УДК (342 + 343) : 004
DOI https://doi.org/10.32782/2524-0374/2024-7/64

СПІВВІДНОШЕННЯ НАЦІОНАЛЬНОЇ ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ У ПЛОЩИНІ ІНФОРМАЦІЙНОГО І КРИМІНАЛЬНОГО ПРАВА

CORRELATION BETWEEN NATIONAL AND INFORMATION SECURITY OF THE STATE IN THE AREA OF INFORMATION AND CRIMINAL LAW

Міхайліна Т.В., д.ю.н., професор,
професор кафедри теорії, історії держави і права та філософії права
Донецький національний університет імені Василя Стуса

Мартинюк О.В., к.ю.н., доцент,
доцент кафедри конституційного, міжнародного і кримінального права
Донецький національний університет імені Василя Стуса

Метою наукової статті є аналіз співвідношення національної та інформаційної безпеки держави у площині інформаційного та кримінального права України.

У процесі дослідження виявлено, що значення співвідношення національної та інформаціної безпеки, передусім, обумовлено двома чинниками: 1) стрімка інформатизація всіх сфер суспільного буття, внаслідок чого вони переплітаються з інформаційною складовою, яка починає впливати на їхню сутність, розвиток та трансформацію; 2) російська агресія, яка на всіх своїх етапах супроводжувалася інформаційними атаками, що й обумовлюють особливу роль інформаційної безпеки у забезпеченні національної безпеки.

Акцентується увага на тому, що нормативне забезпечення національної та інформаційної безпеки в Україні характеризується безсистемністю. Спостерігається значний масив нормативних актів законодавчого та підзаконного характеру, які по-різному характеризують детермінанти порушення національної та інформаційної безпеки, по-різному розставляють пріоритети у боротьбі з інформаційними загрозами, рівно як і визначають самі інформаційні загрози.

Яскравим прикладом відсутності системності інформаційного законодавства у контексті забезпечення національної безпеки є те, що інформаційна безпека та кібербезпека визначаються самостійними елементами національної безпеки. Хоча, як вбачається, це є помилковим, зважаючи на спільний об'єкт посягання, – тобто, інформацію (змінюється тільки середовище її існування та функціонування). Отже, інформаційна безпека має визнаватися родовим поняттям щодо кібербезпеки і таким же чином викладатися у правових нормах.

Наголошується, що безсистемність інформаційного законодавства в аспекті забезпечення національної безпеки держави особливо яскраво виявляє себе у кримінальному праві України, яке для виконання своїх функцій має бути чітко структурованим та узгодженим.

Зроблено висновок, що аспекти співвідношення національної, інформаційної та кібезпезпеки потребують систематизації, як на рівні адміністративного, інформаційного, так і, особливо, на рівні кримінального права.

Ключові слова: національна безпека, інформаційна безпека, інформація, кримінальна відповідальність, злочин, інформаційна культура, воєнний стан, збройна агресія.

The purpose of the scientific article is to analyze the correlation between national and information security of the state in the field of Information Law and Criminal Law of Ukraine.

It was revealed that the importance of the relationship between national and information security is primarily due to two factors: 1) rapid informatization of all spheres of public existence, as a result of which they are intertwined with the information component, which begins to influence their essence, development and transformation; 2) russian aggression, which at all its stages was accompanied by information attacks, which determine the special role of information security in ensuring national security.

Attention is focused on the fact that the regulatory support of national and information security in Ukraine is characterized by haphazardness. There is a significant array of normative acts of a legislative and by-law nature, which characterize the determinants of violations of national and information security in different ways, set priorities in the fight against information threats in different ways, as well as determine the information threats themselves.

A striking example of the lack of systematic information legislation in the context of ensuring national security is that information security and cybersecurity are determined by independent elements of national security. Although this is erroneous, given the general object of encroachment – that is, information (only the environment of its existence and functioning changes). Therefore, information security should be recognized as a generic concept of cybersecurity and similarly set out in legal norms.

It is noted that the haphazardness of information legislation in the aspect of ensuring national security of the state is particularly pronounced in the criminal law of Ukraine, which must be clearly structured and coordinated in order to perform its functions.

It is concluded that aspects of the correlation between national, information and cyber security need to be systematized, both at the level of administrative, informational, and, especially, at the level of criminal law.

Key words: national security, information security, information, criminal liability, crime, information culture, martial law, armed aggression.

Вступ. Останнє десятиліття стало для України часом викликів, коли наша національна безпека піддалася такій кількості загроз, які навіть уявити було складно. Аннексія російською федерацією українських територій, а потім і повномасштабна агресія поклали початок новітньої історії, сповненої ризиків для існування самої української державності. Варто зазначити, що національна безпека є інтегративною категорією, яка складається з комплексу компонентів, які функціонально поєднані і, взаємодоповнюючи один одного, формують стан захищеності національних інтересів. З-поміж компонентів національної безпеки, які, безспірно, всі є важливими, можна вокремити безпеку інформаційну. Вона має підвищене значення з двох причин. По-перше, об'єктивною є стрімка інформатизація всіх сфер суспільного буття, внаслідок чого вони переплітаються з інформаційною складовою, яка починає впливати на їхню сутність, розвиток та трансформацію. По-друге, російська агресія на всіх своїх етапах супроводжувалася інформаційними атаками, які й обумовлюють особливу роль інформаційної безпеки у забезпеченні національної безпеки. Таким чином, співвідношення національної та інформаційної безпеки, і так досить актуальне протягом останніх десятиліть, набуває безпрецедентної актуалізації.

Аналіз останніх наукових досліджень і публікацій. Аналіз співвідношення інформаційної та національної безпеки держави здійснюється науковцями регулярно. Зокрема, цьому питанню присвячували свої роботи такі вчені, як П. Біленчук, І. Діордіца, О. Заріцький, М. Ігна-

тюк, Л. Ковальчук, В. Кононенко, П. Копицька, Б. Кормич, Л. Новікова, Т. Ткачук, Р. Черниш та багато інших. Разом з тим, досліджень співвідношення інформаційної та національної безпеки держави у площині кримінального права не так вже й багато, що робить дослідження своєчаним та необхідним.

Метою статті є аналіз співвідношення національної та інформаційної безпеки держави у площині інформаційного та кримінального права України.

Виклад основного матеріалу. Перше, що необхідно зробити для цілей цього дослідження, це виявити поняття та сутність обох категорій: національної та інформаційної безпеки.

Національна безпека України, відповідно до Закону «Про національну безпеку України», має легальне визначення, а саме: захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних та потенційних загроз [1]. Вона включає в себе, зокрема, воєнну безпеку держави; безпеку конституційного ладу, суспільства та громадського порядку; міжнародну безпеку; економічну безпеку; інформаційну безпеку; кібербезпеку; енергетичну безпеку. Тож, як можна побачити, самостійними складниками національної безпеки України виділяються інформаційна та кібербезпека.

У науковій літературі інформаційна безпека трактується як стан захищеності інформаційного середовища суспільства, який забезпечує його формування, використання і розвиток в інтересах особи, суспільства, держави. На думку науковців, інформаційна безпека включає в себе сукупність організаційних, соціально-економічних, юридичних заходів, спрямованих на забезпечення сталого розвитку суспільства і держави. Безпека в інформаційній сфері, на думку П. Д. Біленчука, передбачає забезпечення інформаційного суверенітету; удосконалення державного регулювання розвитку інформаційної сфери шляхом створення нормативно-правових та економічних передумов для розвитку національної інформаційної інфраструктури та ресурсів, впровадження сучасних технологій у цій сфері, наповнення інформаційного простору достовірною інформацією; забезпечення конституційного права громадян на свободу слова, доступу до інформації, недопущення протиправного втручання органів державної влади у діяльність засобів масової інформації; вживання комплексних заходів щодо захисту національного інформаційного простору та протидії монополізації інформаційної сфери держави [2, с. 64; 3, 54–55]. Тож, як бачимо, інформаційна безпека являє собою комплексне, різновекторне явище, яке покликане забезпечувати стан захищеності відносин та нейтралізувати загрози у досить різних сферах суспільства, які мають неабияку специфіку.

Повністю справедливим та законодавчо обумовленим може бути визнано твердження, що «інформаційна безпека виступає інтегрованим компонентом національної безпеки і позиціонується як пріоритетна функція держави. З одного боку, інформаційна безпека спрямована на забезпечення якісного всебічного інформування громадян та їх необмеженого доступу до різних інформаційних джерел. З іншого боку, вона передбачає контроль за непоширенням дезінформації, сприяння суспільній цілісності, охорону інформаційного суверенітету, протидію негативним інформаційним впливам пропагандистського та психологічного характеру, а також захист державного інформаційного простору від різних маніпуляційних дій та інформаційних війн» [4, с. 214]. Тож, на комплексності інформаційної безпеки наголошують майже всі автори, що присвячували свої дослідження обраній проблематиці, з чим можна повністю погодитися. Тим більше, надважливою є акцентуалізація на воєнному стані в Україні, коли інформаційні загрози виходять на передній план і стають одним із засобів гібридної війни.

У Стратегії національної безпеки України серед основних загроз національній безпеці, які мають безпосередній стосунок до інформаційної сфери, також визначаються агресивні дії росії, що підривають суспільно-політичну стабільність з метою знищення держави Україна й захоплення її території, в тому числі інформаційно-психологічну війну, приниження української мови й культури, фальшування української історії, формування російськими засобами масової комунікації альтернативної до дійсності викривленої інформаційної картини світу, а також ведення інформаційної війни проти України, відсутність цілісної комунікативної політики держави, недостатній рівень медіакультури суспільства, уразливість об'єктів критичної інфраструктури, державних інформаційних ресурсів до кібератак, фізична й моральна застарілість системи охорони державної таємниці та інших видів інформації з обмеженим доступом [5; 6, с. 183]. Як випливає з наведеного, як законодавець, так і науковці виділяють комплексний характер загроз інформаційній безпеці держави, рівно як і їхніх причин. Відповіддю на зазначені загрози, на думку науковців, може стати збалансована та повністю переосмислена інформаційна політика держави.

О. Бусол, а вслід за ним і О. Солдатенко, серед основних пріоритетів державної політики в інформаційній сфері називають: законодавче врегулювання механізму виявлення, фіксації, блокування та видалення з інформаційного простору держави, зокрема з українського сегмента мережі Інтернет, інформації, яка загрожує життю, здоров'ю громадян України, пропагує війну, національну та релігійну ворожнечу, зміну конституційного ладу насильницьким шляхом або порушення територіальної цілісності України, загрожує державному суверенітету; пропагує комуністичний та/або націонал-соціалістичний (нацистський) тоталітарні режими та їхню символіку [7; 8, с. 136]. Зважаючи на поточну ситуацію, перелічені аспекти інформаційної політики набувають особливого значення під час військової агресії, проте, слід зазначити, що навіть зараз ці аспекти здійснюються в нашій державі вкрай неефективно.

Отже, з точки зору співвідношення національної та інформаційної безпеки, суперечок не може бути, оскільки законодавець чітко визначив, що інформаційна безпека є одним з аспектів (компонентів) безпеки національної. У Стратегії інформаційної безпеки від 28 грудня 2021 року зазначається, що інформаційну безпеку слід розглядати як складову частину національної безпеки [9], спрямовану на посилення можливостей захисту інформаційного простору, підтримки інформаційними засобами та заходами соціальної та політичної стабільності держави, в тому числі щодо забезпечення прав людини на збирання, зберігання, використання та поширення інформації, доступу до достовірної та об'єктивної інформації, а також вжиття ефективних заходів протидії деструктивній пропаганді, інформаційно-психологічним спеціальним операціям (ІПСО) та інформаційному тероризму. Тим не менше, з аналізу різних нормативно-правових актів України законодавчого та підзаконного характеру вбачається, що хоча всі вони акцентують увагу на комплексності інформаційної безпеки та на значній кількості загроз у інформаційній сфері, проте, всі вони страждають на порушення правил юридичної техніки. Всі загрози інформаційній безпеці, а також їх наслідки та пріорітети боротьби з ними викладено у несистематизованому, інколи хаотичному вигляді. Деякі з названих характеристик інформаційної безпеки в різних НПА дублюють одна одну, проте наводяться у різних формулюваннях (що з точки зору дотримання принципу системності права є неприпустимим); деякі згадуються в одних НПА, і абсолютно не згадуються в інших; пріоритети у боротьбі з зазначеними негативними проявами також визначаються по-різному. А зважаючи на досить значний масив нормативного матеріалу, сформова-

ний в інформаційній сфері правотворцем за останні десятиліття, така несистематизованість перетворюється на серйозну проблему у правоохоронній діяльності та правозастосовчій практиці.

На наш погляд, однією з ознак відсутності системності правового забезпечення національної та інформаційної безпеки є визначення інформаційної та кібербезпеки самостійними аспектами безпеки національної. Офіційне визначення поняття кібербезпеки міститься в Стратегії кібербезпеки України, в якому під кібербезпекою розуміється стан захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі, що досягається комплексним застосуванням сукупності правових, організаційних, інформаційних заходів. кібернетична безпека, так само як і інформаційна безпека, є не лише невід'ємним складником кожної зі сфер національної безпеки, а й водночас виступає самостійною сферою забезпечення національної безпеки, що зазначено у Доктрині інформаційної безпеки України [10; 11, с. 110, 111]. Тож, як можна побачити, у площині забезпечення національної безпеки України, діють одночасно Стратегія інформаційної безпеки та Стратегія кібербезпеки України. Також паралельно діє Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 р. [12], що робить ці категорії на нормативному рівні ніби-то однопорядковими явищами. Проте, відповідно до філософського закону співвідношення загального та конкретного, так не має бути, оскільки інформаційна безпека та кібербезпека функціонально призначені для протидії одному типу загроз – інформаційних. І об'єкт посягання усіх цих протиправних діянь буде один і той самий – інформація. Змінюється тільки середовище її існування та функціонування.

За твердженням Б. Кормича, з одного боку, інформаційна безпека трактується як самостійний компонент національної безпеки будь-якої держави. З іншого боку, інформаційна безпека – це інтегрований складовий елемент будь-якої іншої безпеки – військової, економічної, політичної тощо [13, с. 83]. З цим твердженням можна повністю погодитися. Але слід також наголосити на тому, що інформаційна безпека є не лише інтегративною категорією, яка знаходить свій вираз у всіх без винятку аспектах національної безпеки держави, а також категорією комплексною, що містить у своєму складі ще й кібербезпеку. Причому, на наше глибоке переконання, таким же чином співвідношення досліджуваних явищ має бути закріплене на нормативному рівні, і ніяк інакше. Неможливо вирвати частину цілісного явища і розглядати її повністю відокремлено, сподіваючись на результат. Тож, кібербезпека має розглядатися спочатку як частина інформаційної безпеки держави (а не відірвано від неї), і тільки потім вони разом мають розглядатися як складник національної безпеки та виступати інтегративною категорією щодо всіх інших складників національної безпеки держави.

Зазначена безсистемність інформаційного законодавства в аспекті забезпечення національної безпеки держави яскраво виявляє себе у кримінальному праві України.

Зокрема, Розділ І Особливої частини КК України присвячено злочинам проти основ національної безпеки України, що включає в себе: дії, спрямовані на насильницьку зміну чи повалення конституційного ладу або на захоплення державної влади (ст. 109); посягання на територіальну цілісність і недоторканність України (ст. 110); фінансування дій, вчинених з метою насильницької зміни чи повалення конституційного ладу або захоплення державної влади, зміни меж території або державного кордону України (ст. 110-2); державна зрада (ст. 111); колабораційна діяльність (ст. 111-1); пособництво державі-агресору (ст. 111-2); посягання на життя державного чи громадського діяча (ст. 112); диверсія (ст. 113); шпигунство (ст. 114); перешкоджання законній діяльності Збройних Сил України та інших військових формувань (ст. 114-1); несанкціоноване поширення інформації про направлення, переміщення зброї, озброєння та бойових припасів в Україну, рух, переміщення або розміщення Збройних Сил України чи інших утворених відповідно до законів України військових формувань, вчинене в умовах воєнного або надзвичайного стану (ст. 114-2).

Як бачимо, окремих складів злочинів, що посягають на інформаційну безпеку держави у межах національної норми цього розділу взагалі не передбачають. Окремі елементи інформаційної безпеки відображаються хіба що у кваліфікованих складах злочинів у вигляді кваліфікаційних ознак. Зокрема, ч. 3 ст. 109 встановлює відповідальність за «публічні заклики до насильницької зміни чи повалення конституційного ладу або до захоплення державної влади, а також розповсюдження матеріалів із закликами до вчинення таких дій, ... вчинені з використанням засобів масової інформації». Але інформаційне середовище є набагато ширшим виключно за засоби масової інформації, тож наведена норма відображає дуже вузький аспект інформаційної безпеки.

Відповідно до ч. 6 ст. 111-1 «Колабораційна діяльність» караними є «організація та проведення заходів політичного характеру, здійснення інформаційної діяльності у співпраці з державою-агресором та/або його окупаційною адміністрацією, спрямованих на підтримку держави-агресора, її окупаційної адміністрації чи збройних формувань та/або на уникнення нею відповідальності за збройну агресію проти України, за відсутності ознак державної зради, активна участь у таких заходах». Але і тут відображено лише один аспект інформаційної безпеки, що обмежується інформаційною діяльністю у співпраці з агресором.

Розділ XIV КК України «Кримінальні правопорушення у сфері охорони державної таємниці, недоторканності державних кордонів, забезпечення призову та мобілізації» також у значній частині (ст. 328; 329; 330) містить склади злочинів, які спрямовані комплексно проти інформаційної та національної безпеки, але викладений окремо, за межами Розділу І «Злочини проти основ національної безпеки».

Частково включають у себе аспекти інформаційної безпеки ст.ст. 158; 163; 168; 171; 176; 182; ч. 3, 4 ст. 190; 220-1; 231; 232; 232-1; 232-2; 232-3; 238; 259; ч. 4 ст. 299; 300; ч. 2 ст. 301; 301-1; 301-2; 359; 360; 376-1; 381 КК України, але вони, у свою чергу, не мають співвідношення з безпекою національною та стосуються безпеки фізичних і юридичних осіб, громадської безпеки, порядку тощо.

Частина 2 ст. 258-2 зазначає, що кримінально караними є публічні заклики до вчинення терористичного акту, «вчинені з використанням засобів масової інформації», що також суттєво обмежує сферу дії цієї норми.

Розділ XVI КК України «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» містить склади виключно інформаційних правопорушень, тобто таких, що посягають на інформаційну безпеку. Але деякі з них включають кваліфікуючі ознаки, що вказують на можливість посягання на національну безпеку.

Так, у частині 5 ст. 361 зазначається, що підлягають кримінальній відповідальності «дії, передбачені частиною третьою або четвертою цієї статті, вчинені під час дії воєнного стану». Ця норма викликає немало зауважень та заперечень. Не в останню чергу, через її санкцію, в якій зазначено, що такі дії «караються позбавленням волі на строк від десяти до п'ятнадцяти років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років». Тож, як можна побачити, санкція цієї норми є більш, ніж суворою. І більше того, усі діяння, передбачені ч. ч. 3 та 4 ст. 361 наразі (тобто, під час дії воєнного стану) підлягають кваліфікації за сукупністю

також за ч. 5 ст. 361 з відповідними юридичними наслідками. Але навряд чи усі ці дії реально відповідають характеристикам особливо тяжких злочинів. Тим більше, якщо вчинені, наприклад, у сфері економіки та не відносяться до сфери національної безпеки.

Крім того, викликає запитання сама назва Розділу XVI, яка, по-перше, є застарілою, а, по-друге, якщо звертатися до інформаційного законодавства, то загальновживаними є терміни «інформаційна безпека» та «кібернетична безпека» (кібербезпека), які доцільно було б використовувати і у кримінальному праві для чіткого розуміння сфери застосування відповідних норм.

Таким чином, виявлено суттєві відмінності у підходах інформаційного та кримінального права щодо співвідношення національної та інформаційної безпеки, що поєднуються зі значними термінологічними неузгодженостями. Оскільки інформаційне право напрацювало значний масив нормативного матеріалу щодо співвідношення національної та інформаційної безпеки, логічно було б втілити цей підхід і в кримінальному праві. Натомість, норми кримінального права щодо досліджуваного питання є несистематизованими, розпорошеними, з величезною кількістю прогалин та дублювань.

Висновки. У процесі дослідження виявлено, що значення співвідношення національної та інформаціної безпеки, передусім, обумовлено двома чинниками: 1) стрімка інформатизація всіх сфер суспільного буття, внаслідок чого вони переплітаються з інформаційною складовою, яка починає впливати на їхню сутність, розвиток та трансформацію; 2) російська агресія, яка на всіх своїх етапах супроводжувалася інформаційними атаками, що й обумовлюють особливу роль інформаційної безпеки у забезпеченні національної безпеки.

Акцентується увага на тому, що нормативне забезпечення національної та інформаційної безпеки в Україні характеризується безсистемністю. Спостерігається значний масив нормативних актів законодавчого та підзаконного характеру, які по-різному характеризують детермінанти порушення національної та інформаційної безпеки, по-різному розставляють пріоритети у боротьбі з інформаційними загрозами, рівно як і визначають самі інформаційні загрози.

Яскравим прикладом відсутності системності інформаційного законодавства у контексті забезпечення національної безпеки є те, що інформаційна безпека та кібербезпека визначаються самостійними елементами національної безпеки. Хоча, як вбачається, це є помилковим, зважаючи на спільний об'єкт посягання, – тобто, інформацію (змінюється тільки середовище її існування та функціонування). Отже, інформаційна безпека має визнаватися родовим поняттям щодо кібербезпеки і таким же чином викладатися у правових нормах.

Наголошується, що безсистемність інформаційного законодавства в аспекті забезпечення національної безпеки держави особливо яскраво виявляє себе у кримінальному праві України, яке для виконання своїх функцій має бути чітко структурованим та узгодженим.

Зроблено висновок, що аспекти співвідношення національної, інформаційної та кібезпезпеки потребують систематизації, як на рівні адміністративного, інформаційного, так і, особливо, на рівні кримінального права.

ЛІТЕРАТУРА

1. Про національну безпеку України: Закон України від 21 червня 2018 року, № 2469-VIII. *Відомості Верховної Ради України*. 2018. № 31. Ст. 241. (Із змінами).
2. Біленчук П.Д. Правові засади інформаційної безпеки України. Харків, 2018. 289 с.
3. Кононенко В.П., Новікова Л.В., Копицька П.О. Політика міжнародних організацій з питань інформаційної безпеки. *Науковий вісник Ужгородського національного університету. Серія ПРАВО*. 2021. Вип. 65. С. 353-358.
4. Черниш Р.Ф., Ігнатюк М.В., Заріцький О.Ю. Протидія деструктивному інформаційному впливу в Україні: правові та організаційні аспекти. *Юридичний науковий електронний журнал*. 2022. № 1. С. 213-216.
5. Рішення Ради національної безпеки і оборони України Про Стратегію національної безпеки України: Введено в дію Указом Президента України від 14 вересня 2020 року, № 392/2020. URL: www.president.gov.ua/documents/3922020-35037
6. Ткачук Т. Сучасні загрози інформаційній безпеці держави: теоретико-правовий аналіз. *Підприємництво, господарство і право*. 2017. №10. С. 182-186.
7. Бусол О. Основні риси контролю за національним інформаційним простором Королівства Велика Британія. http://nbuviap.gov.ua/index.php?option=com_content&view=article&id=2961:osnovni-risi-kontrolyu-za-natsionalniminformatsijnim-prostorom-korolivstva-velikabritaniya&catid=8&Itemid=350.
8. Солдатенко О. Інформаційний простір у мережі Інтернет: правове регулювання та контроль. *Підприємництво, господарство і право*. 2018. № 5. С. 134-140.
9. Стратегія інформаційної безпеки. Затверджено Указом Президента України від 28 грудня 2021 року № 685/2021. *Урядовий кур'єр*. 2021. № 251. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text
10. Стратегія кібербезпеки України. Затверджена Указом Президента України від 26 серпня 2021 року № 447/2021. *Офіційний вісник України* від 10.09.2021. 2021. № 70. стор. 42, стаття 4417, код акта 106911/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#n12
11. Діордіца І. Система забезпечення кібербезпеки: сутність та призначення. *Підприємництво, господарство і право*. 2017. № 7. С. 109-116.
12. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 року, № 2163-VIII *Відомості Верховної Ради України*. 2017. № 45. Ст. 403. (Із змінами).
13. Кормич Б.А. Організаційно-правові засади політики інформаційної безпеки України: монографія. Одеса: Юридична література, 2007. 471 с.