УДК 342.9

Ігор Діордіца,
канд. юрид. наук, доцент,
Національний авіаційний університет

СИСТЕМА ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ: СУТНІСТЬ ТА ПРИЗНАЧЕННЯ

У статті запропоновано авторське розуміння поняття «система забезпечення кібернетичної безпеки». У вузькому сенсі система забезпечення кібербезпеки – сукупність суб'єктів, які здійснюють свою діяльність у кіберпросторі. Зазначено, що система забезпечення кібербезпеки є цілісною системою, елементи якої тісно пов'язані між собою. Основними елементами даної системи є її суб'єкти та об'єкти. Резюмовано, що основним призначенням системи забезпечення кібербезпеки є сприяння у досягненні цілей кібернетичної безпеки, а тому основною функцією даної системи можна визначити забезпечення збалансованого існування інтересів особи, суспільства і держави шляхом здійснення перевірок, діагностування; виявлення та ідентифікацію, запобігання та припинення, мінімізацію та нейтралізацію дії внутрішніх і зовнішніх загроз і небезпек.

Ключові слова: кібернетична безпека, кібернетична загроза, кіберпростір, кібератака, забезпечення кібербезпеки, система забезпечення кібербезпеки.

Масове використання в останні десятиріччя у найрізноманітніших сферах суспільного життя комп'ютерних і телекомунікаційних технологій, включаючи інтернет-технології та надбання кібернетики, поряд зі значною кількістю переваг сприяло виникненню великої кількості загроз. Реалізація цих загроз завдає значної шкоди як на національному рівні, так і на міжнародній арені. Це спонукало до розуміння необхідності вирішення нагальної проблеми з метою мінімізації, ліквідації та попередження кіберзагроз.

За таких умов **актуальною** для здійснення наукового дослідження стає система забезпечення кібербезпеки, а саме її сутність та призначення. У зв'язку з цим можна виокремити декілька причин:

– по-перше, визначення сутності того чи іншого явища та наявність уніфікованої дефініції сприяє ґрунтовному виявленню предмета досліджень та наукових дискусій і вирішення можливих проблем;

– по-друге, проблема кібербезпеки в цілому та системи її забезпечення зокрема через свою специфіку є глобальною і неізольованою і у зв'язку з цим найефективніше може бути вирішена лише за умови скоординованої діяльності суб'єктів кібербезпеки. Тому для забезпечення ефективності взаємодії на міжнародному рівні необхідно узгоджене розуміння терміна «система забезпечення кібербезпеки».

На підставі аналізу сучасних досліджень і публікацій можна дійти висновку про те, що проблеми забезпечення кібернетичної безпеки України в умовах соціальних трансформацій, актуальні напрями підвищення ефективності системи забезпечення кібернетичної безпеки, її функції та завдання розглядаються у наукових працях вітчизняних дослідників, а саме: В. А. Ліпкана [1-2], І. В. Тімкіна, Н. Є. Новікова [3], І. В. Діордіци [4-5], С. В. Мельника, В. І. Кащука [6], В. П. Шеломенцева [8-9] та інших. Проте, незважаючи на значну кількість робіт із даної тематики, натепер залишилось багато невирішених питань щодо сутності та призначення системи забезпечення кібернетичної безпеки України.

> Саме тому **мета** статті полягає у дослідженні системи забезпечення кібербезпеки, для досягнення якої поставлені такі **завдання**: запропонувати авторське розуміння даного поняття, визначити суб'єктів та об'єкт системи, сутність та її призначення.

Виклад основного матеріалу. Щодо визначення самого терміна *система забезпечення кібербезпеки* варто акцентувати увагу на відсутності уніфікованої дефініції як на законодавчому, так і на доктринальному рівні. Незважаючи на певну кількість чинних нормативно-правових актів у сфері кібернетичної безпеки, це питання залишається актуальним та потребує ґрунтовного наукового дослідження, вироблення відповідних пропозицій та рекомендацій і подальшої законодавчої уніфікації.

Із наявних напрацювань у безпековій сфері зазначимо такі визначення:

– *система забезпечення безпеки* – механізм із вироблення, перетворення і реалізації концепції, стратегії і тактики у сфері безпеки за допомогою скоординованої діяльності державних і недержавних структур; сукупність організаційно об'єднаних органів управління, сил і засобів, призначених для вирішення завдань щодо забезпечення національної безпеки [1, с. 314]. Це визначення є досить вдалим і може бути використане у формулюванні терміна «система забезпечення кібербезпеки»;

– У Концепції (основи державної політики) національної безпеки України поняття *системи забезпечення національної безпеки* визначалося як «організована державою сукупність суб'єктів: державних органів, громадських організацій, посадових осіб та окремих громадян,

об'єднаних цілями та завданнями щодо захисту національних інтересів, що здійснюють узгоджену діяльність у межах законодавства України». А у нинішньому Законі України «Про основи національної безпеки України» визначення даного поняття взагалі відсутнє [2, с. 256], що є незрозумілим як із наукової точки зору, так і з практичної, оскільки унеможливлює правозастосування у будь-якій сфері життєдіяльності, адже відсутність легітимованого визначення родового поняття не сприяє його диференціації залежно від різних видів суспільних відносин, у тому числі й у сфері кібербезпеки;

– *система забезпечення національної безпеки* виступає як організаційна система державних та недержавних інституцій, інших суб'єктів, які покликані вирішувати завдання забезпечення національної безпеки у визначений законодавством спосіб [3]. Це визначення є досить абстрактним та потребує конкретики;

– *загальна система забезпечення національної безпеки* України – це єдиний державно-правовий механізм, у якому кожний суб'єкт безпеки виконує функції захисту національних інтересів у межах повноважень, які визначаються законодавством України. Діяльність суб'єктів забезпечення національної безпеки має бути доступною для контролю відповідно до законодавства України [14, с. 128].

У тлумачному словнику української мови містяться такі визначення: *забезпечення* – сукупність методів, засобів і заходів, необхідних для нормального функціонування того чи іншого об'єкта, процесу; процес створення надійних умов для чи то здійснення, чи то гарантування, чи то захисту, чи то охорони кого-, чого-, щонебудь від загрози або безпеки [1, с. 118], а *система* – сукупність об'єктів і відносин між ними, що у своїй органічній єдності утворюють нову якість [17, с. 314].

Виходячи із сукупності спільних «елементів» у вищезазначених дефініціях, зауважу, що в широкому сенсі під *системою забезпечення кібербезпеки* варто розуміти сукупність організаційно об'єднаних органів управління, а саме: державних органів, громадських організацій, посадових осіб та окремих громадян, які спрямовують свою діяльність на створення умов для реалізації національних інтересів у кіберпросторі, а також сил, засобів і методів, які використовуються для досягнення даної цілі відповідно до законодавства України [4]. Також можна додати, що система забезпечення кібербезпеки є єдиним державно-правовим механізмом, та всі його суб'єкти діють чітко в межах, визначених законодавством. Однак, не занурюючись у глибини теоретичних дискусій щодо співвідношення природного та позитивного права, відзначу, що дана система, передусім, спрямовує свою діяльність на реалізацію національних інтересів, тому якщо законодавство у даній сфері не відповідає сучасним тенденціям, то одним із компенсаторних механізмів мають виступати включення недержавного складника у вигляді інформаційних волонтерів із подальшою легітимацією відповідних кібернетичних функцій.

У вузькому сенсі *система забезпечення кібербезпеки* – сукупність органічної об'єднаних спільними цілями суб'єктів, які здійснюють свою діяльність у кіберпросторі з метою реалізації національних інтересів.

Але нині не сформовано чіткої та несуперечливої категорійно-понятійної системи у сфері кібербезпеки, адже:

- немає парадигмальних визначень ключових понять: «кібернетична безпека», «система кібернетичної безпеки», «система забезпечення кібернетичної безпеки»;
- не визначено структурно-генетичні зв'язки між ними та явищами, що вони описують.

Офіційне визначення поняття кібербезпеки міститься в Стратегії кібербезпеки, де, сповідуючи калькований підхід із Закону України «Про основи національної безпеки України», в якому визначено поняття «національна безпека», під ***кібербезпекою*** розуміється стан захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі, що досягається комплексним застосуванням сукупності правових, організаційних, інформаційних заходів.

Помилковість даної конструкції доведена в численних монографіях і дослідженнях. Водночас, зважаючи на відсутність відкритості процесів розроблення документів концептуального значення, збереження даної формули будови поняття свідчить про небажання авторів цих нормативно-правових актів дослуховуватись до науковців і їхнє несприйняття обґрунтованих аргументів щодо неправильності і помилковості ототожнення безпеки зі станом захищеності. Тому в окремих подальших своїх публікаціях, відповідно до теми мого дослідження, я також розгляну більш детально підходи до визначення даного поняття з урахуванням сучасних трансформаційних тенденцій інформаційної глобалізації.

Кожна держава індивідуально визначає сфери, які вона відносить до кібернетичної безпеки, перелік об'єктів і суб'єктів її забезпечення, виходячи зі тих стратегічних цілей і завдань, які стоять перед державою на національному та міжнародному рівнях, та її практичних можливостей реалізації національних інтересів.

На даному етапі, виходячи з проведеного мною структурно-функціонального аналізу елементів національної системи кібербезпеки, поняття кібернетичної безпеки поки розглядається та інтерпретується як складова частина поняття інформаційної безпеки, оскільки сутність та природа загроз, методів, засобів і заходів однакова та обмежується лише кіберпростором.

Водночас, на мій погляд, зважаючи на:

1) віртуалізацію та цифровізацію сучасного світу;

2) перенесення більшості державних функцій у кібернетичний простір;

3) зародження, формування та розвиток окремих національних інтересів безпосередньо в кіберпросторі;

4) залежність ефективного функціонування об'єктів критичної інфраструктури та інформаційної інфраструктури від рівня кібербезпеки;

5) необхідність формування кібербезпекової культури як засади функціонування сучасної людини;

6) формування інфраструктури електронних комунікацій

можу чітко висновувати про **формування кібернетичної функції держави** як однієї з основних функцій. Це є елементом наукової новизни і дане питання в такій інтерпретації порушується **в рамках української науки вперше**.

Нині кіберпростір, незалежно від наявних підходів до його визначення, унікальне явище, оскільки він не має державних кордонів та об'єднує в собі такі складники, як:

- кібернетичний простір,
- кібернетичні ресурси,
- кібернетичну інфраструктуру та
- кібернетичні технології.

Відповідно, кібернетична безпека, так само як і інформаційна безпека, є не лише невід'ємним складником кожної зі сфер національної безпеки, а й водночас виступає самостійною сферою забезпечення національної безпеки, що зазначено в Законі України «Про основи національної безпеки України», а також у Доктрині інформаційної безпеки України.

Отже, можу стверджувати, що, зважаючи на окремий склад правовідносин, кібернетична сфера є самостійною сферою забезпечення національної безпеки, окремим елементом системи стратегічних комунікацій, а також додатково виступає самостійною сферою забезпечення міжнародної безпеки, безпеки громадян і бізнесу у кіберпросторі.

Таким чином, суспільні відносини у сфері кібербезпеки мають особливу специфіку та потребують окремого законодавчого урегулювання, що і підтверджується більшістю випадків міжнародної практики [6, с. 253-254]. Даний факт також знайшов своє адекватне відображення і в українському законодавстві, коли поряд із Доктриною інформаційної безпеки України було ухвалено Стратегію кібербезпеки України. Звичайно, постає питання щодо конкуренції правових норм, але це окрема наукова проблема, яку я розглядатиму в наступних своїх публікаціях.

Система забезпечення кібербезпеки має бути цілісною системою, елементи якої тісно пов'язані між собою. Основними елементами даної системи є її суб'єкти та об'єкти.

Як основні *об'єкти системи забезпечення кібербезпеки* пропоную визначити національні цінності та національні інтереси (не лише у кіберпросторі).

Виходячи зі змісту положень Закону України «Про основи національної безпеки України» та Доктрини інформаційної безпеки України, об'єктами кібернетичної безпеки України слід визначити:

– особу – її права і свободи на збирання, зберігання, використання та поширення інформації, що реалізовуються за допомогою ІТС;

– суспільство – та частина його духовних, морально-етичних, культурних, історичних, інтелектуальних і матеріальних цінностей, що формуються з використанням ІТС;

– державу – її суверенітет і недоторканність у кіберпросторі, спроможність виконувати свої функції за допомогою ІТС [7, с. 312].

Кібернетична безпека будь-якої держави через свою багатоаспектність і комплексність потребує соціальної системи її забезпечення, основним призначенням якої є виконання певних дій, спрямованих, перш за все, на захист національних цінностей, реалізацію національних інтересів. Тобто йдеться про систему забезпечення кібернетичної безпеки.

Система забезпечення кібернетичної безпеки являє собою організаційне об'єднання державних та недержавних інституцій, а також інших суб'єктів.

Суб'єкти забезпечення кібернетичної безпеки – державні органи, (передусім, інституції сфери безпеки і оборони України), органи місцевого самоврядування, підприємства, установи, організації незалежно від форми власності, які здійснюють проектування, впровадження та експлуатацію складових критичних об'єктів національної інформаційної інфраструктури або забезпечують їх кіберзахист [15].

Серед суб'єктів забезпечення кібернетичної безпеки виділяють загальні та спеціальні.

До загальних суб'єктів забезпечення кібернетичної безпеки належать: Президент України; Верховна Рада України; Рада національної безпеки і оборони України; Кабінет Міністрів України; Збройні Сили України; Служба безпеки України; Служба зовнішньої розвідки України; Національний банк України; інші міністерства та центральні органи виконавчої влади; місцеві державні адміністрації та органи місцевого самоврядування; суб'єкти підприємницької діяльності різних форм власності у сфері виробництва інформаційних продуктів та надання інформаційних послуг.

Спеціальними суб'єктами забезпечення кібернетичної безпеки є державні органи, які, крім загальних функцій, уповноважені на здійснення боротьби з кіберзлочинністю та кібертероризмом, а також на забезпечення кібернетичного захисту об'єктів національної критичної інфраструктури. До таких суб'єктів належать: Міністерство внутрішніх справ України; Служба безпеки України; Державна служба спеціального зв'язку та захисту інформації України; Міністерство юстиції України; Генеральна прокуратура України [5].

Суб'єкти системи забезпечення кібернетичної безпеки перебувають у тісній взаємодії між собою, але при цьому кожен із них спеціалізується на вирішенні конкретних завдань відповідно до своєї предметної компетентності та в межах повноважень, визначених законодавством. Незважаючи на це, загрози кібербезпеці актуалізуються через дію таких чинників, як недостатній рівень координації, взаємодії та інформаційного обміну між суб'єктами забезпечення кібербезпеки [16].

У процесі взаємодії об'єктів і суб'єктів системи забезпечення кібербезпеки виникають деякі функціональні особливості. Так, завдання щодо забезпечення національних інтересів покладаються, передусім, на державу та її інсти-

тути, а суспільство і громадяни беруть меншу участь у відповідних процесах.

Зауважу, що у разі відсутності системи забезпечення кібернетичної безпеки стане неможливим надійний захист основ кібернетичної безпеки, що спричинить тотальні модифікації і для окремих елементів, і для всієї системи в цілому.

Одним із понять, що описують зміст діяльності системи забезпечення, є такий термін, як *призначення* – роль, завдання кого-, чого-небудь у житті, існуванні [17, с. 538].

Таким чином, *основним призначенням* системи забезпечення кібербезпеки є сприяння у досягненні цілей кібернетичної безпеки, а тому основною функцією даної системи можна визначити забезпечення збалансованого існування інтересів особи, суспільства і держави шляхом здійснення перевірок, діагностування; виявлення та ідентифікацію, запобігання та припинення, мінімізацію та нейтралізацію дії внутрішніх і зовнішніх загроз і небезпек у кібернетичній сфері. Дані реакції на загрози повинні бути адекватними характеру та масштабам, а також рівню можливого і бажаного стану забезпечення кібернетичної безпеки.

Ефективність функціонування системи забезпечення кібербезпеки насамперед залежить від досконалості нормативно-правового регулювання діяльності відповідної системи державних та громадських органів, а також неурядових організацій.

Щодо законодавчого закріплення, то зауважу, що система забезпечення кібернетичної безпеки України створюється і розвивається відповідно до Конституції України та інших нормативно-правових актів, що регулюють суспільні відносини у сфері управління національною безпекою в цілому та кібернетичною безпекою зокрема. Законодавчо-правову основу забезпечення національної безпеки України становлять Конституція України, Закони України «Про національну безпеку України», «Про Раду національної безпеки і оборони України», «Про Службу безпеки України», Стратегія національної безпеки України, Стратегія кібербезпеки України, Доктрина інформаційної безпеки України, Положення про Національний координаційний центр кібербезпеки тощо, а також інші нормативно-правові акти державних органів влади й управління; міжнародні договори й угоди, укладені чи визнані Україною, які відповідають національним інтересам України.

Таким чином, за своєю організаційно-функціональною та ресурсною спроможністю система забезпечення кібернетичної безпеки повинна гарантувати інформаційний суверенітет, територіальну цілісність, сталий розвиток, добробут та кібернетичну безпеку громадян.

Аналіз законодавства України, а також низки наукових напрацювань фахівців різних відомств, на які покладено завдання забезпечення кібербезпеки, свідчить про фрагментарність понятійного поля вказаної сфери, що унеможливлює формування дієвих нормативно-правових документів із протидії кіберзагрозам. При цьому подекуди законодавець оперує термінами в кіберсфері, юридичних визначень яких фактично немає. Це стосується і таких основоположних термінів, як «кіберпростір» та «кіберзагроза» [12, с. 82].

Забезпечення кібербезпеки України як стану захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі, що досягається комплексним застосуванням сукупності правових, організаційних, інформаційних заходів, має базуватися на принципах:

– верховенства права і поваги до прав та свобод людини і громадянина;

– забезпечення національних інтересів України;

– відкритості, доступності, стабільності та захищеності кіберпростору;

– державно-приватного партнерства, широкої співпраці з громадянським суспільством у сфері забезпечення кібербезпеки та кіберзахисту;

– пропорційності та адекватності заходів кіберзахисту реальним та потенційним ризикам;

– пріоритетності запобіжних заходів;

– невідворотності покарання за вчинення кіберзлочинів;

– пріоритетного розвитку та підтримки вітчизняного наукового, науково-технічного та виробничого потенціалу;

– міжнародного співробітництва з метою зміцнення взаємної довіри у сфері кібербезпеки та вироблення спільних підходів у протидії кіберзагрозам, консолідації зусиль у розслідуванні та запобіганні кіберзлочинам, недопущення використання кіберпростору в протиправних та воєнних цілях;

– забезпечення демократичного цивільного контролю над утвореними відповідно до законів України військовими формуваннями та правоохоронними органами держави, що діють у сфері кібербезпеки.

Проводячи постійно паралель між забезпеченням кібернетичної та національної безпеки, зауважу, виходячи з нормативного закріплення, що основними принципами забезпечення кібернетичної безпеки також можна визначити: пріоритет договірних (мирних) засобів у розв'язанні конфліктів; своєчасність і адекватність заходів захисту національних інтересів реальним і потенційним загрозам; чітке розмежування повноважень та взаємодія органів державної влади у забезпеченні кібернетичної безпеки; демократичний цивільний контроль над всіма державними структурами в системі національної безпеки; використання в інтересах України міждержавних систем та механізмів міжнародної колективної безпеки.

Визначаючи сутність забезпечення кібернетичної безпеки, зазначу, що *сутність* – найголовніше, основне, істотне в кому-, чому-небудь; суть, сенс, зміст [17, с. 631].

Кібербезпека є дуже важливим аспектом у сучасному світі. Захист інформації передбачає досягнення та збереження властивостей безпеки в ресурсах користувачів, що спрямовані на запобігання відповідним кіберзагрозам. Україна посіла п'яте місце в світі (і перше в Євро-

пі) за ризиками зіткнення з веб-загрозами в третьому кварталі 2016 року. Третина (33,7 %) українських користувачів мережі зіткнулися із загрозами, що поширюються через інтернет, що і є дуже важливим показником актуальності кібербезпеки [13, с. 77].

Стрімке впровадження інформаційних технологій у всі сфери життя, глобалізація інформаційних відносин зумовлюють світову тенденцію до перенесення протиправної діяльності у кібернетичний простір. Сьогодні комп'ютерна злочинність, чи кіберзлочинність, для якої не існує державних кордонів, загрожує не лише правам та майну громадян, а й посягає на національні інтереси.

Спостерігається висока вразливість кібернетичного простору перед кібератаками, діяльністю злочинних угруповань, хакерів, промислово-фінансових груп та осіб, допущених до роботи із системами в порядку здійснення службової діяльності (інсайдерів). Випадки негативного кібервпливу стають частішими, організованішими, більш легкими та дешевими в підготовці і реалізації.

Останнім часом збільшується кількість кібератак в Україні. Зокрема, зазначу про одну з останніх.

27 червня 2017 року хакери атакували низку українських банків. Компанія «Київенерго» також у цей день зазнала хакерської атаки. Там розповіли, що були змушені вимкнути всі комп'ютери. ЗМІ повідомили, що вірусна атака хакерів заблокувала майже всі комп'ютери «Запоріжжяобленерго», «Дніпроенерго» та Дніпровської електроенергетичної системи. Державний «Ощадбанк» обмежив деякі функції з обслуговування клієнтів через хакерську атаку на українські банки. Хакери атакували найбільший український аеропорт – «Бориспіль» та здійснили кібератаку на комп'ютерні сервери Кабінету міністрів. Також українська компанія експрес-доставки «Нова пошта» зазнала хакерської атаки. «Укрпошта» і «Укртелеком» теж зазнали хакерської атаки, комп'ютерні системи підприємств не працювали [18].

Масштабна хакерська атака із використанням різновиду віруса Petya, яка відбулася 27 червня 2017 року, спричинила порушення роботи українських державних підприємств, установ, банків, медіа тощо. Внаслідок атаки була заблокована діяльність таких підприємств, як аеропорт «Бориспіль», ЧАЕС, Укртелеком, Укрпошта, Ощадбанк, Укрзалізниця та низка інших великих підприємств.

Жертвою вірусу також стали Кабінет Міністрів України, телеканал «Інтер», медіахолдинг ТРК «Люкс», до складу якого входять «24 канал», «Радіо Люкс FM», «Радіо Максимум», різні інтернет-видання, а також сайти Львівської міської ради, Київської міської державної адміністрації, кіберполіції та Служби спецзв'язку України. Трансляції передач припинили канали «Перший автомобільний» та ТРК «Київ». 28 червня 2017 року Кабінет Міністрів України повідомив, що атака на корпоративні мережі та мережі органів влади зупинена [19].

Хоча запобігти кібернетичним атакам технічно вбачається можливим лише за певних умов, незалежно від складності систем захисту своєчасне виявлення та швидке адекватне реагування на кібернетичні атаки дає змогу значно мінімізувати наслідки таких атак [8, с. 205].

Неконтрольоване поширення та необмежене застосування інформаційного і кіберпросторів протягом останніх десятиріч:

1) призвело до уразливості інформаційної сфери більшості країн світу для стороннього кібернетичного впливу;

2) визначило політичну необхідність контролю і подальшого регулювання відносин у цій царині;

3) дало підстави стверджувати про особливу актуальність: процесів пошуку, збирання й добування інформації у відкритих, відносно відкритих і закритих електронних джерелах; заходів із забезпечення конфіденційності, цілісності та доступності власного ІР, а також протидії цілеспрямованому впливу з боку потенційно можливих кібернетичних втручань і загроз. Зважаючи на це та враховуючи постійно зростаючий потенціал використання мережі Internet у військових цілях, провідні країни світу – США, Японія, Франція, Велика Британія, Росія, Китай та багато інших – протягом останніх років активно модернізують власні сектори безпеки, й передусім безпеки кібернетичної, відводячи при цьому головну роль проблемі завоювання інформаційної переваги в управлінні військами (силами) і зброєю, а також удосконаленню нормативно-правової бази [9, с. 8].

Побудова дієвої системи забезпечення кібернетичної безпеки вимагає від державних органів України чіткого визначення державної політики у цій сфері та випереджального реагування на динамічні зміни, що відбуваються у світі у сфері забезпечення кібернетичної безпеки. При цьому вибір конкретних засобів і шляхів забезпечення кібернетичної безпеки України зумовлюється необхідністю своєчасного вжиття заходів, адекватних характеру і масштабам реальних та потенційних кібернетичних загроз життєво важливим інтересам людини і громадянина, суспільства і держави. Організаційне забезпечення системи кібербезпеки також можна розглядати як цілеспрямовану діяльність суб'єкта забезпечення кібербезпеки, пов'язану:

– зі створенням і впорядкуванням (розвитком) організаційних структур, найбільш доцільних для забезпечення безпеки у кіберпросторі;

– з упорядкуванням (налагодженням) процесу управління у сфері забезпечення безпеки у кіберпросторі, забезпеченням найліпших умов для прийняття та реалізації відповідних управлінських рішень.

Організаційне забезпечення системи кібербезпеки характеризується місцем і роллю спеціальних суб'єктів (відповідних державних органів та їх спеціалізованих підрозділів), їх функціями, повноваженнями, а також підставами, умовами і напрямами їх взаємодії під час здійснення заходів із забезпечення безпеки у кіберпросторі [5].

Досвід іноземних країн та особливості українських реалій свідчать, що розв'язання основних завдань кібербезпеки неможливе без створення:

1) міжвідомчого структурного органу, який на постійній основі забезпечував би координацію діяльності певних відомств, правоохоронних і силових структур України з питань забезпечення кібернетичної безпеки. Кібератака 27 червня 2017 року на Україну довела неефективність діяльності Національного координаційного центру кібербезпеки, поставила питання не про демагогічні та популістські формування недієздатних центрів / органів, а про формування відповідно до національних інтересів національної системи кібербезпеки, власне, як на те вказується безпосередньо в Стратегії кібербезпеки України;

2) центральних органів у структурі певних відомств, правоохоронних і силових структур України з функціями виявлення та оцінювання рівня (визначення ступеня) критичності стороннього кібервпливу, розроблення концептуальних засад та надання рекомендацій щодо протидії його проявам, а також активної протидії кібератакам протиборчих сторін та впливу на їх ІТС;

3) органів власної інформаційної і кібербезпеки – державних установ (відомств) та комерційних структур, які повинні тісно взаємодіяти із зазначеними центральними органами з питань вироблення єдиної політики щодо захисту як власного, так і спільного національного інформаційного і кіберпросторів [9, с. 8-9].

Взявши за приклад досвід Великої Британії, зауважу, що основними напрямами державної політики національної безпеки України в інформаційній сфері варто визначити такі:

– забезпечення інформаційного суверенітету держави, складником якого виступає кібернетичний суверенітет;

– вдосконалення державного регулювання розвитку кібернетичної сфери через створення нормативно-правових, фінансово-економічних та інформаційних передумов для розвитку національної інформаційної інфраструктури й ресурсів, упровадження новітніх кібернетичних технологій у найбільш важливих сферах життєдіяльності;

– активне залучення засобів масової інформації не лише до висвітлення тих чи інших подій, а й до прямого формування кібербезпекової культури, формування масової свідомості безпекової людини, негативне ставлення до тероризму, кібершпигунства, промислового шпигунства, кіберзлочинності в цілому як явищ, що виступають загрозами сучасному кібернетичному світу;

– забезпечення неухильного дотримання прав громадян на свободу слова та доступу до інформації;

– вжиття комплексних заходів щодо захисту національного інформаційного простору й протидії монополізації інформаційної сфери України у тому числі крупними мережами на кшталт Facebook.

Україна нині потребує подальшого нормативного врегулювання суспільних відносин у сфері кібербезпеки. Для цього необхідно здійснити низку заходів із розроблення та прийняття Концепції державної інформаційної політики України, яка має виступати вихідним документом для Доктрини інформаційної безпеки України і Стратегії кібернетичної безпеки. Останні, своєю чергою, мають розвивати положення Концепції у напрямі визначення конкретних шляхів реалізації національних інтересів.

Нині, зважаючи на викладене, я не можу підтримати пропозицію окремих авторів щодо нагальної потреби у прийнятті Закону України «Про кібербезпеку» як необхідного інструмента забезпечення кібернетичної безпеки держави [10, с. 88]. У рамках діяльності наукової школи доктора юридичних наук В.А. Ліпкана було здійснене системне дослідження рівня забезпечення інформаційної безпеки, а також урегульованості численних складників інформаційних правовідносин. Натепер загальна кількість нормативно-правових актів перевищує 4 500. Водночас говорити про злагоджене та ефективне функціонування державно-правового механізму не доводиться й донині. Таким чином, законодавчі ініціативи у цьому разі мають виходити з потреб практики, а не виступати завершальною частиною якоїсь дисертації або наукової статті. За логікою О.О. Климчука тоді потрібно за кожної з 9 сфер життєдіяльності відповідно до Закону України «Про основи національної безпеки України» розробляти окремі закони. Але цей шлях – множення законодавства – є безперспективним.

Тому вбачаємо необхідним приведення у відповідність чинного законодавства і кібернетичної сфери та у разі потреби його доповнення актуальними загрозами та відповідними їм напрямами державної політики кібернетичної безпеки.

Хоча український кіберпростір давно є складником світового, держава ще недостатньо долучилася до міжнародної співпраці щодо досягнення належного рівня його безпеки. Поряд із контролем проведення організаційних та технічних заходів забезпечення кібербезпеки, пріоритетним завданням держави все ж має стати створення несуперечливої законодавчої бази як основи здійснення такої діяльності.

Різними авторами у різні часи неодноразово наголошувалося на необхідності створення власної Стратегії кібербезпеки, основою якої повинна стати Доктрина інформаційної безпеки України [11, с. 397]. Така нормотворча діяльність стала першим кроком у досягненні належного рівня кібербезпеки Україною у світі інформаційних і комунікаційних технологій.

Переформульовуючи положення Доктрини інформаційної безпеки України, зауважу, що пріоритетами державної політики в системі забезпечення кібернетичної безпеки мають бути:

- створення ефективної системи протидії кіберзагроз, їх попередження та усунення негативних наслідків; перегляд та конкретизація повноважень суб'єктів забезпечення кібербезпеки;
- боротьба з дезінформацією та деструктивною пропагандою з боку Російської Федерації;

• забезпечення захисту і розвитку кібернетичного простору України, а також конституційного права громадян на доступ до інформації;

• формування позитивного міжнародного іміджу України.

Актуальність формування дієвої системи забезпечення кібернетичної безпеки України зумовлена тим, що в сучасних глобалізаційних процесах значно зростає уразливість інформаційно-телекомунікаційних систем, що функціонують в інтересах управління державою, забезпечують потреби обороноздатності та безпеки держави; кредитно-банківської та інших сфер економіки; систем управління об'єктами критичної інфраструктури.

Таким чином, у результаті здійсненого дослідження можу **резюмувати**, що система забезпечення кібербезпеки є єдиним державно-правовим механізмом та всі його суб'єкти діють чітко в межах, визначених законодавством.

У вузькому сенсі система забезпечення кібербезпеки – сукупність суб'єктів, які здійснюють свою діяльність у кіберпросторі.

Система забезпечення кібербезпеки є цілісною системою, елементи якої тісно пов'язані між собою. Основними елементами даної системи є її суб'єкти та об'єкти.

Як основні об'єкти системи забезпечення кібербезпеки варто визначити національні цінності та національні інтереси (не лише у кіберпросторі). Суб'єктами забезпечення кібернетичної безпеки є державні органи (передусім, інституції сектору безпеки й оборони України), органи місцевого самоврядування, підприємства, установи, організації незалежно від форми власності, які здійснюють проектування, впровадження та експлуатацію складових критичних об'єктів національної інформаційної інфраструктури або забезпечують їх кіберзахист. Основним призначенням системи забезпечення кібербезпеки є сприяння у досягненні цілей кібернетичної безпеки, а тому основною функцією даної системи можна визначити забезпечення збалансованого існування інтересів особи, суспільства і держави шляхом здійснення перевірок, діагностування; виявлення та ідентифікацію, запобігання та припинення, мінімізацію та нейтралізацію дії внутрішніх і зовнішніх загроз і небезпек.

Список використаних джерел:

1. Ліпкан В. А. Національна і міжнародна безпека у визначеннях та поняттях / В. А. Ліпкан, О. С. Ліпкан. – 2-ге вид., доп. і перероб. – К.: Текст, 2008. – 400 с.

2. Ліпкан В. А. Національна безпека України : навчальний посібник / В. А. Ліпкан. – 2-ге вид. – К. : КНТ, 2009. – 576 с.

3. Тімкін І. Ф. Структурно-функціональна характеристика системи забезпечення національної безпеки України [Електронний ресурс] / І. Ф. Тімкін, Н. Є. Новікова. – Режим доступу : er.nau.edu.ua

4. Поняття та зміст системи забезпечення кібербезпеки [Електронний ресурс]. – Режим доступу : http://goal-int.org

5. Діордіца І. В. Поняття та зміст національної системи кібербезпеки [Електронний ресурс] / І. В. Діордіца. – Режим доступу : http://goal-int.org/ponyattya-ta-zmist-nacionalnoi-sistemi-kiberbezpeki/

6. Мельник С. В. Актуальні напрями попередження правопорушень у кіберпросторі як складова стратегії кібернетичної безпеки держави Інформаційна безпека: виклики і загрози сучасності : зб. матеріалів наук.-практ. конф., 5 квітня 2013 року, м. Київ / С. В. Мельник, В. І. Кащук. – К. : Наук.-вид. центр НА СБ України, 2013. – 416 с.

7. Шеломенцев В. П. Правове забезпечення системи кібернетичної безпеки України та основні напрями її удосконалення / В. П. Шеломенцев // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2012. – Вип. 1. – С. 312–320.

8. Шеломенцев В. П. Формування законодавчих основ забезпечення кібербезпеки України / В. П. Шеломенцев // Інформаційна безпека: виклики і загрози сучасності : зб. матеріалів наук.-практ. конф., 5 квітня 2013 року, м. Київ. – К. : Наук.-вид. центр НА СБ України, 2013. – 416 с.

9. Бурячок В. Л. Характерні ознаки та проблемні аспекти забезпечення кібернетичної безпеки / В. Л. Бурячок, С. О. Гнатюк, О. Г. Корченко // Інформаційна безпека: виклики і загрози сучасності : зб. матеріалів наук.-практ. конф., 5 квітня 2013 року, м. Київ. – К. : Наук.-вид. центр НА СБ України, 2013. – 416 с.

10. Климчук О. О. Правові основи кібернетичної безпеки Великої Британії / О. О. Климчук // Інформаційна безпека: виклики і загрози сучасності : зб. матеріалів наук.-практ. конф., 5 квітня 2013 року, м. Київ. – К. : Наук.-вид. центр НА СБ України, 2013. – 416 с.

11. Морозюк С. П. Шляхи підвищення рівня безпеки кібернетичного простору України / С. П. Морозюк // Інформаційна безпека: виклики і загрози сучасності : зб. матеріалів наук.-практ. конф., 5 квітня 2013 року, м. Київ. – К. : Наук.-вид. центр НА СБ України, 2013. – 416 с.

12. Єрьоміна Л. В. Напрями удосконалення законодавства України у сфері кібербезпеки: термінологічний аспект / Л. В. Єрьоміна // Інформаційна безпека: виклики і загрози сучасності : зб. матеріалів наук.-практ. конф., 5 квітня 2013 року, м. Київ. – К. : Наук.-вид. центр НА СБ України, 2013. – 416 с.

13. Бабич Є. Ю. Забезпечення кібербезпеки в Україні / Є. Ю. Бабич // Актуальні задачі та досягнення у галузі кібербезпеки : матеріали Всеукр. наук.-практ. конф., м. Кропивницький, 23–25 листоп. 2016 р. – Кропивницький : КНТУ, 2016. – С. 77–78.

14. Політологія : навчальний посібник / [М. П. Гетьманчук, В. К. Грищук, Я. Б. Турчин та ін.]; за заг. ред. М. П. Гетьманчука. – К.: Знання, 2010. – 415 с.

15. Стратегія забезпечення кібернетичної безпеки України (Проект) [Електронний ресурс]. – Режим доступу : www.niss.gov.ua/public/File/2013_nauk.../kiberstrateg.pdf

16. Стратегія кібербезпеки України від 15.03.2016 [Електронний ресурс]. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/96/2016

17. Великий тлумачний словник сучасної української мови / гол. ред. В. Т. Бусел, редактори-лексикографи: В. Т. Бусел, М. Д. Василега-Дерибас, О. В. Дмитрієв [та ін.]. – К.: Ірпінь: ВТФ «Перун», 2005. – 1728 с.

18. Кібератака на Україну: СБУ залучила міжнародних експертів, 27 червня 2017 р. [Електронний ресурс]. – Режим доступу : http://espreso.tv/news/2017/06/27/kiberataka_na_ukrayinu_sbu_zaluchyla_mizhnarodnykh_ekspertiv

19. Хакерські атаки на Україну (2017) [Електронний ресурс]. – Режим доступу : https://uk.wikipedia.org/wiki/%D0%A5%D0%B0%D0%BA%D0%B5%D1%80%D1%81%D1%8C%D0%BA%D1%96_%D0%B0%D1%82%D0%B0%D0%BA%D0%B8_%D0%BD%D0%B0_%D0%A3%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D1%83_(2017)

В статье предложено авторское понимание понятия «система обеспечения кибернетической безопасности». В узком смысле система обеспечения кибербезопасности – совокупность субъектов, осуществляющих свою деятельность в киберпространстве. Отмечено, что система кибербезопасности является целостной системой, элементы которой тесно связаны между собой. Основными элементами данной системы являются ее субъекты и объекты. Резюмировано, что основным назначением системы обеспечения кибербезопасности является содействие в достижении целей кибернетической безопасности, а потому основной функцией данной системы можно определить обеспечение сбалансированного существования интересов личности, общества и государства путем осуществления проверок, диагностики; выявление и идентификацию, предотвращение и пресечение, минимизацию и нейтрализацию действия внутренних и внешних угроз и опасностей.

Ключевые слова: кибернетическая безопасность, кибернетическая угроза, киберпространство, кибератака, обеспечение кибербезопасности, система обеспечения кибербезопасности.

It was marked that basing on the set of common elements in the existing definitions, is was offered to understand under the cybersecurity system the totality of organizationally united management bodies, namely: state bodies, public organizations, officials and individuals who direct their activities into protecting of the cyberspace from attacks, as well as the forces, means and methods which are used to achieve the goal within the Ukrainian legislation. It can also be added that the cybersecurity system is the only state-legal mechanism, and all its subjects act clearly within the frameworks of the legislation. It was noted that in the narrow sense, the cybersecurity system is a set of subjects that carry out their activities in cyberspace. The cybersecurity system is an integral system, the elements of which are closely interconnected. The main elements of this system are its subjects and objects. It was proposed to identify national values and national interests (not only in cyberspace) as the main objects. Subjects of the providing of the cybernetic security – state bodies (primarily the institutions of the security and defense sector of Ukraine), local self-government bodies, enterprises, institutions, organizations irrespective of the form of ownership, which carry out the design, implementation and operation of the components of the critical objects of the national information infrastructure or provide their cyber defense. It was argument that the main purpose of the system of the cybersecurity providing is to contribute the achievement of the objectives of the cyber security, and therefore the ensuring of the balanced existence of the interests of the individual, society and the state through the inspection, diagnosis, identification, prevention and termination, minimization and neutralization of the internal and external threats and dangers can be defined as the main function of this system.

Key words: cyber security, cyber threat, cyberspace, cyber-attack, cybersecurity providing, system of the cybersecurity providing.