УДК 342.9

ПОНЯТТЯ ТА ЗМІСТ НАЦІОНАЛЬНОЇ СИСТЕМИ КІБЕРБЕЗПЕКИ

Ігор ДІОРДІЦА,
кандидат юридичних наук, доцент,
голова Інституту адміністративного правосуддя
Глобальної організації союзницького лідерства

SUMMARY

It was noted that there is no unique interpretation of cybersecurity among scientists and the uniform legislation definition also doesn't exist. It was defined that information is the main object of legal information relations which can take place in cyberspace. It was offered the author's understanding of the cybersecurity. "Cybersecurity" (in the narrow sense) – is a condition of the individual, society and state in which risk is absent. And in the broad sense "cybersecurity" – is the state of protection of vital interests of man and citizen, society and the state in cyberspace, where it is possible to create smooth gathering, receipt, possession, use, distribution, security and protection of information. Cyber security system – it is a set of bodies which are involved in the maintenance of the cyber security. It was marked that the building of an effective system of cyber security requires from the state bodies of Ukraine to define clearly the public policy in this area and anticipatory responses to dynamic changes occurring in the world in the area of the cyber security. The system of the cyber security of Ukraine consists of such basic elements: all national system of combating of the cybercrime and cyber terrorism; all national system of the cyber protection of the objects of the national critical infrastructure. The development of the national cyber security system must be accompanied by appropriate adjustments in the process of reforming of the defense and security sector, and operation of this system is impossible without close cooperation with the private sector

Key words: cyber security, cyber security system, national cyber security system, National Cyber Security Coordination Centre, information, cyber police.

АНОТАЦІЯ

У статті автор акцентував увагу на тому, що серед науковців відсутнє єдине тлумачення кібербезпеки, а також немає уніфікованої дефініції на законодавчому рівні. Запропонував авторське розуміння кібербезпеки у вузькому сенсі та широкому сенсі. Аргументував положення про те, 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. Розвиток національної системи кібербезпеки повинен супроводжуватися відповідними корективами в процесі реформування сектору безпеки та оборони, а функціонування вказаної системи є неможливим без тісної співпраці з приватним сектором.

Ключові слова: кібербезпека, система кібербезпеки, національна система кібербезпеки, Національний координаційний центр кібербезпеки, інформація, кіберполіція.

Постановка проблеми. 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 і 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 обумовили виникнення нових загроз національній та міжнародній безпеці. Поряд із інцидентами природного (ненавмисного) походження зростає кількість та потужність кібератак, мотивованих інтересами окремих держав, груп та осіб.

Поширюються випадки незаконного створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації, незаконних фінансових операцій, крадіжок та шахрайства у мережі Інтернет. Кіберзлочинність стає транснаціональною та здатна завдати значної шкоди інтересам особи, суспільства і держави в цілому.

Агресія Російської Федерації, що триває і наразі, інші докорінні зміни у зовнішньому та внутрішньому безпековому середовищі України вимагають невідкладного створення національної системи кібербезпеки як складової системи забезпечення національної безпеки України [1]. Ці та інші фактори і обумовлюють актуальність теми статті.

Основними завданнями, вирішенню яких присвячена стаття, є такі: охарактеризувати поняття кібербезпеки, дослідити існуючі доктринальні підходи щодо цієї дефініції, охарактеризувати національну систему кібербезпеки та визначити основні загрози для неї.

Виходячи з цього, **метою статті** є дослідження поняття та змісту національної системи кібербезпеки.

В роботі використано значну кількість праць науковців різних сфер. Окремо виділяємо праці таких авторів, як В.А. Ліпкан [2–6], Черноног О.О. [7], Баранов О.А. [8], Запорожець О.Ю. [9], Шеломенцев В.П. [10], Куцаєв В.В., Живило Є.О., Срібний С.П., Черниш Ю.О. [11], Петров В.В. [12]. Але відсутність єдиного підходу до визначення кібербезпеки та абсолютної недослідженості національної системи кібербезпеки і є підгрунтям проведення наукових досліджень.

Виклад основного матеріалу. На сьогодні провідні держави світу та суспільство в цілому все більше покладаються і, відповідно, залежать від безперешкодного функціонування п'ятого простору – кіберпростору, під яким пропонується розглядати сукупність взаємопов'язаних інформаційних ресурсів, програмного забезпечення, баз та банків даних, що обробляються в комп'ютерних мережах і пов'язаній з ними інфраструктурі, разом з об'єктами, що підпадають під їх контроль та управління. Захист інтересів держав та громадян в кіберпросторі стає життєво важливим завданням, яке перетворює безперешкодне використан-

ня ІТ-мереж на питання безпеки й оборони. Потенційна небезпека може загрожувати системам державного та військового управління, економіки та промисловості.

Україна інтегрована у світовий кіберпростір і тому зазнає різних загроз і негативних впливів, пов'язаних з його розвитком (наприклад, від наслідків суперництва США і ЄС з РФ та КНР), що гостро актуалізує проблеми кібербезпеки на загальнодержавному рівні. Це призводить до необхідності концептуального розуміння нової кібербезпекової реальності, впорядкування внутрішнього нормативно-правового поля, визначення повноважень відомств та організацій, задіяних у забезпеченні кібербезпеки держави і вирішення комплексу проблем, пов'язаних із розбудовою національної системи кібербезпеки. Найбільш ефективним шляхом вирішення зазначених питань є побудова національної моделі кібербезпеки та розробка першочергових напрямків діяльності державного та приватного секторів у сфері кібербезпеки [7].

В останні 30–40 років збільшується використання у найрізноманітніших сферах життєдіяльності суспільства комп'ютерних і телекомунікаційних технологій, у тому числі інтернет-технологій, що разом з великою кількістю переваг принесло також і чималу кількість загроз. Реалізація цих загроз може завдати значної шкоди як на мікро-, так і на макрорівні в рамках суверенних держав, а також і в світовому масштабі. Це призвело до розуміння необхідності вирішення проблеми нейтралізації або мінімізації цієї нової сукупності загроз. Одночасно з цим виникає термін «кібербезпека».

Вважають, що вперше термін виник у середині 1990-х років, коли уряд США став досліджувати цю тему. З того часу було проведено багато міжнародних і національних форумів, конференцій, семінарів на різних рівнях, опубліковано багато наукових робіт, присвячених найрізноманітнішим аспектам кібербезпеки. Велика кількість країн прийняли або розробляють стратегії кібербезпеки (США, Німеччина, Франція, Канада та багато інших) [8]. У цих умовах актуальною є проблема визначення змісту терміна «кібернетична безпека».

Деякі науковці вважають, що останнім часом термін "cybersecurity" все частіше і частіше використовується, але при цьому багато керівників служб безпеки і просто експерти з інформаційної безпеки досі плутаються в тому, коли і як використовувати цей термін [13], тому пропоную проаналізувати деякі з існуючих доктринальних та законодавчих дефініцій категорії, яка і становить науковий інтерес нашого дослідження.

Наголошую на тому, що серед науковців відсутнє єдине тлумачення кібербезпеки, а також на законодавчому рівні немає уніфікованої дефініції.

Кібербезпека – це деякий стан систем, за якого нейтралізуються загрози доступності, цілісності або конфіденційності даних, що циркулюють в інформаційних системах [8]. На мою думку, ця дефініція є незрозумілою, перш за все, через відсутність пояснення, про стан якої саме системи йдеться; звичайно, можна припускати, що системи, яка існує в кіберпросторі, але для науки потрібна конкретика.

Також під кібербезпекою пропонується розуміти окремий випадок інформаційної безпеки, поява якого обумовлена використанням комп'ютерних систем та/або телекомунікаційних мереж. У такому випадку сформульовано визначення: кібербезпека – інформаційна безпека в умовах використання комп'ютерних систем та/або телекомунікаційних мереж. Або ж розгорнуте визначення: кібербезпека – це такий стан захищеності життєво важливих інтересів особистості, суспільства і держави в умовах використання комп'ютерних систем та/або телекомунікаційних мереж, за якого мінімізується завдання їм шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки функціонування інформаційних технологій; несанкціоноване поширення, використання і порушення цілісності, конфіденційності та доступності інформації [8]. Тобто наскрізна категорія цієї дефініції – інформація, яка і є основним об'єктом інформаційних правовідносин, що можуть мати місце у кіберпросторі.

Варто наголосити на тому, що серед основних ознак інформації виокремлюють системність, селективність, субстанціональну несамостійність, наступництво, невичерпність, масовість, здатність трансформуватися, здатність до обмеження, універсальність, якість.

Пропонуються виключно юридичні особливості та властивості інформації, основними з яких є: фізична невідчужуваність; відособленість; властивість інформаційної речі; властивість тиражування (розповсюджуваність); властивість організаційної форми; властивість екземплярності.

Інформація може тиражуватися й поширюватися в необмеженій кількості екземплярів без зміни її змісту, і це також є її специфічною особливістю. Вона може бути відома багатьом, а якщо зберігається на матеріальному носії – то й належати одночасно необмеженій кількості осіб.

До основних характеристик інформації можна віднести й цільове призначення, обсяг, цінність, повноту, надійність, вірогідність, надмірність, швидкість передавання та обробки інформації [6, с. 44]. Таким чином, існування цих ознак та їх непорушність і будуть підвалинами кібербезпеки.

Під *кібербезпекою* розуміється деяка сукупність необхідних і відповідних заходів, у результаті реалізації яких досягається мінімізація ризиків [14]. На мою думку, таке тлумачення є досить звуженим та не розкриває основної сутності поняття. Аргументом щодо цього твердження є етимологічне тлумачення двох складових цієї правової категорії – «кібер» та «безпека». У «Великому тлумачному словнику української мови» «кібер» або «кібернетичний» – той, що стосується до кібернетики; який створено, працює на основі принципів, методів кібернетики [15, с. 308]. А «безпека» – стан, коли кому-, чому-небудь ніщо не загрожує [15, с. 106], тобто відсутність небезпеки. У запропонованому визначенні абсолютно відсутні ці дві категорії, хоча вони і є його понятійно-категорійним апаратом.

Кібербезпека – захист кіберсистем від шкідливого неправильного використання та від інших деструктивних атак [8]. Я не підтримую цього тлумачення, оскільки в ньому відсутні приклади або пояснення, що ж є неправильним використанням чи іншими деструктивними атаками. Припускаю, що ці дії повинні бути спрямованими, як було зазначено вище, проти інформації – об'єкта правовідносин.

Продовжуючи аналіз визначення, зауважу, що окремо виділяють дії, які порушують безпеку інформаційних мереж і систем:

– перехоплення електронної комунікації, копіювання або модифікація даних;

– неавторизований доступ до комп'ютера або комп'ютерних мереж;

– деструктивні атаки на мережі, зокрема атаки на доменні імена, перевантаження мережі штучними повідомленнями, атаки, спрямовані на порушення маршрутизації;

– шкідливе програмне забезпечення;

– підробка веб-сайтів;

– безпекові інциденти як наслідок непередбачених і ненавмисних подій, таких, як природні катаклізми, збої в роботі апаратних засобів та програмного забезпечення, людські помилки [9, с. 36].

Кібербезпека – захист інформаційних систем, що входять до складу кіберпростору, від нападів; забезпечення конфіденційності, цілісності та доступності інформації, яка обробляється в цьому просторі, виявлення та протидія атакам і кіберінцидентам [16]. На мою думку, доречним в цій дефініції було б уточнення, що саме є основними елементами інформаційних систем як складного явища. Структуру інформаційної системи складає сукупність окремих її частин – підсистем. Підсистема – це частина системи, яка виділена за певною ознакою. Тому структура будь-якої інформаційної системи може бути представлена як сукупність підсистем, що забезпечують інформаційне, технічне, математичне, програмне, організаційне і правове забезпечення [17, с. 60].

Кібернетична безпека – стан захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кібернетичному просторі. Визначення терміна кібернетичної безпеки базується на визначенні терміна *«кібернетичний простір»,* під яким розуміється середовище, яке виникає в результаті функціонування на основі єдиних принципів і за загальними правилами інформаційних (автоматизованих), телекомунікаційних та інформаційно-телекомунікаційних систем. Виходячи з наданого визначення, під середовищем можна розуміти сукупність інформаційних (автоматизованих), телекомунікаційних та інформаційно-телекомунікаційних систем.

Постає питання ідентифікації життєво важливих інтересів людини і громадянина, суспільства та держави в цьому середовищі. Питання явно риторичне тому, що в такому середовищі відсутні суспільні відносини між суб'єктами (людина, громадянин, суспільство, держава).

Таким чином, невдале визначення терміна «кібернетична безпека» логічно приводить до некоректного визначення предмета зазначеної стратегії, її цілей, а найголовніше – до неправильного визначення комплексу заходів щодо її впровадження [18].

З урахуванням того, що проблема кібербезпеки носить глобальний, а не лише локальний характер, досить цікавою видається позиція міжнародних організацій. Так, Міжнародний телекомунікаційний союз (International Telecommunication Union, ITU) у своїй Рекомендації дає таке визначення: *кібербезпека* – це набір засобів, стратегії, принципи забезпечення безпеки, гарантії безпеки, керівні принципи, підходи до управління ризиками, дії, професійна підготовка, практичний досвід, страхування та технології, які можуть бути використані для захисту кіберсередовища, ресурсів організації та користувача [19]. У цій дефініції з'являється ще одна категорія: «кіберсередовище», припускаю, що його можна ототожнювати з кіберпростором. Але наявність нових і почасти неузгоджених понять призводить до їх сплутування, неправильного тлумачення та застосування.

Пропоную узагальнене авторське розуміння кібербезпеки (у вузькому сенсі): стан індивіда, суспільства та держави, в якому відсутня будь-яка небезпека. А в широкому сенсі кібербезпека – 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, охорона, захист інформації.

Зазначу, що зміст будь-якого явища – це його сутність, внутрішня особливість [15, с. 168], отже, зміст національної системи кібербезпеки і становитимуть її певні ознаки та особливості.

Під *системою* розуміється сукупність будь-яких елементів, одиниць, частин, об'єднуваних за спільною ознакою, призначенням [15, с. 368]. Таким чином, *система кібербезпеки* – сукупність органів, які задіяні у забезпеченні кібербезпеки.

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 [10, с. 300].

Система кібернетичної безпеки – 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 [11].

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 обумовлюється 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.

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.

Підтримую думку по доцільність виокремлення в системі кібернетичної безпеки України таких основних елементів: загальнодержавна система протидії кіберзлочинності та кібертероризму; загальнодержавна система кібернетичного захисту об'єктів національної критичної інфраструктури.

При цьому під загальнодержавною системою протидії кіберзлочинності та кібертероризму розуміється сукупність спеціальних суб'єктів протидії кіберзлочинності та кібертероризму, засобів і методів, що ними використовуються, а також комплекс відповідних взаємопов'язаних правових, організаційних та технічних заходів, що ними здійснюються [10, с. 299].

Наприклад, у Європейському Союзі у зв'язку з розумінням важливості проблеми кібербезпеки в 2004 р. було створене Європейське агентство з мережевої та інформаційної безпеки (далі – ENISA), місією якого є допомога спільноті в забезпеченні особливо високого рівня мережевої та інформаційної безпеки; допомога державам-членам та бізнес-спільнотам у виконанні вимог мережевої та інформаційної безпеки [14].

Основними завданнями агентства є інформування громадськості про нові віруси, атаки хакерів і проблеми з безпекою інформаційного простору Європи, а також розслідування епідемій електронних вірусів і електронних атак. Особливо підкреслюється, що ENISA не збирається відігравати роль кіберполіцейських, оскільки для силових операцій є інші структури, а послужить консультативним органом, що надає посильну допомогу як у пійманні злочинців, так і в запобіганні злочинам. Агентство планує розробляти і розповсюджувати навчальні посібники, а також проводити навчання персоналу інформаційним ризикам і способам захисту даних. Планується і проведення науково-дослідницької роботи в галузі захисту інформації [14].

Щодо України, то слід зазначити, що переважна більшість експертів та практично всі національні стратегії щодо забезпечення кібербезпеки пов'язують проблематику кібербезпеки саме з використанням у процесі людської діяльності комп'ютерних систем і телекомунікаційних мереж (до останніх належить і мережа Інтернет) [18], а Національний координаційний центр кібербезпеки має стати системоутворюючим елементом всієї системи кібербезпеки та кіберзахисту України. До складу Центру увійшли представники ключових державних органів, які відповідають за весь спектр питань протидії широкому спектру кіберзагроз [22].

У розвинених країнах кібербезпека і стратегія кібероборони – важлива складова забезпечення миру. Найбільше досягли успіху в цій сфері США й Ізраїль, де є підрозділи кібервійськ.

Кіберпростір давно перетворився в п'ятий вимір ведення війни, крім суші, моря, повітря і космосу. Загальносвітовою є стійка тенденція зростання числа комп'ютерних атак на важливі об'єкти національних інфраструктур іноземних країн, що призводило й призводить до завдання шкоди державам через спотворення та витоки важливої для них інформації, блокування виробничих процесів на стратегічних об'єктах. Зазначене зумовило зміну зовнішньополітичних доктрин провідних ядерних країн світу, згідно з якими кібератаки прирівнюються до військових дій та передбачають можливість завдання воєнних ударів у відповідь.

Наприклад, за кілька днів до виборів президента України хакерські угрупування спробували вивести з ладу сайт ЦВК і систему «Вибори». За словами СБУ, велика частина кібератак була проведена з Росії [23]. Або ж хакерська атака на електромережу в Україні, яка була першою в історії кібератакою на об'єкти постачання, що призвела до перебоїв у подачі електроенергії, які відбулися на заході України 23 грудня 2015 р. [24]. Єдиний державний реєстр юридичних осіб, фізичних осіб – підприємців та громадських формувань в черговий раз піддався DDoS-атаці [25]. Також Всесвітнє антидопінгове агентство (WADA) і Спортивний арбітражний суд (CAS) піддалися хакерській атаці [26].

На сайт Bellingcat здійснювалися хакерські атаки з метою дискредитувати результати їхнього дослідження, більшість з яких підтвердила у своєму звіті міжнародна слідча група в Нідерландах [27]. У США ініціюють введення санкцій проти РФ через кібератаки [28].

Протистояння в кіберпросторі є небезпечною складовою гібридної війни, розв'язаної проти України, тому потрібно швидко, надійно та ефективно реагувати на будь-які кіберзагрози, що неможливо без інтегрування та чіткої взаємодії всіх наявних ресурсів суб'єктів кібербезпеки. Окрім відпрацювання ефективного реагування на кібератаки та кіберінциденти, необхідно вибудувати активний захист кіберпростору, створюючи належні умови для інституційного та технологічного забезпечення кібербезпеки [29]. Наприклад, у 2016 році поліція отримала близько 10 тис. заяв про кіберзлочини [30].

Очевидною є необхідність створення Національної системи кібербезпеки як одного з елементів забезпечення національної безпеки держави, коли нею будуть займатися відповідні підрозділи СБУ, кіберзахистом – відповідні підрозділи Державної служби спеціального зв'язку та захисту інформації (далі – ДСТСЗІ), а боротьбою з кіберзлочинністю – відповідні підрозділи МВС. Координацію та ефективну взаємодію буде забезпечувати відповідний підрозділ РНБО [31], тобто нагальною є потреба підготовки та прийняття відповідних нових нормативно-правових актів та внесення змін до вже існуючих.

Нині у ДСТСЗІ відсутні як повноваження, так і інструментарій та важелі впливу в цій сфері. Разом із тим позитивним є той факт, що в системі Держспецзв'язку функціонує спеціалізований підрозділ, про який уже згадувалося, – команда реагування на комп'ютерні інциденти (CERT-UA) [12, с. 128].

Розвиток національної системи кібербезпеки повинен супроводжуватись відповідними коригивами у процесі реформування сектору безпеки та оборони.

Зауважу, що Верховна Рада у першому читанні підтримала закон про основні засади забезпечення кібербезпеки України. Метою закону є створення національної системи кібербезпеки як сукупності політичних, соціальних, економічних та інформаційних відносин разом із організаційно-адміністративними та техніко-технологічними заходами шляхом комплексного підходу в тісній взаємодії державного і приватного секторів та громадянського суспільства [32].

Незрозумілим є те, що у Положенні про Національний координаційний центр кібербезпеки закріплені його завдання і, з-поміж інших, здійснення аналізу стану кібербезпеки та результатів проведення огляду національної системи кібербезпеки, стану забезпечення кадрами національної системи кібербезпеки та підготовка пропозицій щодо її удосконалення [33], а от нормативно-правовий акт, в якому б тлумачилися всі аспекти цієї системи, досі відсутній.

Національна система кібербезпеки насамперед як система взаємодії суб'єктів кібербезпеки має об'єднати спецслужби, правоохоронні органи, державні органи, що здійснюють регулювання у сфері інформатизації, телекомунікацій та захисту інформації, для своєчасного виявлення, попередження та припинення кіберзагроз, усунення передумов до їх настання та мінімізації негативних наслідків від їх реалізації.

Функціонування зазначеної системи неможливе без тісної співпраці з приватним сектором – операторами та провайдерами телекомунікації, власниками та розпорядниками критичних об'єктів інформаційної інфраструктури

держави, компаній, діяльність яких пов'язана зі сферою інформаційної безпеки [12, с. 128].

Для забезпечення кібербезпеки надзвичайно важливо розуміти загрози кіберпростору.

Кібернетичні загрози (кіберзагрози) – наявні та/або потенційно можливі явища і чинники, що створюють небезпеку життєво важливим інтересам людини і громадянина, суспільства і держави, реалізація яких залежить від належного функціонування інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем [11].

При цьому можна виділити таку типологію кібернетичних загроз: кібервійна, кібертероризм, кібершпигунство, кіберзлочинність [12, с. 130].

Як зазначено у Стратегії національної безпеки України, актуальними загрозами кібербезпеці і безпеці інформаційних ресурсів є: 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.

Пріоритетами забезпечення кібербезпеки і безпеки інформаційних ресурсів є: розвиток інформаційної інфраструктури держави; створення системи забезпечення кібербезпеки, розвиток мережі реагування на комп'ютерні надзвичайні події (CERT); моніторинг кіберпростору з метою своєчасного виявлення, запобігання кіберзагрозам і їх нейтралізації; розвиток спроможностей правоохоронних органів щодо розслідування кіберзлочинів; забезпечення захищеності об'єктів критичної інфраструктури, державних інформаційних ресурсів від кібератак, відмова від програмного забезпечення, зокрема антивірусного, розробленого у Російській Федерації; реформування системи охорони державної таємниці та іншої інформації з обмеженим доступом, захист державних інформаційних ресурсів, систем електронного врядування, технічного і криптографічного захисту інформації з урахуванням практики держав – членів НАТО та ЄС; створення системи підготовки кадрів у сфері кібербезпеки для потреб органів сектору безпеки і оборони; розвиток міжнародного співробітництва у сфері забезпечення кібербезпеки, інтенсифікація співпраці України та НАТО, зокрема, в межах Трастового фонду НАТО для посилення спроможностей України у сфері кібербезпеки [1].

Висновки. Таким чином, резюмуючи вищезазначені положення, зробимо деякі висновки. Негативним явищем є те, що серед науковців відсутнє єдине тлумачення «кібербезпеки», а також на законодавчому рівні немає уніфікованої дефініції. Наскрізною категорією цієї дефініції є інформація – основний об'єкт інформаційних правовідносин, що можуть мати місце у кіберпросторі. Кібербезпека (у вузькому сенсі) – стан індивіда, суспільства та держави, в якому відсутня будь-яка небезпека. А в широкому сенсі кібербезпека – 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, охорона, захист інформації. Система кібербезпеки – сукупність органів, які задіяні у забезпеченні кібербезпеки.

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. У системі кібернетичної безпеки України доцільним є виділення таких основних елементів: загальнодержавна система протидії кіберзлочинності та кібертероризму; загальнодержавна система кібернетичного захисту об'єктів національної критичної інфраструктури. Розвиток національної системи кібербезпеки повинен супроводжуватися відповідними коригувати у процесі реформування сектору безпеки та оборони, а функціонування вказаної системи є неможливим без тісної співпраці з приватним сектором.

Список використаної літератури:

1. Стратегія національної безпеки України від 15.03.2016 р. [Електронний ресурс]. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/96/2016.

2. Ліпкан В.А. Боротьба з тероризмом : [монографія] / В.А. Ліпкан, Д.Й. Никифорчук, М.М. Руденко. – К. : Знання, 2002. – 254 с.

3. Ліпкан В.А. Національна безпека України: нормативно-правові аспекти забезпечення : [монографія] / В.А. Ліпкан. – К. : Текст, 2003. – 180 с.

4. Ліпкан В.А. Правові засади розвитку інформаційного суспільства в Україні : [монографія] / В.А. Ліпкан, І.М. Сопілко, В.О. Кір'ян / за заг. ред. В.А. Ліпкана. – К. : ФОП О.С. Ліпкан, 2015. – 664 с.

5. Ліпкан В.А. Інформаційна безпека України : [глосарій] / В.А. Ліпкан, Л.С. Харченко,О.В. Логінов. – К. : Текст, 2004. – 136 с

6. Рудник Л.І. Право на доступ до інформації : дис... канд. юрид. наук : 12.00.07 / Національний університет біоресурсів і природокористування України / Л.І. Рудник. – К., 2015. – 247 с.

7. Черноног О.О. Напрями підвищення ефективності забезпечення кібербезпеки інформаційних технологій в системі публічного управління [Електронний ресурс]. – Режим доступу : mino.esrae.ru.

8. Баранов О.А. Про тлумачення та визначення поняття «кібербезпека» / О.А. Баранов [Електронний ресурс]. – Режим доступу : ippi.org.ua.

9. Запорожець О.Ю. Політика європейського союзу в сфері інформаційної безпеки / О.Ю. Запорожець // Актуальні проблеми міжнародних відносин : зб. наук. пр. / Київський нац. ун-т ім. Тараса Шевченка, Ін-т міжнар. відносин. – К., 2009. – Вип. 87, ч. 2. – С. 36–45.

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

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

12. Петров В.В Щодо формування національної системи кібербезпеки України / Петров В.В. // Стратегічні пріоритети. – К. : НІСД, 2013. – № 4(29). – С. 127–130.

13. Franscella J. Cybersecurity vs. Cyber Security: When, Why and How to Use the Term / J. Franscella [Електронний ресурс]. – Режим доступу : //www.infosecisland.com/blogview/23287-Cybersecurity-vs-Cyber-Security-When-Why-and-How-to-Use-the-Term.html.

14. Cyber Security Strategy for Germany [Електронний ресурс]. – Режим доступу : // https://www.enisa.europa.eu.

15. Великий тлумачний словник сучасної української мови / [укл. О.О. Єрошенко]. – Донецьк : ТОВ «Глорія Трейд», 2012. – 864 с.

16. National Cyber Security Strategy and 2013-2014 Action Plan. – Republic of Turkey. Ministry of Transport, Maritime Affairs and Communications, 2013. [Електронний ресурс]. – Режим доступу : //www.ccdcoe. org/strategies/TUR_CyberSecurity.pdf.

17. Буйницька О.П. Інформаційні технології та технічні засоби навчання [навч. посіб.] О.П. Буйницька. – К. : Центр учбової літератури, 2012. – 240 с.

18. Аналітична записка щодо законопроекту «Про основні засади забезпечення кібербезпеки України» [Електронний ресурс]. – Режим доступу : www.inau.org.ua/download.php?bd189ae6a731113f59c7d7fcacf193f3.

19. Рекомендация МСЭ-Т X.1205. Обзор кибербезопасности. – Женева : МСЭ, 2009. [Електронний ресурс]. – Режим доступу : //www.itu.int/ITU-T/recommendations/rec.aspx?rec=9136&lang=ru.

20. Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency (Text with EEA relevance) // Official Journal L 077, 13/03/2004 P. 0001–0011. – Режим доступу : //www.eur-lex.europa.eu/ LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML.

21. ENISA: нове європейське агентство мережевої безпеки [Електронний ресурс]. – Режим доступу : http://www.lenta-ua.com.ua/news/communications/4510.html.

22. Турчинов О.В. Національний координаційний центр кібербезпеки повинен мобілізувати весь наявний потенціал для забезпечення надійного кіберзахисту країни [Електронний ресурс]. – Режим доступу : http://www.rnbo.gov.ua/news/2528.html 11.07.2016.

23. На сайт ЦВК здійснюються DDoS-атаки [Електронний ресурс]. – Режим доступу : na_sayt_tsvk_zdiysnyuyutsya_ddosataki__derzhsluzhba_spetszvyazku_n501047.

24. Хакерская атака на электросеть в Украине была первой в истории кибератакой на объекты снабжения, – американские эксперты [Електронний ресурс]. – Режим доступу : http://censor.net.ua/news/368316/hakerskaya_ataka_na_elektroset_v_ukraine_byla_pervoyi_v_istorii_kiberatakoyi_na_obekty_snabjeniya_amerikanskie.

25. Минюст Украины заявляет о повторной хакерской атаке на Госреестр юрлиц и физлиц-предпринимателей [Електронний ресурс]. – Режим доступу : http://interfax.com.ua/news/general/374337.html.

26. WADA и CAS подверглись хакерской атаке [Електронний ресурс]. – Режим доступу : http://rian.com.ua/sport/20160812/1014601844.html.

27. На Bellingcat здійснювались хакерські атаки через розслідування катастрофи МН17 [Електронний ресурс]. – Режим доступу : http://www.unian.ua/politics/1545751-bellingcat-zaznav-hakerski-ataki-cherez-rozsliduvannya-katastrofi-mn17.html.

28. У США ініціюють введення санкцій проти РФ через кібератаки [Електронний ресурс]. – Режим доступу : http://ua.censor.net.ua/news/409590/u_ssha_initsiyuyut_vvedennya_sanktsiyi_proty_rf_cherez_kiberataky.

29. «Ми повинні швидко реагувати на всі кіберзагрози» – Турчинов [Електронний ресурс]. – Режим доступу : http://ua.censor.net.ua/n409349.

30. Департамент кіберполіції НПУ залучив до співпраці 40 хакерів [Електронний ресурс]. – Режим доступу : http://ua.censor.net.ua/n407633.

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

32. Рада зробила перший крок до створення національної системи кібербезпеки [Електронний ресурс]. – Режим доступу : http://espreso.tv/news/2016/09/20/rada_stvoryla_nacionalnu_systemu_kiberbezpeky.

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