УДК 351.865

Лук'янчук Руслан Валерійович,
здобувач, Інститут законодавства Верховної Ради України, 04053, Київ, пров. Несторівський, 4, тел.: 0674443103, e-mail: max-felix@ukr.net

Лукьянчук Руслан Валерьевич,
соискатель, Институт законодательства Верховной Рады Украины, 04053, Киев, переулок Нестеровский, 4, тел.: 0674443103, e-mail: max-felix@ukr.net

Ruslan Valeriyovich Lukyanchuk,
Ph. D student, The Legislation Institute of the Verkhovna Rada of Ukraine, 04053, Kyiv, prov. Nestorivskiy, 4, tel.: 0674443103, e-mail: max-felix@ukr.net

ДЕЯКІ ПИТАННЯ РЕФОРМУВАННЯ СИСТЕМИ ДЕРЖАВНОГО УПРАВЛІННЯ У СФЕРІ ЗАБЕЗПЕЧЕННЯ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ: СУЧАСНИЙ ПОГЛЯД

Анотація. У статті досліджено сучасний стан та основні проблемні питання процесів реформування системи державного управління у сфері забезпечення кібербезпеки. Розкрито пріоритетні завдання реформування системи кібербезпеки з метою розбудови національної системи кібербезпеки відповідно до Положення Стратегії кібербезпеки України. Деталізовано, що актуальним напрямом забезпечення кібербезпеки залишається конструктивний розвиток державно-приватного партнерства з метою налагодження координації та взаємодії суб'єктів забезпечення кібербезпеки на державному рівні з приватним сектором та громадськими об'єднаннями. Доведено, що реформування системи державного управління кібербезпекою потребує впровадження спеціальних методів запобігання кібератакам, розробки галузевих стандартів та вимог щодо забезпечення кіберзахисту об'єктів інформаційної сфери, запровадження на підприємствах, установах та організаціях, що належатимуть до об'єктів критичної інфраструктури, міжнародного стандарту ISO/IEC 27032:2012. Встановлено, що трансформація системи державного управління у сфері забезпечення кібербезпеки потребує правового супроводження, організаційного й методичного забезпечення на національному рівні.

Ключові слова: реформування системи державного управління, сектор безпеки і оборони, державне управління у сфері забезпечення кібербезпеки, кіберпростір, кіберзахист, кіберзлочинність, національна система кібербезпеки, інформаційний суверенітет, інформаційно-комунікаційні технології, об'єкти критичної інформаційної інфраструктури, електронні комунікації.

НЕКОТОРЫЕ ВОПРОСЫ РЕФОРМИРОВАНИЯ СИСТЕМЫ ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ В СФЕРЕ ОБЕСПЕЧЕНИЯ КИБЕРНЕТИЧЕСКОЙ БЕЗОПАСНОСТИ: СОВРЕМЕННЫЙ ВЗГЛЯД

Аннотация. В статье исследовано современное состояние и основные проблемные вопросы процессов реформирования системы государственного управления в сфере обеспечения кибербезопасности. Раскрыто приоритетные задачи реформирования системы кибербезопасности с целью развития национальной системы кибербезопасности в соответствии с Положением Стратегии кибербезопасности Украины. Детализировано, что актуальным направлением обеспечения кибербезопасности остается конструктивное развитие государственно-частного партнерства с целью налаживания координации и взаимодействия субъектов обеспечения кибербезопасности на государственном уровне с частным сектором и общественными объединениями. Доказано, что реформирование системы государственного управления кибербезопасностью требует внедрение специальных методов предотвращения кибератакам, разработку отраслевых стандартов и требований по обеспечению киберзащиты объектов информационной сферы, внедрение на предприятиях, учреждениях и организациях, которые будут принадлежать к объектам критической инфраструктуры, международного стандарта ISO / IEC 27032: 2012. Установлено, что трансформация системы государственного управления в сфере обеспечения кибербезопасности требует правового сопровождения, организационного и методического обеспечений на национальном уровне.

Ключевые слова: реформирование системы государственного управления, сектор безопасности и обороны, государственное управление в области обеспечения кибербезопасности, киберпространство, киберзащита, киберпреступность, национальная система кибербезопасности, информационный суверенитет, информационно-коммуникационные технологии, объекты критической информационной инфраструктуры, электронные коммуникации.

SOME ISSUES OF MODERNIZATION THE SYSTEM OF PUBLIC ADMINISTRATION OF CYBER SECURITY PROVIDING: PRESENT-DAY IDEAS

Abstract. The article researched present state and key problem questions of processes of public administration reform of cyber security providing. The priority tasks of cyber security system reform which concern the development national system of cyber security according to the Strategy of cyber security of Ukraine

was fixed. The actual direction of ensuring cyber security remains a constructive development of public-private partnership with the aim to establish coordination and cooperation the subject of ensuring cyber security at the national level with the private sector and civil society organizations are detailed. It is proved that reform of public administration cyber security requires the introduction of special methods of preventing cyber-attacks, developing industry standards and requirements for object cyber information sphere, introduction of enterprises, institutions and organizations that belong to critical infrastructure, international standard ISO / IEC 27032: 2012. It was established that the modernization the system of public administration of cyber security providing requires a legal support, organizational and methodical provision at the national level.

Keywords: modernization the system of public administration, security sector, public administration of cyber security providing, cyber space, cyber protection, Cybercrime, the national cyber security, information sovereignty, information and communication technology, objects of critical information infrastructure, electronic communication.

Постановка проблеми. Упровадження інформаційно-комунікаційних технологій у повсякденному житті пересічних громадян та у процесах державного управління вбачається однією із фундаментальних основ розбудови демократичного суспільства. Існування сучасної моделі державного управління неможливе без надійних гарантій забезпечення безпекової політики з метою захисту національних інтересів в інформаційній сфері. Обов'язком політичного керівництва будь-якої держави світу є забезпечення безперешкодного та надійного доступу громадян і суспільства до безпечного кібернетичного середовища, шляхом впровадження й реалізації виваженої державної політики, спрямованої на мінімізацію наслідків будь-яких кібератак, кіберінцидентів та кіберзагроз, недопущення блокування спецслужбами іноземних держав або хакерськими групами діяльності стратегічно важливих інформаційно-комунікаційних мереж, електронних комунікацій, цілеспрямованих посягань на об'єкти національної критичної інформаційної інфраструктури.

За аналітичними матеріалами дослідницького центру "Juniper Research" до 2020 р. світовий ринок електронної комерції повинен перевищити 8 трлн дол., хоча у 2015 р. його обсяги склали 4,9 трлн дол. Прогнозується, що електронна комерція у багатьох аспектах залежатиме від стану захищеності цифрового банкінгу, оскільки із розвитком нових продуктів і послуг, пов'язаних з платежами он-лайн, в кіберпросторі виникатимуть все більше кібератак на них, про що свідчить аналіз результатів діяльності кіберзлочинців у 2015 р.

За таких умов ключовими тенденціями прогнозу розвитку ситуації у міжнародному кіберпросторі залишається: збільшення різноманіт-

них атак у кіберпросторі на окремі держави та елементи їхньої критичної інформаційної інфраструктури; посилення інформаційного протистояння у кіберпросторі; зростання загроз для соціальних мереж, втручання у функціонування бізнесу та промисловості, банківські та фінансові операції. Наслідком цих тенденцій є суттєве збільшення рівня контролю за користувачами мережі Інтернет, необхідність посилення регулювання на національному та міжнародному рівнях фінансово-економічної та інших видів діяльності в кіберпросторі.

Формування та розвиток інформаційного простору держави повинні спрямовуватися передусім на об'єднання, інтеграцію інформаційно-телекомунікаційних джерел з метою їх взаємодії, роботи в єдиних форматах і стандартах для забезпечення інформаційної підтримки прийняття рішень у різноманітних сферах управління [18, с. 9].

З огляду на масштабність і динамічність проникнення інформаційно-телекомунікаційних технологій у всі сфери життєдіяльності особи, суспільства та держави, в процесі інтеграції нашої країни до глобальної інформаційної цивілізації проблема забезпечення кібернетичної безпеки залишається актуальною й такою, що потребує негайного та ефективного розв'язання.

Сучасна геополітика стимулює діяльність державного апарату, спрямовану на пошук ефективної моделі оперативного управління кібербезпекою та підвищення ролі і значення реалізації заходів щодо розбудови її національної системи. За таких умов саме гарантування інформаційного суверенітету у кіберпросторі — важливе та відповідальне завдання політичного керівництва будь-якої держави світу в контексті реалізації заходів, спрямованих на забезпечення кібербезпеки, у зв'язку з чим, в рамках діяльності центральних органів державної влади, повинні прийматися та реалізовуватися скеровані заходи, спрямовані на: забезпечення надійного кіберзахисту критичної інформаційної інфраструктури, особливо в умовах кризових ситуацій, надзвичайного або воєнного стану; моніторинг та оцінку стану кіберпростору; розвиток потенціалу сектору безпеки і оборони у сфері забезпечення кібербезпеки; розбудову сучасної національної системи кібербезпеки, посилення відповідальності за заподіяння шкоди державним інтересам у кіберпросторі; вчинення правопорушень у сфері інформаційної безпеки та боротьби з кіберзлочинністю.

Масштабні вияви кібершпіонажу, підвищення активності терористів та шахраїв у глобальній мережі Інтернет, посилення заходів регулятивної діяльності, з метою підвищення контролю над використанням кіберпростору на міжнародному рівні, потребують більш активного залучення держави та її компетентних органів до діяльності щодо гарантування безпеки у кіберпросторі.

Крім того, про тенденцію до збільшення ролі і значення кібербезпеки в майбутньому свідчать й відповідні оприлюднені фінансові звіти провідних гігантів комп'ютерної індустрії. Так, за версією міжнародного видання "Forbes", у 2015 р. ринок кібербез-

пеки був оцінений у 75 млрд дол., а у 2020 р. прогнозується кардинальне збільшення його вартості до 170 млрд дол., що свідчить про необхідність розробки та вдосконалення механізмів забезпечення кібербезпеки з урахуванням викликів та загроз сучасності.

Зазначене дає підстави стверджувати, що необхідним є висвітлення проблемних питань, які доцільно вирішити в рамках реформування системи державного управління щодо забезпечення кібербезпеки з метою гарантування інформаційного суверенітету.

Аналіз останніх досліджень і публікацій. Пошук оптимальної моделі вдосконалення системи державного управління інформаційними ресурсами певною мірою здійснювали у своїх наукових працях: В. В. Антонюк [1], С. Г. Бублик [2], М. А. Будник [3], Ю. П. Бурило [4], В. І. Гурковський [7], Ю. В. Ковбасюк [8], Ю. В. Нестеряк [12], С. Г. Соловйов [16], О. В. Соснін [17] та ін. Розробку концептуальних засад забезпечення кібербезпеки проводили: В. Л. Бурячок [5], О. О. Грицун [6], Д. В. Дубов [9], А. І. Марущак [11], В. В. Петров [13], В. П. Шеломенцев [19].

Проте жоден із зазначених науковців у своїх дослідженнях не розглядав окремі питання реформування системи державного управління у сфері забезпечення кібербезпеки, що свідчить про актуальність обраного автором наукового напряму.

Однією зі сфер реформування в Україні є її система державного управління [3, с. 50]. Основними завданнями державного управління залишаються: оптимізація державного управління; ефективність та результативність вибору державної політики; створення дієвої організації державного управління як на центральному, так і на місцевому рівнях; належне кадрове забезпечення та створення сучасної системи підготовки та перепідготовки управлінського персоналу; достатній рівень фінансування сфери державного управління; запровадження ефективного механізму боротьби з корупційними проявами тощо [14, с. 380].

Проте необхідно констатувати, що аналіз наукової літератури, періодичних видань, вітчизняних нормативно-правових актів свідчить, що проблематика реформування системи державного управління саме у сфері забезпечення кібербезпеки опрацьована ще й досі не в повному обсязі.

Навіть практична реалізація положень Стратегії кібербезпеки України, прийнятої у березні 2016 р. [20], логічно передбачає внесення коректив та суттєвої оптимізації формату діяльності суб'єктів забезпечення кібербезпеки, складових елементів системи державного управління кіберзахистом об'єктів критичної інформаційної інфраструктури.

Зазначене демонструє необхідність визначення та деталізації проблемних питань сучасності в контексті реформування системи державного управління забезпечення кібербезпеки як наукової проблеми.

Мета статті — дослідити проблемні питання реформування системи державного управління кібер-

безпекою з урахуванням базових положень Стратегії кібербезпеки України, визначити шляхи його вдосконалення.

Виклад основного матеріалу. Система державного управління, що існує на сьогодні в Україні, незважаючи на неодноразові спроби її реформування, має рудименти командно-адміністративної системи управління, що ґрунтується на невиправданій централізації функцій і повноважень. При цьому основними причинами такого стану залишається відсутність політичної волі правлячої еліти до зміни цієї системи, внутрішній опір змінам у середині системи державного управління, фрагментарний підхід до реформування (спроби точкових змін), відсутність координації між різними ініціативами щодо реформування сфери державного управління.

Також незавершеність реформування державного управління є одним із джерел корупції, зумовлює низькі міжнародні рейтинги та конкурентоспроможність нашої держави, у тому числі в міжнародному кіберпросторі.

Варто зазначити, що реформи системи державного управління відбулися у багатьох країнах світу з метою трансформації й модернізації життєдіяльності усього суспільства. Зарубіжний досвід свідчить, що ефективне реформування системи державного управління вимагає у тому числі здійснення реалізації послідовної антикорупційної політики завдяки обмеженню контрольно-регуляторних функцій держави; мотивацію працівників державних органів до сумлінної праці; забезпечення невідворотності покарання за корупційні правопорушення.

Доктор наук з державного управління А. Попок у своїй науковій статті, дослідивши позитивний іноземний досвід здійснення реформування державного управління, дійшов висновку, що перспективними напрямами вдосконалення державного управління в Україні мають бути: формування стабільної та ефективної його системи, професіоналізація державної служби, впровадження принципів децентралізації системи державного управління, сервісного адміністрування, корпоративізму, що сприятиме підвищенню продуктивності роботи державних установ, наближенню держави до громадян. При цьому, за його баченням, важливими чинниками підвищення ефективності, результативності державного управління мають бути: розвиток партнерства з приватним сектором, прозорість та відкритість діяльності організацій та установ державного сектору, удосконалення механізмів звітування, моніторингу й контролю [15, с. 19].

Положення Стратегії національної безпеки України, затвердженої Указом Президента України від 26 травня 2015 р. № 287/2015 [21], регламентують, що пріоритетами забезпечення кібербезпеки і безпеки інформаційних ресурсів виступають: розвиток інформаційної інфраструктури держави; розбудова системи забезпечення кібербезпеки, розвиток мережі реагування на комп'ютерні надзвичайні події (CERT); моніторинг кіберпростору з метою своєчасного виявлення, запобігання кіберзагрозам і їх нейтралізації; розвиток

спроможностей правоохоронних органів щодо розслідування кіберзлочинів; забезпечення захищеності об'єктів критичної інфраструктури, державних інформаційних ресурсів від кібератак, відмова від програмного забезпечення, зокрема антивірусного, розробленого у РФ; розвиток міжнародного співробітництва у сфері забезпечення кібербезпеки, інтенсифікація співпраці України та НАТО, зокрема в межах Трастового фонду НАТО для посилення спроможностей України у сфері кібербезпеки.

Одночасно положеннями зазначеного нормативно-правового акта задекларовано доцільність проведення реформування системи державного управління з метою її оптимізації, адаптації відповідно до стандартів ЄС, очищення влади від корупціонерів і агентури іноземних спецслужб, непрофесіоналів, політичної кон'юнктури, унеможливлення переважання особистих, корпоративних, регіональних інтересів над загальнонаціональними.

Як свідчить зарубіжний досвід, реформа державного управління складається із трьох основних складових: реформа державної (публічної) служби; реформа системи виконавчої влади; реформа системи та порядку надання адмінпослуг. Зазначимо, що в нашій державі стартувала лише реформа державної служби після ухвалення у Верховній Раді України 10 грудня 2015 р. оновленого Закону України "Про державну службу" [22].

Динамічний розвиток та безпека кіберпростору, запровадження електронного урядування, гарантування безпеки й сталого функціонування електронних комунікацій та державних електронних інформаційних ресурсів являють собою складові елементи державної політики у сфері розвитку інформаційного простору та становлення інформаційного суспільства в Україні, які також визначені як об'єкти реформування в рамках державного управління кібербезпекою.

За переконанням І. Костюка, перспективою вдосконалення державного управління в Україні повинно бути ефективне впровадження у практику сучасних концепцій державного управління в разі реалізації таких передумов: формування гнучкої, стабільної та ефективної системи органів виконавчої влади; децентралізація системи державного управління; розвиток партнерства з приватним сектором та багатоаспектна взаємодія з громадськістю; упровадження електронного врядування, професіоналізація державної служби [10, с. 40].

Проте практична реалізація процесів реформування державного управління не позбавлена недоліків та прогалин. Основною проблемою державного управління, наприклад, у сфері науково-технологічної діяльності, є функціональна нездатність існуючої системи державних органів влади протистояти глобальним технологічним викликам XXI ст. та недосконаліть чинної нормативно-правової бази [2, с. 153].

Ще однією проблемою залишається відсутність визначення з боку держави відповідальних посадових осіб за реалізацію пакету реформ у сфері державного управління, від-

сутність налагодженої координації та взаємодії державних органів з метою проведення функціонального аудиту та реорганізації "зайвих" структур, уникнення дублювання повноважень суб'єктів забезпечення кібербезпеки, інших міністерств та центральних органів виконавчої влади під егідою Кабінету Міністрів України та Національного координаційного центру кібербезпеки при РНБО України. Таким чином, реформування системи державного управління у сфері кібербезпеки неможливе без організаційного, методичного забезпечення та правового супроводження на національному рівні.

Аналіз положень Стратегії кібербезпеки України вказує, що сфера державного управління, оборонно-промисловий і транспортний комплекси, інфраструктура електронних комунікацій, сектор безпеки і оборони України стають все більш уразливими для розвідувально-підривної діяльності іноземних спецслужб у кіберпросторі. Зазначене свідчить про доцільність, в рамках організаційного забезпечення реформування системи державного управління кібербезпекою, об'єднання спільних зусиль усіх відповідальних структур — Міністерства оборони України, Державної служби спеціального зв'язку та захисту інформації України, Служби безпеки України, Національної поліції України, Національного банку України, розвідувальних органів з метою прискорення проведення їхньої функціональної оптимізації, впровадження організаційно-технічної моделі оперативного управління національною системою кіберзахисту, налагодження між вказаними суб'єктами механізмів оперативної та комплексної взаємодії, обміну інформацією у режимі реального часу з метою реагування на кіберзагрози та кіберінциденти, у тому числі й у напрямі запровадження заходів державної підтримки власних розробок кіберзброї. Також необхідним є, в рамках реформування, розподіл відповідальності сектору безпеки і оборони України за організацію планування та реагування на кризові ситуації у кіберпросторі.

На державному рівні актуальним питанням, в умовах реформування, також залишається координація та взаємодія суб'єктів забезпечення кібербезпеки з приватним сектором, промисловістю, громадянським суспільством, громадськими об'єднаннями з питань кіберзахисту.

Більшою мірою ці проблеми потребують вирішення або в інституційній, або нормативно-правовій площині, однак суттєва їх частина безпосередньо пов'язана із проблемою вироблення взаємної довіри у взаємовідносинах трикутника "держава — бізнес — громадяни" [9, с. 125].

Методичне забезпечення в контексті реформування передбачає розробку, за участю суб'єктів кібербезпеки та Національного координаційного центру кібербезпеки при РНБО України, комплексної системи показників, що охоплюють всі аспекти функціонування вітчизняного кіберпростору та надійного забезпечення його захисту від несанкціонованого втручання й нівелювання будь-яких інноваційних моделей кіберзагроз, включаючи розробку

галузевих індикаторів стану кібербезпеки з метою її оцінки та моніторингу.

Доцільним також є впровадження у практичну площину спеціальних методів запобігання кібератакам, зокрема, методів криптографічного захисту інформації з використанням нейромережевих технологій, інтелектуальних методів забезпечення кібербезпеки: методу інтелектуальної ідентифікації користувачів, методу ситуаційного аналізу стану кібербезпеки. Необхідним є розроблення галузевих стандартів та вимог щодо забезпечення кіберзахисту об'єктів критичної інформаційної інфраструктури тощо.

Розбудова національної системи кібербезпеки, як важливий стратегічний напрям реформування, неможлива без запровадження на підприємствах, установах та організаціях, що належатимуть до об'єктів критичної інфраструктури, ефективних систем менеджменту кібернетичної безпеки, проведення відповідних заходів для їхньої сертифікації, згідно з міжнародними стандартами, наприклад, ISO/IEC 27032:2012 "Information technology — Security techniques — Guidelines for cybersecurity" — підвищення кібербезпеки в глобальній мережі Інтернет. Завдяки використанню рекомендацій ISO/IEC 27032:2012 провайдери інтернет-послуг зможуть підвищити загальний рівень кібербезпеки, забезпечити кіберзахист ресурсів комп'ютерних мереж загального користування.

Правове супроводження реформування передбачає необхідність нормативного визначення базових дефініцій: "кібербезпека", "кіберзахист", "кіберпростір", "кіберзлочин", "кібератака" та єдиної термінології з питань забезпечення кібербезпеки, її гармонізацію з відповідним тезаурусом у сфері інформаційної безпеки. Важливим аспектом також залишається необхідність прискорення прийняття законопроекту "Про основні засади забезпечення кібернетичної безпеки України", доопрацьований варіант якого внесено на розгляд Верховної Ради України 14 квітня 2016 р.

Висновки. Забезпечення кібербезпеки України неможливе без реалізації заходів щодо виваженої державної політики на національному рівні. Стабільність та ефективність функціонування системи державного управління у сфері забезпечення кібербезпеки — стратегічна мета та ключове завдання реформаційних процесів, які тривають в нашій країні у всіх сферах життєдіяльності суспільства.

Поточний аналіз політичних та економічних процесів, які останнім часом відбулися у нашій країні, свідчить, що реформування системи державного управління, з метою прискорення розбудови національної системи кібербезпеки, має перманентний процес, триває досить повільно, без представленої сучасної концепції державного управління вказаною сферою. На жаль, ще й досі остаточно не розроблена комплексна поетапна Програма та План заходів на 2016 рік як із реалізації Стратегії кібербезпеки України, так і у сфері системи державного управління та її забезпечення в умовах

реформування органів виконавчої влади.

У контексті окресленої наукової проблеми необхідно вказати, що реформування системи державного управління є комплексним процесом, який передбачає сукупність організаційно-правових, фінансово-економічних, інформаційно-технічних заходів, реалізація яких повинна: запобігти зловживанням та корупції з боку посадових осіб компетентних органів, які опікуються питаннями кібербезпеки; удосконалити систему державного контролю за станом кібербезпеки; в рамках розвитку державно-приватного партнерства прискорити запровадження на промисловому та національному рівнях міжнародного стандарту ISO/IEC 27032:2012, консолідувати у зазначеному контексті зусилля державних та правоохоронних органів, структур приватного сектору, підприємств та установ різних організаційно-правових форм; сприяти розвитку потенціалу сектору безпеки і оборони у сфері забезпечення кібербезпеки; провести комплексну оцінку стану забезпечення кібербезпеки; удосконалити систему та структуру суб'єктів забезпечення кіберзахисту, провести оптимізацію та конкретизацію їхніх повноважень та пріоритетних завдань, визначити сфери відповідальності; створити ефективну систему аналізу сучасних кіберзагроз, впровадити ефективні технології та сучасні методи формування кадрового потенціалу суб'єктів забезпечення кібербезпеки, підвищити результативність та професіоналізм службової діяльності співробітників відповідальних державних органів, забезпечити стабільність та ефективність оперативного державного управління кібербезпекою.

Зазначимо, що трансформація системи державного управління кібербезпекою в умовах реформування неможлива без організаційного та методичного забезпечення, правового супроводження відповідних процесів на національному рівні.

Окрім зазначених проблемних питань реформування системи державного управління кібербезпекою, самостійними напрямами перспективних досліджень, в рамках науки державного управління, на наш погляд, можуть бути: державні концепти створення ефективного управління сектором безпеки і оборони як цілісної функціональної системи забезпечення кібербезпеки в умовах реформаційних процесів; шляхи вдосконалення фінансово-економічного забезпечення процесів реформування системи державного управління кібербезпекою; особливості впровадження стандартів ЄС та НАТО в діяльності суб'єктів забезпечення кібербезпеки; державна політика формування єдиного підходу щодо комплектування та підготовки кадрів забезпечення кібербезпеки тощо.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Антонюк В. В.* Механізми державного реагування на сучасні виклики та загрози інформаційній безпеці [Електронний ресурс] / В. В. Антонюк // Держ. упр.: удосконалення та розвиток. — Режим доступу: http://www.dy.nayka.com.ua/?op=1&z=747

2. *Бублик С. Г.* Стратегічні напрями реформування державного управління у сфері науково-технічної діяльності / С. Г. Бублик // Держ. упр. та місцеве самоврядування: зб. наук. пр. — Д.: ДРІДУ НАДУ, 2011. — Вип. 1 (8). — С. 152–157.
3. *Будник М. А.* Концептуально-методологічні аспекти реформування системи державного управління в Україні / М. А. Будник // Держ. упр. — 2007. — № 2 (6). — С. 50–58.
4. *Бурило Ю. П.* Організаційно-правові питання державного управління в інформаційній сфері [Текст]: автореф. дис. ... канд. юрид. наук: 12.00.07 "Адміністративне право і процес; фінансове право; інформаційне право" / Ю. П. Бурило; ДВНЗ "Київський нац. екон. ун-т ім. В. Гетьмана". — К., 2008. — 18 с.
5. *Бурячок В. Л.* Основи формування державної системи кібернетичної безпеки: монографія / В. Л. Бурячок. — К.: НАУ, 2013. — 432 с.
6. *Грицун О. О.* Безпека в кіберпросторі: міжнародно-правові аспекти / О. О. Грицун // Наук. вісн. Херсон. держ. ун-ту. — 2014. — С. 197–202. — Т. 4. Секція Міжнародне право. — (Серія. Юридичні науки.).
7. *Гурковський В. І.* Засади державної політики в сфері інформаційного суспільства в Україні: теоретичні та практичні аспекти [Текст]: автореф. дис. ... д-ра наук з держ. упр. наук: спец. 25.00.01 "Теорія та історія держ. упр." / В. І. Гурковський; Ін-т законодавства ВРУ. — К., 2011. — 36 с.
8. *Державна* політика: підручник / Нац. акад. держ. упр. при Президентові України; ред. кол.: Ю. В. Ковбасюк (голова). — К.: НАДУ, 2014. — 448 с.
9. *Дубов Д. В.* Стратегічні аспекти кібербезпеки України [Текст] / Д. В. Дубов // Стратегічні пріоритети: [наук.-аналіт. щокварт. зб.] / Нац. ін-т стратег. дослідж. — Київ: НІСД, 2013. — № 4 (29). — С. 119–126.
10. *Костюк І.* Наукові концепції, підходи та методи реформування державного управління в Україні / І. Костюк // Держ. упр. та місцеве самоврядування: зб. наук. праць. — Д.: ДРІДУ НАДУ, 2014. — Вип. 1 (20). — С. 35–42.
11. *Марущак А. І.* Щодо поняття "інформаційні ресурси держави" / А. І. Марущак // Інформ. безпека людини, суспільства, держави. — 2009. — № 1 (1). — С. 11–15.
12. *Нестеряк Ю. В.* Державна інформаційна політика та управління національними інформаційними ресурсами / Ю. В. Нестеряк // Держ. упр. та місцеве самоврядування: зб. наук. пр. — Дніпропетровськ: ДРІДУ НАДУ, 2013. — Вип. 1 (16). — С. 94–104.
13. *Петров В. В.* Щодо формування національної системи кібербезпеки України [Текст] / В. В. Петров // Стратегічні пріоритети: [наук.-аналіт. щокварт. зб.] / Нац. ін-т стратег. дослідж. — Київ: НІСД, 2013. — № 4 (29). — С. 127–130.
14. *Пилипишин В. П.* Щодо сутності мети та завдань державного управління в Україні / В. П. Пилипишин // Форум права. — 2010. — № 2. — С. 377–381.
15. *Попок А. А.* Сучасні підходи до здійснення реформування державного управління: досвід зарубіжних країн / А. А. Попок // Вісн. Нац. академії держ. упр. при Президентові України. — 2012. — № 2. — С. 13–20.
16. *Соловйов В. Г.* Інформаційна складова державної політики та управління [Текст]: монографія / С. Г. Соловйов, О. Є. Бухтатий, Ю. В. Нестеряк [та ін.]; за заг. ред. Н. В. Грицяк; Нац. акад. держ. упр. при Президен-

тові України, каф. інформ. політики та електрон. урядування. — Київ: К. І. С., 2015. — 319 с.
17. *Соснін О. В.* Державна політика в галузі управління інформаційним ресурсом України [Текст]: автореф. дис. ... д-ра політ. наук: спец. 23.00.02 "Політичні інститути та процеси" / О. В. Соснін; Одес. нац. юрид. акад. — О., 2005. — 36 с.
18. *Твердохліб О. С.* Формування та розвиток інформаційних державно-управлінських ресурсів України [Текст]: автореф. дис. ... канд. наук з держ. упр. наук: спец. 25.00.01 "Теорія та історія держ. управління" / Нац. акад. держ. упр. при Президентові України. — К., 2012. — 22 с.
19. *Шеломенцев В. П.* Сутність організаційного забезпечення системи кібернетичної безпеки України та напрями його удосконалення / В. П. Шеломенцев // Боротьба з організованою злочинністю і корупцією (теорія і практика). Наук.-практ. журн. — 2012. — № 2 (28). — С. 299–309.
20. *Стратегія* кібербезпеки України, затверджена Указом Президента України від 15 березня 2016 р. № 96 // Офіц. вісн. України. — 2016. — № 23.
21. *Стратегія* національної безпеки України, затверджена Указом Президента України від 26 травня 2015 р. № 287/2015 // Урядовий кур'єр. — 2015. — № 95.
22. *Закон* України "Про Державну службу" від 10 грудня 2015 р. № 889 // ВВР України. — 2016. — № 4. — Ст. 43.