ІНФОРМАЦІЙНА ПОЛІТИКА

(шифр)

КОНКУРСНА НАУКОВА РОБОТА

на тему:

«ДЕРЖАВНА ПОЛІТИКА

У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УКРАЇНІ**»**

ЗМІСТ

ВСТУП

Актуальність теми. В Україні, як і в усьому світі, проблеми забезпечення системи безпеки держави, суспільства й особистості все більше виходять на перший план у державній політиці та державному управлінні. Інформаційна безпека належить до числа пріоритетних цілей сучасної держави і є одним з основних факторів його стабільного розвитку. Очевидно, що системні дефекти та збої у функціонуванні механізмів забезпечення інформаційної безпеки можуть привести до соціально-політичних, економічних і техногенних зрушень, здатних підірвати можливість органів державного управління належним чином здійснювати свої основні функції.

Інформаційна безпека суспільства в цілому та його структурних частин – досить актуальна проблема. Це пов'язано з тим, що питання інформації й особливо соціальної інформації в даний час набули особливого значення. Сучасний етап розвитку суспільства характеризується зростаючою роллю інформаційної сфери, що є важливим чинником суспільного життя, багато в чому визначає перспективи успішного здійснення соціально-політичних та державноуправлінських перетворень українського суспільства. Це обумовлено такими основними обставинами: інтенсивний розвиток інформаційної інфраструктури і, насамперед, інформаційно-телекомунікаційних систем, засобів і систем зв'язку, інтеграція у світовий інформаційний простір, а також інформатизація практично всіх сторін суспільного життя, діяльності органів державної влади і управління, які істотно посилили залежність ефективного функціонування суспільства та держави від стану інформаційної сфери; індустрія інформатизації, телекомунікації та зв'язку, демократизація тощо.

У змістовному плані інформаційна безпека є складовою частиною національної безпеки. У її структурі інформаційна безпека займає особливе місце. Це обумовлено тим, що всі види безпеки не можуть бути реалізовані без інформаційного забезпечення. Цінність інформації може бути позитивною або негативною, що пояснюється таким: інформація – універсальний інструмент

прогресу людства, глобальний і найбільш дефіцитний ресурс розвитку сучасного суспільства, одна з основних загальнолюдських і національно-державних цінностей. Саме інформаційні ресурси та процеси є першопричиною багатьох соціальної напруги, конфліктів і кризи. Очевидно, що порушення інформаційних законів світобудови може виявитися фатальним для існування самого людства. Усе вказує на важливість дослідження обраної теми.

Стан наукової розробки проблеми. Загальні питання, що стосуються генезису інформаційного суспільства, аналізуються у працях В. Брижко, Р. Броун, У. Дайзарда, Р. Дарендорфа, Л. Ірвінг, М. Кастельса, К. Поппера, Г. Почепцова та ін. [3; 27; 32]. Проблеми комунікації в управлінні досліджують такі науковці, як С. Арнштейн, В. Дзюндзюк, О. Крюков, О. Крутій, В. Нікітін, О. Радченко, та ін. [7; 22; 31]. Питання державного управління у сфері безпеки (національної, регіональної тощо), її забезпечення організаційними, інформаційними та іншими методами розглядаються у працях А. Голобуцького, Г. Головко, С. Домбровська, В. Косевцова, Ю. Машкарова, Н. Нижник, А. Помази-Пономаренко, В. Садкового, В. Стрельцова та ін. [9; 16; 25]. Проте їх наукові праці здебільшого присвячені теоретичним проблемам щодо розвитку інформаційного суспільства, правового регулювання інформаційної сфери з боку держави чи виключно технічним аспектам упровадження інформаційних технологій. У той же час, залишається недостатньо розробленою проблема реалізації інформаційної безпеки держави в умовах становлення інформаційного суспільства з урахуванням їх дихотомічності та необхідності переходу до сучасних принципів публічного адміністрування та міжсекторної взаємодії, що й актуалізує тему дослідження, визначає його мету та завдання.

Мета і завдання дослідження. Метою дослідження є науково-теоретичне обґрунтування та розробка практичних рекомендацій щодо вдосконалення механізмів державної політики у сфері інформаційної безпеки в Україні. Досягнення визначеної мети зумовило необхідність вирішення таких завдань:

– з’ясувати зміст інформаційної безпеки і її місце в системі державного управління;

– проаналізувати стан дії механізмів державної політики у сфері інформаційної безпеки в Україні;

– визначити шляхи вдосконалення організаційно-правових механізмів державної політики у сфері інформаційної безпеки України;

– обґрунтувати новітні функціонали системи державного управління у сфері інформаційної безпеки України.

Об'єкт дослідження– процес реалізації державного управління у сфері інформаційної політики.

Предмет дослідження – державна політика у сфері інформаційної безпеки в Україні.

Методи дослідження. Цілісність дослідження забезпечують системний підхід. Для теоретичного осмислення різних аспектів проблеми застосовуються аналіз і синтез (можливості адаптації світових зразків в Україні із організації єдиної інформаційно-комунікативної інфраструктури, е-уряду), моделювання (визначення моделі державного регулювання інформаційної сфери суспільства та міжсекторної взаємодії в цій сфері), абстрагування й узагальнення (визначення шляхів удосконалення організаційно-правового забезпечення державної політики у сфері інформаційної безпеки України, порівняння й уточнення новітніх функціоналів системи держу правління нею). Інформаційну базу дослідницької роботи склали нормативно-правові акти, пов'язані з реалізацією державної політики у сфері інформаційної безпеки в Україні, зокрема Міністерством інформаційної політики України, а також наукові напрацювання учених в означеній сфері.

У першому розділі розглянуті підходи до характеристики понять «інформаційна безпека», «національна безпека» і «система державного управління», розкрито цілі державної політики у сфері інформаційної безпеки та сутність дихотомії цієї політики та безпеки, представлено теоретичні передумови формування інформаційного суспільства, а також уточнено сутність інструментальної складової системи держуправління у сфері інформаційної безпеки, що становлять підґрунтя для виокремлення правового й

організаційного механізмів державної політики в цій сфері.

У другому розділі проаналізовано процес формування та функціонування організаційно-правових механізмів державної політики у сфері інформаційної безпеки в Україні, проаналізовано роль суб'єктів інформаційної безпеки в її забезпеченні, причому особлива увага приділена проблемі міжгалузевої взаємодії в контексті інформаційної безпеки держави.

У третьому розділі визначено шляхи вдосконалення правового й організаційного механізмів державної політики у сфері інформаційної безпеки України, зокрема політико-управлінські наслідки упровадження державної інформаційно-комунікативної інфраструктури. Акцентовано на новітніх функціоналах у сфері інформаційної безпеки на всіх рівнях публічного управління – удосконаленні організаційної будови Міністерства інформаційної політики України (основної та функціонально-допоміжної), усуненні дублювання в напрямках його діяльності з тими, що становлять предмет відання місцевих органів виконавчої влади загальної компетенції.

Значення отриманих результатів полягає в тому, що наукові узагальнення доведені до рівня конкретних пропозицій. Висновки, отримані у результаті наукового дослідження, мають важливе значення для подальшої теоретичної розробки питання публічно-управлінської взаємодії в умовах модернізації й інформатизації українського суспільства. Рекомендації та пропозиції, викладені в дослідницькій роботі, можуть використовуватися в діяльності органів державної влади як такі, що стосуються, по-перше, оптимізації організаційно-функціональної структури органів виконавчої влади загальної та спеціальної компетенції, а по-друге, активного залучення громадськості до державного управління у сфері інформаційної безпеки.

Конкурсна робота складається зі вступу, 3-х розділів, висновків, списку використаних джерел. Загальний обсяг роботи 30 стор. друкованого тексту.

Результати дослідження за обраною темою відображено в 3 наукових працях, серед яких 1 стаття, а також 2 публікації у збірниках матеріалів науково-комунікативних заходів.

РОЗДІЛ 1
ХАРАКТЕРИСТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СИСТЕМІ ДЕРЖАВНОГО УПРАВЛІННЯ

У сучасних умовах інформація являє собою без перебільшення один з вирішальних ресурсів розвитку цивілізації, оскільки активно впливає на всі сфери життя як окремих суспільств і держав, так і всього світового співтовариства через розвиток інформаційно-комунікаційних технологій (далі – ІКТ). Разом із тим, інформація може використовуватися не тільки на благо, але і на шкоду інтересам особи, суспільства і держави [3]. Це зумовлено тим, що ІКТ є важливим чинником світової інтеграції, соціального розвитку та економічного зростання, будучи найсильнішим каталізатором інформаційного обміну, такі технології несуть у собі безліч явних і прихованих загроз. Надзвичайну значимість у зв'язку з цим набувають питання визначення дихотомічності та забезпечення інформаційної безпеки, визнаної у нашій країні однією з найважливіших складових національної безпеки, тому що інформаційна безпека в сучасному постіндустріальному світ, впливає на прийняття державою тактичних та стратегічних рішень.

На державному рівні й в експертному науковому співтоваристві [6; 27] існує переконання, що статус члена інформаційного суспільства не змінює тієї обставини, що у кожної з країн, є власні національні інтереси в інформаційній сфері і, тим самим, існує необхідність забезпечувати безпеку цих інтересів. Проте, якщо технічним аспектам забезпечення такої безпеки, науковцями приділяється значна увага, то публічно та політико-управлінські аспекти цієї проблеми, на жаль, досліджуються недостатньо системно. На наш погляд, цей факт відображає уповільнення динаміки реформування українського соціуму, а в багатьох сферах і стагнацію цих процесів.

У правовій науці термін «інформаційна безпека» здебільшого використовується у вузькому – технологічному – сенсі, що притаманно, наприклад, англо-саксонській правовій системі [1]. Сутнісно ця безпека

розуміється як стан захищеності інформації і підтримуючої інфраструктури від випадкових або навмисних впливів природного або штучного характеру, які можуть завдати збитку суб'єктам інформаційних відносин (власникам і користувачам інформації і підтримуючої інфраструктури) [там само]. Отже, слушною є думка, що проблеми інформаційної безпеки слід починати досліджувати із виявлення суб'єктів інформаційних відносин, їх інтересів, пов'язаних з використанням ІКТ, зворотній бік якого становлять загрози інформаційній безпеці, а також правового інструментарію держави.

При аналізі політичних аспектів, з державно-процесуальної точки зору, інформаційна безпека може бути розглянута в ряді сфер, а саме: політичних інтересів, політичних відносин; у виборчому; державно-управлінському, зовнішньополітичному процесах тощо [10–11]. При цьому за основними сферами прояву системне вираження інформаційної безпеки знаходить своє дихотомічне відображення в локалізації в таких сферах: а) у сфері функціонування державних органів політичної влади (державна інформаційна безпека) [21]; б) у сфері громадянського суспільства (інформаційна безпека суспільства); в) у сфері інтересів особистості [8, с. 124]. Крім того, за рівнями соціальної організації і геополітичним змістом інформаційна безпека може забезпечуватися на міждержавному, загальнодержавному та внутрішньодержавному рівні (на рівні регіональних інститутів), а також на рівні органів місцевого самоврядування [9].

Інформаційна безпека є результатом інтеграції змісту понять «національна безпека» та «безпека інформації» [3; 16]. Власне, її можна пов'язувати з інститутом таємниці, а по-друге, ототожнювати з інформаційною (технологічною) сферою.

На основі врахування національних інтересів в інформаційній сфері формуються стратегічні і поточні завдання внутрішньої і зовнішньої політики держави щодо забезпечення інформаційної безпеки. Вона характеризується ступенем захищеності держави та суспільства, стійкістю головних сфер життєдіяльності (економіки, науки, техносфери, сфери управління, військової

справи, суспільної свідомості тощо) по відношенню до небезпечних дестабілізуючих деструктивних явищ, що чинять негативний вплив на публічні та приватні інтереси. Об'єктами небезпечного інформаційного впливу і, отже, інформаційної безпеки можуть бути визнають таке: свідомість, психіку людей; інформаційно-технічні системи різного масштабу і призначення. Якщо говорити про соціальні об'єкти інформаційної безпеки, то до них можна віднести особистість, колектив, суспільство, державу та світове співтовариство. Щодо суб'єктів інформаційної безпеки, то до них варто ті органи і структури, які займаються її забезпеченням. Погоджуємося з С. Домбровською, що в практичному плані інформаційна безпека не існує взагалі, безвідносно до суб'єкта інформаційного середовища, але саме суб'єкт диктує «параметри» такої безпеки [9, с. 283]. Уважаємо, що її забезпечення в аспекті врахування інтересів суб'єкта інформаційних відносин представляє собою процес створення сприятливих умов діяльності, за яких реалізовувалися б його інтереси, здійснювалися б поставлені ним цілі.

Аналіз наукових напрацювань В. Дзюндзюка, Ю. Древаля, О. Карпеко та ін. [7; 8; 13] дозволяє відзначити, що інтереси людини, які необхідно охороняти в інформаційному суспільстві, полягають, насамперед, у реальному забезпеченні конституційних прав і свобод людини та громадянина на доступ до інформації, на використання інформації в інтересах здійснення незабороненої законом діяльності, а також у захисті інформації, що забезпечує особисту безпеку, духовний та інтелектуальний розвиток. Інтереси суспільства в інформаційній сфері полягають у захисті життєво важливих інтересів особистості у цій сфері, забезпечення реалізації її конституційних прав і свобод в напрямку зміцнення демократії, досягнення і підтримання суспільної злагоди, підвищення творчої активності населення. Відтак, інтереси держави в інформаційній сфері передбачають створення умов для гармонійного розвитку інформаційної інфраструктури країни, реалізацію конституційних прав і свобод людини в інтересах зміцнення конституційного ладу, суверенітету і територіальної цілісності країни, установлення політичної, соціальної й

економічної стабільності, виконання законів та підтримки правопорядку, розвитку міжнародного співробітництва.

Підсумовуючи вищевикладене, уважаємо зазначити, що досить поширеною є точка зору, з якою ми погоджуємося [3; 9], що інформаційна безпека – це такий стан соціуму, за якого забезпечується надійний і всебічний захист особистості, суспільства і держави від впливу на них особливого виду загроз, що виступають у формі організованих або стихійно виникаючих інформаційних потоків, що здійснюються в інтересах регресивних, реакційних або екстремістські налаштованих політичних і соціальних сил і спрямованих на усвідомлену деформацію суспільної й індивідуальної свідомості. Погоджуємося з С. Бєлаєм, О. Вербицьким, А. Колотом та ін., що наслідком цього може виступати девіантна поведінка особистості, соціальних груп і об’єднань, посилення соціально-політичних, економічних і духовних колізій, наростання, розвиток і закріплення напруженості в соціумі [2; 5; 14].

Ефективна державна політика в інформаційній сфері [13; 22], у т. ч. в аспекті інформаційної безпеки, дихотомічно із нею пов’язана, вона багато в чому залежить від правильного вибору пріоритетів у організаційно-правового вирішення цих проблем, науково обґрунтованої розробки адекватних моделей і підходів до їх розв’язання. Оскільки національна безпека суттєвим чином залежить від забезпечення інформаційної безпеки країни (і, як свідчить В. Косевцов, у ході технічного прогресу ця залежність буде тільки зростати [16]), елементами якої виступають сукупність інформації, засобів її виробництва, обробки та зберігання, інформаційної інфраструктури, суб'єктів, що здійснюють збір, формування, розповсюдження і використання інформації, а також системи регулювання виникаючих при цьому відносин.

Отже, аналіз стану і проблем інформаційної безпеки передбачає здійснення його крізь призму визначення і характеристики правового й організаційного механізмів державної політики у цій сфері, підґрунтям для класифікації яких є відповідні методи впливу (про які дет. ідеться в таких загальновідомих наукових розробках [15]).

РОЗДІЛ 2
АНАЛІЗ МЕХАНІЗМІВ ДЕРЖАВНОЇ ПОЛІТИКИ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

2.1. Аналіз стану дії організаційно-правових механізмів державної політики у сфері інформаційної безпеки України

Органи державної влади, у компетенцію яких входить регулювання соціально-політичних відносин в інформаційній сфері, а також недержавні суб'єкти даної діяльності, які залучаються для вирішення завдань державного управління, виступають в якості суб'єктів державної інформаційної політики та забезпечують рух її правового й організаційного механізмів [27]. Власне, суб'єктами забезпечення інформаційної безпеки є органи, організації й особи, уповноважені законом на здійснення відповідної діяльності. Умовно їх можна поділити на три основних типи залежно від інтересів у здійсненні цієї діяльності: 1) індивіди як особистості; 2) громадські організації та громадськість; 3) органи державної влади.

Суб'єкти державної політики у сфері інформаційної безпеки можна розділити також на дві основні категорії: а) державні інституції, які здійснюють інформаційну політику; б) суб'єкти масового інформування і комунікації. У системі суб'єктів державної інформаційної політики державні інституції поділяються на групи залежно від: 1) рівня влади й управління (центральний, регіональний, місцевий); 2) гілки державної влади (законодавча, виконавча, судова); 3) спрямування діяльності органів державної влади (органи цивільного, економічного управління, «силовий блок», зовнішньополітичні відомства тощо) [там само]. У системі державної інформаційної політики суб'єкти масового інформування та комунікації поділяються на групи за такими категоріями: 1) за видом власності (державні ЗМІ і МК; недержавні ЗМІ та МК, у т. ч. ті, що контролюються іноземними фізичними і юридичними особами);

2) за способом поширення інформації (електронні ЗМІ та МК, друковані ЗМІ та МК, Internet-ЗМІ) [9].

Держава посідає особливе місце як серед суб'єктів державної інформаційної політики, так і серед суб'єктів забезпечення інформаційної безпеки, оскільки вона володіє унікальними засобами і силами протидії загрозам у даній сфері [21]. Загальна структура державної системи забезпечення інформаційної безпеки включає чотири основні владні підсистеми, що утворюють гілки влади, які різняться функціями у сфері забезпечення інформаційної безпеки відповідно до компетенції: голови держави, законодавча влада, виконавча влада, судова влада. Цілі діяльності, повноваження і предмети відання кожної з підсистем детально аналізуються в [25]. Складність реалізації державної політики в означеній сфері покладено на центральний орган виконавчої влади (ЦОВВ) – Міністерство інформаційної політики України, який з 2015 року є основним у забезпеченні інформаційної безпеки держави [26]. Особливість реалізації цієї функції даним ЦОВВ полягає в тому, що він повинен здійснювати свою діяльність на базі використання інформаційної інфраструктури, виробляти і споживати інформаційні ресурси, і як представник власника державних інформаційних ресурсів вчиняти певні дії із забезпечення збереження цих ресурсів і безпеки функціонування інформаційних і телекомунікаційних систем, мереж зв'язку, систем автоматизації управління [там само]. Діяльність зазначеного Міністерства у сфері інформаційної безпеки ґрунтується на таких принципах:

1) дотримання Конституції та законодавства України, а також загальновизнаних принципів і норм міжнародного права;

2) відкритість у реалізації функцій державної влади й управління, з урахуванням обмежень, установлених законодавством України;

3) правову рівність усіх учасників процесу інформаційної взаємодії незалежно від їх політичного, соціального та економічного статусу;

4) пріоритетний розвиток вітчизняних сучасних інформаційних і телекомунікаційних технологій тощо.

Згідно з Положенням про Міністерство інформаційної політики його завданнями є (у систематизованому вигляді) [там само]:

– реалізація конституційних прав і свобод громадян української держави у сфері інформаційної діяльності;

– удосконалення і захист вітчизняної інформаційного простору, інтеграція України у світовий інформаційний простір;

– протидія загрозі розв'язування протистояння в інфосфері тощо.

Першочерговими заходами щодо реалізації державної політики забезпечення інформаційної безпеки України на сучасному етапі повинні бути: 1) розробка й упровадження дієвих організаційно-правових механізмів, що регулюють відносини в інформаційній сфері, а також підготовка концепції публічно-приватного забезпечення інфобезпеки України; 2) розвиток системи підготовки кадрів, які використовуються в галузі забезпечення інформаційної безпеки держави й інформаційної інфраструктури; 3) створення системи культурно-освітнього забезпечення безпеки інформаційної сфери тощо.

Узагальнюючи думки експертів в даній області [3; 9; 27], можна сказати, що чинником, який визначає в цілому державну інформаційну політику, є існування в інформаційній сфері джерел загроз інтересам держави, найнебезпечніші з яких криються не тільки в неконтрольованому розповсюдженні «інформаційної зброї», активізації «комп'ютерного тероризму», а в недосконалості процесу організації та реалізації такої політики.

Слід відзначити, що динаміка зрушень у системі державного управління вимагає проведення подальших наукових досліджень усієї сукупності проблем, пов`язаних із діяльністю органів публічної влади, вивчення практики розвинутих країн з цього питання з метою її застосування в Україні. Потребують удосконалення організаційно-правові механізми державного впливу в цій сфері, з метою соціально-економічного розвитку та забезпечення інформаційної безпеки. Залишається невирішеною проблема, по-перше, механізму розподілу напрямів діяльності органів виконавчої влади загальної компетенції та спеціальної компетенції – Міністерства інформаційної політики

України та місцевих державних адміністрацій. А по-друге, щодо приведення системи та роботи ЦОВВ (Міністерства інформаційної політики України) у відповідність до світової позитивної практики у цій сфері, що передбачає узгодження його системи із публічними та приватними інтересами, її ієрархізацію.

Наразі згідно з положенням про це міністерство питаннями інформаційної безпеки покликаний займатися відповідний його сектор [26]. У той же час, реалізація політики з питань забезпечення інформаційної безпеки покладається на місцеві органи виконавчої влади загальної компетенції [28, пп. 5, 9 ч. 1 ст. 13, пп. 12 ч. 1 ст. 14], а не спеціальної (до яких слід віднести зазначене міністерство), що порушує такі основоположні, загальновідомі принципи державного управління:

1) єдності та системності;

2) виваженості виконання функцій, їхньої не розпорошеності;

3) результативності й ефективності;

4) виваженого використання «портфелю» ресурсів;

5) публічності (прозорості та відкритості); 6) оперативності та соціальної орієнтованості тощо.

Отже, для України сьогодні актуальними є завдання із розвитку інформаційного суспільства, аналіз загроз в інформаційній сфері та забезпечення інформаційної безпеки української держави як частини глобального інформаційного співтовариства. Розробка заходів держави щодо забезпечення інформаційної безпеки громадян, суспільства і держави – один з найважливіших пріоритетів публічного управління в цій сфері, що вимагає дієвої міжсекторної взаємодії, зокрема між державними органами та за умови участі приватного сектору.

2.2. Сучасні механізми міжсекторної взаємодії у сфері інформаційної безпеки

Вирішальним фактором у державному регулюванні процесів інформаційної взаємодії залишається згода, консенсус міжнародних компетентних органів, учених, діячів політики, культури та бізнесу. При цьому їх головне завдання сьогодні полягає в тому, щоб зробити інформацію, канали її поширення більш надійними, засоби отримання більш доступними, форми подачі інформації культурно прийнятними, знання та цінності, які в ній містяться, більш ефективні, корисні для держави, людини і суспільства. З огляду на це варто наполягати на ефективному функціонуванні механізмів міжсекторної взаємодії у сфері інформаційної безпеки, які формуються в межах публічного адміністрування. Організація його системи та міжсекторної взаємодії, що існує в Україні, базується на двох центрах публічної влади, з одного боку, на органах виконавчої гілки влади в класичному розумінні й місцевого самоврядування, а з другого – на громадських об'єднаннях і населенні, яке долучається до формування та реалізації державної без пекової й інформаційної політики. Дану особливість пов`язано з тим, що обидва центри відповідальні за соціально-економічний розвиток окремо взятих територій і держави в цілому (див. Стратегію сталого розвитку «Україна – 2020» [29]).

Практика свідчить, що діяльність, у тому числі із взаємодії, таких інституцій подекуди не відповідає новим умовам і потребам розвитку суспільства, його очікуванням, подекуди гальмує проведення соціально-економічних та політичних перетворень і, як наслідок, не забезпечує безпеку «з боку соціуму», не сприяє поліпшенню іміджу України на міжнародній арені, реалізації політики інтеграції, а також погіршує якість послуг, які надаються населенню. Серед причин цього слід виокремити прагнення органів влади до її абсолютизації, незавершеність формування механізму розподілу сфер діяльності (а точніше компетенції) державних і самоврядних інституцій,

нетраспарентність (непрозорість) управлінських відносин, низьку активність громадськості та представників бізнесу в забезпеченні соціальної, економічної й інформаційної безпеки тощо.

Питання міжсекторної взаємодії в процесі становлення держави знаходять відгук у працях багатьох науковців (В. Вакуленка, М. Гончаренко, Т. Дерун, О. Коротич, Л. Костіної, А. Кузнецова, О. Лебединської, Н. Мирної, М. Орлатого та ін. [17; 18]). Проте більшість робіт стосується окремих аспектів, залишаючи поза увагою комплексну характеристику міжсекторної взаємодії щодо забезпечення інформаційної безпеки. Так, деякі питання формування державно-владних і самоврядних структур з оптимально забезпеченим рівнем повноважень порушуються в працях А. Лелеченко [19], А. Матвієнко досліджує зміст деконцентрації та децентралізації в державному управлінні [20], Р. Сметанін та Ю. Торохтій порушують питання взаємодії при аналізі делегування повноважень органів держвлади [30], С. Арнштейн досліджує форми та рівні співпраці державних органів і громадськості [31]. Як справедливо зауважує цей автор, рівні та форми міжсекторної взаємодії різні, кожен з яких позначає свій ступінь корисності й реальної можливості включення останньої в діяльність державної влади. Учена вважає, що публічні агенти приймають участь у підготовці правових документів, реалізації програм загальнонаціонального, регіонального або місцевого значення, виконанні соціальних замовлень, а також можуть здійснювати нагляд за роботою органів влади [там само]. Агрегаторами й артикуляторами індивідуальних і колективних рішень є такі актори: громадсько-політичні об’єднання, громадські ради та ін. Разом з тим, в Україні з цього приводу ще недостатньо наукових розробок, адже довгий час актори не визнавалися за виразників соціальних рішень. Завдання цих акторів полягає в тому, що вони беруть безпосередню участь у політичному процесі, лобіюють інтереси, які мають стратегічний характер, впливають на наслідки прийняття управлінських рішень своєю участю, чим забезпечують соціально-політичну стабільність, ієрархізоване функціонування влади та повсюдність упровадження е-

урядування [23–24].

Зважаючи на це, можемо стверджувати, що механізми міжсекторної взаємодії щодо забезпечення інформаційної безпеки відзначаються вже не суб'єкт-об'єктними, а суб'єкт-суб'єтними відносинами. Їх учасниками є певні актори – публічно-владні інституції (державні, самоврядні та громадські), узаємодія яких має бути спрямована на задоволення інтересів кінцевих користувачів – жителів окремих регіонів, які, з іншого боку, становлять усе населення України й уможливлюють її інформаційну безпеку.

Розробка заходів, які необхідно зробити державі для забезпечення інформаційної безпеки громадян, суспільства і держави, залишається одним із найважливіших пріоритетів державного управління інформаційною сферою держави. Застосування нових інформаційно-комунікаційних технологій у державному секторі поки здійснюється в значній мірі в інтересах забезпечення діяльності самих державних структур (побудова інформаційних систем, баз даних, локальних і корпоративних мереж, впровадження електронного документообігу тощо). Так, сьогодні багато як державні, так і бізнес структури створюють потужні інформаційні системи — ситуаційні центри, інформаційно-аналітичні центри тощо. Їх поява часто носить несистемний характер, а де-то й просто є віянням моди. Не визначено цілі, завдання, механізми і архітектура системи управління, в інтересах якої вони повинні працювати. Так, завантаженість та ефективне використання таких інформаційних систем зводиться до мінімуму за причини того, що функціонують вони в значній мірі в автономному режимі. У питаннях міжвідомчої взаємодії, як правило, відсутні взаємопов'язані інформаційні завдання та технології підтримки прийняття рішень, що не дозволяють об'єднати такі інформаційні системи в єдину мережу.

Такі ж проблеми мають місце і на регіональному рівні і, як наслідок, управлінські рішення приймаються в обхід створених інформаційних систем, що стоять адміністративно й організаційно-технологічно осібно в стороні, на основі наявної не завжди повної інформації, а взаємодія втрачає повноту і

оперативність. У розвинених країнах уже понад 15 років ведуться роботи щодо створення забезпечення відкритості в роботі органів влади і зворотного зв'язку. Лідерство в цій сфері належить США, їх головний урядовий портал – FirstGov – об'єднує в собі близько 30 млн урядових Web-сторінок з метою забезпечення більш ефективного пошуку необхідної інформації і надання державних послуг громадянам країни [12; 32]. Як показує українська практика створення «е-уряду», систематичність у забезпеченні інформаційної безпеки, сьогодні спостерігається значне викривлення у бік надання інформаційних послуг (довідкова інформація, стрічки новин тощо), менше уваги приділяється механізмам активного спілкування з громадянами, віддаленість від них органів спеціальної компетенції [23]. Створені в «Internet» офіційні сайти органів державної влади часто мають недостатнє інформаційне наповнення і не завжди підтримують надання державних послуг. Усе це свідчить про те, що існує реальна потреба в науково-теоретичному обґрунтуванні можливостей і напрямів використання ІКТ у системі державного управління [24].

Отже, міжсекторна взаємодія в означеній сфері має відбуватись із дотриманням таких вимог:

1) цілі спільної діяльності повинні бути зрозумілими, прозорими і чітко визначеними як для представників державної, регіональної та місцевої влади, так і для громадськості;

2) визначення рівнів і меж спільного вирішення проблем інфобезпеки;

3) залучення та участь громадськості повинно бути гнучким і відбуватися з урахуванням інтересів громадян і суспільно-політичних процесів, що повинно включати освіту населення з питань діяльності влади і законів, на яких ця діяльність базується;

4) процес формування та реалізації державної політики повинен відбуватися із дотриманням принципу ієрархічності, системності та публічності (тобто бути чітко зрозумілим і відкритим для громадськості).

РОЗДІЛ 3
НАПРЯМКИ ВДОСКОНАЛЕННЯ ОРГАНІЗАЦІЙНО-ПРАВОВИХ МЕХАНІЗМІВ ДЕРЖАВНОЇ ПОЛІТИКИ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

3.1. Шляхи вдосконалення організаційно-правового забезпечення державної політики у сфері інформаційної безпеки

На підставі аналізу стану організаційно-функціонального та правового забезпечення державної політики у сфері інформаційної безпеки можемо наполягати на необхідності створення не тільки інформаційного простору, а й стійкої організаційно-інформаційної мережі та системи, об'єднані в *державну інформаційно-комунікативну інфраструктуру* (ДІКІ). Вона передбачає запровадження моделі міжсекторної взаємодії щодо забезпечення інформаційної безпеки та розширення спектру функцій сектору щодо забезпечення інформаційної безпеки Міністерства інформаційної політики України, а також її громадської ради із визначення й оцінки ризиків і загроз інформаційній безпеці України (рис. 1). Формування ДІКІ – завдання в основному технологічне, міжгалузевого характеру, досягнення якого повинно відбуватися програмними заходами та методами управління (організації, координації, аналізу, моніторингу, прогнозування тощо), а також шляхом уніфікації, яка характерна для міжсекторної взаємодії.

Запропонована інфраструктура передбачає наявність інформаційно-аналітичних центрів у регіонах, що можуть спочатку функціонувати в межах різних структур, підрозділів сфери державного регіонального управління загальної компетенції (тобто місцевих державних адміністрацій). Створення таких центрів – перший крок, наступний передбачає створення міжвідомчої інформаційної системної мережі спеціальної компетенції. Основна її мета – це інтеграція інформаційних ресурсів за рахунок створення сховищ, банків даних

документованої інформації й отримання на їх основі аналітичних і зведених даних про хід реалізації соціально-економічних, безпеково орієнтованих програм, у т. ч. щодо інформатизації, демократизації тощо. Система узгодженої інформаційної взаємодії дозволить об'єднати існуючі бази, банки даних в органах державної влади регіонального рівня та іншими структурними підрозділами системи державного управління центрального рівня (зокрема Міністерства інформаційної політики України). Перспективи розвитку інноваційних систем держуправління (Центр – регіон) багато в чому пов'язані з її інформатизацією, з повсюдністю використання ІКТ при вирішенні завдань органів державного управління, його деконцентрацією.

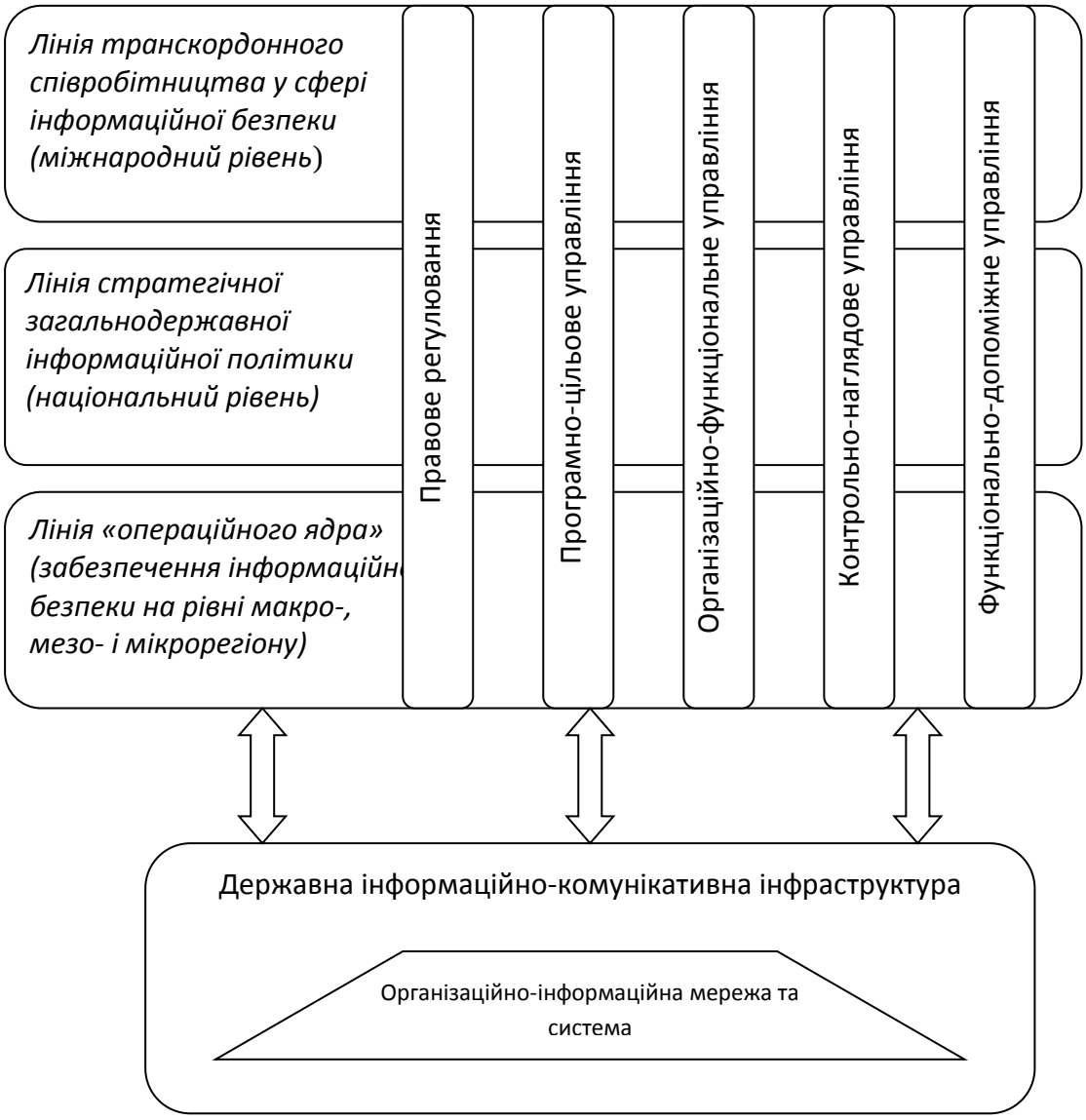

Рис.1. Модель міжсекторної взаємодії щодо забезпечення інформаційної безпеки. *Джерело:* авторська розробка.

Аналіз наявних даних свідчить про те, що кожне з органів і відомств, які належать до системи державного управління (Центр – регіон), йде своїм шляхом при зборі, обробці, зберіганні та використанні інформації. Кожен орган державної влади вирішує проблеми інформаційного забезпечення своєї діяльності самостійно, без належної взаємодії з іншими інституціями, що виключає можливість виявлення фактори взаємовпливу, відображення динаміки проблемних змін в залежності від часу. Отже, інформація не може бути повною й об'єктивною, якщо ускладнює прийняття ефективних державноуправлінських рішень і їх аналіз, а, відтак, не гарантує необхідний рівень інформаційної безпеки держави, регіонів і суспільства. Багатофакторність і необхідність урахування цих обставин вимагають відповідного рівня структуризації інформації, створення міжвідомчої інформаційної мережі, що відбиває стан системи державного управління, її інформаційного поля, що можливо, на наш погляд, за допомогою формування державної інформаційно-комунікативної інфраструктури.

Існуюча практика збору інформації, особливо статистичних даних (саме на цьому рівні значною мірою знаходиться використання інформаційних технологій) не відповідає завданням державного управління на сучасному етапі суспільного розвитку. У статистичній інформації не завжди узгоджені між собою формати, розмірність показників різних розділів, галузей, підрозділів статистичних форм звітності. Одні можуть бути представлені в абсолютному вигляді з певною розмірністю, інші – у відсотках тощо [2; 5].

Багатоаспекність державноуправлінських проблем у сфері забезпечення прозорості, відкритості, повноти й достовірності інформації, що чекають свого вирішення, вимагає координації діяльності, посилення взаємодії державних структур і різних неурядових, громадських організацій, деконцентрації державної влади. Це має дозволити забезпечити оперативність й ефективність державноуправлінських рішень, стійкість розвитку регіонів, інформаційну безпеку держави, суспільства й особистості.

3.2. Обґрунтування новітніх функціоналів системи державного управління у сфері інформаційної безпеки

Слід зазначити, що існуючі сьогодні західні схеми побудови управління державою за допомогою ІКТ, формування інформаційної політики та безпеки повністю не адаптовані до українських реалій, тому вимагають ґрунтовного аналізу і модифікації. Для цього вітчизняні науковці займаються розробкою проблем «електронної демократії» і «е-уряду». Не заглиблюючись у їх зміст у межах цього дослідження, підкреслимо, що основною метою е-уряду є підвищення рівня участі громадськості, за рахунок нетрадиційних форм, із застосуванням ІКТ [23, с. 360; 24, с. 99]. У межах реалізації цих форм має відбуватися підвищення відповідальності в процесі прийняття рішень, а також ефективна комунікація між владними структурами і громадянами. Сучасна е-демократія й управління допускають не тільки наявність високого рівня соціально-економічного розвитку, плюралістичність традицій політичної участі й управління, але широке й ефективне використання державно-політико-комунікативних технологій і новітніх форм узаємодії [там само].

Удосконалення організаційно-функціонального забезпечення державного управління у сфері інформаційної безпеки України покликано сприяти уникненню дублювання функцій державного управління, посиленню контролю та відповідальності з боку держави і громадськості в цій сфері, адаптації механізму формування та реалізації державної безпекової й інформаційної політики до передових світових практик. Вони передбачають наближення влади до населення, публічність процесу прийняття управлінських рішень, що дає можливість зробити більш точним його аналіз з метою коригування й оптимізації своєї роботи; викликає в громадськості відчуття причетності до творення та реалізації політики; населення починає сприймати її як партнера, помічника, а не як щось відокремлене та вороже, тим самим, забезпечуючи інформаційну безпеку в державі [31–33]. Це, на нашу думку, може допомогти

більш чіткому визначенню основних функцій і завдань органів державної влади в центрі та регіонах під час її забезпечення й організації процесу залучення громадськості. Для цього необхідно розробити і реалізувати державну довгострокову програму створення основ інформаційного суспільства, яка може стати об'єднуючим ідейним початком для України, оскільки поряд з концепцією моделі стійкого її розвитку дає цільову спрямованість суспільного розвитку і на цій основі можуть бути визначені конкретні шляхи досягнення цілей, пов’язаних з інформаційною безпекою України.

У продовження відзначимо, що вдосконалення потребує, насамперед, організаційно-функціональне забезпечення роботи Міністерства інформаційної політики України. Ураховуючи напрацювання А. Михайлова [21] і, оцінюючи результати перспектив забезпечення інформаційної безпеки України в умовах глобалізації, робимо висновок, що воно та розвиток її інформаційного суспільства відбуваються в межах формування публічної *системи* інформаційної безпеки. Для поступального переходу України на новий етап розвитку необхідно забезпечити умову, при якій її загальнодержавні інтереси будуть невід'ємною складовою частиною інтересів регіонального інформаційного співтовариства. Це можливо, насамперед, за умови дієвої деконцентрації повноважень і міжінституційної взаємодії – центральних і регіональних державних органів (загальної та спеціальної компетенції), тобто шляхом узгодження їх напрямків діяльності у сфері інформаційної безпеки. Реалізація їх можливостей – питання адекватної політики і своєчасних публічно-управлінських рішень. Для цього Міністерство інформаційної політики України, як інші ЦОВВ, що виконують специфічні функції державного управління в окремій сфері та галузі економіки, повинно мати розгалужену, ієрархізовану та найбільш наближену до об’єкта впливу організаційну будову. Ідеться, з одного боку, про вдосконалення *основної* організаційної будови Міністерства інформаційної політки України, тобто про необхідність створення регіональних структурних підрозділів і представництв,

як оперативного ядра, найбільш наближеного до вияву та нейтралізації загроз інформаційній безпеці України на регіональному рівні. А з другого боку, про вдосконалення *функціонально-допоміжної* організаційної будови Міністерства інформаційної політки України, тобто про необхідність створення регіональних громадських рад при структурних його регіональних представництвах.

Паралельно слід здійснити таке: місцеві державні адміністрації, як органи виконавчої влади загальної компетенції, повинні бути відсторонені від виконання невластивих їм функцій, що дозволить комплексно й ефективно підійти до їх реалізації, уникнути розпорошеності, неперсоніфікованості відповідальності тощо.

Зважаючи на вищевикладене, уважаємо, що вимагає вдосконалення положення про типову структуру системи органів виконавчої влади спеціальної компетенції у сфері інформаційної безпеки, наразі представленої Міністерством інформаційної політики України, в якому слід визначити перелік обов'язкових підсистем:

1) організаційно-функціональних підсистем (основних і функціонально-допоміжних);

2) інформаційних підсистем (наприклад, електронний документообіг, електронний цифровий підпис, збір, аналіз, пошук і захист інформації, електронна комерція, електронний архів, доступ до Інтернету тощо);

2) інформаційних ресурсів тощо [25].

Наявність такого оновленого положення дозволить виробити критерії об'єктивної оцінки рівня інформатизації й ефективності діяльності органів виконавчої влади спеціальної компетенції у сфері інформаційної безпеки як на регіональному рівні, так і на загальнодержавному.

ВИСНОВКИ

1. *З'ясовано* зміст інформаційної безпеки, який правомірно розглядати в межах дихотомічності *інформаційної сфери*, елементами якої визнано сукупність інформації, засобів її виробництва, обробка та зберігання, інформаційний простір й інфраструктура, суб'єктів, що здійснюють збір, формування, розповсюдження і використання інформації, а також *системи державного управління,* виникаючих при цьому державно-владних відносин. Така система передбачає здійснення цілеспрямованого й організуючого впливу керованої підсистеми (держави) на сферу інформаційної безпеки шляхом застосування правового й організаційного інструментарію, який становить підґрунтя для класифікації механізмів державної політики в означеній сфері.

2. *Під час аналізу* дії правового й організаційного механізмів державної політики у сфері інформаційної безпеки в Україні *встановлено* таке:

1) відсутня єдина інфраструктура зв'язку й інформації державних органів влади, побудована на єдиних стандартах і платформах, ускладнюючи тим самим процес своєчасного впровадження сучасних технологій;

2) діючі інформаційні системи органів державної влади були розроблені і введені в експлуатацію в різний час, що й зумовило несумісність програмно-технічних рішень сьогодні;

3) вітчизняна правова база відзначається розпорошенням і дублюванням напрямків діяльності органів виконавчої влади загальної та спеціальної компетенції щодо забезпечення інформаційної безпеки тощо.

3. Зважаючи на це, *визначено* шляхи вдосконалення організаційно-правових механізмів державної політики у сфері інформаційної безпеки України, які передбачають адаптацію в Україні світового досвіду (зокрема, США) щодо створення єдиної державної інформаційно-комунікаційної інфраструктури. Вона, з одного боку, передбачає формування стійкої організаційно-інформаційної мережі та системи, а з другого – покликана

забезпечити системне «виробництво – споживання – захист» інформаційних і комунікаційних засобів, продуктів і послуг. При цьому *уточнено* модель міжсекторної взаємодії щодо забезпечення інформаційної безпеки.

4. На підставі аналізу стану організаційно-функціонального та правового забезпечення державної політики у сфері інформаційної безпеки *обґрунтовано* новітні функціонали системи державного управління, покликані забезпечити комплексне дотримання основоположних державноуправлінських принципів. Їх урахування *дозволило запропонувати* напрямки вдосконалення основної та допоміжно-функціональної організаційної будови Міністерства інформаційної політики України. Це можливо шляхом формування його представництв на регіональному рівні, як установ з узгодженим розподілом повноважень і сфер відповідальності, а також створення регіональних громадських рад при них.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Аналітичний огляд проблем інформаційного й електронного права в Україні [Електронний ресурс] // Сайт “АМВ” group. – Режим доступу: http://www.itsway.kiev.ua/index.php?language=ru&main_managemen=about&managemen=eGov_Zak.

2. Бєлай С. В. Державні механізми протидії кризовим явищам соціально-економічного характеру: теорія, методологія, практика : монографія / С. В. Бєлай. – Х. : Національна акад. НГУ, 2015. – 349 с.

3. Брижко В. М. Інформаційне суспільство. Дефініції / В. М. Брижко, О. М. Гальченко, В. С. Цимбалюк, О. А. Орєхов, А. М. Чорнобров. – К., 2002. – 220 с.

4. Васильєва О. І. Трансформація регіонального управління в умовах реформування владних відносин в Україні : автореф. дис. ... д-ра наук з держ. упр. : 25.00.02 / О. І. Васильєва ; НАН України, Рада по вивч. продуктив. сил України. – К., 2010. – 38 с.

5. Вербицький О. В. Поняття соціальної напруженості та роль держави в управлінні нею й інформаційною безпекою / О. В. Вербицький // Проблеми управління соціальним і гуманітарним розвитком : матеріали наук.-прак. конф. (01.12.2017 р.). – Дніпро, 2017. – С. 47–49.

6. Глобалізація і безпека розвитку : монографія / О. Г. Білорус, Д. Г. Лук’яненко та ін. ; кер. авт. колективу і наук. ред. О. Г. Білорус. – К. : КНЕУ, 2001. – 733 с.

7. Дзюндзюк В. Б. Ефективність діяльності публічних організацій / В. Б. Дзюндзюк ; Укр. акад. держ. упр-ня при Президентові України, Харк. регіон. ін-т. – Х. : Вид-во ХарРІ УАДУ «Магістр», 2003. – 236 с.

8. Древаль Ю. Д. Безпека особистості як фактор сучасних державно-управлінських відносин [Елеткронний ресурс] / Ю. Д. Древаль // Наукові записки Інституту законодавства Верховної Ради України. – С. 123–127. – Режим доступу: http://instzak.rada.gov.ua/instzak/doccatalog/document?id=72940.

9. Домбровська С. М. Механізми інформаційної безпеки як складові державної безпеки України / С. М. Домбровська // Державне управління науково-освітнього забезпечення підготовки конкурентоспроможних фахівців у сфері цивільного захисту : матеріали Всеукраїнської наук.-практ. конф. / за заг. ред. В. П. Садкового. – Х., 2015. – С. 282–286.

10. Енциклопедія державного управління: у 8 т. / Нац. акад. держ. упр. при Президентові України ; наук.-ред. колегія : Ю. В. Ковбасюк (голова) та ін. – К. : НАДУ, 2011. Т. 1 : Теорія державного управління / наук.-ред. колегія : В. М. Князєв (співголова), І. В. Розпутенко (співголова) та ін. – 2011. – 748 с.

11. Енциклопедія державного управління: у 8 т. / Нац. акад. держ. упр. при Президентові України ; наук.-ред. колегія : Ю. В. Ковбасюк (голова) та ін. – К. : НАДУ, 2011. Т. 2 : Методологія державного управління / наук.-ред. колегія : Ю. П. Сурмін, П. І. Надолишній та ін. – 2011. – 692 с.

12. Іщенко В. М. Міжнародний досвід упровадження електронного урядування [Електронний ресурс] / В. М. Іщенко // Держава та регіони, 2012. – № 4. – Режим доступу: http://pa.stateandregions.zp.ua/archive/4_2012/5.pdf.

13. Карпенко О. В. Механізми формування та реалізації сервісно-орієнтованої державної політики в Україні : автореф. дис. ... д-ра наук з держ. упр. : 25.00.02 / О. В. Карпенко ; Нац. акад. держ. упр-ня при Президентові України. – К., 2016. – 39 с.

14. Колот А. Соціальна згуртованість як доктрина забезпечення стійкості розвитку суспільства в умовах глобальних викликів / А. Колот // Україна: аспекти праці, 2009. – № 7. – С. 11–19.

15. Корженко В. В. Теоретико-методологічні засади державного управління: формування понятійного апарату: метод. рек. / авт. кол. В. В. Корженко, В. В. Говоруха, О. Ю. Амосов та ін. – К. : НАДУ, 2009.

16. Косевцов В. Національна безпека України: проблеми та шляхи реалізації пріоритетних національних інтересів : монографія / В. Косевцов, І. Бінько - К. : НІСД, 1996. – 53 с.

17. Коротич О. Б. Державне управління регіональним розвитком

України : монографія / О. Б. Коротич. – Х. : «Магістр», 2006. – 220 с.

18. Кузнецов А. О. Інноваційні технології в державному регулюванні соціально-економічного розвитку регіону : автореф. дис... канд. наук з держ. упр.: 25.00.02 / А. О. Кузнецов ; Нац. акад. держ. упр. при Президентові України, Харк. регіон. ін-т держ. упр. – Х., 2006. – 20 с.

19. Лелеченко А. П. Децентралізація системи державного управління в Україні: теоретико-методологічний аналіз : автореф. дис... канд. наук з держ. упр. : 25.00.01 / А. П. Лелеченко ; Нац. акад. держ. упр. при Президентові України. – К., 2006. – 20 с.

20. Матвієнко А. С. Політико-правові засади децентралізації влади в контексті адміністративної реформи в Україні : автореф. дис... канд. політ. наук : 23.00.02 / А. С. Матвієнко ; Ін-т держави і права ім. В.М. Корецького НАН України. – К., 2010. – 20 с.

21. Михайлов А. О. Оптимізація причинно-наслідкового зв’язку функцій держави та механізмів державного управління в Україні : автореферат дис. ... канд. наук з держ. упр. : 25.00.02 / А. О. Михайлов ; Акад. муніц. управління. – К., 2015. – 20 с.

22. Никитин В. А. Проблемы становления публичной политики в Украине / В. А. Никитин // Публичная полтика – 2006 : сб. ст. / под ред. А. Ю. Сунгурова. – СПб. : Норма, 2006. – 32 с.

23. Опанасенко Я. О. Електронне врядування як складова державного управління соціально-економічним розвитком регіонів / А. Л. Помаза-Пономаренко, Я. О. Опанасенко // Діяльність органів публічної влади щодо забезпечення стабільності та безпеки суспільства : матеріали Міжнарод. наук.-практ. конф., м. Суми, 22 березня 2016 р. – Суми : Сумський державний ун-тет. – С. 360–363.

24. Опанасенко Я. О. Організаційно-правові засади електронного врядування в системі державного управління соціально-економічним розвитком регіонів / А. Л. Помаза-Пономаренко, Я. О. Опанасенко // Сучасні суспільні комунікації: проблеми, пріоритети та першочергові завдання в

євроінтеграційних процесах : матеріали міжнар. конф. (м. Хелм, Польща, 27 листопада 2015 р.). – Хелм : Вид-во ВШМВСК, 2016. – С. 98–103.

25. Опанасенко Я. О. Роль і місце організаційної, соціальної й інформаційної складових у реалізації державної регіональної політики в умовах невизначеності регіонів / А. Л. Помаза-Пономаренко, Р. Т. Лукиша, Я. О. Опанасенко // Вісник Національного університету цивільного захисту України (Серія: Державне управління), 2016. – № 1 (4). – С. 203–209.

26. Офіційний веб-сайт Міністерства інформаційної політики України [Електронний ресурс]. – Режим доступу: http://mip.gov.ua/ru/.

27. Почепцов Г. Інформаційна політика : навч. посіб. / Г. Почепцов, С. Чукут. – К. : Вид-во УАДУ, 2002. – 88 с.

28. Про місцеві державні адміністрації [Електронний ресурс] : Закон України від 1990 р. (у редакції від 16.04.2017 р.). – Режим доступу: http://zakon3.rada.gov.ua/laws/show/586-14.

29. Про Стратегію сталого розвитку «Україна – 2020» [Електронний ресурс] : Указ Президента України від 12.01.2015 р. № 5/2015. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/5/2015#n10.

30. Сметанін Р. В. Управління процесом децентралізації державної влади в Україні : автореф. дис... канд. наук з держ. упр. : 25.00.04 / Р. В. Сметанін ; Донец. держ. ун-т упр. – Донецьк, 2010. – 19 с.

31. Arnstein S. A ladder of citizen participation in the USA / S. Arnstein // Journal of the Royl Town Planning Institute. – 1971. – Vol. 57. – № 4. – pp. 176–182.

32. The Global Information Infrastructure: Agenda for Coohtration / R. Brown, L. Irving, A. Prfbhakar, S. Katzen. – 1995. – 680 p.

33. Pitter A. Steinbuch. Projekt organization und management auf dem Gebiet der Informationssicherheit, 1998. – № 1. – S. 24 –25.