УДК 329.09.5
DOI https://doi.org/10.32851/tnv-pub.2022.4.3

ПОНЯТІЙНО-КАТЕГІОРІАЛЬНИЙ АПАРАТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ В ЗАБЕЗПЕЧЕННІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Дикий А. П. *– кандидат економічних наук, доцент, доцент кафедри національної безпеки, публічного управління та адміністрування Державного університету «Житомирська політехніка»*
ORCID: 0000-0002-5819-0236

Дика О. С. *– кандидат економічних наук, доцент, доцент кафедри національної безпеки, публічного управління та адміністрування Державного університету «Житомирська політехніка»*
ORCID ID: 0000-0002-4195-5124

Наумчук К. М. *– доктор філософії, доцент кафедри національної безпеки, публічного управління та адміністрування Державного університету «Житомирська політехніка»*
ORCID: 0000-0002-4195-5124

Тростенюк Т. М. *– доктор філософії, доцент кафедри національної безпеки, публічного управління та адміністрування Державного університету «Житомирська політехніка»*
ORCID: 0000-0001-7130-7454

В статті досліджено основні поняття інформаційної безпеки України які впливають на національну безпеку з врахуванням умов, що склались. Початок повномасштабного вторгнення російських військ на територію України змусив всю нашу країну не лише перейти в режим воєнного стану але й кардинально змінити тактику дій задля збереження своєї цілісності. Підступність ворога криється не лише в загарбництві, але й в особливостях ведення боротьби, яка відображається в розповсюдженні недостовірної інформації. Таким чином, ворог застосовує тактику гібридної війни, в якій окрім крилатих ракет, збройного наступу, психологічного тиску зазнають громадяни не лише тимчасово окупованих територій. Завдяки активним спробам інформаційних атак однією з основних загроз інформаційної безпеки є дезінформація всього суспільства.

Світові тенденції свідчать, що саме активне поглиблення сфер професійної діяльності, освіти, науки, техніки пов'язане з динамічним розвитком суспільного життя. Сучасний стан розвитку інформаційних технологій повинен відповідати динаміці розвитку державних та приватних інформаційних структур. Як результат – Україна активно реалізовує усі вимоги щодо забезпечення усіх сфер життєдіяльності висококваліфікованими кадрами галузі інформаційного забезпечення. Проте, активні спроби ворога атакувати інформаційні ресурси, задля використання у своїх цілях, змушують дослідити поняття інформаційної безпеки з іншого боку.

Негативний інформаційний вплив відбувається за рахунок застосування найновітніших технологій впливу шляхом розповсюдження завідомо неправдивої інформації яка спричиняє внутрішні конфлікти національного та релігійного характеру, підриває віру громадян до державного управління, пропагандує початок внутрішніх озброєних конфліктів, порушує суверенітет і територіальну цілісність держави.

Своєчасне виявлення негативного інформаційного впливу потребує наукового обґрунтування поняття інформаційної безпеки та можливості оцінки усіх можливих загроз та впливів задля мінімізації їх наслідків. Актуальність застосування такого підходу обумовлена пошуком та застосуванням актуальних моделей виявлення інформаційних впливів.

Ключові слова: *інформація, інформаційна безпека, національна безпека, професійна підготовка, держава, державне управління.*

Dykiy A. P., Dyka O. S., Naumchuk K. M., Trosteniuk T. M. Conceptual and categorical apparatus of information security of Ukraine in ensuring national security

The article examines the main concepts of information security of Ukraine, which affect national security, taking into account the existing conditions. The beginning of a full-scale invasion of Russian troops on the territory of Ukraine forced our entire country not only to go into martial law, but also to radically change the tactics of actions in order to preserve its integrity. The insidiousness of the enemy lies not only in the invasion, but also in the peculiarities of the struggle, which is reflected in the spread of false information. Thus, the enemy uses the tactics of a hybrid war, in which, in addition to cruise missiles, armed offensives, and psychological pressure, citizens of not only temporarily occupied territories are subjected. Due to active attempts of information attacks, one of the main threats to information security is disinformation of the entire society.

World trends indicate that the active deepening of the spheres of professional activity, education, science, and technology is connected with the dynamic development of social life. The current state of information technology development should correspond to the dynamics of the development of state and private information structures. As a result, Ukraine actively implements all requirements for providing all spheres of life with highly qualified personnel in the field of information provision. However, the enemy's active attempts to attack information resources for their own purposes force us to examine the concept of information security from another angle.

Negative informational influence occurs due to the use of the latest technologies of influence through the dissemination of known false information that causes internal conflicts of a national and religious nature, undermines the faith of citizens in state administration, promotes the beginning of internal armed conflicts, violates the sovereignty and territorial integrity of the state.

Timely detection of negative information impact requires scientific substantiation of the concept of information security and the ability to assess all possible threats and impacts in order to minimize their consequences. The relevance of using such an approach is due to the search and application of current models for the detection of informational influences.

Key words: *information, information security, national security, professional training, state, public administration.*

Постановка проблеми. Інтенсивний розвиток інформаційних технологій є одним із основних чинників подальшого соціально-економічного, духовного та інтелектуального розвитку країни. Разом з тим, стрімка інформатизація суспільства є одночасним викликом, адже використання передових інформаційних технологій відбувається не лише в цілях підтримки життєдіяльності країни але й навпаки, для розгортання воєн. Зокрема, інформаційна складова становить серйозну загрозу національній безпеці та виступає ключовим елементом гібридної війни проти України.

Аналіз останніх досліджень і публікацій. Питаннями інформаційної безпеки, проблемами її захисту, захисту національного інформаційного простору було присвячено багато наукових праць. Зокрема, дослідження проблеми можна зустріти в працях таких вчених як: Марущака А., Петрика В., Ліпкана В., Кормича Б., В. Почепцова та інших фахівців. Однак, не зважаючи на значну увагу вищезазначених фахівців, дослідження понятійно-категоріальний апарат інформаційна безпека потребує уточнення.

Метою статті є аналіз основних понять інформаційної безпеки, що впливають на забезпечення національної безпеки України.

Виклад основного матеріалу. Явище інформаційної безпеки є достатньо складним, воно певним чином інтегровано в складову національної безпеки, що розглядається як одна з пріоритетних функцій держави. Саме тому, успішне дослідження є можливим завдяки успішно-розробленому понятійному апарату. Для цього нам необхідно розглянути основні поняття, визначення та терміни, які розширять наше уявлення про інформаційну безпеку в цілому. Тому, за допомогою табл. 1. розглянемо та порівняємо поняття «Інформація».

Таблиця 1

Огляд основних понять явища інформація

Джерело	Характеристика
Цивільний кодекс України. [1]	Відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді.
Законом України «Про захист економічної конкуренції» [2]	Відомості в будь-якій формі й вигляді та збережені на будь-яких носіях (у тому числі 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 та будь-які інші публічно оголошені чи документовані відомості (п. 2 ст. 1) .
Закон України «Про інформацію» [3]	Матеріальний носій, що містить інформацію, основними функціями якого є її збереження та передавання у часі та просторі.
Енциклопедичний словник [4]	Первинно відомості, які передаються людьми усним, письмовим або іншим способом (за допомогою умовних сигналів, технічних засобів і т.д.); з середини XX століття загальнонаукове поняття, що включає обмін відомостями між людьми, людиною і автоматом, автоматом і 4 автоматом; обмін сигналами в тваринному і рослинному світі; передачу ознак від клітини до клітини, від організму до організму» .
К. Шеннон [5]	Ті повідомлення, які зменшують невизначеність у одержувача інформації».
Н. Вінер [6].	Позначення змісту, отриманого із зовнішнього світу (людиною) в процесі нашого пристосування до нього і пристосування до нього наших почуттів.

В таблиці наведено лише незначну частину різних тлумачень поняття, проте ми можемо спостерігати його різноманітність, що свідчить про розкриття тієї чи іншої грані даного феномена. На нашу думку, в сучасних реаліях доцільніше всього було б вважати, що *інформація – проаналізовані та оброблені відомості про дії, події, яким характерне збереження для подальшого вивчення, використання та розповсюдження.*

Наступним кроком нашого дослідження є доцільним розглянути поняття «Інформаційна безпека», яке відображено в табл. 2.

Визнання поняття інформаційної безпеки як однієї з функції держави, зі своїми цілями і завданнями, складною структурою, властивою тільки їй специфікою, викликала необхідність більш детального вивчення питання кодифікації інформаційного законодавства, яка підтримується багатьма науковцями-юристами та дослідниками національного інформаційного простору.

Отже, у загальному випадку інформаційна безпека – стан захищеності інформаційного суспільного середовища, який виступає як одна зі складових його формування.

Аналізуючи державну політику в інформаційній сфері, розглядаючи інформаційну безпеку як складову національної безпеки, виходимо з того, що інформаційна безпека – це такий стан захищеності життєво важливих інтересів, а, отже, й інформаційної озброєності держави, суспільства, особистості, за якого жодні інформаційні впливи на них неспроможні викликати деструктивні думки і дії, що

Таблиця 2

Огляд основних понять явища інформаційної безпеки

Джерело	Характеристика
Конституція України [7]	Захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього українського народу
Ільницька У. [8]	Інформаційну безпеку слід розуміти як сукупність засобів забезпечення інформаційного суверенітету України, захист інформаційної сфери від зовнішніх і внутрішніх інформаційних загроз
Навчальний посібник [9]	Інформаційна безпека – це невід'ємне право людини, суспільства, держави на самовизначення та участь у формуванні, розвитку та здійсненні національної інформаційної політики відповідно до чинних правових актів країни, міжнародного права. Інформаційну небезпеку створюють інформаційні загрози, що поширюються в інформаційному просторі, який більшість учених розглядає як місце формування, поширення та споживання інформації за допомогою різноманітних технічних пристроїв
В. Богуш	Стан захищеності інформаційного середовища, який відповідає інтересам держави, за якого забезпечується формування, використання і можливості розвитку незалежно від впливу внутрішніх та зовнішніх інформаційних загроз.
Б.А Кормич	Захищеність встановлених законом правил, за якими відбуваються інформаційні процеси в державі, що забезпечують гарантовані Конституцією умови існування і розвитку людини, всього суспільства та держави.
О.І. Барановський	Стан захищеності національних інтересів України в інформаційному середовищі, за якого не допускається (або зводиться до мінімуму) завдання шкоди особі, суспільству, державі через неповноту, несвоєчасність, недостовірність інформації й несанкціоноване її поширення та використання, а також через негативний інформаційний вплив та негативні наслідки функціонування інформаційних технологій.

призводять до негативних відхилень на шляху стійкого прогресивного розвитку названих суб'єктів [10].

Якщо враховувати виклики, з якими зіштовхнулись країна 24 лютого, інформаційну безпеку слід розглядати як поняття інформаційної безпеки держави, що є певним станом захищеності за якої спеціальні інформаційні операції, зовнішні інформаційні агресії, незаконне розповсюдження та використання інформації є неможливим, адже це є деструктивним фактором який впливає на національну безпеку.

На сьогодні існують аспекти, які визначають категорії «інформаційна безпека», до яких відносять:

1. Аспекти нормативно-правового характеру, що ґрунтується на аналізі нормативно-правових актів. Основними нормативними документами зазначеного аспекту є: Закон України «Про Концепцію Національної програми інформатизації» (розглядає інформаційну безпеку як невід'ємну частину політичної, економічної, оборонної та інших складових національної безпеки); Закон України «Про основи національної безпеки України» (в зазначеному нормативному документі

поняття «інформаційна безпека» не розкривається, проте основна увага фокусується на інформаційній сфері національної безпеки, при чому, не дається визначення навіть і даного поняття, а лише перераховуються загрози та напрями державної політики).

2. Доктрильний аспект, який виходить з аналізу трактувань терміну в роботах дослідників, фахівців цієї галузі. В зазначеному аспекті під інформаційною безпекою розуміють такий стан правових норм і відповідних їм інститутів безпеки, які беруть на себе відповідальність за гарантування постійної наявності даних для прийняття стратегічних рішень та захист інформаційних ресурсів країни;

3. Енциклопедичний аспект. За основу взято – багаторічний аналіз визначень, наведених у словниках, енциклопедіях різних країн та вчених. В цьому контексті інформаційна безпека означає: законодавче формування державної інформаційної політики; гарантування свободи інформаційної діяльності та права доступу до інформації у національному інформаційному просторі України; створення і впровадження безпечних інформаційних технологій; охорону державної таємниці, а також інформації з обмеженим доступом; захист національного інформаційного простору України від розповсюдження спотвореної або забороненої для поширення інформаційної продукції.

Враховуючи всі події, які відбуваються на території нашої країни, необхідно приділяти увагу поняттю загрози (англ. threat) – будь-які обставини або події, що можуть бути причиною порушення політики безпеки інформації і/або нанесення збитків автоматизованій системі. Спробу реалізації загрози називають «атакою». Загроза безпеці інформації (англ. security threat) – загрози викрадення, зміни або знищення інформації. Вони бувають випадковими або навмисними. [11].

На сьогоднішній день, до основних загроз інформаційній безпеці системі управління національною безпекою можна віднести:

– розкриття інформаційних ресурсів;
– порушення їх цілісності;
– збій в роботі самого обладнання.

Існування таких загроз більшою мірою пов’язане з значною кількістю хакерських атак з боку країни агресора, який прагне усіма можливими способами вивести наше суспільство з рівноваги, шкодити розповсюдженню правдивої інформації про стан справ, незаконно збагатитись за рахунок використання наших активів.

Існування значної чисельності загроз, відповідно до загальної класифікації загроз національній безпеці, вимагає виокремлення загроз інформаційній безпеці та поділити їх за різними критеріями. Отже, загрози інформаційній безпеці можна поділити за :

1. Джерелами походження:

– природного походження. Можуть виникати в результаті масового руйнування каналів зв’язку через повені, торнадо, грози та ін.;

– техногенного походження. Вони можуть бути спричинені аваріями на інженерних мережах і спорудах життєзабезпечення, аваріях головних серверів системи управління національною безпекою, ракетними обстрілами з боку країни агресора;

– антропогенного походження. В більшості випадків спричинені помилковим запуском програм, навмисного/ненавмисного допущення через недотримання правил безпеки роботи в Інтернеті інсталяції закладок.

2. Характером реалізації:

– реальні – ті, в яких дестабілізації є неминучою і не обмежена ні часом ні простором;

– потенційні – ті шляхи, де дестабілізації можливі за певних умов середовища функціонування органів публічної влади;

– здійснені – ті загрози, які вже втілені у життя;

– уявні – ті, реалізація яких є умовно чи схожа з існуючими, але такими не є.

3. Ступенем гіпотетичної шкоди:

– загроза яка є явною чи потенційною дією, яка ускладнює або унеможливлює реалізацію національних інтересів у інформаційній сфері;

– небезпека яка є безпосередньою дестабілізацією функціонування системи управління національною безпекою.

4. Ймовірністю реалізації:

– вірогідні, тобто можливі за виконання певного комплексу умов;

– неможливі, тобто ті за виконання певного комплексу умов ніколи не настануть;

– випадкові, ті які за виконання певного комплексу умов можуть реалізуватись по-різному.

5. Рівнем детермінізму:

– випадкові (загрози, які можуть трапитися або не трапитися – загрози хакерів дестабілізувати інформаційній системи органів влади) [12].

Саме необхідність протидії загрозам зумовлює можливість дослідження національної безпеки з погляду функціонально-діяльнісного підходу, відповідно до якого національна безпека розглядається як динамічне явище, котре постійно еволюціонує, забезпечуючи реалізацію національних інтересів [13, с. 39] в умовах можливого розгортання загроз, а також дає змогу оцінювати можливості суспільства щодо належного забезпечення «гомеостатичного стану» об'єктів національної безпеки.

Загрози національній безпеці можуть бути класифіковані за різними підставами, що висвітлює їх складну та багатошарову систему. Зокрема, у науковій політологічній думці загрози національній безпеці класифікуються за місцем знаходження джерела – зовнішні та внутрішні; за масштабами можливих наслідків – загальнонаціональні, регіональні, локальні, поодинокі; за ступенем сформованості – потенційні, реальні; за ступенем суб'єктивного сприйняття – завищені, занижені, мінімальні, умовні, адекватні; за характером виникнення – загрози природного, техногенного й соціального характеру; за сферами життєдіяльності – загрози в економічній, політичній, оборонній, міжнародній, соціальній, інформаційній, науково-технічній, екологічній, культурній і духовній сферах [13, с. 203–205] тощо.

Таким чином, варто відзначити, що інформаційна безпека займає особливе місце в системі національної безпеки країни. Оскільки інформатизація суспільства є основою його активного розвитку, слід зауважити що саме від інформаційної безпеки залежить уся інформаційно-мережева економіка країни, адже інформаційний продукт є її основою. Саме тому, дослідження основних понять інформаційної безпеки є основою забезпечення національної безпеки. В свою чергу, слід відмітити, що дослідження небезпечності загроз інформаційній безпеці було приділено багато уваги таким вченим як Г. Сащук. Вчений зазначав: «Ураховуючи той факт, що під впливом інформаційних атак може цілеспрямовано змінюватися світогляд і мораль як окремих осіб, так і суспільства загалом, нав'язуються чужі інтереси, мотиви, спосіб життя, на перший план випливає аналіз сутності й форм виявів сучасних методів прихованого агресивного впливу, вияву дій, що мають цілеспрямований агресивний характер і які суперечать

інтересам національної безпеки» [10]. Важко не погодитись, адже ми спостерігаємо активні інформаційні атаки з боку країни агресора, які намагаються вплинути на свідомість людей задля розповсюдження недостовірної інформації про стан справ, владу, економічну, політичну та інші ситуації. Такі дії потребують постійного державного нагляду та впливу, оскільки саме транскордонні інформаційні загрози (ті, що мають політичне забарвлення) є однією з складових не лише інформаційної війни. Від 24 лютого уся країна перебуває не лише під впливом активних воєнних дій на сході та ракетних обстрілів всієї території, але й зазнає удару з боку інформаційної зброї. Активні спроби заволодіння та використання інформаційних ресурсів, які не входять в групу загальнодоступних, прагнення їх незаконного розповсюдження, знищення та модифікацію є спробою ворога дійти до своєї мети.

Таким чином, ми можемо стверджувати, що в ході дослідження понятійно-категоріального апарату інформаційної безпеки ми дійшли згоди, що в сучасних умовах проти українського народу досить активно відбувається використання інформаційних технологій аби створювати реальну загрозу усьому інформаційному простору. Ворог реалізовує свої плани через розповсюдження листів на корпоративні пошти (задля виведення операційних систем з ладу, блокування роботи державних установ, використання інформаційних ресурсів в своїх цілях), зламує офіційні сайти (розміщення інформації, яка наводить паніку серед населення) та виведення з ладу роботу банківських систем (блокування роботи програм, наведення хаосу серед населення та гальмування внутрішніх та зовнішніх розрахункових операцій). Дієвим вирішенням зазначених загроз мають бути наступні дії: активна інтеграція України до світового інформаційного простору; інтеграція у міжнародні інформаційно-комунікаційні системи; створення власної інформаційної моделі; модернізація усієї інформаційної системи; удосконалення існуючого законодавства з питань інформаційної безпеки.

Висновки і пропозиції. Підсумовуючи вищезазначене, можемо стверджувати, що дослідженнями понять інформаційної безпеки займались вчені ще на початку 90-х років, проте цьому питанню не приділяли значної уваги через відсутність активної зацікавленості. В ході дослідження ми виявили, що відсутні концептуальні документи, які врегульовували б питання інформаційної безпеки. Стрімкий розвиток суспільства, активне впровадження науки та техніки в усі сфери життєдіяльності, перехід до цифрової економіки та електронного документообігу – змусило розглянути обрану тему по новому. В результаті дослідження було виявлено, що інформаційна безпека є достатньо складним, системним та багаторівневим явищем на яке можуть впливати чинники внутрішнього та зовнішнього середовища, світові зміни, внутрішньополітична ситуація в країні, стан інформатизації суспільства. Враховуючи події, які відбуваються в нашій країні – значна увага була приділена загрозам інформаційної безпеки адже саме вони впливають на економічний, політичний та соціальний простір. Інформаційний простір є достатньо потенціальною сферою для усвідомлення, адже інтегруючий характер, можливість проникнення – все це є загрозою національній безпеці та має враховуватись посадовцями нашої держави. Слід зауважити, що активне інформаційне протистояння є основним елементом протидії гібридній війні з росією, однією з основних загроз й досі є можливість впливу ворога на інформаційну структуру. Подолати ворога в цій війні можливо, завдяки активному захисту інформаційного суверенітету, розробка дієвої тактики протидії медіа загрозам на стадії їх поширення.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ:

1. Цивільний Кодекс України від 16.01.2003 р. № 435-IV. URL: http://zakon1.rada.gov.ua
2. Закон України «Про захист економічної конкуренції» від 11.01.2001 р. № 2210-III: URL: https://zakon.rada.gov.ua/laws/show/2210-14
3. Закон України «Про інформацію» від 02.10.1992 р. № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text
4. Большой энциклопедический словарь. URL: http://www.vedu.ru/bigencdic/24156/
5. Shannon C.E. A Mathematical Theory of Communication. Bell System Technical Journal, Vol. 27, pp. 379–423, 623–656, July, 11 October, 1948.
6. Винер Н. Кибернетика и общество. М., 1958.
7. Конституція України від 28.06.1996 р № 254к/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text
8. Ільницька У. Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам. Humanitarian vision. 2016. Вип. 2 (1). С. 27–32.
9. Інформаційна безпека держави у контексті протидії інформаційним війнам : навчальний посібник. Заг. ред. В. Толубка. Київ : НАОУ, 2004. 177 с.
10. Сащук Г. Інформаційна безпека в системі забезпечення національної безпеки. URL: http:// journ. univ.kiev.ua/trk/publikacii/satshuk_publ.php.
11. Інформаційна загроза. URL: https://uk.wikipedia.org/wiki/%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B0_%D0%B7%D0%B0%D0%B3%D1%80%D0%BE%D0%B7%D0%B0
12. Інформаційна безпека підприємства та особливості її організації. URL: https://pidruchniki.com/15341220/politologiya/ponyattya_vidi_zagroz_natsionalnim_interesam_ natsionalniy_bezpetsi_informatsiyniy_sferi
13. Горбулін В.П., Качинський А. Засади національної безпеки України. К. : Інтертехнологія, 2009. 272 с.

REFERENCES:

1. Cyvil'nyj Kodeks Ukrai'ny [The Civil Code of Ukraine] (n.d.). zakon.rada.gov.ua. Retrieved from: http://zakon1.rada.gov.ua [in Ukrainian].
2. Zakon Ukrai'ny “Pro zahyst ekonomichnoi' konkurencii”' [Law of Ukraine "On Protection of Economic Competition"] (n.d.). zakon.rada.gov.ua. Retrieved from: https://zakon.rada.gov.ua/laws/show/2210-14 [in Ukrainian].
3. Zakon Ukrai'ny “Pro informaciju” [Law of Ukraine "On Information"]. (n.d.). zakon.rada.gov.ua. Retrieved from: https://zakon.rada.gov.ua/laws/show/2657-12#Text [in Ukrainian].
4. Bol'shoj jenciklopedicheskij slovar' [Big encyclopedic dictionary]. Retrieved from: http://www.vedu.ru/bigencdic/24156/ [in Russian].
5. Shannon C.E. (1948) A Mathematical Theory of Communication. Bell System Technical Journal, Vol. 27, pp. 379–423, 623–656, July, 11 October, 1948
6. Viner, N. (1958) Kibernetika i obshhestvo. Moscow. [in Russian].
7. Konstytucija Ukrai'ny [Constitution of Ukraine] (n.d.). zakon.rada.gov.ua. Retrieved from: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text [in Ukrainian].
8. Il'nyc'ka, U. (2016) Informacijna bezpeka Ukrai'ny: suchasni vyklyky, zagrozy ta mehanizmy protydii' negatyvnym informacijno-psyhologichnym vplyvam [Information security of Ukraine: modern challenges, threats and countermeasures against negative information and psychological influences.]. Humanitarian vision – Humanitarian vision, 2 (1), 27–32.

9. Tolubko, V. (Eds.). (2004) Informacijna bezpeka derzhavy u konteksti protydii' informacijnym vijnam [State information security in the context of combating information wars]. Kyiv : NAOU [in Ukrainian].

10. Sashhuk, G. Informacijna bezpeka v systemi zabezpechennja nacional'noi' bezpeky [Information security in the national security system]. Retrieved from: http:// journ. univ.kiev.ua/trk/publikacii/satshuk_publ.php

11. Informacijna zagroza [Information threat]. Retrieved from: https://uk.wikipedia.org/wiki/%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B0_%D0%B7%D0%B0%D0%B3%D1%80%D0%BE%D 0%B7%D0%B0

12. Informacijna bezpeka pidpryjemstva ta osoblyvosti i'i' organizacii' [Information security of the enterprise and peculiarities of its organization]. Retrieved from: https://pidruchniki.com/15341220/politologiya/ponyattya_vidi_zagroz_natsionalnim_interesam_natsionalniy_bezpetsi_informatsiyniy_sferi

13. Gorbulin, V.P. & Kachyns'kyj, A. (2009) Zasady nacional'noi' bezpeky Ukrai'ny [Principles of national security of Ukraine]. Kyiv: Intertehnologija. 272 s. [in Ukrainian].