

Адміністративне право і процес; фінансове право; інформаційне право
УДК 351.746.1:159.964

Ковалів Мирослав Володимирович

кандидат юридичних наук, професор

Львівський державний університет внутрішніх справ

Kovaliv Myroslav

PhD in Law, Professor

Lviv State University of Internal Affairs

ORCID: 0000-0002-9730-8401

Петков Сергій Валерійович

доктор юридичних наук, професор

Військовий інститут

Київського національного університету імені Тараса Шевченка

Petkov Sergey

D. Sc. (Law), Professor

Military Institute of

Taras Shevchenko National University of Kyiv

ORCID: 0000-0003-4160-767X

Скриньковський Руслан Миколайович

кандидат економічних наук, професор

Львівський університет бізнесу та права

Skrynkovskyu Ruslan

PhD in Economics, Professor

Lviv University of Business and Law

ORCID: 0000-0002-2180-8055

Хмиз Мар’яна Василівна

доктор філософії в галузі права, доцент

Львівський університет бізнесу та права

Khmyz Mariana

PhD in Law, Associate Professor

Lviv University of Business and Law

ORCID: 0000-0003-3553-8022

Кокотайло Роман Олегович

аспірант

Львівського університету бізнесу та права

Kokotailo Roman

Postgraduate Student of the

Lviv University of Business and Law

ORCID: 0009-0001-5453-0272

Лозинський Юрій Романович

кандидат юридичних наук

Львівський державний університет внутрішніх справ

Lozynskyyi Yurii

PhD in Law

Lviv State University of Internal Affairs

ORCID: 0000-0003-2908-7747

Сидор Маркіян Ярославович

кандидат юридичних наук

Львівський державний університет внутрішніх справ

Sydor Markiian

PhD in Law

Lviv State University of Internal Affairs

ORCID: 0000-0002-0605-5366

**ПРИНЦИПИ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ
БЕЗПЕКИ
PRINCIPLES OF LEGAL ENSURING FOR INFORMATION
SECURITY**

Анотація. У статті на основі комплексного та системного аналізу чинного законодавства України, нормативно-правових актів Європейського Союзу та Організації Північноатлантичного договору (НАТО) розглянуто принципи правового забезпечення інформаційної безпеки. Об'єктом дослідження є суспільні відносини, пов'язані з правовим забезпеченням інформаційної безпеки України в умовах нових викликів та загроз, а також цифрової трансформації та геополітичних змін. Предмет дослідження утворює сукупність правових норм нормативно-правових актів, міжнародних договорів, що регулюють суспільні відносини у сфері забезпечення інформаційної безпеки, правозастосовну практику, закордонний досвід правового регулювання, положення теоретичних міждисциплінарних досліджень у зазначеній сфері. У статті використовувалися спеціальні приватно-правові методи пізнання, такі як історико-правовий, порівняльно-правовий, формально-юридичний та інші. Вказано на системоутворюючу роль принципів правового забезпечення інформаційної безпеки, детерміновану зростанням ризиків та загроз в інформаційному просторі, в умовах цифровізації, геополітичних змін та необхідності захисту інформаційних ресурсів. Зазначено, що у системі правового забезпечення інформаційної безпеки застосовується сукупність правових засобів, що реалізується на основі поєднання загальних, спеціальних та особливих правових режимів об'єктів інформаційного простору, розвиток яких визначається принципами та напрямками державної політики в інформаційній сфері. За результатами дослідження обґрунтовано необхідність розвитку та законодавчого закріплення системи спеціальних принципів права за допомогою

доповнення принципами: універсальності інформаційної безпеки; обов'язковість забезпечення інформаційної безпеки; забезпечення технічної взаємодії України та країн НАТО щодо інформаційної безпеки. Правове забезпечення процесів стандартизації в інформаційній безпеці є комплексом організаційно-правових засобів, що створюють пріоритетні умови для українського розробника та виробника цифрових технологій на підставі стандартів НАТО та Європейського Союзу, атестацію об'єктів інформатизації, сертифікацію засобів захисту інформації, технічне регулювання об'єктів і процесів інформаційного середовища.

Ключові слова: інформація, інформаційна безпека, інформаційні загрози, інформаційний простір, технічні засоби, НАТО, норми права, державна політика, національна безпека, Україна.

Summary. The article, based on a comprehensive and systematic analysis of the current legislation of Ukraine, legal acts of the European Union and the North Atlantic Treaty Organization (NATO), examines the principles of legal provision/ensuring for information security. The object of the study is public relations related to the legal provision of information security in Ukraine in the context of new challenges and threats, as well as digital transformation and geopolitical changes. The subject of research forms a set of legal norms, regulatory legal acts, international treaties regulating public relations in the field of information security, law enforcement practice, foreign experience of legal regulation, provisions of theoretical interdisciplinary research in this area. The article used special private law methods of cognition, such as historical-legal, comparative-legal, formal-legal and others. The system-forming role of the principles of legal support for information security, determined by the growth of risks and threats in the information space, in the conditions of digitalization, geopolitical changes and the need to protect information resources, is indicated. It is noted that in the system of legal support of information security, a set of legal means is used, which is implemented on

the basis of a combination of general, special and special legal regimes of objects of the information space, the development of which is determined by the principles and directions of state policy in the information sphere. According to the results of the study, the need for the development and legislative consolidation of the system of special principles of law with the help of supplementing with principles is substantiated: the universality of information security; obligation to ensure information security; ensuring technical cooperation between Ukraine and NATO countries on information security. Legal support for standardization processes in information security is a set of organizational and legal means that create priority conditions for the Ukrainian developer and manufacturer of digital technologies based on NATO and European Union standards, attestation of informatization objects, certification of information security means, technical regulation of objects and processes of the information environment.

Key words: *information, information security, information threats, information space, technical means, NATO, legal norms, state policy, national security, Ukraine.*

Постановка проблеми. Характерною особливістю сучасних суспільних відносин є стрімкий розвиток інформаційних систем та технологій, що відкрили можливості для масштабного «цифрування» документів, створення різних видів інформації, ефективного зберігання, опрацювання, використання та обміну інформацією (відомостями та/або даними [1]), вираженою в цифровій (електронній) формі. У період впровадження цифрових технологій, загальної цифровізації та подальшого розвитку інформаційних систем і процесів, питання визначення принципів забезпечення інформаційної безпеки мають ключове значення для вдосконалення системи правових засобів, які використовуються у цій галузі [2–4]. Актуальним і водночас важливим є питання про наукове осмислення системи принципів, особливостей становлення та розвитку,

впливу на правовідносини, що виникають у процесі забезпечення інформаційної безпеки.

Аналіз останніх досліджень і публікацій. Цьому питанню приділено досить багато уваги як у наукових працях вчених-юристів [2–4], так і законодавцями, серед практикуючих юристів, військових. За значний вклад у теоретичні розробки принципів правового регулювання інформаційної безпеки доцільно відмітити роботи: І. Арістової, О. Баранова, В. Дубаса, А. Берлача, Н. Бортник, П. Діхтієвського, І. Гриценка, О. Карасса, Л. Кисіль, В. Курила, Є. Курінного, Р. Калюжного, Н. Лесько, Р. Мельника, В. Настюка, О. Остапенка, А. Селіванова, О. Харитонової, В. Цимбалюка, В. Шамрая, Я. Шевченко, Ю. Шемчушенка та інших вчених. В умовах воєнного стану і враховуючи його особливості в Україні, дослідження принципів інформаційної безпеки зумовлено практичними цілями вдосконалення правового регулювання та правозастосовної практики.

Мета статті. Метою статті є дослідження принципів правового забезпечення інформаційної безпеки.

Виклад основного матеріалу дослідження. Зростаюча роль інформаційної сфери, яка є системоутворюючим чинником життя суспільства, активно впливає на стан політичної, економічної, військової та інших складових національної безпеки України [5]. У зв'язку з цим інформаційна безпека набуває значущості в загальній системі забезпечення національної безпеки. Роль правових принципів при забезпеченні інформаційної безпеки, особливо у зв'язку з реалізацією завдань, пов'язаних із забезпеченням територіальної цілісності, суверенітету та інших національних інтересів України [5; 6], зростає.

Правові принципи є основними засадами та орієнтиром для законодавця, оскільки правові норми, що формулюються законодавцем, не повинні суперечити принципам права. Принципи права мають фундаментальне значення для регулювання суспільних відносин у галузі

забезпечення інформаційної безпеки та знаходять нормативно-правове закріплення на державному та міжнародному рівнях. Стосовно права у сфері забезпечення інформаційної безпеки, правові принципи можна позначити як нормативно встановлені основні ідеї, засади, вихідні положення, визначальний зміст і закономірності правового регулювання суспільних відносин у сфері інформаційної безпеки.

Проблеми безпеки в інформаційному просторі, цифрова трансформація як ефект розвитку цифрових технологій, транскордонність інформаційних відносин дозволяють відзначити важливість принципів національного та міжнародного права.

Одним із принципів, закріплених у Статуті Організації Об'єднаних Націй (далі – ООН) [7], Декларації про принципи міжнародного права, що стосуються відносин і співробітництва між державами (відповідно до Статуту ООН) [8] є принцип вирішення спорів міжнародно-правового характеру мирним способом, недопущення виникнення загроз миру та безпеці, відповідно до принципів справедливості та міжнародного права тощо [7; 8].

Геополітичні аспекти на тлі широкомасштабної збройної агресії (війни) російської федерації проти України [9], враховуючи воєнно-політичну, воєнно-економічну, воєнно-стратегічну обстановку, вимагають особливої уваги до питань, що належать до сфери міжнародної та національної інформаційної безпеки.

У сфері міжнародної інформаційної безпеки, враховуючи принципи ООН, зокрема – принцип незастосування сили і утримання від погрози силою проти територіальної цілісності чи політичної незалежності будь-якої держави або будь-яким іншим способом (пункт 4 ст. 2 Статуту ООН [7]), актуальними є питання про інформаційні загрози, компоненти гібридної війни, методи і особливості використання сучасної інформаційної зброї залежно від об'єкту впливу (інформаційно-технічної, інформаційно-психологічної зброї [10]), виходячи із результатів

дослідження російсько-української інформаційної війни, яку розпочала росія ще задовго до початку злочинного прямого повномасштабного вторгнення в Україну. Збройна агресія російської федерації проти України і Українського народу є тяжким міжнародним злочином, відповідно до норм міжнародного права. Типовими компонентами злочинної гібридної російсько-української війни, під час збройної агресії російської федерації проти України є пропаганда війни та інші прояви інформаційної агресії (війни) з боку росії. Нагадаємо, що «будь-яка пропаганда війни заборонена законом» (ст. 20 Міжнародного пакту про громадянські та політичні права, який прийнято 16 грудня 1966 року Генеральною Асамблеєю ООН) [11].

Акти російської інформаційної агресії, що містять підбурювання до насильницького повалення та захоплення державної влади України, включаючи зміни статусу української мови як єдиної державної мови, шляхом використання традиційних ЗМІ, медіа та інтернет-ресурсів, порушують інший основний принцип ООН (пункт 7 ст. 2 Статуту ООН [7]) – невтручання у справи, що входять до внутрішньої компетенції України.

Співробітництво держав при реалізації завдань забезпечення безпеки в інформаційній сфері вимагає формування та вжиття організаційно-правових заходів, спрямованих на протидію інформаційним загрозам, що посягають на безпеку інформаційного простору та на національні інтереси держав. Зазначений принцип є актуальним через підвищення рівня інтеграційної взаємодії у регіональних міждержавних союзах та взаємодії між державами, зумовлену транскордонним характером інформаційного простору.

Враховуючи існуючі проблеми міждержавної взаємодії в умовах геополітичних ризиків та невизначеності, при формуванні державної політики України у сфері національної безпеки і оборони зростає значення міждержавної взаємодії між Україною з Європейським Союзом (далі – ЄС) та НАТО (Організацією Північноатлантичного договору; англ. NATO – North Atlantic Treaty Organisation).

Принцип суверенної рівності держав (пункт 1 ст. 2 Статуту ООН [7]) визначає можливість України брати участь у вирішенні проблем міжнародної інформаційної безпеки, бути активним членом на всіх рівнях і етапах розвитку глобального інформаційного простору тощо. Зазначений принцип відіграє ключову роль у частині контролю національного інформаційного простору та розвитку суверенного сегменту Інтернету, що дозволяє враховувати рішення у сфері забезпечення безпеки і оборони, на підставі національного законодавства у контексті Директиви Європейського Парламенту і Ради (ЄС) 2022/2555 від 14 грудня 2022 року про заходи щодо забезпечення високого загального рівня кібербезпеки в усьому Союзі, яка вносить зміни до Регламенту (ЄС) № 910/2014 та Директиви (ЄС) 2018/1972, та скасування Директиви (ЄС) 2016/1148 [12].

Вищезгаданий принцип дозволяє надавати публічно-правові послуги в електронній формі, забезпечувати взаємодію у фінансово-кредитній сфері, розвивати електронну комерцію, інтернет-технології у військових структурах, у сфері безпеки на транспорті та інші види діяльності як у мирний час, так і у період дії правовою режиму воєнного стану, з певними особливостями.

Поряд з використанням глобальної мережі Інтернет, в умовах кібервійни важливе значення мають відповіді на питання щодо доступу, контролю або встановлення обмежень до мережі Інтернет з боку держави на власній території, а також щодо аспектів на предмет становлення і розвитку суверенного сегменту Інтернету для забезпечення національної безпеки і оборони, який може працювати в ізольованому режимі (за потреби) у певний період часу, на різних рівнях або в конкретних сферах. Наприклад, це може бути локальна та/або автономна інтернет-мережа у сфері безпеки і оборони України в умовах воєнного часу при застосуванні сил безпеки і сил оборони для виконання завдань з оборони України, захисту її суверенітету, територіальної цілісності і недоторканності тощо. Сутність, мета створення, інструментарій та особливості використання

суверенного Інтернету в умовах воєнного часу потребують додаткового спеціального дослідження з належною аргументацією. В контексті цього, тут слід також врахувати і те, що російська федерація є державою-агресором, державою-терористом і державою-спонсором тероризму [13], тому в путінській росії розробка і використання російського суверенного Інтернету в умовах ізоляції, враховуючи особливості злочинної війни росії проти України, на думку експертів – це можливість для злочинного вищого політичного та військового керівництва росії, російської православної церкви здійснювати маніпуляції громадською думкою серед росіян, яке і так є абсолютно аморальним суспільством, це пропаганда війни, тероризм, підбурювання до дискримінації, ворожнечі чи насильства, технологія провокацій, залякування та дезінформації, психологічні впливи та інші аспекти.

Міжнародний принцип сумлінного виконання зобов'язань і узгодження дій реалізується через належне виконання державами обов'язків, що випливають із міжнародних договорів у різних сферах, включаючи сферу захисту інформації. Звідси очевидно, що порушення цього принципу спричиняє деструктивний вплив на довіру між державами, викликаючи конфронтацію, певне інформаційне протистояння чи протиборство між державами, неурядовими, економічними або іншими структурами. Особливого значення набуває принцип достовірності інформації як основа довіри.

Джерела міжнародного інформаційного права включають принцип поваги до прав людини та основних свобод, який стосовно сфери забезпечення інформаційної безпеки конкретизується у Міжнародному пакті про громадянські та політичні права [11], Міжнародному пакті про економічні, соціальні та культурні права [14] та в Загальній декларації прав людини [15]. Зазначені акти закріплюють норми про таємницю кореспонденції та заборону незаконного посягання на честь та репутацію особи.

Загальноновизнані принципи міжнародного права у досліджуваній сфері зазначені у резолюціях ООН, присвячених проблемам кібербезпеки та розвитку науково-технічного прогресу. Зазначені принципи узгоджуються з документами стратегічного планування України, ЄС і НАТО та наголошують на важливості відкритості та прозорості діяльності держави в інформаційному просторі, необхідності формування глобальної культури інформаційної безпеки.

Розглядаючи міжнародно-правові засади, важливо звернути увагу на принципи, закріплені в Окінавській хартії глобального інформаційного суспільства, де підкреслюється роль та значення функціонування електронної ідентифікації, електронного підпису, криптографії та інших засобів забезпечення безпеки та достовірності операцій; розвиток ефективного механізму захисту приватного життя споживача, розвиток технічних засобів забезпечення безпеки [16].

Принципи інформаційної безпеки отримали відображення в Женевській декларації принципів «Побудови інформаційного суспільства: глобальна задача в новому тисячолітті» (2003 р.), включаючи принцип зміцнення довіри та безпеки при використанні цифрових технологій, що детермінує розвиток правових основ для цифрового довірчого середовища, включаючи захист інформаційно-комунікаційних мереж, ідентифікацію, безпеку відомостей обмеженого доступу, захист недоторканності приватного життя та прав користувачів, протидію кіберзлочинності [17]. Аналогічні позиції закріплені у Туніській програмі для інформаційного суспільства, ухваленої у 2005 році.

Важливе значення для інформаційного права мають принципи права інтеграційної взаємодії. Можемо констатувати особливе значення інтеграційного міждержавного співробітництва у сфері інформаційної безпеки внаслідок геополітичних і соціально-економічних змін [18; 19]. Актуальні головні виклики та загрози національній безпеці України в інформаційній сфері в умовах сучасного міжнародного безпекового

середовища, а також стратегічні цілі та завдання, які спрямовані на протидію таким загрозам, включаючи захист прав осіб на інформацію та захист персональних даних, визначає Стратегія інформаційної безпеки України [19].

У Північноатлантичному альянсі (НАТО) держави-учасниці керуються принципами рівних прав щодо захисту критично важливих інформаційних об’єктів, сприяння отриманню та розповсюдженню інформації з урахуванням захисту інтересів національної та суспільно значимої інформації.

У роботі Європейського Союзу основним напрямом щодо забезпечення інформаційної безпеки є спільна розробка та затвердження організаційних і технічних вимог для національного сегменту інтегрованої системи та комплексний захист інформації від зовнішніх загроз.

Закладені принципи інформаційної безпеки у роботі міждержавних організацій є механізмом захисту інформаційних технологій та запобігання кіберзагрозам в міжнародному просторі.

Гармонізація законодавства країн-членів НАТО та Європейського Союзу сприяє зміцненню партнерських відносин у сфері побудови безпечного інформаційного середовища, дозволяє виробити принципи правового забезпечення інформаційної безпеки, дотримання яких є обов’язковим для всіх членів інтеграційного об’єднання.

В умовах, коли інформаційний простір фактично розмиває кордони між державами, не обмежуючись територією однієї держави, регіону чи континенту, питання міжнародної інформаційної безпеки, враховуючи базові засади її забезпечення, повинні включати аспекти протидії розповсюдженню недостовірної інформації про сили безпеки і сили оборони держав, зокрема – про Збройні Сили України та їх дії в умовах злочинної війни росії проти України, про інші сили безпеки і сили оборони України, які протистоять міжнародному тероризму, що вчиняє російська федерація. Нагадаємо [9; 13; 20–29], що «російсько-українська війна – це

не лише війна за незалежність України, а й війна України за цінності: життя, демократію та свободу в усьому світі. ... Дії вищого керівництва РФ і російської православної церкви – це продумана, послідовна і заздалегідь чітко спланована російська політика геноциду Українського народу. Президент РФ В. Путін, вище політичне і військове керівництво Росії – це воєнні злочинці і терористи, а армія РФ – це виключно російський механізм вбивства, катування, гвалтування, зокрема й неповнолітніх дівчат і навіть немовлят, глумління над тілами вбитих і замучених, мародерства в Україні тощо» [20, с. 147]; декларованою метою діяльності ООН є підтримання та зміцнення міжнародного миру й безпеки, а також розвиток співробітництва між державами світу, та розвиток поваги до прав людини й основних свобод для всіх, без розрізнення раси, статі, мови та релігії [7]. Міністерство закордонних справ України вказує на нелегітимність перебування російської федерації в Раді Безпеки ООН та загалом в ООН [30], погоджуємося з цією позицією.

Транскордонний характер інформаційного простору обумовлює потребу у застосуванні колективних міждержавних заходів щодо забезпечення безпечного обміну інформацією. Принцип неподільності безпеки реалізується через сприйняття інформаційного простору всіх держав як єдиного цілого, що вимагає неухильного підтримання та зміцнення інформаційного суверенітету кожною державою у межах визначених нормативними документами НАТО і Європейського Союзу. У зв'язку з цим інформаційні загрози, які посягають на національні інтереси, безпеку однієї з держав-членів НАТО, повинні кваліфікуватися як агресивні дії щодо інших держав.

Юридична спільнота повинна розробити підходи до формування єдиної системи стандартів та вимог щодо безпеки в інформаційному середовищі, які будуть визначати ступінь захищеності інформаційної інфраструктури та протидію поширенню недостовірної інформації. Сьогодні актуальність принципу неподільної безпеки виходить на новий

рівень з огляду на посилення напруженості між росією у зв'язку з агресією проти України та країнами НАТО з питань гарантій безпеки.

Досліджувані правові засади знайшли закріплення на національному рівні. Принципи загально-правового характеру мають стратегічне значення для системи права та поширюють свою дію на всі галузі права, знаходячи правове закріплення у нормах Конституції України [31]. Законність, недоторканність і захист приватного життя, а також свобода інформації є прикладами загально-правових засад, які діють щодо правового забезпечення інформаційної безпеки.

Забезпечення інформаційної безпеки на належному рівні передбачає розвиток конституційно-правових засад, які визначають сферу оборони та безпеки, обіг цифрових даних стратегічною значимістю, а також вдосконалення національного законодавства у цій сфері.

Принципи забезпечення доступу до інформації діють у різних галузях права, отже відносяться до міжгалузевих принципів.

У цивільному процесуальному праві діє принцип гласності, наприклад, одним із аспектів якого є доступ до інформації про діяльність судів. До міжгалузевих принципів слід віднести принцип достовірності та повноти інформації.

Галузеві принципи у сфері інформаційної безпеки включають принципи, які діють виключно у галузі інформаційного права, відображають специфіку підгалузі та окремих інститутів інформаційного права. Враховуючи це, тут слід відмітити принципи розвитку законодавства у сфері засобів забезпечення конфіденційності інформації, ідентифікації в цифровому середовищі та інші принципи правових інститутів.

Спеціальні принципи у сфері забезпечення інформаційної безпеки включають принципи: законності, збалансованості, реальності завдань, поєднання централізованого управління з передачею повноважень органам місцевої влади та місцевого самоврядування, інтеграції в ЄС та НАТО.

Інтеграція України в ЄС та НАТО є досить важливим аспектом, оскільки вона сприяє стандартизації та взаємодії на міжнародному рівні, що є важливим для впровадження ефективних систем і технологій та реалізації стратегій інформаційної безпеки.

Відповідно до Стратегії національної безпеки України, затвердженої Указом Президента України від 14 вересня 2020 року № 392/2020, складовою національної безпеки держави є інформаційна безпека; водночас, серед принципів, які слід зарахувати у зазначеній сфері, є принципи, закріплені у чинному Законі України «Про національну безпеку України» [5]. Діяльність державних органів, які забезпечують інформаційну безпеку, підпорядковується принципам правового забезпечення, вказаним у цьому Законі. До таких принципів можна віднести засади, закріплені у Доктрині інформаційної безпеки України [32]. Доктрина інформаційної безпеки України визначає організаційну основу системи забезпечення інформаційної безпеки, що складається з органів управління та забезпечення інформаційної безпеки [32; 33].

Принципи правового регулювання відносин, що виникають в інформаційній сфері, мають для забезпечення інформаційної безпеки основний характер та регламентовані у Законі України «Про захист інформації в інформаційно-комунікаційних системах» від 05.07.1994 р. № 80/94-ВР (із змінами) [34].

У цьому Законі [34] визначено цілі, що досягаються за допомогою різних способів для захисту інформації, які можна розглядати як принципи, оскільки фактично вони є базовими правовими засадами, на основі яких здійснюється захист інформації: цілісність, конфіденційність та доступність, відповідно до міжнародних стандартів і стандартів ЄС.

Актуальною та важливою сферою інформаційної безпеки є інститут персональних даних, норми якого ґрунтуються на правових засадах, закріплених у Законі України «Про захист персональних даних» від 01.06.2010 р. № 2297-VI (із змінами) [35]. Цей Закон [35] встановлює

принцип розумної достатності при обробці даних, що передбачає відсутність надмірності змісту та обсягу оброблюваних персональних даних і відповідність заздалегідь визначеним цілям такої обробки. Обробка персональних даних вимагає дотримання балансу між надмірністю та достатністю інформації.

Інформаційна безпека включає захист інформації та об'єктів, що пов'язані з нею. Одним із таких об'єктів є критична інформаційна інфраструктура. Її безпека та захист, відповідно до Закону України «Про критичну інфраструктуру» від 16.11.2021 р. № 1882-IX (із змінами) [36], здійснюється за допомогою реалізації певних принципів. Це визначає обов'язковість застосування організаційно-правових заходів щодо забезпечення національної інформаційної безпеки в Україні.

Розвиток політики побудови цифрової економіки в Україні вплинув на формулювання принципів забезпечення інформаційної безпеки. У Національній економічній стратегії на період до 2030 року міститься комплекс заходів, реалізація яких базується на засадах забезпечення інформаційної безпеки [37]. «Першочерговим етапом є формування конкурентоспроможних умов для бізнесу та інвестицій, а також відновлення довіри до державних інститутів. ... Україна – найпривабливіша країна економічних можливостей для інвестицій, інновацій, ведення бізнесу; найкраще місце для реалізації творчого потенціалу, втілення ідей і власного розвитку» [37].

Система принципів вимагає вдосконалення з погляду законодавчих змін, а також теоретичного осмислення. Особливо важливим є принцип реалізації політики технічної взаємодії та стандартизації у сфері інформаційно-комунікаційних технологій з НАТО і ЄС з метою забезпечення інформаційної безпеки. Реалізація цього принципу дозволить зменшити фінансові витрати на розробку систем та технологій захисту інформації, а також підвищить ефективність системи забезпечення інформаційної безпеки, що позитивно вплине на розвиток інформаційної

інфраструктури та сприятиме виведенню інформаційних технологій на новий рівень, враховуючи стандарти та технології НАТО і ЄС. Вплив зазначеного на забезпечення інформаційної безпеки та захисту інформації і персональних даних підкреслено в національних актах стратегічного планування.

Зазначений вище принцип визначає вектор розвитку державної інформаційно-правової політики України з урахуванням напруженості в міжнародних відносинах та воєнної агресії росії проти України у всіх сферах протистояння. Практична реалізація цього принципу дозволить зміцнити технічний та технологічний суверенітет України, що вплине на зміцнення стану інформаційної захищеності.

На розвиток системи правових принципів забезпечення інформаційної безпеки мають вплив організаційні принципи, включаючи принцип реальності завдань, керованості, комплексності, безперервності процесів реалізації та контролю, реагування на загрози, пріоритету превентивних заходів.

Висновки. Дослідження принципів інформаційної безпеки вказує на необхідність формування системи базових принципів на основі критеріїв класифікації доктринального характеру, що впливають зі стратегічних завдань у сфері забезпечення національної інформаційної безпеки НАТО і ЄС, у співвідношенні з принципами міжнародного права у сфері інформаційної безпеки; закріплення у законодавстві України про інформаційну безпеку.

У результаті дослідження обґрунтовано необхідність розвитку та законодавчого закріплення системи спеціальних принципів права за допомогою доповнення принципами: універсальності інформаційної безпеки; обов'язковості забезпечення інформаційної безпеки; забезпечення технічної взаємодії України та країн НАТО щодо інформаційної безпеки.

Література

1. Про інформацію: Закон України від 02.10.1992 р. № 2657-XII (із змінами). URL: <https://zakon.rada.gov.ua/laws/show/2657-12#Text> (дата звернення: 02.01.2024).
2. Нашинець-Наумова А. Ю. Інформаційна безпека: питання правового регулювання: монографія. Київ: Видавничий дім «Гельветика», 2017. 168 с.
3. Біленчук П. Д., Борисова Л. В., Неклонський І. М., Собина В. О. Правові засади інформаційної безпеки України: монографія / За ред. П.Д. Біленчука. Харків: 2018. 289 с.
4. Левченко О. В. Система забезпечення інформаційної безпеки держави у воєнній сфері: основи побудови та функціонування: монографія. Житомир: Видавець ПП «Євро-Волинь», 2021. 172 с.
5. Про національну безпеку України: Закон України від 21.06.2018 р. № 2469-VIII (із змінами). URL: <https://zakon.rada.gov.ua/laws/show/2469-19#Text> (дата звернення: 02.01.2024).
6. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки»: Указ Президента України від 28.12.2021 р. № 685/2021. URL: <https://zakon.rada.gov.ua/laws/show/685/2021#Text> (дата звернення: 02.01.2024).
7. United Nations Charter (full text) // *United Nations websites*. URL: <https://www.un.org/en/about-us/un-charter/full-text> (дата звернення: 02.01.2024).
8. Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations: UN. General Assembly (25th sess.: 1970) // *UN Digital Library*. URL: <https://digitallibrary.un.org/record/202170> (дата звернення: 02.01.2024).
9. Україна під час російсько-української війни 2014–2023 рр.: генеза національної стійкості крізь призму наукових досліджень: монографія

- / Вановська І. М., Джус О. А., Ляшко О. О., Копотун І. М., Коропатнік І. М., Первак І. О., Петков С. В., Попков Б. О., Скрябін О. Л., Стецюк С. П., Скриньковський Р. М., Сопільник Л. І., Трубчанінов М. А., Хан Є. В., Шемчук В. В.; за заг. ред. Б. Попкова, С. Петкова. Київ: Видавництво Ліра-К. 2023. 272 с.
10. Хорошко В., Козел Т., Ярошенко О. Особливості застосування сучасної інформаційної зброї // *Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні*. 2015. Вип 1(29). С. 9– 14. URL: http://old.pnzzi.kpi.ua/29/29_p9.pdf (дата звернення: 02.01.2024).
11. International Covenant on Civil and Political Rights: Adopted and opened for signature, ratification and accession by General Assembly resolution 2200A (XXI) of 16 December 1966, entry into force 23 March 1976, in accordance with Article 49 // *United Nations websites*. URL: <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights> (дата звернення: 02.01.2024).
12. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) // *Official Journal of the European Union*. L 333. Vol. 65. 27.12.2022 (ISSN 1977-0677). URL: <http://data.europa.eu/eli/dir/2022/2555/oj> (дата звернення: 02.01.2024).
13. Скриньковський Р. М., Козяр Р. Я., Петков С. В., Хмиз М. В., Чистоклетов Л. Г. Державна охорона в Україні щодо глав іноземних держав та посадових осіб міжнародних організацій в умовах воєнного стану // *Міжнародний науковий журнал «Інтернаука». Серія: «Юридичні науки»*. 2023. № 6(64). С. 114–128. doi: <https://doi.org/10.25313/2520-2308-2023-6-8998>.

14. Міжнародний пакт про економічні, соціальні і культурні права: Прийнято 16.12.1966 р. Генеральною Асамблеєю ООН. Док. ООН A/RES/2200 А (XXI). URL: https://zakon.rada.gov.ua/laws/show/995_042#Text (дата звернення: 02.01.2024).
15. Загальна декларація прав людини: Прийнята і проголошена резолюцією 217 А (III) Генеральної Асамблеї ООН від 10.12.1948 р. URL: https://zakon.rada.gov.ua/laws/show/995_015#Text (дата звернення: 02.01.2024).
16. Okinawa Charter on Global Information Societ // *Ministry of Foreign Affairs of Japan websites*. URL: <https://www.mofa.go.jp/policy/economy/summit/2000/documents/charter.html> (дата звернення: 02.01.2024).
17. Declaration of Principles building the information society: a global challenge in the new millennium: Document WSIS-03/GENEVA/DOC/4-E, 12 December 2003 // *World Summit on the Information Society, Geneva 2003 – Tunis 2005*. URL: <https://www.itu.int/net/wsis/docs/geneva/official/dop.html> (дата звернення: 02.01.2024).
18. Yesimov S., Borovikova V. Methodological foundations of information security research // *Social & Legal Studios*. 2023. Vol. 6, No. 1. P. 49–55. doi: <https://doi.org/10.32518/sals1.2023.49>.
19. Стратегія інформаційної безпеки: Затверджена Указом Президента України від 28.12.2021 р. № 685/2021. URL: <https://zakon.rada.gov.ua/laws/show/685/2021#Text> (дата звернення: 02.01.2024).
20. Скриньковський Р. М., Петков С. В., Хмиз М. В., Далик В. П., Катаєв А. В., Ільчишин С. М. Вплив російсько-української війни на туристичну галузь в Україні та світі // *Міжнародний науковий журнал «Інтернаука»*. Серія: «Економічні науки». 2023. № 9(77), т. 2. С. 140–

153. doi: <https://doi.org/10.25313/2520-2294-2023-9-9075>.
21. Скриньковський Р. М., Козяр Р. Я., Петков С. В., Хитра О. Л., Комісаров О. Г. Державна охорона посадових осіб в Україні в умовах воєнного стану // *Міжнародний науковий журнал «Інтернаука». Серія: «Юридичні науки»*. 2023. № 5(63). С. 109–119. doi: <https://doi.org/10.25313/2520-2308-2023-5-8867>.
22. Скриньковський Р. М., Цюх С. І., Процевят О. С., Тиркало Ю. Є., Горбонос Ф. В. Тенденції і проблеми у сфері будівництва України в умовах війни // *Міжнародний науковий журнал «Інтернаука». Серія: «Економічні науки»*. 2022. № 7(63). С. 63–71. doi: <https://doi.org/10.25313/2520-2294-2022-7-8146>.
23. Скриньковський Р. М., Горбонос Ф. В., Цюх С. І., Хмиз М. В., Процевят О. С., Князь С. В. Тенденції і питання продовольчої безпеки України в умовах війни // *Міжнародний науковий журнал «Інтернаука». Серія: «Економічні науки»*. 2022. № 8(64). С. 38–48. doi: <https://doi.org/10.25313/2520-2294-2022-8-8196>.
24. Скриньковський Р. М., Мазур Ю. М., Козяр Р. Я., Петков С. В., Чистоклетов Л. Г. Особливості роботи судів України в умовах воєнного стану // *Міжнародний науковий журнал «Інтернаука». Серія: «Юридичні науки»*. 2023. № 4(62). С. 51–59. doi: <https://doi.org/10.25313/2520-2308-2023-4-8832>.
25. Історія України без міфів: генеза національної стійкості крізь призму наукових досліджень: монографія / Боднарчук О., Вановська І., Караіванов М., Коломоєць О., Коломоєць С., Петков С., Попков Б., Трубчанінов М., Хан Є.; за заг. ред. Б. Попкова, С. Петкова. Київ: Видавництво Ліра-К, 2024. 280 с.
26. Рік війни за свободу: Воєнно-історичний нарис російсько-української війни (24.02.2022– 24.02.2023) у чотирьох книгах. Книга I / Апарат Головнокомандувача Збройних Сил України, Генеральний штаб Збройних Сил України та Центр досліджень воєнної історії Збройних

- Сил України; голова робочої групи: генерал В. Залужний. Київ: Видавництво Ліра-К, 2023. 270 с.
27. Рік війни за свободу: Воєнно-історичний нарис російсько-української війни (24.02.2022 – 24.02.2023) у чотирьох книгах. Книга II / Міністерство оборони України, Апарат Головнокомандувача Збройних Сил України, Генеральний штаб Збройних Сил України та Центр досліджень воєнної історії Збройних Сил України; голова робочої групи: генерал В. Залужний. Київ: Видавництво Ліра-К, 2023. 198 с.
28. Рік війни за свободу: Воєнно-історичний нарис російсько-української війни (24.02.2022 – 24.02.2023) у чотирьох книгах. Книга III / Міністерство оборони України, Апарат Головнокомандувача Збройних Сил України, Генеральний штаб Збройних Сил України та Центр досліджень воєнної історії Збройних Сил України; голова робочої групи: генерал В. Залужний. Київ: Видавництво Ліра-К, 2023. 198 с.
29. Зброя російсько-української війни 2022–2023 років: Довідник-каталог основних зразків озброєння та військової техніки які застосовувалися протиборчими сторонами під час відсічі широкомасштабного вторгнення рф в Україну (24.02.2022 – 30.06.2023) / Міністерство оборони України, Апарат Головнокомандувача Збройних Сил України, Генеральний штаб Збройних Сил України, Центр досліджень воєнної історії Збройних Сил України; голова робочої групи: генерал В. Залужний. Київ: Видавництво Ліра-К, 2023. 243 с.
30. Абрамова Ю. Україна ініціює процес виключення Росії з ООН, – заява МЗС // *Матеріали загальноукраїнського сайту новин «ТСН.ua» (Телевізійної служби новин, що виходить на телеканалі «1+1»)*. 26.12.2022. URL: <https://tsn.ua/svit/ukrayina-iniciyuue-proces-viklyuchennya-rosiyi-z-oon-zayava-mzs-2230984.html> (дата звернення: 02.01.2024).

31. Конституція України: прийнята на п'ятій сесії Верховної Ради України 28 червня 1996 року (із змінами). URL: <https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text> (дата звернення: 02.01.2024).
32. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»: Указ Президента України від 25.02.2017 р. № 47/2017 (із змінами). URL: <https://zakon.rada.gov.ua/laws/show/47/2017#Text> (дата звернення: 02.01.2024).
33. Малашко О. Є., Єсімов С. С. Зміст державної діяльності із забезпечення інформаційної безпеки // *Міжнародний науковий журнал «Інтернаука»*. 2020. № 15(95), т. 1. С. 46–54. doi: <https://doi.org/10.25313/2520-2057-2020-15-6341>.
34. Про захист інформації в інформаційно-комунікаційних системах: Закон України від 05.07.1994 р. № 80/94-ВР (із змінами). URL: <https://zakon.rada.gov.ua/laws/show/80/94-вр#Text> (дата звернення: 02.01.2024).
35. Про захист персональних даних: Закон України від 01.06.2010 р. № 2297-VI (із змінами). URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text> (дата звернення: 02.01.2024).
36. Про критичну інфраструктуру: Закон України від 16.11.2021 р. № 1882-IX (із змінами). URL: <https://zakon.rada.gov.ua/laws/show/1882-20#Text> (дата звернення: 02.01.2024).
37. Про затвердження Національної економічної стратегії на період до 2030 року: Постанова Кабінету Міністрів України від 03.03.2021 р. № 179 (із змінами). URL: <https://zakon.rada.gov.ua/laws/show/179-2021-п#Text> (дата звернення: 02.01.2024).

References

1. Pro informatsiiu: Zakon Ukrainy vid 02.10.1992 r. № 2657-XII (iz

- zminamy). URL: <https://zakon.rada.gov.ua/laws/show/2657-12#Text> (date of access: 02.01.2024).
2. Nashynets-Naumova A. Y. *Informatsiina bezpeka: pytannia pravovoho rehuliuвання: monohrafiia*. Kyiv: Vydavnychy dim «Helvetyka», 2017. 168 s.
 3. Bilenchuk P. D., Borysova L. V., Neklonskyi I. M., Sobyna V. O. *Pravovi zasady informatsiinoi bezpeky Ukrainy: monohrafiia / Za red. P.D. Bilenchuka*. Kharkiv: 2018. 289 s.
 4. Levchenko O. V. *Systema zabezpechennia informatsiinoi bezpeky derzhavy u voiennoi sferi: osnovy pobudovy ta funktsionuvannia: monohrafiia*. Zhytomyr: Vydavets PP «Ievro-Volyn», 2021. 172 s.
 5. Pro natsionalnu bezpeku Ukrainy: Zakon Ukrainy vid 21.06.2018 r. № 2469-VIII (iz zminamy). URL: <https://zakon.rada.gov.ua/laws/show/2469-19#Text> (date of access: 02.01.2024).
 6. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 15 zhovtnia 2021 roku «Pro Stratehiiu informatsiinoi bezpeky»: Ukaz Prezydenta Ukrainy vid 28.12.2021 r. № 685/2021. URL: <https://zakon.rada.gov.ua/laws/show/685/2021#Text> (date of access: 02.01.2024).
 7. United Nations Charter (full text) // *United Nations websites*. URL: <https://www.un.org/en/about-us/un-charter/full-text> (date of access: 02.01.2024).
 8. Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations: UN. General Assembly (25th sess.: 1970) // *UN Digital Library*. URL: <https://digitallibrary.un.org/record/202170> (date of access: 02.01.2024).
 9. *Ukraina pid chas rosiisko-ukrainskoi viiny 2014–2023 rr.: geneza natsionalnoi stiikosti kriz pryzmu naukovykh doslidzhen: monohrafiia / Vanovska I. M., Dzhus O. A., Iliashko O. O., Kopotun I. M., Koropatnik I.*

- M., Pervak I. O., Petkov S. V., Popkov B. O., Skriabin O. L., Stetsiuk S. P., Skrynkovskyy R. M., Sopilnyk L. I., Trubchaninov M. A., Khan Y. V., Shemchuk V. V.; za zah. red. B. Popkova, S. Petkova. Kyiv: Vydavnytstvo Lira-K. 2023. 272 s.
10. Khoroshko V., Kozel T., Yaroshenko O. Osoblyvosti zastosuvannya suchasnoi informatsiinoi zbroi // *Pravove, normatyvne ta metrolohichne zabezpechennia system zakhystu informatsii v Ukraini*. 2015. Vyp 1(29). S. 9– 14. URL: http://old.pnzzi.kpi.ua/29/29_p9.pdf (date of access: 02.01.2024).
 11. International Covenant on Civil and Political Rights: Adopted and opened for signature, ratification and accession by General Assembly resolution 2200A (XXI) of 16 December 1966, entry into force 23 March 1976, in accordance with Article 49 // *United Nations websites*. URL: <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights> (date of access: 02.01.2024).
 12. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) // *Official Journal of the European Union*. L 333. Vol. 65. 27.12.2022 (ISSN 1977-0677). URL: <http://data.europa.eu/eli/dir/2022/2555/oj> (date of access: 02.01.2024).
 13. Skrynkovskyy R. M., Koziar R. Y., Petkov S. V., Khmyz M. V., Chystokletov L. H. Derzhavna okhorona v Ukraini shchodo hlav inozemnykh derzhav ta posadovykh osib mizhnarodnykh orhanizatsii v umovakh voiennoho stanu // *Mizhnarodnyi naukovyi zhurnal «Internauka». Serii: «Iurydychni nauky»*. 2023. № 6(64). S. 114–128. doi: <https://doi.org/10.25313/2520-2308-2023-6-8998>.
 14. Mizhnarodnyi pakt pro ekonomichni, sotsialni i kulturni prava: Pryiniato

- 16.12.1966 r. Heneralnoiu Asambleieiu OON. Dok. OON A/RES/2200 A (XXI). URL: https://zakon.rada.gov.ua/laws/show/995_042#Text (date of access: 02.01.2024).
15. Zahalna deklaratsiia prav liudyny: Pryiniata i proholoshena rezoliutsiieiu 217 A (III) Heneralnoi Asamblei OON vid 10.12.1948 r. URL: https://zakon.rada.gov.ua/laws/show/995_015#Text (date of access: 02.01.2024).
16. Okinawa Charter on Global Information Societ // *Ministry of Foreign Affairs of Japan websites*. URL: <https://www.mofa.go.jp/policy/economy/summit/2000/documents/charter.html> (date of access: 02.01.2024).
17. Declaration of Principles building the information society: a global challenge in the new millennium: Document WSIS-03/GENEVA/DOC/4-E, 12 December 2003 // *World Summit on the Information Society, Geneva 2003 – Tunis 2005*. URL: <https://www.itu.int/net/wsis/docs/geneva/official/dop.html> (date of access: 02.01.2024).
18. Yesimov S., Borovikova V. Methodological foundations of information security research // *Social & Legal Studios*. 2023. Vol. 6, No. 1. P. 49–55. doi: <https://doi.org/10.32518/sals1.2023.49>.
19. Stratehiia informatsiinoi bezpeky: Zatverdzhena Ukazom Prezydenta Ukrainy vid 28.12.2021 r. № 685/2021. URL: <https://zakon.rada.gov.ua/laws/show/685/2021#Text> (date of access: 02.01.2024).
20. Skrynkovskyy R. M., Petkov S. V., Khmyz M. V., Dalyk V. P., Kataiev A. V., Ilchyshyn S. M. Vplyv rosiisko-ukrainskoi viiny na turystychnu haluz v Ukraini ta sviti // *Mizhnarodnyi naukovyi zhurnal «Internauka». Serii: «Ekonomichni nauky»*. 2023. № 9(77), t. 2. S. 140–153. doi: <https://doi.org/10.25313/2520-2294-2023-9-9075>.
21. Skrynkovskyy R. M., Koziar R. Y., Petkov S. V., Khytra O. L., Komisarov

- O. H. Derzhavna okhorona posadovykh osib v Ukraini v umovakh voiennoho stanu // *Mizhnarodnyi naukovyi zhurnal «Internauka». Serii: «Iurydychni nauky»*. 2023. № 5(63). S. 109–119. doi: <https://doi.org/10.25313/2520-2308-2023-5-8867>.
22. Skrynkovskyy R. M., Tsyuh S. I., Protseviat O. S., Tyrkalo Y. Y., Horbonos F. V. Tendentsii i problemy u sferi budivnytstva Ukrainy v umovakh viiny // *Mizhnarodnyi naukovyi zhurnal «Internauka». Serii: «Ekonomichni nauky»*. 2022. № 7(63). S. 63–71. doi: <https://doi.org/10.25313/2520-2294-2022-7-8146>.
23. Skrynkovskyy R. M., Horbonos F. V., Tsyuh S. I., Khmyz M. V., Protseviat O. S., Kniaz S. V. Tendentsii i pytannia prodovolchoi bezpeky Ukrainy v umovakh viiny // *Mizhnarodnyi naukovyi zhurnal «Internauka». Serii: «Ekonomichni nauky»*. 2022. № 8(64). S. 38–48. doi: <https://doi.org/10.25313/2520-2294-2022-8-8196>.
24. Skrynkovskyy R. M., Mazur Y. M., Koziar R. Y., Petkov S. V., Chystokletov L. H. Osoblyvosti roboty sudiv Ukrainy v umovakh voiennoho stanu // *Mizhnarodnyi naukovyi zhurnal «Internauka». Serii: «Iurydychni nauky»*. 2023. № 4(62). S. 51–59. doi: <https://doi.org/10.25313/2520-2308-2023-4-8832>.
25. Istoriiia Ukrainy bez mifiv: heneza natsionalnoi stiikosti kriz pryzmu naukovykh doslidzhen: monohrafiia / Bodnarchuk O., Vanovska I., Karaivanov M., Kolomoiets O., Kolomoiets S., Petkov S., Popkov B., Trubchaninov M., Khan Y.; za zah. red. B. Popkova, S. Petkova. Kyiv: Vydavnytstvo Lira-K, 2024. 280 s.
26. Rik viiny za svobodu: Voienno-istorychnyi narys rosiisko-ukrainskoi viiny (24.02.2022– 24.02.2023) u chotyrokhn knykh. Knyha I / Aparat Holovnokomanduvacha Zbroinykh Syl Ukrainy, Heneralnyi shtab Zbroinykh Syl Ukrainy ta Tsentri doslidzhen voiennoi istorii Zbroinykh Syl Ukrainy; holova robochoi hrupy: heneral V. Zaluzhnyi. Kyiv: Vydavnytstvo Lira-K, 2023. 270 s.

27. Rik viiny za svobodu: Voienno-istorychnyi narys rosiisko-ukrainskoi viiny (24.02.2022 – 24.02.2023) u chotyrokhn knykhakh. Knyha II / Ministerstvo oborony Ukrainy, Aparat Holovnokomanduvacha Zbroinykh Syl Ukrainy, Heneralnyi shtab Zbroinykh Syl Ukrainy ta Tsentri doslidzhen voiennoi istorii Zbroinykh Syl Ukrainy; holova robochoi hrupy: heneral V. Zaluzhnyi. Kyiv: Vydavnytstvo Lira-K, 2023. 198 s.
28. Rik viiny za svobodu: Voienno-istorychnyi narys rosiisko-ukrainskoi viiny (24.02.2022 – 24.02.2023) u chotyrokhn knykhakh. Knyha III / Ministerstvo oborony Ukrainy, Aparat Holovnokomanduvacha Zbroinykh Syl Ukrainy, Heneralnyi shtab Zbroinykh Syl Ukrainy ta Tsentri doslidzhen voiennoi istorii Zbroinykh Syl Ukrainy; holova robochoi hrupy: heneral V. Zaluzhnyi. Kyiv: Vydavnytstvo Lira-K, 2023. 198 s.
29. Zbroia rosiisko-ukrainskoi viiny 2022–2023 rokiv: Dovidnyk-kataloh osnovnykh zrazkiv ozbroiennia ta viiskovoi tekhniky yaki zastosovuvalysia protyborchymy storonamy pid chas vidsichi shyrokomasshtabnoho vtorhnennia rf v Ukrainu (24.02.2022 – 30.06.2023) / Ministerstvo oborony Ukrainy, Aparat Holovnokomanduvacha Zbroinykh Syl Ukrainy, Heneralnyi shtab Zbroinykh Syl Ukrainy, Tsentri doslidzhen voiennoi istorii Zbroinykh Syl Ukrainy; holova robochoi hrupy: heneral V. Zaluzhnyi. Kyiv: Vydavnytstvo Lira-K, 2023. 243 s.
30. Abramova Yu. Ukraina initsiiuie protses vykliuchennia Rosii z OON, – zaiava MZS // *Materialy zahalnoukrainskoho saituv novyn «TSN.ua» (Televiziinoi sluzhby novyn, shcho vykhodyt na telekanali «1+1»)*. 26.12.2022. URL: <https://tsn.ua/svit/ukrayina-iniciyuye-proces-viklyuchennya-rosiyi-z-oon-zayava-mzs-2230984.html> (date of access: 02.01.2024).
31. Konstytutsiia Ukrainy: pryiniata na piatii sesii Verkhovnoi Rady Ukrainy 28 chervnia 1996 roku (iz zminamy). URL: <https://zakon.rada.gov.ua/laws/show/254k/96-Br#Text> (date of access: 02.01.2024).

32. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 29 hrudnia 2016 roku «Pro Doktrynu informatsiinoi bezpeky Ukrainy»: Ukaz Prezydenta Ukrainy vid 25.02.2017 r. № 47/2017 (iz zminamy). URL: <https://zakon.rada.gov.ua/laws/show/47/2017#Text> (date of access: 02.01.2024).
33. Malashko O. Y., Yesimov S. S. Zmist derzhavnoi diialnosti iz zabezpechennia informatsiinoi bezpeky // *Mizhnarodnyi naukovyi zhurnal «Internauka»*. 2020. № 15(95), t. 1. S. 46–54. doi: <https://doi.org/10.25313/2520-2057-2020-15-6341>.
34. Pro zakhyst informatsii v informatsiino-komunikatsiinykh systemakh: Zakon Ukrainy vid 05.07.1994 r. № 80/94-BP (iz zminamy). URL: <https://zakon.rada.gov.ua/laws/show/80/94-Bp#Text> (date of access: 02.01.2024).
35. Pro zakhyst personalnykh danykh: Zakon Ukrainy vid 01.06.2010 r. № 2297-VI (iz zminamy). URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text> (date of access: 02.01.2024).
36. Pro krytychnu infrastrukturu: Zakon Ukrainy vid 16.11.2021 r. № 1882-IX (iz zminamy). URL: <https://zakon.rada.gov.ua/laws/show/1882-20#Text> (date of access: 02.01.2024).
37. Pro zatverdzhennia Natsionalnoi ekonomichnoi stratehii na period do 2030 roku: Postanova Kabinetu Ministriv Ukrainy vid 03.03.2021 r. № 179 (iz zminamy). URL: <https://zakon.rada.gov.ua/laws/show/179-2021-П#Text> (date of access: 02.01.2024).