УДК 323.1: 327.39

М. М. Алексєєв

ФОРМАЛІЗАЦІЯ ПРОЦЕСУ ЗАБЕЗПЕЧЕННЯ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ ДЕРЖАВИ

Пріоритетність забезпечення кібернетичної безпеки як складової національної безпеки держави у сучасному інформаційному суспільстві швидко зростає. Революційні перетворення в області інформатизації та комунікації породжують нові виклики й у воєнній сфері. Актуальними сьогодні стають таки поняття як "кіберзброя" та "кібервійна". З метою адекватного реагування на сучасні загрози в кібернетичному просторі провідні країни світу створюють власні кібернетичні війська, витрачають значні матеріальні та фінансові ресурси. Тому найважливішим завданням для нашої держави стає напрацювання теоретичних основ для визначення оптимальних, в умовах обмежених можливостей, кроків на шляху створення ефективної системи забезпечення кібернетичної безпеки України. В роботі розглянутий методологічний підхід до формалізації процесу забезпечення кібернетичної безпеки, який дозволить здійснити виявлення й опис як вербальний у прийнятих термінах, так і математичний, складових цього процесу, їх зв'язків і відношень.

Ключові слова: кібернетична безпека, формалізація, кібервиклик, кібернебезпека, кіберзагроза, кібервійна, кіберзброя.

Вступ

Тенденції розвитку сучасних світових подій все частіше свідчать про зростання ескалації не лише в традиційному геостратегічному просторі, але й перенесення протиборства провідних держав у штучно створену "віртуальну" реальність – кібернетичний простір, світ електронних засобів масової комунікації та управління.

Відповідно до ключових положень Стратегії національної безпеки США [1] сучасні кібернетичні загрози є одним з найбільших викликів державній, суспільній та економічній безпеці, що повстали перед нацією. У рамках зв'язків із суспільством посадовці Агенції національної безпеки США (АНБ) постійно фокусують увагу американського населення на зростанні загрози кібернетичних атак проти Сполучених Штатів.

При цьому, на думку фахівців АНБ, найбільш небезпечними з них є такі, що спрямовуються на порушення функціонування систем енергозабезпечення та водопостачання, фінансів, транспорту, комунікації, оборонної промисловості, військового управління, безперебійної роботи мережі Інтернет, від якої залежить економіка країни [2].

Одним з останніх прикладів важливості згаданої проблематики наводиться факт таємного доступу невідомих осіб (або держави) до американської захищеної бази даним (БД), відомої як "Державний перелік дамб", виявлений у травні 2013 року співробітниками Агенції національної безпеки. Як повідомляється в [2], зазначена БД налічує наявні вразливості 13 397 небезпечних гідроспоруд країни, включаючи приблизну кількість осіб, які можуть загинути у разі аварії на них.

Таким чином сьогоднішні кібернетичні загрози вже можна порівняти із загрозами військового та (або) терористичного характеру. Тому в [3] кіберпростір вже об'явлено п'ятою середою для ведення бойових дій, як суша, море, повітряний та космічний простір. При цьому автори дослідження передбачають, що у найближчі чотири роки США та інші провідні країни світу значно збільшать власні інвестиції в розвиток кіберзробї як для оборони, так і для нападу (рис. 1)

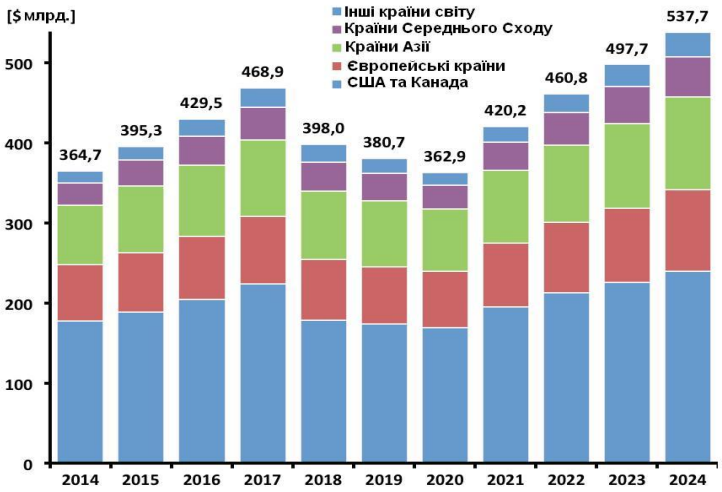

Рис. 1. Прогнозні показники передбаченого зростання глобального ринку кіберзброї в наступні 10 років (витрати по регіонах світу в мільярдах доларів США)

У свою чергу, відповідно до [4] країни-учасниці НАТО також постійно розробляють нові заходи та посилюють захист своїх інформаційно-комунікаційних систем від кібернападів. Ці зусилля, а також можливості надавати допомогу країнам у захисті їхніх мереж від масштабних нападів, обумовлюють практичну реалізацію політики НАТО щодо кібернетичного захисту, яку було ухвалено країнами-членами НАТО в січні 2008 року після масштабних кібернападів на Естонію в 2007 році.

На Лісабонському саміті НАТО 2010 року кіберзагрози визначено головним викликом НАТО в галузі безпеки. У ході проведення саміту були опрацьовані подальші політичні кроки та завдання щодо кіберзахисту, які потребуватимуть докладного аналізу сучасної політики в цієї галузі, уточнень та плану дій з реалізації нової політики.

В рамках даного процесу в Естонії було створено Центр передового досвіду в галузі кіберзахисту , а Військовий комітет НАТО нещодавно затвердив Концепцію кіберзахисту , яка передбачає практичні програми дій [5].

Аналіз існуючих досліджень

Нажаль, в Україні навіть теоретичне обґрунтування питань кібернетичної безпеки держави, як складової національної безпеки, лише починають знаходити своє відображення у спеціалізованих виданнях. З’являються спроби узаконити саме значення "кібернетичної безпеки" у винесених на обговорення проектах нормативно-правових актів [6-7].

При цьому в Стратегії національної безпеки України [8], Законі України "Про основи національної безпеки України" [9] сформульовані основні положення державної політики, спрямованої на захист національних інтересів, гарантії безпеки особистості, суспільства й держави від зовнішніх і внутрішніх загроз у визначальних сферах життєдіяльності. Серед найбільш актуальних таких загроз визначається нездатність України протистояти новітнім викликам національній безпеці, пов'язаним із застосуванням інформаційних технологій в умовах глобалізації, насамперед кіберзагрозам.

Враховуючи наведене, на нашу думку, у зазначеній галузі залишаються недостатньо опрацьованими проблеми методологічного характеру. У першу чергу це стосується формалізації основ формування системи кібернетичної безпеки України, яка б забезпечила захист національних інтересів в інформаційній сфері нашої держави як у вигляді окремого суб’єкту, так і суспільства у цілому.

Водночас, саме від методологічних засад, покладених в основу організації відповідного процесу великою мірою залежить якість функціонування системи забезпечення кібернетичної безпеки держави.

Метою даної статті є розгляд методологічного підходу до формалізації процесу забезпечення кібернетичної безпеки, який дозволить здійснити виявлення й опис як вербальний у прийнятих термінах, так і математичний, складових цього процесу, їх зв'язків і відношень.

Основна частина дослідження

Термін "формалізація" є досить поширеним як у наукових дослідженнях, так і в організації управління в різних галузях діяльності. У загальному вигляді під формалізацією розуміють відображення результату мислення в точних поняттях і твердженнях [10]. Формалізація полягає в тому, що об'єктам, їх властивостям і відношенням знаходять стійкі, добре доступні для огляду і тотожні матеріальні конструкції, які дають змогу виявити і зафіксувати суттєві сторони об'єкта. Формалізація уточнює зміст завдяки виявленню його форми і може бути здійснена з різним ступенем повноти.

Виходячи с такого тлумачення формалізації, можна визначити завдання формалізації процесу забезпечення кібернетичної безпеки держави як об'єкта розгляду таким чином: "Формалізація процесу забезпечення кібернетичної безпеки держави є виявлення й опис як вербальний у прийнятих термінах, так і математичний, складових цього процесу, їх зв'язків і відношень".

Складність такого завдання зумовлена тим, що не виявлено чітких закономірностей і тенденцій процесів, які відбуваються в сфері забезпечення кібернетичної безпеки. Завдання ускладнюється тим, що необхідно враховувати важливий вплив на цей процес особливостей зовнішнього і внутрішнього середовищ, збільшення невизначеності, непередбаченості, мінливості, взаємозалежності, зростання масштабів можливих негативних наслідків тощо.

Цілком очевидно, що вербальний опис використовується, в першу чергу, для визначення категорійно-понятійного апарату, який застосовується у згадані сфері. Термінологічна невизначеність у галузі забезпечення кібернетичної безпеки проявляється в неузгодженості та, в окремих випадках, у суперечності формулювань одних і тих самих термінів, понять, визначень, викладених у різних наукових роботах та проектах відповідних нормативно-правових документів. Ускладнює використання термінів і відсутність наукового обґрунтування категорійно-понятійного апарату.

Перелік термінів і понять у сфері кібернетичної безпеки досить великий. Значна їх кількість не має сталого характеру та потребує розгляду в аспекті подальшої формалізації. У першу чергу, слід звернути увагу на ті поняття, які стосуються предметної області питання - процесу забезпечення кібернетичної безпеки держави.

Розглядаючи поняття кібернетичної безпеки, необхідно зазначити, що існує декілька її визначень. Наприклад, [11] характеризує кібербезпеку як стан захищеності кіберпростору держави в цілому або окремих об'єктів його інфраструктури (ІТС тощо) від ризику стороннього кібервливу, за якого забезпечується її сталий розвиток, а також своєчасне виявлення, запобігання й нейтралізація реальних і потенційних викликів, кібернетичних втручань і загроз особистим, корпоративним та/або національним інтересам.

У контексті нормативно-правового розуміння національної та інформаційної безпеки в [12] кібербезпека визначається як захищеність життєво важливих інтересів людини і громадянина, суспільства і держави, за якої забезпечуються сталий розвиток суспільства, своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз національним інтересам у сфері функціонування інформаційно-телекомунікаційних систем.

У гуманітарному тлумачення кібербезпека надається в [13], де вона характеризується як один з видів національної безпеки, котрий є частиною інформаційно-психологічної (духовної) безпеки, та є станом захищеності від зовнішніх та внутрішніх загроз віртуальної реальності в кібернетичному просторі соціуму, засобів масової комунікації військового, загальнодержавного та громадянського призначення, а також суспільної свідомості, як одного з національних інформаційних ресурсів.

Запропонований для обговорення фахівцями Національного Інституту стратегічних досліджень при Президенті України проект Стратегії забезпечення кібернетичної безпеки України [7] визначає кібербезпеку як стан захищеності критичних об'єктів національної інформаційної інфраструктури та окремих її складових, за якого забезпечується їх стале функціонування і розвиток, своєчасне виявлення, запобігання і нейтралізація кібернетичних загроз в інтересах людини, суспільства, держави.

Подальший аналіз цього й інших термінів проводився з метою практичної реалізації теоретичних міркувань. В узагальненому вигляді реалізація включає визначення необхідних заходів, обґрунтування обсягів потрібних ресурсів тощо. А основним принципом досягнення цієї мети є її вимірність.

Аналізуючи з цих позицій визначення кібернетичної безпеки, можна підкреслити наявність у ньому [12] об'єктів захищеності – життєво важливих інтересів людини і громадянина, суспільства; а у визначенні [7] ще й критичних об'єктів національної інформаційної інфраструктури, які також потребують тлумачення. Усе це не дає змоги здійснення над ними процедур в інтересах формалізації процесу забезпечення кібернетичної безпеки.

Водночас можна стверджувати, що присутність у понятті кібернетичної безпеки людини і громадянина носить декларативний характер, бо не дає змоги визначити заходи і їх реалізацію щодо забезпечення кібернетичної безпеки стосовно кожного з 46 млн. громадян України. Не несуть у собі необхідної для організації забезпечення кібернетичної безпеки держави конкретики і згадані "життєво важливі інтереси суспільства". Це підтверджується й іншими фахівцями в галузі безпеки держави. Окремої уваги заслуговує підхід у [13] до визначення та розкриття таких понять як національні цінності, інтереси та цілі. Ураховуючи все це, слід зазначити, що найбільш вдалим, хоча й складним для подальшої формалізації, є формулювання поняття кібернетичної безпеки як стану захищеності держави від загроз кібернетичного характеру.

Є ще декілька важливих термінів зі сфери кібернетичної безпеки держави, які потребують уваги і також не знайшли свого однакового розуміння. Так, особливе місце у формалізації процесу забезпечення кібернетичної безпеки держави займає проблема визначення таких понять як "кібервиклик", "кіберризик", "кібернебезпека", "кіберзагроза" та "кібервійна".

На перший погляд, кіберзагроза і кібернебезпека близькі, можна сказати, однорідні поняття. Але, зосереджуючи увагу під час формалізації в аспекті розвитку конфлікту в кібернетичному просторі, можна виділити ряд розходжень між ними. Як показано в [14], вони полягають у ступені готовності до заподіяння того чи іншого збитку. При цьому, кіберзагроза – це стадія крайнього, найвищого загострення протиріч, безпосередньо передконфліктний стан. Кібернебезпека ж розуміється як стадія зародження й інтеграції протиріч, коли в одного із суб'єктів є потенційна можливість застосувати силу, але він ще не готовий до цього. Крім того, кіберзагроза повинна включати дві складові – наміри і можливість завдання збитків інтересам кібернетичної безпеки, а кібернебезпека має тільки одну з них (табл. 1) [15].

Таблиця 1

Схематичні відмінності кіберзагроз і кібернебезпек

Явища	Компоненти		Готовність до завдання збитку
	наміри	можливості	
Кіберзагроза	Є	Є	Реальна (явна)
Кібернебезпека	Немає	Є	Гіпотетична (можлива)
	Є	Немає	
	Немає	Немає	Уявна

Кібернебезпеку і кіберзагрозу відрізняють ще й за тим, що перша з них носить гіпотетичний, часто безадресний характер, але остання завжди персоніфікована відносно джерел (суб'єктів) загрози й об'єкта, на який спрямована її дія.

Таким чином, можна прийняти, що кіберзагроза конкретизує найбільш вірогідний спосіб усунення протиріч між суб'єктами конфліктних стосунків за допомогою сили.

Зіставляючи поняття "кібернебезпека" та "кіберзагроза" можна бачити, що вони за своєю суттю є конкретними проявами реально існуючих між суб'єктами (особами, групами осіб, окремими державами або коаліціями держав) певних суперечливих відносин. Їх можна прийняти за показники ступеня ескалації конфлікту, причому більш високий ступінь напруженості властивий кіберзагрозі, а менший – кібернебезпеці. Можна стверджувати, що кіберзагроза виникає безпосередньо з кібернебезпеки в результаті її посилення.

Під терміном "виклик" у [16] розуміється можливість протидіяти досягненню цілей стратегії національної безпеки. На наш погляд, у такому формулюванні відображено лише усвідомлену діяльність деякого суб'єкту міждержавних відносин проти іншої держави, що дещо звужує значення цього терміна. У ньому не знаходять свого відображення інші обставини різного характеру як регіональні, так і глобальні, які явно не спрямовані проти конкретної держави, але за своїми наслідками будуть загрожувати досягненню цілей стратегії національної безпеки (наприклад, посилення кібернетичної злочинності). Не виключено, що такого роду виклики потребуватимуть застосування тих чи інших кібернетичних методів.

Виходячи з цього, пропонується в сучасному контексті під викликом розуміти намір суб'єктів міжнародних відносин або наслідки процесів розвитку воєнно-політичної, соціальної обстановки як у регіоні, так і в глобальному вимірі, які за певних умов можуть загрожувати досягненню цілей стратегії національної безпеки держави.

Є ще одне, досить розповсюджене поняття – "ризик", яке вбачає два підходи до свого тлумачення [16]. У широкому розумінні – це характеристика ситуації, яка має невизначеність результату, за обов'язкової наявності несприятливих наслідків. Ризик у вузькому розумінні – вимірювана або обчислювана ймовірність несприятливого наслідку. Ризик завжди означає невизначеність результату, при цьому під словом "ризик" частіше за все розуміють імовірність втрат (збитків).

Під ризиком також іноді розуміють фактор, який потенційно може мати негативний вплив на хід процесу [17]. Це більш вдале визначення ризику, тому що розвиток різних сфер держави – це завжди процеси, яким обов'язково притаманні фактор, або їх група, що несе негативний потенціал. Крім того, введення поняття потенціалу вже передбачає вимірність ризику з можливим застосуванням відповідного розрахункового апарату, що прямо відповідає потребам формалізації. Розходження у визначеннях ризику залежить від контексту втрат, їхнього оцінювання й виміру. Коли вже втрати є зрозумілими і фіксованими, оцінювання ризику фокусується тільки на ймовірності події (частоті події) і пов'язаних з нею обставинах.

Для ілюстрації складності питання врахування ризику в сфері кібернетичної безпеки можна привести класифікацію ризиків, що надано в [16].

Згідно з цією класифікацією ризики поділяються на: суб'єктивний (ризик, наслідки якого неможливо об'єктивно оцінити); об'єктивний (ризик із точно вимірюваними наслідками); фінансовий (ризик, прямі наслідки якого полягають у грошових втратах); динамічний (ризик, імовірність і наслідки якого змінюються залежно від ситуації); фундаментальний (несистематичний ризик з тотальними наслідками); чистий (ризик, наслідками якого можуть бути лише збиток чи збереження поточного становища); нефінансовий (ризик із негрошовими втратами); статичний (ризик, що практично не змінюється в часі); частковий (систематичний ризик з локальними наслідками).

З огляду на наведену класифікацію ризиків можна стверджувати, що поняття ризику зі сфери кібернетичної безпеки має бути комплексним. Зміст і взаємозв'язок понять "виклик",

"небезпека" і "загроза" у сфері безпеки добре розкрито в [17] на основі розгляду їх співвідношення на умовній шкалі ескалації напруженості (табл. 2).

Таблиця 2

Шкала ескалації напруженості в кібернетичному просторі

Характеристики	Фази ескалації напруженості в кібернетичному просторі			
	кібервиклик	кібернебезпека	кіберзагроза	кібервійна
Зміст	Прагнення до протидії здійсненню інтересів національної безпеки у кібернетичній сфері	Імовірність завдання гіпотетичного збитку національним інтересам і безпеці із застосуванням кібернетичних засобів	Готовність (намір і можливість) завдати шкоди життєво важливим інтересам і безпеці держави із застосуванням кібернетичних засобів	Реалізація загрози застосування кіберзасобів (кіберзборї) для досягнення політичних, військових та інших цілей
Характер	Абстрактний, гіпотетичний, безадресний характер (відсутність конкретного об'єкта і суб'єкта)		Конкретний, персоніфікований, адресний і спрямований характер (наявність конкретних, явно виражених цілей суб'єкта й об'єкта)	
Стадії ризику	Зародження причини можливого збитку інтересам і безпеці	Стадія насичення, ймовірність заподіяння збитку потенційна або непряма	Висока ймовірність (готовність) до завдання кібернетичними засобами збитку життєво важливим інтересам і безпеці	Заподіяння прямого і явного збитку життєво важливим інтересам і безпеці держави, суспільству і стабільності
Стосунки між суб'єктами	Суперництво суб'єктів	Протидія потенційних (абстрактних) противників	Протидія персоніфікованих (конкретних) противників	Кібернетична війна
Розвиток протиріч між суб'єктами	Зародження протиріч	Компромісне вирішення існуючих протиріч переважно без використання кіберзасобів	Готовність одного із суб'єктів відкрито використовувати кіберзасобів для вирішення протиріч на свою користь	Вирішення протиріч методом використання кіберзасобів (кіберзборї)
Противник	Абстрактний (потенційний)		Конкретний (реальний)	
Суб'єкти системи забезпечення кібербезпеки (ССЗКБ)	Режим повсякденної діяльності, підготовка до протидії кібервикликам, потенційній і реальній кібернебезпеці		Проведення заходів, адекватних кіберзагрозі	Захист національних інтересів з виростанням всіх наявних сил та засобів
Готовність ССЗКБ	"Постійна"	"Підвищена"	"Кіберзагроза"	"Повна"

З таблиці чітко видно, що початковою фазою ескалації напруженості є кібервиклик, який має свій прояв у прагненні однієї зі сторін до протидії іншій стороні в реалізації національних інтересів.

Кібернебезпека як гіпотетична ймовірність завдання збитків національним інтересам стає наступною фазою ескалації напруженості в кібернетичному просторі. Напруженість досягає, за умови наявності в конкретного суб'єкта реальних намірів і достатніх кібернетичних можливостей для завдання збитків іншому суб'єкту, своєї вищої фази – кіберзагрози, за якої виникає розв'язування кібервійни. Слід підкреслити, що кожна фаза кібернетичної напруженості має свої специфічні властивості.

Таким чином, аналіз співвідношення небезпеки і загрози показав, що такому співвідношенню властиві закономірності, які описуються законом переходу кількісних змін у якісні, тобто з ескалацією напруженості в кібернетичному просторі кібервиклик переростає в кібернебезпеку, та в свою чергу може перетворитися в кіберзагрозу, остання в кібервійну. У свою чергу, у разі накопичення відповідних змін (наприклад, деескалація напруженості), кіберзагроза трансформується в кібернебезпеку. Цілком очевидно, що із зниженням рівня кіберзагрози сама вона не зникає повністю, а трансформується у відповідний стан кібернебезпеки.

Стримування кіберзагроз розглядається як можливість відвернути чинник (або компенсувати його вплив), який може заподіяти шкоду об'єкту (державі). Звісно, що стримування загроз, як і їх нейтралізація, потребує певних матеріальних, людських, інформаційних та інших ресурсів.

У формальному виді забезпечення кібернетичної безпеки описується цільовою функцією системи, яку можна сформулювати таким чином:

система забезпечення кібербезпеки спрямовує свої зусилля на недопущення зростання інтегрального рівня кіберзагрози вище визначеного порогу $\mathbf{P_{п1}}$ за умови, що ресурси, які виділяються на забезпечення визначеного рівня кібербезпеки $\mathbf{R_{bн}}$ не меньші, ніж мінімально потрібні $\mathbf{R_{bp}}$, (рис. 2)

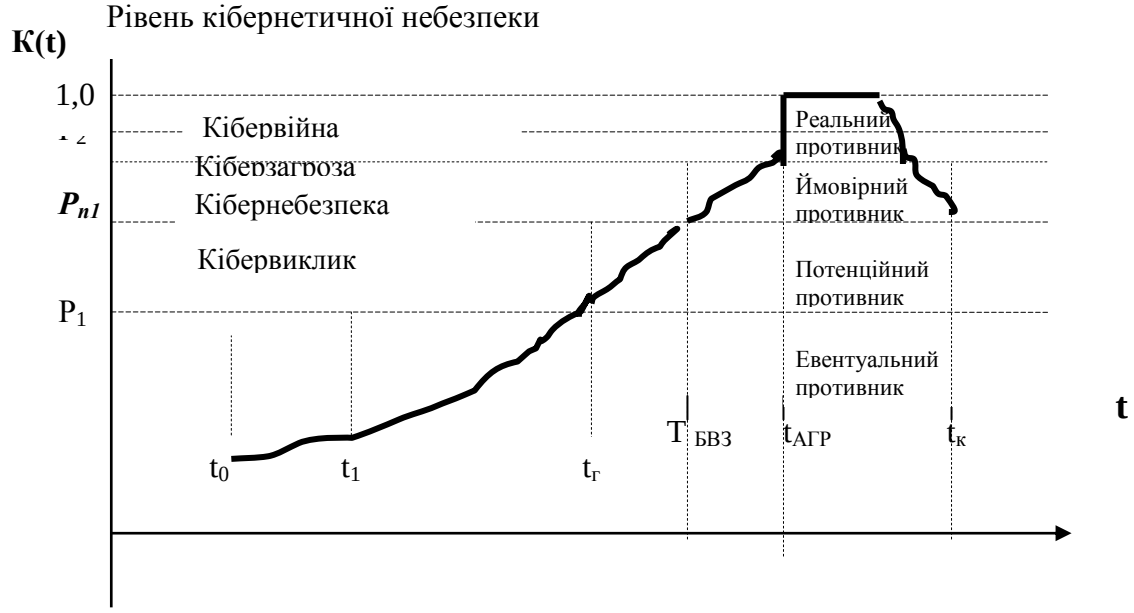

Рис. 2. Залежність зміни рівня кібернебезпеки з плином часу

При цьому слід враховувати, що функціонування системи забезпечення кібернетичної безпеки України повинно базуватися на специфічних принципах [17]:

- підпорядкованість діяльності ССЗКБ Конституції України і законам України;
- єдність і взаємозв'язок кібернетичної безпеки з іншими складовими національної безпеки держави;
- залежність складу і структури системи забезпечення кібернетичної безпеки держави від рівня прогнозованої кібернебезпеки (загрози) реалізації національних інтересів держави;
- пріоритетність заходів у практичній реалізації політики кібернетичної безпеки;
- своєчасну постановку реальних (за часом, ресурсами, силами і засобами) завдань із забезпечення кібернетичної безпеки держави та всебічного забезпечення їх ефективного виконання;
- використання прогнозно-аналітичного підходу до обґрунтування функцій системи забезпечення кібернетичної безпеки та її структурних елементів.

Реалізація зазначених принципів можлива на основі їх системного врахування при формуванні цільової функції системи забезпечення кібернетичної безпеки держави шляхом вибору відповідної системи показників оцінки її ефективності.

Перспективи подальшого розвитку в даному напряму. У подальших публікаціях буде запропоновано обгрунтування системи показників, що характеризують рівень кібернетичної небезпеки.

Література

1. National security strategy USA, may 2010, The White House, Washington, [Електронний ресурс]. – режим доступу: http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf;

2. The Secret War, by James Bamford, 06.12.13, [Електронний ресурс]. – режим доступу: http://www.wired.com/threatlevel/2013/06/general-keith-alexander-cyberwar;

3. Offensive and Defensive Cyber Weapons for Government and Private Sectors Global Market and Technologies Forecast - 2014-2024, Published: Oct 18, 2013, [Електронний ресурс]. – режим доступу: http://www.giiresearch.com/report/mig287441-offensive-defensive-cyber-weapons-government.html;

4. NATO and cyber defence [Електронний ресурс]. – режим доступу: http://www.nato.int/cps/en/natolive/topics_78170.htm;

5. Alexander Klimburg (Ed.), National Cyber Security Framework Manual, NATO CCD COE Publication, Tallinn 2012, [Електронний ресурс]. – режим доступу: http://www.ccdcoe.org/publications/ books/ National Cyber Security Framework Manual.pdf;

6. Проект закону України «Про кібернетичну безпеку України» від 04.06.2013 № 2207а. [Електронний ресурс]. – режим доступу: http://search.ligazakon.ua/l_doc2.nsf/link1/JG1PBA0A.html;

7. Проект «Стратегія забезпечення кібернетичної безпеки України» [Електронний ресурс]. – режим доступу: http://www.niss.gov.ua/public/File/2013_nauk_an_rozrobku/kiberstrateg.pdf;

8. Указ Президента України «Про Стратегію національної безпеки України» м. Київ 12 лютого 2007 року № 105/2007 [Електронний ресурс]. – режим доступу: http://zakon4.rada.gov.ua/laws/show/105/2007;

9. Закон України "Про основи національної безпеки України" // Відомості Верховної Ради України. — 2003. — № 39. — Ст. 351.;

10. Философский энциклопедический словарь. — М.: Советская энциклопедия. Гл. редакция: Л. Ф. Ильичёв, П. Н. Федосеев, С. М. Ковалёв, В. Г. Панов. 1983.;

11. Бурячок В.Л. Основи формування державної системи кібернетичної безпеки Монографія./ В.Л. Бурячок, – К.: НАУ.- 2013. – 432с.;

12. Мельник С.В. Тихомиров О.О. Лєнков О.С. "До проблеми формування понятійно-термінологічного апарату кібербезпеки" Збірник наукових праць Військового інституту Київського національного університету ім. Т.Г. Шевченка № 30 2011р.;

13. А.В. Тонконогов. Обеспечение кибернетической безопасности России в современных геополитических условиях. "Закон и право".-2011.-№10.-С.5-6;

14.Богданович В.Ю. Воєнна безпека України: методологія дослідження та шляхи забезпечення: [монографія] / В.Ю.Богданович. – К.: Тираж, 2003. – 322 с.

15.Богданович В.Ю. Теоретические основы анализа проблем национальной безопасности в военной сфере: [монографія] / В.Ю. Богданович. – К.: Основа, 2006. – 296 с

16.Богданович В.Ю. Теоретичні основи забезпечення національної безпеки України в умовах позаблоковості: монографія / В.Ю.Богданович, І.С.Романченко, І.Ю.Свида.- Львів: АСВ, 2011.-414 с.

17. Богданович В.Ю. Теоретико-методологічні основи забезпечення національної безпеки України (в 7 томах). Том 1. Теоретичні основи, методи і технології забезпечення національної безпеки України: монографія / В.Ю.Богданович, І.Ю.Свида, Є.Д.Скулиш. - К.: Наук.-вид.відділ НА СБ України. 2012.-548с.

Надійшла 05.11.2014 р. Рецензент: д.т.н., проф. Богданович И.Ю.