

ІНФОРМАЦІЙНА БЕЗПЕКА ДЕРЖАВИ В СИСТЕМІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

STATE INFORMATION SAFETY IN THE SYSTEM NATIONAL SECURITY OF UKRAINE

**Гаврильців М.Т., к.ю.н., доцент,
доцент кафедри адміністративно-правових дисциплін
Львівський державний університет внутрішніх справ**

Стаття присвячена дослідженню питання інформаційної безпеки держави через з'ясування сутності інформаційного захисту людини, суспільства, держави як важливої складової частини національної безпеки України в умовах гібридної війни. Зазначено, що сьогодні в Україні фактично відсутня система інформаційної безпеки, яка б могла забезпечити виявлення, аналіз інформаційних загроз національній безпеці, а також протидію цим загрозам.

Стверджується, що інформаційна складова частина є безумовним об'єктом маніпулювання в умовах гібридної війни, адже складна політична ситуація, в якій перебуває Україна останні шість років, постійне погіршення іміджу держави на міжнародній арені зумовлені низкою чинників, серед яких важливим фактором є неналежний стан системи інформаційної безпеки. Забезпечення інформаційної безпеки сьогодні стає важливою складовою частиною національної безпеки України.

Основними складовими елементами інформаційної безпеки автор називає забезпечення якісного інформування громадян, вільного доступу до різних джерел інформації, захист від негативних інформаційних впливів, що у сукупності мають сприяти цілісності суспільства.

У статті зазначено, що забезпечення інформаційної безпеки завдяки послідовній реалізації чітко сформульованої національної інформаційної стратегії значною мірою може сприяти забезпеченню досягнення успіху при вирішенні завдань у політичній, військово-політичній, військовій, соціальній, економічній та інших сферах державної діяльності. Так, втілення у життя вдалої інформаційної політики може суттєво вплинути на розв'язання внутрішньополітичних, зовнішньополітичних і військових конфліктів.

Автор доводить, система інформаційної безпеки держави є складовою частиною загальної системи національної безпеки країни і становить сукупність органів державної влади, недержавних структур і громадян, котрі повинні узгоджено здійснювати діяльність по забезпеченню інформаційної безпеки на основі єдиних правових норм, ефективно протистояти інформаційним загрозам за сучасних умов.

Ключові слова: інформація, інформаційна безпека, державна інформаційна політика, загрози інформаційній безпеці, національна безпека, стратегія національної безпеки.

The article is devoted to the study of information security of the state. The essence of information protection of human, society, state as an important component of national security of Ukraine in the conditions of hybrid war is revealed. It is noted that in Ukraine there is practically no information security system that could provide detection, analysis of information threats to national security, as well as counteracting these threats.

It is claimed that information is the object of manipulation in the context of the hybrid war that is taking place in Ukraine today. This is explained by the fact that the difficult political situation in which our country has been for the last six years, the constant deterioration of the state image in the international arena, are caused by a number of factors, among which is the poor state of the national information security system. Information security is becoming an important component of Ukraine's national security today.

The author calls the main components of information security the provision of quality information to citizens, free access to various sources of information, and protection against negative information influences. The totality of these elements should promote the unity of society.

The article states that providing information security through the consistent implementation of a clearly formulated national information strategy can help ensure success in solving problems in political, military, political, military, social, economic and other spheres of state activity. Implementing the right information policy can influence the resolution of internal political, external political and military conflicts.

The author argues that the system of information security of the state is an integral part of the general system of national security of the country and is a collection of state authorities, non-governmental organizations and citizens. Together they should carry out activities to ensure information security on the basis of legal norms, effectively withstand information threats in the current conditions.

Key words: information, information security, state information policy, threats to information security, national security, strategy of national safety.

Вступ. Протягом останньої чверті століття у світі відбувся глобальний сплеск розвитку інформаційних мереж, який можна вважати унікальним поєднанням комп'ютерів і комунікацій соціуму. Цивілізація вступила в еру інформаційного суспільства, в якому інформація стає вирішальним чинником у багатьох сферах життєдіяльності. Сьогодні практично неможливо знайти площину соціальної активності, яка б не зазнала впливу інформаційних технологій: політика, право, економіка, медицина, освіта, культура, релігія, сфера послуг і розваги. Потреба у засобах накопичення, систематизації, зберігання, пошуку, передачі інформації, забезпечення безпеки зростає.

Гостроти проблематиці додає також те, що інформаційна складова частина є безумовним об'єктом маніпулювання в умовах гібридної війни, адже складна політична ситуація, в якій перебуває Україна останні шість років, постійне погіршення іміджу держави на міжнародній арені зумовлені низкою чинників, серед яких важливим фактором є неналежний стан системи інформаційної безпеки. Дехто з фахівців навіть вважає, що в Україні фактично відсутня система інформаційної безпеки, яка б могла забезпечити виявлення, аналіз інформаційних загроз національній безпеці, а також протидію цим загрозам.

Проблематика інформаційної безпеки складна і багатоаспектна, що зумовлює необхідність вивчення й узагальнення наукових праць представників різних галузей юридичної науки. Окремі аспекти правового регулювання інформаційної сфери стали об'єктом наукового аналізу в працях українських і зарубіжних дослідників, зокрема І. Арістової, І. Бачило, Р. Каложного, Т. Костецької, О. Кохановської, Е. Макаренко, В. Цимбалюка. Ключовими для вивчення проблеми забезпечення інформаційної безпеки стали дослідження В. Гурковського, О. Золотар, В. Копилова, Б. Кормича, В. Ліпкана, В. Настюка, Н. Нижник, М. Швеца, А. Селіванова.

Постановка завдання. Мета статті – дослідження інформаційної безпеки держави через з'ясування сутності інформаційного захисту людини, суспільства, держави як важливої складової частини національної безпеки України в умовах гібридної війни.

Результати дослідження. Інформаційна сфера стала системоутворюючим фактором життя суспільства й активно впливає на стан політичної, економічної, оборонної та інших складових частин безпеки України. Проте, оперуючи інформацією, потрібно бути переконаним у тому, що використовувана інформація якісна

й у процесі передачі, поширення не була спотворена. Тому питання інформаційної безпеки є важливим компонентом усієї системи національної безпеки країни [6, с. 65].

Законодавче визначення поняття «інформація» міститься у Законі України «Про інформацію», згідно зі ст. 1 якого: «Інформацією є будь-які відомості та/або дані, що можуть бути збережені на матеріальних носіях або відображені в електронному вигляді» [16]. Аналогічне визначення міститься у ч. 1 ст. 200 Цивільного кодексу України.

Деталізоване визначення поняття «інформація» знаходимо в іншому нормативно-правовому акті – Законі України «Про захист економічної конкуренції»: це відомості в будь-якій формі й вигляді та збережені на будь-яких носіях (у т. ч. листування, книги, помітки, ілюстрації (карти, діаграми, органіграми, малюнки, схеми тощо), фотографії, голограми, кіно-, відео-, мікрофільми, звукові записи, бази даних комп'ютерних систем або повне чи часткове відтворення їх елементів), пояснення осіб і будь-які інші публічно оголошені чи документовані відомості (ст. 1 Закону [15]).

У контексті нашого дослідження необхідно звернути увагу на зміст категорії «безпека», котра у житті людини відіграє роль орієнтиру, навколо якого групуються цінності людського існування. Це поняття багатопланове, з цього приводу в науці існує багато думок. У буквальному розумінні безпека означає відсутність небезпеки. Потреба безпеки належить до числа базових мотиваційних механізмів у життєдіяльності людини, і в цьому відношенні людина мало чим відрізняється від будь-кого з інших живих істот. Крім того, безпека становить безсумнівну цінність, що має універсальний характер, оскільки визнається всіма людьми незалежно від їхньої расової, національної чи соціальної належності.

Про важливість захисту інформаційної безпеки наголошується в Конституції України: «Захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього українського народу» (ст. 17) [9].

Законодавче визначення інформаційної безпеки зафіксоване в Законі України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 рр.»: «Інформаційна безпека – стан захищеності життєво важливих інтересів людини, суспільства і держави, за якого запобігається нанесення шкоди через: неповноту, невчасність і невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації» (п. 13 Закону) [20].

Інформаційна безпека є складним, системним, багатовимірним явищем, на стан і перспективи розвитку якого мають безпосередній вплив зовнішні та внутрішні чинники, найважливішими з яких є: 1) політична обстановка у світі; 2) наявність потенційних зовнішніх і внутрішніх загроз; 3) стан і рівень інформаційно-комунікаційного розвитку країни; 4) внутрішньополітична обстановка в державі. Водночас інформаційна безпека є складною, динамічною, цілісною соціальною системою, компонентами якої є підсистеми безпеки особистості, держави і суспільства. Саме взаємозалежна, системна інформаційна єдність останніх складає якісну визначеність, покликану здійснити захист життєво важливих інтересів людини, суспільства і держави, забезпечити їх конкурентоздатний, прогресивний розвиток [7, с. 154–155].

Забезпечення інформаційної безпеки завдяки послідовній реалізації грамотно сформульованої національної інформаційної стратегії значною мірою може сприяти забезпеченню досягнення успіху при вирішенні завдань

у політичній, військово-політичній, військовій, соціальній, економічній та інших сферах державної діяльності. Так, втілення в життя вдалої інформаційної політики може суттєво вплинути на розв'язання внутрішньополітичних, зовнішньополітичних і військових конфліктів.

Чітке розуміння і виокремлення факторів, що зумовлюють загострення загроз інформаційній безпеці, мають системний характер, а тому вони охоплюють усі без винятку сфери життєдіяльності людини, суспільства і держави. На практиці аналіз викликів – це завжди суб'єктивний процес сприйняття суб'єктом певних факторів через призму власних інтересів і професійності.

Фахівці називають важливий компонент гібридної війни – вторгнення в інформаційно-комунікаційний простір певної країни з метою придушення опору та формування світового політичного стандарту, узгодженого з інтересами агресора. Для цього використовуються найрізноманітніші інструменти маніпулювання громадською думкою: втручанням у функціонування інформаційно-телекомунікаційних систем і мереж; розвиток кіберзлочинності; вплив на засоби масової комунікації та маніпуляція суспільною думкою [3, с. 18].

Як справедливо зауважує М. Дмитренко: «Характер та особливості ведення російсько-української війни свідчать, що її метою є зміна самоідентифікації населення і перетворення східного регіону нашої держави на «сіру зону», яка залишить РФ важелі свого впливу через постійну загрозу поширення нестабільності на всю Україну. Це війна не за території, а за світогляд, думки і душі людей. А оскільки контроль над інформаційною інфраструктурою дає підстави для формування суспільної думки, яка завжди спочатку виявляється в певних переконаннях, а вже потім у конкретних діях, то в умовах конкурентної боротьби контроль над інформаційною сферою перетворюється на один із основних ресурсів влади» [4, с. 40–41].

Основними визначальними факторами, що негативно впливають на інформаційний простір в Україні, слід вважати: 1) постійні втрати серед особового складу (загиблі, полонені, поранені), які ведуть до формування недовіри до українського воєнно-політичного керівництва, що нібито нездатне контролювати ситуацію, яка склалася в Україні; 2) недосконала національна система інформаційної безпеки сприяє зниженню рівня патріотизму; 3) активність зовнішніх інформаційних заходів із боку РФ впливає на формування твердження про прийнятність для України федеративного устрою держави та завершення бойових дій на Сході України на умовах кремлівського режиму [10, с. 39].

Нова редакція Доктрини інформаційної безпеки України 2017 р. актуальними загрозами національній безпеці України в інформаційній сфері визначила: здійснення спеціальних інформаційних операцій, спрямованих на піддрив обороноздатності, деморалізацію особового складу Збройних Сил України та інших військових формувань, провокування екстремістських проявів, підживлення панічних настроїв, загострення і дестабілізацію суспільно-політичної та соціально-економічної ситуації, розпалювання міжетнічних і міжконфесійних конфліктів в Україні; проведення державою-агресором спеціальних інформаційних операцій в інших державах з метою створення негативного іміджу України у світі; інформаційна експансія держави-агресора та контрольованих нею структур, зокрема шляхом розширення власної інформаційної інфраструктури на території України та в інших державах; інформаційне домінування держави-агресора на тимчасово окупованих територіях; недостатню розвиток національної інформаційної інфраструктури, що обмежує можливість України ефективно протидіяти інформаційній агресії; неефективність державної інформаційної політики, недосконалість законодавства

стосовно регулювання суспільних відносин в інформаційній сфері, невизначеність стратегічного нарративу, недостатній рівень медіа-культури суспільства; поширення закликів до радикальних дій, пропаганду федералізму та сепаратизму в Україні [5].

Специфіка забезпечення національної інформаційної безпеки відображена в Законах України «Про національну безпеку України» [19], «Про концепцію національної програми інформатизації» [18], «Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» [20], а також у затвердженій указом Президента Стратегії національної безпеки України [21], у зв'язку з реалізацією Стратегії Національна рада безпеки і оборони України ухвалила рішення про створення спеціального нового органу як робочого органу – Національного координаційного центру кібербезпеки. Створення такого центру є обґрунтованим, оскільки повноваженнями щодо забезпечення інформаційної безпеки наділена значна кількість державних органів та установ (Національна рада України з питань телебачення і радіомовлення, Держкомтелерадіо України, Служба безпеки України, Служба зовнішньої розвідки України, Міністерство оборони України, МВС України, Міністерство закордонних справ України, Міністерство юстиції України та ін.).

Значна кількість норм, що регулюють державний вплив в інформаційній сфері, вимагає їх певної класифікації для системного сприйняття. Найбільш доцільним для цілей нашого дослідження є їх розмежування за призначенням у системі державного управління, а також за об'єктом державного регулювання. Залежно від призначення тієї чи іншої правової норми в регулюванні функціонування складових елементів інформаційної сфери ці норми можливо об'єднати в такі чотири групи:

1) норми, що закріплюють цілі, основні завдання та напрями діяльності держави в інформаційній сфері, визначають основні параметри розвитку останньої. Ця група норм, до яких належать, зокрема, норми, закріплені у ст. 3, 10, 17, 31, 32, 34 Конституції, у ст. 6 Закону України «Про інформацію» [16], в розділах IV, VI Закону «Про Концепцію Національної програми інформатизації» [18], Законі «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» [20] та в інших, має цілеспрямоване значення для функціонування всієї системи державного управління в інформаційній сфері;

2) норми, що визначають систему органів (суб'єктів) державного регулювання в інформаційній сфері та їх адміністративно-правовий статус. До таких норм належать вже згадані норми Конституції України, які стосуються Держкомтелерадіо та Національної ради. Правовий статус окремих органів влади визначається і нормами законів. Так, у ст. 20 Закону «Про Кабінет Міністрів України» серед його повноважень згадується проведення державної політики у сфері інформатизації, сприяння становленню єдиного інформаційного простору та ін. [17].

Важливе місце в цій групі норм займають також норми, закріплені в підзаконних нормативно-правових актах, передусім ті з них, що містяться в актах Президента України та Кабінету Міністрів України, якими визначається адміністративно-правовий статус міністерств, інших органів державного управління в інформаційній сфері;

3) норми, що регулюють порядок взаємодії органів (суб'єктів) влади з керованими ними суб'єктами інформаційних та інформаційно-інфраструктурних відносин у процесі реалізації прямих і зворотних зв'язків між ними. До цієї групи належать норми, які регламентують процедури застосування різних методів державного регулювання в інформаційній сфері, визначають форми їх реалізації. Такі норми закріплені, зокрема, у ст. 23–37 Закону «Про телебачення і радіомовлення», які регламентують процедуру здійснення такого методу регулювання, як ліцензування в галузі телебачення і радіомовлення [22]. У Законі «Про

друковані засоби масової інформації (пресу) в Україні» врегульовано порядок здійснення обов'язкової державної реєстрації друкованих засобів масової інформації [14]. У ст. 22 Закону «Про державну таємницю» регламентовано порядок надання допуску громадян до державної таємниці [12]. Застосування цілої низки заходів адміністративного примусу врегульовано нормами Кодексу України про адміністративні правопорушення [8]. У цих же законах та інших нормативно-правових актах визначаються і вимоги до форми правових актів, що приймаються при застосуванні зазначених методів. Після тривалих дискусій у 2011 р. законодавчу базу країни поповнив закон «Про доступ до публічної інформації» [13], яким встановлено більш ефективні механізми звернення до органів державної влади для отримання інформації, яка перебуває в їх розпорядженні;

4) норми, що визначають адміністративно-правовий статус суб'єктів інформаційних відносин. Так, наприклад, ст. 39 Закону «Про телекомунікації» на операторів телекомунікацій покладаються обов'язки: своєчасно надавати щорічно до центрального органу виконавчої влади в галузі зв'язку інформацію про свої телекомунікаційні мережі для відпрацювання мобілізаційних планів; за власні кошти встановлювати на своїх телекомунікаційних мережах технічні засоби, необхідні для здійснення уповноваженими органами оперативного-розшукових заходів, і забезпечувати функціонування цих технічних засобів, а також сприяти проведенню оперативного-розшукових заходів тощо [23].

Стратегія національної безпеки України актуальними загрозами національній безпеці України в інформаційній сфері визначає ведення інформаційної війни проти України та відсутність цілісної комунікативної політики держави, недостатній рівень медіа-культури суспільства [1, с. 12]. Не менш гостро в умовах гібридної війни постає питання кібербезпеки. У сучасному світі кібернетичний простір дедалі частіше слугує для проведення широкого спектра підривних операцій: від викрадення цінної інформації до актів кібертероризму [3, с. 18].

Насамперед мережі та інформаційні системи містять конфіденційні дані й економічно цінну інформацію, що підвищує стимул для атак. Атаки на інформаційні системи можуть мати серйозні у національному масштабі наслідки, як то перебої у роботі систем комунікацій, витік конфіденційної інформації тощо [2, с. 28].

Зрозуміло, що сьогодні українське суспільство перебуває під постійною загрозою отримання недостовірної, а подеколи – шкідливої інформації, її несвоечасного надходження, шпигунства, комп'ютерної злочинності тощо. Ці фактори є елементами гібридної війни, які сприяють вторгненню агресора в національну свідомість громадян, підриву національної та інформаційної безпеки.

Основними складовими елементами інформаційної безпеки є як забезпечення якісного інформування громадян і вільного доступу до різних джерел інформації, так і захист від негативних інформаційних впливів, що у сукупності мають сприяти цілісності суспільства. Першочерговим завданням соціальних і державних інститутів має бути розробка термінових ефективних заходів щодо нейтралізації інформаційно-диверсійної діяльності РФ проти України та запобігання її подальшому розгортанню. Вирішення цієї комплексної проблеми дозволить захистити інтереси суспільства і держави, сприяти реалізації права громадян на отримання всебічної та якісної інформації [11, с. 38].

В умовах гібридної війни держава, що стала об'єктом агресії, неминує наражатися на широкий спектр інформаційних загроз, нейтралізація яких, з одного боку, вимагає вжиття надзвичайних правових і адміністративних заходів, а з іншого – може супроводжуватися істотним згортанням демократичних прав і свобод. Пошук балансу між інтересами національної безпеки й ідеями верховенства права – це стратегічно важливе завдання держави.

Мас-медіа є чи не найфективнішою зброєю, яка використовується в сучасних гібридних війнах. Зважаючи на це, державна політика в галузі інформаційного права має орієнтуватися на вибіркоче застосування обмежень щодо конкретних ЗМІ, які зарекомендували себе недружніми, заангажованими та маніпулятивними. Такий підхід вимагає максимальної правової визначеності обмежувальних критеріїв, оскільки за їх відсутності існує ризик потрапляння під заборону незаангажованих і політично нейтральних мас-медіа (наприклад, у разі нецілеспрямованого поширення недостовірної інформації). Водночас широке коло громадських діячів та організацій наголошують, що встановлені заборони позбавлені фактичних підстав, не мають правового обґрунтування, суперечать Конституції, утискають демократичні права і свободи. Тому будь-які обмеження в інформаційному середовищі повинні мати точковий характер і стосуватися лише тих ресурсів, які скомпromетували себе конкретними діями або є джерелом загроз для держави та суспільства [3, с. 21–22].

Нормативно-правова регламентація формування єдиного інформаційного простору України повинна сприяти гармонійному розвитку інформаційних ресурсів, інформаційних послуг та інформаційного продукту в країні. Важливість проблеми розвитку законодавства у сфері інформації та інформаційної безпеки, становлення інформаційного суспільства визначається тією обставиною, що норми законів цієї сфери суттєво впливають на законодавче регулювання відносин суб'єктів у всіх сферах життя держави.

В умовах проведення країною-агресором РФ деструктивного інформаційного впливу на цільову аудиторію України та інших держав світу можна визначити такі основні напрями вжиття заходів щодо захисту національного інформаційного простору і забезпечення національної системи інформаційної безпеки України: по-перше, удосконалити нормативно-правову базу у сфері інформаційної політики держави, яка б визначала взаємодію силових структур України з органами місцевого самоврядування, державними органами та громадськими інституціями; по-друге, створити єдиний міжвідомчий координаційний орган, який би здійснював керівництво, координацію та контроль заходів інформаційної безпеки, (його, наприклад, можна створити у вигляді міжвідомчої комісії при РНБО); по-третє, створити систему комплексного моніторингу популярних аудіовізуальних і друкованих ЗМІ, а також популярних Інтернет-ресурсів; по-четверте, заохочувати подальші комплексні наукові дослідження у сфері інформаційної безпеки.

На основі Стратегії національної безпеки України Указом Президента України була затверджена Доктрина інформаційної безпеки України, що лягла в основу національної політики інформаційної безпеки. Метою доктрини є уточнення засад формування та реалізації державної інформаційної політики, насамперед щодо протидії руйнівному інформаційному впливу РФ в умовах розв'язаної нею гібридної війни. Доктрина визначає національні інтереси України в інформаційній сфері, загрози їх реалізації, напрями, пріоритети державної політики в цій сфері.

Державна інформаційна політика в умовах глобалізації буде ефективною лише у тому разі, якщо вона матиме комплексний, системний характер і, безперечно, буде відкритою, наведеною на удосконалення інтересів громадян, суспільства і держави.

Загалом політика інформаційної безпеки як суспільне явище має комплексний характер, включаючи внутрішню та зовнішньополітичні, економічні, технологічні, військові та інші елементи, тому вимагає комплексного підходу. Діяльність органів державної влади повинна спрямовуватися на виконання конкретних завдань у цій сфері й об'єднуватися єдиною метою – надання належних умов для реалізації забезпечення інформаційної безпеки України.

Система інформаційної безпеки держави є складовою частиною загальної системи національної безпеки країни та становить сукупність органів державної влади, недержавних структур і громадян, які повинні узгоджено здійснювати діяльність по забезпеченню інформаційної безпеки на основі єдиних правових норм, ефективно протистояти інформаційним загрозам за сучасних умов.

ЛІТЕРАТУРА

1. Белай С.В., Корнієнко Д.М. Інформаційна безпека сьогодення – невід'ємна складова воєнної безпеки. *Актуальні проблеми управління інформаційною безпекою держави*. Київ : Національна академія Служби безпеки України, 2018. 408 с.
2. Войціховський А.В. Кібербезпека як важлива складова системи захисту національної безпеки європейських країн. *Журнал східноєвропейського права*. 2018. № 53. С. 26–37.
3. Гуржій Т. Інформаційне право: виклики гібридної війни. *Зовнішня торгівля: економіка, фінанси, право*. 2018. № 4. С. 16–26.
4. Дмитренко М.А. Проблемні питання інформаційної безпеки України. *Міжнародні відносини. Серія Політичні науки*. 2017. № 17. С. 236–243.
5. Доктрина інформаційної безпеки України : затверджено Указом Президента України від 25 лютого 2017 р. № 47/2017. URL: <http://zakon.rada.gov.ua/laws/show/47/2017>.
6. Задірака В.К. Сучасні методи розв'язання задач інформаційної безпеки. *Вісник НАН України*. 2014. № 5. С. 65–69.
7. Золотар О.О. Інформаційна безпека людини: теорія і практика : монографія. Київ : ТОВ «Видавничий дім «АртЕк», 2018. 446 с.
8. Кодекс України про адміністративні правопорушення від 07 грудня 1988 р. № 80731-10. URL: <http://zakon2.rada.gov.ua/laws/show/80731-10>.
9. Конституція України від 28 червня 1996 р. URL: <http://zakon5.rada.gov.ua/laws/show/254к/96-вр>.
10. Косоков О.М., Сірик А.О. Завдання захисту національного інформаційного простору за досвідом ведення гібридної війни РФ на Сході України. *Системи озброєння і військова техніка*. 2017. С. 38–41.
11. Левченко Ю.О. Проблеми протидії інформаційній окупації в умовах гібридної війни. *Інформаційна безпека в умовах гібридної війни: Міжнародна науково-практична конференція (м. Хмельницький, 16–17 листопада 2017 р.)*. Хмельницький : МВС УКРАЇНИ, 2017. 50 с.
12. Про державну таємницю : Закон України від 21 січня 1994 р. № 3855-XII. URL: <http://zakon.rada.gov.ua/laws/show/3855-12>.
13. Про доступ до публічної інформації : Закон України від 13 січня 2011 р. № 2939-VI. URL: <http://zakon.rada.gov.ua/laws/show/2939-17>.
14. Про друковані засоби масової інформації (преси) в Україні : Закон України від 16 листопада 1992 р. № 2782-XII. URL: <http://zakon.rada.gov.ua/laws/show/2782-12>.
15. Про захист економічної конкуренції : Закон України від 11 січня 2001 р. № 2210-III. URL: <http://zakon.rada.gov.ua/laws/show/2210-14>.
16. Про інформацію : Закон України від 02 жовтня 1992 р. № 2657-XII. URL: <http://zakon.rada.gov.ua/laws/show/2657-12>.
17. Про Кабінет Міністрів України : Закон України від 27 лютого 2014 р. № 794-18. URL: <http://zakon2.rada.gov.ua/laws/show/794-18>.
18. Про Концепцію Національної програми інформатизації : Закон України від 04 лютого 1998 р. № 75/98-ВР. URL: <http://zakon.rada.gov.ua/laws/show/75/98-%D0%B2%D1%80>.
19. Про національну безпеку України : Закон України від 21 червня 2018 р. № 2469-VIII. URL: <http://zakon.rada.gov.ua/laws/show/2469-19#n355>.
20. Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 рр. : Закон України від 09 січня 2007 р. № 537-V. URL: <http://zakon.rada.gov.ua/laws/show/537-16?find=1&text=%E1%E5%E7%E>.
21. Про Стратегію державної політики сприяння розвитку громадянського суспільства в Україні та першочергові заходи щодо її реалізації : указ Президента України від 26 травня 2015 р. № 287/2015. URL: <http://zakon.rada.gov.ua/laws/show/287/2015#n14>.
22. Про телебачення і радіомовлення : Закон України від 21 грудня 1993 р. № 3759-XII. URL: <http://zakon.rada.gov.ua/laws/show/3759-12>.
23. Про телекомунікації : Закон України від 18 листопада 2003 р. № 1280-IV. URL: <http://zakon.rada.gov.ua/laws/show/1280-15>.