Електронне "**Державне управління: удосконалення та розвиток**"
включено до переліку наукових фахових видань України з питань державного управління
(Наказ Міністерства освіти і науки України від 22.12.2016 № 1604)
www.dy.nayka.com.ua | № 12 2018 р. | 27.12.2018

DOI: 10.32702/2307-2156-2018.12.101

УДК 351.86:004:007]:005.591.6

Д. М. Костенко,
аспірантка кафедри глобалістики, євроінтеграції та управління національною безпекою
Національної академії державного управління при Президентові України

ВИКОРИСТАННЯ НОВІТНІХ ТЕХНОЛОГІЙ У ПУБЛІЧНОМУ УПРАВЛІННІ В КОНТЕКСТІ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Diana Kostenko
post-graduate student of the Chair of Globalistics, European Integration
and National Security Management at National Academy for Public Administration
under the President of Ukraine

USING OF NEW TECHNOLOGIES IN THE PROVIDING OF NATIONAL SECURITY

У статті здійснено аналіз чинників, які обумовлюють використання новітніх технологій у публічному управлінні в контексті забезпечення національної безпеки, розкривається їх сутність та охарактеризовано їх функціональний зміст з огляду на відповідну здатність системи публічного управління використовувати інноваційні технології у процесі публічно-управлінської практики забезпеченням національної безпеки. Розглянуто проблематику інновацій в публічному управлінні в органах влади центрального рівня, що формують засади і напрями політики держави. Наголошено на пріоритетних завданнях вироблення концептуального бачення і стратегії формування нової якості публічного управління, ефективної системи державної служби, яка була б здатна в умовах наростаючої невизначеності розробляти і впроваджувати інновації, щоб налаштувати систему публічного управління на ефективну взаємодію з бізнесом, структурами громадянського суспільства, що задіяні у процесах розробки та впровадження новітніх технологій для продуктивного застосування їх можливостей у процесах публічної політики та забезпечення національної безпеки.

The article analyzes the factors that determine the use of the latest technologies in public administration in the context of providing national security, reveals their essence and describes their functional content, taking into account the appropriate ability of the public administration system to use innovative technologies in the process of public management practice providing national security. The problems of innovations in public administration in central government bodies that form the principles and directions of state policy are considered. The priority tasks of developing a conceptual vision and strategy of forming a new quality of public administration, an effective civil service system that would be able, in conditions of growing uncertainty, to develop and implement innovations in order to set up a public administration system for effective interaction with business, civil society organizations involved in the processes of developing and implementing the latest technologies for the effective use of their capabilities in the processes of public policy and ensuring national security.

We are living in an age of dramatic technological progress. That progress has brought us many conveniences and advantages, but one result has been a rash of new spying and surveillance technologies. These include new or greatly improved imaging devices, location-tracking technologies, communications eavesdropping systems, and new means of collecting ever-more-granular data of all kinds about individuals and their activities.
All too often, the deployment of these technologies happens faster than our social, political, educational, or legal systems can react, producing a "land rush" in which companies and government agencies deploy new privacy-invasive technologies before subjects are aware that they exist—and certainly before we have consented to their use through our democratic political system.
Promoting the preservation of privacy and other values in a manner that maximizes the advantages that such technology might bring us. In some cases, technology-specific rules might be warranted. In all cases, we would benefit from the application of basic privacy principles, such as the globally recognized Fair Information Practice Principles.
The peculiarity of the deployment of the processes of using the newest technologies in the public management of the provision of national security is the need for certain public support or the shifting of the corresponding responsibilities to management entities that carry out their activities in this area. Implementation of the latest technologies in this area depends on the available resources in such entities of ensuring national security. The modern science of public administration and practice convincingly proves that effective innovative technological changes are the main factor in the long-term socio-economic development of any country and its overall security. In this regard, the "national innovation system of public administration and administration" should be formed in Ukraine. In such circumstances, the effectiveness of public administration depends on the use of sufficient amount of innovative forms and management methods. For Ukraine, this problem is even more relevant in connection with the challenges and threats that require the immediate modernization of the public administration system for ensuring national security in order to meet the needs of society.

***Ключові слова**: публічне управління; забезпечення національної безпеки; кібербезпека; інноваційні технології; комунікаційні мережі; BigData.*

***Key words**: public administration; national security; cybersecurity; surveillance technology; communication networks; big data.*

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями. Особливістю розгортання процесів використання новітніх технологій у публічному управлінні забезпеченням національної безпеки є необхідність певної публічної підтримки або перекладання відповідного обов'язку на суб'єкти управління, що здійснюють свою діяльність у цій сфері. Упровадження новітніх технологій у згаданій сфері залежить від наявних ресурсів у таких суб'єктів забезпечення національної безпеки. Сучасна наука державного управління і практика переконливо доводять, що ефективні інноваційні технологічні зміни є головним чинником довгострокового суспільно-економічного розвитку будь-якої країни та її загальної безпеки. У зв'язку із цим в Україні має бути сформовано "національну інноваційну систему публічного управління та адміністрування". В таких умовах результативність державного управління залежить від використання достатнього обсягу інноваційних форм і методів управління. Для України ця проблема ще більше актуалізується у зв'язку з викликами й загрозами, які вимагають негайної модернізації системи публічного управління забезпеченням національної безпеки для задоволення потреб суспільства.

Аналіз останніх досліджень і публікацій свідчить, що дослідженню питань використання новітніх технології у публічному управлінні розглядається такими вченими, як: І. Дегтярьова [2], С. Князєв [7], В. Куйбіда [8], А. Михненко [11], О. Орлов [13], Х. Хачатурян [14] та ін. Питання інновацій в державному управлінні у сфері забезпечення національної безпеки з позицій існуючих проблем їх упровадження в сучасній Україні досліджується такими вченими, як: В. Абрамов [1], О. Зозуля [4], Р. Марутян [9], М. Шевченко [15] та ін., але питання механізмів використання новітніх технологій у публічному управлінні в контексті забезпечення національної безпеки ще не досліджені в повному обсязі.

Постановка завдання. У даній статті автор ставить за мету розглянути чинники, що діють на здатність системи публічного управління використовувати інноваційні технології у процесі публічно-управлінської практики.

Виклад основного матеріалу. У розвитку сфери публічного управлінні забезпеченням національної безпеки важливе місце належить застосуванню сучасних новітніх інноваційних управлінських технологій

У часи кризи традиційні способи осмислення не встигають за швидкістю соціальних змін [1]. Як в індивідуальній, так і в колективній кризі її учасниками відчувається смутна загроза щодо способу їх буття, що супроводжується реакцією, яка зміцнює старі смисли як засіб погашення цієї загрози. Як вважає датський дослідник Б.Томассен, лімінальність передбачає «раптову актуалізацію суб'єктності, і часом драматичне переплетення думки і досвіду» [16, p.14].

Ми живемо в епоху технічного прогресу. Цей прогрес приніс нам багато зручностей та переваг, але ж з тим, як результат, і вибух нових технологій шпигунства та нагляду. До них відносяться нові чи значно поліпшені пристрої обробки зображень, технології відстеження місцезнаходження, системи підслуховування повідомлень та нові способи збору все більш детальних даних про осіб та їх діяльність[10].

Занадто часто, розгортання цих технологій відбувається швидше, ніж наші соціальні, політичні, освітні або правові системи можуть реагувати, створюючи таку ситуацію, в якій компанії та державні установи впроваджують нові технології конфіденційності, до того, як суб'єкти знають, що вони існують - і, звичайно, до того, як ми погодились на їх використання.

“Big data” –"Великі дані" – термін, який використовується для збору та агрегації величезної кількості інформації, яку можна обробляти та аналізувати лише потужними комп'ютерами. Великі корпорації накопичують особисту інформацію про осіб та складають максимально деталізовані профілі, що містять конфіденційну інформацію, яка включає в себе політичні погляди, релігію, расу та медичні дані про людину. Як правило, такі дані збираються для продажу іншим компаніям, які бажають скористатися всіма можливостями споживачів. Проте брокери даних також займаються хижою діловою практикою, яка спрямована на вразливі категорії населення: малозабезпечених людей похилого віку, інвалідів тощо.

Штучний інтелект покладений в основу технологій розпізнавання обличчя. Так, за даними компанії Dahua Technology USA 2-мегапіксельна камера являє собою автономне інтелектуальне рішення з інтерфейсом, яке виконує складне розпізнавання обличчя без додаткових ліцензій або серверів. Камера пропонує точний аналіз обличчя в режимі реального часу, який включає шість видів особових рис: вік, стать, вираз, окуляри, маска для рота та вуса, а також п'ять видів виразу обличчя, включаючи веселий, нормальний, здивований, сумний і лють. Камера містить в собі базу даних порівняння до 10 000 зображень особи та п'ять бібліотек даних.

Так наприклад, китайські підприємства та військові ведуть моніторинг діяльності мізків та емоцій співробітників. Як повідомляється, технологія підвищує продуктивність та рентабельність. Невідомо, чи всі співробітники, що піддаються технології, знають про те, що вони підлягають моніторингу. Широке використання даного моніторингу може стати новим етапом у системі державного контрою Китаю над населенням, який в основному зосереджувався на розпізнаванні обличчя та збільшенні цензури в Інтернеті.

Згідно з доповіддю CB Insights в Китаї в п'ять разів більше патентів, ніж у США в 2017 році. Шістнадцять областей у Китаї використовують технологію розпізнавання обличчя, яка має рейтинг точності 99,8%. Система достатньо швидка для сканування населення Китаю за одну секунду, і займе дві секунди, щоб сканувати населення світу. Протягом останніх двох років система була використана для арешту 2000 людей. Технологія розпізнавання обличчя зростає в Китаї, де вона використовується для допомоги споживачам, а також поліції, які можуть відслідковувати рухи людей, друзів і навіть спробувати передбачити злочин.

На даний час в Китаї існує 170 мільйонів камер відеоспостереження, і до 2020 року країна сподівається збільшити їх кількість до 570 мільйонів.

Протягом багатьох років існує достатньо доказів того, що авторитарні уряди в усьому світі спираються на технології, розроблені американськими, канадськими та європейськими компаніями для порушення прав людини. Завдяки програмному забезпеченню, що дозволяє фільтрувати та блокувати Інтернет-контент, уряди цих країн шпигують за своїми громадянами, багато таких компаній активно обслуговують автократичні уряди як «маленькі помічники репресій».

Досягнення цих технологій надзвичайно широке: спеціальні служби можуть слухати розмови у мобільних телефонах, використовувати розпізнавання голосу для сканування мобільних мереж, читати електронні листи та текстові повідомлення, цензурувати веб-сторінки, відстежувати кожен рух громадянина за допомогою GPS та навіть змінювати вміст електронної пошти перебуваючи на шляху до одержувача. Деякі інструменти встановлюються за допомогою того самого шкідливого програмного забезпечення та програм-шпигунів, що використовуються інтернет-злочинцями для крадіжки кредитної картки та банківської інформації. Вони можуть таємно включити веб-камери, вбудовані в персональні ноутбуки та мікрофони, у мобільних телефонах, які не використовуються. І вся ця інформація відфільтровується та організовується у такому великому масштабі, що її можна використовувати для контролю над кожною людиною у всій країні. Постає питання щодо встановлення кордонів між правами людини і забезпеченням безпеки держави та суспільства, на які обмеження власної свободи може погодитися громадянин заради забезпечення особистої та національної безпеки.

Зростаюча активність злочинних угруповань в комунікаційних мережах, поширення кібертероризму, розповсюдження матеріалів загрозливого та аморального характеру, залежність усіх сфер життєдіяльності держави від інформації зумовлюють необхідність активної взаємодії правоохоронних органів з провайдерами інформаційно-комунікативних послуг. Велікобританія має значний та досить прогресивний досвід подолання названих проблем, що обумовлює необхідність його аналізу та визначення можливостей адаптації британських досягнень та законодавства до потреб України.

Правоохоронні та спеціальні структури Великобританії, незважаючи на ґрунтовну нормативно-правову базу, намагаються взаємодіяти з провайдерами, за можливості, на основі добровільних домовленостей. Головною структурою, що взаємодіє з комунікаційними операторами, насамперед, у питаннях дозволеного контенту та фільтрації інформації є Офіс з комунікацій (Office of Communications, скорочено – Ofcom, створений у 2003 році Актом про комунікації – Communications Act 2003) – установа, що має статус державної корпорації, підзвітна парламенту, фінансується за рахунок надходжень від учасників телекомунікаційного ринку та урядових грантів. Ofcom визначає перелік фільтрів, які провайдери мають "добровільно" встановлювати для забезпечення онлайн-безпеки користувачів, а саме фільтрів, які блокують матеріали: порнографічного характеру; матеріалів, що зображують жорстокість, наркотики, ненависть, суїцид; сприяють поширенню шкідливих звичок; заохочують хакерство та незаконний обмін файлами. Згідно даним Ofcom чотири головні ІКТ-провайдери (British Telecom, TalkTalk, Sky, Virgin Media), що покривають 95 % британських домогосподарств, встановили фільтрування за замовчуванням – тобто користувачі не можуть відключити його за бажанням[13].

Однією із важливих структур в системі взаємодії державних органів та ІКТ провайдерів є Internet Watch Foundation (IWF) – незалежна неурядова благодійна саморегульована організація, створена у 1996 році для виявлення та ліквідації незаконних матеріалів в інтернеті. Організацією керують спільно ІКТ-провайдери, представники уряду та правоохоронних установ, представники благодійних організацій, громадського сектору. Найбільша увага приділяється видаленню матеріалів, пов'язаних з дитячою порнографією, але також розглядаються випадки ліквідації іншого контенту, розміщення якого порушує чинне законодавство. IWF самостійно шукає неправомірний матеріал, а також розглядає скарги від користувачів. У випадку оцінки матеріалу як неправомірного, IWF з'ясовує, хто є провайдером, що надає доступ до такого матеріалу. Якщо провайдер діє на території Великобританії, фонд надсилає йому попередження з вимогою видалити матеріал чи закрити до нього доступ; якщо провайдер відмовляється задовольнити вимогу, IWF має право передати справу на розгляд правоохоронних органів[13] (так, у 2010 році між IWF та Асоціацією начальників поліції (Association of Chief Police Officers, ACPO) було підписано спеціальну Угоду про співробітництво з метою сприяння обміну інформацією та пришвидшення процедур виявлення та видалення неправомірного контенту[6]). На сьогодні членами IWF є більшість ІКТ-провайдерів, що діють у Великобританії, а також провідні інтернет-компанії, такі як Google, Facebook, Twitter, Yahoo!, на яких поширюється дія Кодексу поведінки членів IWF.

Процедура отримання доступу та вилучення незаконних матеріалів у провайдерів та компаній, розміщених поза межами Великобританії, насамперед, Facebook, Google та Twitter, є значно складнішою. Так, Facebook на своєму сайті зазначає, що дані користувачів надаються урядовим органам інших держав на основі договорів між США та цією державою про правову взаємодопомогу. Кожен запит перевіряється на правову обґрунтованість та відповідність правилам діяльності компанії. Якщо уповноважений орган у США надасть Facebook (відповідно до Закону про США про збереження повідомлень, Stored Communications Act) судовий запит (що надає право розкривати основні дані користувача – ім'я, адресу електронної пошти, IP-адресу, дані кредитних карток), судове рішення (що дозволяє отримати доступ до певних записів та іншої інформації з аккаунта) або судовий ордер (згідно з яким можна розкрити матеріали включно з повідомленнями, фотографіями, відеозаписами, записами на стіні, інформацію про місцезнаходження), такі дані можуть бути передані за рішенням Міністерства юстиції США іншій державі[3]. Подібні можливості перераховує на своєму сайті і Google, додаючи, що у випадку, якщо певне розпорядження видається безпосередньо закордонним органом, то йому можуть бути надані лише реєстраційні дані аккаунта Google чи YouTube (ім'я, адреса електронної пошти, IP-адреса, відмітки часу) [6]. Аналогічним чином діє Twitter. Кожна з цих провідних компаній щороку публікує відповідний звіт (transparency report).

Згідно з британським законодавством та судовою практикою соціальні мережі підпадають під визначення «публічна електронна комунікаційна мережа». Будь-які повідомлення протиправного характеру, розміщені у соціальних мережах, можуть стати причиною відповідальності за чинними законами. Акт про комунікації 2003 року (Communications Act 2003), зокрема стаття 127 «Неправильне використання поштових та електронних засобів комунікації», містить положення про те, що особа вважається винною, якщо вона засобами «публічної електронної комунікаційної мережі» надсилає повідомлення загрозливого, непристойного чи дуже образливого характеру (grossly offensive) (п. 1 ст. 127), надсилає заздалегідь помилкове повідомлення для навмисного роздратування, незручності чи занепокоєння адресата (п. 2); відповідальність за таке порушення – ув'язнення на строк максимум 6 місяців та / або штраф до 5000 фунтів стерлінгів. Як показує практика, дана стаття може бути застосована для висунення обвинувачень за скоєння злочинів на ґрунті ненависті (расової, релігійної, сексуальної тощо), хакерські злочини, знущання та переслідування у кіберпросторі.

В умовах боротьби України проти зовнішньої агресії та діяльності терористичних організацій ДНР /

ЛНР, необхідно шукати механізми більш інтенсивного впливу на діяльність цих терористичних структур в інформаційній сфері. Доцільним є рекомендувати СБУ та МВС посилити співпрацю (зокрема, через механізми щотижневих зустрічей, офіційних роз'яснень тощо) із вітчизняними учасниками телекомунікаційного ринку та власниками контенту (сервісів). Запропонувати всім гравцям телекомунікаційного ринку утворення українського аналогу Internet Watch Foundation із широкими механізмами впливу самого співтовариства на його роботу (участь державних структур тут має бути мінімальна і суто формальною). Це дозволить частково зменшити необхідність безпосереднього державного примусу при закритті тих чи інших інтернет-ресурсів. Механізми роботи цієї структури можна визначити по аналогії з британський досвідом. Проаналізувати перспективу об'єднання у єдиний конвергентний орган Національної ради, що здійснює регулювання у сфері зв'язку та інформатизації, та Національної ради України з питань телебачення і радіомовлення. Це дозволить більш цілісно вирішити питання взаємодії з різними гравцями інформаційної (телекомунікаційної) сфери. У взаємодії з вітчизняними інтернет-провайдерами (напряму чи через посередницькі структури накшталт Інтернет асоціації України) обговорити можливі обсяги добровільної допомоги гравців ринку у питаннях протидії розповсюдження протизаконного контенту, або такого, що шкодить національній безпеці. Зважаючи на те, що значна кількість антидержавницьких матеріалів поширюється через іноземні соціальні мережі чи сервіси, доречною є оптимізація процедур подання скарг (запитів) щодо відповідних шкідливих / незаконних матеріалів до правоохоронних та судових органів США. В рамках співробітництва правоохоронних структур України та Великобританії доцільним є вивчення відповідного британського досвіду та тих складнощів, які виникають в процесі переслідування правопорушників у таких мережах, зокрема, через запити профільних відділів правоохоронних структур, що займаються міжнародним співробітництвом.

Україна повинна докласти усі необхідні сили, щоб налаштувати систему публічного управління на ефективну взаємодію з бізнесом, структурами громадянського суспільства, що задіяні у процесах розробки та впровадження новітніх технологій для ефективного використання їх можливостей у процесах публічної політики та забезпечення національної безпеки.

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі. У межах статті автором проаналізовано особливості діяльності інформаційно-комунікативних підрозділів публічного управління й на основі чого визначено їх призначення та основні функції (інформаційна, аналітична, комунікативна), а також сформовано ряд висновків, зокрема: – обґрунтовано, що аналітична (інформаційно-аналітична) діяльність інформаційно-комунікативних підрозділів є видом управлінської діяльності, яка складається з моніторингу інформації, встановлення тенденцій суспільного розвитку, виявлення сфер інтересів, підготовки пропозицій до реагування на суспільні виклики, інформаційно-аналітичний супровід її рішень (прогнозування, планування, підготовка до прийняття), оцінки ризиків та здійснення відповідного методологічного забезпечення.

На сьогодні необхідне усвідомлення проблематики інновацій в публічному управлінні, насамперед в органах влади центрального рівня, що формують засади і пріоритетні напрями політики держави. Головним завданням при цьому є вироблення концептуального бачення і стратегії формування нової якості публічного управління, ефективної системи державної служби, яка була б здатна в умовах наростаючої невизначеності розробляти і впроваджувати інновації.

Отже здійснений аналіз чинників, що діють на здатність системи публічного управління використовувати інноваційні технології у процесі публічно-управлінської практики у контексті забезпечення національної безпеки. На підставі цього охарактеризовані відповідні аспекти: суб'єкти публічного управління України мають вкласти великі ресурси в розвиток науки, співпрацю з структурами громадянського суспільства та бізнес-сектору і виступати головними замовниками та отримувачами інтелектуального продукту в інтересах використання новітніх технологій у публічному управлінні забезпечення необхідного рівня національної безпеки.

Таким чином, можна констатувати, що публічне управління в контексті забезпечення національної безпеки при застосуванні новітніх технологій може сприяти усуненню негативних явищ у цій сфері.

У подальших розвідках необхідно провести детальний аналіз основних параметрів і критеріїв реалізації впровадження новітніх технологій в публічному управлінні в контексті забезпечення національної безпеки.

Список літератури.

1. Абрамов В. І. Концепт «номадична сингулярність» публічного врядування в умовах збройного конфлікту / В. І. Абрамов // Публічне врядування в Україні: стан, виклики та перспективи розвитку : матеріали щоріч. Всеукр. наук.-практ. конф. за міжнародною участю (Київ, 25 травня 2018 р.) : у 5 томах. / за заг. ред. В. С. Куйбіди, М. М. Білинської, О. М. Петроє. – Київ : НАДУ, 2018. – Т. 4. – С. 102–104.

2. Дегтярьова І. О. Інновації в державному і муніципальному управлінні як необхідна умова соціально-економічних досягнень в сучасній Україні // Вісник Національного університету цивільного захисту України. Серія : Державне управління. – 2014. – Вип. 1. – С. 96–105.

3. Ефективність державного управління : монографія / Ю. М. Бажал, О. І. Кілієвич, О. В. Мертенс [та ін.] ; за заг. ред. І. В. Розпутенкав. – Київ : К.І.С., 2002. – 420 с.

4. Зозуля О.С. Науковий дискурс інформаційної безпеки та пріоритетні напрями дослідження в рамках

спеціальності “теорія та історія державного управління” / О.С. Зозуля // Держава та регіони. – Запоріжжя, 2015. – № 2 (50). – С. 59-67.

5. Ігнатенко О. П. Використання новітніх технологій у державному регулюванні сфери благоустрою населених пунктів / О. П. Ігнатенко // Збірник наукових праць Національної академії державного управління при Президентові України. – 2014. – Вип. 2. – С. 96–105.

6. Інформаційно-комунікативна діяльність органів публічної влади : монографія / В. С. Куйбіда, О. В. Карпенко, А. В. Дуда [та ін.] ; за заг. ред. В. С. Куйбіди, О. В. Карпенка. – Київ : ЦП “Компрінт”, 2018. – 364 с.

7. Князев С. Н. Управление инновациями и инновации в управлении [Електронний ресурс] / С. Н. Князев, И. И. Ганчеренок // Государственное управление. – 2007. – Вып. 11. – Режим доступу : http://www.vivakadry.com/29.htm.

8. Куйбіда В. С. Досвід впровадження стандартів доброго врядування на місцевому рівні в Україні та інших європейських країнах / В. С. Куйбіда, В. В. Толкованов. – Київ: ТОВ Поліграфічний Центр Крамар, 2010 – 258 с.

9. Марутян, Р.Р. Інформаційна складова гібридної війни проти України: сучасні виклики та загрози Режим доступу : http://matrix-info.com/2017/04/13/informatsijna-skladova-gibrydnoyi-vijny

10. Марутян, Р.Р. "Інформаційні ресурси у системі забезпечення національної безпеки." Режим доступу: http://www. dsaua. org/index. php.

11. Михненко А. М. Інновації в управлінні суспільним розвитком : [навч. посіб.] / А. М. Михненко, В. Д. Бакуменко, С. О. Кравченко. – Київ : Вид-во НАДУ, 2009. – 115 с.

12. Орлов О. В. Інноваційні процеси в державному управлінні : [монографія] / О. В. Орлов. – Харків : Вид-во ХарРІ НАДУ "Магістр", 2012. – 196 с.

13. Федорчак О. В. Проектний підхід як інноваційний механізм державного управління / О. В. Федорчак // Державне управління : теорія та практика [Електрон. ресурс] : електрон. наук. фах. журнал НАДУ при Президентові України. – Вип. 1. – К. : НАДУ, 2006. – Режим доступу : http://www.academy.gov.ua./ej3/txts/02-FEDORCHAK.pdf

14. Хачатурян Х. В. Теоретико-методологічні засади інновацій у державному управлінні [Електронний ресурс] / Х. В. Хачатурян. – Режим доступу : http://law.kymu.edu.ua/ndgu_st27_ua.htm.

15. Шевченко М.М. Соціально-філософська концепція науково-освітнього забезпечення публічного управління у сфері національної безпеки України / М.М. Шевченко // Гілея: науковий вісник. Збірник наукових праць / Гол. ред. В. М. Вашкевич. – К. : «Видавництво «Гілея», 2018. – Вип. 134. – С. 320-325.

16. Thomassen, B. The Uses and Meanings of Liminality (International Political Anthropology, Mar 3; 2 (1), 2009.–P. 5-28.

References.

1. Abramov V. I. (2018), "Concept "nomadic singularity" of public governance in conditions of armed conflict", *Materialy shchorich. Vseukr. nauk.-prakt. konf. za mizhnarodnoiu uchastiu (Kyiv, 25 travnia 2018 r.)* [Materials of the annual All-Ukrainian scientific and practical conference on international participation (Kyiv, May 25, 2018)], *Publichne vriaduvannia v Ukraini: stan, vyklyky ta perspektyvy rozvytku* [Public governance in Ukraine: state, challenges and development prospects], vol. 4, NADU, Kyiv, Ukraine, pp. 102–104.

2. Dehtiarova, I. O. (2014), "Innovations in state and municipal governance as a prerequisite for socio-economic achievements in modern Ukraine", *Visnyk Natsionalnoho universytetu tsyvilnoho zakhystu Ukrainy. Seriia: Derzhavne upravlinnia*, vol. 1, pp. 96–105.

3. Bazhal, Yu. M. Kiliievych, O. I. Mertens, O. V. and others (2002), *Efektyvnist derzhavnoho upravlinnia* [Efficiency of public administration], K.I.S., Kyiv, Ukraine, P.420.

4. Zozulia, O.S. (2015), " Scientific discourse on information security and priority directions of research within the specialty "Theory and History of Public Administration"", *Derzhava ta rehiony*, vol. 2 (50), pp. 59-67.

5. Ihnatenko, O. P. (2014), "Use of the newest technologies in the state regulation of the sphere of improvement of settlements", *Zbirnyk naukovykh prats Natsionalnoi akademii derzhavnoho upravlinnia pry Prezydentovi Ukrainy*, vol. 2, pp. 96–105.

6. Kuibida, V. S. Karpenko, O. V. Duda, O. V. and others (2018), *Informatsiino-komunikatyvna diialnist orhaniv publichnoi vlady* [Information and communicative activity of public authorities], TsP “Komprint”, Kyiv, Ukraine, P. 364.

7. Knjazev, S. N. and Gancherenok, I. I. (2007), "Management of innovations and innovations in management", *Gosudarstvennoe upravlenie*, vol. 11, [Online], available at: http://www.vivakadry.com/29.htm.

8. Kuibida, V. S. and Tolkovanov, V. V. (2010), *Dosvid vprovadzhennia standartiv dobroho vriaduvannia na mistsevomu rivni v Ukraini ta inshykh yevropeiskykh krainakh* [Experience in implementing good governance standards at the local level in Ukraine and other European countries], TOV Polihrafichnyi Tsentr Kramar, Kyiv, Ukraine, P. 258.

9. Marutian, R.R. "Information component of the hybrid war against Ukraine: modern challenges and threats", [Online], available at: http://matrix-info.com/2017/04/13/informatsijna-skladova-gibrydnoyi-vijny

10. Marutian, R.R. "Information resources in the system of providing national security", [Online], available at: http://www. dsaua. org/index. php.

11. Mykhnenko, A. M. Bakumenko, V. D. and Kravchenko, S. O. (2009), *Innovatsii v upravlinni suspilnym rozvytkom* [Innovation in the management of social development], Vyd-vo NADU, Kyiv, Ukraine, P115.

12. Orlov, O. V. (2012), *Innovatsiini protsesy v derzhavnomu upravlinni* [Innovative processes in public administration], Vyd-vo KharRI NADU "Mahistr", Kharkiv, Ukraine, P.196.

13. Fedorchak, O. V. (2006), "Project Approach as an Innovative Mechanism of Public Administration", *Derzhavne upravlinnia: teoriia ta praktyka*, vol. 1, [Online], available at: http://www.academy. gov.ua./ej3/txts/02-FEDORCHAK.pdf

14. Khachaturian, Kh. V. "Theoretical and Methodological Principles of Innovation in Public Administration", [Online], available at: http://law.kymu.edu.ua/ndgu_st27_ua.htm.

15. Shevchenko, M.M. (2018), "Socio-philosophical concept of scientific and educational provision of public administration in the sphere of national security of Ukraine", *Hileia: naukovyi visnyk. Zbirnyk naukovykh prats*, vol. 134, Kyiv, Ukraine, pp. 320-325.

16. Thomassen, B. The Uses and Meanings of Liminality (International Political Anthropology, Mar 3; 2 (1), 2009.–P. 5-28.

Стаття надійшла до редакції 17.12.2018 р.