

Ю. Д. Кунєв,

доктор юридичних наук, професор

ORCID ID: <https://orcid.org/0000-0002-5952-2052>

ПРАВОВА ОРГАНІЗАЦІЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ: СИСТЕМОДІЯЛЬНІСНИЙ ПІДХІД

Державний університет «Київський авіаційний інститут»
проспект Любомира Гузара, 1, 03058, Київ, Україна
E-mail: kunev@ukr.net

Мета статті полягає у дослідженні теоретичних основ та законодавства України у сфері інформаційної безпеки та напрямків їх розвитку. **Методи дослідження:** системодіяльнісний підхід до створення теоретичної картини об'єкта та застосування методологічної схеми знання про об'єкт та про знання, що його описують; порівняльно-правового та доктринального пізнання законодавства, а також метод узагальнення та моделювання нових теоретичних знань інформаційного права. **Результати:** визначені проблеми подальшого розвитку інформаційної безпеки та запропоновані теоретичні підходи для їх розв'язання. Для системного вирішення сукупності виявлених проблем необхідним є визначення складових інформаційної системи, її підсистем. Наведені приклади підсистем адміністративної діяльності та її інформаційних складових. Правильне визначення меж системи сприятиме вірному визначенню напрямків забезпечення інформаційної безпеки та її правового забезпечення. Правова організація інформаційної безпеки означає взаємозалежний процес взаємодії інформаційної та правової підсистем діяльності. Предметом правової організації інформаційної безпеки будемо вважати правові організованості інформаційної діяльності та інформаційних складових адміністративної діяльності публічної влади в нормах законодавства. **Обговорення:** визначені критерії, які найбільше впливають на правову організацію інформаційної безпеки та моделі норм інформаційного права, необхідні для набуття якостей інформаційного законодавства України.

Ключові слова: інформаційна безпека; забезпечення інформаційної безпеки; інформаційне право; інформаційне законодавство; правова організація інформаційної діяльності; інформаційна діяльність.

Постановка проблеми та її актуальність. Подолання проблем та недоліків у сфері правового забезпечення інформаційної безпеки вимагає від правової науки: створення сучасної теоретико-методологічної основи пізнання державно-правових явищ; побудови наукових моделей діяльності із забезпечення інформаційної безпеки та їх реалізації в моделях правової діяльності, зокрема у реалізації правотворчої, правозастосовчої і правозабезпечуючої діяльності. Розв'язання цих проблем забезпечить більшу

стійкість інформаційної системи і державної влади в Україні.

Проблематика ефективної організації безпеки інформаційної системи та діяльності привернула до себе пильну увагу в останнє десятиріччя, особливо під час гібридної війни.

Існуючі моделі організаційних та правових норм інформаційної діяльності мають систему суперечностей за різними взаємозалежними аспектами: соціальними, правовими, організаційними тощо. Основна причина проблем практичного плану – відсутність системної моделі норм

інформаційної діяльності на організаційно-діяльнісному та законодавчому рівнях. Необхідність системного усунення комплексу причин і проблем практичного плану переходить у площину розв'язання проблем теоретичного та методологічного характеру.

Таким чином, прогалини у розробках основ теорії та методології дослідження правових та організаційних аспектів забезпечення інформаційної безпеки потребують комплексного дослідження і вироблення нових підходів до формування основ правової моделі систем інформаційної діяльності та діяльностей з інформаційними складовими.

Аналіз досліджень і публікацій з проблеми. На нашу думку, до основних інформаційно-правових понять можна зарахувати такі: «інформаційна діяльність», «інформаційна безпека», «інформаційне законодавство», «інформаційно-правова діяльність», «правова організація інформаційної безпеки», які визначають логічний і смисловий взаємозв'язок та логіку формування й зміни інших пов'язаних з ними понять. Основним результатом діяльності з упорядкування виступають норми, які регулюють діяльність як у системі, так і поза нею.

Питанням розкриття сутності та змісту вищезазначених понять присвячували свої праці багато науковців, зокрема, І.В. Арістова [1], К.І. Беляков [2], В.М. Брижко, О.Г. Дубовський [3], Р.А. Калюжний [4], Л.П. Коваленко, І.Ф. Корж, Б.А. Кормич [5], Г.М. Красноступ, А.І. Марущак, О.Г. Марценюк, О.А. Ніщименко, О.М. Селезньова, В.С. Цимбалюк тощо.

Утім існуючі погляди та моделі організаційних й правових норм інформаційного права мають систему суперечностей та теоретичних прогалин за різними взаємозалежними аспектами й потребують подальшого дослідження й розвитку цілісності сприйняття та організації основних інформаційно-правових понять.

Незважаючи на достатню розробленість теми, деякі питання, зокрема щодо змісту правової організації діяльнісної складової інформаційної безпеки, залишилися поза увагою вчених, що зумовлює актуальність обраної теми.

Ця стаття є продовженням оприлюдненої статті «Правове забезпечення інформаційної

безпеки як предмет правового дослідження», де продовжується деталізація підходів до правової організації діяльнісної складової інформаційної безпеки.

Мета статті – дослідити теоретичні основи та законодавство України у сфері інформаційної безпеки та напрямки їх розвитку.

Виклад основного матеріалу дослідження. Достатньо сталим є визначення «правова організація». Правова організація означає набуття певної якості за допомогою та у сфері дії права. Організація як універсальна ознака діяльності має процесуальну й структурну складову» [6].

Тоді визначили, що «об'єктом вивчення, проєкції, оперування або реальним об'єктом правознавства суспільну діяльність (практику); ідеальним об'єктом – модель або теоретичну модель реального об'єкта, знання про діяльність, пов'язану з правом (теорію)» [7].

«Через складність державно-правових систем і явищ рівні абстракції при побудові їх моделей мають бути досить високими (хоча їх обирає сам дослідник, залежно від мети та критеріїв оцінки результатів) і методологія має відповідати останнім досягненням науки. Відповідно, вибір методології – це основоположне питання для адекватного та повного визначення об'єкта правознавства» [7].

Один з основоположних моментів системодіяльнісної методології (СД-методології) – уявлення діяльності як системи.

Під час з'ясування змісту інформаційної безпеки важливо з'ясувати яку систему мають на увазі: 1) система інформаційної діяльності; 2) система із технічної обробки інформації; 3) сама інформація її властивості (цілісність, охоронюваність, вчасність надходження тощо) 4) усі соціальні системи, у яких може бути завдана шкода інформаційним зв'язкам між суб'єктами.

Поняття «забезпечення безпеки інформаційної системи» – це діяльність, яка повинна забезпечуватися в межах певної підсистеми обігу інформації.

Правова організація інформаційної діяльності – це система взаємодії двох діяльностей: правової діяльності та інформаційної.

Така діяльність може мати назву «Інформаційно-правова діяльність» – це організована

за стандартами інформаційного законодавства кооперована діяльність суб'єктів правової взаємодії державних органів та осіб, яких це стосується, що виконують власні зобов'язання (умови та формальності), спрямовані на розгляд і реалізацію державних та приватних інтересів, пов'язаних із обігом інформації та існуванням інформаційних об'єктів [8].

Визначення системи і її підсистем є ознакою якості її опису й визначенню системи інформаційної безпеки.

Основними складовими системи інформаційної безпеки є те, що інформація є складовою багатьох підсистем:

1) як елементи багатьох різновидів діяльностей, інформації в якості: матеріалу, продукту, засобу, інструменту.

2) як складові елементи безпосередньо інформаційної діяльності, пов'язаної з «обігом інформації» та із «створенням, функціонуванням та розпорядженням певними інформаційними об'єктами».

3) як інформаційного зв'язку між елементами будь-якої соціально-діяльничої системи (СДС);

4) як складові елементи управлінської діяльності.

5) як складові елементи правової діяльності: правотворчої, правозастосовної.

«Напрямки інформаційно-адміністративної діяльності узагальнили наступним чином:

- напрямки приватної інформаційної діяльності, які підлягають адміністративно-правовому регулюванню;

- напрямки інформаційної діяльності публічної адміністрації з реалізації основних функцій держави;

- юрисдикційна діяльність органів публічної адміністрації з питань правопорушень у сфері обігу інформації» [8].

Якщо розглядати велику соціально-діяльничу систему (СДС), то можна згадати систему принципів, котрі найбільше впливають на безпеку соціальної системи, зокрема держави. В системі загальних принципів значну частину займають принципи, які стосуються інформації та інформаційних зав'язків в СДС.

«1. Найуразливішою для втрати стійкості є структура системи, тобто відносини між еле-

ментами, їх взаємозв'язки, а не закони функціонування цих одиниць, які також визначають динаміку системи, але меншою мірою її існування.

2. У сфері державно-правової організації соціальних систем істотне значення має нормативно-правова база їх функціонування. Остання може розглядатися як один з найважливіших елементів будь-якої системи (а правове регулювання діяльності і відносин є визначальним для діяльності державних органів), отже, істотний чином впливати на рівень оптимальності функціонування системи.

3. Структура неоднаково чутлива до руйнування. Найбільшої шкоди завдають порушення у верхніх рівнях ієрархії, а саме в центрах обробки узагальненої інформації, вироблення і прийняття адміністративних рішень.

4. Руйнуванню структури еквівалентні розрив інформаційних каналів або їх перевантаження, оскільки це призводить до ускладнення комунікації між елементами системи та зовнішнім середовищем.

5. На якість роботи системи сильно впливає достовірність інформації, що надходить. Цілеспрямоване перекручення останньої, дезінформація може привести систему до стійкої дезорганізації. Важливу роль відіграє й рівень розвитку інформаційного права в державі» [8].

Приклади інформаційного забезпечення основної діяльності публічної адміністрації є ілюстрація наведена в монографії «Діяльність митної служби України : проблеми правової організації».

«Як ілюстрацію процесу прийняття рішення щодо пропуску об'єкта переміщення через митний кордон можна подати змістовно інформаційну складову митної діяльності у вигляді "кентавр" об'єкта (рис. 4.1), де перша зона – площа потенційних знань, друга – площа достатніх для виконання митних формальностей знань, третя – площа існуючих у митній службі формалізованих знань у вигляді інформації. Тоді концепцією побудови унормованої моделі діяльності, яка забезпечить легальне переміщення необхідних та безпечних товарів, є максимальне охоплення площиною існуючої інформації сфери достатньої.

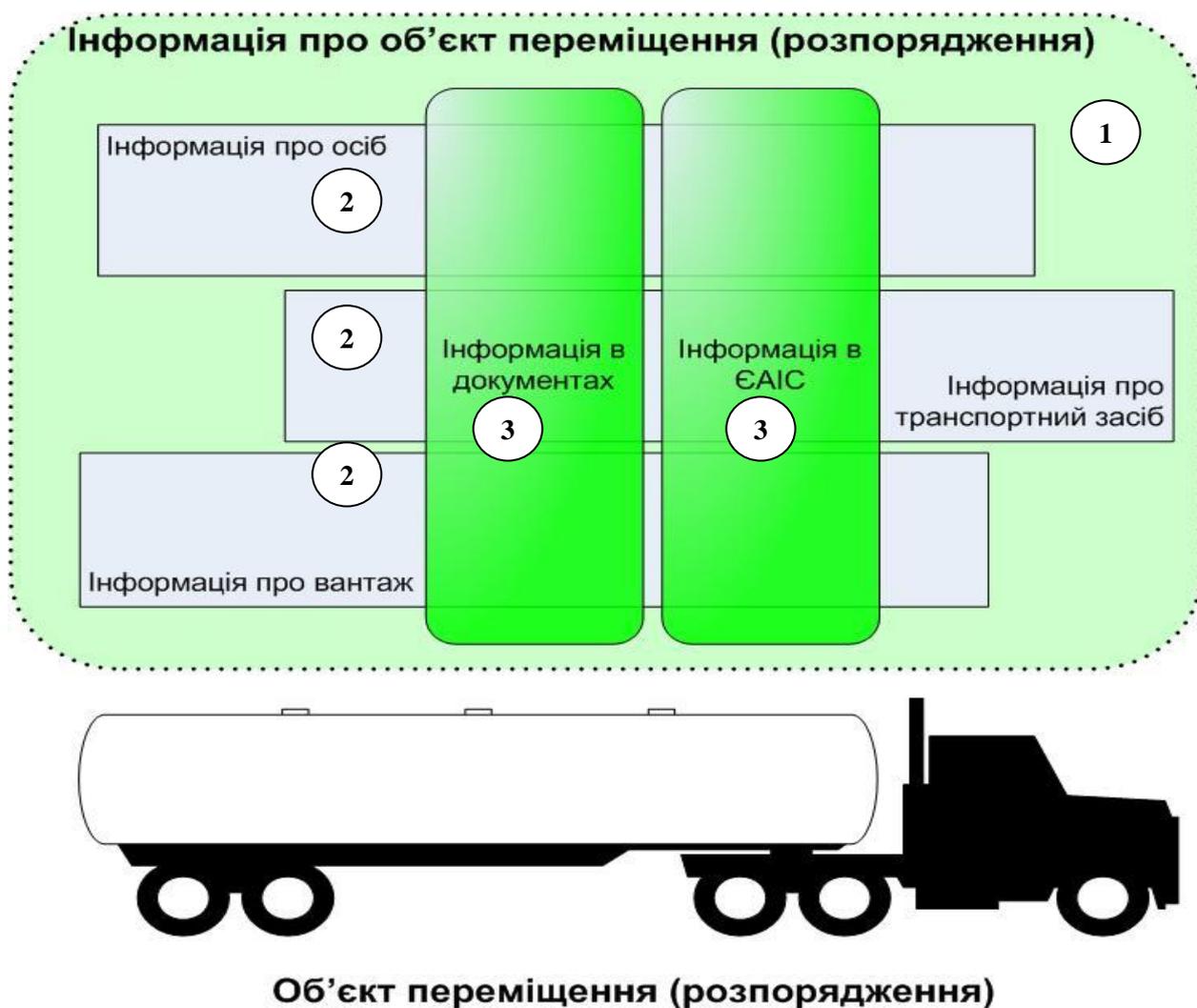


Рис. 4.1. Схема моделі змістовної складової митного контролю та митного оформлення

Запропонований методологічний підхід (системомиследяльній) до побудови моделі митного контролю та митного оформлення є універсальним для розроблення і визначення підпроцесів загального процесу, можливості побудови процесуально-правової моделі та закріплення її у законодавстві. Вищевикладені методологічні підходи – засіб створення моделей митної діяльності, де визначено всі елементи акту діяльності, з наступним створенням систем кооперації діяльності суб'єктів (митників і клієнтів), які в сукупності становитимуть механізм митної діяльності з подальшим проектуванням його на структуру й організованість митної служби України.

Системне зображення діяльності дає можливість застосовувати універсальні методики ліквідації розривів у діяльності або успішного моделювання нових видів діяльності, тобто складає основу діяльності з розвитку адміністративно-правової організації митної служби» [9, с. 153–154].

Якщо мова йде про безпеку інформаційної складової СДС, то стійкість великої СДС (її безпека) визначається стійкістю кожної з підсистем та стійкістю її найслабшої ланки.

Це визначає багатовимірність та взаємозалежність наукових досліджень інформаційного забезпечення багатьох підсистем, зокрема, інформаційних складових адміністративної діяльності публічної влади.

Сфери правового регулювання інформаційної діяльності обіймає індивідуально-правові й інституціональні шари.

Індивідуально-правовий шар

Основні положення індивідуально-правового шару в тому, що інформаційна правова позиція громадянина, забезпечується концепціями нормативного обмеження дій адміністрації і системного захисту даних.

Інституційні шари

Інституційні шари полягають у об'єктивно-правовому забезпеченні зростання інформаційних потреб і зростання важливості інформаційної діяльності під час комунікаційних стосунків між громадянином та публічною адміністрацією, а також між самими адміністративними одиницями [8].

Якщо мова про правову організацію інформаційної безпеки та з огляду на напрямки інформаційної діяльності предметом будемо вважати правові організованості інформаційної діяльності в нормах законодавства із забезпечення інформаційної безпеки.

Правова організація інформаційної безпеки означає взаємозалежний процес взаємодії інформаційної та правової підсистем діяльності.

Аналіз стану розвитку інформаційного суспільства повністю відображає і стан розвитку інформаційної безпеки взагалі.

«Поглиблення міжнародного співробітництва для консолідованого протистояння гібридній агресії РФ є вкрай важливим, але ключові причини його успішності знаходяться всередині держави. А тому й зусилля з розбудови державних можливостей України протистояти гібридним загрозам стосуються переважно внутрішнього виміру» [10].

Головною небезпекою гібридної війни РФ на усіх етапах є використання громадськості у процесі досягнення поставлених агресором цілей через інформаційно-пропагандистський вплив на їхню свідомість, стимулювання недовіри до державних і правоохоронних органів, нав'язування переконання, що життя у державі-агресорі краще, у порівнянні з державою-жертвою, та пониження рівня безпеки суспільства в цілому.

Як відзначає Національний інститут стратегічних досліджень у своїй монографії «Світова гібридна війна: Український фронт», вперше Путін випробував контрольований медіаресурс як інформаційну зброю у поєднанні з військовими діями під час агресії Росії проти Грузії у 2008 році. Відпрацьовані інформаційно-пропагандистські механізми потім були використані в Україні: швидке та масштабне наповнення зони бойових дій контрольованими російськими журналістами; спроба монополізувати контроль за наданням контенту із зони бойових дій; продукування фейків; направлення до зони бойових дій російських діячів культури; використання найманих іноземних журналістів. Кремль зробив висновки з невдач інформаційного висвітлення війни проти Грузії та більш уважно поставився до можливостей і потреб інформаційного інструменту. Бюджет Russia Today був збільшений з 30 до 100 млн. дол. США, а в останні роки він сягнув 250 млн. дол. США. З метою поширення інформаційно-пропагандистського продукту на закордонну аудиторію, на базі «РИА Новости» і радіокомпанії «Голос России» була сформована «МИА Россия сегодня», з бюджетом 99,7 млн. дол. США у 2016 році, у складі якої був створений новий інформаційний інструмент Sputnik, що поширює інформацію більш як 30-ма мовами у десятках країн, переважно Європи, досягнувши рівня місцевого н'юс-мейкера [10].

Для протистояння і протидії таким серйозним викликам необхідні державні програми і їх бюджетне забезпечення.

На тлі російської агресії перед Україною постали декілька взаємопов'язаних задач у контексті інформаційних викликів. Потребувала негайного вирішення проблема невідповідності національного законодавства новим викликам інформаційної війни. Незважаючи на велику кількість нормативних актів у інформаційній сфері, не вдалося подолати причини і наслідки інформаційної агресії, яка більшістю (51,4%) українських експертів названа головним фактором уразливості українського суспільства [10].

Важливим при цьому є декілька факторів за важливістю впливу на стан безпеки:

- 1) економічна база;

2) наявність проблем розвитку інформаційного суспільства в цілому;

3) політична воля для розв'язання проблем;

4) усвідомлення та знання забезпечення розв'язання проблем;

5) правове забезпечення розв'язання проблем;

6) організаційно-кадрове забезпечення реалізації правових норм.

Якість правового забезпечення, в першу чергу, залежить від чотирьох перших критеріїв, оскільки якість правового забезпечення інформаційної безпеки (якості інформаційного законодавства) є продуктом інформаційної політики держави (діяльності із формування інформаційної політики).

Загострення інформаційної безпеки і напрямків її реалізації відбулося з 2014 року. У 2015 році розпочалася робота над концептуальними документами в сфері інформаційної безпеки. У рамках роботи Експертної ради при МПП України було розроблено Доктрину інформаційної безпеки України та Концепцію інформаційної безпеки України. Хоча цей процес носив відкритий та інклюзивний характер, не всі напрацювання вдалося втілити в життя. Наприклад, Концепція інформаційної безпеки так і залишилася на стадії проекту. Схвалена в лютому 2017 року Доктрина інформаційної безпеки визначила пріоритети та національні інтереси України в інформаційній сфері, загрози для їх реалізації. Однак, вона не стала основою для розробки цілісної нормативної системи інформаційної безпеки держави.

Під час гібридної війни, потрібно приділити значну увагу розвитку інформаційної безпеки, в першу чергу, визначивши та уніфікувавши загальні положення інформаційної безпеки держави та низки правових норм, які охоплюють надважливі її складові за означеними вище напрямками.

Важливим для розвитку інформаційної безпеки є приватна ініціатива суб'єктів громадянського суспільства України та правове регулювання невтручання держави в сферу дії приватного права в інформаційній сфері.

Системний підхід може бути реалізований в межах одного нормативно-правового акта, зок-

рема, в «Концепції інформаційної безпеки», або у низці нормативно-правових актів.

Висновки. Предметом правової організації інформаційної безпеки будемо вважати правові організованості інформаційної діяльності та інформаційних складових адміністративної діяльності публічної влади в нормах законодавства.

Правова організація інформаційної безпеки означає взаємозалежний процес взаємодії інформаційної та правої підсистем діяльностей.

Аналіз стану розвитку інформаційного суспільства повністю відображає і стан розвитку інформаційної безпеки взагалі. Під час гібридної війни, потрібно приділити значну увагу розвитку інформаційної безпеки.

Література

1. Арістова І.В., Сулацький Д.В. Інформаційна безпека людини як споживача телекомунікаційних послуг: монографія. Київ: Ред. журн. «Право України». Харків: Право, 2013. 184 с.

2. Беляков К.І. Організаційно-правове та наукове забезпечення інформатизації в Україні: проблеми теорії та практики: автореф. дис... д-ра юрид. наук: 12.00.07. Київ: Ін-т держави і права ім. В.М. Корецького НАН України. 2009. 38 с.

3. Дубовський О.Г. Інформаційна безпека України в умовах глобалізації світового інформаційного простору: дис. ... д-ра філософії: 291 Міжнародні відносини, суспільні комунікації та регіональні студії. Київ, 2025. 207 с.

4. Калюжний Р.А. Теоретико-методологічні підходи до розуміння інформаційної безпеки людини. *Наукові праці Національного авіаційного університету. Серія: Юридичний вісник «Повітряне і космічне право»*. Київ: НАУ, 2018. № 2(47). С. 197-198. DOI: <https://doi.org/10.18372/2307-9061.47.12962>

5. Правове регулювання інформаційної діяльності: навч.-метод. посіб. / Б.А. Кормич, О.П. Федотов, Т.В. Аверочкіна. Одеса: ОНЮА, 2018. 150 с.

6. Кунев Ю.Д. Правова організація діяльності митної служби України: теоретичні та методологічні основи: дис. ... д-ра юрид. наук: спец. 12.00.07. Харків: ХНУВС, 2010. 442 с.

7. Кунев Ю.Д. Об'єкт правознавства: системодіальнісний підхід. *Право України*. 2008. № 3. С. 35–38.

8. Кунев Ю.Д. Правове забезпечення інформаційної безпеки як предмет правового дослідження. *Наукові праці Національного авіаційного університету. Серія: Юридичний вісник «Повітряне і космічне право»*. Київ: НАУ, 2021. № 1(58). С. 95–102. DOI: <https://doi.org/10.18372/2307-9061.58.15314>

9. Кунев Ю.Д. Діяльність митної служби України: проблеми правової організації. Дніпропетровськ: Академія митної служби України, 2009. 244 с.

10. Гібридні загрози Україні і суспільна безпека. Досвід ЄС і східного партнерства. Аналітичний документ. Київ. 2018. 106 с.

References

1. Aristova I.V., Sulatsky D.V. Informatsiyna bezpeka lyudyny yak spozhyvacha telekomunikatsiynikh posluh: monohrafiya. Kyiv: Red. zhurn. «Pravo Ukrayiny». Xarkiv: Pravo, 2013. 184 s.

2. Byelyakov K.I. Orhanizatsiyno-pravove ta naukove zabezpechennya informatyzatsiyi v Ukrayini: problemy teorii ta praktyky: avtoref. dys... d-ra yuryd. nauk: 12.00.07. Kyiv: In-t derzhavy i prava im. V.M. Koretskoho NAN Ukrayiny. 2009. 38 s.

3. Dubovskyy O.H. Informatsiyna bezpeka Ukrayiny v umovakh hlobalizatsiyi svitovoho informatsiynoho prostoru: dys. ... d-ra filosofiyi: 291 Mizhnarodni vidnosyny, suspilni komunikatsiyi ta rehionalni studiyi. Kyiv, 2025. 207 s.

4. Kalyuzhnyy R.A. Teoretyko-metodolohichni pidkhody do rozuminnya informatsiynoyi bezpeky lyudyny. *Naukovi pratsi Natsionalnoho aviatsiynoho universytetu. Seriya: Yurydychnyy visnyk «Povitryane i kosmichne pravo»*. Kyiv: NAU, 2018. № 2(47). S. 197-198. DOI: <https://doi.org/10.18372/2307-9061.47.12962>

5. Pravove rehulyuvannya informatsiynoyi diyalnosti: navch.-metod. posib. / B.A. Kormych, O.P. Fedotov, T.V. Averochkina. Odesa: ONYUA, 2018. 150 s.

6. Kunyev Yu.D. Pravova orhanizatsiya diyalnosti mytnoyi sluzhby Ukrayiny: teoretychni ta metodolohichni osnovy: dys. ... d-ra yuryd. nauk: spets. 12.00.07. Kharkiv: KHNUVS, 2010. 442 с.

7. Kunyev Yu.D. Obyekt pravознавства: systemodiyalnisnyy pidkhid. *Pravo Ukrayiny*. 2008. № 3. S. 35–38.

8. Kunyev Yu.D. Pravove zabezpechennya informatsiynoyi bezpeky yak predmet pravovoho doslidzhennya. *Naukovi pratsi Natsionalnoho aviatsiynoho universytetu. Seriya: Yurydychnyy visnyk «Povitryane i kosmichne pravo»*. Kyiv: NAU, 2021. № 1(58). S. 95–102. DOI: <https://doi.org/10.18372/2307-9061.58.15314>

9. Kunyev Yu.D. Diyalnist mytnoyi sluzhby Ukrayiny: problemy pravovoyi orhanizatsiyi. Dnipropetrovsk: Akademiya mytnoyi sluzhby Ukrayiny, 2009. 244 s.

10. Hibrydni zahrozy Ukrayini i suspilna bezpeka. Dosvid YES i skhidnoho partnerstva. Analitichnyy dokument. Kyiv. 2018. 106 s.

LEGAL ORGANIZATION OF INFORMATION SECURITY: A SYSTEMATIC APPROACH

State University «Kyiv Aviation Institute»
Lyubomyr Huzar Avenue, 1, 03058, Kyiv, Ukraine
E-mail: kunev@ukr.net

*The purpose of the article is to study the theoretical foundations and legislation of Ukraine in the field of information security and the directions of their development. **Research methods:** a systemic approach to creating a theoretical picture of the object and applying a methodological scheme of knowledge about the object and about the knowledge that describes it; comparative legal and doctrinal knowledge of legislation, as well as a method of generalizing and modeling new theoretical knowledge of information law. **Results:** problems of further development of information security are identified and theoretical approaches for their solution are proposed. For a systematic solution to the set of identified problems, it is necessary to determine the components of the information system, its subsystems. Examples of subsystems of administrative activity and its information components are given. Correct definition of the boundaries of the system will contribute to the correct definition of the directions of ensuring information security and its legal support. The legal organization of information security means an interdependent process of interaction between the information and legal subsystems of activities. The subject of the legal organization of information security will be the legal organization of information activities and information components of the administrative activities of public authorities in the norms of legislation. **Discussion:** the criteria that most influence the legal organization of information security and the models of the norms of information law necessary for acquiring the qualities of information legislation of Ukraine are determined.*

***Key words:** information security; ensuring information security; information law; information legislation; legal organization of information activities; information activities.*

Стаття надійшла до редакції 16.12.2025