УДК 351.746.1
DOI https://doi.org/10.32836/2310-9653-2019-2-149-156

Р. Ю. Прав, аспірант
Міжрегіональної академії управління персоналом

УДОСКОНАЛЕННЯ СТРАТЕГІЧНОГО ТА ОПЕРАТИВНОГО УПРАВЛІННЯ ДЕРЖАВНОЮ БЕЗПЕКОЮ В ІНФОРМАЦІЙНІЙ СФЕРІ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

Процес забезпечення державної безпеки має бути безперервним і безпосереднім на всіх рівнях управління. Автор підкреслює важливість прийняття рішень щодо інформаційної безпеки на стратегічному рівні і розроблення детальних завдань на тактичному рівні. Вони стають основою для забезпечення реалізації рішень на оперативному рівні.

Завдання ефективного управління процесом забезпечення державної безпеки в інформаційній сфері – це точне і швидке переведення стратегічної концепції, розробленої на вищому управлінському рівні, в конкретні цілі для окремих ланок системи управління державної безпеки або виконавців в окремих секторах управління (міністри, керівники підрозділів), потім детальні завдання виконуються на оперативному рівні. Розподіл системи державної безпеки в інформаційній сфері на підсистеми (координування та виконання) сприяє ефективному управлінню у цій сфері, а також відповідає сучасним умовам і викликам гібридної війни.

Ключові слова: *інформаційна безпека, державна безпека в інформаційній сфері, стратегічне управління, оперативне управління, координаційний орган.*

R. Yu. Prav. Improving strategic and operational governance of state security in the informational field in the conditions of hybrid war

The process of ensuring state security should be continuous and direct and at all levels of government. The author emphasizes the importance of decision-making on information security at the strategic level and the development of detailed tasks at the tactical level. They become the basis for implementation of decisions at the operational level.

The task of efficient management of the process of securing state security in the information sphere is the precise and rapid transfer of the strategic concept to specific purposes. The strategic concept is being developed at the top management level. Specific objectives are defined for individual parts of the state security management system or executives in individual management sectors (ministers, unit managers). Then the detailed tasks are performed at the operational level. The distribution of the system of state security in the information sphere on the subsystem (coordination and implementation) promotes effective management, meets the modern conditions and challenges of the hybrid war.

Information security management should respond to actual changes in a dynamic, modern environment. Therefore, the analysis of opportunities and threats in the information sphere should be continuously conducted. Conclusions of state and non-governmental research organizations should be submitted for consideration to the President and the Government. According to their results, the tasks specified for implementation by state security bodies are corrected or changes are made to the hierarchy of tasks.

The author believes that in Ukraine it is necessary to create a coordination structure that will comprehensively consider information security. It will contribute to the formation of an actual system of ensuring state security in the information sphere, the development and implementation of the most effective solutions. Basic structure features: analysis of threats to state security in the information sphere, consideration of proposals to counter these threats, organization of the process and information security system in important areas (defense, foreign policy, economy, law enforcement system, etc.); the development of a unified technical policy, coordination of work on the implementation of information security programs, coordination of the national strategy of information security with international strategies.

Key words: *information security, state security in the information sphere, strategic management, operational management, coordination body.*

Постановка проблеми. Безпека, зокрема, в інформаційній сфері є необхідною та обов'язковою умовою національної цілісності та розвитку держави, тому забезпечення безпеки слід визнати одним з основних завдань державного управління. Динамічні зміни у зовнішньому оточенні змушують держави для свого захисту створювати комплексну систему безпеки. Особливо актуальним таке завдання стало для України після воєнного вторгнення іноземної держави на нашу територію і намагання захопити її. Після невдалої спроби Росія всі зусилля спрямувала на інформаційну війну з Україною – захоплення інформаційного простору, інформаційні атаки на суспільно значимі об'єкти тощо.

Інформація стала знаряддям пропаганди і впливу, зброєю у гідридній війні, яку веде Росія з Україною. Інформація як елемент soft power (м'якої сили) може створювати привабливу або ж непривабливу картину держави у світі або ж для своїх громадян без застосування примусу. Поширення неприйнятних для українського суспільства ідей, маніпуляція і дезінформація російських спецслужб стають щораз агресивнішими, підтверджуючи небезпечність інформаційної війни Росії.

Аналіз останніх досліджень і публікацій. Серед останніх досліджень у цій сфері виділимо публікацію Я. Малика (2015), в якій автор розглядає стан і перспективи розвитку інформаційної безпеки України [1]. В. Савицький (2017) досліджує інформаційну безпеку в системі національної безпеки України [2]. Ґрунтовний аналіз сучасних загроз в інформаційній сфері представлено в аналітичній доповіді до щорічного послання Президента України до Верховної Ради України «Про внутрішнє та зовнішнє становище України в 2018 році», підготовленій Національним інститутом стратегічних досліджень [3]. Проте такі дослідження є фрагментарними в аналізі всієї системи інформаційної безпеки.

Мета статті – розглянути проблеми вдосконалення стратегічного та оперативного управління державної безпеки в інформаційній сфері в умовах гібридної війни. Протидія загрозам в інформаційній сфері є постійним завданням державного управління, вирішення якого забезпечить недоторканність суверенітету України і гарантуватиме безпеку громадян.

Виклад основного матеріалу. Оскільки законодавчо закріпленого терміна «інформаційна безпека» наразі немає, ми звернулися до проекту Концепції інформаційної безпеки. У ньому пропонується розглядати її як «стан захищеності життєво важливих інтересів людини і громадянина, суспільства і держави, за якого досягається завдання шкоди через неповноту, несвоєчасність і недостовірність поширюваної інформації, порушення цілісності та доступності інформації, несанкціонований обіг інформації з обмеженим доступом, а також через негативний інформаційно-психологічний вплив та умисне спричинення негативних наслідків застосування інформаційних технологій» [4].

Безпека в інформаційній сфері є частиною системи державної безпеки і, у свою чергу, включає взаємопов'язані складові: людей, організації, технічні засоби, що працюють на її забезпечення.

Головним координатором і виконавцем функцій у системі державної безпеки є Служба безпеки України, а головним координатором і виконавцем діяльності, спрямованої на боротьбу з інформаційними загрозами, також має бути спеціальний орган, відповідальний за інформаційну безпеку. Інші структури, навіть на рівні вищого державного управління, міністерства та відомства, беруть участь у цих процесах як співвиконавці. Окрім того, виконавчими органами системи безпеки в інформаційній сфері можуть бути інші ланки державного управління, включно з місцевими органами влади, а також неурядові організації, інститути, дослідні центри, що займаються інформаційними загрозами.

Систему управління державною безпекою в інформаційній сфері можна визначити як сукупність взаємопов'язаних складових: органів державної влади та керівників спеціальних державних структур, які забезпечують безперервність прийняття рішень і виконання завдань

у сфері інформаційної безпеки [3, с. 18]. У процес управління державною безпекою в інформаційній сфері включені основні органи управління держави, відповідальні за виконання завдань, пов'язаних із забезпеченням державної інформаційної безпеки як у зовнішньому, так і внутрішньому вимірах, разом з їх офісами та необхідною інфраструктурою. До цих органів належать такі: Президент України (спільно з дорадчими органами), Кабінет Міністрів України, керівники, які очолюють державні спеціальні структури, на які покладені завдання щодо державної безпеки в інформаційній сфері, а також місцеві державні адміністрації разом з їх офісами (рис. 1).

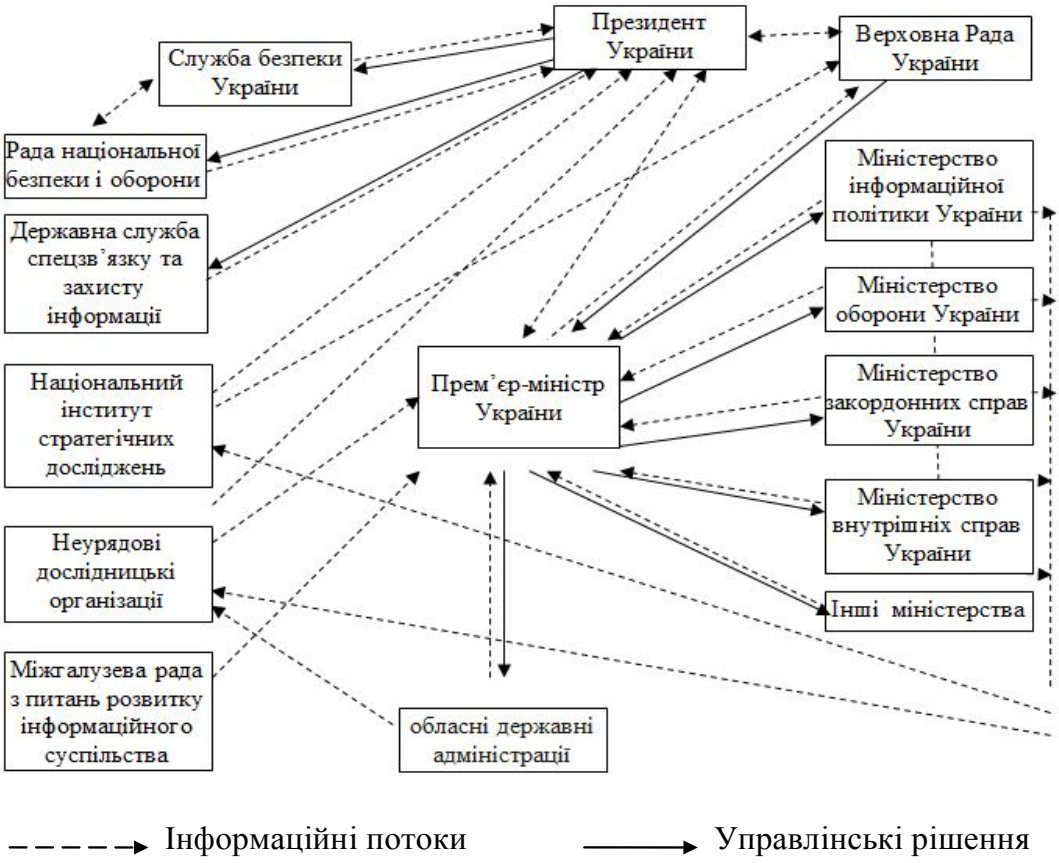

Рис. 1. Рух інформації та управлінських рішень
між ланками системи управління державною безпекою в інформаційній сфері

Джерело: створено автором

У структуру обміну інформацією та рішеннями між елементами системи управління державною безпекою включений парламент, який є законодавчим органом і не є частиною системи управління державною безпекою. Однак роль парламенту дуже важлива в процесі прийняття рішень головними органами виконавчої влади, особливо коли рішення вимагає швидких законодавчих змін. Крім того, компетенція парламенту щодо забезпечення державної безпеки в інформаційній сфері включає періодичні обговорення різних аспектів інформаційної безпеки. Унаслідок дебатів парламент визначає місію держави, бачення державної безпеки, цілі та цінності, що стають основою для стратегії державної безпеки, яка потім інтерпретується в інших безпекових стратегіях, зокрема інформаційній.

На рис. 1 представлені також неурядові аналітичні центри (think tanks, мозкові центри), які повинні сприяти комунікаціям органів державної влади з громадськістю. Неурядові дослідницькі організації (далі – НДО) можуть збирати та аналізувати дані щодо багатьох аспектів державної безпеки в інформаційній сфері, включно з можливостями протистояння загрозам і використання цих можливостей. Вироблені ними думки та позиції можуть бути різними, і вони необов'язково узгоджуються з офіційною позицією влади.

За кордоном неурядові аналітичні центри мають вплив на державну політику, проводять прикладні дослідження, здійснюють консультування органів державної влади та надають їм рекомендації. За визначенням, «неурядова дослідна організація – це незалежна, неприбуткова організація, яка об'єднує фахівців, що мають спеціальні знання, метою діяльності якої є досягнення суспільного блага, а головними засобами його досягнення – дослідження конкретних суспільно значущих проблем, вироблення відповідних рекомендацій, їх просування в державну політику» [5].

Врахування напрацювань НДО, безперечно, сприятиме розробленню ефективних рішень щодо безпеки держави в інформаційній сфері за різних зовнішніх і внутрішніх умов. Тому важливо, щоб такі організації були в системі управління державною безпекою. В Україні, вважаємо, необхідне створення неурядового організаційного аналітичного центру, який узагальнюватиме напрацювання всіх НДО, що дасть змогу комплексно розглядати проблеми державної інформаційної безпеки.

Важливим елементом системи державної безпеки в інформаційній сфері є державні інституції, які займаються аналітичною діяльністю. В Україні це – Національний інститут стратегічних досліджень, підпорядкований Президентові. Серед основних завдань цієї установи – науковий супровід реалізації Президентом, Радою національної безпеки і оборони повноважень у сфері національної безпеки України. Його наукові розроблення мають сприяти виробленню найбільш доцільних методів державного управління.

Недоліком системи управління державної безпеки в Україні є відсутність спеціалізованого науково-дослідного інституту національної безпеки. Інститут проблем національної безпеки був створений у 2003 році з метою розроблення наукових засад національної безпеки України, забезпечення наукової обґрунтованості та ефективності державної політики щодо захисту національних інтересів і безпеки особи, захисту суспільства і держави від зовнішніх і внутрішніх загроз. Установа забезпечувала Президента, Раду національної безпеки і оборони, Кабінет міністрів України інформаційно-аналітичними та концепційними матеріалами з проблем нацбезпеки. Науковці прогнозували і оцінювали зовнішні та внутрішні загрози національній безпеці, надавали пропозиції щодо їх запобігання / усунення. 2010 року Інститут був ліквідований указом Президента і сьогодні не відновлений [6].

Серед інших ланок системи забезпечення державної безпеки в інформаційній сфері – Президент України, Рада національної безпеки і оборони, Прем'єр-міністр України, Міністерство інформаційної політики, Міністерство оборони (Головна розвідувальна служба у його складі), Міністерство закордонних справ, Міністерство внутрішніх справ, інші міністерства в межах компетенції, Служба безпеки України, Адміністрація Державної служби спеціального зв'язку та захисту інформації (центральний орган виконавчої влади зі спеціальним статусом), Міжгалузева рада з питань розвитку інформаційного суспільства (тимчасовий консультативно-дорадчий орган), обласні державні адміністрації (місцеві органи влади).

Загальновідомо, що у процесі управління виділяються такі основні функції: планування, організація, мотивація та контроль. На основі оцінки поточних загроз, внутрішніх і зовнішніх, Кабінет Міністрів України повинен періодично формувати відповідні керівні принципи планування державної безпеки, зокрема, в інформаційній сфері. Завдяки їм усі суб'єкти державної влади вищого рівня та місцеві адміністрації, які беруть участь у виконанні завдань щодо державної безпеки, повинні мати плани з однаковим змістом, які б відрізнялись ступенем деталізації та го-

ризонтом планування. Водночас на місцевому рівні у планах мають враховуватися територіальні особливості і загрози в інформаційній сфері. Особливо актуально це в ситуації гібридної війни.

Функція організації особливо значима для кінцевого результату – досягнення визначених цілей; неправильно сформована організаційна структура може в процесі реалізації планів не тільки віддалити, але й перешкодити досягненню кінцевих цілей. Конкретні зв'язки в організуванні повинні бути визначені на всіх рівнях державного управління – національному, регіональному та місцевому; їх проектування є компетенцією уряду. Організаційні зв'язки повинні не тільки сприяти виконанню завдань щодо усунення інформаційних загроз окремими суб'єктами, але й забезпечити досягнення синергетичного ефекту. Особлива увага має бути приділена організаційній структурі на рівні оперативного управління, де перебувають виконавчі органи системи державної безпеки в інформаційній сфері.

Щодо мотивації, то хочемо зазначити, що безпека в ієрархії потреб є однією з основних, для суспільства і держави це – найвище благо. Ефективна держава повинна забезпечити своїм громадянам достатній рівень безпеки, створити безпечні умови для гідного життя і розвитку всієї нації. Як показує недалекий історичний досвід України, безпека народу, відповідно, впливає і на безпеку урядовців.

Контрольна функція в управлінні безпекою здійснюється державними органами, визначеними законодавчо. В Україні процес контролю забезпечення державної безпеки в інформаційній сфері ускладнений розпорошеністю обов'язків між різними органами, уникненням через це відповідальності та відсутністю єдиного координаційного центру.

Вважаємо, що в Україні необхідне створення координаційної організаційної структури, яка комплексно розглядатиме інформаційну безпеку в усіх її вимірах, сприятиме формуванню актуальної системи забезпечення державної безпеки в інформаційній сфері, виробленню та реалізації найбільш ефективних рішень. Основними функціями такої структури мають бути: аналіз загроз державній безпеці в інформаційній сфері, розгляд пропозицій із протидії цим загрозам, організація процесу і системи захисту інформації в життєво важливих сферах держави (обороні, зовнішній політиці, економіці, правоохоронній системі тощо), розроблення єдиної технічної політики, координація роботи щодо реалізації програм захисту інформації, узгодження національної стратегії інформаційної безпеки з міжнародними.

Наразі аналіз безпеки інформаційного середовища проводиться Національним інститутом стратегічних досліджень, неурядовими дослідницькими організаціями і окремими відділами міністерств, які проводять такі дослідження на постійній основі. Проблема полягає в тому, щоб зібрати ці аналізи в одному центрі, який оцінював би їх у вигляді синтетичного матеріалу.

Ефективність прийняття рішень у процесі управління державною безпекою в інформаційній сфері визначають такі суб'єкти: Верховна Рада України, Президент України, РНБО, Кабінет Міністрів України, Міністерство інформаційної політики, інші міністерства в межах компетенції, Служба безпеки України, державні та недержавні аналітичні організації (див. рис. 1).

Верховна Рада України формально не входить до складу системи державної безпеки, однак відіграє важливу роль у процесі прийняття рішень головними органами виконавчої влади. У Стратегії національної безпеки України (указ Президента 26 травня 2015 року), Доктрині інформаційної безпеки України (затвердженій 25 лютого 2017 року) на основі актуальних загроз визначено низку пріоритетів держави в інформаційній сфері. На їх основі мають бути сформульовані стратегічні цілі держави у сфері інформаційної безпеки, які, у свою чергу, повинні бути відображені в положеннях Стратегії інформаційної безпеки України. Положення Стратегії мають враховуватися під час розроблення іших документів суб'єктів безпеки України в інформаційній сфері.

Така стратегія мала б ранг настановчого державного документа, і тоді визначення цілей безпеки в інформаційній сфері стало б керівним принципом для кожного наступного уряду,

який може розробляти власну концепцію реалізації політики державної безпеки в інформаційній сфері. Це впливатиме на прозорість процесу стратегічного планування в державі.

Стратегія державної безпеки в інформаційній сфері є довгостроковим документом, а термін повноважень уряду становить 4 роки. Забезпечення державної безпеки в інформаційній сфері вимагає також безперервності процесу управління та тривалої перспективи, отже, зміна уряду раніше терміну дії стратегії не повинна одночасно означати зміну чи скасування визначеної державної стратегії. Водночас кожний новий уряд може ставити нові детальні цілі в межах, визначених стратегічним документом, і реалізовувати їх.

Водночас, зважаючи на умови гібридної війни, в яких перебуває нині Україна, а також на можливість виникнення нових непередбачених раніше загроз (або ж усунення старих), сукупність стратегічних цілей щодо безпеки держави в інформаційній сфері може змінитися. Відповідно, виникне підґрунтя для перегляду стратегії державної безпеки в інформаційній сфері.

Коли поточні виклики, реальні можливості та потенційні загрози в інформаційній сфері визначено, конкретні цілі затверджено, то на тактичному рівні починається їх реалізація окремими виконавчими органами системи державної безпеки. Отже, можемо розглядати три рівні управління державною безпекою в інформаційній сфері: стратегічний, тактичний та оперативний (рис. 2).

Стратегічний рівень
Верховна Рада, Президент, Кабінет Міністрів (вище керівництво) визначають стратегію державної безпеки в інформаційній сфері, включно зі стратегічними цілями (що робити? коли? в якому напрямку йти?), а також деякі заходи і методи досягнення цілей. Планування рішень щодо стратегічних цілей безпеки держави в інформаційній сфері у часовому горизонті 4 роки.
⇩
Тактичний рівень
Міністри, керівники головних органів державного управління (середнє керівництво) – зосереджуються на шляхах реалізації стратегічних цілей (як їх реалізувати? коли? які конкретні методи і засоби?) Планування рішень щодо конкретних цілей, планування основних завдань у часовому горизонті 2-4 роки.
⇩
Оперативний рівень
Виконавчі органи зосереджуються на виконанні завдань та постійному контролі за їх виконанням (що робити? хто буде? де? якими конкретними засобами та методами?) Планування рішень, що стосуються однієї деталізованої цілі, як правило, у часовому горизонті 1-2 роки.

Рис. 2. Рівні управління державною безпекою в інформаційній сфері

Джерело: створено автором

Останнім етапом є реалізація конкретних завдань, визначених відповідно до стратегії державної безпеки в інформаційній сфері. Виконавцями цих завдань безпосередньо будуть відділи державних органів безпеки, які працюють в інформаційній сфері. На оперативному рівні має бути проведено наліз сил і ресурсів, які є в розпорядженні окремих виконавчих органів системи державної безпеки в інформаційній сфері.

Важливо приділити особливу увагу контролю на цьому рівні, який повинен враховувати будь-які відхилення процесу реалізації від запланованих планів. Тільки повне виконання всіх завдань на оперативному рівні означає досягнення конкретних цілей, що, у свою чергу, є показником реалізації стратегії державної безпеки в інформаційній сфері.

Висновки з дослідження і перспективи подальших розвідок у цьому напрямі. Динаміка змін у зовнішньому оточенні та внутрішньому середовищі держави накладають на органи влади необхідність ефективного управління державною безпекою в інформаційній сфері. У цьому процесі важливими є рішення, прийняті на стратегічному рівні, та їх виконання на тактичному та оперативному рівнях спеціально уповноваженими органами безпеки. Треба пам'ятати, що інформаційні загрози можуть постійно змінюватися і зростати у динамічному, різноспрямованому середовищі. Тому аналіз проблем із погляду можливостей і загроз повинен бути безперервним процесом. Відповідно, мають змінюватися стратегічні цілі та конкретні завдання державної безпеки в інформаційній сфері, які повинні відповідати актуальним загрозам. В Україні необхідне створення координаційної організаційної структури, яка комплексно розглядатиме проблеми державної інформаційної безпеки в усіх її вимірах, сприятиме ефективності системи управління захисту державної безпеки в інформаційній сфері.

Список використаних джерел:

1. Малик Я.М. Інформаційна безпека України: стан та перспективи розвитку. *Збірник наукових праць*. 2015. № 44. С. 13-20.

2. Савицький В.Т. Інформаційна безпека в системі національної безпеки України. *Університетські наукові записки.* 2017. № 62. С. 195-207.

3. Аналітична доповідь до Щорічного Послання Президента України до Верховної Ради України «Про внутрішнє та зовнішнє становище України в 2018 році». *Послання Президента України*. 2018. 688 с.

4. Концепція інформаційної безпеки України. URL: https://www.osce.org/uk/fom/175056?download=true (дата звернення: 25.04.2019).

5. Тинкован О.В. Неурядові організації як суб'єкти вироблення державної політики : дис. … канд. наук з держ. Управління : 25.00.01; ДРІДУ НАДУ при Президентові України, Дніпропетровськ, 2007. 213 с.

6. Про Інститут проблем національної безпеки: Указ Президента України від 6 листопада 2008 р. URL: https://zakon.rada.gov.ua/laws/show/1396/2003 (дата звернення: 25.04.2019).

References:

1. Malyk, Ya. (2015). Informaciina bezpeka Ukrainy: stan ta perspektyvy rozvytku [Information security of Ukraine: the state and prospects of development]. *Zbirnyk naukovykh prac "Efektyvnist derzhavnogho upravlinnia"* – Collection of scientific works "Efficiency of Public Administration". No. 44. P. 13-20 [in Ukrainian].

2. Savytskyi, V.T. (2017). Informaciina bezpeka v systemi nacionalnoi bezpeky Ukrainy [Information security in the system of national security of Ukraine]. *Universytetski naukovi zapysky* – University scientific notes. No. 62. P 195-207 [in Ukrainian].

3. Analitychna dopovid do Shhorichnogho Poslannia Prezydenta Ukrainy do Verkhovnoi Rady Ukrainy "Pro vnutrishnie ta zovnishnie stanovyshhe Ukrainy v 2018 roci" [Analytical report to the Annual Message of the President of Ukraine to the Verkhovna Rada of Ukraine "On the Internal and External Situation of Ukraine in 2018"]. (2018). Kyiv: NISS – Kyiv: NISD, 688 s. [in Ukrainian].

4. Koncepciia informaciinoi bezpeky Ukrainy. Proekt [The Concept of Information Security of Ukraine. Project]. Retrieved from: https://www.osce.org/uk/fom/175056?download=true (related to: 25.04.2019) [in Ukrainian].

5. Tynkovan, O.V. (2007). Neuriadovi orghanizacii yak subiekty vyroblennia derzhavnoi polityky : dys. ... kand. nauk z derzh. Upravlinnia : 25.00.01 [Non-governmental organizations as subjects of development of state policy : dissertation. state sciences Management : 25.00.01]. DRIDU NADU pry Prezydentovi Ukrainy – DRIDU NAPA under the President of Ukraine, 213 s. [in Ukrainian].

6. PU, Decree of the President of Ukraine (2018), Pro Instytut problem natsionalnoi bezpeky. URL: https://zakon.rada.gov.ua/laws/show/1396/2003 (related to: 25.04.2019) [in Ukrainian].