УДК 340+35.078.3

ДОВГАНЬ О.Д., *доктор юридичних наук, професор.*
НДІ інформатики і права НАПрН України.
ТАРАСЮК А.В., *кандидат юридичних наук*. НДІ інформатики і права НАПрН України.

НАЦІОНАЛЬНІ ІНТЕРЕСИ УКРАЇНИ В КІБЕРНЕТИЧНІЙ СФЕРІ

Анотація. *У статті проаналізовано основні засади розвитку національних інтересів України в кібернетичній сфері, а також визначені пов'язані із цим актуальні проблеми забезпечення кібербезпеки.Обґрунтовано, що нормативно-правова база – головна передумова забезпечення кібербезпеки держави. За результатами дослідження визначені можливі шляхи вирішення відповідних проблем та підвищення ефективності забезпечення кібербезпеки.*

Ключові слова: *кібербезпека, інформаційна безпека, кіберпростір, кіберзагрози, національні інтереси.*

Summary. *The article analyzes the main principles of development of national interests of Ukraine in the cyber sphere, as well as identifies related current issues of cybersecurity. It is substantiated that the legal framework is the main prerequisite for ensuring cybersecurity of the state. According to the results of the study, possible ways to solve the relevant problems and increase the effectiveness of cybersecurity are identified.*

Keywords: *cybersecurity, information security, cyberspace, cyberthreats, national interests.*

Аннотация. *В статье проанализированы основные принципы развития национальных интересов Украины в кибернетической сфере, а также определены связанные с этим актуальные проблемы обеспечения кибербезопасности. Обосновано, что нормативно-правовая база – главная предпосылка обеспечения кибербезопасности государства. По результатам исследования определены возможные пути решения соответствующих проблем и повышения эффективности обеспечения кибербезопасности.*

Ключевые слова: *кибербезопасность, информационная безопасность, киберпространство, киберугрозы, национальные интересы.*

Постановка проблеми. У другому десятилітті XXI ст. завдяки небувалому прогресу техніки й інформаційно-телекомунікаційних технологій наші традиційні уявлення про відстані та часовий простір зазнали докорінних змін, внаслідок яких сформувався новий тип цивілізації – інформаційна. Сутність інформаційної цивілізації полягає у розвитку Інтернет-технологій і розширенні супутникового зв'язку, у практично необмежених в обсязі взаєминах і спілкуванні поза просторовими рамками, у розробці та миттєвому поширенні інформації і новин, а також появі та розвитку цифрової дипломатії.

У зазначених умовах глобальний кіберпростір перетворюється на майданчик зіткнення економічних, політичних і культурних інтересів та центрів сили сучасного світу, на дієвий інструмент формування громадської думки та її спрямування в інтересах певних гравців. Слід визнати, що поряд із позитивними і конструктивними тенденціями, які забезпечують поінформованість про новітні досягнення людства у ході розвитку світового кіберпростору, можна помітити і негативні процеси, що містять ризики для кібербезпеки держав, зокрема й України.

З огляду на зазначене, забезпечення кібербезпеки України має бути головною метою і в межах реалізації та відстоювання цієї мети слід прикладати значні зусилля для виконання таких завдань:

– забезпечення адекватного і реального сприйняття широкою міжнародною громадськістю суті зовнішньої та внутрішньої політики України;

– сприяння створенню ефективних засобів інформаційного впливу на закордонну громадську думку з метою позитивного сприйняття України;

– здійснення активної міжнародної співпраці в інформаційній сфері;

– розширення можливостей засобів масової інформації країни в міжнародному кіберпросторі;

– своєчасна й ефективна протидія кіберзлочинам і кіберзагрозам державній незалежності та національним інтересам України, духовно-етичним цінностям українського народу та історичним святиням.

Результати аналізу наукових публікацій. В основу написання даної статті покладено аналіз чинного інформаційного законодавства, законопроекти, які стосуються предмету дослідження, а також творчий доробок відомих вчених, зокрема О. Сегеда, С. Харченко, Т. Ткачук, А. Носач, А. Баровська, Н. Литвин та ін.

Метою статті є визначення концептуальних засад правового співвідношення інформаційної та кібернетичної безпеки на сучасному етапі з урахуванням сучасних загроз та перспектив розвитку.

Виклад основного матеріалу. Україна є прихильницею розробки комплексу міжнародних правових та етичних норм, націлених на забезпечення кібербезпеки, та їхнього всебічного дотримання у світовому кіберпросторі. Зважаючи на це, реалізація інформаційної дипломатії України спиратиметься на широке використання можливостей сучасних інформаційно-комунікаційних технологій [1, с. 141].

Аналіз актуальних загроз конфіденційній інформації, на основі якого формується система кібербезпеки і будується організація захисту інформації, розпочинається з усвідомлення та класифікації цих загроз. У зв’язку із цим підкреслимо, що теорія кібербезпеки оперує кількома формами класифікації інформаційних ризиків і загроз захисту інформації. Вважаємо за доцільне акцентувати увагу на поділі загроз кібербезпеці, що бувають зовнішніми і внутрішніми.

У разі зовнішніх атак супротивник відшукує слабкі місця в інформаційній структурі, що уможливлять доступ до ключових вузлів внутрішньої мережі, сховищ даних, локальних комп’ютерів співробітників. При цьому зловмисник використовує широкий набір інструментів і шкідливе програмне забезпечення для виведення з ладу систем захисту, шпигунства, фальсифікації або знищення даних, копіювання, завдання шкоди об’єктам власності тощо. З огляду на це не дивно, що у доповіді Всесвітнього економічного форуму “Глобальні ризики 2012” (“Global Risks 2012”) [2] кібератаки визначені як одна з основних загроз світовій економіці. За ймовірністю настання кібератаки входять до п’ятірки найбільших потенційних глобальних загроз. Зазначений висновок Всесвітнього економічного форуму доводить значну актуальність і велику небезпеку електронної злочинності. Спектр загроз кібербезпеці, викликаних застосуванням шкідливого програмного забезпечення, дуже широкий. Нині, наприклад, фахівці виокремлюють такі види загроз захисту інформації [3 – 5]:

– упровадження вірусів та застосування інших руйнівних програмних впливів;

– упровадження програм-шпигунів з метою аналізу мережевого трафіку й отримання даних про систему та стан мережевих з’єднань;

– аналіз і модифікація/знищення встановленого програмного забезпечення;

– розкриття, розкрадання та перехоплення секретних паролів і кодів;

– використання вразливостей ПЗ для виведення з ладу програмного захисту з метою отримання несанкціонованих прав читання, копіювання, модифікації або знищення інформаційних ресурсів, а також порушення їхньої доступності;

– блокування роботи користувачів системи програмними засобами тощо.

Варто відзначити, що нами наведено базовий склад загроз кібербезпеці держави, у зв'язку з тим, що вичерпний перелік таких загроз зробити не можливо. Адже вони, значною мірою, залежать від динаміки розвитку суспільно-політичної та міжнародної обстановки. З огляду на це стали реальними загрози: а) створенню і розвитку національної індустрії інформації, зокрема й індустрії засобів інформатизації, зв'язку та телекомунікації, задоволенню потреб внутрішнього ринку в її продукції, а також забезпеченню накопичення, ефективного використання та збереження вітчизняних і зарубіжних інформаційних ресурсів; б) безпеці інформаційних і телекомунікаційних засобів та систем, як створюваних на території України, так і вже розгорнутих й упроваджуваних.

Згідно з теоретичними і практичними джерелами складовими кібербезпеки є:

– стан безпеки кіберпростору, за якого забезпечується його формування і розвиток в інтересах держави, організацій та громадян;

– стан безпеки інформаційної інфраструктури, за якого інформація використовується суворо за призначенням і при цьому не здійснює негативного впливу на об'єкт;

– стан безпеки самої інформації, за якого унеможливлюється або суттєво ускладнюється погіршення таких її характеристик, як конфіденційність, доступність, цілісність.

Нині ні в кого не викликає заперечень, що нормативно-правова база – *головна передумова забезпечення кібербезпеки держави*. А важливою складовою нормативно-правової бази забезпечення кібербезпеки є також сукупність правових норм, що регламентують відносини у сфері функціонування органів держави, які входять до складу системи забезпечення кібербезпеки України. Варто підкреслити, що останнім часом дедалі вагомішого значення набуває взаємодія державних органів із громадськими організаціями та громадянами. У цьому контексті розвиток державно-приватного партнерства має стати одним із пріоритетних завдань державної політики у забезпеченні кібербезпеки.

Інша проблема, яка потребує теоретичного осмислення та практичного вирішення це рівень інформаційно-просвітницької, ідеологічної й освітньої роботи із протидії радикальній ідеології та екстремізму. Така робота потребує значного посилення. Серед найбільших проблем можемо виокремити, зокрема такі:

– брак фахівців у галузі інформаційної протидії екстремізму і тероризму;

– недостатня кількість інформаційної та довідкової літератури стосовно екстремістських і терористичних організацій;

– спостерігається відсутність пропаганди та наочної агітації;

– слабка роль засобів масової інформації у запобіганні та профілактиці екстремізму, а також у висвітленні антитерористичної й антиекстремістської діяльності державних органів.

У розрізі зазначеного ми підтримуємо думку авторів статті "Превентивна протидія екстремістським проявам в Україні: правові та організаційні аспекти", що запобігти екстремізму можна лише спільними зусиллями державних органів та громадськості, спрямованими на підвищення правової і загальної культури населення,

поліпшення соціально-економічних умов життя людей, формування позитивного іміджу держави [6, с. 43].

Зважаючи на це, необхідно вживати дієвих заходів із формування потужного ідеологічного корпусу, зміцнення його потенціалу в запобіганні радикалізації й екстремізму, із підготовки фахівців у напрямі інформаційної протидії тероризму й екстремізму, підвищення профілактичної ролі засобів масової інформації та інституційного забезпечення аналітичної, пропагандистської й інформаційної роботи в цій площині. Отже, питання забезпечення кібербезпеки, проблеми зовнішньої та внутрішньої загрози і протидії інформації, де пропагують релігійно-екстремістські і терористичні ідеї та явища в Україні, є одними з найактуальніших завдань суспільства й уряду на найближчу перспективу. Слід наголосити, що в нинішніх умовах радикальна ідеологія активніша, ніж будь-коли, і створює серйозну загрозу конституційному ладу держави. Дотепер в Україні таємно ведуть пропагандистську підривну діяльність рухи й організації релігійно-екстремістського напряму, що містять основну загрозу миру та стабільності держави.

До найнебезпечніших загроз безпеці в сучасній Україні в зазначеній сфері також належать:

– наявність зовнішніх і внутрішніх центрів політичної, релігійної, міжнаціональної та іншої напруженості у прикордонних районах суміжних Україні країн;

– збільшення на державному кордоні та прикордонній території масштабів розвідувально-підривної діяльності іноземних спецслужб;

– здійснення бандформуваннями бойових дій і терористичних акцій у прикордонній смузі та прикордонних територіях, зокрема проти військ й органів Державної прикордонної служби України.

Отже, з огляду на зазначене вище варто підкреслити, що державним органам необхідно вдосконалювати нормативно-правові акти, які регулюють питання протидії використанню Інтернету в терористичних й екстремістських цілях, а також забезпечують національні інтереси суверенної України в інформаційній сфері.

Іншим важливим напрямом державної політики у сфері правового забезпечення кібербезпеки України на сучасному етапі включення України у глобальні інформаційні процеси є міжнародний чинник.

Не викликає жодних сумнівів той факт, що виникнення нових засобів інформації і комунікації та їхнє поширення у країнах сучасного світу є одним із найвагоміших чинників процесу глобалізації. Стрімке розширення інформаційної та комп’ютерної павутини зменшило відстань між людьми в різних регіонах нашої планети ще більше, ніж розвиток шляхів наземної, повітряної та водної комунікації. Щоб уявити всю глибину інформаційної трансформації, яка відбувається останнім часом, і зрозуміти динаміку, необхідно усвідомити: в умовах глобальної інформатизації зникає географія, стираються межі між зовнішньою та внутрішньою політикою, що неминуче деформує не лише “національну”, але й “соціальну” ідентичності. Глобальна інформатизація розкриває багатопланові можливості для соціального інтегрування та транснаціональної взаємодії людей. Інтернет створює інші реалії для вільних контактів між людьми, які мешкають у різних країнах і є членами недержавних об’єднань.

Завдяки застосуванню сучасних інформаційно-комунікаційних технологій уявлення суб’єктів у реальному часі інтернаціоналізуються рідше, а їхню оцінку й відповідь на різні міжнародні події можна почути одразу ж після події. Усе це сприяє веденню дискусій на міжнародному рівні, створенню асоціацій між новими учасниками політичної інтерактивності.

Щоб розв'язати проблему "цифрового розриву", міжнародне співтовариство здійснює важливі кроки. На саміті "Великої вісімки", що проходив у липні 2000 р. в Японії (Окінава), наприклад, було ухвалено "Хартію глобального інформаційного співтовариства" [7]. У документі вперше у світовий контекст було введено поняття "цифровий розрив" й одним з основоположних принципів визначено імператив доступності інформаційних технологій для громадян усіх держав світу. Відповідно до основних положень Хартії було засновано міжнародну експертну раду "Група з можливостей цифрових технологій" (Digital Opportunity Task Force, G8DOT Force), головним завданням якої є пошук шляхів подолання існуючої нерівності між різними державами у доступі до новин та інформації. Рада також розробила програму дій і представила її очільникам держав "вісімки" на саміті, що проходив улітку 2001 р. в Генуї. Результати саміту уможливили вироблення плану конкретних рекомендацій (т. зв. "генуезька ініціатива") стосовно зазначеного питання [8]. Слід додати, що нині ініціатива з координації дій програми перейшла до Міжнародної експертної ради з інформаційно-комунікаційних технологій ООН, яку згодом було перетворено в Робочу (цільову) групу ООН з інформаційно-комунікаційних технологій (ІКТ). Виконання завдання подолання інформаційної нерівності в загальному контексті боротьби з бідністю нині покладено на ООН. Крім того, ООН у межах надання допомоги у впровадженні інформаційних технологій країнам, що розвиваються, ухвалила рішення про створення спеціального фонду обсягом 500 млн. дол. Звісно, цього поки що явно недостатньо для врегулювання проблеми. З огляду на це можна зробити висновок, що нині розвиток і поширення інформаційно-комунікативних технологій у державах світу проходить дуже незбалансовано, щоб стати переконливою передумовою для соціальної інтеграції та рівності у масштабі всієї планети. Подолання цифрової нерівності сьогодні стало пріоритетом у багатьох міжнародних організаціях. Проблема особливо посилилась з поширенням на планеті коронавірусної інфекції COVID-19 [9].У цій ситуації ми спостерігаємо й іншу сторону проблеми: протягом останнього року спостерігалося безпрецедентне впровадження цифрових технологій в усі сфери життя. Працівники почали виконувати свою роботу он-лайн, освітні заклади усіх рівнів перейшли на дистанційну форму навчання, що значно підвищило рівень обізнаності щодо інформаційно-комунікаційних технологій як учителів, викладачів так і тих, хто отримує знання, лікарі та пацієнти звернулися до телемедицини, політичні лідери почали відвідували віртуальні саміти, та багато інших прикладів.

Весь цифровий світ акумулював свої можливості для пошуку дієвих засобів протидії подальшому поширенню хвороби. Цифрові інструменти, такі як програми та дані смартфонів, також використовуються для перевірки розповсюдження вірусу, тоді як технічні компанії, включаючи Alibaba та Tencent в Китаї та IBM, Google і Microsoft в США, почали застосовувати свої високопродуктивні комп'ютерні можливості, щоб допомогти дослідникам у пошуку ліків від цієї хвороби.

Отже, процес глобальної інформатизації, поряд із розмиванням традиційних основ національно-державної ідентичності, може сприяти актуалізації інших форм об'єднання людей. Наслідком нерівномірної та експансіоністської інформатизації може бути посилення релігійної та етнічної ідентичності людей і їхнє об'єднання за ідеологічними принципами. Це, зі свого боку, може створити передумови для появи так званих конфліктів "нового покоління".

Оскільки останнім часом інформація перетворилася на особливий ресурс будь-якої діяльності, отже вона, як і будь-який інший ресурс, потребує захисту в забезпеченні її безпеки, цілісності та збереження. Проведений аналіз доводить, що членство в

регіональних організаціях дозволяє Україні виконувати актуальні завдання у сферах політичної комунікації та кібербезпеки. Україна на цій основі має гостру потребу у спільних із розвиненими державами діях, що можуть гарантувати їй безпеку на регіональному та глобальному рівнях. З огляду на це вона здійснює політику "відкритих дверей" та активно співпрацює з міждержавними об'єднаннями, що не пред'являють попередніх вимог до рівня її військової могутності (ООН, НАТО, ОБСЄ та ін.) та соціально-економічного розвитку.

Проте, визначальним у міжнародному співробітництві нашої держави з іноземними партнерами є російський чинник. Даний чинник досить вдало визначив голова Парламентської асамблеї НАТО Паоло Алліу своєму виступі на урочистому засіданні Верховної Ради, присвяченому 20-ій річниці підписання Хартії про особливе партнерство між Україною та Організацією Північноатлантичного договору: *"Агресія Росії проти України в 2014 році відкрила нову главу в міжнародних відносинах. Україна і Східна Європа на сьогоднішній день є лінією фронту із захисту європейської безпеки і захисту того світового порядку, який склався після Другої світової війни"* [10].

Сьогодні беззаперечним пріоритетом державної політики у сфері забезпечення кібербезпеки є і має бути подальша інтеграція в НАТО. Серед останніх здобутків нашої держави на цьому шляху слід вважати надання у червні 2020 року Північноатлантичною радою статусу партнера з розширеними можливостями (Enhanced Opportunities Partner, EOP). EOP дозволяє країні-партнеру досягти т.зв. секторальної (оперативної) взаємосумісності з НАТО (на рівні системи логістики, зв'язку, управління військами, конкретних родів військ тощо). Крім того, EOP дає запрошеним до неї країнам-партнерам низку особливих можливостей взаємодії з НАТО [11]. До цього такий статус мали лише п'ять країн, зокрема Грузія, а також країни-члени ЄС Швеція та Фінляндія.

Варто зауважити, що на теперішньому етапі розвитку України стан її національної безпеки, насамперед, залежить від ефективності результатів процесу інформатизації та прогресу у впровадженні ІКТ у військовій сфері.

У сучасних умовах проникнення глобалізації в усі сторони суспільного життя забезпечення кібербезпеки вимагає від дослідників виконання завдання наукового осмислення та здійснення наукового аналізу проблем, що тісно пов'язані з гарантуванням кібербезпеки, як найважливішого компонента міжнародної та національної безпеки. Однак, на жаль, слід констатувати: нині майже всі підходи, що покликані забезпечити кібербезпеку України, орієнтовані на військово-політичні процеси. Безумовно, це пріоритетний напрям у забезпеченні національної безпеки. Та попри це, вони мають також акцентувати увагу на таких проблемах, як регіональна політична нестабільність, незаконний обіг наркотиків, злочинність, захист інформаційних прав людини тощо. Та й імідж держави залишається ще одним проблемним аспектом, що прямо залежить від її інформаційної політики. Нерідко нас сприймають як зручний полігон кіберзлочинності. Отже, глобалізація кіберпростору породила таке явище, як всеосяжний взаємообмін інформацією на загальносвітовому рівні.

В експертному середовищі останнім часом дедалі голосніше лунає така думка: щоб успішно втілювати в життя державну інформаційно-іміджеву політику, Україні слід створити інформаційну систему, яка б формувала та затверджувала позитивний образ нашої країни в російсько- та англомовному медіапросторах [12; 13]. У контексті зазначеного вище усе ж варто додати, що нині проблемі забезпечення кібернетичної безпеки приділяється достатня увага як на державному, так і на приватному рівнях. У зв'язку з проникненням технічних засобів обробки і передачі даних практично в усі сфери людської діяльності особливої актуальності набуває протидія кіберзагрозам.

Уже цілком очевидно, що інформаційна сфера є самостійною галуззю національної безпеки, де необхідно гарантувати охорону інформаційних ресурсів, механізми їхнього створення, застосування та поширення, комунікаційну інфраструктуру, реалізацію прав на інформацію держави, суспільства і громадян тощо.

На сучасному етапі перед Україною постало завдання здійснення переходу до якісно нового рівня управління шляхом забезпечення всіх учасників інформаційних правовідносин достовірною, своєчасною та повною інформацією. Це можливо виконати лише завдяки послідовному реформуванню інформаційного впровадження в системі органів державної влади й управління та правильній реалізації інформаційної політики. Інформаційна політика – це здатність і можливість суб'єктів політики впливати на свідомість та психіку людей, їхню діяльність і поведінку за допомогою інформації в інтересах держави та громадянського суспільства [14]. Нині вже ні в кого не викликає сумнівів той факт, що доступність і якість інформаційних ресурсів багато в чому визначають рівень розвитку країни, її статус у світовому співтоваристві і, безперечно, стануть базовим показником статусу в перші десятиліття XXI ст. Зважаючи на це, стратегічними напрямами національної політики забезпечення кібербезпеки мають бути:

– захист національних інформаційних інтересів, забезпечення кібербезпеки, захист від інформаційних експансій, кіберзагроз та інших недружніх акцій, їхнє усунення;

– створення, розвиток і забезпечення безпеки національних інформаційних ресурсів;

– входження у світове інформаційне співтовариство.

Продовжуючи аналіз, варто додати, що стан формування інформаційних ресурсів в Україні нині, на жаль, перебуває на низькому рівні. Однією з найважливіших умов розвитку єдиного кіберпростору України є всеохопна (домашня) комп'ютеризація, що дозволила б розширити кіберпростір і відкрити широкий доступ до інформаційних ресурсів, готуючи ґрунт для діалогу влади із населенням. Заслуговує на увагу те, що в Україні поступово формується ринок інформаційно-комунікаційних технологій, продуктів і послуг, зростає мережа абонентів відкритих світових мереж, збільшується кількість персональних комп'ютерів. Прискореними темпами здійснюється забезпечення населення мобільними засобами зв'язку, розширюються національна мережа зв'язку та супутникова мережа. Триває інформатизація органів державної влади, галузей економіки, банківської сфери, зв'язку, транспорту, освіти та культури тощо.

Іншим важливим аспектом внутрішнього чиннику забезпечення кібербезпеки є теоретичне осмислення та практична реалізація на рівні законодавчого забезпечення національних інтересів України в кіберсфері. Попри те, що поняття національного інтересу в різних дослідників інтерпретується неоднозначно, усе ж проглядається розуміння загальної концепції щодо нього. Концепція національного інтересу це також і концепція ідеологічна, ціннісна та суб'єктно-абстрактна. Його визначення (національного інтересу) залежить не тільки від усвідомлення та сприйняття реальної дійсності суб'єктом, що формує національний інтерес, а й від світоглядних аспектів, ціннісних орієнтирів, особистісних характеристик суб'єкта і рівня амбіційності впливу на нього з боку груп інтересів.

Висновки.

Вивчення й аналіз забезпечення кібербезпеки, насправді, охоплює різні вияви інформації та інформування, а також є необхідним для розвитку інформаційної сфери. Під джерелами загроз кібербезпеці розуміють, зокрема, загострення міжнародної конкуренції за володіння інформаційно-технічними ресурсами, прагнення потенційних супротивників до ущемлення інтересів України у світовому кіберпросторі, витіснення її

із зовнішнього та внутрішнього ринків тощо. Цілком очевидно, що в кібернетичній сфері національні інтереси і національна безпека України будуються на основі стратегічних і поточних завдань зовнішньої та внутрішньої політики держави щодо забезпечення кібербезпеки. Їх слід узгодити із цілями забезпечення кібербезпеки України.

У кібернетичній сфері можна виокремити чотири основні складові національних інтересів України:

– *Перша складова* національних інтересів України забезпечує дотримання конституційних прав і свобод людини та громадянина у сфері отримання інформації та користування нею, сприяння духовному оновленню держави, збереження та зміцнення моральних цінностей суспільства, традицій гуманізму і патріотизму, наукового і культурного потенціалу країни.

– *Другий компонент* національних інтересів України в кібернетичній сфері передбачає інформаційне забезпечення державної політики, що пов'язане з доведенням до міжнародної громадськості та народу України правдивої інформації про державну національну політику, офіційну позицію держави щодо соціально-значимих подій держави та міжнародного життя, із наданням громадянам доступу до відкритих національних інформаційних ресурсів.

– *Третя складова* національних інтересів України в кібернетичній сфері забезпечує застосування новітніх інформаційних технологій, створення вітчизняної індустрії інформації, зокрема й індустрії засобів інформатизації, телекомунікації та зв'язку, задоволення потреб внутрішнього ринку її продукцією, а також забезпечення накопичення, ефективного використання та збереження національних інформаційних ресурсів.

– *Четвертий компонент* національних інтересів України в кібернетичній сфері передбачає захист інформаційних ресурсів від несанкціонованого доступу, забезпечення безпеки телекомунікаційних й інформаційних систем, як створюваних, так і тих, що функціонують на території України. Іншими словами, четверта складова зазначає, що в разі несанкціонованого доступу до інформаційних систем, що містять персональні дані громадян, можуть бути порушені їхні конституційні права.

Отже, досліджуючи національні інтереси України в кібернетичній сфері, необхідно наголосити, що особливість національних інтересів полягає в тому, щоб створити в українського народу захисні механізми, які б унеможливлювали будь-які спроби зсередини і ззовні використовувати національне різноманіття в недружніх цілях національного розколу з далекосяжними намірами.

З огляду на все це національна політика в галузі забезпечення кібербезпеки має будуватися з урахуванням необхідності захисту життєво важливих інтересів людини, суспільства та держави, дотримання їх балансу, поступового розширення можливостей та неухильного дотримання основоположних прав та свобод. Представники державної влади зобов'язані надавати всебічну допомогу в захисті національних й актуальних для держави життєво важливих інтересів в кібернетичній сфері.

Зважаючи на це, та з метою вироблення концептуальних підходів до забезпечення кібербезпеки, підготовки проектів постанов і розпоряджень з питань кібербезпеки та захисту інформації, організації і проведення експертизи проектів галузевих нормативних документів з кібербезпеки, а також надання пропозицій щодо виконання вимог нормативних актів з кібербезпеки тощо, було б доцільно створити спеціальний аналітичний Центр з кібернетичної політики при РНБО України.

Використана література

1. Сегеда О.О. Цифрова дипломатія України як елемент нової публічної дипломатії. *ПОЛІТИКУС*. Вип 3. 2020. С. 139-147.

2. Global Risks 2012 Seventh Edition. Insight Report. URL: http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2012.pdf

3. Ткачук Т.Ю. Механізми протидії інформаційним загрозам зовнішніх джерел. *Вісник НТУ України "Київський політехнічний інститут". Політологія. Соціологія. Право*. 2017. № 1 – 2. С. 242-246.

4. Харченко С.О. Наукові підходи до класифікації загроз інформаційній безпеці. Серія: *Державне управління*. 2019 р. № 2 (66). С. 191-197.

5. Носач А.В. Загрози національній безпеці як обов'язкова ознака злочинності, що посягає на державний суверенітет і територіальну цілісність України. *Право і суспільство*. 2019. № 3. С. 50-56.

6. Стрельбицький М.П., Благодарний А.М. Превентивна протидія екстремістським проявам в Україні: правові та організаційні аспекти. *Information Security of the Person, Society and State*. 2019. № 1 (25). С. 37-45.

7. Окинавская хартия глобального информационного общества (Окинава, 22 июля 2000 года). URL: https://zakon.rada.gov.ua/laws/show/998_163#Text

8. Jeffrey A. Hart The Digital Opportunities Task Force: The G8's Effort to Bridge the Global Digital Divide. 26 p. URL: https://www.researchgate.net/publication/228852360_The_Digital_Opportun ities_Task_Force_The_G8's_Effort_to_Bridge_the_Global_Digital_Divide

9. Coronavirus underscores urgency to bridge digital divide. DW. URL: https://www.dw.com/en/coronavirus-underscores-urgency-to-bridge-digital-divide/a-53070723

10. Урочисте засідання, присвячене 20-ій річниці підписання Хартії про особливе партнерство між Україною та Організацією Північно-Атлантичного договору. – (Прес-служба Апарату Верховної Ради України). URL: https://www.rada.gov.ua/preview/anons_acred/146596.html

11. 12 червня 2020 року Україна отримала статус члена Програми розширених можливостей НАТО (NATO's Enhanced Opportunities Program – EOP). Урядовий портал: URL: https://www.kmu.gov.ua/news/ukrayina-otrimala-status-chlena-programi-rozshirenih-mozhlivostej-nato

12. Довгань О.Д., Ткачук Т.Ю. Правове забезпечення інформаційної безпеки держави як підгалузь інформаційного права: теоретичний дискурс. *Інформація і право.* № 2(25)/2018. С. 73-85.

13. Баровська А.В. Понятійно-категоріальний апарат інформаційної сфери: правовий аспект. – (Аналітична записка). Національний інститут стратегічних досліджень. URL: http://old2.niss.gov.ua/articles/532

14. Литвин Н.А. Наукові підходи щодо визначення поняття державної інформаційної політики в Україні. *Наука і правоохорона*. 2019. № 1(43). С. 253-261.

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~
~~~~~~~~~~~~~~