УДК 141.7:316.774

І. М. Сопілко,
доктор юридичних наук, професор

СТАНОВЛЕННЯ МЕРЕЖЕВОГО СУСПІЛЬСТВА ТА ПИТАННЯ КІБЕРБЕЗПЕКИ

У статті досліджуються передумови інформаційно-правової концепції мережевого суспільства, визначаються основні її елементи та основні інформаційні загрози, що існують в інформаційному суспільстві. Авторка деталізує елементи та тенденції розвитку мережевого суспільства.

Виходячи з розуміння, що концепція інформаційного суспільства виражає ідею нової фази в історичному розвиткові передових країн, обґрунтовано, що на сучасному етапі його формування одним із елементів такого суспільства є мережеве суспільство.

***Ключові слова**: мережеве суспільство, інформаційне суспільство, інформаційно-правова концепція, державна інформаційна політика, інформаційне право, інформаційна безпека, систематизація інформаційного законодавства.*

И. Н. Сопилко

Становление сетевого общества и вопросы кибербезопасности

В статье исследуются предпосылки информационно-правовой концепции сетевого общества, определяются основные ее элементы и основные информационные угрозы, существующие в информационном обществе. Автор детализирует элементы и тенденции развития сетевого общества.

Исходя из того, что концепция информационного общества выражает идею новой фазы в историческом развитии передовых стран, обосновано, что на современном этапе его формирования одним из элементов такого общества является сетевое общество.

***Ключевые слова**: сетевое общество, информационное общество, информационно-правовая концепция, государственная информационная политика, информационное право, информационная безопасность, систематизация информационного законодательства.*

I. Sopilko

Formation of the network society and the issues of cybersecurity

The article deals with the preconditions of the information and legal concepts of the network society, with its basic elements and basic information threats that exist in the information society. The author details the elements and trends in the network society.

Based on the understanding that the concept of the information society expresses the idea of a new phase in the historical development of the advanced countries, it proved that at the present stage of forming an element of a society is the network society.

***Key words**: network society, information society, information and legal concept, the state information policy, information law, information security, systematization of information legislation.*

Постановка проблеми та її актуальність. Сьогодні ми спостерігаємо активізацію наукових досліджень, які пов'язані із інформацією, інформаційним суспільством та інформаційними відносинами. Актуалізація подібних досліджень напряму пов'язана від тих суспільних, політичних, інформаційних та економічних подій, що відбуваються в Україні. Крім того, так звані інформаційні загрози сучасної України, що випливають із військових подій на Сході України, мають важливий вплив на процеси, що проходять в Україні. Паралельно, існують загрози територіальній цілісності та безпеці України, а інформаційна безпека є однією із суттєвих складових частин національної безпеки країни. Відповідно, проведення державою та громадянським

суспільством вдалої інформаційної політики може суттєво вплинути на розв'язання внутрішньополітичних, зовнішньополітичних та військових конфліктів та наблизити Україну до світових стандартів в питаннях інформаційної безпеки і в цілому безпеки країни. Основним простором для інформації є розвинуте інформаційне суспільство, одним із елементів якого є мережеве суспільство. Інформаційне суспільство забезпечує залучення великої кількості людей до інформаційних ресурсів, сприяє покращенню обміну інформацією між різними суб'єктами інформаційних правовідносин, пришвидшує розвиток інформаційних відносин. Загалом, формування інформаційного суспільства – це тривала діяльність відповідних суб'єктів, як в аспекті проведення організаційних заходів, так і в питанні формування інформаційно-правового законодавства в зазначеній сфері.

Мета даної статті – визначити основні загрози мережевого суспільства в контексті забезпечення інформаційної безпеки держави.

Аналіз досліджень і публікацій. В українській науковій літературі, передусім з інформаціологічної тематики, зазначена тема майже не порушується. Розглядаються різноманітні аспекти інституціоналізації інформаційного права (А. Марущак і його учні), структуризації інформаційного законодавства й інформаційної безпеки (М. Швець, В. Ліпкан, Р. Калюжний та їх учні), різноманітні проекти інформаційного Кодексу (В. Брижко, К. Бєляков, В. Цимбалюк, В. Гавловський та їх учні), аналізуються напрями державної інформаційної політики (І. Арістова та її учні), проте наявність даних напрацювань не вичерпало всіх можливостей для дослідження концепції мережевого суспільства у її співвідношенні з концепцією інформаційного суспільства.

Виклад основного матеріалу. Нинішня глобалізація виступає чи не найнеоднозначнішим виявом сучасної дійсності. З одного боку, чимало дослідників описують позитивні моменти як формування інформаційного суспільства, так і необхідності розроблення інформаційного права як загального регулятора інформаційних правовідносин [1–3]; з іншого – дослідники зосереджують увагу на забезпеченні інформаційної безпеки, реалізації окремих положень державної інформаційної політики [4; 5; 6]. Разом із тим автори дещо на свій лад трактують інформаційне суспільство, виходячи з постульованих в інформаціологічній парадигмі положень. Передусім, це стосується розуміння інформації та її значення в суспільному житті.

Онтологічно концепція інформаційного суспільства не носить парадигмального характеру і сприймається нами лише як висхідне, базове положення для формування нового сітьового світогляду.

Гносеологічно концепція інформаційного суспільства допомагає операціоналізувати методологію його формування та розвитку, застосувати її з відповідним додаванням адекватного методологічного інструментарію до формування сітьового суспільства з урахуванням сучасних тенденцій як в інформаційних відносинах, так і щодо міждисциплінаризації наук.

Аксіологічно концепція інформаційного суспільства виступає цінністю, що розширила розуміння значення інформації, дозволила сформулювати висхідні положення до розуміння її визначального місця в сучасній світобудові та формуванні сітьового універсуму.

«Інформаційне суспільство» виражає ідею нової фази в історичному розвиткові передових країн. Тобто, не прихід «постіндустріального» суспільства, а створення нового соціального зразка, що є результатом «другої індустріальної революції», яка в основному грунтується на мікроелектронній технології. Зростаюча кількість людей з необхідністю втягується в безпрецедентне розмаїття інформаційно орієнтованих типів робіт. Наукові й технічні працівники збирають і продукують інформацію, менеджери й фахівці опрацьовують її, викладачі й працівники комунікаційної сфери поширюють її. Цей процес «інформатизації» не залишає недоторканою жодну сферу соціальної активності: від повсякденного життя до міжнародних відносин та від сфер дозвілля до виробничих відносин [7, с. 362].

Інформаційне суспільство можна визначити як «орієнтоване на інтереси людей, відкрите для всіх і спрямоване на формування інноваційної моделі розвитку високотехнологічне суспільство, в якому кожен громадянин має можливість створювати і накопичувати інформацію та знан-

ня, мати до них вільний доступ, користуватися та обмінюватися ними, щоб дати змогу кожній людині повною мірою реалізувати свій потенціал для забезпечення особистого і суспільного розвитку та підвищення якості життя» [8].

Усвідомлюючи глибокі протиріччя і загрози в розвитку інформаційного суспільства, мислителі стали активно здійснювати дослідження інших вимірів нового соціального порядку. Наслідком такого пошуку стало формування на рубежі століть концепції суспільства знань [9, с. 32]. Таке суспільство заклало основи для формування нового еволюційного типу суспільства – мережевого суспільства, яке, в свою чергу, є водночас і соціальною структурою, що характеризує інформаційну епоху розвитку суспільства та відповідними комунікаціями.

Мережеве суспільство – це суспільство вище за інформаційне, оскільки, крім усіх ознак інформаційного, його вирізняє кластеризація групи користувачів за певними критеріями, і отримання на їх підставі певних не тільки інформаційних, а й економічних, політичних, культурних та інших переваг.

В межах цього суспільства набуває широкої популярності мережева комунікація, що виражається, в тому числі, у помітному зростанні числа соціальних Інтернет-мереж. Ці мережі виступають інструментом, за допомогою якого велика кількість користувачів глобальної мережі отримують додаткові можливості у спілкуванні. Прикладом значимості мережевого суспільства є період Революції гідності, організація якої була завдяки соціальним Інтернет-мережам, інші соціальні та волонтерські акції. Підґрунтям формування мережевого суспільства стало розроблення у кіберпросторі соціальних мереж: мереж, які за допомогою запропонованих алгоритмів визначають спільні інтереси, здійснюють пошук і фактично формують замкнений і цікавий світ для конкретної людини: починаючи від її інтересів у книжках, закінчуючи привілеями щодо спілкування з тими чи іншими особами за фаховими й іншими ознаками. У рамках цих мереж людина отримує нове реальне життя з реальними привілеями та перевагами перед іншими – не членами конкретної мережі.

Схильність людей до більш відкритого спілкування саме у віртуальному просторі використана програмістами, внаслідок чого за допомогою різноманітних скриптів, фішінгових та інших програм можна скласти психологічний та інтелектуальний портрет конкретної людини за лічені секунди. Привабливість таких мереж пояснюється також тим, що заздалегідь закладені похибки у пошукові механізми мереж складають нове відкриття для людей, які здебільшого це сприймають як свій власний вибір і фактично починають думати й обирати за розробленим у рамках мережі алгоритмом. Маніпулювання свідомістю та фактичний вплив на неї в таких мережах має опосередкований характер, оскільки самі події не сприймаються і не є спочатку наслідком суворо детермінованих причин, але справляють відчутний ефект: адже людина, яка має проблеми в реальному житті із спілкуванням, у віртуальному світі через соціальні мережі та різноманітні програми пошуку контактів фактично набуває нового життя.

Недостатність на даному етапі статистичного матеріалу, а також великий масив імовірнісних рішень дають змогу висувати наукові гіпотези. Але з часом наші положення набудуть більшої, передусім наукової, аргументації через їх верифікативність на практиці.

Ключовим моментом будови соціальних мереж виступає те, що в них потрібно аналізувати не зв’язки між вузлами мережі, а властивості відносин між учасниками мережі. Застосування банальних методів інформаційного моделювання, зокрема метода графів, не дають змоги проаналізувати різнорідні та почасти різнокласові вибірки вузлів, що пов’язані різними типами зв’язків.

Характерною ознакою соціальної мережі є не тільки джерела відомостей, а й знання методів, які можуть досліджувати ці невідомості. У реальних соціальних мережах невизначеність інформації є іманентною, чим саме і пояснюється необхідність застосування положень синергетики до вивчення мережевих суспільств. Одним із методів, які можна застосувати для вивчення невизначеностей, є байесовські імовірнісні мережі, які використовуються в умовах невизначеності, коли сутність набутого знання полягає

в розумінні того, чи впливає отримана інформація на наші очікування відносно інших подій.

Концепція мережевого суспільства є важливою для розуміння джерел і витоків формування державної інформаційної політики. Термін «мережеве суспільство» описує сучасні тенденції щодо викликів базовим концептам теорії інформаційного суспільства, концептам інтеракції та солідарності людей, пов'язані з десоціалізацією особи, кластерізацією суспільства на певні групи. Визначальним чинником даного процесу виступають інформаційні чинники, які урешті-решт надають певні переваги конкретній групі серед інших і більше можливостей учасникам цієї групи реалізовувати власні інтереси. Яскравим прикладом цього можуть бути терористичні організації. Адже терористи утворюють власні соціальні мережі і нагальність підготовки мережевих фахівців виступає кричущою потребою, оскільки терористичні мережі, які нині функціонують в Інтернеті, носять завуальований конспіративний характер, а їх виявлення співробітниками правоохоронних органів, які не володіють спеціальним, передусім методологічним інструментарієм, відповідними знаннями й інформаційними технологіями, стає дедалі складнішим.

Наша позиція зумовлена не стільки намаганням викласти не схожу на інших наукову позицію, скільки прагненням застосувати адекватну сучасним реаліям методологію й отримати нові науково значущі результати. Мережеве суспільство має стати об'єктом окремого наукового розгляду, а формування та вивчення закономірностей його побудови дозволить обрати правильну й ефективну методологію щодо його дослідження та управління з метою досягнення всезагального блага.

Мережеве суспільство несе в собі чимало загроз для держави, тому знання методології побудови, базових концептів та аксіоматичних імовірностей виявлення деструктивних зв'язків стане запорукою в реалізації державної інформації політики у XXI ст.

Отже, ми погоджуємось із думкою вчених, що мережеве суспільство виникло як глобальна система, знайшовши вираз у новому вимірі глобалізації нашого часу. Однак, у той час як все і всі на нашій планеті відчувають вплив цієї нової соціальної структури, глобальні мережі об'єднують деяких людей та території, одночасно виключаючи інших, що сприяє появі географії соціальної, економічної та технологічної нерівності [10].

Правова регламентація розвитку єдиного інформаційного простору в умовах розвитку мережевого суспільства повинна сприяти гармонічному розвитку інформаційних ресурсів, інформаційних послуг та засобів інформаційного виробництва в країні у процесі її руху до інформаційного суспільства та усунення інформаційних загроз.

Безумовно, тематика мережевого суспільства впливає на питання інформаційної безпеки та інформаційних загроз. Сучасний світ, як і Україна, з розвитком інформаційних технологій вступили в еру інформаційних загроз, кібератак та, відповідно, інформаційних воєн. Окремі інформаційні війни можуть бути значно результативніші, чим звичайні наземні із використанням людей, території і зброї, так як несуть ураження на невизначені території шляхом використання інформаційних можливостей.

Так, на думку І. В. Діордіца, в сучасних умовах зростає загроза використання проти інтересів України кібернетичних засобів як зсередини держави, так і з-за меж її кордонів. Також як загрози в сфері кібернетичної безпеки можна виділити: кіберзлочинність, кібертероризм та кібершпигунство, кібервійна, а самі інформаційні інтервенції і можуть бути складовими перерахованих дій. Злочини із використанням сучасних інформаційно-телекомунікаційних технологій стають все звичнішою практикою в житті українських громадян. Найбільша увага злочинців зосереджена на спробах порушення роботи або несанкціонованого використання можливостей інформаційних систем державного, кредитно-банківського, комунального, оборонного, виробничого секторів [11].

Сьогодні однозначно можна констатувати, що українські парламентарії та урядовці повинні усвідомлювати необхідність розвитку кібернетичних стратегій, що повинні відігравати ключову роль у захисті комп'ютерних систем. Треба розуміти той факт, що тепер ураження комп'ютерних систем вірусними технологіями можна очікувати не тільки від країн із сильним

військовим потенціалом, а також від менших країн, що поставлять собі за мету активно розвивати кібернетичні системи. Усі ці загрози сьогодні стали не лише предметом наукових дискусій, але й елементом нашого інформаційного простору. Так, наприклад, у грудні проти українських компаній – постачальників електроенергії було скоєно низку кібератак, які були спрямовані на виведення підприємств з ладу. Як повідомляє Reutes, мова йде про Прикарпаттяобленерго та ще кілька компаній. «Хоча Прикарпаття-обленерго була єдиною українською компанією з постачання електроенергії, яка заявила про збої в роботі, подібні шкідливі програми були виявлені в мережах ще як мінімум двох інших підприємств», – розповів Роберт Ліповський, старший дослідник шкідливого програмного забезпечення компанії ESET, яка обслуговувала українські підприємства.

Разом з тим, за даними експертів комп'ютерної безпеки з Trend Micro і iSight Partners, атака на Прикарпаттяобленерго може стати першим випадком, коли за допомогою кібератаки вдалося припинити електропостачання. «Вперше ми маємо доказ і можемо пов'язати шкідливу програму і конкретний збій у роботі системи», – підкреслив дослідник Trend Micro Кайл Вілойт. Відзначається також, що хакери отримали доступ до мереж і встановили програму KillDisk, здатну видаляти і перезаписувати файли [12].

Проблема невдалої української інформаційної політики полягає в тому, що органи державної влади самовідсторонилися від активної політики як на національному, так і на міжнародному інформаційному полі, нехтуючи навіть участю у тих поважних міжнародних структурах, де їх участь передбачена відповідними угодами, зокрема – ООН, ЮНЕСКО. Особливої загрози такі недосконалі дії посадових осіб несуть у час коли в Україні існують реальні загрози територіальної цілісності і безпеки країни. Про якість роботи міністерства інформації в цей складний історичний період, було неодноразовано заявлено як на рівні національних, так і на рівні міжнародних інституцій та фахівців. Так, наприклад, посол США в Україні Джефрі Пайєт заявив, що «є великою помилкою для української влади, для українських людей, створити фабрику тролів як Санкт-Петербург, фабрикуючи контрпропаганду в соціальних медіа. Це величезна помилка створити «Міністерство правди», яке намагається створити альтернативні історії. Це не шлях до перемоги на цьому інформаційному полі бою» [15].

Реалізація національних інтересів щодо забезпечення національної безпеки є одним з найважливіших напрямів цієї трансформації. Так, в тексті «Доктрини інформаційної безпеки України», яку було прийнято від 28 квітня 2014 року сказано, що за умов швидкого формування і розвитку інформаційного суспільства в Україні та глобального інформаційного простору, широкого використання інформаційно-комунікаційних технологій у всіх сферах життя особливого значення набувають проблеми інформаційної безпеки [14], що свідчить про актуальність тематики нашого дослідження як в Україні так і в світі.

Так, наприклад в травні 2015 року стало відомо про хакерську атаку на комп'ютерну мережу німецького парламенту. Атака тривала впродовж кількох днів. Лише в 2016 році було з'ясовано джерело атаки і заявлено, що кібератаки на парламент Німеччини в 2015 році організували саме російські спецслужби. Напад вимкнув мережу на кілька днів і загрожував знищенню великій кількості даних німецького уряду. Не названий виданням Der Spiegel високопосадовець німецьких служб безпеки відзначив, що Берлін вважає: напад «очевидно» пов'язаний із «російською військовою розвідкою» [13].

Даний факт свідчить про новий рівень інформаційний загроз, які в стані паралізувати великі території держави та завдати значного збитку економіці через використання відповідних інформаційних мереж. Відповідні дії хакерів потребують належного реагування зі сторони держави шляхом вдосконалення системи захисту програмного забезпечення та унеможливлення відповідних загроз.

Але, на жаль, як ця доктрина, так і ряд інших програм на державному рівні не відповідають сучасним умовам та є неадекватними з позиції відповіді на існуючі загрози. В лютому 2016 року, критикуючи діяльність української влади

в питаннях захисту інформаційного простору від інформаційних загроз і адекватності реакції держави, посол США в Україні Джеффрі Пайєтт вважає, що найбільшою помилкою з боку України буде витрачати весь час та енергію на спростування брехні … . Є феномен у психології, на його думку, який називається віддзеркалювання, коли ви звикаєте просто відображати поведінку вашого опонента. Це не шлях до перемоги на цьому інформаційному полі бою [15].

Висновки. Тому, з метою попередження зловживання інформацією та для захисту інформаційних прав, сучасний стан забезпечення національної та інформаційної безпеки України потребує розробки науково обґрунтованої державної політики та стратегії в цій галузі, визначення системи національних цінностей, життєво важливих інтересів особистості, суспільства та держави, визначення зовнішніх і внутрішніх загроз цим інтересам, пошуку ефективних заходів для забезпечення безпеки в усіх її сферах, захисту від інформаційних загроз та реалізації права на отримання достовірної інформації. Паралельно, усе вищевикладене свідчить про потребу прийняття нормативно-правових актів, у яких був би передбачений механізм захисту інформаційних прав громадян від протиправних дій третіх осіб щодо інформації та обмеження її впливу на особу у зв'язку із використанням відповідних інформаційних мереж. Особливої актуальності заслуговує питання вдосконалення програмного забезпечення діяльності основних державних інституцій, організацій та підприємств. Крім того, потребує вдосконалення система протидії інформаційним атакам із використанням соціальних мереж. До діяльності щодо протидії інформаційним загрозам слід долучитись громадянському суспільству із креативними підходами до розв'язання цієї проблеми, а також відповідним міжнародним інформаційним організаціям, які виступають за чесні правила в журналістиці.

Література

1. *Бєляков К. І.* Інформаційне право: аналіз термінологічно-понятійного апарату / К. І. Бєляков // Науковий вісник Київського національного університету внутрішніх справ. – 2007. – Вип. 3. – С. 67-79.

2. *Бєляков К. І.* «Інформаційна» аксіоматика у праві: проблеми формування / К. І. Бєляков // Науковий вісник Юридичної академії МВС України. – 2004. – № 3. – С. 263-268.

3. *Гурковський В. І.* Державне управління розбудовою інформаційного суспільства в Україні (історія, теорія, практика) / В. І. Гурковський. – К.: Наукова думка, 2010. – 396 с.

4. *Арістова І. В.* Державна інформаційна політика: організаційно-правові аспекти / за ред. О. М. Бандурки. – Х.: Вид-во Ун-ту внутр. справ, 2000. – 368 с.

5. *Баскаков В. Ю.* Захист інформації з обмеженим доступом в умовах боротьби з організованою злочинністю / В. Ю. Баскаков // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2011. – № 24. – С. 263–269.

6. *Ліпкан В. А.* Інформаційна безпека України в умовах євроінтеграції / В. А. Ліпкан, Ю. Є. Максименко, В. М. Желіховський. – К.: КНТ, 2006. – 280 с.

7. *Лайон Д.* Інформаційне суспільство: проблеми та ілюзії. Інформація, ідеологія та утопія / Д. Лайон // Сучасна зарубіжна соціальна філософія. – К., 1996. – С. 362-380.

8. *Про схвалення* Концепції розвитку електронного урядування в Україні: Розпорядження Кабінету Міністрів України від 13 грудня 2010 р. № 2250-р. [Електронний ресурс]. – Режим доступу: http://zakon2.rada. gov.ua/laws/ show/ 2250-2010-%D1%80.

9. *Наумкина Е. А.* Информационное общество и модернизация образования / Е. А. Наумкина / Наука и образование: современные трансформации: монография / Ин-т философии им. Г. С. Сковороды НАН Украины. – К.: ПАРАПАН, 2008. – С. 267-280.

10. *Передмова* до видання 2010 року книги Мануеля Кастельса «Підйом мережевого суспільства» («The Rise of the Network Society») [Електронний ресурс]. – Режим доступу: http://champtheplanet.blogspot.com/ 2012/11/2010-rise-of-network-society.html

11. *Діордіца І. В.* Інформаційні інтервенції як загроза кібернетичній безпеці [Електронний ресурс]. – Режим доступу: http://goal-int.org/

informacijni-intervencii-yak-zagroza-kibernetichnij-bezpeci/.

12. *Reuters* дізналося подробиці кібератаки на українські об'єкти енергетики [Електронний ресурс]. – Режим доступу: http://nv.ua/ukr/ ukraine/ events/reuters-diznalasja-podrobitsi-kiberataki-na-ukrajinski-ob-jekti-energetiki-89667.html.

13. *Кібератаку* на німецький парламент у 2015 році організував уряд Росії – Der Spiegel [Електронний ресурс]. – Режим доступу: http://www.unian.ua/world/ 1250722-kiberataku-na-nimetskiy-parlament-u-2015-rotsi-organizuvav-uryad-rosiji-der-spiegel.html.

14. *Доктрина* інформаційної безпеки України від 28 квітня 2014 року [Електронний ресурс]. – Режим доступу: http://comin.kmu.gov.ua/control/uk/publish/article?art_id=113319&cat_id=61025.

15. *Пайєтт* назвав найбільшу помилку України в боротьбі з російською пропагандою [Електронний ресурс]. – Режим доступу: http://tyzhden.ua/News/ 157332.

References

1. *Beljakov K. I.* Informacijne pravo: analiz terminologichno-ponjatijnogo aparatu / K. I. Beljakov // Naukovij visnik Kiivs'kogo nacional'nogo universitetu vnutrishnih sprav. – 2007. – Vip. 3. – S. 67-79.

2. *Beljakov K. I.* «Informacijna» aksiomatika u pravi: problemi formuvannja / K. I. Beljakov // Naukovij visnik Juridichnoi akademii MVS Ukraini. – 2004. – № 3. – S. 263-268.

3. *Gurkovs'kij V. I.* Derzhavne upravlinnja rozbudovoju informacijnogo suspil'stva v Ukraini (istorija, teorija, praktika) / V. I. Gurkovs'kij. – K.: Naukova dumka, 2010. – 396 s.

4. *Aristova I. V.* Derzhavna informacijna politika: organizacijno-pravovi aspekti / za red. O. M. Bandurki. – H.: Vid-vo Un-tu vnutr. sprav, 2000. – 368 s.

5. *Baskakov V. Ju.* Zahist informacii z obmezhenim dostupom v umovah borot'bi z organizovanoju zlochinnistju / V. Ju. Baskakov // Borot'ba z organizovanoju zlochinnistju i korupcieju (teorija i praktika). – 2011. – № 24. – S. 263–269.

6. *Lipkan V. A.* Informacijna bezpeka Ukraini v umovah evrointegracii / V. A. Lipkan, Ju. Є. Maksimenko, V. M. Zhelihovs'kij. – K.: KNT, 2006. – 280 s.

7. *Lajon D.* Informacijne suspil'stvo: problemi ta iljuzii. Informacija, ideologija ta utopija / D. Lajon // Suchasna zarubizhna social'na filosofija. – K., 1996. – S. 362-380.

8. *Pro shvalennja* Koncepcii rozvitku elektronnogo urjaduvannja v Ukraini: Rozporjadzhennja Kabinetu Ministriv Ukraini vid 13 grudnja 2010 r. № 2250-r. [Elektronnij resurs]. – Rezhim dostupu: http://zakon2.rada.gov.ua/laws/show/ 2250-2010-%D1%80.

9. *Naumkina E. A.* Informacionnoe obshhestvo i modernizacija obrazovanija / E. A. Naumkina / Nauka i obrazovanie: sovremennye transformacii: monografija / In-t filosofii im. G. S. Skovorody NAN Ukrainy. – K.: PARAPAN, 2008. – S. 267-280.

10. *Peredmova* do vidannja 2010 roku knigi Manuelja Kastel'sa «Pidjom merezhevogo suspil'stva» («The Rise of the Network Society») [Elektronnij resurs]. – Rezhim dostupu: http://champtheplanet.blogspot.com/ 2012/11/2010-rise-of-network-society.html

11. *Diordica I. V.* Informacijni intervencii jak zagroza kibernetichnij bezpeci [Elektronnij resurs]. – Rezhim dostupu: http://goal-int.org/informacijni-intervencii-yak-zagroza-kibernetichnij-bezpeci/.

12. *Reuters* diznalosja podrobici kiberataki na ukrains'ki ob'ekti energetiki [Elektronnij resurs]. – Rezhim dostupu: http://nv.ua/ukr/ukraine/events/ reuters-diznalasja-podrobitsi-kiberataki-na-ukrajinski-ob-jekti-energetiki-89667.html.

13. *Kiberataku* na nimec'kij parlament u 2015 roci organizuvav urjad Rosii – Der Spiegel [Elektronnij resurs]. – Rezhim dostupu: http://www.unian.ua/world/ 1250722-kiberataku-na-nimetskiy-parlament-u-2015-rotsi-organizuvav-uryad-rosiji-der-spiegel.html.

14. *Doktrina* informacijnoi bezpeki Ukraini vid 28 kvitnja 2014 roku [Elektronnij resurs]. – Rezhim dostupu: http://comin.kmu.gov.ua/control/uk/publish/ article?art_id =113319&cat_id=61025.

15. *Pajett* nazvav najbil'shu pomilku Ukraini v borot'bi z rosijs'koju propagandoju [Elektronnij resurs]. – Rezhim dostupu: http://tyzhden.ua/News/ 157332.