

УДК 341.1:355.45

DOI <https://doi.org/10.32836/2521-6473.2020-3.20>

Б. М. Тична, старший науковий співробітник
науково-дослідного відділу проблем військового законодавства
Центру воєнно-стратегічних досліджень
Національного університету оборони України
імені Івана Черняхівського

НАПРЯМИ ВДОСКОНАЛЕННЯ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ ЗБРОЙНИХ СИЛ УКРАЇНИ В УМОВАХ ПІВНІЧНОАТЛАНТИЧНОЇ ІНТЕГРАЦІЇ

У статті піднято питання вдосконалення інформаційної діяльності ЗС України з урахуванням євроатлантичної інтеграції. Для цього, досліджені окремі види інформаційної діяльності у практиці Північноатлантичного альянсу; з'ясовані позитивні тенденції інформаційної діяльності в Організації Північноатлантичного договору; визначені проблемні аспекти на шляху удосконалення інформаційної діяльності ЗС України; сформовані напрями покращення інформаційної діяльності ЗС України.

Зазначено, що збільшення ролі інформації в діяльності держави, обумовлює необхідність якісного правового забезпечення державної інформаційної політики у сфері функціонування ЗС України. Загалом формування інформаційної діяльності ЗС України, її правове забезпечення, має будуватися на системній основі, що дозволить досягти бажаної мети – оборони України, захисту її суверенітету, територіальної цілісності й недоторканності із дотриманням гласності, відкритості для демократичного цивільного контролю, реалізацією інформаційних прав громадян щодо інформації, володільцем і розпорядником якої є ЗС України.

З урахуванням обраного курсу євроатлантичної інтеграції перед Україною стоїть завдання, забезпечення впровадження ефективної інформаційної політики у сферах європейської та євроатлантичної інтеграції. Практичний позитивний досвід країни Північноатлантичного альянсу щодо інформаційної діяльності є необхідним для удосконалення діяльності ЗС України. Така діяльність здійснюється переважно у межах одного із напрямків, – адміністративного (у процесі управління, забезпечення документообігу та обміну інформацією).

З урахуванням досвіду НАТО, запропоновано такі напрями удосконалення інформаційної діяльності ЗС України: зміцнення правової бази для впровадження інформаційної діяльності; створення чітких механізмів інформаційної діяльності з урахуванням стандартів НАТО; формування відповідальних структур за комплексне втілення інформаційної діяльності з урахуванням досвіду Північноатлантичного альянсу; розвиток стратегічних комунікацій; забезпечення відкритості для громадського моніторингу; систематичне інформування громадськості про впровадження стандартів НАТО у діяльності ЗС України; забезпечення ефективної системи протидії кіберзагрозам у сфері діяльності ЗС України.

Ключові слова: інформаційна діяльність, Збройні Сили України, інтеграція, НАТО, Північноатлантичний альянс.

B. M. Tychna. Directions of improvement of information activities of the Armed Forces of Ukraine under North Atlantic integration

The article deals with the issue of improvement of the information activities of the Armed Forces of Ukraine taking into account Euro-Atlantic integration. The certain types of information activities in the North Atlantic Alliance's practice are studied; positive trends in the North Atlantic Treaty Organization information activities are clarified; problematic aspects on the way to improving the information activities of the Armed Forces of Ukraine are identified; the directions of improvement of information activities of the Armed Forces of Ukraine are formed.

It is noted that the increasing role of information in the state activities demands qualitative legal support of the state information policy in the field of functioning of the Armed Forces of Ukraine. In general, the formation of information activities of the Armed Forces of Ukraine, its legal support, should be based on a systematic basis that will help to achieve the desired goal – defense of Ukraine, protection of its sovereignty, territorial integrity and inviolability respecting publicity, openness to democratic civilian control, realization of citizens' information rights towards the information the owner and administrator of which is the Armed Forces of Ukraine.

Taking into account the chosen course of Euro-Atlantic integration, Ukraine faces the task of ensuring the implementation of an effective information policy in the areas of European and Euro-Atlantic integration. The practical positive experience of the North Atlantic Alliance countries in the field of information activities is necessary for improving the activities of the Armed Forces of Ukraine. Such activities are carried out mainly within the administrative area (in the process of management, document control and information exchange).

Taking into account the experience of NATO, the following areas of improving the information activities of the Armed Forces of Ukraine are suggested: strengthening the legal framework for the implementation of information activities; creating clear mechanisms for information activities basing on NATO standards; formation of responsible structures for the comprehensive implementation of information activities considering the experience of the North Atlantic Alliance; development of strategic communications; ensuring openness for public monitoring; systematic informing the public about the implementation of NATO standards in the activities of the Armed Forces of Ukraine; ensuring an effective system of counteracting cyber threats in the sphere of activities of the Armed Forces of Ukraine.

Key words: information activities, the Armed Forces of Ukraine, integration, NATO, the North Atlantic Alliance.

© Б. М. Тична, 2020

Постановка проблеми. Дослідження питання удосконалення інформаційної діяльності Збройних Сил України (далі – ЗС України) зумовлено низкою факторів, таких як: наявність недоліків (відсутність чи неузгодженість інформаційних норм) нормативно-правового забезпечення і проблем практичної реалізації; відставання нормотворення від розвитку суспільних інформаційних відносин; недостатні правові заходи щодо забезпечення відповідальності за порушення норм інформаційного законодавства; недосконалість (відсутність) механізму реалізації інформаційних норм, програм розвитку інформаційної сфери, безсистемне орієнтування на кращі закордонні практики у цих питаннях. Так, зокрема Указом Президента України від 20 квітня 2019 року передбачено: постійне забезпечення впровадження ефективної інформаційної політики у сферах європейської та євроатлантичної інтеграції України. Така вимога мотивована забезпеченням незворотності європейського та євроатлантичного курсу України [1].

Північноатлантична інтеграція передбачає впровадження «стандартів» НАТО, а саме основних засадничих вимог передбачених «Угодою про стандартизацію». Основні положення якої мають трискладове підґрунтя адміністративне, оперативне і матеріально-технічне. Інформаційна діяльність переважно, перебуває у межах адміністративних стандартів, зокрема у процесі управління, забезпечення документообігу та обміну інформацією. Тому, з урахуванням обраного Україною курсу, а також інтенсивного зростання вимог інформаційного суспільства щодо відповідності діяльності органів державної влади інформаційним потребам, очевидно є актуальність піднятої у статті теми.

Аналіз останніх досліджень і публікацій. Удосконалення інформаційної діяльності сьогодні привертає увагу багатьох науковців, з урахуванням багатоманітності інформаційних відносин така діяльність вивчалась у різних її видових функціональних проявах, як самостійне явище, так і у діяльності різних державно-владних органів, зокрема у працях: І.В. Арістової, В.М. Брижка, Р.А. Калюжного, Л.П. Коваленко, І.П. Кушнір, Н.А. Литвин, Д.О. Маріц, А.І. Марушака К.В. Меліхова, Д.О. Мороза, В.О. Негодченка, Є. Павліченко, В.Г. Пилипчука, І.М. Сопілко, Т.Ю. Ткачука, О. Фаріона, М.Я. Швеця та багатьох інших. Зважаючи на ці, та інші численні наукові публікації, зауважимо про відсутність комплексного аналізу інформаційної діяльності ЗС України в аспекті її удосконалення з урахуванням сучасних інтеграційних процесів.

Мета статті – обґрунтувати напрямки удосконалення інформаційної діяльності ЗС України з урахуванням досвіду Північноатлантичного альянсу. Для досягнення мети визначено вирішити такі завдання:

– з’ясувати позитивні тенденції інформаційної діяльності в Організації Північноатлантичного договору;

– визначити проблемні аспекти на шляху удосконалення інформаційної діяльності ЗС України;

– сформувати напрямки покращення інформаційної діяльності ЗС України.

Виклад основного матеріалу. Збільшення ролі інформації в діяльності держави, дозволяє підкреслити актуальність та необхідність якісного правового забезпечення державної інформаційної політики у сфері функціонування ЗС України. Загалом формування інформаційної діяльності ЗС України, її правове забезпечення, має будуватися на системній основі, що дозволить досягти бажаної мети – оборони України, захисту її суверенітету, територіальної цілісності і недоторканності із дотриманням гласності, відкритості для демократичного цивільного контролю, реалізацією інформаційних прав громадян щодо інформації, володільцем і розпорядником якої є ЗС України (структурні підрозділи).

Важливим чинником у трансформаційних процесах інформаційної складової діяльності ЗС України є урахування стандартів НАТО. «Коли ми говоримо про розробку і прийняття стандартів НАТО у Збройних Силах України, то маємо на увазі перехід на сучасні системи управління і технології прийняття управлінських рішень, допуск до нових розробок та практичного і бойового досвіду країн НАТО тощо» [2].

Триваюча на сході України гібридна війна, проявами якої є інформаційні загрози, сприяла впровадженню системи стратегічних комунікацій за підтримки НАТО. У Доктрині інформаційної безпеки, затвердженій Указом Президента України від 25 лютого 2017 р. під стратегічними комунікаціями розуміється, скоординоване і належне використання комунікативних можливостей держави – публічної дипломатії, зв’язків із громадськістю, військових зв’язків, інформаційних та психологічних операцій, заходів, спрямованих на просування цілей держави [3]. Аналогічне тлумачення міститься і у Воєнній доктрині України [4].

Саме поняття «стратегічні комунікації» є дещо новим для українського суспільства й для практики ЗС України. Основний посыл передбачає реагування на сучасні загальні загрози шляхом взаєморозуміння та ефективний обмін інформацією. «За словами Міністра національної оборони Польщі Маріуш Блашак, потрібна ефективна модель – як на національному рівні, так і на міжнародному, яка дозволить швидко обмінюватися інформацією про виникнення загроз в інформаційному просторі та правильно реагувати на них» [5]. Отже, стратегічні комунікації певна покращена форма (модель) пришвидшеного обміну інформацією для реагування на інформаційні загрози. З цього приводу, варто зазначити наявність негативного свідомого та вольового фактора, що залишається ще з радянських часів. Коли будь-яка, зокрема важлива інформація отримана командуванням повинна бути оцінена керівництвом на предмет необхідності її доведення до широкого загалу. Особливо коли загрози чи виклики можуть негативний характер (до прикладу, приховування інформації про аварію на ЧАЕС, небажання визнавати війну на сході України). Такий суб’єктивний чинник може зламати, послабити й загалом зробити неефективними будь-які сучасні системи комунікацій, який потрібно викоринювати, але для цього важливі політичні рішення.

Для реалізації стратегічних комунікацій необхідно завершити здійснення комплексу заходів із побудови ефективної системи координації дій влади з ключовими каналами комунікації, розробки і впровадження єдиної системи взаємодії усіх органів влади в інформаційній сфері, узгодження донесення до всіх категорій населення інформації про ситуацію в Україні, зокрема й стан на сході країни [6, с. 25]. Під час взаємодії військових формувань, кожен орган, виконуючи свої завдання, досить часто намагається самостійно їх реалізувати (там, де можлива спільна діяльність із взаємодіючими суб'єктами), створює ілюзію активної діяльності, результативність якої могла б стати вищою при застосуванні ефективної координації, інформаційної взаємодії в управлінні їх спільною діяльністю [7, с. 150].

Т.Ю. Ткачук зазначає, що система інформаційної політики НАТО є похідною від реалізації демократичного принципу цивільного контролю над військово-політичною сферою в умовах участі громадськості в міжнародному військово-політичному процесі [8, с. 241]. Забезпечення демократичного принципу цивільного контролю у багатьох питаннях залишається обмеженим і політизованим.

Важлива роль у проведенні інформаційної діяльності відводиться Атлантичній раді, шляхом оприлюднення для ЗМІ і громадськості своїх заяв та рішень. Аналогічні функції належать Бюро інформації та преси [9]. Для збереження та захисту інформації у діяльності країн НАТО застосовуються п'ять рівнів захисту інформації з обмеженим доступом [10; 11].

Зasadничим принципом безпеки інформації в системі НАТО є при цьому те, що інформація має зберігати свій ступінь захисту протягом усього циклу її обігу, починаючи від джерела. При цьому контроль за розподілом і поширенням інформації має унеможливити її витік [8, с. 244].

У межах розширення безпеки та співробітництва вагоме значення у діяльності НАТО відводиться консультуванню з політичних та військових безпекових питань. Для цього постійно розвивається обмін інформацією, зокрема сьогодні діють офіцери зв'язку між NOS і національним органом з безпеки інформації [8, с. 245].

Поки у ЗС України формується система кіберзахисту, що є важливою складовою безпеки сучасної держави, у країнах НАТО цей процес розпочався ще з 2002 року, і сьогодні вони вийшли на новий якісний рівень своєчасного реагування на інформаційні загрози їх інформаційно-телекомунікаційним системам. Загрози в Інтернеті визнані, як стратегічно важливі. Сьогодні НАТО забезпечує розвиток засобів запобігання, виявлення, реагування й відновлення після атак за допомогою створених статур: Органу з управління кібернетичною безпекою (який підпорядкований Комісії з управління діяльністю в галузі кіберзахисту), Спільного Центру передового досвіду з кіберзахисту і Сил реагування на комп'ютерні інциденти [12, с. 198]. Комісія з управління діяльністю в галузі кіберзахисту консультує країни-члени НАТО з питань, що стосуються забезпечення кіберзахисту.

Окремо здійснюється робота у галузі аналізу та підготовки ведення у віртуальному просторі інформаційних операцій, забезпечення переговорів експертів у цій сфері, навчання та обмін інформацією із зацікавленими партнерами, у межах діяльності Центру передового досвіду в галузі кіберзахисту [13].

Дієвим засобом отримання даних обстановки у Північноатлантичному альянсі є збирання інформації у режимі реального часу, але це вимагає вартісного обладнання засобами відстежування та відеоспостереження.

Обробка інформації в інформаційних системах створює додаткову загрозу для порушення її цілісності й безпеки. Тому одночасно з веденням, обробкою, передачею даних в інформаційних системах, забезпеченням їх функціонування необхідно постійно вживати заходів з убезпеченням змісту інформації. Такі заходи повинні мати комплексний характер (правові, організаційні, технічні, здійснення контролю, притягнення винних до відповідальності тощо) та реалізовуватись не тільки спеціальними підрозділами із кіберзахисту, але й усіма посадовими особами ЗС України [14, с. 102].

Отже, досвід інформаційної діяльності країни Північноатлантичного альянсу свідчить про зосередження на вирішенні таких ключових моментів, як: обмін інформацією, консультування, сприяння розвитку та передача досвіду іншим країнам; збереження та захист інформації; використання сучасного обладнання з метою отримання інформації про стан безпеки чи виникнення загроз; організацій та підтримання ефективної системи кіберзахисту, підготовка та перепідготовка для цього персоналу.

Недоліком реформаційних процесів в українських реаліях, з урахуванням бажання отримати членство у НАТО, є повільна нормотворча діяльність із запровадженням натівських стандартів й незлагодженість механізмів їх впровадження. Так, ще у 2015 році із прийняттям Стратегія національної безпеки України серед основних напрямків державної політики національної безпеки України визначено:

– забезпечення інформаційної безпеки (забезпечення наступальності заходів політики інформаційної безпеки на основі асиметричних дій проти всіх форм і проявів інформаційної агресії; створення інтегрованої системи оцінки інформаційних загроз та оперативного реагування на них; протидія інформаційним операціям проти України, маніпуляціям суспільною свідомістю і поширенню спотвореної інформації, захист національних цінностей та зміцнення єдності українського суспільства; розробка і реалізація скоординованої інформаційної політики органів державної влади; виявлення суб'єктів українського інформаційного простору, що створені та/або використовуються Росією для ведення інформаційної війни проти України, та унеможливлення їхньої підривної діяльності; створення і розвиток інститутів, що відповідають за інфор-

маційно-психологічну безпеку, з урахуванням практики держав – членів НАТО; удосконалення професійної підготовки у сфері інформаційної безпеки, упровадження загальнонаціональних освітніх програм з медіакультури із залученням громадянського суспільства та бізнесу [15, п. 4.11];

забезпечення кібербезпеки і безпеки інформаційних ресурсів (розвиток інформаційної інфраструктури держави; створення 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 Російській Федерації; реформування системи охорони державної таємниці та іншої інформації з обмеженим доступом, захист державних інформаційних ресурсів, систем електронного врядування, технічного і криптографічного захисту інформації з урахуванням практики держав – членів НАТО та ЄС; створення системи підготовки кадрів у сфері кібербезпеки для потреб органів сектору безпеки і оборони; 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 [15, п. 4.12].

Пройшло вже п'ять років з моменту прийняття Стратегії національної безпеки України, а в Указі Президента України «Про Річну національну програму під егідою Комісії Україна – НАТО на 2019 рік» від 10 квітня 2019 року до кінця 2020 року заплановано удосконалення системи захисту інформаційних ресурсів та інформації, кіберзахисту інформаційно-телекомунікаційних систем органів системи Міністерства внутрішніх справ України, зокрема щодо:

- упровадження інноваційних рішень та інструментів системи захисту інформаційних ресурсів, підвищення ефективності роботи і взаємодії через максимальне використання інформаційно-комунікаційних технологій у реалізації завдань органами системи Міністерства внутрішніх справ України;
- введення в експлуатацію єдиної інформаційної системи Міністерства внутрішніх справ України (далі – ЄІС) із впровадженням систем кіберзахисту ЄІС та захисту інформації, яка в ній оброблялася;
- організація формування, наповнення та підтримки в ЄІС баз даних, необхідних для забезпечення діяльності правоохоронних та інших державних органів.

Для цього першочергово передбачено здійснити: створення галузевих центрів реагування на кіберзагрози Міністерства внутрішніх справ України та органів системи Міністерства внутрішніх справ України; впровадження та забезпечення функціонування в органах системи Міністерства внутрішніх справ України систем управління інформаційною безпекою; розроблення організаційно-технічних заходів з попередження та реагування на кіберзагрози; створення резервного центру обробки даних Міністерства внутрішніх справ України [16, п. 2.6.3].

Варто відмітити позитивні зрушення у напрямку розроблення програм, що визначають вектор спрямування ЗС України до НАТО, але переважно такі рішення є декларативними без конкретних механізмів, у зв'язку із чим не завжди реалізуються вчасно.

Окремий напрямок інформаційної діяльності становить інформування громадськості з приводу функціонування НАТО. Пояснення громадянам національної політики в галузі оборони й безпеки та роль цієї країни в НАТО забезпечує Уряд кожної держави НАТО. Кожна країна НАТО забезпечує фінансування та обрання шляхів інформування громадськості. В основі цієї діяльності лежить забезпечення демократичних прав громадян, зокрема на отримання інформації про діяльність міжнародних структур, які підтримують національну безпеку, а також усвідомлюють важливість забезпечення розуміння і підтримки урядової політики безпеки з боку громадськості [17, с. 170].

Головною метою політики Альянсу в галузі інформації та преси є розширення громадського розуміння питань безпеки та залучення громадян до ґрунтовного і конструктивного обговорення поточних аспектів безпеки та формування політики на майбутнє. Всі плани заходів та робочі програми, розроблені з метою підтримки головних ініціатив, започаткованих державами НАТО в останні роки, містять окремі розділи, присвячені інформаційному забезпеченню [17, с. 171].

Для сприяння інформування громадськості створено Відділу інформації та преси НАТО, який надає допомогу у здійсненні заходів, спрямованих на інформування громадськості в країнах НАТО; забезпечує щоденні зв'язки НАТО із засобами масової інформації; поширює інформації про Альянс в державах не членах НАТО, які виявляють у цьому зацікавленість [17, с. 170].

Роз'яснення здійснюється з таких основних питань: роз'яснення ролі НАТО у врегулюванні конфлікту; ініціативи «Партнерство заради миру», реструктуризація збройних сил НАТО та внутрішня перебудова Альянсу, посилення європейської складової в Альянсі; процес зовнішньої трансформації НАТО тощо. Така діяльність зумовлена зростанням громадського інтересу і потребою у відповідних інформаційних заходах.

Уряди країни, що бажають вступити до НАТО повинні вживати активних заходів з інформування громадськості щодо наслідків членства їхніх країн в НАТО та забезпечення підтримки з боку населення подальшої діяльності [17, с. 171]. Так у 1996 році в Києві відкрився Центр інформації та документації НАТО., який комплектується і фінансується Відділом інформації та преси НАТО. Центр забезпечує доступ до відповідної

документації, а також до участі в інших інформаційних заходах, зокрема в ознайомлювальних візитах до штаб-квартири НАТО і в семінарах, що спонсоруються НАТО [16, с. 173]. Але таке інформування в Україні не має системного та постійного поширення. Тільки до кінця 2020 року планується: інформування громадськості на регіональному та місцевому рівнях, спрямоване на підвищення рівня обізнаності стосовно відносин особливого партнерства України з НАТО; досягнення високого рівня підтримки громадянами України державної політики у сфері євроатлантичної інтеграції [16]. На нашу думку, основна мета такої діяльності щодо інформування уже давно могла бути досягнута. Лише постійно оновлювати актуальну інформацію.

Висновки з дослідження і перспективи подальших розвідок у цьому напрямі. Отже, повільні процеси у системі нормотворення, відсутність системних механізмів, які є дієвими у НАТО, негативно впливають на розвиток інформаційної складової у діяльності ЗС України, невідповідність системи захисту інформації, інформаційної безпеки сучасним загрозам, у тому числі в умовах ведення проти України гібридної (інформаційної) війни, що загалом позначається на стані національної безпеки держави.

З урахуванням досвіду НАТО, нами сформовані основні напрямки удосконалення інформаційної діяльності ЗС України у контексті Північноатлантичної інтеграції: зміцнення правової бази для впровадження інформаційної діяльності; створення чітких механізмів інформаційної діяльності з урахуванням стандартів НАТО; формування відповідальних структур за комплексне втілення інформаційної діяльності з урахуванням досвіду Північноатлантичного альянсу; розвиток стратегічних комунікацій; забезпечення відкритості для громадського моніторингу; систематичне інформування громадськості про впровадження стандартів НАТО у діяльності ЗС України; забезпечення ефективної системи протидії кіберзагрозам у сфері діяльності ЗС України.

Детальний аналіз окремих напрямків удосконалення інформаційної діяльності ЗС України становить перспективу для подальших наукових досліджень.

Список використаних джерел:

1. План заходів з реалізації стратегічного курсу держави на набуття повноправного членства України в Європейському Союзі та в Організації Північноатлантичного договору : Указ Президента України від 20.04.2019 р. № 155/2019. *Урядовий кур'єр*. № 78.
2. Радіо свобода. Політика. URL: <https://www.radiosvoboda.org/a/30486029.html>
3. Про рішення Ради національної безпеки і оборони України від 29.12.2016 р. «Про Доктрину інформаційної безпеки України» : Указ Президента України від 25.02.2017 р. № 47/2017. *Офіційний вісник Президента України*. 2017. № 5. Ст. 102.
4. Про рішення Ради національної безпеки і оборони України від 02.09.2015 р. «Про нову редакцію Воєнної доктрини України» : Указ Президента України від 24.09.2015 р. № 555/2015. *Офіційний вісник Президента України*. 2015. № 22. Ст. 1291.
5. Стратегічні комунікації Міноборони України: представники держав-членів НАТО ознайомились з українським досвідом. URL: <https://www.mil.gov.ua/news/2019/09/26/strategichni-komunikaczii-minoboroni-ukraini-predstavniki-derzhav-chleniv-nato-oznajomilis-z-ukrainskim-dosvidom/>
6. Петров В. В. Щодо становлення системи стратегічних комунікацій органів державної влади у контексті розвитку відносин з НАТО. *Стратегічні пріоритети*. № 4 (41), 2016. С. 24-Калюжний Р. А., Кушнір І. П. Правове забезпечення взаємодії публічної адміністрації у прикордонній сфері : монографія. Київ : «МП Леся», 2015. 224 с.
7. Ткачук Т. Ю. Правове забезпечення інформаційної безпеки в умовах євроінтеграції України. дис... д-ра юрид. наук : 12.00.07. Ужгород, 2019. 487 с.
8. Background information on the Alliance, its policies, activities and structures. URL: <http://www.nato.int/cps/en/natohq/topics.htm>
9. Kaija E. Schilde. Cosmic top secret Europe? The legacy of North Atlantic Treaty Organization and cold war US policy on European Union information policy. URL: <http://dx.doi.org/10.1080/09662839.2014.911175>.
10. William D. Gerhard, Henry W. Millington Attack on a Sigint Collector. URL: <http://nsarchive.gwu.edu/NSAEBB/NSAEBB24/nsa10.pdf>
11. Белоусова Н. Б., Афанасьєва П. А. Основні вимоги НАТО щодо забезпечення безпеки інформаційного простору. Актуальні проблеми міжнародних відносин. Вип. 102, частина 1. 2011 С. 196-NATO Cyber defence. URL: http://www.nato.int/cps/en/natohq/topics_78170.htm
12. Kushnir I. Topical directions for improvement of information relations in activities of the State Border Guard Service of Ukraine : collective monograph : Low and Border: Addressing Security Threats at the Ukrainian Border Lviv-Torun : Liha-Pres. 2019. P. 89–108.
13. Стратегія національної безпеки України затверджена Указом Президента України від 26 травня 2015 року № 287/2015.
14. Про Річну національну програму під егідою Комісії Україна – НАТО на 2019 рік : Указ Президента України від 10.04.2019 р. № 117/2019. *Офіційний вісник України*. 2019. № 31. Ст. 1109.
15. Handbook NATO. Office of Information and Press NATO -