-doslidnu robotu udoskonalennya ponyatijno-kategorijnogo aparatu u sferi kiberoborony` shy`fr “Definiciya” (zaklyuchny`j) # derzhreyestraciyi 0120U103696 8.06.5.035, K.-2020, s. 203.

43. Zakon Ukrayiny` “Pro kontrrozviduval`nu diyal`nist`” vid 26.12.2002 r. # 374-IV// Zakonodavstvo Ukrayiny` [Elektronny`j resurs] – Rezhy`m dostupu: https://zakon.rada.gov.ua/laws/show/374-15#Text.

44. Proekt Zakonu Ukrayiny` vid 27.05.2019 N 10328 Pro kry`ty`chnu infrastrukturu ta yiyi zaxy`st [Elektronny`j resurs]. – Rezhy`m dostupu:http://search.ligazakon.ua/l_doc2.nsf/link1/JH7YW00A.html.

45. Koncepciya borot`by` z terory`zmom v Ukrayini, zatverdzhena Ukazom Prezy`denta Ukrayiny` vid 5 bereznya 2019 roku # 53/2019. [Elektronny`j resurs] – Rezhy`m dostupu: https://zakon.rada.gov.ua/laws/show/53/2019#Text.

46. Ukaz Prezy`denta Ukrayiny` # 473/2021 vid 17 veresnya 2021 roku Pro rishennya Rady` nacional`noyi bezpeky` i oborony` Ukrayiny` vid 20 serpnya 2021 roku “Pro Strategichny`j oboronny`j byuleten` Ukrayiny`” [Elektronny`j resurs] – Rezhy`m dostupu: https://www.president.gov.ua/documents/4732021-40121.

47. Informacijna ta kiberbezpeka: sociotexnichny`j aspekt: pidruchny`k / V.L. Buryachok, V.B. Tolubko, V.O. Xoroshko, S.V. Tolyupa; za zag. red. V.B. Tolubka. – K.: DUT, 2015. – 288 s.

48. European Program for Critical Infrastructure Protection (EPCIP). [Elektronny`j resurs] – Rezhy`m dostupu:https://ec.europa.eu/home-affairs/e-library/glossary/critical-infrastructure_en.

49. European Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve the protection [Elektronny`j resurs] – Rezhy`m dostupu: http://eurlex.europa.eu/legal-content/EN/NOT/?uri=CELEX:32008L0114.

50. European Critical Infrastructure Warning Information Network, CIWIN COM(2008) 676 [Elektronny`j resurs] – Rezhy`m dostupu: https://www.eumonitor.eu/9353000/1/j9vvik7m1c3gyxp/viampa6xdqyw.

51. Kry`minal`ny`j kodeks Ukrayiny` [Elektronny`j resurs] – Rezhy`m dostupu: https://zakon.rada.gov.ua/laws/show/2341-14#Text.

52. Kodeks Ukrayiny` pro administraty`vni pravoporushennya [Elektronny`j resurs] – Rezhy`m dostupu: https://zakon.rada.gov.ua/laws/show/80731-10#Text.

53. Trofy`menko O.G. Analiz definicij riznovy`div informacijny`x vijn: [Elektronny`j resurs] – Rezhy`m dostupu: http://conf.inf.od.ua/doklady-konferentsii/150-trofimenko.

Vdovenko S.G., Ph.D. Zhivilo E.A., Chernonog A.A., Dokil V.N.

ANALYSIS OF THE REGULATORY AND LEGAL FRAMEWORK OF THE FUNCTIONING OF THE CYBER DEFENSE SYSTEM AND THE CYBER DEFENSE SYSTEM IN THE INFORMATION AND TELECOMMUNICATION SYSTEMS OF MILITARY PURPOSE

The urgency of this work is due to one of the priorities of the national security system of Ukraine to perform the functions and tasks of the defense forces of Ukraine in conditions of destructive activity on the cybersecurity environment of the state.

Modern development of information and cyber technologies and global informatization in the world have led to the fact that the information and cybersphere have become the object of various destructive influences on all spheres of society through cyberspace, which complemented existing ones, namely land, sea, air, space and became a sphere conflicts and possible hostilities.

States, depending on the degree of their development, build different systems (models) of protection of their information, telecommunications infrastructures, determine the use of technological processes circulating in these systems and protect critical infrastructure from cyber threats, determine the functions, directions and ways of action in cyberspace. Today, more than 60 countries in the world are openly and / or covertly working to improve the functionality of national cybersecurity and cyber defense systems. National and coalition cyber forces are being created, their functions and tasks are being determined, the content and procedure of activity, composition, algorithms for training units, military and civilian specialists are being formed, strategies are being developed, regulatory framework, hardware and software complexes, and special cyber defense software are being improved. and tactics of their application.

In general, the development and widespread implementation of communication systems and systems using innovative information and telecommunications technologies in military systems is in accordance with international rules for cyberwarfare, such as the Geneva Convention. At the same time, the main principles of formation of cybersecurity and cyber defense systems of the leading countries of the world are scientifically substantiated legislative, normative-legal, definition-terminological support. Under these conditions, the transformation of the regulatory framework takes into account the constant militarization of national segments of cyberspace, taking into account the criteria (indicators) of threats in cybersecurity and cyber defense of leading countries, the level of system readiness and acquisition of capabilities, etc.

To address the issues of regulation and implementation of norms and rules of international organizations in the field of cybersecurity and cyber defense, it is proposed to analyze the current provisions (axiomatics) of the existing legislative, state and departmental regulatory framework, as well as the regulatory framework of international organizations. ITU) on cybersecurity.

Keywords: cyberspace, cybersecurity, cyber defense, law of Ukraine, normative - legal base, normative legal act, object of critical information infrastructure.