1. ТЕОРІЯ ТА ІСТОРІЯ ДЕРЖАВИ І ПРАВА. ІСТОРІЯ ПОЛІТИЧНИХ І ПРАВОВИХ ВЧЕНЬ. ФІЛОСОФІЯ ПРАВА

УДК 329.09.5(477):340.1

Андрій Грубінко,
доктор історичних наук,
професор кафедри теорії та історії
держави і права
Тернопільського національного
економічного університету

ІНФОРМАЦІЙНА БЕЗПЕКА УКРАЇНИ: ПРАВОВЕ ГАРАНТУВАННЯ ТА РЕАЛІЇ ЗАБЕЗПЕЧЕННЯ

Проаналізовано особливості правового гарантування інформаційної безпеки України в умовах сучасних викликів та загроз (насамперед гібридної війни Росії проти України). Розглянуто практичні аспекти та виявлено проблеми забезпечення інформаційної безпеки України.

Ключові слова: *інформаційна безпека, Україна, правові гарантії, законодавство, гібридна війна.*

Грубинко А.

Информационная безопасность Украины: правовое гарантирование и реалии обеспечения

Проанализированы особенности правового обеспечения информационной безопасности Украины в условиях современных вызовов и угроз (прежде всего гибридной войны России против Украины). Рассмотрены практические аспекты и выявлены проблемы обеспечения информационной безопасности Украины.

Ключевые слова: *информационная безопасность, Украина, правовые гарантии, законодательство, гибридная война.*

Hrubinko A.

The informational security of ukraine: legal guarantee and reality of providing

In the article the peculiarities of legal guarantee of the informational security of Ukraine in the conditions of modern challenges and threats (first of all, the hybrid war of Russia v. Ukraine) are analyzed. Practical aspects and problems of providing of the informational security of Ukraine are revealed.

Keywords: *informational security, Ukraine, legal guarantees, legislation, hybrid war.*

Актуальність статті та постановка наукової проблеми. Розвиток світопорядку XXI ст. відзначається новою політико-економічною та безпековою ситуацією, в якій змушені діяти і виживати Українська держава і суспільство. Україна послідовно відстоює національні інтереси у сучасному глобалізованому світі. До таких інтересів належить, зокрема, участь України в міжнародних інформаційних процесах, пов'язана з проблемами гарантування безпеки держави, суспільства, суб'єктів господарювання, кожного індивіда.

Суспільний розвиток України характеризується формуванням інформаційного суспільства. Впровадження новітніх інформаційних технологій значно прискорює процес отримання, обробки та аналізу інформації. Широкий і оперативний доступ до інформації підвищує ефективність її використання, що стає невід'ємним елементом управління всіма інститутами і процесами. Сучасна Україна повною мірою включена в процеси глобальної інформатизації, формування єдиного світового інформаційного ринку. Інформаційний фактор відіграє унікально важливу роль у державотворчому процесі, репрезентації та відстоюванні інтересів держави на міжнародній арені. Тому особливе місце у цьому спектрі суспільних відносин займають проблеми правового забезпечення інформаційної безпеки.

Мета статті – проаналізувати особливості правового гарантування інформаційної безпеки України в умовах сучасних викликів та загроз, розглянути практичні аспекти та виявити проблеми функціонування системи інформаційної безпеки України.

Аналіз останніх досліджень і публікацій. Дослідження стану інформаційної безпеки України ґрунтується на наукових здобутках відомих дослідників О. Бандурки, В. Горбуліна, Є. Скулиш, І. Івченко, Р. Калюжного, А. Качинського, В. Ліпкана, А. Марущака, Г. Новицького, В. Пилипчука, М. Стрельбицького та ін. Проблему інформаційної безпеки безпосередньо вивчають В. Богданов, О. Глазов, О. Гуровський, О. Данільян, К. Пархоменко, А. Корсунський**,** В. Ніколаєв, Г. Остапович, І. Костицька. Згадані науковці сходяться на думці, що сучасна Україна опинилася у стані інформаційної війни з країнами, які намагаються нав'язати їй свої цінності, зруйнувати традиційні морально-етичні засади українського суспільства. Оскільки загрози інформаційній безпеці держави в сучасних умовах є динамічними та постійно змінюються, відповідна проблематика наукових досліджень не втрачає актуальності.

Виклад основного матеріалу дослідження. Поняття «інформаційна безпека» вперше згадується наприкінці 1980-х рр. у праці німецького вченого Г. Одермана, де йдеться про важливий інформаційний компонент у міжнародній безпеці та робиться спроба розглянути проблеми безпеки, комплексно пов'язані з інформаційними загрозами. У вітчизняній пресі, починаючи з кінця 1991 – початку 1992 р., спостерігається тенденція до відкритого дослідження проблеми інформаційної безпеки як окремого питання [1, с. 17–18].

Інформаційна безпека – це сукупність засобів забезпечення інформаційного суверенітету України, захисту держави та її громадян від зовнішніх і внутрішніх інформаційних загроз. Інформаційна безпека є складовою загальної безпеки і набуває все більшої актуальності в світі загалом та в Україні. Глобальна інформатизація охоплює усі сфери функціонування держави: економічну, військову, політичну, промислову, гуманітарну. Інформаційна безпека, як і будь-який інший об'єкт, є відповіддю на загрози, які посягають як на модельну фізичну цілісність, так і її похідні. Як відомо, інформаційна безпека, захист якої згідно зі ст. 117 Конституції України поряд із суверенітетом, територіальною цілісністю та економічною безпекою є найважливішою функцією держави, досягається шляхом розробки і впровадження сучасних безпечних інформаційних технологій, побудови функціонально повної національної інфраструктури, формування і розвитку інформаційних відносин тощо [2]. Згідно із Законом «Про основи національної безпеки України» однією з основних загроз національним інтересам і національній безпеці України в інформаційній сфері є намагання маніпулювати суспільною свідомістю, зокрема шляхом поширення недостовірної, неповної або упередженої інформації [3]. Поряд із цим ст. 3 Закону України «Про інформацію» передбачає такі напрями державної інформаційної політики: забезпечення доступу кожного до інформації; забезпечення рівних можливостей щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації; створення умов для формування в Україні інформаційного суспільства; забезпечення відкритості та прозорості діяльності суб'єктів владних повноважень; створення інформаційних систем і мереж інформації, розвиток електронного управління; постійне оновлення, збагачення та зберігання національних інформаційних ресурсів; забезпечення інформаційної безпеки України; сприяння міжнародній співпраці в інформаційній сфері та входженню України до світового інформаційного простору [4].

Закон України «Про основи національної безпеки України» виділяє три об'єкти національної та відповідно інформаційної безпеки, до яких належать: людина і громадянин – їх конституційні права і свободи; суспільство – його духовні, моральноетичні, культурні, історичні, інтелектуальні та матеріальні цінності; інформаційне і навколишнє природне середовище і природні ресурси; держава – її конституційний лад, суверенітет, територіальна цілісність і недоторканість [3].

Основою нормативно-правового регулювання системи забезпечення інформаційної безпеки в Україні є Конституція України, Закон України «Про основи національної безпеки України», Закон України «Про інформацію», Закон України «Про Концепцію Національної програми інформатизації», інші нормативно-правові акти. Від початку 2000-х рр. в Україні реалізовано комплекс заходів щодо удосконалення правового забезпечення інформаційної безпеки держави, прийнято Закони «Про державну таємницю», «Про розвідувальні органи України», «Про контррозвідувальну діяльність», «Про боротьбу з тероризмом», «Про Державну прикордонну службу», «Про основи інформаційної безпеки України», «Про національну безпеку України» тощо. Розгорнута робота з формування механізмів їх реалізації, підготовки інших законопроектів, які регламентують суспільні відносини у даній сфері.

Важливі завдання з гарантування інформаційної безпеки виконує Служба безпеки України, яка згідно з нормами ст. 1 Закону України «Про Службу безпеки України» визначається як «державний правоохоронний орган спеціального призначення, який забезпечує державну безпеку України» [5]. Для захисту

українського простору від зовнішньої пропаганди та для координації діяльності приватних ЗМІ з донесення інформації до громадян на окупованих територіях 2 грудня 2014 року створено Міністерство інформаційної політики України, що викликало значний резонанс як серед політиків, так і серед працівників засобів масової інформації.

Водночас чинний механізм реалізації державної політики у сфері розвитку інформаційної безпеки не можна вважати досконалим. Свідченням цьому стало фактичне захоплення Росією інформаційного простору Криму, Сходу та Півдня України, що створило передумови для російської окупації АРК у 2015 р. та організації збройного конфлікту у Донецькій і Луганській областях. Цілеспрямована діяльність Росії дає змогу провокувати напругу в інших регіонах, підтримувати антиукраїнські настрої серед власного населення, дискредитувати Україну та виправдовувати свою політику у державах-членах ЄС. Це передусім пов'язано з несформованістю недержавного сектору забезпечення інформаційної безпеки в Україні. Сучасні умови соціально-економічного, інформаційного і політичного розвитку країни викликають загострення протиріч між потребами особи у гарантуванні безпеки та можливостями держави щодо надання адекватних послуг. Багато науковців зазначають, що елементом реагування на цю проблему є створення загальнодержавної системи інформаційної (зокрема кібернетичної) безпеки України, наступальної спрямованості як з питань захисту суверенітету, так і просування українських національних інтересів.

Головними викликами та загрозами інформаційної безпеки сьогодні для України є інформаційна війна, інформаційний тероризм та інформаційні злочини. Їх причиною є глобальні процеси інформатизації, прогрес у сфері розвитку інформаційних технологій та інформаційна складова гібридної війни Російської Федерації проти України.

Сучасний тероризм характеризується масштабністю здійснюваних терористичних атак, високим рівнем організації та фінансування, різким зростанням технічної та технологічної оснащеності. Хакерські групи у РФ, терористичні організації Хезболла, Хамас та ІГІЛ мають складну структуру, органи управління, свої теле- та радіостанції. Це зумовлює появу міжнародного тероризму, його нових форм. З кожним роком збільшуються кількісні показники терористичної злочинності. Вкрай гострою залишається інформаційна складова гібридної війни РФ проти України, елементом якої є кібертероризм, втручання у критичну інформаційну інфраструктуру України вірусів-шпигунів тощо. Інформаційний тероризм застосовується з метою дезінформації, дезорієнтації та профанації для помилкового сприймання, розуміння і неадекватної поведінки суспільства.

Інформаційний простір використовується терористичними організаціями (спільнотами) з метою втручання в інформаційно-технологічні системи великих організацій і підприємств, фінансування терористичної діяльності, встановлення зв'язків між терористами, організації діяльності терористичних організацій (спільнот), пропаганди, вербування населення тощо.

З метою виправдання свого втручання у внутрішні справи України Росія вже тривалий час спрямовує свою пропаганду проти української влади, намагається дискредитувати європейський вибір нашої держави, виставляє АТО «каральною акцією» з «хаотичними бойовими діями», які призводять до невиправданих жертв серед мирного населення, поширює чутки про непрофесійність і деморалізованість української армії. В інформаційний простір України запускаються проекти тотального соціального зомбування, які начебто не пов'язані з політичними питаннями і подіями в АТО, але насправді спрямовані на просування ідеології «Русского мира» та використовують маніпулятивні технології, маскуючись під пропаганду добра, людяності, взаємодопомоги з метою здійснення масштабного впливу на свідомість українців [6, с. 171–172].

До виявів інформаційної війни може бути зарахована так звана «інформаційна злочинність», левова частка якої припадає на кіберзлочини. Якщо за станом на 2015 р. Україна посідала 5 місце у світовому рейтингу з ризику зіткнення з Веб-загрозами, то після атаки вірусу «Petya» у 2017 р., від якого постраждали енергетичні компанії, банки, урядові сайти, антирейтинг нашої країни в питаннях кібербезпеки відчутно зріс. Особливою групою загроз інформаційній безпеці, актуальних для України, є загрози, зумовлені віртуалізацією – соціальним відчуженням людини, зміненими станами свідомості, переходом до особистісного віртуального світу.

Чинне законодавство України у сфері забезпечення інформаційної безпеки недостатнє і значною мірою відстає від рівня розвитку інформаційного суспільства. Перші спроби вплинути на державному рівні на інформаційний простір в Україні, пронизаний проросійською пропагандою, були здійснені в діяльності українських медіа вже на початку війни на Донбасі. Наприкінці червня 2014 р. у Нацгвардії з'явилося Управління інформаційної безпеки, а в грудні створене Міністерство інформаційної політики України. У лютому 2015 р. з'явився проект «Інформаційні війська України», одним із завдань якого стало об'єднання

«лідерів думок» і «тролів» з великою аудиторією у соцмережах з метою адекватної відповіді на інформаційні атаки Росії та формування патріотичного порядку денного в онлайн-медіа. Де-факто це була перша публічна спроба дати «дзеркальну відповідь» російській пропаганді на державному рівні.

У 2014–2016 рр. Національна рада України з питань телебачення і радіомовлення заборонила мовлення на території України понад 70 російським каналам, а Держагентство з питань кіно відмовило в реєстрації та скасувало прокатні посвідчення на трансляцію понад 500 російських фільмів та серіалів. Розвивається нормативно-правова база інформаційної безпеки. Указом Президента України № 287/2015 від 26 травня 2015 р. введено в дію рішення Ради національної безпеки і оборони України від 6 травня 2015 р. «Про Стратегію національної безпеки України». Документ спрямований на реалізацію до 2020 р. пріоритетів державної політики національної безпеки шляхом запровадження докорінних змін у зовнішньому і внутрішньому безпековому середовищі України [7].

Події на Сході України називають гібридною війною з боку Росії. Гібридна війна – це змішання класичного ведення війни з використанням нерегулярних збройних формувань. Держава, яка веде гібридну війну, здійснює операцію з недержавними виконавцями – бойовиками, групами місцевого населення, організаціями, зв'язок з якими формально повністю заперечується. Особливістю цього конфлікту є його потужна інформаційна складова, яку правдиво можна вважати інформаційною війною. У 2014 р. Російська Федерація порушила територіальну цілісність України шляхом тимчасової окупації території Автономної Республіки Крим і міста Севастополь, а також окремих районів Донецької та Луганської областей, чому передувала активна пропагандистська діяльність як російських, так і юридично українських, проте проросійських за змістом мас-медіа. До актуальних загроз національній безпеці України належить подання неякісної, недостовірної або сфальсифікованої інформації, неправомірна заборона третіми особами права доступу громадян до інформації тощо. Зокрема, у середині літа 2014 р. в захоплених терористами районах Донецької та Луганської областей провайдери кабельного телебачення вимкнули українські телеканали. Громадян позбавили права на отримання інформації з диверсифікованих джерел, що у подальшому призвело до формування уявлення про ситуацію в країні та світі на основі неякісних, недостовірних, часто неправдивих повідомлень [8, с. 66–67]. Також інструменти інформаційної гібридної війни Росії, окрім традиційного телебачення, радіо і підвладних путінському режиму ЗМІ, включає в себе тексти, відео, аудіо, зображення, котрі поширюються через Інтернет-медіа, блоги і сайти та супутникове телебачення. Залучаються до співпраці на платній основі «тролі», котрі залишають свої пости на дискусійних форумах, беруть участь в Інтернет-чатах, а також залишають свої коментарі під статтями і в розділах новин.

З боку Російської Федерації продовжуються системні посягання на інформаційну безпеку нашої держави, пов'язані здебільшого з намаганнями інформаційних суб'єктів, у тому числі й закордонних, свідомо викривити зміст подій за участю України, подати у сфальсифіковано вигляді відомості про розвиток політичних, соціальних, економічних та інших подій з метою дискредитації держави в очах міжнародної спільноти та свого власного народу, підриву довіри до неї як до надійного партнера, вагомого суб'єкта міжнародного права. Наприклад, у січні 2018 р. база Повітряно-космічних сил Росії у Сирії зазнала атаки саморобних безпілотників. На брифінгу в Москві Генштаб РФ доповів, що вибухова речовина саморобних бомб (ТЕН) не може бути виготовлена в кустарних умовах і зауважив, що подібна речовина виготовляється в Україні, на заводі у місті Шостка. 5 липня 2018 р. інформаційний простір був наповнений повідомленнями про нібито прострочені протитанкові керовані ракети »Javelin«, що були передані Україні. Для цього російською стороною було створено підроблений лист від директора КБ «Луч» Олега Коростельова до секретаря РНБО Олександра Турчинова, де той нібито нарікає на якість поставлених ПТРК »Javelin». Підроблений документ був вперше опублікований у Telegram-каналі з назвою «НачШтабу», створеному за кілька тижнів до того. Сам канал «НачШтабу» займається розповсюдженням фейків, дезінформації та пропаганди, що чергуються із перепостами достовірних повідомлень української сторони. 7 серпня 2018 р. окупаційні сили РФ на Донбасі втратили підбиту військову вантажівку «Урал», де загинув фельдшер. Вони звинуватили у підбитті Збройні Сили України, вказавши, що фельдшер нібито їхав у с. Набережне на виклик місцевої жительки і вантажівка була підбита з ПТКР. Проте розслідування ситуації встановило, що ситуація була іншою. Вантажівка, що розвозила провіант воякам окупаційних військ, вибухнула на мінах біля с. Біла Кам'янка. Учасники окупаційних військ не пропустили до вантажівки представників Спеціальної моніторингової місії ОБСЄ для об'єктивного аналізу ситуації [9, с. 1–5].

Висновки. Інформаційна безпека є складним, системним, багаторівневим явищем, на стан якого впливають зовнішні та внутрішні чинники: політична обстановка у світі; внутрішньополітична ситуація в державі; стан і рівень інформаційно-комунікаційного розвитку країни тощо. Загрози інформаційній безпеці здебільшого

супроводжують виникнення й реалізацію загроз в економічний і політичній сферах, у сфері виконання функцій держави тощо. Заподіяння шкоди в інформаційні сфері є передусім засобом досягнення інших цілей. Поряд із суто корисливою метою в сучасних умовах інформаційні загрози пов'язані з розпалюванням міжнаціональної, міжконфесійної та іншої ворожнечі, дискредитацією правоохоронної системи й органів державної влади загалом, заподіянням шкоди честі, гідності та діловій репутації фізичних осіб, формуванням «образу ворога», «зомбуванням» населення задля створення умов щодо управління масовою свідомістю. При цьому потенціал інформаційної сфери через її інтегрувальний характер і здатність «проникнення» до інших сфер життєдіяльності суспільства внаслідок їх інформаційного обслуговування поки що недостатньо усвідомлюється політиками та правоохоронцями (за винятком виявів кіберзлочинності), але успішно використовується представниками організованих злочинних угруповань і політичними супротивниками України.

Аналіз чинної законодавчої та нормативно-правової бази з позиції забезпечення інформаційної безпеки України свідчить, що у цій галузі характерна термінологічна невизначеність, неоднозначність та певна непослідовність. Покращення існуючого стану інформаційної безпеки потребує розвитку законодавства, де б визначалась сутність державної інформаційної політики України на основі чіткого і коректного понятійного апарату, уточнювались напрями її реалізації, головним із яких має бути забезпечення інформаційної безпеки держави. Україна, її державні інституції та суспільство мають формувати адекватну комплексну систему посиленого оперативного реагування на ризики інформаційної безпеки. При цьому варто перенести акценти з реакції «post factum» на превентивну діяльність, адже усі основні загрози є добре відомі.

Стратегічне інформаційне протистояння становить небезпечний компонент гібридної війни, розгорнутої Росією проти України. Головною загрозою інформаційній безпеці нашої держави залишається загроза впливу ворога на інформаційну інфраструктуру, інформаційні ресурси, суспільство, свідомість і підсвідомість особистості з метою нав'язати власну систему цінностей, поглядів, інтересів і рішень у життєво важливих сферах суспільної й державної діяльності. Інформаційна складова гібридної війни Росії проти України – це психологічна війна, метою якої є не знищення мільйонів людей, а залякування, деморалізація, світоглядне, духовно-моральне, національне покалічення українців і таким шляхом – підпорядкування їх російській імперській ідеології та політиці.

Список використаних джерел

1. *Ніщименко О. А. Інформаційна безпека України на сучасному етапі розвитку держави і суспільства / О. А. Ніщименко // Наше право. – 2016. – № 1. – С. 17–23.*
2. *Конституція України від 28.06.1996 (із змінами) // Відомості Верховної Ради України (ВВР). – 1996. – № 30. Ст. 141.*
3. *Про національне безпеке України : Закон України № 2469-VIII від 21.06.2018 // Відомості Верховної Ради (ВВР). – 2018. – № 31. – Ст. 241.*
4. *Про інформацію : Закон України № 2657-XII від 02.10.1993 // Відомості Верховної Ради України (ВВР). – 1992. – № 48. – Ст. 650.*
5. *Про Службу Безпеки України : Закон України № 2229-XII від 25.03.1992 // Відомості Верховної Ради України (ВВР). – 1992. – № 27. – Ст. 382.*
6. *Литвиненко О. Інформаційна складова у сучасній гібридній війні проти України: виклики й загрози / О. Литвиненко // Українознавчий альманах. – 2017. – Вип. 19. – С. 171–174.*
7. *Указ Президента України від 26 травня 2015 року № 287/2015 «Про введеннння в дію рішення Ради національної безпеки і оборони України» від 6 травня 2015 року «Про Стратегію національної безпеки України». [Електронний ресурс]. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/287/2015.*
8. *Курбан О.В. Інформаційне супроводження російської гібридної агресії на Донбасі (2014–2016) / О. В. Курбан // Бібліотекознавство. Документознавство. Інформологія. – 2017. – № 2. – С. 66–73.*
9. *Жайворонок О.І. Сучасні загрози інформаційного тероризму в умовах гібридної війни Росії проти України / О. І. Жайворонок // Державне управління: удосконалення та розвиток. – 2018. – № 4. – С. 1–5.*

References

1. *Nishchymenko, O.A. (2016). Informatsiyna bezpeka Ukrayiny na suchasnomu etapi rozvytku derzhavy i suspilstva [Information security of Ukraine at the present stage of development of the state and society]. Nashe parvo - Our right, (1), (pp. 17–23) [in Ukrainain].*
2. *Konstytutsiya Ukrayiny vid 28.06.1996 (iz zminamy) [The Constitution of Ukraine dated June 28, 1996 (as amended)]. (1996). Vidomosti Verkhovnoyi Rady Ukrayiny - Bulletin of the Verkhovna Rada of Ukraine. (30, (pp. 141) [in Ukrainain].*

3. *Zakon Ukrayiny «Pro natsionalne bezpeke Ukrayiny»: № 2469-VIII vid 21.06.2018 [Law of Ukraine «On National Security of Ukraine» № 2469-VIIII dated June 21, 2018]. Vidomosti Verkhovnoyi Rady - Bulletin of the Verkhovna Rada of Ukraine. (31), (pp. 241) [in Ukrainain].*
4. *Zakon Ukrayiny «Pro informatsiyu»: № 2657-KHII vid 02.10.1993 [Law of Ukraine «About information»: № 2657-XII dated 02.10.1993]. Vidomosti Verkhovnoyi Rady Ukrayiny - Bulletin of the Verkhovna Rada of Ukraine. (48), (pp. 650) [in Ukrainain].*
5. *Zakon Ukrayiny «Pro Sluzhbu Bezpeky Ukrayiny»: № 2229-KHII vid 25.03.1992 [Law of Ukraine «On the Security Service of Ukraine»: № 2229-XII of March 25, 1992]. Vidomosti Verkhovnoyi Rady Ukrayiny - Bulletin of the Verkhovna Rada of Ukraine. (27), (pp. 382) [in Ukrainain].*
6. *Lytvynenko, O. (2017). Informatsiyna skladova u suchasniy hibrydniy viyni proty Ukrayiny: vyklyky y zahrozy [Information Component in the Modern Hybrid War Against Ukraine: Challenges and Threats]. Ukrayinoznavchyy almanakh - Ukrainian Studies Almanac. (issue 19), (pp. 171-174) [in Ukrainain].*
7. *Ukaz Prezydenta Ukrayiny vid 26 travnya 2015 roku № 287/2015 «Pro vvedennnya v diyu rishennya Rady natsionalnoyi bezpeky i oborony Ukrayiny» vid 6 travnya 2015 roku «Pro Stratehiyu natsionalnoyi bezpeky Ukrayiny» [Decree of the President of Ukraine dated May 26, 2015 № 287/2015 «On the Decision of the National Security and Defense Council of Ukraine» dated May 6, 2015 «On the Strategy of National Security of Ukraine»]. http://zakon3.rada.gov.ua Retrieved from http://zakon3.rada.gov.ua/laws/show/287/2015 [in Ukrainain].*
8. *Kurban ,O.V. (2017). Informatsiyne suprovodzhennya rosiyskoyi hibrydnoyi ahresiyi na Donbasi (2014–2016) [Information support of Russian hybrid aggression on the Donbass (2014-2016)]. Bibliotekoznavstvo. Dokumentoznavstvo. Informolohiya - Library Science. Documentation. Informology (2), (pp. 66-73) [in Ukrainain].*
9. *Zhayvoronok, O.I. (2018). Suchasni zahrozy informatsiynoho teroryzmu v umovakh hibrydnoyi viyny Rosiyi proty Ukrayiny [Modern threats of informational terrorism in the context of the hybrid war against Russia]. Derzhavne upravlinnya: udoskonalennya ta rozvytok - Public administration: improvement and development. (4), (pp. 1-5) [in Ukrainain].*

Стаття надійшла до редакції 25.01.2019.