UDC: 32.329 DOI: 10.15421/172164

Анна Стичинська
Київський національний університет імені Тараса Шевченка (Київ, Україна)

Теоретичні основи політики інформаційної безпеки

Метою цієї статі є визначення теоретичних основ політики інформаційної безпеки як ключового фактору життя суспільства у сучасному світі.

В Україні, так само як і у всьому світі, проблеми забезпечення безпеки держави, суспільства і особистості все більше виходять на перший план у державній політиці. Національна безпека одна з пріоритетних цілей сучасної держави і є основних чинником її стабільного розвитку. Впровадження сучасних інформаційних технологій в усі сфери суспільного життя істотно підвищило залежність суспільства від надійності функціонування інформаційного простору, достовірності отриманої інформації, її захисту від несанкціонованого втручання. Політика держави у цій сфері повинна ґрунтуватися на нормах міжнародного права та активної співпраці держав у міжнародних відносинах.

Необхідність дослідження даної теми викликана тим, що в даний час міждержавні та міжнаціональні конфлікти все частіше протікають саме в інформаційному полі. Для України інформаційна політика є додатковим потужним ресурсом у здійсненні модернізації країни і вирішенні багатьох поточних внутрішніх і зовнішніх проблем. Цілком очевидним є той факт, що відставання країни в області технологій інформаційної політики не може сприяти успіху у вирішенні поставлених завдань.

Ефективність здійснення влади в будь-якій державі, в тому числі і в Україні залежить від її інформаційного забезпечення. Без інформації неможливо уявити позитивно функціонуючу політичну структуру, розвиток масової політичної свідомості, взаємодію суб'єктів політики. В процесі інформаційно-комунікативного впливу в свідомості народу формується образ державної влади, його політичних інститутів і лідерів, а керуючі функції держави здійснюються з найбільшим потенціалом і найменшими енергетичними затратами лише тоді, коли досить добре розвинена система інформаційних зав'язків між державою, громадянським суспільством і особистістю.

При цьому політика держави в області інформаційної безпеки повинна ґрунтуватися на принципах забезпечення нормального соціального, політичного економічного і технологічного розвитку суспільства.

Ключові слова: *інформаційна безпека, міжнародні відносини, державна політика національної безпеки, загрози кіберпростостору.*

Anna Stychynska
Taras Shevchenko National University of Kyiv (Kyiv, Ukraine)

Theoretical Fundamentals of Information Security Policy

The purpose of this article is to determine the theoretical foundations of information security policy as a key factor in society in today's world.

In Ukraine, as well as throughout the world, the problems of ensuring the security of the state, society and the individual are increasingly coming to the fore in state policy. National security is one of the priority goals of a modern state and is the basis for its stable development. The introduction of modern information technologies in all spheres of public life has significantly increased the dependence of society on the reliability of the information space, the reliability of the information received, and its protection from unauthorized access. The state policy in this area should be based on the norms of international law and active cooperation of states in international relations.

The need to study this question is due to the fact that currently interstate and interethnic conflicts are increasingly taking place in the information field. For Ukraine, information policy is an additional powerful resource in the modernization of the country and solving many current internal and external problems. It is quite obvious that the country's backwardness in the field of information policy technologies cannot contribute to success in solving the set tasks.

The effectiveness of the exercise of power in any state, including Ukraine, depends on its information support. Without information, it is impossible to imagine a positively functioning political structure, the development of mass political consciousness, the interaction of political actors. In the process of information and communication influence in the minds of the people the image of state power, its political institutions and leaders is formed, and the governing functions of the state are carried out with the greatest potential and lowest energy costs only when the system of information links between the state, civil society and personality.

At the same time, the state policy in the field of information security should be based on the principles of ensuring normal social, political, economic and technological development of society.

Keywords: *Information Security, International Relations, State National Security Policy, Danger of Cyberspace*

Вступ.

Важливим теоретичним джерелом дослідження проблем інформаційної безпеки є комплекс робіт, присвячених проблемам національної та міжнародної безпеки. Традиційно фахівці в області безпеки приділяли основну увагу її військовим аспектам і проблемам роззброєння. У зв'язку з цим особливу важливість для проведеного дослідження набувають роботи, в яких безпека розглядається як багатофакторне, «структурне» явище, що не зводиться тільки до військово-політичних та військово-технічних компонентів, в яких соціальний вимір набуває все більшого значення. Цього підходу до проблем безпеки дотримуються, наприклад, Р.Алман, Р. Смоук, Дж. Коллінз, Р. Уоккер, П.Бек, М. Берковитц, А. Беламі.

Що стосується проблем саме інформаційної безпеки, то дану проблему вивчали В.Ю. Богданов, О.В. Глазов, О.Л Гуровський, О.Г. Данільян, О.П. Дзюбань, В.К. Пархоменко, Д.В. Дмитрієв, А.Л. Корсунський, В.А. Ліпкан, В.В. Лунєєва, М.М. Тугай, І.В. Соркі, О.В. Ющук та ін. Вищезгадані науковці зазначають, що на сьогодні Україна опинилася у стані інформаційної війни з країнами, які намагаються нав'язати свої цінності, зруйнувати традиційні морально-етичні засадиукраїнськогосуспільстватавпливатина дестабілізацію політичної системи. Розвиток інформаційних технологій призвів до того, що інформаційна експансія відбувається постійно, а злочини проти інформаційної безпеки стають все більш витонченими і небезпечними. За останній час інформація набувала властивості потужного засобу впливу на громадсько-політичні, ідеологічні та соціально-економічні процеси і стала свого роду зброєю, яка вимагає створення системи протидії, захисту інформаційних ресурсів, які належать державним органам, що становлять державну, професійну та особисту таємницю (Гуровський, 2014). У роботі «Національна безпека України: сутність, структура та напрямки реалізації» О. Г. Данільян, О. П. Дзюбань, В. К. Пархоменко, Д. В. Дмитрієв зазначають, що розвиток інформаційних засобів веде до можливості встановлення такого тотального контролю над людьми, якого ще не було в історії людства (Національна безпека України, 2002).

Філософ А.Зіновєв у роботі визначає: «Теперь история не происходит по своей прихоти, стихийно. Она теперь осуществляется сознательно, можно сказать - по заказу сильных мира сего». Причини, через які це стало можливо він розглядає у наступному:

- прогрес збору, обробки і передачі інформації;
- прогрес засобів комунікації;
- прогрес засобів маніпулювання людьми, спостереження за ними, застереження масових рухів;
- вплив масової культури на стандартизацію способу життя людей (Зиновьев, 1996)

З точки зору О. Л. Сорокіна, інформаційна безпека становить стан захищеності особистості, суспільства, держави від інформації, що носить шкідливий або протиправний характер, від інформації, що надає негативний вплив на свідомість особистості, перешкоджає сталому розвитку особистості, суспільства і держави. Інформаційна безпека включає також комп'ютери та інформаційно-телекомунікаційну інфраструктуру і інформацію, що в них знаходиться, яка також забезпечує сталий розвиток особистості, суспільства і держави (Баровська, 2014).

Результати дослідження.

Проблема інформаційної безпеки стала пріоритетним питанням саме з виникненням нового типу загрози – «інформаційної війни». Одне з визначень «інформаційної війни» було дано І. Завадським, він зазначає, що «Інформаційна війна складається з дій, які застосовуються для досягнення інформаційної переваги у забезпеченні національної військової стратегії шляхом впливу на інформацію та інформаційні системи суперника, з одночасним укріпленням і захистом нашої власної інформації та інформаційних систем».

Фактично, завданням інформаційної безпеки стає не знищення живої сили, а підрив цілей, поглядів та світосприйняття населення, тобто у зруйнуванні соціуму. На думку Завадського, основні інформаційні війни розвернулись у кібернетичному просторі, а сьогоднішня задача будь-якої держави полягає у тому, щоб виростити гідних військових, які спроможні здобути перемогу. Сучасні інформаційні перемоги у своїй більшості засновані не на серйозних інформаційних технологіях, а як і всі попередні війни, на тому, що «окремі джерела інформації» продаються і купляються (Завадський, 1996).

Д. С. Черешкин, Г. Л. Смолян та В. Н. Цигичко визначають, що інформатизація веде до створення єдиного світового інформаційного простору, в рамках якого здійснюється використання інформації, створення, зміна, збереження та обмін нею між суб'єктами цього простору – людьми, організаціями та державами.

Виникнення інформаційного простору призводить до появи бажаючих домінувати у цьому просторі, чи хоча б розділити цей простір, а також контролювати і управляти процесами, які відбуваються у ньому. Відповідно, для цього потрібно використовувати так звану інформаційну зброю, до якої можна віднести:

- засоби знищення, пошкодження чи викрадення інформації;
- засоби обходження систем захисту;
- засоби обмеження допуску законних користувачів та інші.

До варіантів цих видів зброї зазвичай відносять таку атакуючу зброю як комп'ютерні віруси, логічні бомби (програмні закладки), засоби перешкоджання інформаційному обміну у телекомунікаційних мережах, фальсифікацію інформації в каналах державного та військового управління, засоби нейтралізації текстових програм, помилки спеціально внесені в програмне забезпечення об'єкту.

Ще у 1996 році під егідою уряду США відбулася V Міжнародна конференція по інформаційній війні, на якій було анонсовано положення, що «стратегія застосування інформаційної зброї носить виключно наступальний характер» (Смолян, 2014). Відповідно, атакуючий і наступальний характер інформаційної зброї багато у чому визначає обличчя інформаційної війни і дозволяє визначити потенційного інформаційного агресора. І як наслідок, мірою інформаційної агресивності можна визначити обсяг інформації, яка передається від однієї країни до іншої. Щодо самої інформаційної зброї, то деякі науковці і політики вважають її небезпечніше ядерної, так як до її складових може входити не лише кібернетична складова, а й засоби масової інформації у вигляді баз даних, доступу до файлових носіїв, як елемент маніпуляції і пропаганди..

Якщо порівнювати наслідки від звичайної війни та інформаційної війни, то у першій можна визначити такі:

- загибель та імміграція частини населення;
- зруйнування промисловості;
- втрата частини території;
- політична залежність від сторони переможця;
- знищення армії потерпілої сторони;
- вивіз з країни найбільш перспективних технологій.

Щодо то наслідків другої, то вони можуть бути такими:

- стабільне скорочення інформаційної ємкості системи, знищення елементів цієї системи, що робить її безпечною для агресора;
- вирішення раніше непритаманних задач (тобто, вирішення задач на користь переможця, що часто суперечить ідеологічним, етичним чи юридичним нормам;
- переможена система підлаштовується чи повністю поглинається системою переможця.

Основна різниця також полягає у тому, що інформаційна війна не має закінчення, так як вичерпність та варіанти інформаційної зброї необмежені. У випадку війни з вогнестрільною зброєю переможцю залишаються зруйновані міста і покалічене населення, так як такий вид зброї в першу чергу направлений на знищення військової техніки та живої сили суперника. І таким чином, така зброя, особливо ядерна зброя, часто використовується як фактор «залякування» її подальшого використання, що призводить до психологічного тиску зі сторони більш сильної сторони.

Інформаційна зброя в свою чергу направлена на зміну поведінки інформаційних систем, а у випадку з її застосування проти населення – на зміну його свідомості і відповідно, на зміну його подальшої поведінки без попереднього «залякування» і фізичного знищення.

Таким чином, можна виокремити певні складові у типах війн відповідно до видів зброї яка у них використовується:

- знищення (використання фактичної зброї);
- залякування (домінування сторони, яка володіє потужнішою зброєю;)
- зміна поведінки (інформаційна зброя).

Мета будь-якої війни, в решті решт однакова і полягає у зміні поведінки противника, з метою поставити його на те місце, яке потрібне агресору. Переможцем інформаційної війни стає та сторона, яка більш повно здатна промоделювати поведінку противника у різних ситуаціях, визначити власний алгоритм поведінки та реалізувати його. А саме в більших об'ємах збирати, зберігати та опрацьовувати інформацію про суперника (його політичну, економічну, соціальну ситуацію, культуру, релігію і т.п.) Інформаційна війна – перестає бути просто війною між окремими державами, це війна між сучасними цивілізаціями. Виникнення сучасних телекомунікаційних засобів, за допомогою яких можна управляти масами, обходячи територіальні кордони, дозволяє розширити театр військових дій та залучати більшу кількість учасників.

Параг Ханна висунув щодо цього ідею переходу світу до мегаміст, які врешті решт зроблять держави другорядними акторами. Він каже про новий тип геополітики, коли війна за території змінюється війною за зв'язки. Відповідно і економіка буде вимагати від мегаміст вкладень у розвиток зав'язків, оскільки економіки стають все більш інтегрованими, а населення - більш мобільним. Конфлікти через зв'язки він вважає менш небезпечними ніж конфлікти через кордони між державами. «Карти комунікацій краще відображають геополітичну динаміку між наддержавами, містами-державами, транснаціональними компаніям, а також різного роду віртуальними співтовариствами у їх боротьбі за ресурси, ринки і популярність. Ми вступаємо в епоху, коли міста будуть означати більше, ніж держави, а ланцюжки поставок стануть важливішим джерелом влади, ніш військова потужність, головним завданням якої буде захист ланцюжків постачання, а не кордонів. Конкурентоспроможні комунікації – гонка озброєння двадцять першого сторіччя. І справді, можна сказати, що він бачить в майбутньому перетворення людства в одну багатонаціональну державу. І, по суті, Європейський Союз є таким прикладом, коли роль кордонів виявляється заниженою. «Інфодержава використовує як демократію, так інформацію для визначення ключових пріоритетів громадян і реальності (економічної, освітньої, інфраструктурної). Держава використовує комбінацію громадянина та інформації для породження політики, її моніторингу, відстеження зворотного зв'язку, аналізу в реальному часі» (Расторгуєв, 2003).

Війна є справою держави, але одночасно багато військових досягненнь автоматично стають цивільними. Першопочатково створення компьютерів, баз данних кібермереж були чисто військовими винаходами.

Основними перетинами війни і нових медіа на сьогодні є такі сфери:

- кібератаки та інформаційна безпека;
- гібридні війни;
- підтримка населення.

Інформаційна безпека і кібератаки стали прикметою сьогоднішнього дня, і вони ж зберігаються як чіткий тренд на майбутнє. І хоч ця сфера, яку можна позначити як інформаційно-технічна, набула найбільшого поширення і підтримки на сьогодні (Denning,2007), інтенсивний розвиток і креативний характер кібератак будуть робити її небезпечною ще довгий час. Тим більше що вона пов'язана з найбільш вразливим місцем будь-якої кіберсистеми - людським фактором. До того ж, в цій сфері має місце інтерес військових щодо цивільних цілей. Можна навести приклади останнього часу, такі як російське втручання у вибори президента Сполучених Штатів Америки - Трампа або президента Франції - Макрона, парламентські вибори в Німеччині, референдуми в Британії і Каталонії. На сьогоднішній день все це так би мовити

«тренінги», оскільки реальні наслідки не виявляються такими серйозними, але все одно одні військові розробляють атаки, в той час як інші намагаються їм протистояти.

Сучасні інформаційні війни є більш небезпечними і їх успіх базується саме на інформаційній перемозі. Анексія Криму 2014 року показала, що російська інтерпретація подій перемогла як українську, так і міжнародну. Російські солдати були у військовій формі, але без характерних відзнак. Відсутність пострілів позбавило страху з боку мирного населення і створювало хорошу телевізійну картинку, і завдяки проросійській пропаганді у ЗМІ та спотворенні інформації про новообрану владу після Революції Гідності викликало довіру до країни агресора. Донбас, а потім Одеса і Харків моделювалися вже картинкою народного повстання. Але тут ситуація переросла в збройну форму і створила зовсім іншу інтерпретацію, ніж та, яка була в Криму.

Сучасні соціальні мережі дають абсолютно новий арсенал для організації підтримки населення, для оцінки динаміки змін, яку проходить в цей період масова свідомість. Маніпуляція через ЗМІ, використання фейкової інформації, блокування доступу до теле- і радіотрансляцій на окупованих територіях, призвело до трагічних наслідків.

Ми бачимо, що сучасні медіа типу соцмереж висуваються на все більш важливі позиції в управлінні масовою свідомістю. Першими це зрозумів бізнес, за ним - політтехнологи, після них - військові. І це зрозуміло, оскільки сьогодні немає іншого механізму подібного типу, що дозволяє синхронно охоплювати мільйони людей в комфортному для них інформаційному середовищі.

Говорячи про забезпечення безпеки у будь-якій сфері варто дати відповідь на питання «Що теоретично можна зробити щоб захиститись від агресора?». Одними з варіантів відповідей є:

1. Поставити бар'єр між собою та джерелом небезпеки.
2. Приховатися від небезпеки за межі її досягнення.
3. Знищити джерело небезпеки.

Але якщо фізичне знищення може остаточно припинити діяльність агресора, то абсолютне викорінення інформаційної зброї неможливе. Будь-яка держава повинна посилювати систему інформаційної безпеки, основною задачею якої є забезпечення невтручання у внутрішню політику зовнішніх факторів, недопущення деструктивізму з середини та в першу чергу забезпечення прав і свобод своїх громадян і територіальної цілісності держави.

С. Расторгуєв приводить ряд аналогій в системі інформаційного захисту держави:

- прогнозування зовнішніх подій – розвідка;
- прогнозування внутрішніх подій – міністерство внутрішніх справ;
- перший ступінь захисту – кордон (прикордонні війська);
- другий спосіб захисту – зміна місця (переселення населення);
- третій ступінь захисту – знищення (армія);
- четвертий ступінь захисту – внесення змін (пропаганда, терор – через ЗМІ, спецслужби і т.п.);
- блок прийняття рішень – уряд;
- блок занесення інформації у бази даних – аналітичні служби (Расторгуєв, 2003).

Кожна складова є невід'ємною у процесі забезпечення інформаційної безпеки. Держава – це управлінська і регулююча структура. Але у більшості випадків інформаційна війна ведеться не проти держави, а за державу, за контроль над державою, яка стає інструментом у руках переможця для управління переможеним народом.

Не варто забувати, що в інформаційній війні перемагає як правило той, хто атакує і постійно посилює тиск. Якщо говорити про інформаційну атаку, то її ефективність прямо залежить від наявності елементів новизни, інакше до неї буде легко пристосуватись. В сучасних умовах всі науки, які мають відношення до інформаційного впливу повинні мати пріоритет, це і інформаційні технології, так і психологічні науки, щоб розуміти психологію противника.

При зміні державної форми правління у більшості країн світу, зміні політичного курсу чи правлячої верхівки в тій чи іншій державі вже давно використовують прийоми і методи боротьби за владу як одну з форм ведення інформаційної війни. Її суть полягає

у тому, щоб залучити до керівництва іншої держави своїх представників, носіїв власної ідеології та власних інтересів виключно інформаційними методами впливу. Не варто вважати, що в епоху інформаційних технологій та економічних зав'язків, вибори в державах залишаються справою виключно громадян держави і не мають відношення до геополітики. Інколи інші держави не тільки слідкують за процес боротьби за владу у інших країнах, але і втручаються у нього використовуючи всі можливі засоби. При цьому, втручання у виборний процес завжди відбувається таємно, використовуючи виключно інформацію, а сама влада, як результат, повинна дістатися інформаційному переможцю. Поле бою включає в себе ЗМІ, правоохоронні органи, виборчі комісії та інше. При недостатньому забезпеченню інформаційної безпеки, навіть підрахунок голосів комп'ютерними системами стоїть під загрозою. У чиїх руках механізми впливу, у тому числі ЗМІ, той і переможець. Тому переможцем інформаційної війни у виборах стає той, хто спроможний своєю системою управління охопити максимальну кількість осіб, які приймають участь у прийнятті остаточного рішення.

Щоб отримати перемогу у інформаційній війні, структура системи інформаційного забезпечення – так звана «інформаційна армія» - повинна працювати постійно, так як інформаційна загроза – це постійна загроза. Армія не створюється після того, як війна вже оголошена. Вона існує і в мирний час, однак під час загрози мобілізується.

Ведення поєдинку будь-яким видом зброї передбачає наявність певних структурних компонентів, одними з яких є:

- керівництво;
- аналітичний штаб (прогнозування розвитку подій та визначення стратегії і тактики ведення інформаційних дій по відношенню до суперника);
- відділ, відповідальний за збір інформації про суперника (розвідка);
- відділ, відповідальний за забезпечення безпеки власної інформації (контррозвідка);
- відділ, відповідальний за промислове виробництво необхідної інформації (реклама, фільми, друкована література та ін.);
- відділ, відповідальний за донесення інформації до об'єкта та інші.

Висновки.

Важливим фактором підвищення рівню інформаційної безпеки є забезпечення ефективної роботи всіх структурних елементів, через абсолютно реальну загрозу підкупу, шантажу чи залякування зі сторони супротивника. І саме відділ контррозвідки повинен розуміти всю небезпеку зовнішнього втручання і проводити ретельні перевірки як інформаційних складових, так і штатних працівників.

У зіткненні двох чи більше структур, які задіяні у інформаційному протиборстві, перемога дістанеться тій стороні, яка не лише більш детально збере відкриту і закриту інформацію про свого суперника і проведе її аналіз, але й зробить це швидше. Тільки у такому випадку одна сторона може, скориставшись знаннями про можливі майбутні дії суперника, нав'язати вигідний для себе сценарій.

Отже, виникнення і розвиток кіберпростору та інформаційного суспільства дає можливість державам прогресувати у розширенні комунікацій на міжнародній арені та на внутрішньому рівні. Але в той самий час це призводить до виникнення загроз втручання ззовні у політичну ситуацію держави. Інформаційна зброя на сьогоднішній день є найпотужнішою серед усіх відомих, так як її варіанти і методи застосування є необмеженими і не залежать від державних кордонів, фізичної сили комбатантів і вона дає змогу приховати істинного агресора. Інформаційна війна як новий виклик людству ставить пріоритетне завдання перед світовою спільнотою – розробити потужну систему інформаційної безпеки, як на рівні однієї держави, так і на глобальному рівні.

БІБЛІОГРАФІЧНІ ПОСИЛАННЯ

Баровська А. Інституційне забезпечення державної комунікативної політики : досвід країн Європи : аналітична доповідь. URL: http://www.niss.gov.ua /articles/1730

Бінько І.Ф. Національна безпека України в умовах глобальної інформатизації / І.Ф. Бінько. – К.: Національний ін–т стратегічних досліджень, 1996. – Вип.61. – 54 с.

Бурич К. Л. Інформаційна безпека України у сучасному кіберпросторі / К. Л. Бурич, І. Н. Єфименко, Б. Д. Коган // Національна безпека і оборона. – 2014. – №10. – С. 21–27.

Глобальний індекс кібербезпеки 2018. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/draft-18-00706_Global-Cybersecurity-Index-EV5_print_2.pdf

Горбулін В. П. Актуальні проблеми системного забезпечення інформаційної безпеки України / В.П. Горбулін, М.М. Биченок, П.М. Копка // Матеріали міжар. наук.-практ. конф. «Форми та методи забезпечення інформаційної безпеки держави». – К.: Нац. Акад. СБ України. – 2008. – С. 7985.

Горовий В. М. Правові перспективи національного розвитку. URL: http://uaforeignaffairs.com/ua/ekspertna-dumka/view/article/nablizhajuchi-derzhavu-do-suspilstva/#st hash.AgJjKJa4.dpuf

Гриняев С. Н. Информационная война: история, день сегодняшний и перспектива. URL: http://ww–4.narod.ru/warfare/grinyaev /page009.htm

Гуровський В. О. Роль органів державної влади у сфері забезпечення інформаційної безпеки України / В. О. Гуровський // Вісник Української академії державного управління при Президентові України. – К., 2014. – №3. – С. 21–31.

Довгань О. Д. Організація правового гарантування безпеки інформаційних обмінів у контексті глобалізації // Правова інформатика. – 2013. – № 4(40). – С. 79-88.

Доктрина інформаційної безпеки України від 25 лютого 2017 року. URL: http://disarmament.un.org/DDApublications/index.html.

Долженко К. І. Нормативно-правове регулювання інформаційної безпеки регіону / К. І. Долженко // Право і Безпека. – 2014. – № 3. – С. 43-48.

Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности. Доклад Генерального секретаря ООН. №A/71/172, 19 июля 2016 г. URL: http://undocs.org/ru/A/71/172

Дубов Д. Підходи до формування тезаурусу у сфері кібербезпеки / Д. Дубов // Політичний менеджмент. – 2010. – № 5. – С. 19–30

Забара І. М. Міжнародна інформаційна безпека в міжнародному праві: до питання визначення / І. М. Забара // Український часопис міжнародного права. – 2012. - № 4. – С. 63–69.

Завадский И. И. Информационная война, что это такое? // защита информации.Конфидент. №4, 1996.

Зиновьев А. Русский експеремент. – Москва.: Наш дом, 1995.

Караулов О. Н. Захист комп'ютерної інформації з точки зору міжнародного права / О.Н. Караулов, Г.С. Смушков // Вісник Української академії державного управління при Президентові України. – 2014. – №11. –С. 53–63.

Колин К. К. Половинчатая стратегия: критический анализ глобальных целей ООН в области устойчивого развития. Партнерство цивилизаций. 2016. № 1-2. С. 33-41.

Конвенция об обеспечении международной информационной безопасности (концепция). URL: http://www.mid.ru/bdomp/nsosndoc.nsf/ e2f289bea6297f9c325787a0034c255/542df9e13d28e06ec3257925003542c4!OpenDocu ment.

Конвенції про кіберзлочинність від 23 листопада 2001 р. URL: http://zakon2.rada.gov.ua/laws/show/994_575.

Конституція України від 28.06.1996 // Відомості Верховної Ради України (ВВР), 1996, № 30, ст. 141

Косач П. Д. Інформаційна безпека як основа національної безпеки / П. Д. Косач. – К.: ЗАТ Видавничий дім «ДЕМІЦ», 2002. – 144 с.

Крутрских А.В. Федоров А.В. О международной информационной безопасности / А. В. Крутских, А. В. Федоров // Международная жизнь. – 2000. – № 2. – С. 37–47. 2

Леваков А. В США готовятся к защите информационных систем. URL: http://ww–4.narod.ru/index.html

Лунеев В. В. Криминологические проблемы глобализации / В. В. Лунеев // Государство и право, 2015 – № 1. – С. 45–61.

Макаренко Є.А. Міжнародне співробітництво у сфері інформаційної безпеки: регіональний контекст // Актуальні проблеми міжнародних відносин. – Випуск 102 (Частина І). – 2011.

Національна безпека України: сутність, структура та напрямки реалізації / О. Г. Данільян, О. П. Дзюбань, В. К. Пархоменко, Д. В. Дмитрієв. – Х. : "Фоліо", 2002. – С. 152-167.

Об общих вызовах World Summit on the Information Society (WSIS). URL: http://www.itu.int/net/wsis

Онищенко О. С. Національні інформаційні ресурси як інтегративний чинник вітчизняного соціокультурного середовища : монографія / [О.С. Онищенко, В.М. Горовий, В.І. Попик та ін.] ; НАН України, Національна бібліотека України ім. В.І. Вернадського. – К., 2014.

Пилипчук В. Г. Системні правові проблеми формування інформаційного суспільства : зб. наук. ст. та тез ; наукове повідомлення за матеріалами міжнародної науково-практичної конференції ["Інформаційне суспільство і держава : проблеми взаємодії на сучасному етапі"], (Харків, 26 жовтня 2012 р.). – Х. : НДІ державного будівництва та місцевого самоврядування, 2012. – 214 с.

Правове регулювання інформаційної безпеки у сфері підприємницької діяльності / В. Ніколаєв, Г. Остапович, І. Костицька та ін. – К., 2002. – С. 19 –25

Про інформацію: Закон України від 02.10.1992. URL: http://zakon3. rada.gov.ua/laws/show/2657-12

Про основи національної безпеки України : Закон України від 19.06.03 р. // Відомості Верховної Ради України (ВВР). – 2003. – № 39. – Ст. 351.

Про основні засади розвитку інформаційного суспільства в Україні на 20072015 рр.: Закон України від 09.01.2007 [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/ laws/show/537-16

Про службу безпеки України: Закон України від 25.03.1992. URL: http://zakon4.rada.gov.ua/laws/show/2229-12

Расторгуев С. П. Философия информационной войны. – Москва. Московский психологический институт, 2003, 496 с.

Расторгуев С.П. Философия информационной войны. – Москва. Московский психологический институт, 2003, 496 с.

Систематизація інформаційного законодавства України: Монографія / В. А. Ліпкан, В. А. Залізняк / За заг. ред. В. А. Ліпкана. – К. : ФОП О. С. Ліпкан, 2012. – 304 с.

Смолян Г., Цыгичко В., Черешкин Д. Новости информационной войны.// Защита информации. Конфидент. №6, 996.Сорокін О. Л. Інформаційна безпека та її складові: проблеми визначення концепту / О. Л. Сорокін // Держава та право. – 2014. – №8. – С. 18-22.

Соглашение о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации от 1 июня 2001 г. // Московский журнал международного права. – 2008. – № 4 (72). – С. 244–250.

Стратегія національної безпеки України : Указ Президента України від 26.05.15 р. № 287/2015. URL: //www.president.gov.ua

Суббот А. Інформаційна безпека суспільства / А. Суббот // Віче. – 2015. - № 8. – С. 29-31.

Тоффлер Э., Тоффлер Х. Революционное богатство. Москва : АСТ, 2008. 569 с.

Тугай М. М. Проблеми боротьби з комп'ютерними злочинами в Україні / М.М. Тугай, І.В. Соркін // Закон і бізнес. – 2014. – №7. – С. 22–25.

Шубіна О. В. Державна інформаційна безпека: проблеми визначення концепту / О.В. Шубіна // Держава та права. – 2014. – №3. – С. 26-31.

Denning D.E. Information warfare and security. - New York, 1999; Clarke R.A. Cyber war. The next threat to national security and what to do about it. - New York, 2010; Libicki M.C. Conquest in cyberspace. National security and information warfare. — New York, 2007

European Commission. (2017). EU – U.S. Privacy Shield – First annual Joint Review. Retrieved April 1, 2018. URL: https://www.huntonprivacyblog.com/wpcontent/uploads/sites/28/2017/12/WP-29-Privacy-Shield-Opinion.pdf

Khanna P. Connectography. Mapping the Global Network Revolution. - New York, 2016

Report on World Internet Development 2016 of World Internet Conference «Innovation-driven Internet Development for the Benefit of All – Building a Community of Common Future in Cyberspace». URL: http://www.wuzhenwic.org/2016-11/18/c_61834.htm

REFERENCES

Barovs`ka, A. (2014). Instytucijne zabezpechennja derzhavnoji komunikatyvnoji polityky : dosvid krajin Jevropy : analitychna dopovidj. Retrieved from http: //www.niss.gov.ua /articles/1730

Binjko, I. (1996). Nacionaljna bezpeka Ukrajiny v umovakh ghlobaljnoji informatyzaciji. K.: Nacionaljnyj in–t strateghichnykh doslidzhenj,

Burych, K., Jefymenko, I. & Koghan, B. (2014). Informacijna bezpeka Ukrajiny u suchasnomu kiberprostori. Nacionaljna bezpeka i oborona. 10, 21–27.

Denning, D. E. (1999). Information warfare and security. New York,

Clarke, R. A. (2010). Cyber war. The next threat to national security and what to do about it. New York.

Libicki, M. C. (2007). Conquest in cyberspace. National security and information warfare. New York.

Doktryna informacijnoji bezpeky Ukrajiny vid 25 ljutogho 2017 roku. Retrieved from http://disarmament.un.org/DDApublications/index.html.

Dolzhenko, K. I. (2014). Normatyvno-pravove reghuljuvannja informacijnoji bezpeky reghionu. Pravo i Bezpeka. 3, 43-48.

Dostyzhenyja v sfere ynformatyzacyy y telekommunykacyj v kontekste mezhdunarodnoj bezopasnosty. Doklad Gheneraljnogho sekretarja OOH. A/71/172, 19 yjulja 2016 gh. Retrieved from http://undocs.org/ru/A/71/172.

Dovghanj, O. D. (2013). Orghanizacija pravovogho gharantuvannja bezpeky informacijnykh obminiv u konteksti ghlobalizaciji. Pravova informatyka. 4(40),79-88.

Dubov, D.(2010). Pidkhody do formuvannja tezaurusu u sferi kiberbezpeky. Politychnyj menedzhment. 5, 19–30.

European Commission. (2017). EU – U.S. Privacy Shield – First annual Joint Review. Retrieved from https://www.huntonprivacyblog.com/wpcontent/uploads/ sites/28/2017/12/WP-29-Privacy-Shield-Opinion.pdf

Ghlobaljnyj indeks kiberbezpeky. (2018). Retrieved from https://www.itu.int/en/ITU-D/Cybersecurity/Documents/draft-18-00706_Global-Cybersecurity-Index-EV5_print_2.pdf

Ghorbulin, V. P. (2008) Aktualjni problemy systemnogho zabezpechennja informacijnoji bezpeky Ukrajiny. Materialy mizhar. nauk.-prakt. konf. «Formy ta metody zabezpechennja informacijnoji bezpeky derzhavy». K.: Nac. Akad. SB Ukrajiny.

Ghorovyj V. M. (2017). Pravovi perspektyvy nacionaljnogho rozvytku. Retrieved from http://uaforeignaffairs.com/ua/ekspertna-dumka/view/article/nablizhajuchi-derzhavu-do-suspilstva/#st hash.AgJjKJa4.dpuf

Ghrynjaev S. N. (2018). Ynformacyonnaja vojna: ystoryja, denj seghodnjashnyj y perspektyva. Retrieved from http://ww–4.narod.ru/warfare/grinyaev /page009.htm

Ghurovsjkyj, V. O. (2014). Rolj orghaniv derzhavnoji vlady u sferi zabezpechennja informacijnoji bezpeky Ukrajiny. Visnyk Ukrajinsjkoji akademiji derzhavnogho upravlinnja pry Prezydentovi Ukrajiny. 3, 21–31.

Karaulov, O. N. & Smushkov, Gh. S. (2014). Zakhyst komp'juternoji informaciji z tochky zoru mizhnarodnogho prava. Visnyk Ukrajinsjkoji akademiji derzhavnogho upravlinnja pry Prezydentovi Ukrajiny. 11,53–63.
Khanna, P. (2016). Connectography. Mapping the Global Network Revolution. New York.
Kolyn, K. K. (2016). Polovynchataja strateghyja: krytycheskyj analyz ghlobaljnыkh celej OON v oblasty ustojchyvogho razvytyja. Partnerstvo cyvylyzacyj. 1-2, 33-41.
Konstytucija Ukrajiny vid 28.06.1996.Vidomosti Verkhovnoji Rady Ukrajiny (VVR), 1996, 30, st. 141
Konvenciji pro kiberzlochynnistj vid 23 lystopada 2001 r. Retrieved from http://zakon2.rada.gov.ua/laws/show/994_575.
Konvencyja ob obespechenyy mezhdunarodnoj ynformacyonnoj bezopasnosty (koncepcyja) Retrieved from http://www.mid.ru/bdomp/nsosndoc.nsf/ e2f289bea6297f9c325787a0034c255/542df9e13d28e06ec3257925003542c4!OpenDocument.
Kosach, P. D. (2002). Informacijna bezpeka jak osnova nacionaljnoji bezpeky. K.: ZAT Vydavnychyj dim «DEMShh».
Krutrskykh, A. V. & Fedorov. A. V. (2002). O mezhdunarodnoj ynformacyonnoj bezopasnosty. Mezhdunarodnaja zhyznj. 2, 37–47.
Levakov, A. V SShA ghotovjatsja k zashhyte ynformacyonnыkh system Retrieved from http://ww–4.narod.ru/index.html
Luneev, V. V. (2015). Krymynologhycheskye problemы ghlobalyzacyy. Ghosudarstvo y pravo. 1, 45–61.
Makarenko, Je. A. (2011). Mizhnarodne spivrobitnyctvo u sferi informacijnoji bezpeky: reghionaljnyj kontekst. Aktualjni problemy mizhnarodnykh vidnosyn. 102 (I).
Ob obshhykh vyzovakh World Summit on the Information Society (WSIS). Retrieved from http://www.itu.int/net/wsis
Onyshhenko, O. S. (2014). Nacionaljni informacijni resursy jak integhratyvnyj chynnyk vitchyznjanogho sociokuljturnogho seredovyshha. NAN Ukrajiny, Nacionaljna biblioteka Ukrajiny im. V.I. Vernadsjkogho. Kyiv.
Nikolajev, V. et al. (2002). Pravove reghuljuvannja informacijnoji bezpeky u sferi pidpryjemnycjkoji dijaljnosti. Kyiv.
Pro informaciju: Zakon Ukrajiny vid 02.10.1992. Retrieved from http://zakon3. rada.gov.ua/laws/show/2657-12
Pro osnovni zasady rozvytku informacijnogho suspiljstva v Ukrajini na 2007-2015. Zakon Ukrajiny vid 09.01.2007 Retrieved from http://zakon3.rada.gov.ua/ laws/show/537-16
Pro osnovy nacionaljnoji bezpeky Ukrajiny : Zakon Ukrajiny vid 19.06.03 r. // Vidomosti Verkhovnoji Rady Ukrajiny (VVR). – 2003. – # 39. – St. 351.
Pro sluzhbu bezpeky Ukrajiny: Zakon Ukrajiny vid 25.03.1992 Retrieved from http://zakon4.rada.gov.ua/laws/show/2229-12
Pylypchuk, V. Gh. (2012). Systemni pravovi problemy formuvannja informacijnogho suspiljstva : zb. nauk. st. ta tez ; naukove povidomlennja za materialamy mizhnarodnoji naukovo-praktychnoji konferenciji “Informacijne suspiljstvo i derzhava : problemy vzajemodiji na suchasnomu etapi”, (Kharkiv, 26 zhovtnja 2012 r.). Kh. : NDI derzhavnogho budivnyctva ta miscevogho samovrjaduvannja,
Rastorghuev, S. P. (2003). Fylosofyja ynformacyonnoj vojny. – Moskva. Moskovskyj psykhologhycheskyj instytut.
Report on World Internet Development. (2016). World Internet Conference «Innovation-driven Internet Development for the Benefit of All – Building a Community of Common Future in Cyberspace» Retrieved from http://www.wuzhenwic.org/2016-11/18/c_61834.htm
Shubina, O. V. (2014). Derzhavna informacijna bezpeka: problemy vyznachennja konceptu. Derzhava ta prava.3, 26-31.
Smoljan, Gh., Cyghychko, V., & Chereshkyn D. (2014). Novosty ynformacyonnoj vojny. Zashhyta ynformacyy.
Sorokin, O. L. (2014). Informacijna bezpeka ta jiji skladovi: problemy vyznachennja konceptu. Derzhava ta pravo. 8, 18-22.
Soghlashenye o sotrudnychestve ghosudarstv-uchastnykov Sodruzhestva Nezavysymыkh Ghosudarstv v borjbe s prestuplenyjamy v sfere kompjjuternoj ynformacyy ot 1 yjunja 2001 gh. // Moskovskyj zhurnal mezhdunarodnogho prava. – 2008. – # 4 (72). – S. 244–250.
Strateghija nacionaljnoji bezpeky Ukrajiny : Ukaz Prezydenta Ukrajiny vid 26.05.15 r. # 287/2015. Retrieved from http: // www.president.gov.ua
Subbot, A. (2015). Informacijna bezpeka suspiljstva. Viche. 8, 29-31.
Lipkan, V., & Zaliznjak, V. (2012). Systematyzacija informacijnogho zakonodavstva Ukrajiny. K. : FOP.
Toffler, Kh. (2008). Revoljucyonnoe baghatstvo. Moskva : ACT.
Tughaj, M. M. & I.V. Sorkin, I. V. (2014). Problemy borotjby z komp'juternymy zlochynamy v Ukrajini. Zakon i biznes. 7,22–25.
Zabara, I. M. (2012). Mizhnarodna informacijna bezpeka v mizhnarodnomu pravi: do pytannja vyznachennja. Ukrajinsjkyj chasopys mizhnarodnogho prava. 4,63–69.
Zavadskyj, Y. Y. (1996). Ynformacyonnaja vojna, chto эto takoe? Zashhyta informacyy. 4.
Zynovj'ev, A. (1995). Russkyj eksperement. Moskva.: Nash dom.

Stychynska Anna
Ph.D., https://orcid.org/0000-0002-0519-4305, by_stycha@ukr.net

Стаття надійшла / Article arrived: 17.05.21 Схвалено до друку / Accepted: 29.06.21