Інформаційна і національна безпека

УДК 340+35.078.3

ТАРАСЮК А.В., *кандидат юридичних наук,*
НДІ інформатики і права НАПрН України

СПІВВІДНОШЕННЯ ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Анотація. *У статті досліджується концептуальні засади співвідношення інформаційної та кібернетичної безпеки України. На основі теоретичного аналізу запропоновано авторські визначення базових категорій кібернетичної безпеки, а також визначено та проаналізовано стан законодавчого забезпечення та розроблено пріоритетні напрями його вдосконалення.*

Ключові слова: *інформаційна безпека України, забезпечення інформаційної безпеки, кібербезпека, загроза.*

Summary. *The article explores the conceptual principles of information and cyber security of Ukraine. On the basis of theoretical analysis, author's definitions of basic categories of cyber security have been proposed, as well as the state of legislative support has been determined and analyzed and priority directions for its improvement have been developed.*

Keywords: *information security of Ukraine, information security, cyber security, threat.*

Аннотация. *В статье исследуются концептуальные основы соотношения информационной и кибернетической безопасности Украины. На основе теоретического анализа предложены авторские определения базовых категорий кибернетической безопасности, а также определено и проанализировано состояние законодательного обеспечения и разработаны приоритетные направления его совершенствования.*

Ключевые слова: *информационная безопасность Украины, обеспечение информационной безопасности, кибербезопасность, угроза.*

Постановка проблеми. Цілком очевидно, що й сьогоднішні, й перспективні, адекватні соціальній дійсності наукові розвідки у сфері інформаційної безпеки без опори на класичну спадщину будуть досить сумнівними. Водночас, не менш очевидно, що творчість найвидатніших представників світової філософської думки, незважаючи на її беззаперечну цінність і неминущу актуальність, далеко не вичерпує усіх аспектів філософського осягнення проблеми кібербезпеки.

А прецінь, їх погляди є найбільш показовими як у своїй протилежності, так і в єдності, що може стати тим перспективним аспектом осмислення сутності кібербезпеки, навколо якого й будуватиметься майбутня система забезпечення інформаційної безпеки як на національному, так і на глобальному рівнях. Принаймні сучасні методологічні підходи до соціально-філософського аналізу феномена інформаційної безпеки мають увібрати в себе якомога більше позитивних елементів проаналізованої історичної спадщини. Ретроспективний аналіз даної проблеми потрібен для вибору перспективної методології дослідження питань кібербезпеки України.

Нині у глобальному медіапросторі, в публіцистичних і наукових працях, а також у політичних і державних документах багатьох країн широкого вжитку набули терміни “інформаційна війна”, “інформаційне протиборство”, “інформаційний вплив”, “інформаційна зброя” тощо. Інформаційно-комунікаційні технології (далі – ІКТ) відіграють ключову роль у світовій політиці, економіці та системах безпеки.

До інформаційних диверсій у кіберпросторі сьогодні вдаються як організовані групи, так і окремі особи. Дедалі важливішою складовою військового потенціалу держав стає інформаційна зброя (далі – ІЗ) як доповнення до власне військового арсеналу. При цьому за своїми наслідками інформаційні війни між державами можуть бути не менш руйнівними і жорстокими, ніж традиційні.

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 В. Білоуса, В. Брижка, О. Довганя, І. Дороніна, Є. Захарова, М. Присяжнюка, В. Рубана, Т. Ткачука, В. Фурашева та ін.

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

Виклад основного матеріалу. Сьогодення постає перед Україною з новими викликами та надскладними завданнями. Під час опору різноплановим проявам гібридної війни, розгорнутої Російською Федерацією, стало очевидним, що наразі наша держава стикнулася з життєвою необхідністю захисту фундаментальних національних цінностей – незалежності, територіальної цілісності й суверенітету держави, свободи, прав людини й верховенства права, добробуту, миру й безпеки, – а також у стислі терміни має забезпечити ефективне функціонування сектору безпеки й оборони в умовах обмежених ресурсів. Запорукою успішної протидії широкомасштабній зовнішній агресії та сталого розвитку інформаційного суспільства в Україні є сьогодні не лише нарощування технологічних можливостей здійснення інформаційного обміну, а й глибоке усвідомлення усіма суб'єктами інформаційних відносин необхідності здійснення усіх заходів захисту інформаційних ресурсів та забезпечення інформаційної безпеки держави [1, с. 45-46], що неможливо без чіткого усвідомлення сутності останньої. Цікавим є й той факт, що самі російські дослідники відзначають, що інформаційна безпека від другої половині XX сторіччя стає одним із найважливіших елементів національної безпеки.

Стаття 17 Конституції України визначає, що "захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу" [2], що свідчить про набуття категорією "інформаційна безпека" в нормативно-правовому аспекті конституційного статусу [3, с. 30].

Незважаючи на те, що напрямок наукових досліджень, предметом якого є питання інформаційної безпеки, почав формуватись у період інтенсивної інформатизації, саме це явище існує стільки ж, скільки існує людство, дістаючи прояву в усіх сферах життєдіяльності суспільства. В повсякденному житті під інформаційною безпекою розуміють зазвичай необхідність протидії витоку інформації з обмеженим доступом, а також поширенню недостовірної інформації, однак застосування системного підходу дозволяє побачити відмінність наукового розуміння цієї проблеми від побутового [4, с. 174].

Зауважимо, що система інформаційної безпеки, особливо на рівні її вихідних компонентів, може бути структурована за різними критеріями. Щодо кібернетичної безпеки, то Законом України "Про основні засади забезпечення кібербезпеки України" [5] вона визначена як "захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного

середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі". Виокремлення кібербезпеки зумовлене специфікою середовища, у якому функціонують інформаційні системи, здійснюється обіг інформації, реалізації законних інтересів суб'єктів інформаційних процесів. Тож "кібернетичний вимір" властивий усім складовим інформаційної безпеки. Варто зауважити, що кібербезпека нами розглядається як складова інформаційної безпеки Далі на Рис. представлено співвідношення інформаційної та кібернетичної безпеки.

Саме прийняття Закону України "Про основні засади забезпечення кібербезпеки України" означає для України закріплення на законодавчому рівні понятійного апарату з приставкою "кібер" і початок регулювання цифрової економіки в цілому.

Закон розширив і доповнив положення Стратегії кібербезпеки України, затвердженої указом президента у 2016 році. Метою стратегії було створення умов для безпечного функціонування кіберпростору, його використання в інтересах особистості, суспільства і держави. При цьому основний масив положень стратегії стосується сфери національної оборони і не зачіпає бізнес. Стратегія стала підтвердженням прийнятого Україною курсу на євроінтеграцію, початком якого було підписання і ратифікація Україною Конвенції про кібербезпеку. Держави-члени Ради Європи та деякі інші держави, які підписали конвенцію, взяли на себе зобов'язання ужити загальних та індивідуальних заходів для запобігання злочинам у цифровій сфері.

Основним досягненням Закону "Про основні засади забезпечення кібербезпеки України" є імплементація в правове поле визначень, що стосуються кібербезпеки, кібератак і кіберзахисту.

Не вдаючись в детальний аналіз вказаного Закону, відзначимо ряд принципово важливих, на нашу думку, дискусійних аспектів, які у перспективі слід буде доопрацьовувати та вдосконалювати:

- чи поширюється Закон на приватні мережі суб'єктів господарювання, адже такі мережі, все ж таки підключені до мережі Інтернет;

- неузгодженість та відсутність конкретизації повноважень суб'єктів національної системи кібербезпеки;

- декларативний зміст ряду положень, що потребує прийняття цілого ряду конкретизуючих підзаконних нормативно-правових актів.

Крім практичної площини та зважаючи на відсутність єдності науковців щодо місця кібербезпеки у системі інформаційної безпеки, запропонуємо авторське розуміння її основних складових, а також її співвідношення з інформаційною безпекою держави.

Кібернетичний, або *спеціальний програмно-математичний вплив* реалізується з використанням засобів знищення, перекручення або розкрадання інформаційних масивів. Після подолання систем захисту противника з його інформаційних масивів отримується інформація, володіння якою вважається необхідним; доступ до них для законних користувачів при цьому обмежується чи взагалі унеможливлюється. У рамках кібервпливу вдаються також до дезорганізації роботи технічних засобів, виведення з ладу телекомунікаційних мереж, комп'ютерних систем тощо [6, с. 132-133].

Кібервплив провадять у *кібернетичному просторі* (кіберпросторі), під яким розуміють сферу діяльності в інформаційному просторі, утворену сукупністю комунікаційних каналів мережі Інтернет та інших телекомунікаційних мереж, технологічної інфраструктури, що забезпечує їх функціонування, і будь-яких форм здійснюваної за їх допомогою людської активності (окремого індивіда, організації, держави тощо).

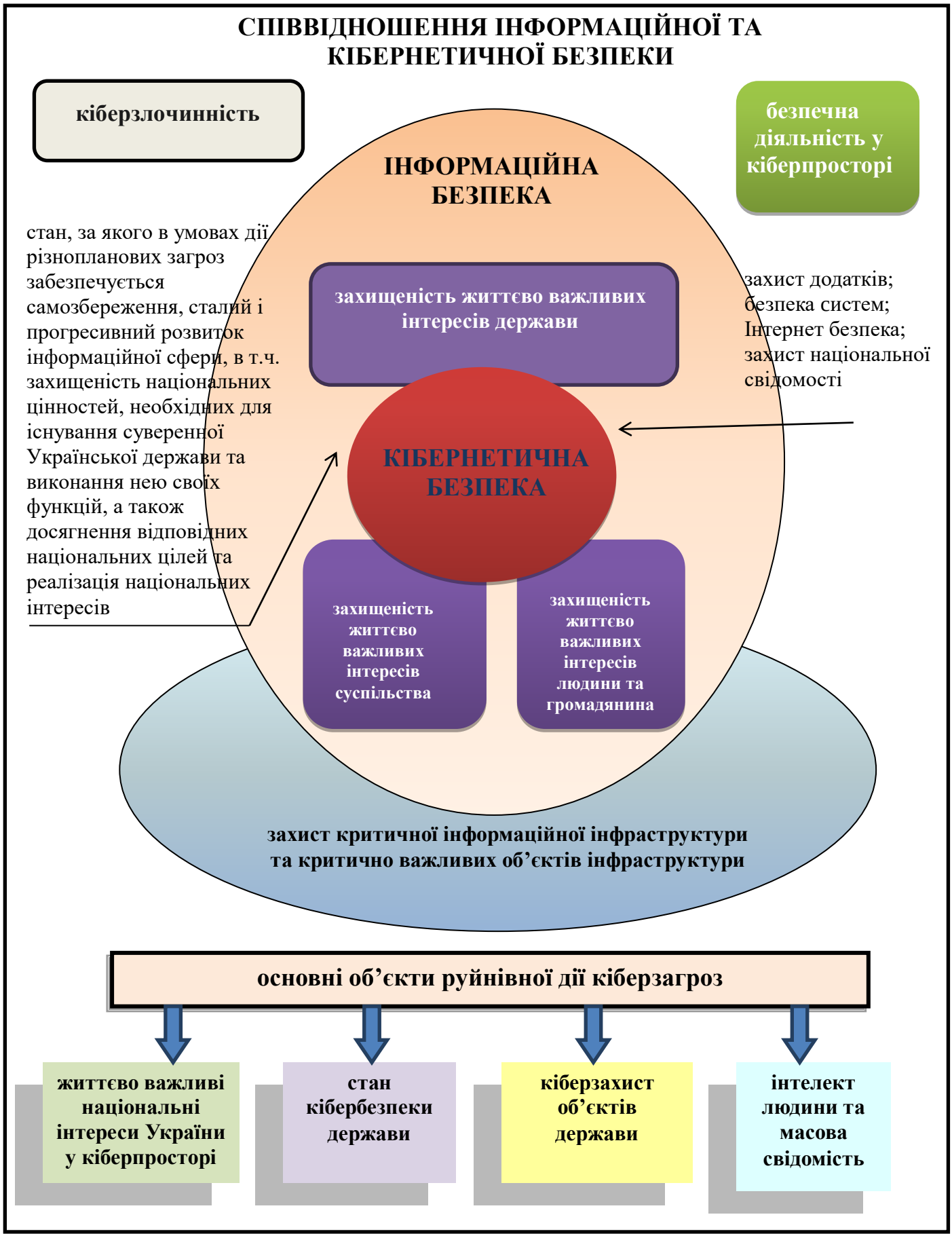
СПІВВІДНОШЕННЯ ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ
кіберзлочинність
безпечна діяльність у кіберпросторі
ІНФОРМАЦІЙНА БЕЗПЕКА
стан, за якого в умовах дії різнопланових загроз забезпечується самозбереження, сталий і прогресивний розвиток інформаційної сфери, в т.ч. захищеність національних цінностей, необхідних для існування суверенної Української держави та виконання нею своїх функцій, а також досягнення відповідних національних цілей та реалізація національних інтересів
захищеність життєво важливих інтересів держави
захист додатків; безпека систем; Інтернет безпека; захист національної свідомості
КІБЕРНЕТИЧНА БЕЗПЕКА
захищеність життєво важливих інтересів суспільства
захищеність життєво важливих інтересів людини та громадянина
захист критичної інформаційної інфраструктури та критично важливих об'єктів інфраструктури
основні об'єкти руйнівної дії кіберзагроз
життєво важливі національні інтереси України у кіберпросторі
стан кібербезпеки держави
кіберзахист об'єктів держави
інтелект людини та масова свідомість

Рис.

Кіберзагрози, або *інформаційно-технічні загрози*, хоча і є відносно новим видом інформаційних загроз, становлять суттєву небезпеку, серед іншого й через доволі швидкі темпи розвитку цього напряму. За сферами впливу кіберзагрози класифікують на дві групи. Перша з них пов'язана з атаками на бізнес і включає комерційне шпигунство, крадіжки баз даних, інформаційні дії з метою завдання шкоди репутаційному капіталу і т. ін. У разі подібних атак хакерам протистоять комп'ютерні фахівці корпорацій, кіберспецслужби. Якщо йдеться про кіберзагрози другої групи, то вони спрямовані на пристрої, що забезпечують життєдіяльність суспільства, контролюють пересування, роботу великої кількості служб і мають на меті злам комп'ютерних систем, крадіжку даних, нелегальне набуття можливості безкоштовно користуватися різними сервісами, видалення і зміну інформації про себе, свою (або замовника) активність і т. ін.

У Європейській Конвенції з кібернетичних злочинів наведено таке визначення цього поняття: *кіберзлочини – це правопорушення, спрямовані проти конфіденційності, цілісності та доступності комп'ютерних систем, мереж і даних, а також їх неправомірне використання* [7]. Віртуальний характер кіберзлочинів, а також засоби, за допомогою яких вони здійснюються, дозволяє зловмисникам швидко знищити сліди. Це значно ускладнює з'ясування обставин і пошук винуватців, тож постає нагальна потреба в розробленні нових методів розслідування кіберзлочинів і відповідних законодавчих норм, що регламентують сферу інформаційної безпеки.

Таким чином, на сучасному етапі бойові дії ведуться і в *інформаційному просторі* – принципово новому середовищі, де формується, перетворюється, передається, використовується, зберігається інформація, що впливає на індивідуальну і суспільну свідомість, інформаційну інфраструктуру і власне інформацію. Можна констатувати наявність не лише інформаційного простору як частини загального геостратегічного ландшафту, а й передумов для створення, розвитку й поширення інформаційної зброї. З огляду на це збройні конфлікти дедалі більше тяжіють до формату багатовимірних інформаційних війн і можуть одночасно вестися на різних рівнях. Термін "інформаційна війна" вперше був офіційно застосований у документах Міністерства оборони США. в директиві МО США DODD 3600 від 21 грудня 1992 року [8, с. 6-7].

В інформаційно-технічному протиборстві головними об'єктами нападу і захисту є системи управління та зв'язку, телекомунікаційні системи, радіоелектронні засоби, а також інформаційні ресурси держави – інформація на матеріальних носіях або наявна в будь-який інший формі. Саме в цій сфері сформувалося поняття ІЗ як *сукупності засобів розвідки, управління, зв'язку, навігації та радіоелектронної боротьби*. Загальновживаним термін "інформаційна зброя" став після завершення військової операції "Буря в пустелі" (Ірак, 1991), у ході якої комплексне застосування вищенаведеного переліку засобів на театрі військових дій зіграло вирішальну роль у досягненні стратегічної мети [6, с . 22-23].

Інформаційно-комунікаційні технології є одним з найбільш важливих факторів, що впливають на формування суспільства XXI століття, – зазначається в Окінавській Хартії глобального інформаційного суспільства. Їх революційний вплив стосується способу життя людей, їх освіти і роботи, а також взаємодії уряду та громадянського суспільства. Інформаційні технології швидко стають життєво важливим стимулом розвитку світової економіки [9]. Відповідно міжнародне законодавство останнім часом почало приділяти значну увагу кіберзагрозам та протидії їм.

Серед основних загроз національним кіберпросторам стратегії більшості країн визначають:

- *Кібершпигунство та військові дії, які здійснюються за підтримки або з відома*

держави. Усі технологічно розвинені держави та корпорації стають об'єктом кібершпигнуства, яке має на меті заволодіння державними або промисловими таємницями, персональними даними або іншою цінною інформацією [10]. Так, однією з найрезонансніших кібератак за останній час стали дії КНДР проти компанії "Sony Pictures Entertainment", внаслідок яких зловмисники заволоділи конфіденційними даними, в тому числі інформацією про комерційні операції компанії [11].

- *Використання Інтернету у терористичних цілях*. Терористичні угрупування використовують Інтернет з метою пропаганди, збору коштів і вербування прихильників [10].
- *Кіберзлочинність: викрадення персональних даних та відмивання коштів, отриманих незаконним шляхом*. Зловмисники продають інформацію про номери банківських карток, паролі від комп'ютерних серверів та шкідливе ПЗ.

Відповідно, національні законодавства країн, як правило, регулюють питання захисту:

- персональних даних (Канада, Нідерланди, Естонія, Швеція, Фінляндія, Іспанія);
- електронної комерції та безпеки електронних транзакцій та платіжних інструментів (США, Канада, Польща, Естонія, Італія);
- дітей (США);
- важливих об'єктів інфраструктури та інформаційних систем (Франція) [12, с. 244].

По-різному й трактують поняття "кібербезпека" в зарубіжних країнах:

– сукупність організаційних, правових, технічних та освітніх заходів, спрямованих на забезпечення безперервного функціонування кіберпростору (*Політика захисту кіберпростору Республіки Польща*).

– бажаний стан безпеки інформаційних технологій, за якого ризики для кіберпростору скорочені до прийнятного мінімуму (*Стратегія кібербезпеки Німеччини*).

– заходи з попередження шкоди від збоїв в роботі ІКТ та в її усуненні (*Національна стратегія кібербезпеки Королівства Нідерланди*).

– бажаний стан інформаційної системи, за якого вона може протидіяти викликам кіберпростору, які можуть негативно вплинути на достовірність, цілісність та конфіденційність даних, що зберігаються або обробляються даною системою (*Стратегія безпеки та оборони інформаційних систем Франції*) [13, с. 143].

Щодо вітчизняного правового регулювання окреслених питань, на законодавчому рівні системи інформаційної безпеки досі комплексно не вирішено. Навіть нова Доктрина інформаційної безпеки України [14], яка готувалася в умовах, коли наша країна потерпає від гібридної агресії Російської Федерації, а отже – вже треба було б усвідомлювати значення інформації, інформаційних впливів та інформаційної сфери в цілому, не орієнтує на вирішення усього комплексу виявлених проблем, не загострює проблеми необхідності їх законодавчого врегулювання.

Так, виходячи з необхідності вдосконалення нормативно-правового забезпечення та попередження й нейтралізації потенційних і реальних загроз національній безпеці в інформаційній сфері, з початком гібридної війни проти України виникла необхідність кардинальних змін у системі забезпечення інформаційної безпеки нашої держави. Основний план заходів було запроваджено рішенням РНБО від 28 квітня 2014 року "Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України", затвердженим Указом Президента України від 01.05.14 р. № 449/2014 [15]. Згідно з цим рішенням Кабінету Міністрів України було доручено розробити й подати на розгляд парламенту законопроекти про внесення змін у закони України щодо протидії інформаційній агресії іноземних держав, передбачивши, зокрема:

визначення механізму протидії негативному інформаційно-психологічному впливу, в тому числі шляхом заборони ретрансляції телевізійних каналів; запровадження для іноземних ЗМІ системи інформування та захисту журналістів, які працюють у місцях збройних конфліктів, вчинення терористичних актів, при ліквідації небезпечних злочинних груп. Крім того, приписувалося підготувати проект стратегії розвитку інформаційного простору України, розробити і впровадити комплексні заходи організаційного, інформаційного й роз'яснювального характеру щодо всебічного висвітлення заходів з реалізації державної політики у сфері забезпечення інформаційної безпеки, а також посилити контроль за дотриманням законодавства з питань інформаційно-психологічної та кібернетичної безпеки. Відповідно до вказаного плану заходів й було розроблено Доктрину інформаційної безпеки України [14].

Метою Доктрини є уточнення засад формування та реалізації державної інформаційної політики, насамперед щодо протидії руйнівному інформаційному впливу РФ в умовах розв'язаної нею гібридної війни. Її правовою основою є Конституція України, закони України, Стратегія національної безпеки України, затверджена Указом Президента від 26 травня 2015 року № 287, а також міжнародні договори, згода на обов'язковість яких надана Верховною Радою України.

У тексті Доктрини йдеться про національні інтереси України в інформаційній сфері, актуальні загрози національним інтересам та національній безпеці, пріоритети державної політики в інформаційній сфері й механізм її реалізації. Втілення положень цього документа покладено на Кабінет Міністрів, Міністерство інформаційної політики, Міністерство закордонних справ, Міністерство культури України, Державне агентство України з питань кіно, Національну раду України з питань телебачення і радіомовлення, Державний комітет телебачення і радіомовлення України, Службу безпеки України, розвідувальні органи, Державну службу спеціального зв'язку та захисту інформації, Національний інститут стратегічних досліджень, а також на Верховну Раду України, оскільки Доктриною передбачається внесення змін до чинного законодавства України.

Доктрина спрямована на захист українського суспільства від "агресивного інформаційного впливу Російської Федерації", розвиток публічної дипломатії, в тому числі культурної та цифрової, видалення шкідливої інформації з українського сегменту Інтернету та квотування національного аудіовізуального контенту, захист права на вільний доступ до інформації, створення механізмів захисту від пропаганди тощо.

Утім, в експертному середовищі Доктрина отримала переважно негативну оцінку, на кшталт: "Доктрина інформаційної безпеки України – це лише декларація" або "Замість інтеграції Україна встановлює паркан" тощо. Справді, у Доктрині держава виклала бачення розвитку й функціонування свого інформаційного простору і визначила, що Російська Федерація є противником, котрий веде системну інформаційну війну. У документі є пропозиції, як реагувати на агресію та забезпечувати інформацією громадян. Доктрина також визначає поняття "стратегічного наративу" і вказує, що медіа мають самі себе регулювати, але при цьому мають нести соціальну відповідальність. Доктрина закладає державну систему постійного моніторингу веб-ресурсів та блокування сайтів, що загрожують безпеці, однак виписані в документі підстави для блокування доволі абстрактні – орган державної влади на свій розсуд зможе тлумачити, що загрожує безпеці, а що ні. Відповідно, виникає небезпека встановлення цензурних шлюзів, які відокремлять український Інтернет від світу. Крім того, механізм реалізації Доктрини, навіть у її позитивних аспектах, не містить жодної конкретики, тож у чинній редакції вона не може слугувати базовим документом, на підставі якого мають формуватися й інші правові акти у сфері забезпечення інформаційної безпеки, в тому числі стратегічні та програмні.

Відтак, сьогодні вкотре слід порушувати питання щодо розробки нормативного акта (закону), яким визначатиметься єдиний поняттєво-категорійний апарат, державна політика забезпечення інформаційної безпеки, об'єкти інформаційної безпеки та суб'єкти її забезпечення, правові зони відповідальності відомств, залучених до сфери забезпечення інформаційної безпеки, механізми координування їх діяльності щодо реагування на виклики та загрози національній безпеці в інформаційній сфері, порядок правового закріплення взаємовідносин державних безпекових структур з іншими органами та відомствами, віднесеними законодавством до суб'єктів забезпечення національної безпеки України, тощо [16, с. 37-38]. Вважаємо, що такий нормативний акт неодмінно має дати чітке визначення як системи інформаційної безпеки, так і системи забезпечення інформаційної безпеки.

Усе це зайвий раз доводить нагальну потребу розробки та прийняття Закону України "Про інформаційну безпеку України" як базового нормативно-правового акта, що регулюватиме відповідні питання [17, с. 89]. Такий закон як фундамент для побудови ефективної стратегії інформаційної безпеки має містити не абстрактні декларації, а чітко визначені основоположні категорії у сфері інформаційної безпеки та підходи до формування системи її забезпечення, механізм її функціонування, повноваження і схему взаємодії суб'єктів забезпечення інформаційної безпеки тощо.

Дане зумовлюється і досить динамічним розвитком інформаційного суспільства. У цьому ракурсі ми поділяємо думку В. Брижка, що у наш час життєдіяльність світової цивілізації дедалі більше спрямовується інформаційною сферою, яка завдяки інформаційно-технологічним змінам, що почалися наприкінці XX століття, об'єктивно зумовили появу нового типа суспільства – інформаційного суспільства [19, с. 20]. Досить цікавою у ракурсі даного дослідження є думка В. Фурашева про те, що інформаційний простір – це форма співіснування сукупності матеріальних та нематеріальних об`єктів і процесів, спрямованих на задоволення інформаційних потреб всіх живих істот на Землі [20, с. 166].

Висновки.

Сьогодні Україна відстоює свій євроінтеграційний курс в умовах окупації Криму й частини Донецької та Луганської областей унаслідок неоголошеної війни, яка ведеться Російською Федерацією проти нашої держави з активним використанням методів інформаційного протиборства. У зв'язку зі значним негативним інформаційним впливом на інформаційний суверенітет нашої держави, питання правового забезпечення кібербезпеки України набувають особливої актуальності.

Можливо багато говорити про важливість і актуальність посилення регулювання на національному та міжнародному рівнях діяльності в кіберпросторі і зростання ролі в цьому і приватного сектора; встановлення контролю над кіберзброєю, а також посилення охорони критичної інфраструктури України; впровадження інновацій в сфері кібербезпеки та вдосконалення освітніх напрямів підготовки фахівців даної сфери діяльності тощо. Однак без набуття системного та комплексного характеру всі зазначені підходи не дозволять вивести рівень кібербезпеки, а звідси – і національної безпеки України загалом, на новий якісний рівень. Боротьба з кіберзлочинністю повинна носити системний характер, виходячи із сучасних ризиків та викликів у кіберпросторі, а інституційне середовище забезпечення кібербезпеки постійно вдосконалюватися. Ефективність заходів у цій сфері повинна досягатися завдяки здійсненню оцінки загроз організованої кіберзлочинності, що дозволить визначати сучасні загрози та ризики у кіберпросторі.

Використана література

1. Присяжнюк М.М. Інформаційна безпека України в сучасних умовах. *Вісник Київського національного університету імені Тараса Шевченка. Військово-спеціальні науки*. 2013. Вип. 30. С. 42-46.

2. Конституція України: Основний Закон України від 28.06.96 р. № 254к/96-ВР. URL: http://zakon3.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80 (дата звернення: 05.12.2019).

3. Цимбалюк В. Окремі питання щодо визначення категорії "інформаційна безпека" у нормативно-правовому аспекті. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. Науково-технічний збірник*. Київ, 2004. С. 30-33.

4. Рубан В.Я. Інформаційна безпека України: сутність та проблеми. Стратегічна панорама. 1998. № 3-4. С. 170-175.

5. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.17 р. URL: http://zakon3.rada.gov.ua/laws/show/2163-19 (дата звернення 05.12.2019).

6. Ткачук Т.Ю. Забезпечення інформаційної безпеки в умовах євроінтеграції України: правовий вимір: монографія. Київ: ТОВ "Видавничий дім "АртЕк", 2018. 422 с.

7. Европейская Конвенция по киберпреступлениям. URL: http://inter.criminology.onua.edu.ua/?p=2263 (дата звернення: 05.12.2019)

8. Брижко В.М. та ін. е-боротьба в інформаційних війнах та інформаційне право: монографія; за ред. члена-кореспондента АПрН України, д.е.н., професора М. Швеця. – (НДЦПІ АПрН України). Київ: Видавництво ТОВ "Пан-Тот", 2007 р. 234 с.

9. Окінавська хартія глобального інформаційного суспільства від 22.07.2000 р. URL: http://zakon4.rada.gov.ua/laws/show/998_163 (дата звернення 05.12.2019).

10. Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada URL: http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf (дата звернення 05.12.2019).

11. The Department Of Defense Cyber Strategy URL: http://www.defense.gov/home/features/2015/0415_cyberstrategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf (дата звернення 05.12.2019).

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

13. Ткачук Т.Ю. Кібербезпека: підходи до визначення в окремих країнах: мат. наук.-практ. конф. *Актуальні проблеми управління інформаційної безпекою держави,* м. Київ, 24.05.17 р. Київ: Нац. акад. СБУ, 2017. С. 142-144.

14. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року "Про Доктрину інформаційної безпеки України": Указ Президента України від 25.02.17 р. № 47/2017. URL: www.president.gov.ua/documents/472017-21374 (дата звернення 05.12.2019).

15. Про рішення Ради національної безпеки і оборони України від 28 квітня 2014 року "Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України": Указ Президента України від 01.05.14 р. № 449/2014. URL: www.president.gov.ua/documents/4492014-17157 (дата звернення 05.12.2019).

16. Довгань О.Д. Інформаційна безпека: стан, проблеми, тенденції. Інформаційні ресурси, інтелектуальна власність, комунікації в освітньо-науковій та інноваційній сферах: матеріали круглого столу *Філософсько-правові та прикладні аспекти*, м. Вінниця 12 травня 2017 р., Вінницький державний педагогічний університет ім. М. Коцюбинського / упоряд.: О.Д. Довгань, М.В. Беланюк, С.А. Лапшин, О.Г. Радзієвська, О.І. Яременко [та ін.]. Київ: Видавничий дім "АртЕк", 2017. С. 31-39.

17. Довгань О.Д. Ткачук Т.Ю. Концептуальні засади законодавчого забезпечення інформаційної безпеки України. *Інформація і право*. 2019. № 1. С. 86-100.

18. Довгань О.Д., Доронін І.М. Ескалація кіберзагроз національним інтересам України та правові аспекти кіберзахисту: монографія. – (НДІІП НАПрН України). Київ: Видавничий дім "АртЕк". 2017. 107 с.

19. Брижко В.М. Філософія права: герменевтика в сфері інформаційного права. *Правова інформатика*. № 1(41)/2014. С. 18-22.

20. Фурашев В.М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності. *Інформація і право*. № 2(5)/2012. С. 162-169.

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