УДК 340+35.078.3

ДОВГАНЬ О.Д., *доктор юридичних наук, професор,*
ДНУ ІІБП НАПрН України.
ТАРАСЮК А.В., *доктор юридичних наук, доцент*,
ДНУ ІІБП НАПрН України.

КІБЕРБЕЗПЕКА “СУСПІЛЬСТВА ЗНАНЬ” ЯК НЕВІД’ЄМНА СКЛАДОВА ПОСТУПАЛЬНОГО РОЗВИТКУ УКРАЇНИ У ПОСТВОЄННИЙ ПЕРІОД

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 та розвитку суспільства знань і післявоєнний період.*

Ключові слова: *кібербезпека, інформаційна безпека, кіберпростір, кіберзагрози, суспільство знань.*

Summary. *The article analyzes the main principles of the development of Ukraine's national interests in the cyber sphere, as well as identifies the related current problems of ensuring cyber security. It is substantiated that the regulatory and legal framework is the main prerequisite for ensuring the cyber security of the state. According to the results of the study, possible ways of solving the relevant problems and increasing the effectiveness of ensuring cyber security and the development of the knowledge society and the post-war period are determined.*

Keywords: *cyber security, information security, cyber space, cyber threats, knowledge society.*

Постановка проблеми. Майже рік як Україна героїчно протистоїть російському вторгненню. Демократичний світ всебічно підтримує народ України у продовж всього часу протистояння. Кіберпростір не є винятком, оскільки росія атакує не тільки фізично, а й віртуально. Організації, що переймаються ситуацією в Україні, не тільки допомагають Україні, але й вивчають поточні моделі впливу та захищають українську та західну інфраструктуру. Кіберпростір став повноцінним театром військових дій. На цьому фронті присутні найбільше виявлення місць дислокації ворога та багато іншого. Попри таке розмаїття арсеналу зброї, практично усі українці стали в ряди інформаційних військ і ведуть боротьбу проти загарбника. У боротьбі з різним асортиментом зброї (маніпуляції, інформаційні впливи, фейки, пропаганда), чітко знаємо яку інформацію і куди слід передавати щоб ЗСУ та інші суб’єкти змогли оперативно відреагувати. У перші дні війни у додатку “Дія” запустили чат-бот “єВорог”, куди можна надсилати фото та відео, де видно перебування російських військ та їхньої техніки, трохи згодом з’явився застосунок “єППО”. Через нього українці можуть повідомити про ворожі літаки, ракети, гелікоптери чи безпілотники. А щоб уникнути фальшивих повідомлень, розробники ввели авторизацію через додаток “Дія”. Створена у перші дні війни ІТ-армія стала українським ноу-хау у світі і безпрецедентним прикладом миттєвої реакції на дії ворога у кіберпросторі. Отже, проблематика цієї статті визначається, перш за все, гостротою самої проблеми забезпечення кібербезпеки, викликаної воєнною агресією рф, особливо її правової складової, сфокусованої на забезпеченні безпеки суспільства нової генерації, вивченні ціннісних уподобань людини на тлі трансформування реальності.

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.Г. Данильяна, О. Дзьобаня, С. Жданенка та ін.

Метою статті є визначення концептуальних засад розвитку кібербезпеки національного "суспільства знань" у післявоєнний період.

Виклад основного матеріалу. Осмислення сукупності інформаційних процесів щодо забезпечення їх безпеки набуває пріоритетного значення. Ситуація, що склалася свідчить про необхідність адекватної філософської рефлексії, подальший розвиток основних онтологічних вимірів, вироблення нової аксіологічної парадигми, у відповідності новим формам буття пов'язаних як з сучасними можливостями так і сучасними загрозами в інформаційній сфері. У зв'язку з цим цілком закономірний пошук основоположних цінностей, цілей та інтересів, які зададуть орієнтири майбутнього розвитку "суспільства знань" у післявоєнний період, заснованого на широкому використанні інформаційних технологій, закладуть фундамент, що підтримує внутрішній світ людини, визначає стійкість суспільства та безпеку держави в цілому.

На сьогоднішній день очевидна необхідність в тому, що діюча система кібербезпеки нашої держави повинна першочергово орієнтуватися на захист державної безпеки. Захист основних прав і свобод громадян України, гарантування рівноправної участіусіх суб'єктів інформаційної взаємодії в системі глобальної кібербезпеки, правовий захист національних цінностей, цілей та інтересів у кіберпросторі займають другорядну роль. Адже, перемога у війні є основою функціонування як самої держави так і її громадян. У зв'язку з цим значення досліджень характеру кібербезпеки суспільства тільки зростає, оскільки сприятиме реалізації таких ключових обов'язків держави, як формування оптимальних умов для її інтеграції в глобальний інформаційний простір, вироблення науково обґрунтованої загальної теорії інформаційної безпеки, що є архіважливим у воєнний час. Дослідження кібербезпеки з правничої точки зору пов'язане з формуванням якісної системи безпеки, що відповідає вимогам сучасного світу, що створює безпечні умови для подальшого післявоєнного поступального руху цивілізації, а також для нагальних потреб даного етапу розвитку України як повноправного та надійного партнера та співучасника європейського суспільства.

Підтвердженням висловленої думи є аналіз кіберзагроз, джерелом яких сьогодні також є РФ. Так, Державні установи та компанії Литви зазнали більшої кількості кібератак. Перша половина липня була насиченою через напруження, викликане тим, що ЄС перекрив залізничне сполучення з Росії до Калінінграда. Ця санкція зробила Литву мішенню для російських груп APT. Національний центр кібербезпеки та регіональний центр кіберзахисту повідомили про збільшення кількості DDoS атак. Атаки переважно були спрямовані на урядові організації, банківську систему і систему зв'язку, тим самим тимчасово унеможливлюючи надання певних послуг. В Україні також спостерігається збільшення випадків шахрайства (фішингу), пов'язаних з темами війни. Було виявлено кілька сторінок Facebook, що мали зв'язок із зловмисним веб-сайтом під назвою "Єдиний компенсаційний центр повернення несплачених коштів". Після введення інформації платіжної карти, банківські реквізити жертви компрометувалися (були під загрозою розголошення). CERT-UA виявила масове розповсюдження шахрайських електронних листів під назвою "Інформаційний бюлетень" та "Бойове розпорядження", що були нібито надіслані Національною академією Служби безпеки України. Листи надходили на приватні адреси електронної пошти. Якщо користувач відкриває

вкладення, то відбувається зараження шкідливим програмним забезпеченням “GammaLoad.PS1_v2” [1, с. 4].

Більш відчутною була атака, здійснена групою XakNet, яка зламала систему одного з найбільших виробників металопродукції в Україні, групи AV metal, що призвело до витоку понад 2 Гб даних, включаючи: рахунки-фактури та персональні дані, інформацію по операціям, кредитним і платіжним карткам, а також конфіденційну банківську інформацію за період з 2016 по 2022 роки. Протягом ІІІ кварталу поточного року, Міністерство Оборони Грузії зазнавало постійних атак. Механізмом доставки шкідливого ПЗ було обрано шахрайство (фішинг) електронною поштою. Декількох користувачів попросили завантажити та відкрити рахунок-фактуру або інший документ, що в подальшому призвело до активізації і встановлення “NanoCore RAT” в комп’ютерну систему жертви.

Після того, як група KillNet оголосила кібервійну більшості європейських країн у ІІ кварталі і провела одну з найбільших DDoS-атак проти великої кількості суб'єктів, наразі останні тенденції вказують на те, що оскільки російські війська програють на полі бою, то хектівісти/хакери KillNet також втрачають мотивацію. Після активного літа, коли група провела численні кампанії проти організацій в багатьох різних країнах, восени KillNet сповільнила свої атаки і перейшла до поширення дезінформації про війну. KillNet також оголосив кібервійну Японії націлившись на онлайн-ресурси японського уряду, системи метро Токіо і Осаки, порт Нагоя, платформу соціальних медіа mixi і податкову систему eLTAX [1, с. 4].

Успішне ведення інформаційної війни неможливе без масиву надійних специфічних даних про супротивника, зауважує професор Лібіцкі. “Накопичення цих знань включає аналіз ЗМІ супротивника, оцінку впливу мас-медіа на прийняття рішень на державному рівні, детальне вивчення бюрократичного апарату країни, національної комунікаційної інфраструктури, особливостей програмного забезпечення систем управління і т. ін. У цих умовах ґрунтовна підготовка фахівців для кваліфікованого провадження інформаційних операцій на всіх їхніх етапах набуває винятково важливого значення. Придушення противника не є пріоритетом діяльності таких фахівців – їхня головна мета полягає в забезпеченні інтересів *своєї* держави” [2]. Зазначена теза професора Лібіцкі цілком актуальна і в наші дні.

На наше переконання ми вже сьогодні маємо думати про післявоєнний стан і запроваджувати можливі механізми прискорення розвитку нашої держави у всіх сферах. Кіберпростір, як і нині, відіграватиме особливе значення. А тому фундаментальні основи мають бути не тільки закладені, а й набувати поступального розвитку. Що стосується “суспільства знань”, то фундаментальні основи цієї концепції закладені у Всесвітній доповіді ЮНЕСКО “До суспільств знання” ще у 2005 році [3]. У цьому стратегічному документі дані критерії розмежування між інформаційним суспільством та суспільством знань, в основі чого покладено технології, характерні для інформаційного суспільства, натомість, суспільство знань має ширші соціальні, етичні та політичні параметри. Основна ідея суспільства знань, відповідно до цього документу – це гуманізація процесу глобалізації.

У теперішній час не існує єдиної загальновизнаної концепції постіндустріального суспільства, проте аналіз праць багатьох дослідників дозволяє виявити певні спільні погляди. Так, практично усі вони погоджуються з такою періодизацією розвитку людства: суспільство доіндустріальне, індустріальне й постіндустріальне [4 – 8]. При цьому головним відмінними рисами останнього періоду від попередніх називаються: інформація стає провідним виробничим ресурсом замість сировини й енергії; пріоритет

у виробничій діяльності переміщується з видобутку й вироблення на обробку; на зміну попереднім праце- та капіталомістким виробничим методам і процесам приходять технології, засновані на науці.

Крім того, у розвитку постіндустріального суспільства підкреслюється провідна роль знань і технологій. І, нарешті, більшість дослідників погоджуються, що сучасний період суспільного розвитку є перехідним.

Як зазначав у праці "Інформаційне суспільство як суспільство постіндустріальне" Й. Масуда, на відміну від матеріального виробництва в індустріальному суспільстві в суспільстві інформаційному на пріоритет належить виробництву знання й інформації. Соціальні зв'язки, потрібні для суспільного розвитку, формуються у процесі масового виробництва інформації, а відтак значно зростає роль комунікативної діяльності й соціального управління. Зникає примат речей, їх вироблення, а натомість відбувається масове виробництво знань. Таким чином, кожен член соціуму реалізує свої здібності, виробляючи нове знання й інформацію за допомогою комп'ютерних й інформаційно-телекомунікаційних технологій [9, с. 25]. Крім того, зважаючи на те, що інформація за своєю сутністю є транскордонною, Й. Масуда атрибутивною складовою переходу до інформаційного суспільства вважає загальні глобалізаційні процеси.

Підсумовуючи аналіз теорій, зазначимо, що перші спроби людини зберегти таємність будь-якої інформації поклали початок формуванню теоретичних основ інформаційної безпеки. З розвитком технологій і обсягів передачі даних змінювалися методи захисту інформації. Як бачимо, на сучасному етапі розвитку суспільства ефективне забезпечення інформаційної безпеки дозволяє вирішувати ключові питання практично всіх видів національної безпеки. Кібернетична безпека є важливою складовою системи національної безпеки, і від успішного вирішення питань даної сфери залежить забезпечення глобальної загальносвітової безпеки.

Ми підтримуємо позицію тих науковців, які виокремлюють ще одну концепцію інформаційного суспільства – *суспільство знань*. Ця концепція не є новою для нашого часу, проте її найбільший прояв відбувся саме із розвитком інформаційно-комунікаційних технологій у 21 ст. У 1993 р. з'явилася праця одного з найбільш впливових теоретиків менеджменту 20 століття Пітера Друкера "Постекономічне суспільство" [10], перший розділ якої дослідник назвав "Від капіталізму до суспільства знань". До речі, сам вчений називав себе "соціальним екологом".

Цікавою з цього приводу є позиція ЮНЕСКО, у Всесвітній доповіді якої "До суспільств знання" у 2005 році [3], зазначалося, що "суспільство знань відрізняється від інформаційного суспільства, оскільки інформаційне суспільство ґрунтується на понятті технології, а суспільство знань має ширші соціальні, етичні та політичні параметри". Абсолютно вірний на наш погляд підхід з єдиною поправкою: якщо в основі інформаційного суспільства завжди покладено інформацію та технології її обробки, поширення, перетворення та передачі, то в основі суспільства знань – завжди процес перетворення інформації на знання.

Варто також, на нашу думку, акцентувати увагу, що існуючі форми та способи комунікацій, характерні для суспільства знань, здійснюються задля задоволення потреб, реалізації інтересів і цінностей особи й суспільства, а не заради інформаційної взаємодії як такої. Саме це, вважаємо, і є ціннісним самопізнанням під час аналізу інформаційної картини післявоєнного періоду розвитку нашої держави. Саме в цьому полягає сутність аксіологічного підходу до вивчення інформаційної сфери – процесів, взаємодії, обміну, продукції, послуг та ін., які ми розглядали в попередніх розділах нашої роботи.

При формуванні інформаційної картини світу ціннісними міркуваннями неодмінно охоплюється широке коло явищ і проблем, амплітуда оціночних суджень щодо яких може бути вельми значною, аж до протилежних. Це стосується, скажімо, оцінювання беззаперечної користі чи абсолютної шкоди будь-чого, кібербезпеки чи кіберризиків і загроз тощо.

Отже, розвиток суспільства знань – це не лише матеріалізація технологічних досягнень в інформаційній сфері, а передовсім прогрес самої соціальної структури людської спільноти, котра прагне до максімальн повного задоволення своїх потреб у цій царині. А втім, розбудова інформаційного суспільства ще більшою мірою зумовлена еволюцією людини як носія соціальних цінностей, розвитком творчих потенцій особи, її здатності до критичного мислення, зростанням індивідуалізації, обсягів особистих та громадянських прав і свобод, демократичних основ організації суспільного життя, формуванням інформаційної культури. Важливим аспектом у розвитку суспільства знань є наявність кіберпатріотизму, під яким ми розуміємо набуту суспільством систему характеристик, що постійно розвивається в процесі комунікацій як через вплив різних інституцій громадянського суспільства, ЗМІ та ін., є усвідомленням суспільством своєї приналежності до нації, високим духовно-моральним ставлення громадянин до своєї Батьківщини, яке виявляється в активній і цілеспрямованій діяльності з пропаганди національних інтересів, відстоювання їх у кіберпросторі та високим рівнем інформаційної культури. Невід'ємним елементом кіберпатріотизму є національна самосвідомість, під якою ми розуміємо глибоке усвідомлення суспільством своєї приналежності до української нації.

Із соціально-економічної точки зору передумовами прогресу суспільства знань є вільний розвиток індивідуально-творчої конкуренції, коли з-поміж соціально спрямованих технологій обираються найкращі та найефективніші. З огляду на примат вільної творчості до числа атрибутивних передумов удосконалення інформаційного суспільства слід віднести також соціальне забезпечення, медицину, освіту, культуру, тобто ті галузі, котрі забезпечують поступальний і безпечний розвиток особистості, життєдіяльність людини.

Соціально-політичними засадами розвитку суспільства знань є, безперечно, перманентна демократизація політичного ладу, формування громадянського суспільства, толерантність і плюралізм, пріоритет прав і свобод людини.

Без втілення наведених вище цінностей як атрибутів суспільства знань та інформаційної картини світу недосяжним є формування нового типу соціуму, котрий ґрунтується на глобальних інформаційних комунікаціях (взаємодії та обміні) і який ми хочемо сформувати у післявоєнній Україні. Відображенням аксіологічного підходу саме і є наведений вище аспект розгляду, який виходить із засадничих особистісних і соціальних цінностей.

Таким чином, можна стверджувати, що новостворене суспільство знань сформувало й нову дійсність – віртуальну реальність. Ця ж формація продемонструвала новий тип соціального поступу – нелінійний розвиток суспільства, що зробило проблематичними усі прогнози. Формування нової реальності зумовило виникнення нових соціальних цінностей – інформаційних, котрі на цьому етапі еволюції світової спільноти стали визначальними.

Відтак, створення глобального суспільства знань, нового світу, де усі соціальні процеси об'єднані у всеосяжні форми інформаційно-комунікативної взаємодії й інформаційного обміну спричинило те, що включення розрізнених до того елементів соціуму, різноманітних устроїв і способів господарювання в єдину загальну інформаційну

картину світу, стало однією із фундаментальних цінностей цього світу й, відповідно, його інформаційної картини. Іншими словами, інтегративні концептуальні чинники перетворилися на атрибутивні цінності світу інформаційного суспільства. І в цій іманентній системі цінностей всеохоплююча інформаційна взаємодія, якою охоплені відокремлені раніше форми соціальної комунікації, виступає як цілісна картина світу. Тому на вказаному етапі розвитку людства показником розвиненості, інноваційності, цивілізованості врешті-решт, стає включеність, інтегрованість у цілісний інформаційний світ.

Стосовно суспільства знань вказаний вище показник передбачає високий рівень розвиненості інформаційно-комунікативної інфраструктури, відповідних техніки й технологій, поширення сучасних цифрових технологій на всі сфери життєдіяльності соціуму. Зазначені вище рівні соціального розвитку не є суто технічними й технологічними. Аби вони такими стали, потрібні належні соціально-економічні умови – розвиток науки й інноваційного виробництва, високоякісна освіта, розвинена інфраструктура забезпечення вказаних процесів (медична, соціальна, правова та ін.). Утім, і виконання цих умов замало, позаяк втілення в життя цього цивілізаційного поступу неможливе без низки базових чинників: побудови правової держави з рівними для всіх правами й можливостями; вдосконалення усієї сукупності соціальних відносин, загальної культури суспільства, політичних, державних і громадських інституцій, які забезпечують вільний і всебічний розвиток особистості.

Що стосується особистості, то, крім високої освіченості й загальної культури, для її "вписування" в єдину інформаційну післявоєнну картину нашої держави необхідні такі властивості, як інформаційна компетенція, комп'ютерна (цифрова) культура, спроможність і бажання кожної людини не бути лише пасивним "нейтроном" інформаційної взаємодії, а стати її активним, творчим суб'єктом, "електроном" інформаційної соціальності. До єдиної глобальної системи інформаційного світоустрою людина має увійти чинником вільного й творчого особистісного розвою як запоруки відповідного розвитку всієї світової спільноти. І як слушно зауважують О.П. Дзьобань та С.Б. Жданенко, усе суспільство стає системою освіти, протягом усього життя людина повинна отримувати нову освіту [11, с. 64].

Саме вказані консолідуючі чинники, котрі стосуються не лише суспільства загалом, а й кожної людини, є незаперечними фундаментальними цінностями інформаційного суспільства як сучасного етапу цивілізаційного розвитку людства. При цьому більшість проблем щодо інформаційної безпеки особи й соціуму на етапі інформаційного суспільства розв'язуються за допомогою саме цих незаперечних фундаментальних цінностей.

Ще одна базова властивість суспільства знань – інноваційність. Специфікою інформаційної епохи є вибухове зростання нового знання. Його потенціал настільки значний, що чимало фахівців іменують сучасну економіку розвинутих країн "заснованою на знанні", "знаннєвою" і т.п. Адже сучасність вимагає, щоби здобуті наукою знання негайно втілювалися в техніці, технологіях, виходили продуктом на світові ринки, а базисом будь-якого знання є інформація [12, с. 44].

В інформаційну епоху однією із найважливіших цінностей стає оволодіння інноваційними знанням і технологіями. Їх величезний потенціал здатен докорінно трансформувати економіки країн. Лавиноподібне поширення заснованих на інноваційному знанні інформаційних технологій, їх активне застосування в організації економіки, у виробництві та споживанні, фінансовій та інших сферах виводять відповідні знання в лідери в ринковій конкуренції.

Про те, що інновації є не просто популярним віянням сучасності, а однією із фундаментальних цінностей інформаційної епохи, може свідчити хоча б різке зростання попиту на високотехнологічну інноваційну продукцію. Знаннєва економіка базується на найпрогресивніших, найсучасніших, інноваційних досягненнях, а стрімке впровадження відповідних технологій сприяє тому, що найважливішими складовими сучасного ринкового продукту (товарів, послуг) стають знання й інноваційність.

У теперішній час економіка все більше тяжіє до сфери надання послуг, а не, як раніше, до товарного виробництва. Інформаційна епоха зумовлює зміщення пріоритетів від матеріальної товарної форми, фізичного існування засобів виробництва, капіталів, техніки тощо до інноваційно-технологічної, тобто інтелектуальної, розумової, знаннєвої, інформаційної. Мало того, сучасна економіка все більше охоплює увесь світовий простір, долаючи географічні перешкоди й національні кордони, як зазначає багато вітчизняних і зарубіжних фахівців. Відтак, економіка, заснована на знаннях, є передовсім економікою епохи інформаційної, економічної й культурної глобалізації.

Плюралізм як базова цінність інформаційної епохи означає рівне співіснування, багатоманітність поглядів, ідеалів, ідеологій, підходів до шляхів розвитку суспільства тощо. Його цінність полягає в урахуванні варіативності шляхів розвитку, соціального прогресу, соціальної динаміки.

Розв’язання проблеми забезпечення глобальної кібербезпеки лежить у площині створення умов захищеності особи як суб’єкта глобального інформаційного суспільства від внутрішніх і зовнішніх загроз. Тому вбачається за доцільне детальніше дослідити специфіку інформаційного суспільства в контексті створення належних умов для реалізації людиною усіх своїх прав і законних інтересів, усебічного особистісного розвитку.

Висновки.

Серед концептуальних засад правового забезпечення кібербезпеки України на етапі розвитку розвитку національного “суспільства знань” визначено наступні:

1) розвиток державно-приватного партнерства у сфері взаємодії державних органів із громадськими організаціями та громадянами з метою забезпечення кібербезпеки України;

2) інформаційно-просвітницька, ідеологічна й освітня роботи із протидії радикальній ідеології та екстремізму;

3) вдосконалення нормативно-правового забезпечення протидії використанню Інтернету в терористичних й екстремістських цілях, а також забезпечення національних інтересів суверенної України в інформаційній сфері;

4) розвиток міжнародного чинника з метою утвердження України як повноправного учасника глобальних інформаційних процесів заради подальшої інтеграції в НАТО та покращення іміджу нашої держави серед міжнародних партнерів;

5) створення, розвиток і забезпечення безпеки національних інформаційних ресурсів;

6) практична реалізація на рівні законодавчого забезпечення національних інтересів України в кіберсфері;

З урахуванням міжнародного досвіду та на основі аналізу національної практики можемо запропонувати наступні чотири основні складові національних інтересів, які мають стати базовими принципами післявоєнного періоду України в кіберсфері:

1) 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;

2) 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;

3) 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;

4) захист інформаційних ресурсів від несанкціонованого доступу, забезпечення безпеки телекомунікаційних й інформаційних систем, як створюваних, так і тих, що функціонують на території України.

Очевидним є той факт, що кіберзагрози стрімко зростають через поточні події та впливають на нас різними способами. Відзначаємо, що державна влада і приватні компанії більш серйозно ставляться до завдання убезпечення власної інфраструктури. Факти вказують, що не всі захищені від DDoS-атак або фішингових кампаній, тому необхідно більше уваги приділяти саме деталям. Відповідно кібербезпека має стосуватися кожного працівника організації, а не лише IT-фахівців. Політика кібербезпеки важлива, оскільки кібератаки та викрадання даних потенційно дорого коштують, особливо в час війни. Посилення захисту від загроз, що постійно змінюються, стане легшим зі знанням нових технологій кібербезпеки, методології, тактики та організаційної структури. Кібербезпека – це нескінченна битва. Тривалої остаточної відповіді на це питання в осяжному майбутньому не буде. Складність системи інформаційних технологій, невід'ємна природа інформаційних технологій і людська помилковість у винесенні суджень про те, які дії та інформація є безпечними чи небезпечними з точки зору кібербезпеки – особливо коли такі дії та інформація дуже складні – є головними причинами проблем кібербезпеки. Загрози кібербезпеці також змінюються з часом. Зловмисники пристосовуються, створюючи нові інструменти та тактики для підриву безпеки, коли розробляються нові засоби захисту для протистояння нещодавнім атакам. Тому покращення стану системи кібербезпеки – і, як наслідок, організації, в яку вона вбудована, – слід розглядати як безперервний процес, а не щось, що можна завершити один раз, а потім проігнорувати. Саме цей постулат і є невід'ємною складовою і характерною рисою "суспільства знань".

Пріоритетами подальших наукових пошуків можуть бути питання імплементування передових та дієвих освітніх практик в національну систему підготовки кадрів для сфери кібербезпеки, систематизація досвіду протидії російській агресії в кіберпросторі, міжнародний обмін досвідом в означених сферах.

Використана література

1. 3rd QUARTER REPORT, 2022. Issued by the regional cyber defence centre. 1 July – 30 September. 13 s.

2. Martin C., Libicki M. What is information warfare? Washington, 1995. URL: http//www. rand.org/about/people/l/libicki_martin_c.html

3. К обществам знания: Всемирный доклад ЮНЕСКО 2005. URL: http//unesdoc.unesco

4. McKinsey Global Institute. Applying artificial intelligence for social good . Global Institute. 2018. URL: https://www.mckinsey.com/featuredinsights/artificial-intelligence/applying-artificial-intelligence-for-social-good

5. The Global Competitiveness Report 2018. *World Economic Forum*. Geneva. 2018. URL: https://www.weforum.org

6. Сучасне суспільство: філософсько-правове дослідження актуальних проблем: монографія / О.Г. Данильян, О.П. Дзьобань, С.Б. Жданенко та ін.; за ред. О.Г. Данильяна. Харків: Право, 2016. 488 с.

7. Інформаційне суспільство в світі та Україні: проблеми становлення та закономірності розвитку: колективна монографія / за ред. д.ф.н., проф. В.Г. Воронкової. Запоріжжя: Вид-во ЗДІА, 2017. 292 с.

8. Dzeban O., Aleksandrova O., Vinnikova N. Axiological portrait of information society. *Схід: аналітично-інформаційний журнал*. 2019. № 5 (163). С. 13-19.

9. Yoneji Masuda The Information Society as Post-industrial Society. World Future Society, 1981. P. 171.

10. Drucker P.F. The Age of Discontinuity: Guidelines to our Changing Society. London: Heinemann, 1969.

11. Дзьобань О.П., Жданенко С.Б. Від "інформаційного суспільства" до "інформаційної безпеки": до проблеми концептуалізації сутності понять. *Інформація і право*. № 2(29)/2019. С. 60-73.

12. Довгань О.Д., Тарасюк А.В., Ткачук Т.Ю. Кібербезпека "суспільсва знань": монографія. Київ-Одеса: Фенікс, 2021. 176 с.

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