

Торічний Вадим Олександрович,

к.психол.н., докторант Навчально-науково-виробничого центру,
Національний університет цивільного захисту України,
м. Харків

ORCID 0000-0003-3336-6386

УДК 351:342.57

doi: 10.34213/ap.19.02.04

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ДЕРЖАВИ В КОНТЕКСТІ ВИКОРИСТАННЯ КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ: ДЕРЖАВНО-УПРАВЛІНСЬКИЙ АСПЕКТ

Розглянуто питання інформаційного забезпечення державної політики в контексті використання комп'ютерних технологій. Проаналізовано вплив мережевих комунікацій на систему управління взагалі та державне управління зокрема. Охарактеризовано специфіку інформаційного забезпечення у формуванні державної інформаційної політики, визначено його основні функції, що впливають на безпеку держави. Обґрунтовано положення про те, що в умовах економічного спаду, політичної нестабільності й загострення протиріч між інтересами різних груп населення без розуміння ролі, значення та функцій сучасних засобів комунікації неможливе ефективне управління державою, а також соціально-політичними процесами. Підкреслено, що від розумності й виваженості державної політики в галузі розвитку мережевих комунікацій, а також виробництва інформації та її поширення у глобальному інформаційному просторі значною мірою залежить благополуччя країни та її місце у світовій цивілізації. Доказано, що у цілому перспективи інформаційної безпеки у сфері використання мережевих комунікацій та Інтернет значною мірою залежать від продуманої державної політики у сфері масових комунікацій. Реалізація принципів ліберальної теорії на практиці означає віддання електронних мереж зв'язку на відкуп комерційним структурам, що, на наш погляд, не відповідає повною мірою наявним соціально-політичним потребам сучасного українського суспільства. Тому державна концепція розвитку мережевих комунікацій та Інтернету повинна рівною мірою враховувати як наявний світовий досвід, так і національні особливості розвитку та використання українських комунікаційних систем.

Ключові слова: інформаційне забезпечення, державна політика безпеки, "всесвітня павутина", інформаційні технології.

Постановка проблеми. В умовах глобальної інтеграції та жорсткої геополітичної протидії головною ареною зіткнень і боротьби різновекторних національних інтересів держав стає інформаційний простір. З огляду на це інформаційне забезпечення національної безпеки в сучасних умовах стає вкрай актуальною проблемою.

Як зазначається в офіційних документах України, сучасні інформаційні технології дають змогу державам реалізувати власні інтереси без застосування воєнної сили, послабити або завдати значної шкоди безпеці конкурентної держави, яка не має дієвої системи захисту від негативних інформаційних впливів [1]. Зокрема, в Основах державної політики України наголошується на необхідності забезпечення інформаційної безпеки як однієї з найважливіших функцій держави, тому Концепцією національної безпеки України витік інформації, що становить державну таємницю, визначено як загрозу національній безпеці [2].

Аналіз останніх досліджень і публікацій. В сучасних умовах значно зростає вразливість інформації, у зв'язку з чим розширення міжнародного співробітництва України, упровадження досягнень науки і новітніх технологій, розвиток теле- і мережевих комунікацій інформація стає стратегічним національним ресурсом. У той же час, згідно з доктриною національної безпеки України, інформаційна безпека є невід'ємною складовою кожної з її сфер і виступає важливою самостійною сферою забезпечення національної безпеки.

© Торічний В. О., 2019

Саме тому розвиток України як суверенної, демократичної, правової та економічно стабільної держави можливий тільки за умови забезпечення належного рівня її інформаційної безпеки [3].

Теоретичну основу досліджень у сфері інформаційного забезпечення національної безпеки складають роботи зарубіжних авторів, зокрема Д. Белла М. Кастельса, М. Маклюєна, Е. Тофлера, а також вітчизняних науковців О. Бухтатого, О. Крюкова, О. Логінова, С. Луценка, А. Панарина, Г. Почепцова, В. Степанова, С. Чукут та ін.

Мета статті – вивчення інформаційного забезпечення національної безпеки держави в контексті використання комп'ютерних технологій, в основі яких знаходяться процеси інформаційності й інформатизації, та їх впливу на безпеку держави.

Виклад основного матеріалу. Як зазначає український дослідник О. Логінов, в інформаційному просторі з позиції інформаційної загрози у сфері державного управління найбільш виділяються два види небезпеки: контроль інформаційних ресурсів держави, який здійснюється несанкціонованим проникненням в інформаційні та керуючі системи, та активна участь зарубіжних фірм у створенні інформаційної структури України, у зв'язку з чим інформаційні ресурси країни опиняються під контролем відповідних іноземних структур. Саме тому інформаційні ресурси та інформаційні системи відносяться до числа основних елементів об'єктів безпеки в усіх сферах життєдіяльності держави [4, с. 199–201].

Інформаційне забезпечення безпеки держави, на наш погляд, буде міцним і надійним тільки тоді, коли воно спирається на такі ціннісні підстави, як інформаційна цивілізованість та інформаційна культурність.

Сучасний етап розвитку людської цивілізації свідчить про те, що сформовані параметри інформаційної безпеки, стереотипи і звички в цій сфері значною мірою не відповідають завданням забезпечення національної безпеки. Водночас інформаційне забезпечення безпеки України тісно пов'язане з її включенням в технічне співробітництво у глобальному масштабі.

На нашу думку, концепція національної безпеки України повинна включати в себе і концепцію інформатизації українського суспільства, оскільки загрози безпеці, викликані відсутністю сучасних засобів інформаційного забезпечення в галузі державного управління, економіки, соціальної політики, у багато разів перевищують допустимі витрати на їх інформатизацію.

У зв'язку з цим необхідно розуміти, що можливе оволодіння потенційним противником інформаційними центрами здатне забезпечити миттєву і повну дезорганізацію державного управління і суспільного життя всього суспільства.

Створення єдиної міжнародної інформаційної системи ставить країни-учасниці в залежність від обслуговуючого персоналу інформаційних центрів: інженерів, програмістів, операторів, наділених усіма людськими якостями, в тому числі недобросовісністю й недекатністю. Певну небезпеку становлять і фактори, пов'язані з інформацією складової сучасного суспільства – його надмірною відкритістю.

Зростаючу небезпеку для особистості, суспільства, держави являє також новий вид соціально небезпечних злочинів, заснованих на використанні сучасної інформаційної техніки і технології. Основні види цих злочинів включають у себе махінації з електронними грошима; комп'ютерне хуліганство; розкрадання різноманітної інформації, що зберігається або передається у "безпаперовому" вигляді, незаконне її копіювання та ін.

Бурхливий розвиток спеціальних технічних засобів нового покоління, які здатні впливати на психіку, свідомість людей та інформаційно-технічну інфраструктуру суспільства й системи безпеки держав, досягло такого рівня, що їх характеризують як новий клас зброї – електронна або інформаційна зброя.

Інформаційна зброя включає в себе різні засоби нападу на комп'ютерні мережі, починаючи з електронного шпигунства – до вірусів, здатних руйнувати ключові системи. До неї відносяться програмні засоби (комп'ютерні віруси, програмні закладки та ін.), засоби радіоелектронної боротьби, психотропні генератори та ін.

Застосування й розробка різних видів інформаційної зброї здійснюється все частіше й ширше. Подекуди інформаційний тероризм стає елементом державної політики. За даними ЦРУ США, сьогодні майже 30 країн світу активно працюють над комп'ютерними програмами інформаційної зброї [6]. Причому об'єктами такої зброї все частіше стають окремі особистості, соціальні групи, а не тільки люди і державні структури, як це було не так давно. Іншими словами, вибірковість цієї зброї зростає.

Відмінною рисою такої зброї є її дешевизна і складність виявлення. Система Інтернет, яка пов'язала комп'ютерні мережі всієї планети, змінила правила, що стосуються сучасної зброї. Анонімність, що забезпечується Інтернетом, дозволяє противнику стати невидимим і виявити його дуже складно.

З іншого боку, сучасні військові дії – це вже не тільки вогневе (матеріально-енергетичне), але й інформаційно-технічне протистояння. У військовій справі настає новий, пост'ядерний етап, розгортається нова військово-технічна революція, перехід від зброї масового ураження до високоточної, виборчої контрсилової та інформаційної зброї.

Навіть поверхневий розгляд проблем інформаційної культури та їх впливу на інформаційне забезпечення безпеки держави дозволяють зробити деякі узагальнення в цьому напрямку.

По-перше, фактор інформаційності та інформатизації став настільки всеосяжним, що вимагає тісного практичного сполучення з тим, що вводить його реалізацію в певні рамки – правові, гуманітарні, моральні та демократичні. Без цих рамок, характер яких визначається національно-державними умовами конкретної країни, інформаційність поступово генерує антисоціальні прояви, а, отже, стає джерелом соціальної й особистісної небезпеки.

По-друге, надійне інформаційне забезпечення безпеки держави та особистості вже неможливе без урахування й цілеспрямованого культивування зрілої інформаційної культури на всіх рівнях соціальної організації. Культурний “вимір” усього процесу інформатизації та інформаційного забезпечення безпеки означає, що фактор інформатизації тісно пов'язаний із ціннісно-ментальними основами, іншими результатами освіти та виховання, які визначають і направляють можливості інформатизації в соціально- та особистісно-значущі кордони реалізації.

По-третє, нашу думку, інформаційність – це якісно нова і ще недостатньо освоєна особистістю й суспільством сфера соціальності та соціалізації, яка об'єктивно діє з усіма можливими наслідками.

Для українського суспільства важливо глибоко освоїти цю сферу як джерело соціалізації, дослідити особливості її впливу на особистість і соціальні групи, визначити наслідки цього впливу й постаратися зробити цей вплив керованим і регульованим. В іншому випадку процес інформатизації набуде (і вже багато в чому набув) власну логіку, в якій інтереси суспільства та особистості, їх безпека зовсім не гарантовані.

Проблема дослідження можливостей мережевих засобів масової комунікації особливо актуальна в сучасному світі взагалі та в Україні зокрема. Це обумовлено тим, що в умовах економічного спаду, політичної нестабільності й загострення протиріч між інтересами різних груп населення без розуміння ролі, значення та функцій сучасних засобів комунікації неможливе ефективне управління державою, а також соціально-політичними процесами. Від розумності й виваженості державної політики в галузі розвитку мережевих комунікацій, а також виробництва інформації та її поширення у глобальному інформаційному просторі значною мірою залежить благополуччя країни та її місце у світовій цивілізації.

З одного боку, в сучасних умовах все більшого значення набуває процес створення глобального інформаційного простору. З іншого – зміни, що відбуваються в суспільстві під впливом мережевих засобів масової комунікації, не обмежуються тільки певними перевагами і вигодами, що відкриває найширші можливості для ведення інформаційного протиборства в соціально-політичній сфері. Інформаційний тероризм, поширення нелегальних матеріалів (в тому числі порносайтів – інформації аморальної, що збуджує найнижчі людські почуття), освіта в Мережі неформальних молодіжних об'єднань, деструктивний вплив нових комунікаційних технологій на особистість – це також атрибут існування мережевих засобів масової комунікації.

Сьогодні мережеві засоби масової комунікації являють собою *нову історичну форму забезпечення взаємодії людей*, а Інтернет виступає основою формування єдиного електронного комунікаційного середовища, соціально-політичний сенс якого полягає в можливості створення системи, яка стоїть над національними культурами, цивілізаціями та державами й здатної якісно змінити світ, хоча розширення соціальних функцій системи масової комунікації при цьому не відбувається. Характер і розвиток цього обнадійливого й водночас небезпечного явища залежить від світових соціальних і політичних процесів й, у свою чергу, спричиняє на них певний вплив

Говорячи про *інформаційне забезпечення безпеки*, пов'язане з функціонуванням мережних комунікацій, і, перш за все Інтернету як нової форми комунікації, доцільно відзначити як позитивні, так і негативні їх властивості.

Перше. Електронні мережі забезпечують можливість не лише масової, але й міжособистісної і групової комунікації. В історії засобів комунікації є приклади, коли одна технологія забезпечувала комунікацію всіх трьох рівнів. Достатньо згадати радіо як засіб міжособистісної (діалог по радію), групової (використання певної частоти будь-яким відомством) і масової (традиційні радіостанції) комунікації. Принципова відмінність радіо та Інтернету в нашому контексті полягає в тому, що в першому випадку різні рівні комунікації розділені й не змішуються, тоді як у другому випадку користувач мережі може одночасно виступати як суб'єкт і міжособистісної, і групової, і масової комунікації. Крім того, як підкреслюють фахівці, поява й поширення Інтернету стимулює в сучасному інформаційному суспільстві нові соціокультурні процеси, головними з яких, як видається, є особливі якості спілкування – відкритість, щирість, можливість відходу від традиційного для засобів масової інформації бажання впливати, впливати, виховувати [7].

Друге. Інтернет з його особливими можливостями зворотного зв'язку з приймаючою стороною і навіть стиранням граней між розповсюдженцем і одержувачем інформації може докорінно змінити всі мас-медіа процеси. Відкритість, масовість, інтимність – все це – не протиріччя, а синоніми, що характеризують нову якість спілкування людей. Немає меж, немає простору, немає цензури,

немає обмежень у візуальному самовираженні, повна й абсолютна анонімність, що поєднується з аналогічною відкритістю, можливістю самому обирати джерело інформації й можливість миттєвого відгуку на те, що відбувається.

Нескінченна кількість можливостей пошуку і вибору забезпечує кожному користувачеві Інтернету рівноправне й повноцінне спілкування, за якого досягається взаєморозуміння мотивів і цілей співрозмовників, тобто справжній діалог. У зв'язку з цим можна говорити не лише про соціальну значущість самої мережі Інтернет, а й про соціальну значущість будь-яких двонаправлених варіантів спілкування з прозорістю і щирістю "розмови".

Трете. Сьогодні стає цілком очевидним, що Інтернет може виявитися не лише засобом обміну інформацією, діалогічного спілкування і розваги, а й, як і всі інші ЗМІ, використовуватись як *засіб впливу*. Нині кількість його користувачів в Україні, як і в усьому світі, зростає лавиноподібно. Все більша кількість фірм, підприємств, інститутів, шкіл підключаються до "всесвітньої павутини". Число користувачів "домашнього" Інтернету також постійно зростає (хоча дозволити його можуть далеко не всі – тут домінує матеріальний принцип), охоплюючи чи не найбільш дієздатну частину сучасного суспільства (як правило, від 15 до 35 років).

Сьогодні ми є свідками своєрідної інформаційної війни за свідомість цієї категорії людей, тобто за формування світогляду користувачів Інтернету. Оскільки деякі із сайтів явно спрямовані на дестабілізацію ситуації в суспільстві, то актуалізується необхідність науково вивіреного проектування інформаційного середовища в мережах Інтернет.

З огляду на те, що Інтернет почав формувати соціокультурне середовище далеко за своїми віртуальними межами, впливати на життя навіть тих людей, які ніколи ним не користувалися, постає питання про *інформаційну складову екології сучасної людини у світі комп'ютерних мереж*. Доводиться констатувати, що в нашому суспільстві багато чуток, суперечливих думок з приводу соціально значимої інформації одержується саме з Інтернету.

Звертають на себе увагу і деякі методи використання Інтернету в сучасній політичній боротьбі. Йдеться про оперативне скидання на інтернетівські сайти компромату, як правило, неперевіреного, а часто й помилкового, про його негайне використання іншими засобами масової інформації, які сповідують принцип вихоплення "гарячих фактів". В Інтернет, з його специфікою безіменності сайтів і безвідповідальності за достовірність інформації, неможливо встановити не тільки людину, яка породила інформацію, але навіть місто або країну, звідки ця інформація надійшла. Безсумнівно, що кількість анонімних сайтів в умовах гострої політичної боротьби буде зростати, безсумнівно й те, що безконтрольний "злив" компроматів являє собою певну загрозу соціальної стабільності й вочевидь може становити загрози національній безпеці держави.

З огляду на це видається доцільним ведення інститутами системи державного управління оперативного моніторингу появи сайтів подібного роду, оцінки, прогнозу їх можливих соціально-політичних наслідків, а в деяких випадках – і створення "противаг" у вигляді інших альтернативних сайтів. Свобода слова, яка є одним з основних принципів цієї комп'ютерної мережі, в даному випадку зовсім не порушується.

Четверте. Оскільки специфіка мережі Інтернет забезпечує будь-якому її користувачеві можливість стати комунікатором, який має необмежену аудиторію, а самому при цьому залишатися персоною анонімним, у крайньому випадку – користується псевдонімом, цілком природним є бурхливий сплеск соціальної активності, що знаходить своє відображення у багатьох сайтах.

Очікувати, що люди, які отримали доступ до комунікації, не скористаються можливістю висловитися з принципово значущих для себе і для суспільства проблем і не стануть шукати варіанти самоствердження, було б наївно.

Оскільки свобода слова в мережі – річ непорушна, неважко спрогнозувати, що різні організації та особи будуть продовжувати декларувати тут свої завдання і цілі. У зв'язку з цим виникають природні запитання: чи повинен хтось оцінювати те, що відбувається у віртуальному просторі цієї глобальної мережі, і які повинні бути критерії цієї оцінки? Звісно ж, що таку функцію може й повинна взяти на себе соціальна наука, що орієнтується на позитивні загальнолюдські норми і цінності.

Гласність у наукових підходах змісту й мотиваційної спрямованості сайтів, орієнтованих на дестабілізацію в суспільстві, науковий прогноз можливих соціальних наслідків, використання для такої інформації і друку, і радіо, і телебачення, і Інтернету – єдиний спосіб проектування здорового соціокультурного середовища.

Однак існує й інша сторона цієї проблеми – правова. Останнім часом в Інтернеті з'явилася величезна кількість пропозицій всляких комерційних фірм про продаж найрізноманітніших баз даних, що містять інформацію, яка є власністю державних структур. Цей факт свідчить про те, що інформаційні ресурси держави не захищені належним чином ні в правовому, ні в технічному плані.

У зв'язку з цим повинно бути уточнено поняття власності на інформаційні ресурси та всі механізми забезпечення відповідних прав власності. Необхідно також забезпечити правовий захист конфіденційної інформації, що не містить відомостей, які становлять державну таємницю.

П'яте. Інтернет створює нову мовну характеристику інформації та організації комунікації, що призводить до англосмовної експансії. Сьогодні громадяни України, як і жителі багатьох інших країн світу, стають свідками потужного й динамічного процесу трансформації соціокультурного простору під впливом зразків американської й європейської культури, що все більш активно проникають в наше життя, а також англосмовних запозичень, безпосередньо пов'язаних з цими новими поняттями. Такі слова, як “комп'ютер”, “бізнес”, “менеджмент”, “маркетинг”, “офіс”, “консалтинг” і т. д. вже міцно увійшли в нашу повсякденну мову, побут і свідомість.

Тут є і свої особливості, але виходити потрібно насамперед із реалій дійсності. На сьогоднішній день у світі склався певний детермінізм: США більшою мірою, ніж інші промислові й технологічно просунуті держави, беруть на себе функції центру не лише в галузі економіки, фінансів та підприємництва, а й у галузі культури, науки, освіти, ЗМІ та інформаційних технологій. Відповідно і у сфері форм мовного втілення культурних норм і зразків найбільший вплив належить тим же Сполученим Штатам. Зокрема, найважливіше місце в сучасній культурі глобалізації, в тому числі мовної, відіграє сам Інтернет. Мова цієї нової культури – англо-американська, оскільки більшість фахівців і користувачів Інтернету живуть в англосмовних країнах.

Звідси можна дійти висновку, що сучасна світова культура епохи глобалізації надзвичайно американо-центрична. Отже, в міру того, як освоюються й беруться на озброєння американські нововведення в різних сферах життєдіяльності, поступово змінюються й цінності, настанови, менталітет людей і характер породжуваних в комунікаційних мережах текстів, а нові англосмовні терміни, що використовуються в них, заповнюють смислові конструкції національних мов – носіїв іншомовних культур.

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямку. Таким чином, мережеві засоби масової комунікації та Інтернет є технологічною основою інформаційного суспільства, що формується із промислово розвинених держав світу, де значна частина економічного потенціалу утворюється за рахунок інтенсивного розвитку “електронної” економіки, ефективного використання наявних інтелектуальних ресурсів.

На цьому фоні не досить високим виглядає існуючий в Україні рівень розвитку і використання системи Інтернет. Основною причиною такого становища є, на нашу думку, *невизначеність державної політики України у сфері розвитку системи Інтернет* на території держави, а також невизначеність взаємодії з питань розвитку та використання даної системи з міжнародною спільнотою.

На нашу думку, при формуванні державної політики необхідно враховувати, що закономірності розвитку комп’ютерних мереж та Інтернету носять універсальний характер. Іншими словами, Інтернет в Україні змушений буде пройти ті ж етапи розвитку, що й в цілому у світі, хоча його інституціоналізація в США, Канаді, деяких інших країнах Західної Європи та Азії завершилася раніше, ніж в Україні.

Для того, щоб державна політика України у сфері використання і розвитку мережевих засобів масової комунікації була успішною, необхідно обов’язково враховувати не лише соціальну, економічну, політичну та культурну своєрідність нашої країни, а й особливості вітчизняних мережевих засобів масової комунікації.

У цілому перспективи інформаційної безпеки у сфері використання мережевих комунікацій та Інтернет значною мірою залежать від продуманої державної політики у сфері масових комунікацій. Реалізація принципів ліберальної теорії на практиці означає віддання електронних мереж зв’язку на відкуп комерційним структурам, що, на наш погляд, не відповідає повною мірою наявним соціально-політичним потребам сучасного українського суспільства. Тому державна концепція розвитку мережевих комунікацій та Інтернету повинна рівною мірою враховувати як наявний світовий досвід, так і національні особливості розвитку та використання українських комунікаційних систем. Оптимальним уявляється комбінований підхід, що поєднує в собі комерційний шлях розвитку мережевих засобів масової комунікації з їх контролем і підтримкою з боку держави.

Список використаних джерел

1. Про Доктрину інформаційної безпеки України : Указ Президента України від 08.07.2009 р. № 514/2009. URL: <https://zakon.rada.gov.ua/laws/show/514/2009> (дата звернення: 16.09.2019).
2. Про Концепцію (основи державної політики) національної безпеки України : Постанова Верховної Ради України від 16.01.1997 р. № 3/97-ВР. *Відомості Верховної Ради України*. 1997. № 10. Ст. 85.
3. Про рішення Ради національної безпеки і оборони України від 31 жовтня 2001 року з питання “Про заходи щодо вдосконалення державної інформаційної політики та забезпечення інформаційної безпеки” : Указ Президента України від 06.12.2001 р. № 1193/2001. URL: <https://zakon.rada.gov.ua/laws/show/1193/2001> (дата звернення: 16.09.2019).
4. Логінов О. М. Сучасні проблеми забезпечення інформаційної безпеки в контексті формування системи державного управління. *Науковий вісник Юридичної академії Міністерства внутрішніх справ*. 2003. № 3. С. 199–204.
5. Васильєв Ю. Класифікація та аналіз загроз інформаційної безпеки в ключових системах інформаційної інфраструктури. *Правове, нормативне та методологічне забезпечення системи захисту інформації в Україні*. 2015. Вип. 1 (29). С. 56–61.
6. Низинг Й. Общественная оборона как логическая альтернатива. От утопии к выбору. Москва : Наука, 1993. 273 с.
7. Тофлер Е. Метаморфозы власти. Знание, богатство и сила на пороге XXI века. Москва : ООО “Издательство АСТ”, 2002. 669 с.
8. Домбровська С. М., Удяньський М. М., Домбровський Л. В., Карпеко Н. М. Державне регулювання забезпечення інформаційної безпеки : монографія. Київ : НУЦЗУ, 2019. 279 с.

References

1. Pro Doktrynu informatsiinoi bezpeky Ukrainy: Ukaz Prezydenta Ukrainy vid 08.07.2009 r. № 514/2009. (2009). URL: <https://zakon.rada.gov.ua/laws/show/514/2009>.
2. Pro Kontseptsiu (osnovy derzhavnoi polityky) natsionalnoi bezpeky Ukrainy: Postanova Verkhovnoi Rady Ukrainy vid 16.01.1997 r. № 3/97-VR. (1997). *Vidomosti Verkhovnoi Rady Ukrainy*, 10, art. 85.
3. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 31 zhovtnia 2001 roku z pytannia "Pro zakhody shchodo vdoskonalennia derzhavnoi informatsiinoi polityky ta zabezpechennia informatsiinoi bezpeky": Ukaz Prezydenta Ukrainy vid 06.12.2001 r. № 1193/2001. (2001). URL: <https://zakon.rada.gov.ua/laws/show/1193/2001>.
4. Lohinov, O.M. (2003). Suchasni problemy zabezpechennia informatsiinoi bezpeky v konteksti formuvannia systemy derzhavnoho upravlinnia. *Naukovyi visnyk Yurydychnoi akademii Ministerstva vnutrishnikh sprav*, 3, 199–204 [in Ukrainian].
5. Vasylyev, Yu. (2015). Klasyfikatsiia ta analiz zahroz informatsiinoi bezpeky v kliuchovykh systemakh informatsiinoi infrastruktury. *Pravove, normatyvne ta metodolohichne zabezpechennia systemy zakhystu informatsii v Ukraini, issue 1 (29)*, 56–61 [in Ukrainian].
6. Nizing, J. (1993). Obshhestvennaja oborona kak logicheskaja alternativa. Ot utopii k vyboru. Moscow: Nauka [in Russian].
7. Tofler, E. (2002). *Metamorfozy vlasti. Znanie, bogatstvo i sila na poroge XXI veka*. Moscow: OOO "Izdatelstvo AST" [in Russian].
8. Dombrovska, S.M., Udianskyi, M.M., Dombrovskiy, L.V., Karpeko, N.M. (2019). *Derzhavne rehuliuвання zabezpechennia informatsiinoi bezpeky*. Kyiv: NUTsZU [in Ukrainian].

Torychnyi V. O., PhD of Psychology Sciences, Postdoctoral Student of Training-Production-Research Center, National University of Civil Defence of Ukraine, Kharkiv
ORCID 0000-0003-3336-6386

INFORMATION SUPPORT FOR NATIONAL SECURITY OF STATE WITH REFERENCE TO USING COMPUTER TECHNOLOGIES: PUBLIC-ADMINISTRATIVE ASPECT

Under the conditions of global integration and rigorous geopolitical counteraction, the information space becomes the main arena of collisions and struggle of multidirectional national interests of states. In view of this, the information support for the national security turns into a vital problem in the present context.

The theoretical basis for the research in the field of information support for the national security has been laid by the works of such foreign authors as D. Bell, M. Castells, M. McLuhan, A. Toffler, as well as domestic scientists O. Bukhtatyi, S. Chukut, O. Kriukov, O. Lohinov, S. Lutsenko, A. Panaryn, H. Pocheptsov, V. Stepanov and others.

The paper objective is exploration of the information support for the national security of the state in the context of using computer technologies which are based on informativeness and informatization, and their impact on state security.

The current stage of human civilization development testifies to the fact that the formed information security parameters, stereotypes and habits, to a large extent, do not conform to the tasks of providing national security. At the same time, information support for the security of Ukraine is closely connected with its being part of technical cooperation worldwide.

In our opinion, the national security concept of Ukraine should also include the concept of the Ukrainian society's informatization, since the security risks, caused by the lack of modern means of information support for public administration, economy, and social policies, are in large excess over the affordable expenses on their informatization.

In general, the prospects of information security in the sphere of using network communications and the Internet depend largely on a considered state mass communications policy. Practical realization of the liberal theory principles means giving a complete control over e-networks to business entities, which, to our mind, does not fully comply with the existing socio-political needs of the present-day Ukrainian society. This is why a state concept of developing network communications and the Internet should take into account both the available world practices and the national features of using the Ukrainian communications systems. An integrated approach, combining a commercial way to development of network mass communication means with their control on behalf of the state seems quite optimal.

Key words: information support, national security policy, „world wide web”, information technologies.

Надійшла до редакції 14.08.2019 р.