УДК 342.9

Володимир Ліпкан,
докт. юрид. наук, доцент,
голова
Інституту стратегічних комунікацій
Глобальної організації союзницького лідерства

Ігор Діордіца,
канд. юрид. наук, доцент
голова
Інституту адміністративного правосуддя
Глобальної організації союзницького лідерства

НАЦІОНАЛЬНА СИСТЕМА КІБЕРБЕЗПЕКИ ЯК СКЛАДОВА ЧАСТИНА СИСТЕМИ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

Автором було проведено дослідження національної системи кібербезпеки як складової частини системи забезпечення національної безпеки України. У дещо спрощеному вигляді під національною системою кібербезпеки пропонується розуміти сукупність суб'єктів забезпечення кібернетичної безпеки, властивих конкретній нації чи державі, які взаємодіють із метою створення сприятливих умов для реалізації інтересів індивіда, суспільства і країни загалом. Аргументовано, що очевидною є необхідність створення Національної системи кібербезпеки, коли нею будуть займатися відповідні підрозділи СБУ, ДССЗЗІ та МВС. Координацію та ефективну взаємодію буде забезпечувати відповідний підрозділ РНБО. Зазначено, що кібербезпека стала пріоритетним питанням нормативно-правової бази органів інформаційно-комп'ютерного захисту, але на сьогодні не існує уніфікованої моделі побудови національної системи кібербезпеки. Акцентовано увагу на тому, що одним із ключових питань організації ефективної роботи національних систем кібербезпеки залишається налагодження взаємодії між компетентними державними органами, які є суб'єктами кібернетичної безпеки, та здійснення координації з такої діяльності.

Ключові слова: кібербезпека, система кібербезпеки, національна система кібербезпеки, національна безпека, забезпечення національної безпеки, система забезпечення національної безпеки.

Постановка проблеми. Останнім часом проблема забезпечення національної безпеки зміщується у бік не стільки декларованої, скільки реально розглядуваної. Передусім, це обумовлено активізацією зовнішніх загроз безпечного розвитку України: посиленням мілітаризації держав у регіоні, використанням положення енергетичної та торговельно-економічної залежності нашої країни, посиленням економічного та інформаційного тиску на неї тощо. Разом із тим, зовнішні загрози посилюються наявністю внутрішніх викликів національній безпеці, зокрема, йдеться про розбалансованість та незавершеність системних реформ, зниження обороноздатності держави, боєздатності Збройних Сил України, незадовільний стан фінансування, складне економічне становище.

Варто констатувати, що сучасний стан системи національної безпеки не забезпечує у повному обсязі нейтралізацію наявних загроз і викликів. Національна безпека забезпечується проведенням єдиної державної політики у всіх сферах життєдіяльності, системою заходів економічного, політичного та організаційного характеру, адекватним загрозам і небезпекам життєво важливих інтересів особи, суспільства і держави. Враховуючи той факт, що система національної безпеки є багатокомпонентною, звичайно постає потреба в існуванні спеціальної підсистеми, мета функціонування якої полягала б у забезпеченні функціонування та розвитку цієї системи, тобто у забезпеченні життєздатності її системоутворюючих елементів, зокрема національних інтересів людини, суспільства, держави. Такою системою і є система забезпечення національної безпеки [1, с. 57], а також національна система кібербезпеки. Ці та інші фактори і підтверджують актуальність даної статті.

Метою статті є дослідження національної системи кібербезпеки як складової частини системи забезпечення національної безпеки України, для досягнення якої буж поставлені наступні завдання: дослідити зміст даного поняття, проаналізувати наявні дефініції, окреслити актуальні проблеми та можливі шляхи їх вирішення.

Виклад основного матеріалу. У процесі розвитку високих технологій виникло принципово нове середовище – кіберпростір, що формується із соціальної, технічної, телекомунікаційної, інформаційної, мережевокомп'ютерної складової частини. Кіберпростір одночасно виступає як суб'єкт та об'єкт впливу. Сучасна успішна геополітика неможлива без стійкого домінування у кіберпросторі. Кібероборотьба набула стратегічного

управлінського спрямування. Вона проводиться без міжнародних правових обмежень у просторі та часі і характеризується високою ефективністю щодо досягнення воєнно-політичної мети. Вирішальним чинником досягнення успіху у світовому протиборстві стає інформаційно-технічна дезорганізація систем державного і воєнного управління та інформаційно-психологічна деморалізація населення країн, насамперед, складу їх збройних сил. Кіберпростір став невід'ємною частиною інформаційного простору та п'ятою сферою ведення збройної боротьби. Сама збройна боротьба, завдяки інформаційному чиннику, набула високого ступеня керованості. Деякі країни, з метою захисту свого кіберпростору, почали просування проектів регулювання (правил поведінки) у кіберпросторі (або за визначенням деяких відповідних документів – «сфері міжнародної інформаційної безпеки»). У 2013 р. свої стратегії кібербезпеки прийняли Нідерланди, Іспанія, Туреччина, Угорщина, Польща, Індія і в 2016 р. –Україна [2].

Розпочинаючи дослідження, перш за все, визначимось із категорією «система забезпечення національної безпеки України». Найбільш вдалим тлумаченням, на мою думку, є дефініція, запропонована В.А. Ліпканом. Під *системою забезпечення національної безпеки* варто розуміти систему теоретико-методологічних, нормативно-правових, інформаційно-аналітичних, організаційно-управлінських, розвідувальних, контррозвідувальних, оперативно-розшукових, кадрових, науково-технічних, ресурсних та інших заходів, спрямованих на забезпечення процесу управління загрозами за небезпеками, за якого державними і недержавними інституціями гарантується прогресивний розвиток українських національних інтересів, джерел духовного і внутрішнього добробуту народу України, ефективне функціонування самої системи забезпечення національної безпеки України [1, с. 60].

Також, розмірковуючи у резонанс із В.А. Ліпканом, фактично дублюючи змістовні описові ознаки поняття, автори підручника з політології твердять: *система забезпечення національної безпеки* визначена як організована державою сукупність суб'єктів: державних органів (законодавчої, виконавчої та судової гілок влади), громадських організацій, посадових осіб та окремих громадян, об'єднаних цілями та завданнями щодо захисту національних інтересів, що здійснюють узгоджену діяльність у межах законодавства України [3].

Діяльність із формування системи забезпечення національної безпеки України була невід'ємною складовою частиною і чинником державотворчих процесів незалежної України. Вже в Декларації про державний суверенітет України (16 липня 1990 р.) питання безпеки розглядалися в розділах «Зовнішня і внутрішня безпека», «Міжнародні відносини», «Екологічна безпека». Питання внутрішньої та зовнішньої безпеки аналізуються крізь призму права України на власні збройні сили, власні внутрішні війська та органи державної безпеки. З проблемами безпеки пов'язаний намір України стати у майбутньому нейтральною державою, яка не бере участі у військових блоках і дотримується трьох неядерних принципів: не приймати, не виробляти і не набувати ядерної зброї. Україна задекларувала прагнення активно сприяти зміцненню загального миру і міжнародної безпеки, брати активну участь у роботі міжнародних організацій в обсязі, необхідному для ефективного забезпечення національних інтересів [3].

Система національної безпеки будь-якої країни базується на концептуальних нормативно-правових документах, у яких викладаються офіційні погляди на роль і місце держави у світі, її національні цінності, інтереси й цілі, способи й засоби запобігання зовнішнім і внутрішнім небезпекам і загрозам [1, с. 58]. Аналогічна позиція через 12 років дублюється іншими авторами [4, с. 3].

Забезпечення належного рівня кібернетичної безпеки є необхідною умовою розвитку інформаційного суспільства. В умовах глобалізації інформаційних процесів, їх інтеграції в різні сфери суспільного життя керівництво провідних держав світу приділяє посилену увагу створенню та удосконаленню ефективних систем захисту критичної інфраструктури від зовнішніх і внутрішніх загроз кібернетичного характеру. У багатьох провідних країнах світу вже сформовані загальнодержавні системи кібернетичної безпеки – як найбільш оптимальні організаційні структури, що здатні за короткий проміжок часу акумулювати сили та засоби різних державних органів і приватного сектору для протидії кіберзагрозам. В Україні також відбувається процес формування системи кібернетичної безпеки. Як складову частину такої системи варто розглядати єдину загальнодержавну систему протидії кіберзлочинності, пропозиції щодо створення якої ще у 2011 р. доручалося розробити Кабінету Міністрів України за участю Служби безпеки України [5].

Як *система кібернетичної безпеки (система кібербезпеки)* розглядається сукупність спеціальних суб'єктів забезпечення кібернетичної безпеки, засобів та методів, що ними використовуються, а також комплекс відповідних взаємопов'язаних правових, організаційних та технічних заходів, що ними здійснюються [6].

Система кібернетичної безпеки – сукупність узгоджених за завданнями елементів кібернетичної безпеки, які комплектуються та розгортаються за єдиним замислом і планом у кібернетичному просторі з метою забезпечення кібернетичної безпеки інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем. Розвиток національної системи кібербезпеки має супроводжуватись відповідними корективами у процесі реформування сфери національної безпеки, а функціонування вказаної системи є неможливим без тісної співпраці з приватним сектором [7].

Досліджуючи національну систему кібербезпеки як складової частини системи забезпечення національної безпеки України, наголошу на необхідності етимологічного тлумачення понятійно-категорійного ряду, який і є предметом дослідження.

Перш за все, це *«національний»* – стосується нації, національності, пов'язаний з їхньою суспільно-політичною діяльністю; властивий певній нації, національності; державний, який належить даній країні або стосується її народу [8].

Наступною категорією є *«система»* – порядок, зумовлений правильним, планомірним розташуванням і взаємним зв'язком частин чого-небудь; сукупність яких-небудь елементів, одиниць, частин, об'єднуваних за спільною ознакою, призначенням [8].

Щодо «кібербезпеки», зауважу відсутність уніфікованої законодавчої чи доктринальної дефініції. Використовуючи наявні напрацювання в даній сфері, зазначу таке визначення «кібербезпеки»: це стан захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кібернетичному просторі, в якому є можливим безперешкодне створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації, а у вузькому сенсі – стан індивіда, суспільства та держави, де відсутня будь-яка небезпека [7].

Як *система кібернетичної безпеки (система кібербезпеки)* розглядається сукупність спеціальних суб'єктів забезпечення кібернетичної безпеки, засобів та методів, що ними використовуються, а також комплекс відповідних взаємопов'язаних правових, організаційних та технічних заходів, що ними здійснюються.

Система кібернетичної безпеки – сукупність узгоджених за завданнями елементів кібернетичної безпеки, які комплектуються та розгортаються за єдиним замислом і планом у кібернетичному просторі для забезпечення кібернетичної безпеки інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем. Розвиток національної системи кібербезпеки має супроводжуватись відповідними коригивами у процесі реформування сфери національної безпеки, а функціонування вказаної системи є неможливим без тісної співпраці з приватним сектором [7].

Також окремо пропонується використовувати термін *«система кібернетичної безпеки Міністерства оборони України та Збройних сил України»* – сукупність узгоджених за завданнями елементів кібернетичної безпеки, які комплектуються та розгортаються за єдиним замислом і планом в кібернетичному просторі для забезпечення кібернетичної безпеки інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем [9].

Тобто у дещо спрощеному вигляді під *національною системою кібербезпеки* пропонується розуміти сукупність суб'єктів забезпечення кібернетичної безпеки, властивих конкретній нації чи державі, які взаємодіють з метою забезпечення відсутності безпеки для індивіда, суспільства і країни загалом.

Стрімкий розвиток інформаційних технологій поступово трансформує світ. Відкритий та вільний кіберпростір розширює свободу і можливості людей, збагачує суспільство, створює новий глобальний інтерактивний ринок ідей, досліджень та інновацій, стимулює відповідальну та ефективну роботу влади й активне залучення громадян до управління державою та вирішення питань місцевого значення, забезпечує публічність та прозорість влади, сприяє запобіганню корупції.

Водночас переваги сучасного цифрового світу та розвиток інформаційних технологій зумовили виникнення нових загроз національній та міжнародній безпеці. Крім інцидентів природного (ненавмисного) походження, зростає кількість та потужність кібератак, вмотивованих інтересами окремих держав, груп та осіб.

Поширюються випадки незаконного збирання, зберігання, використання, знищення, поширення, персональних даних, незаконних фінансових операцій, крадіжок та шахрайства у мережі Інтернет. Кіберзлочинність стає транснаціональною та здатна завдати значної шкоди інтересам особи, суспільства і держави.

Агресія Російської Федерації, що триває й досі, інші докорінні зміни у зовнішньому та внутрішньому безпековому середовищі України, зокрема отримання безвізу, що є знаковою подією для стратегічного розвитку України, вимагають невідкладного створення національної системи кібербезпеки як складової частини системи забезпечення національної безпеки України [10].

Кіберпростір характеризується відсутністю кордонів, динамікою і відносною анонімністю. Забезпечення безпеки в кіберпросторі має бути організовано на конституційному рівні.

Очевидною є необхідність створення Національної системи кібербезпеки, коли нею будуть займатися відповідні підрозділи СБУ, кіберзахистом – відповідні підрозділи ДССЗЗІ (Державної служби спеціального зв'язку та захисту інформації), а боротьбою з кіберзлочинністю – відповідні підрозділи МВС. Координацію та ефективну взаємодію буде забезпечувати відповідний підрозділ РНБО [11].

Національна система кібербезпеки створюється і розвивається відповідно до Конституції України та інших нормативно-правових актів, що регулюють суспільні відносини у сфері національної безпеки, зокрема: Закон України «Про основи національної безпеки України» [12], Концепція розвитку сектору безпеки і оборони України [13], Положення про Національний координаційний центр кібербезпеки [14], Стратегія національної безпеки України [15], Стратегія кібербезпеки України [10], Воєнна доктрина України, Доктрина інформаційної безпеки України [16] тощо.

Українська держава прагне до забезпечення кібербезпеки на національному рівні, відповідно до стандартів країн-членів ЄС (із метою пришвидшення подальшого вступу). Кібербезпека стала пріоритетним питанням нормативно-правової бази органів інформаційно-комп'ютерного захисту.

Останнім часом воєнно-політичне керівництво України здійснює комплекс заходів щодо підвищення ефективності та поліпшення координації діяльності своїх силових структур у сфері кібернетичної безпеки.

Війна в кіберпросторі спричиняє нові кіберзагрози. Кіберзагрози – це наявні та потенційно

можливі явища і чинники, що створюють небезпеку життєво важливим інтересам людини та громадянина, суспільства і держави, реалізація яких залежить від належного функціонування інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем [17].

Конкретні загрози в кібербезпековому просторі характеризуються асиметрією і мають розширений, динамічний і глобальний характер, що ускладнює їх виявлення та реалізацію заходів протидії. Глобальність кіберпростору збільшує його потенційні ризики.

Загрози інформаційній безпеці становлять ведення інформаційної війни проти України, відсутність цілісної комунікативної політики держави, недостатній рівень медіа-культури суспільства, загрози кібербезпеці і безпеці інформаційних ресурсів – уразливість об'єктів критичної інфраструктури, державних інформаційних ресурсів до кібератак; фізична і моральна застарілість системи охорони державної таємниці та інших видів інформації з обмеженим доступом [15].

Кіберзагрози матеріалізуються за рахунок використання людського фактору та вразливостей технічних засобів у сферах приватного та державного секторів, а також фінансового, транспортного, енергетичного та інших, які зумовлюють загальну сферу національних інтересів. І з метою протидії цим загрозам необхідним є створення та ефективне функціонування національної системи кібербезпеки як складової частини системи забезпечення національної безпеки України. Також акцентую на тому, що кібербезпека існує в системі національної безпеки.

Створення національної системи кібербезпеки передбачено Стратегією кібербезпеки для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави.

Погоджуюся з тим, що 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 в 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;

– впорядкуванням (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 при здійсненні заходів із забезпечення безпеки у кіберпросторі [7].

Національна система кібербезпеки має, насамперед, забезпечити взаємодію з питань кібербезпеки державних органів, органів місцевого самоврядування, військових формувань, правоохоронних органів, наукових установ, навчальних закладів, громадських об'єднань, а також підприємств, установ та організацій незалежно від форми власності, які провадять діяльність у сфері електронних комунікацій, захисту інформації та/або є власниками (розпорядниками) об'єктів критичної інформаційної інфраструктури. *Основу національної системи кібербезпеки* становитимуть Міністерство оборони України, Державна служба спеціального зв'язку та захисту інформації України, Служба безпеки України, Національна поліція України, Національний банк України, розвідувальні органи [10].

На різних рівнях було проведено багато форумів, семінарів та конференцій міжнародного і національного масштабу. Публікуються наукові праці, присвячені різноманітним аспектам кібербезпеки. Провідні держави світу активно займаються не тільки стратегіями кібербезпеки, а й інституційними системами. Прикладом є Канада, США, Франція та Німеччина [18].

Аналізуючи системи кібербезпеки провідних країн світу, доходимо висновку, що на сьогодні не існує уніфікованої моделі побудови національної системи кібербезпеки. Наприклад, відповідно до прийнятого 25 листопада 2002 р. комплексного нормативно-правового акта у сфері безпеки – закону ***США*** «Про внутрішню безпеку» (Homeland Security Act of 2002) – урядові структури, які займались забезпеченням комп'ютерної безпеки, перейшли під контроль цього новоствореного відомства. Вказаний закон також посилив відповідальність за комп'ютерні злочини (включаючи довічне ув'язнення), зобов'язав інтернет-провайдерів надавати інформацію про клієнтів за вимогою правоохоронних органів, розширив їх права щодо можливості перехоплення інформації (прослуховування телефонних переговорів і перлюстрацію електронних повідомлень) без дозволу суду, визначив основні напрями діяльності федеральних органів із підвищення ефективності захисту критичної інфраструктури США від кібератак, зокрема об'єктів стратегічного значення, що перебувають у приватній власності [19].

Стратегія кібербезпеки ***Канади*** визначає кібертероризм та ворожі дії в кіберпросторі з боку інших країн (кібершпигунство і кібервійну) основними загрозами кібернетичній безпеці держави, а ключовим органом, на який покладена координація та контроль за імплементацією вказаної Стратегії, реалізація державної політики та координація заходів у сфері кібербезпеки та протидії

кіберзагрозам, визначене Міністерство громадської безпеки Канади (Public Safety Canada).

Законом ***ФРН*** «Про посилення безпеки інформаційних систем» завдання попередження, реагування на інциденти, викликані кібернетичними загрозами, управління й координація сил та засобів із захисту критичної інформаційної інфраструктури, зокрема у взаємодії з приватним сектором, покладене на Федеральне відомство безпеки інформаційних систем (BSI) ФРН.

Головним державним органом ***Великої Британії,*** на який покладено завдання захисту критичної інфраструктури, мінімізації загроз сталому її функціонуванню, насамперед, від загроз тероризму, є Центр захисту національної інфраструктури (Centre for the Protection of National Infrastructure, CPNI). Крім того, у Великобританії наприкінці березня 2013 р. було створено Центр із протидії кібернетичним загрозам із метою попередження та нейтралізації кібернетичних атак на об'єкти критичної інфраструктури, а також швидкого реагування на скоєні правопорушення у цій сфері.

Стратегією кібернетичної безпеки ***Австрії*** національним координатором і центральним органом у сфері кібербезпеки визначено Центр боротьби з кіберзлочинністю Федерального міністерства внутрішніх справ Австрії (Cyber Crime Competence Center (C4) of the Federal Ministry of the Interior). Крім того, на нього покладено головні функції щодо здійснення правоохоронної діяльності у сфері кібербезпеки та боротьби з кіберзлочинністю.

Ключову роль у забезпеченні кібернетичної безпеки ***Польщі*** відіграє Агентство внутрішньої безпеки (АВБ) – польський контррозвідувальний орган. Так, у 2013 р. АВБ розробило Стратегію кібербезпеки Польщі та ініціювало створення Центру криптології при Міністерстві національної оборони Польщі, на який покладено завдання із захисту інформації, кібероборони та проведення наступальних кібероперацій (активний кіберзахист).

Ключова роль у забезпеченні кібербезпеки ***Румунії*** відводиться її спеціальному контррозвідувальному органу – Румунській службі інформації (РСІ) [19].

Аналіз нормативно-правових та організаційних основ системи кібербезпеки провідних країн світу свідчить про домінантну роль спецслужб у забезпеченні кібернетичної безпеки держави, що пов'язано із характером кібернетичних загроз сьогодення, протидія яким потребує інструментарію (повноважень, форм і методів), притаманного виключно спеціальним, а саме, контррозвідувальним органам держави. Враховуючи міжнародний досвід та з метою ефективного вирішення завдань із забезпечення кібернетичної безпеки держави, відомством, що здійснює координацію діяльності всіх суб'єктів забезпечення кібернетичної безпеки (Національної системи кібербезпеки), доцільно визначити Службу безпеки України, яка є спеціально уповноваженим органом державної влади у сфері контррозвідувальної діяльності, а також протидіє внутрішнім та зовнішнім загрозам, у тому числі в інформаційній (кібернетичній) сфері. Також, зважаючи на світову практику, було запропоновано створити Національний центр кібербезпеки, який повинен був підпорядковуватися СБ України [19].

Нині такою державною структурою є Національний координаційний центр кібербезпеки, який є робочим органом Ради національної безпеки і оборони України. Центр має забезпечити координацію діяльності суб'єктів національної безпеки і оборони України під час реалізації Стратегії кібербезпеки України, підвищити ефективність системи державного управління у формування та реалізації державної політики у сфері кібербезпеки.

Серед основних завдань Центру: аналіз стану кібербезпеки; результатів проведення огляду національної системи кібербезпеки; стану готовності суб'єктів забезпечення кібербезпеки до виконання завдань з питань протидії кіберзагрозам; стану виконання вимог законодавства щодо кіберзахисту державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, а також критичної інформаційної інфраструктури; даних про кіберінциденти стосовно державних інформаційних ресурсів в інформаційно-телекомунікаційних системах тощо. Національний координаційний центр кібербезпеки має стати системоутворюючим елементом всієї системи кібербезпеки та кіберзахисту України [20].

Окремо в національній системі кібербезпеки України акцентую увагу на Команді реагування на комп'ютерні надзвичайні події України (англ. Computer Emergency Response Team of Ukraine, CERT-UA) – спеціалізованому структурному підрозділі Державного центру захисту інформаційно-телекомунікаційних систем Державної служби спеціального зв'язку та захисту інформації України, який заснований у 2007 р. Метою діяльності CERT-UA є забезпечення захисту державних інформаційних ресурсів та інформаційних і телекомунікаційних систем від несанкціонованого доступу, неправомірного використання, а також порушень їх конфіденційності, цілісності та доступності. Діяльність CERT-UA передбачена Законом України «Про Державну службу спеціального зв'язку та захисту інформації» [21], Законом України «Про телекомунікації» [22] та підзаконними актами.

Підтримую думку про те, що одним із ключових питань організації ефективної роботи національних систем кібербезпеки залишається налагодження взаємодії між компетентними державними органами, які є суб'єктами кібернетичної безпеки, та здійснення координації з такої діяльності [19].

Україні необхідно створити ключові механізми державного управління інформаційною безпекою в умовах кіберзагроз у вигляді спеціалізованих центрів, інститутів та експериментувати з операціями щодо ведення інформаційної війни, фінансувати експертні дослідження у сфері інформаційних операцій і створювати структури для наукових досліджень і та дослідно-конструкторських розробок. На порядку денному стоїть завдання поетапно сформувати індустрію програмного забезпечення; пришвидшити роботи щодо створення української національної мережі

суперкомп'ютерних комплексів, об'єднаних високошвидкісними оптико-волоконними каналами передачі даних; сформувати чітку інформаційну політику з просування вітчизняних ІТ-компаній за кордоном; об'єднати інтереси освіти, науки та ІТ-бізнесу; визначити базові вищі навчальні заклади, на основі яких сформувати кластери, що дадуть змогу вирішувати питання кадрової підготовки фахівців ІТ-технологій. Узагальнюючи досвід передових країн світу, кіберзахисту України необхідно йти шляхом створення національної операційної системи та необхідних пакетів прикладних програм, зокрема й вітчизняного антивірусу, створення (відновлення) вітчизняних потужностей з виробництва матеріально-технічної телекомунікаційної бази. Матеріально-технічну базу інформаційно-аналітичних систем, автоматизованих робочих місць доречно формувати виключно через вітчизняних постачальників. Забезпечення кібернетичної безпеки та ефективне державне управління нею у провідних країнах світу реалізовується з позицій системного підходу шляхом упровадження комплексу нормативно-правових, організаційних, функціональних, фінансових, технічних, навчально-тренувальних заходів та дій і цю практику Україні доречно перейняти. Також необхідно підняти рівень особистої кібербезпеки, тобто відповідальності кожного громадянина перед своєю країною [17].

Одними з першочергових заходів на шляху побудови системи кібербезпеки є вдосконалення державного управління у цій сфері та створення нормативно-правової бази для забезпечення такої діяльності.

З метою забезпечення кібербезпеки має бути створено національну систему кібербезпеки як формат співробітництва державних органів, установ, організацій, приватного сектору економіки, наукових установ і організацій, професійних асоціацій та неурядових організацій у сфері кібербезпеки.

Основою національної системи кібербезпеки є державні органи, які, відповідно до покладених завдань, безпосередньо виконують функції із забезпечення безпеки кіберпростору України.

До участі у здійсненні заходів, пов'язаних з виявленням, запобіганням і нейтралізацією кіберзагроз, залучаються інші суб'єкти забезпечення кібербезпеки.

Координація діяльності всіх суб'єктів забезпечення кібербезпеки здійснюється Радою національної безпеки і оборони України через її координаційно-дорадчий (робочий) орган з питань кібербезпеки [23].

Висновки

Позитивним моментом є те, що деякі країни розпочали просування проектів стратегій кібербезпеки і Україна не є винятком. Система національної безпеки є багатокомпонентною, національна система кібербезпеки є її спеціальною підсистемою, мета функціонування якої полягає у забезпеченні функціонування та розвитку цієї системи. Забезпечення належного рівня кібернетичної безпеки є необхідною умовою розвитку інформаційного суспільства. У дещо спрощеному вигляді під національною системою кібербезпеки пропонується розуміти сукупність суб'єктів забезпечення кібернетичної безпеки, властивих конкретній нації чи державі, які взаємодіють з метою забезпечення відсутності безпеки для індивіда, суспільства і країни загалом.

Очевидною є необхідність створення Національної системи кібербезпеки, коли нею будуть займатися відповідні підрозділи СБУ, відповідні підрозділи ДСТСЗІ та МВС. Координацію та ефективну взаємодію буде забезпечувати відповідний підрозділ РНБО.

Кібербезпека стала пріоритетним питанням нормативно-правової бази органів інформаційно-комп'ютерного захисту, але на сьогодні не існує уніфікованої моделі побудови національної системи кібербезеки.

Окремо в національній системі кібербезпеки України акцентую на Команді реагування на комп'ютерні надзвичайні події України.

Одним із ключових питань організації ефективної роботи національних систем кібербезпеки залишається налагодження взаємодії між компетентними державними органами, які є суб'єктами кібернетичної безпеки, та здійснення координації з такої діяльності.

Список використаних джерел:

1. Ліпкан В.А. Поняття системи забезпечення національної безпеки України / В.А. Ліпкан // Право і Безпека. – 2003. – Т. 2. – № 4. – С. 57–60.

2. Коваль З.В. Динаміка світової управлінської реакції на кіберзагрози: уроки для України / З.В. Коваль // Демократичне врядування. – 2014. – Вип. 14 [Електронний ресурс]. – Режим доступу : http://nbuv.gov.ua/UJRN/DeVr_2014_14_5.

3. 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.

4. Ткаченко В.І. Шляхи формування системи забезпечення національної безпеки / В.І. Ткаченко, Є.Б. Смірнов, О.О. Астахов // Збірник наукових праць Харківського національного університету Повітряних Сил. – 2015. – № 2. – С. 3–8.

5. 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.

6. Шеломенцев В.П. Сутність організаційного забезпечення системи кібернетичної безпеки України та напрями його удосконалення / В.П. Шеломенцев // Боротьба з організованою злочинністю і корупцією (теорія і практика). Київ: Міжвідом. наук.-дослід. центр з проблеми боротьби з організ. Злочинністю. – 2012. – № 2 (28). – С. 299–309.

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

8. 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.

9. Куцаєв В.В., Живило Є.О., Срібний С.П., Черниш Ю.О. Розширення термінології сучасного кіберп-

ростору / Куцаєв В.В., Живило Є.О., Срібний С.П., Черниш Ю.О. [Електронний ресурс]. – Режим доступу: mino.esrae.ru/pdf/2014/3Sm/1387.doc.

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

11. В Україні буде створена Національна система кібербезпеки, 27 січня 2016 [Електронний ресурс]. – Режим доступу : http://zaxid.net/news/showNews.do?v_ukrayini_bude_stvorena_natsionalna_sistema_kiberbezpeki&objectId=1380648.

12. Про основи національної безпеки України : Закон України від 19.06.2003 р. [Електронний ресурс]. – Режим доступу : http://zakon0.rada.gov.ua/laws/show/964-15.

13. Концепція розвитку сектору безпеки і оборони України від 14.03.2016 р. [Електронний ресурс]. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/92/2016.

14. Положення про Національний координаційний центр кібербезпеки від 07.06.2016 р. [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/242/2016.

15. Стратегія національної безпеки України від 26.05.2015 р. [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/555/2015.

16. Доктрина інформаційної безпеки України [Електронний ресурс]. – Режим доступу : http://www.president.gov.ua/documents/472017-21374.

17. Коваль З.В. Динаміка світової управлінської реакції на кіберзагрози: уроки для України / З.В. Коваль // Демократичне врядування. – 2014. – Вип. 14 [Електронний ресурс]. – Режим доступу : http://nbuv.gov.ua/UJRN/DeVr_2014_14_5.

18. Мінін Д.С. Підходи до визначення поняття «кібербезпека» / Д.С. Мінін [Електронний ресурс]. – Режим доступу : http://istfak.org.ua/tendentsii-rozvytku-suchasnoi-systemy-mizhnarodnykh-vidnosyn-ta-svitovoho-politychnoho-protsesu/185-heopolitychna-dumka-ta-heostratehichni-protsesy-v-khkhi-st/971-pidkhody-do-vyznachennya-ponyattya-kiberbezpeka.

19. Климчук О.О. Роль і місце спецслужб та правоохоронних органів провідних країн світу в національних системах кібербезпеки / О.О. Климчук, Н.А. Ткачук // Інформаційна безпека людини, суспільства, держави. — 2015. – № 3. – С. 75–83.

20. Турчинов заявив про нові кіберзагрози з боку Росії, 11 липня 2016 р. [Електронний ресурс]. – Режим доступу : https://www.ukrinform.ua/rubric-politycs/2048633-turcinov-zaaviv-pro-novi-kiberzagrozi-z-boku-rosii.html.

21. Про Державну службу спеціального зв'язку та захисту інформації : Закон України від 23.02.2006 р. [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/3475-15.

22. Про телекомунікації : Закон України від 18.11.2003 р. [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/1280-15/.

23. Проект Стратегії забезпечення кібернетичної безпеки України [Електронний ресурс]. – Режим доступу : www.niss.gov.ua/public/File/2013_nauk_an_rozrobku/kiberstrateg.pdf

Автором было проведено исследование национальной системы кибербезопасности как составляющей системы обеспечения национальной безопасности Украины. В несколько упрощенном виде под национальной системой кибербезопасности предлагается понимать совокупность субъектов обеспечения кибернетической безопасности, свойственных конкретной нации или государству, которые взаимодействуют с целью обеспечения отсутствия безопасности для индивида, общества и страны в целом. Аргументировано положение о том, что очевидна необходимость создания Национальной системы кибербезопасности, когда ей будут заниматься соответствующие подразделения СБУ, ГССЗИУ и МВД. Координацию и эффективное взаимодействие будет обеспечивать соответствующее подразделение СНБО. Отмечено, что кибербезопасность стала приоритетным вопросом нормативно-правовой базы органов информационно-компьютерной защиты, но на сегодняшний день не существует унифицированной модели построения национальной системы кибербезопасности. Акцентировано внимание на том, что одним из ключевых вопросов организации эффективной работы национальных систем кибербезопасности остается налаживание взаимодействия между компетентными государственными органами, субъектами кибернетической безопасности и осуществления координации с такой деятельностью.

Ключевые слова: кибербезопасность, система кибербезопасности, национальная система кибербезопасности, национальная безопасность, обеспечение национальной безопасности, система обеспечения национальной безопасности.

It was noted as the positive aspect that some countries have started promoting of the drafts on the cybersecurity strategies and Ukraine is no exception. The system of the national security is a multicomponent and national system of the cyber security is its special subsystem the operation objective of which is to ensure the functioning and development of the system. It was marked that ensuring of the proper level of the cyber security is a prerequisite for the development of the information society. It was offered to understand under the national system of the cyber security – a set of subjects which provide the cyber security which are inherent to a particular nation or state which interact with the aim to ensure the absence of security for the individual and society and a state as a whole. It was noted that the need of creation of the National Cybersecurity system is obvious. And relevant departments of the Security service of Ukraine, the relevant departments of the State Service for Special Communication and Information Protection of Ukraine and MIA should be involved in the activity. And coordination and effective interaction will provide the relevant unit of the CNSP. The attention was paid to the position that establishment of cooperation between the competent state authorities which are the subjects of the cyber security and coordination of such activities is one of the key issues of effective operation of national cyber security.

Key words: cybersecurity, cybersecurity system, national cybersecurity system, national security, ensuring of the national security, system of ensuring of the national security.