УДК 32.019.51
DOI https://doi.org/10.32782/2663-6170/2022.31.21

ІНФОРМАЦІЙНА БЕЗПЕКА ДЕРЖАВИ: ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ТА ОСОБЛИВОСТІ В УМОВАХ ЗБРОЙНОГО КОНФЛІКТУ

INFORMATION SECURITY OF THE STATE: THEORETICAL AND METHODOLOGICAL PRINCIPLES AND FEATURES IN THE CONDITIONS OF ARMED CONFLICT

Ломака І.І.,
кандидат політичних наук,
доцент кафедри політології факультету історії, політології і міжнародних відносин
Прикарпатського національного університету імені Василя Стефаника

Липчук О.І.,
кандидат політичних наук,
доцент кафедри політології факультету історії, політології і міжнародних відносин
Прикарпатського національного університету імені Василя Стефаника

Кобець Ю.В.,
кандидат політичних наук,
доцент кафедри політичних інститутів та процесів
факультету історії, політології і міжнародних відносин
Прикарпатського національного університету імені Василя Стефаника

В статті розглядається питання інформаційної безпеки держави, визначаються вимоги до діяльності держави щодо протидії інформаційним війнам. Державі необхідно бути готовою до запобігання та протидії сучасним способам ведення війни – розробка методів протидії інформаційній зброї, створення суспільства, несприйнятливого до методів інформаційної боротьби, формування концепції протидії інформаційній війні. Крім того, підкреслюється думка, що необхідно виділити проблему інформаційної війни як окрему, вкрай серйозну загрозу інформаційній безпеці та систематизувати поняття, вимоги та методи протидії.

Автором статті зазначено, що сьогодні не рідкістю в інформаційному суспільстві стає демонстрація військової могутності різними державами, яка ініціюється елітами та тиражується засобами масової інформації. Інформація та інформаційна інфраструктура для багатьох розвинених країн вже стали критичними компонентами, вплив на які здатний викликати великомасштабні наслідки, дезорганізувати державне управління, викликати нові конфлікти. Чим вище рівні інтелектуалізації та інформатизації суспільства, тим важливішою стає його інформаційна безпека, оскільки реалізація інтересів, цілей держав і народів дедалі більше здійснюється за допомогою інформаційних, а не матеріально-енергетичних впливів.

Автор поділяє думку багатьох сучасних учених, які вважають, що інформаційне протиборство характеризується, перш за все цілеспрямованим використанням інформації для досягнення політичних, економічних, військових та інших цілей, воно притаманне людському суспільству з моменту його виникнення, а сьогоднішнє підвищення інтересу до цієї проблеми пояснюється різким збільшенням ефективності впливів інформації внаслідок інформатизації та формування глобального інформаційного простору. Саме такі багатозначно-негативні парадокси соціальної реальності, як ніколи раніше, актуалізують використання інформаційних технологій для маніпуляції суспільною свідомістю, що пов'язано з інформаційною безпекою.

Ключові слова: інформація, інформаційна безпека, держава, національна безпека, інформаційний простір, інформаційна політика, інформаційні загрози.

The article examines the issue of information security of the state, defines the requirements for the state's activity in countering information wars. The state needs to be ready to prevent and counter modern ways of waging war – developing methods of countering information weapons, creating a society immune to information warfare methods, forming the concept of countering information warfare. In addition, the opinion is emphasized that it is necessary to single out the problem of information war as a separate, extremely serious threat to information security and to systematize concepts, requirements, and methods of countermeasures.

The author of the article states that today it is not uncommon in the information society to demonstrate military power by various states, which is initiated by the elites and replicated by mass media. Information and information infrastructure have already become critical components for many developed countries, the influence of which can cause large-scale consequences, disorganize public administration, and cause new conflicts. The higher the level of intellectualization and informatization of society, the more important its information security becomes, since the realization of the interests, goals of states and peoples is increasingly carried out with the help of information, rather than material and energy influences.

The author shares the opinion of many modern scientists, who believe that information warfare is characterized, first of all, by purposeful use of information to achieve political, economic, military and other goals, it is inherent in human society

from the moment of its emergence, and today's increase in interest in this problem is explained by a sharp increasing the effectiveness of information effects as a result of informatization and the formation of the global information space. It is such multi-valued and negative paradoxes of social reality that, like never before, actualize the use of information technologies for the manipulation of public consciousness, which is related to information security.

Key words: information, information security, state, national security, information space, information policy, information threats.

Постановка проблеми. Проблематика інформаційної безпеки посідає центральне місце у стратегії державної інформаційної політики сучасної держави. У короткостроковій, середньостроковій та довгостроковій перспективі обґрунтовано очікується подальше наростання у цій сфері загроз та викликів як у всьому світовому співтоваристві. Недостатня захищеність інформаційних ресурсів створює загрози національній та міжнародній безпеці загалом, веде до часткової чи повної втрати державного інформаційного суверенітету. Держава має бути в змозі ефективно протистояти їм керуючись продуманою комплексною стратегією ефективних скоординованих дій за різними напрямами, цілеспрямовано задіяючи весь арсенал сил і засобів, що є в його розпорядженні.

Актуальність теми зумовлена загостренням інформаційного протистояння на міждержавному рівні. Насамперед слід зазначити, що ведення бойових дій у всі часи супроводжувалися спеціальними інформаційними операціями. Але в останні десятиліття спостерігаються дві тенденції, що паралельно розвиваються. Перша полягає у трансформації характеру та оновленні методів ведення інформаційної війни в ході бойових дій. Друга, найбільш актуальна, полягає у перетворенні інформаційної агресії на самостійний вид міждержавного протистояння.

Слід зазначити зростання значимості інформаційних кампаній під час військових операцій. Основна відмінність від подібних операцій минулого полягає в тому, що раніше конфлікт двох країн торкався інтересів лише залучених держав, рідше – їхніх союзників. Сьогодні безпека стає глобальним поняттям, тобто будь-який конфлікт торкається інтересів усієї світової спільноти. Саме тому інформаційний супровід бойових дій сьогодні здійснюється не лише щодо противника, а й у глобальному інформаційному просторі з метою заручитися підтримкою демократичної більшості країн.

Аналіз останніх досліджень і публікацій. Загальні питання теорії забезпечення національної безпеки і дослідження проблематики інформаційної безпеки викладені у працях О. Бакалінської , О. Бакалінського, Ю. Кунєва, Р. Калюжного, М. Вавринчук М.П., А. Нашинець-Наумової, О. Жайворонок, А. Головка, О. Панченка, В. Лопатіна, О. Фролової, А. Войціховського та ін. В напрацюваннях зазначених авторів подано опис цілей, завдань, методів, прийомів, засобів забезпечення системи інформаційної безпеки держави.

Мета статті. Метою статті є дослідження форм та методів деструктивного впливу на інформаційну безпеку, дослідження теоретико-методологічних засад і обґрунтування значущості забезпечення інформаційної безпеки, вдосконалення процесу забезпечення інформаційної безпеки в умовах збройного конфлікту, для формування комплексу адекватних заходів протидії.

Виклад основного матеріалу. Забезпечення військової безпеки сучасної держави залежить як від фактичного в наявності власного, адекватного ймовірному противнику військового потенціалу, а й дедалі більше базується на якісно інших чинниках, які передусім носять економічний, інформаційний, технологічний, політичний і соціальний характер.

З розвитком глобальних інформаційно-комунікаційних технологій наприкінці минулого століття суттєво зросли загрози інформаційній безпеці, і тому виникла об'єктивна необхідність розробки нових міжнародних критеріїв інформаційної безпеки з метою уникнення військових та політичних конфліктів. Виходячи із загальноприйнятого визначення інформаційної безпеки держави як стану захищеності життєво важливих інтересів особистості, суспільства і держави йдеться про можливість запобігти шкоді населенню через: неповноту, несвоєчасність і недостовірність використовуваної та споживаної інформації; негативний інформаційний вплив; негативні наслідки інформаційних технологій; несанкціоноване використання, поширення порушення цілісності, конфіденційності та доступності інформації.

У широкому значенні інформаційна безпека є сукупністю засобів і методів захисту інформації та підтримує її інфраструктури від навмисного або випадкового впливу, в обох випадках власник (держава, бізнес, фізичні особи) даних зазнає тих чи інших збитків. Її ключовими принципами є:

- цілісність інформаційних даних – збереження початкового виду та структури у процесі зберігання та передачі, це означає, що змінювати чи видаляти інформацію може лише її власник чи особи з офіційним доступом;
- конфіденційність даних – інформація доступна лише тим користувачам, які пройшли ідентифікацію та включені до цієї інформаційної системи;
- доступність – інформація, яка знаходиться у вільному доступі, повинна надаватися користувачам, які мають відповідні права, безперешкодно та своєчасно;

• достовірність – інформація належить конкретному власнику, який своєю чергою є її джерелом [8].

Під безпекою інформації розуміється такий її стан, у якому виключена можливість зовнішнього чи внутрішнього впливу цілісність даних, і доступу особам, які мають відповідних прав. Чим більше цифрові технології стають частиною нашого життя, чим складніше їхня система, тим більше вони вразливі. На сьогоднішній день існує безліч видів загроз інформаційній безпеці, які класифікуються за різними ознаками:

• за джерелом загроз (внутрішні та зовнішні);

• характером порушення (конфіденційність даних, збій ІТ-систем, дезінформація);

• за фактором виникнення (природні – стихійні лиха, пожежа, повені; людські мотиви);

• за мотивацією (зловмисні та незловмисні);

• за розмірами збитків (незначні, значні, критичні);

• за ступенем впливу (пасивні – без зміни даних, активні – зі зміною інформації, структури чи системи);

• по об'єкти впливу (орієнтовані всю інформаційну систему чи окремі компоненти) [9].

Процеси цифровізації та глобалізації актуалізують проблеми інформаційної безпеки держави. У світі інтернету, інновацій, єдиного світового інформаційного простору, де обсяги даних збільшуються з неймовірною швидкістю, з кожним роком стає все важче контролювати та керувати їх масивами з метою протидії загрозам, збереження стабільної внутрішньополітичної та соціальної ситуації в країні. У обставинах розробка технологій, які захищають від ворожого проникнення, набуває категоричну значимість [1].

Наукове міжнародне співтовариство досі, незважаючи на багаторічну практику використання терміну «інформаційна безпека держави», не прийшло до єдиного розуміння сутності цього поняття. Визначають два основні підходи: перший – під інформаційною безпекою розуміється інформаційно-технічні та інформаційно-психологічні аспекти, другий – «інформаційна безпека держави – це стан захищеності особистості, суспільства та держави та їх інтересів від загроз, деструктивних та інших негативних впливів на інформаційному просторі» [12; 15].

При цьому в США трактування цього терміну обмежується лише технологічними аспектами і визначається як «захист інформації та інформаційних систем та мереж від несанкціонованого доступу, використання, розкриття, пошкодження, внесення змін або знищення з метою забезпечення цілісності, конфіденційності та доступності» [16; 18].

Інформація для держави – це насамперед стратегічний ресурс, що визначає функціонування різних областей, які за нинішніх умов набули статусу публічності, де будь-які події, з нижчеперелічених сфер, підлягають розголосу:

економічна сфера – сучасна економіка характеризується як рівнем фактичного виробництва, а й престижем країни світової торгової арені, довірою до внутрішніх економічних інститутів, це свого роду маркетинг, де об'єктом виступає державна економіка як бренд ("made in");

сфера міжнародної політики – міжнародні відносини від фізичного протистояння перейшли у інформаційну боротьбу, де першорядну роль грають дипломатія та медіа;

сфера засобів масової інформації – використання ЗМІ для формування вигідної точки зору з того чи іншого питання, або прямого тиску на політичні інститути;

сфера внутрішньої політики – виборність державної влади є територією для інформаційного протистояння, де інформація може як підняти, так і знищити політичну кар'єру, а також загалом змінити траєкторію політичної ситуації в країні;

оборонна сфера – як інноваційна та високотехнологічна галузь, вона безпосередньо залежить від цілісності, обмеженості, конфіденційності та збереження даних, а також контролю над інформаційними потоками [2].

Розвиток технологій та програмного забезпечення, зберігання практично всієї інформації на цифрових носіях, поява безлічі каналів та засобів комунікації, висока швидкість передачі інформації, її нелімітованість, не контрольованість, повсюдність, варіативність інтерпретацій, а також зниження якості та достовірності формує безліч загроз системам та інтересам держави . Суб'єктами деструктивних дій можуть виступати інші держави, спецслужби, бізнес-структури, інсайдери, кримінальні групи, шпигуни, активісти, спамери, хакери і терористи [5; 13].

Загрози інформаційної безпеки пов'язані з протиправними діями, спрямованими на об'єкти інформаційної інфраструктури країни, а саме – на програмно-апаратні, мережеві та інформаційні компоненти, що підтримують функціональність значущих сфер держави: інтернет, інформаційний простір, телекомунікаційні мережі, комп'ютерні системи та програми, процесори та системи управління, внаслідок їх уразливості [11; 17].

Узагальнюючи інформацію з різних джерел [3], виділимо основні загрози інформаційної безпеки держави: інформаційні війни, кібератаки, кібершпигунство, кіберзлочинність, кібертероризм, поширення секретної інформації (дія інсайдерів):

інформаційні війни – дії, метою яких є створення інформаційної переваги, впливу на противника за допомогою втручання в інформаційні процеси, діяльність місцевих ЗМІ, психологічних кампаній у соцмережах, формування вигідної громадської думки, де простежувалися ознаки

інформаційного впливу на маси, у тому числі за допомогою сучасних методи комунікації;

кібератаки – являють собою наступальні спецоперації з метою фізичного впливу (знищення, спотворення, фальсифікація) на інформацію або інформаційно-технологічну інфраструктуру, які можуть змінюватись від відключення мереж та «відмови в доступі», до атак на ключові системи та мережі, виводячи їх з ладу (наприклад, кібератака на британський парламент, метою якої було отримати доступ до електронної пошти парламентаріїв та співробітників);

кібершпигунство – вплив на програми, системи та комп'ютерні мережі з метою отримання доступу до військової, оборонної, дипломатичної чи економічної інформації;

кіберзлочинність – протизаконні дії, пов'язані з використанням комп'ютерних систем, з метою отримання особистої та фінансової вигоди (прибутку), у тому числі крадіжка персональних даних, інтелектуальної власності та шахрайство;

кібертероризм – комп'ютерна атака, націлена на залякування та примус (уряду чи громадян) здійснити ті чи інші політичні дії: заборонені терористичні угруповання активно використовують Інтернет у своїх протиправних діях, у тому числі для атак та пропаганди екстремістських ідей;

поширення секретної інформації – дії інсайдерів, які використовують свій доступ до секретних даних та здійснюють їх передачу державі-противнику, хакерам, терористам або іншим особам, виходячи зі своїх мотивів та переконань.

Таким чином, реалізація деструктивних дій в інформаційному середовищі загрожує національній безпеці, суверенітету та незалежності, підриває стабільність, внутрішній лад, породжує розмиття єдиного інформаційного та правового простору, витісняє ЗМІ та інформагентства з внутрішнього ринку, часто є причиною ксенофобії, просування ідей виняткової нації, нетерпимості та пропаганди екстремістської поведінки.

Потрібно відмітити, що інформаційна безпека передбачає професійну діяльність відповідних державних управлінь та відомств, зокрема, в нашій країні вона здійснюється Радою національної безпеки і оборони України, Службою Безпеки України, Міністерством оборони України, Кіберполіцією України та іншими органами. Крім того, розроблено нормативні документи, які покликані забезпечити національну безпеку країни, серед них:

Закон України «Про інформацію» від 02.10.1992 № 2657-XII;

Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 № 80/94-ВР;

Закон України «Про державну таємницю» від 21.01.1994 № 3855-XII;

Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI;

Постанова Кабінету Міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» від 29.03.2006 № 373;

Постанова Кабінету Міністрів України «Про затвердження Типової інструкції щодо порядку ведення обліку, зберігання, використання та знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію» від 19 жовтня 2016 р. № 736.

Таким чином, інформаційна безпека держави є захистом її інтересів, суверенітету та територіальної цілісності від дестабілізації та загроз інформаційно-технічного та інформаційно-психологічного характеру в інформаційному просторі [11; 14].

Стрімкий розвиток інформаційних технологій та засобів масової комунікації призвів до появи глобальних проблем, пов'язаних із роллю та місцем засобів масової інформації в інформаційній безпеці держави. В умовах сучасної цифровізації, де інформація стала найважливішим ресурсом розвитку, а численні процеси в суспільстві визначаються інформаційним середовищем, підвищується цілеспрямований, неправомірний вплив на неї з боку зовнішніх та внутрішніх джерел, які можуть завдати істотних збитків стабільності та суверенітету.

Глобальне та локальне медіасередовище охоплює соціальні інститути, духовну та матеріальну культуру, суспільну свідомість, все те, що соціалізує та оточує людину щодня. Через посередництво засобів масової комунікації – друк, телебачення, радіо, електронні медіа, соціальні мережі, а також різноманітність інформаційних каналів, журналістів, інсайдерів, неформальних комунікацій, вона пов'язує людей з навколишнім світом, інформує, надає ідеологічне, моральне, естетичне, організаційне вплив на поведінку, думку, судження та оцінки за допомогою інфоприводів, що генеруються [7].

Головним завданням засобів масової інформації у забезпеченні інформаційної безпеки держави є підтримання постійної циркуляції достовірної, неспотвореної інформації, підтримання її якості та дотримання прав та інтересів суб'єктів її здобуття, особливо в умовах збройного конфлікту. Звідси випливає їхня головна мета – інформаційне забезпечення демократії. ЗМІ як інструмент впливу на масову аудиторію повинні ретельно відбирати інформацію, що транслюється по своїх каналах, оскільки неперевірені факти можуть завдати шкоди життєдіяльності держави і суспільства.

У сучасній цифровій епосі влада інформації стає основою для впливу та управління суспільством, а план вплив державного примусу та грошей

виходять на другий план. Це підвищує кількість загроз інформаційній безпеці країни в медіасередовищі, на сьогоднішній день основними з них є:

розширення масштабів використання методів інформаційно-психологічного впливу на медіа спецслужбами окремих держав, метою яких є дестабілізація соціальних та політичних процесів у різних регіонах, при цьому до цієї діяльності активно залучаються етнічні, релігійні та інші громадські організації;

підвищення у російських ЗМІ матеріалів, що містять недостовірну чи упереджену оцінку політики іншої держави, зокрема України, дискримінація національних суспільно-політичних видань та перешкоди для роботи журналістів;

нарощування інформаційно-комунікаційного впливу на населення іншої держави, з метою усунення національних цінностей та орієнтирів;

професійні та непрофесійні інформаційні вкидання з метою формування громадської думки, ескалації ситуації, резонансу чи емоційної реакції;

використання медіасередовища екстремістами та терористичними угрупованнями для впливу на групову та індивідуальну свідомість з метою розпалювання міжнаціональної та релігійної ненависті, просування ідеології, а також вербування та залучення прихильників [4; 10].

Формування глобального інформаційного простору суттєво посилило застосування стратегічними супротивниками протиправних дій у медіасередовищі. Сучасна інформаційна зброя не має територіальних кордонів, інтернет-простір через свою доступність і вразливість дозволяє опонентам наносити «удари» з будь-якого місця в будь-який час, часто переростаючи з разових атак у гібридні війни. В умовах, що склалися, відбувається зростання різних інформаційних кампаній у соціальних мережах, спрямованих на маніпуляцію суспільною думкою з актуальних політичних, соціальних, економічних та інших питань.

Ще одна проблема полягає в тому, що нові численні канали комунікації, обсяги та швидкість поширення контенту призводять до надлишку інформації. У цьому людина поступово починає втрачати здатність аналізувати і критично підходитимемо оцінці контенту, легко довіряючи будь-яким новинам, ідеям і судженням [6]. У цьому такий інструмент інформаційної війни як “fake news” стає найефективнішим методом на противника в інформаційному середовищі, що створює паралельну медіареальність.

Слід зазначити, що у зв’язку зі стрімким технологічним розвитком, розширенням каналів комунікації та диджиталізацією медіасередовища, знижується інформаційна безпека держави, посилюються такі загрози як нарощування інформаційного впливу у ЗМІ на державу-противника; підвищення кількості вкидань та недостовірних матеріалів; дискримінація національних медіа та журналістів; зниження якості контенту; зростання різних маніпуляційних кампаній у соціальних мережах; втрата здатності аудиторії критично оцінювати та аналізувати інформацію.

Висновки. У сучасному інформаційному суспільстві відбуваються процеси, які актуалізують питання забезпечення інформаційної безпеки країни. Саме тому для більш ефективного протистояння цим загрозам та забезпеченню достатньо високого рівня безпеки сучасного суспільства необхідно перейти до забезпечення комплексної безпеки:

– розвиток інформаційної інфраструктури, індустрії обробки інформації, дотримання прав та свобод громадян в інформаційному просторі, що гарантують безпеку та конфіденційність інформації;

– пріоритетність у забезпеченні інформатизації соціальної сфери, матеріального виробництва, ресурсів, більш професійного регіонального управління для реалізації ефективної інформаційної державної політики, а також високопрофесійна підготовка спеціалістів у галузі інформаційних технологій для більш ефективного захисту телекомунікаційних систем, інформаційних ресурсів;

– нагромадження та збереження інформаційних ресурсів для використання в системі безпеки з урахуванням динамічного руху, ініціювання інформаційної індустрії з метою виходу на міжнародні ринки.

В умовах інформаційної війни об’єктами руйнування стають ціннісні орієнтири суспільства, національний менталітет, суспільний ідеал, а одним із основних інструментів деструктивного інформаційного впливу стають засоби масової інформації. Таким чином, проблема державного забезпечення інформаційної безпеки країни має комплексний характер і для її вирішення потрібне системне дослідження та планування.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Бакалінська О., Бакалінський О. Правове забезпечення кібербезпеки в Україні. *Підприємництво, господарство і право.* 2019. № 9. С. 100–108.

2. Вавринчук М.П., Когут О.В. Інформаційна безпека держави. *Правові засади організації та здійснення публічної влади* : зб. тез II Всеукр. наук.-практ. інтернет-конф. (м. Хмельницький, 2–8 трав. 2019 р.). Хмельницький : ХУУП, 2019. С. 37–40.

3. Войціховський А.В. Інформаційна безпека як складова системи національної безпеки (Міжнародний і зарубіжний досвід). *Вісник Харківського національного університету імені В. Н. Каразіна. Серія «Право»*. 2020. № 29. С. 281–288. doi: 10.26565/2075-1834-2020-29-38

4. Головка А.А. Діяльність сучасних ЗМІ в контексті інформаційної безпеки України. *Актуальні проблеми гуманітарних та природничих наук* (м. Ужгород, 08–09 квітня 2016 р.). Херсон : Видавничий дім «Гельветика», 2016. С. 85–87.

5. Грубінко А. Інформаційна безпека України: правове гарантування та реалії забезпечення. *Актуальні проблеми правознавства*. 2019. Вип. 1 (17). С. 5–10.

6. Жайворонок О.І. Сучасні загрози інформаційного тероризму в умовах гібридної війни Росії проти України. *Державне управління: удосконалення та розвиток*. 2018. № 4. С. 1–5.

7. Кунєв Ю.Д. Правове забезпечення інформаційної безпеки як предмет правового дослідження. *Юридичний вісник «Повітряне і космічне право»*. 2021. № 1(58). С. 95–102. DOI: 10.18372/2307-9061.58.15314

8. Нашинець-Наумова А.Ю. Інформаційна безпека: питання правового регулювання. Київ : «Гельветика», 2017. 168 с.

9. Ніщименко О.А. Інформаційна безпека України на сучасному етапі розвитку держави і суспільства. *Наше право*. 2016. № 1. С. 17–23.

10. Панченко О.А. Роль засобів масової інформації в системі державного управління інформаційною безпекою. *Публічне управління та митне адміністрування*. 2020. № 1 (24). С. 97–102. doi: 10.32836/2310-9653-2020-1.19

11. Про національну безпеку України : Закон України № 2469-VIII від 21.06.2018. *Відомості Верховної Ради (ВВР).* 2018. № 31. С. 241.

12. Про інформацію : Закон України № 2657-XII від 02.10.1993. *Відомості Верховної Ради України (ВВР*).1992. № 48. С. 650.

13. Про Службу Безпеки України : Закон України № 2229-XII від 25.03.1992. *Відомості Верховної Ради України (ВВР).* 1992. № 27. С. 382.

14. Указ Президента України від 26 травня 2015 року № 287/2015 про введення в дію рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України». URL: http://zakon3.rada.gov.ua/laws/show/287/2015 (дата звернення: 17.11.2022).

15. Указ Президента України від 25 лютого 2017 року № 47/2017 про введення в дію рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» URL: http://www.president.gov.ua/documents/472017-21374 (дата звернення: 17.11.2022).

16. Nieles M., Dempsey K., Pillitteri V. Y. An introduction to information security. Gaithersburg, MD : National Institute of Standards and Technology, 2017. URL: https://doi.org/10.6028/nist.sp.800-12r1 (date of access: 17.11.2022).

17. Kuniev Y., Sopilko I., Kolpakov V. Object and subject of information law. *Journal of law and political sciences scientific and academy journal*. 2020. Vol. 23. Issue 2. P. 9–41.

18. Federal Information Security Modernization Act, December 18, 2014. Subchapter III – Informational Security. § 3542. Definitions. URL: https://csrc.nist.gov/topics/laws-and-regulations/laws/fisma. (date of access: 17.11.2022).