Journal of Scientific Papers "Social development & Security"
home page: https://paperssds.eu/index.php/JSPSDS/

Dzhalladova I., Batechko N., Kolomiyets-Ludwig E. (2018) Systemnyy pidkhid do analizu normatyvno-pravovoho zabezpechennya informatsiynoyi bezpeky [Systemic approach to the analysis of the Legal framework of information security]. *Social development & Security*. 5(7), 3–20. Retrieved from https://paperssds.eu/index.php/JSPSDS/article/view/61/52
DOI: http://doi.org/10.5281/zenodo.1450873

СИСТЕМНИЙ ПІДХІД ДО АНАЛІЗУ НОРМАТИВНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Ірада Джалладова *, Ніна Батечко **, Євгенія Коломієць-Людвіг ***

** Київський національний економічний університет імені Вадима Гетьмана,*
проспект Перемоги, 54/1, Київ, 03057, Україна,
e-mail: idzhalladova@gmail.com
д.фіз.-мат.н., професор,
завідувач кафедри комп'ютерної математики та інформаційної безпеки

*** Національний університет біоресурсів і природокористування України,*
вул. Героїв оборони, 12, Київ, 03041, Україна,
e-mail: batechko_n_@ukr.net
д.пед.н., доцент,
завідувач кафедри вищої та прикладної математики

**** Київський національний економічний університет імені Вадима Гетьмана,*
проспект Перемоги, 54/1, Київ, 03057, Україна,
e-mail: evheniakl@kneu.edu.ua
к.ю.н.,
доцент кафедри правового регулювання економіки

OPEN ACCESS

Article history:
Received: September, 2018
1st Revision: September, 2018 Accepted: October, 2018
УДК : 34[361.746:007]

DOI: http://doi.org/10.5281/zenodo.1450873

Анотація: *У статті обґрунтовано методологічні засади застосування системного підходу до аналізу нормативно-правового забезпечення інформаційної безпеки. Вказано на необхідність створення єдиного термінологічного поля, яке б стало основою для формування теоретико-методологічного підґрунтя інформаційної безпеки та її нормативно-правового супроводу. Доведено динамічний характер інформаційних загроз та відставання законодавчої сфери від розвитку інформаційного суспільства в Україні та світі. Запропоновано інтерпретацію структури нормативно-правового забезпечення інформаційної безпеки у вигляді багаторівневої моделі, компоненти якої знаходяться у певній ієрархії та взаємодіють між собою. Систематизацію об'єктів дослідження здійснено з урахуванням таких властивостей систем, як цілісність, структурність, ієрархічність, а також і з точки зору динамічної системи зі зворотними зв'язками та наявністю нелінійних ефектів. Доведено, що багаторівневий підхід дозволяє впорядкувати нормативно-правове*

регулювання відносин у сфері законодавчого забезпечення інформаційної безпеки між суспільством, його членами та державою, між фізичними та юридичними особами з урахуванням міжнародних тенденцій.

Ключові слова: *інформаційна безпека, нормативно-правове забезпечення, системний підхід.*

Джалладова І. А., Батечко Н. Г., Коломієць-Людвіг Є. П. Системний підхід до аналізу нормативно-правового забезпечення інформаційної безпеки. *Social development & Security.* 2018. Вип. 5 (7). С. 3–20.
URL: https://paperssds.eu/index.php/JSPSDS/article/view/61/52
DOI: http://doi.org/10.5281/zenodo.1450873

1. Постановка проблеми

Кіберпростір став ареною багаточисельних конфліктів, що різняться формами і методами, інтенсивністю у часовому вимірі та ступенем загроз, які вони спричиняють.

На сьогодні актуальним є не лише подальший розвиток практичної діяльності суб'єктів світового політичного процесу, організацій, груп (organized attackers), окремих громадян у кіберпросторі, а й правове забезпечення такої діяльності, що полягає у розробці та прийнятті різних за своєю юридичною силою нормативно-правових документів.

Зауважимо, що розробка та прийняття на національному рівні багаточисельних стратегій та інших нормативно-правових актів не повною мірою відображають загрози та небезпеки військового характеру, що виникають під час діяльності держав у кіберпросторі. У зв'язку з цим особливої актуальності набуває отримання теоретичних та практичних навичок з основ використання сучасних методів правового захисту державної, службової, комерційної, професійної таємниці та персональних даних у комп'ютерних системах; ліцензування та сертифікації у галузі захисту інформації, формування практичних навичок та вмінь щодо забезпечення правового захисту інформації.

Повсюдне впровадження сучасних інформаційних та телекомунікаційних технологій у процеси виробництва та управління потребує відповідної правової підтримки. Прийняття важливих рішень з урахуванням використання інформаційних технологій вимагає їх обов'язкового закріплення у відповідних локальних нормативних актах (наказах, розпорядженнях). Також, принципово важливим є те, що розвиток інформаційних технологій значно випереджає розвиток законодавчої сфери, що, у свою чергу, заважає правовому регулюванню розвитку інформаційного простору. Так, наприклад, Д. В. Сулацький зауважує, що «діюче законодавство «у низці аспектів» відстає від динаміки змін, що виникають у процесі розвитку інформаційного суспільства в Україні та світі». [40, С. 18].

2. Аналіз останніх досліджень та публікацій

Зважаючи на актуальність, досліджувана тематика все частіше стає полем наукових пошуків багатьох науковців як в Україні, так і за її межами. Зокрема, різні аспекти правового регулювання протидій кіберзагроз досліджували П. Д. Біленчук, В. Л. Бурячок, В. М. Бутузов, В. Д. Гавловський, В. А. Голубев, Ю. М. Супрунов, А. Л. Татузов, В. М. Фурашев, В. П. Шеломенцев [4; 5; 6; 8; 41; 3; 43; 44] та інші. Водночас, кожен із дослідників вивчав певну локальну проблему, тоді як автори акцентують увагу на інтегрованому підході до

вивчення нормативного-правового забезпечення інформаційної безпеки та його систематизації.

Перш за все, варто вказати на розбіжності у поглядах вчених, пов'язані з предметом дослідження – інформаційною безпекою та її складовою – кібербезпекою. Так, зокрема, В.М. Фурашев вважає, що «інформаційна безпека – це стан захищеності життєво важливих інтересів людини, суспільства і держави, за якого запобігається завдання шкоди через: негативний інформаційний вплив за допомогою, в першу чергу, несанкціонованого створення, розповсюдження, використання свідомо спрямованої із визначеною метою неповної, невчасної, невірогідної та упередженої інформації; негативні наслідки застосування інформаційних технологій; несанкціоноване порушення режиму доступу до інформації з подальшим її розповсюдженням та використанням». [43, С. 60]

Інші вчені (В. А. Ліпкан, О. С. Ліпкан, А. А. Яковенко) вважають інформаційну безпеку складовою поняття національної безпеки, що характеризує певний вид соціальної діяльності, основний зміст якої полягає у створенні сприятливих (необхідних і достатніх) умов для розвитку й реалізації національних інтересів. [16, С. 146–147]

Вже, певною мірою, тенденційними стали наміри наукових кіл створити єдине термінологічне поле, яке б стало платформою для формування теоретико-методологічної основи забезпечення інформаційної безпеки та її нормативно-правового супроводу. Розгляд наукових джерел засвідчив також диверсифікацію у поглядах науковців щодо змісту поняття інформаційної загрози та критеріїв її класифікації.

Аналітик Лондонського Королівського інституту закордонних справ (Chatam House) П. Корниш у своїх працях наводить наступну класифікацію інформаційних загроз:

- діяльність хакерів – одинаків;
- організована злочинність, що діє у глобальних інтернет-мережах;
- ідеологічний та політичний екстремізм (кібертероризм);
- інформаційна агресія, що проводиться певною державою (кібервійна) [1].

На думку науковця, лише перші два різновиди загроз із вищенаведеної класифікації мають практичне втілення у сучасній світовій політиці. Дослідник стверджує, що кібертероризм та кібервійна між державами є насьогодні лише уявними загрозами, а не реальністю, і можуть стати такою за десятиліття.

Автори статті вважають зазначену позицію не достатньо вірною, оскільки насьогодні кібертероризм, як один із способів протиборства між державними, громадськими та іншими суб'єктами, широко представлений на міжнародній арені, а кібервійна, як один із видів та типів сучасних війн, характеризується стрімким розвитком наукових розробок та зростаючою кількістю епізодів їх практичного застосування.

3. Постановка завдання

Важливо підкреслити, що інформаційні загрози постійно еволюціонують, тоді як нормативно-правова сфера зазвичай розглядається не у динаміці, а у статиці, що вочевидь зашкоджує розвитку інформаційної та кібербезпеки. Переконливою у зв'язку з цим є позиція С.А. Галушка, який вважає, що раптова актуалізація будь-якої нової загрози не завжди сприяє своєчасному адекватному реагуванню на неї. Ось чому дослідник вважає доцільним не лише визначати перелік загроз, а й законодавчо виокремити їх можливі рівні та встановлювати (як у розвинутих країнах) систему загроз і відповідні ступені реагування на них з боку держави. [7, С. 18]

Зважаючи на розбіжності у поглядах науковців на основні складові поняття «інформаційна безпека», відсутність інтегрованого підходу до чинного нормативно-правового забезпечення інформаційної безпеки в Україні, а також його систематизації на

різних рівнях імплементації, була сформульована **мета статті:** систематизація загальних теоретичних знань, здобутих у процесі вивчення нормативно-правових документів та інформаційних технологій, поглиблене вивчення правового регулювання інформаційних процесів та удосконалення навичок розробки, редагування та оцінки відповідних правових документів. **Основне завдання** – аналіз та систематизація сучасних нормативно-правових актів, що регулюють забезпечення інформаційної безпеки у кіберпросторі України та країн ЄС, а також розробка рекомендацій з впровадження на різних рівнях ефективних правових механізмів попередження кіберзагроз та захисту від них.

4. Виклад основного матеріалу

Зазначимо, що складність та багатогранність функціональних сфер, де відбувається розвиток параметрів інформаційної безпеки, зокрема – у правовій, а також наявність системних взаємозв'язків між ними, обумовлює необхідність застосування у науковому пошуку системного підходу.

Так, вибудовуючи структуру нормативно-правового забезпечення інформаційної безпеки з використанням для цього багаторівневого підходу, пропонуємо розглянути її у певній ієрархії по відповідним рівням, взаємопов'язаних між собою. Багаторівневий підхід у такому випадку буде виступати своєрідною «моделлю взаємодії, де набір інтелектуальних систем та їх компонентів взаємодіють та обмінюються знаннями» [13, С. 4]

Концепція рівнів, як пояснюють А.В. Щербакова та Г.С. Федорова [45, С. 97], це одна з моделей, що використовуються для розподілу складних систем на простіші складові. За такого підходу виділяють верхній рівень, який описує систему у цілому, під ним розміщується нижчий рівень, який описує категорії з використанням поняття вищого рівня і т.д. Таким чином, кожен нижчий рівень забезпечує функціональність для наступного вищого рівня, який, у свою чергу, забезпечує методи для рівня, що над ним. Однак, найскладнішим у використанні рівнів, на думку вчених, є визначення змісту та меж відповідальності кожного рівня.

У нашому випадку, для подолання цієї складності у процесі систематизації нормативно-правового забезпечення інформаційної безпеки доречно розглядати його як традиційну систему, що має такі властивості: цілісність, комплекс взаємодіючих елементів, структурність, ієрархічність, взаємозалежність системи та оточуючого середовища), так і динамічну систему зі зворотними зв'язками та наявністю нелінійних ефектів. Такий підхід дозволяє впорядкувати ієрархію складових системи – рівнів, а також збудувати своєрідну ієрархію взаємозв'язків всередині самої системи.

Вибудовуючи механізми взаємозв'язків між рівнями у системі, автори тим самим визначають її структуру та механізми її функціонування. За визначенням А.І. Ільяша, структуру складають суб'єкти та об'єкти, які є її елементами, а механізм функціонування – відповідний набір правил (процедур, функцій), які регламентують дії елементів системи у процесі її функціонування [10, С. 28]

Наголосимо на наявності окремих особливих властивостей системи в інформаційній безпеці, які впливають на загальні властивості системи її нормативно-правового забезпечення. Це – стабільність (тривале збереження певного стабільного стану або оптимального рівня безпеки); стійкість (здатність системи належним чином функціонувати та чинити опір дестабілізуючим факторам); відносна самостійність (здатність системи функціонувати без зовнішньої підтримки); цілісність (сприйняття системного утворення як єдиного цілісного об'єкту).

Авторське дослідження нормативно-правового забезпечення, як багаторівневої системи, буде враховувати послідовне вертикальне розміщення підсистем, що утворюють

дану систему (вертикальну декомпозицію), а також пріоритет дій або право втручання підсистем верхнього рівня; залежності дій підсистем верхнього рівня від фактичного виконання своїх функцій нижніми рівнями.

Зауважимо, що ієрархічне упорядкування системи часто пов'язують (А. В. Щербакова, Г. С. Федорова) з процесом зміни її структури перш за все з метою підвищення ефективності її функціонування [45].

Для глибшого вивчення проблеми зазначимо чинні нормативно-правові акти України, що регулюють сферу інформаційної та кібербезпеки: Конституція України [14], Закони України «Про основні засади забезпечення кібербезпеки України» [33], «Про національну безпеку України» [32], «Про інформацію» [30], «Про захист інформації у телекомунікаційних системах» [28], рішення Кабінету Міністрів України «Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018–2020 рр. та затвердження плану заходів щодо її реалізації» [38] та ін. Важливо згадати також Укази Президента України, що регулюють зазначене питання, положення Кримінального кодексу [15] та Кодексу України про адміністративні правопорушення [12], окремі постанови та рішення Кабінету Міністрів України, рішення РНБО України. Так, зокрема, стратегічне значення для вирішення поставленої задачі має Указ Президента України від 25 лютого 2017 р. «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 р. «Про Доктрину інформаційної безпеки України» [35].

До речі, практичним кроком у реалізації нормативно-правового регулювання інформаційної безпеки було створення ще у 2007 році Центру реагування на комп'ютерні інциденти, який увійшов до складу Державної служби спеціального зв'язку та захисту інформації. Окрім того, статтею 5 Закону України «Про основні засади забезпечення кібербезпеки України» [33] передбачено перелік суб'єктів забезпечення кібербезпеки (у межах своєї компетенції): від Ради національної безпеки і оборони України та її робочого органу – Національного координаційного центру кібербезпеки, органів державної влади та місцевого самоврядування (наприклад, Міністерство оборони, Міністерство фінансів, Міністерство юстиції, Міністерство внутрішніх справ, Міністерство закордонних справ, Генеральний штаб Збройних Сил) до юридичних та фізичних осіб, які є які провадять діяльність та/або надають послуги, пов'язані з національними інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом. [33, Ст. 5]

Окремою категорією законодавства є міжнародні акти, ратифіковані Україною. Це, перш за все, Конвенція Ради Європи про кіберзлочинність від 23 листопада 2001 р., ратифікована Законом України від 07 вересня 2001 р. №2824-IV [31]; Міжнародна Конвенція про боротьбу з фінансовим тероризмом від 12 вересня 1999 р., ратифікована Законом України від 12 вересня 2002 р. [18]; Конвенція про відмивання, пошук, арешт та конфіскацію доходів, одержаних злочинним шляхом від 08 листопада 1990 р., ратифікована Законом України від 17 грудня 1997 року [19]; Резолюція Генеральної Асамблеї ООН 57/239 «Елементи для створення глобальної культури кібербезпеки» від 20 грудня 2002 р. [9] тощо.

Враховуючи багатогранність нормативних актів у сфері інформаційної безпеки, постає питання ефективності їх застосування як на локальному, національному, так і на міжнародному рівнях, оскільки вирішення проблем інформаційної та кібербезпеки, по суті, не має кордонів. Розуміння імплементації нормативно-правових актів на різних рівнях, на думку авторів, дозволить врахувати особливості їх застосування як на рівні життєдіяльності суспільства, так і на рівні національних інтересів.

Такий багаторівневий підхід (на мега рівні – міжнародному, мета рівні – національному, макро рівні – рівні держави, мезо рівні – рівні регіону, мікро рівні – рівні підприємства та нано рівні – рівні фізичної особи) дозволяє впорядкувати нормативно-

правове регулювання відносин між суспільством, його членами та державою, між фізичними та юридичними особами з урахуванням міжнародних тенденцій у сфері нормативно-правового забезпечення інформаційної безпеки (Рис. 1).

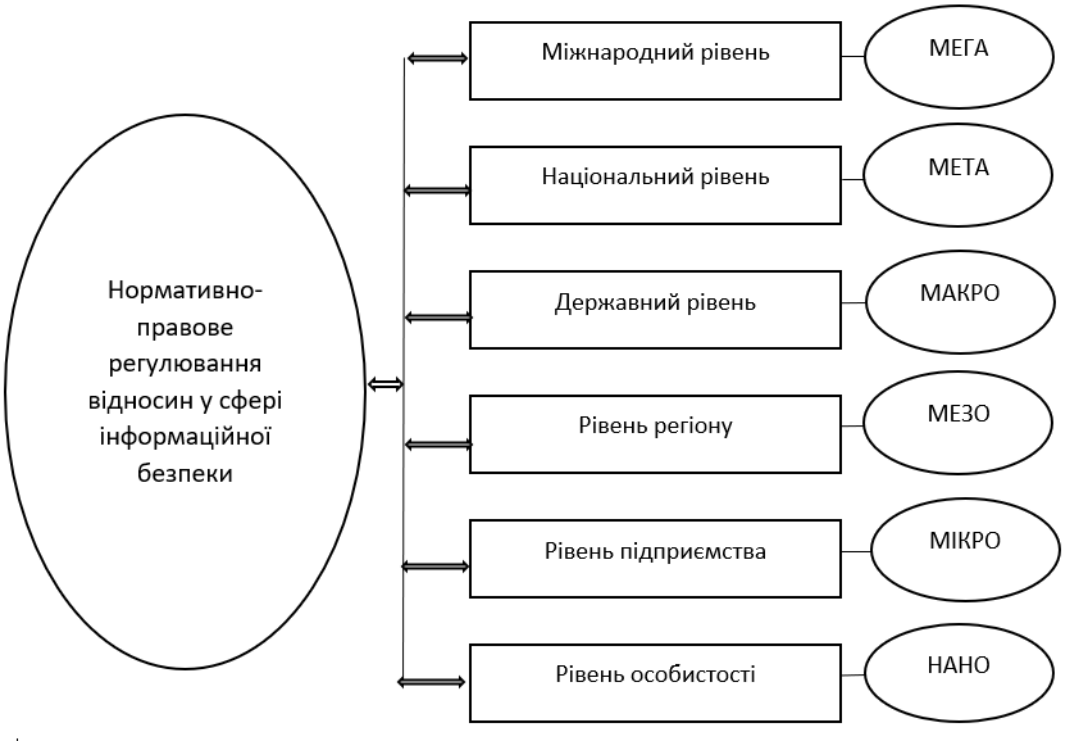

Рис. 1. Багаторівневий підхід до регулювання відносин у сфері інформаційної безпеки

Для ефективного регулювання відносин між різними рівнями принциповим є чітке розуміння основних складових інформаційної безпеки та функцій, які покликана виконувати нормативно-правова база її забезпечення.

Вирішуючи поставлені завдання, необхідно, на думку авторів, виокремити наступні складові системи нормативно-правового забезпечення інформаційної безпеки:

1. Законодавча, нормативно-правова та наукова база.
2. Структура і завдання органів (підрозділів), що забезпечують безпеку інформаційних технологій.
3. Організаційно-технічні й режимні заходи і методи (політика інформаційної безпеки).
4. Програмно-технічні засоби і способи забезпечення інформаційної безпеки.

Відносно функцій, які має виконувати нормативно-правове забезпечення інформаційної безпеки, вважаємо за доцільне виокремити наступні:

1. Регулювання взаємовідносин між суб'єктами інформаційної безпеки на різних рівнях, визначаючи їх права, обов'язки та відповідальність.
2. Нормативно-правове забезпечення дій суб'єктів інформаційної безпеки на всіх рівнях, зокрема, підприємства, регіону, держави, нації.
3. Встановлення порядку використання різних сил та засобів забезпечення інформаційної безпеки.

Зважаючи на вищезазначене, нормативно-правову базу забезпечення інформаційної безпеки доцільно розглядати на зазначених вище рівнях, що враховують існуючу ієрархію нормативних актів, зміст відносин, які регулюються, та коло осіб, на яких поширюються зазначені норми (Рис. 2):

на мега рівні – міжнародні акти про забезпечення інформаційної безпеки;

на мета рівні – норми Конституції України, що є концептуальними для всіх сфер, а також положення таких актів, як Закон України «Про національну безпеку України» [32] та Указ Президента «Про Стратегію національної безпеки України» [36]. Зазначені документи враховують, у свою чергу, основні положення міжнародних актів та угод (мега рівень), ратифікованих Україною;

на макро рівні – спеціальні закони та інші нормативні акти, що стосуються забезпечення національної безпеки в інформаційній сфері: розпорядження Кабінету Міністрів України «Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки та затвердження плану заходів щодо її реалізації» [38], постанова Кабінету Міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» [27], постанова Кабінету Міністрів України «Деякі питання документування управлінської діяльності» [42], Законів України «Про інформацію» [30], «Про доступ до публічної інформації» [22], «Про державну таємницю» [21], «Про захист персональних даних» [29], «Про захист інформації в інформаційно-телекомунікаційних системах» [28] тощо, а також Закони України інституційного напрямку, що закріплюють компетенції органів державної влади у процесі забезпечення національної безпеки в інформаційній та інших сферах життєдіяльності особистості, суспільства та держави: «Про національну безпеку України» [32], «Про службу безпеки України» [37], «Про Державну службу спеціального зв’язку та захисту інформації України» [20] тощо;

на мезо рівні – акти нормативного та директивного характеру органів місцевого самоврядування (наприклад, [34]), а також акти вищої юридичної сили, що стосуються їх повноважень у контексті оперативного вирішення питань забезпечення національної, у тому числі й кібер, безпеки (про боротьбу з наслідками стихійних лих, техногенних аварій, катастроф, кібератак тощо), що є обов’язковими для виконання усіма установами, підприємствами та організаціями, а також посадовими особами та громадянами на території даного органу місцевого самоврядування;

на мікро рівні – це локальні акти юридичних осіб щодо забезпечення інформаційної безпеки у межах функціонування конкретного підприємства, установи або організації та акти вищої юридичної сили, що стосуються їх організаційної та оперативної діяльності (наприклад, ДСТУ 4145-2002 (Інформаційні технології. Криптографічний захист інформації… [11]) накази Адміністрації державної служби спеціального зв'язку та захисту інформації України «Про затвердження Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації» [25] та «Про затвердження вимог до форматів, структури та протоколів, що реалізуються у надійних засобах електронного цифрового підпису» [23], Методичні рекомендації щодо дій організаційно-технічного характеру державних та приватних нотаріусів України у сфері безпеки використання Єдиних та Державних реєстрів України [17], Положення про забезпечення безперервного функціонування інформаційних систем Національного банку України та банків України [24]);

на нано рівні – нормативні акти будь-якого рівня ієрархії, що стосуються інформаційної безпеки особистості як у концептуальному, так і в прикладному сенсі (наприклад, Загальний регламент про захист даних [2], Закон України «Про захист персональних даних» [29]).

Особливістю сучасної системи нормативно-правового забезпечення інформаційної безпеки України є те, що окремі сфери мезо, мікро та нано рівнів перебувають або на стадії розвитку (стратегічного планування), коли прийняття окремих актів вже передбачено стратегічними документами макро та мета рівнів (наприклад, проект постанови Кабінету Міністрів України «Про затвердження порядків формування об’єктів критичної інформаційної інфраструктури, порядку внесення об’єктів критичної інформаційної інфраструктури до

державного реєстру об'єктів критичної інформаційної інфраструктури, його формування та забезпечення функціонування» [26]), або на стадії, коли правове регулювання вже існуючих у реальності процесів та явищ ще не заплановано вводити у правове поле [39]).

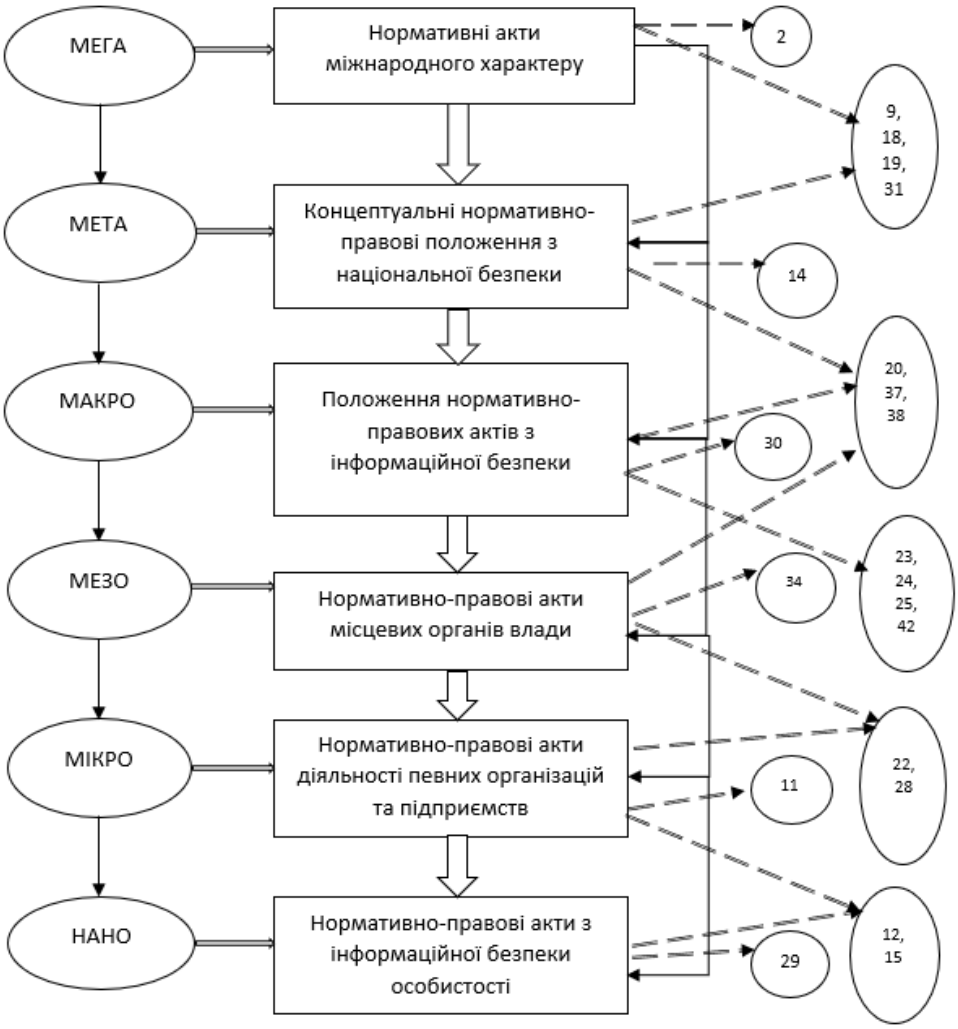

Рис. 2. Класифікація нормативно-правових актів з інформаційної безпеки по рівням

Таким чином, з урахуванням вищезазначеного під системою нормативно-правового забезпечення інформаційної безпеки пропонуємо розуміти динамічну, багатофункціональну структуру зі зворотними зв'язками, всі компоненти якої розподілені по рівнях, взаємодіють між собою, створюючи синергетичний ефект, та спрямовані на досягнення головного результату – нормативно-правового супроводу інформаційної безпеки.

5. Висновок

У процесі проведеного дослідження встановлено, що методологічним підґрунтям дослідження нормативно-правового забезпечення інформаційної безпеки може бути сукупність науково-методичних знань, накопичених у процесі системного аналізу. На думку авторів, це дозволить ліквідувати дисбаланс між динамічним розвитком інформаційного суспільства як в Україні та світі, та його нормативно-правовим супроводом. Доведено, що задля ефективного використання основних принципів системного підходу до досліджуваного об'єкту варто створити єдине термінологічне поле. Вибудовуючи структуру нормативно-

правового забезпечення інформаційної безпеки, використано багаторівневий підхід з певною ієрархією рівнів, взаємозв'язків між ними та загальним механізмом функціонування, зокрема, на мега рівні – міжнародному, мета – національному, макро – на рівні держави, мезо – на рівні регіону, мікро рівні – рівні підприємства, установи, організації (юридичної особи) та нано рівні – рівні фізичної особи.

Систематизація нормативно-правових актів на різних рівнях дозволить врахувати особливості їх імплементації як на рівні життєдіяльності суспільства, так і на рівні національних інтересів.

До перспектив подальших досліджень відносимо реалізацію запропонованої моделі нормативно-правового забезпечення інформаційної безпеки на певному рівні з виокремленням організаційно-технічних заходів та методів.

Author details (in Russian)

СИСТЕМНЫЙ ПОДХОД К АНАЛИЗУ НОРМАТИВНО-ПРАВОВОГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Ирада Джалладова *, Нина Батечко **, Евгения Коломиец-Людвиг ***

** Киевский национальный экономический университет имени Вадима Гетьмана,*
проспект Победы, 54/1, Киев, 03057, Украина,
e-mail: idzhalladova@gmail.com
д.физ.-мат.н., профессор,
заведующая кафедрой компьютерной математики и информационной безопасности

*** Национальный университет биоресурсов и природопользования Украины,*
ул. Героев обороны, 12, Киев, 03041, Украина,
e-mail: batechko_n_@ukr.net
д.пед.н., доцент,
заведующая кафедрой высшей и прикладной математики

**** Киевский национальный экономический университет имени Вадима Гетьмана,*
проспект Победы, 54/1, Киев, 03057, Украина,
e-mail: evheniakl@kneu.edu.ua
к.ю.н.,
доцент кафедры правового регулирования экономики

Аннотация**:** *В статье обосновываются методологические основы применения системного подхода к анализу нормативно-правового обеспечения информационной безопасности. Указывается необходимость создания единого терминологического поля, которое бы стало основой формирования теоретико-методологической базы информационной безопасности и её нормативно-правового сопровождения. Доказан динамический характер информационных угроз и отставание законодательной сферы от развития информационного общества в Украине и мире. Предложена интерпретация структуры нормативно-правового обеспечения информационной безопасности как многоуровневой модели, компоненты которой находятся в определённой иерархии и взаимодействуют между собой. Систематизация объектов исследования произведена с учётом таких особенностей систем, как целостность, структурность, иерархичность, и в то же время с точки зрения динамической системы с обратными связями и наличием нелинейных эффектов. Доказано, что многоуровневый подход позволяет упорядочить*

нормативно-правовое регулирование отношений в сфере законодательного обеспечения информационной безопасности между обществом, его членами и государством, между физическими и юридическими лицами с учетом международных тенденций.

Ключевые слова: *информационная безопасность, нормативно-правовое обеспечение, системный подход.*

Author details (in English)

SYSTEMIC APPROACH TO THE ANALYSIS OF THE LEGAL FRAMEWORK OF INFORMATION SECURITY

Irada Dzhalladova *, Nina Batechko **, Evhenia Kolomiyets-Ludwig ***

** Kyiv National Economic University named after Vadym Hetman*
54/1 Prospect Peremogy, 03057, Kyiv, Ukraine,
e-mail: idzhalladova@gmail.com
Doctor Science of Economics, Professor,
Head of the Department of computer mathematics and information security

*** National University of Life and Environmental Sciences of Ukraine,*
12, Heroes of Defense str., Kiev, 03041, Ukraine,
e-mail: batechko_n_@ukr.net
Doctor Science of Economics, associate professor,
Head of the Department of higher and applied mathematics

**** Kyiv National Economic University named after Vadym Hetman,*
54/1 Prospect Peremogy, 03057, Kyiv, Ukraine,
e-mail: evheniakl@kneu.edu.ua
PhD in Laws,
Associate professor of the Department of legal regulation of the economy

Abstract: *The article substantiates the methodic bases for the usage of the systemic approach to analyze the legal framework of information security provision. The authors prove the necessity of the creation of common special vocabulary to be the basis of the theoretical methodological grounds of the information security and its legal framework. The conclusion has been approved that information threats are of dynamic character and moreover, the legal regulation of this sphere usually falls behind the development of the information society in Ukraine and all over the world. The multilevel interpretation of the information security legal framework structure has been suggested, with the components of the latter to be interacting and been arranged by hierarchy. The systematization of the objects for research has been performed basing on its following features: integrity, organization structurality, hierarchy, but considering also its features of the dynamic system such as feedback links and non-linear effects. The multilevel approach has been proved to be effective in arranging of the legal framework of information security provision, which considers global tendencies and works for the society, its members and state, as well as for natural persons and legal entities.*

Keywords: *information security, legal framework, systemic approach.*

Використана література

1. Cornish P. Cyber Security and Politically, Socially and Religiously Motivated Cyber

Attacks. Brussels: European Parliament, 2009. 34 p.

2. On the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) : REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 №2016/679. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679 (Last assessed: 10.09.2018)

3. Безкоровайный М. М., Татузов А. Л. Кибербезопасность – подходы к определению понятия. *Вопросы кибербезопасности*. 2014. № 1(2). С. 22-27.

4. Біленчук П. Д. Стратегія інформаційної безпеки України: правові засади захисту інформації: монографія / ред. П. Д. Біленчук. Київ: Укр ДГРІ, 2018. 288 с.

5. Бурячок В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / ред. В. Б. Толубко. Київ: ДУТ, 2015. 288 с.

6. Гавловський В.Д., Бутузов В. М., Тітуніна К. В. Комп'ютерна злочинність: міжнародний досвід боротьби і перспективи для України. *Правова інформатика.* 2009. № 1(21). С. 72-77. URL: http://ippi.org.ua/sites/default/files/09gvdbpu_0.pdf (дата звернення: 10.09.2018).

7. Галушко С. О. Протиборство в інформаційному просторі. *Оборонний вісник.* Київ, 2011. № 11. С. 16-19.

8. Голубев В. А. Аналіз кіберзлочинності у сфері економічної безпеки. *Information Technology and Security.* 2013. № 1. С. 26-32. URL: http://nbuv.gov.ua/UJRN/inftech_2013_1_5 (дата звернення 10.09.2018).

9. Елементи для створення глобальної культури кібербезпеки : Резолюція Генеральної Асамблеї ООН від 20 грудня 2002 р. № 57/239. URL: http://zakon2.rada.gov.ua/laws/show/995_b42 (дата звернення: 10.09.2018).

10. Ильяш А.И. Трансформации системы социальной безопасности Украины : региональное измерение : монография. Львов: ПАИС, 2012. 592 с.

11. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння : Державний Стандарт України (ДСТУ 4145-2002) : затв. наказом Державного комітету України з питань технічного регулювання та споживчої політики від 28 грудня 2002 року № 31. URL: http://gostshifr.URL: .ph/dstu_4145_2002.pdf (дата звернення: 10.09.2018).

12. Кодекс України про адміністративні правопорушення: Закон УРСР від 07.12.1984 р. № 8073-X. Дата оновлення: 28.08.2018. URL: http://zakon0.rada.gov.ua/laws/show/80731-10 (дата звернення: 10.09.2018).

13. Колесников А. В. Гибридные интеллектуальные системы: Теория и технология разработки: монография / под ред. А. М. Яшина. Санкт-Петербург: изд-во СПбГТУ, 2001. 711 с.

14. Конституція України: закон України від 28 червня 1996 р. № 254к/96. *Відомості Верховної Ради України*. 1996. № 30. Ст. 141.

15. Кримінальний кодекс України: Закон України від 05.04.2001 р. №2341-III. Дата оновлення: 28.08.2018. URL: http://zakon5.rada.gov.ua/laws/show/2341-14 (дата звернення 10.09.2018).

16. Ліпкан В. А. Національна і міжнародна безпека в визначеннях та поняттях. Київ: Текст, 2006. 256 с.

17. Методичні рекомендації щодо дій організаційно-технічного характеру державних та приватних нотаріусів України у сфері безпеки використання Єдиних та Державних реєстрів України : Нотаріальна палата України. URL: https://www.notar.ks.ua/wp-content/uploads/2016/07/metod-npu-kiber.pdf (дата звернення 10.09.2018).

18. Міжнародна Конвенція про боротьбу з фінансовим тероризмом: Закон України від 12.09.2002 р. № 149-IV. URL: http://zakon2.rada.gov.ua/laws/show/995_518 (дата звернення 10.09.2018).

19. Про відмивання, пошук, арешт та конфіскацію доходів, одержаних злочинним шляхом : Конвенція Ради Європи від 08 листопада 1990 р.: Закон України від 17.12.1997 р. № 738/97. URL: http://zakon2.rada.gov.ua/laws/show/995_029 (дата звернення 10.09.2018).

20. Про Державну службу спеціального зв'язку та захисту інформації України: Закон України від 23 лютого 2006 р. №3475-IV. *Відомості Верховної Ради України*. 2006. № 30. Ст. 258.

21. Про державну таємницю: Закон України від 21 січня 1994 р. №3855-XII. *Відомості Верховної Ради України*. 1994. № 16. Ст. 422.

22. Про доступ до публічної інформації: Закон України від 13 січня 2011 р. № 2939-VI. *Відомості Верховної Ради України*. 2011. № 32. Ст. 314.

23. Про затвердження вимог до форматів, структури та протоколів, що реалізуються у надійних засобах електронного цифрового підпису: наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 20 серпня 2012 р. № 1236/5/453. URL: http://zakon5.rada.gov.ua/laws/show/z1398-12 (дата звернення 10.09.2018).

24. Про затвердження Положення про забезпечення безперервного функціонування інформаційних систем Національного банку України та банків України: Постанова Національного банку України від 17 червня 2004 р. № 265. *Офіційний вісник України*. 2004. № 28 Ст. 1910.

25. Про затвердження Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації: наказ Адміністрації державної служби спеціального зв'язку та захисту інформації України від 20 липня 2007 р. № 141. URL: http://zakon1.rada.gov.ua/laws/show/z0862-07 (дата звернення 10.09.2018).

26. Про затвердження порядків формування об'єктів критичної інформаційної інфраструктури, порядку внесення об'єктів критичної інформаційної інфраструктури до державного реєстру об'єктів критичної інформаційної інфраструктури, його формування та забезпечення функціонування: проект постанови Кабінету Міністрів України. URL: http://www.drs.gov.ua/wp-content/uploads/2018/08/10345-23.07.2018_2018.pdf (дата звернення 10.09.2018).

27. Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах: Постанова Кабінету Міністрів України від 29 березня 2006 р. № 373. URL: http://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF (дата звернення 10.09.2018).

28. Про захист інформації у телекомунікаційних системах: Закон України від 5 липня 1994 р. №80/94-ВР. *Відомості Верховної Ради України*. 1994. № 31. Ст. 286.

29. Про захист персональних даних: Закон України від 01 червня 2010 р. № 2297-VI.. *Відомості Верховної Ради України.* 2010. № 34. Ст. 481.

30. Про інформацію: Закон України від 2 жовтня 1992 р. № 2657-XII. *Відомості Верховної Ради України*. 1992. № 48. Ст. 650.

31. Про кіберзлочинність: Конвенція Ради Європи від 23 листопада 2001 р. URL: http://zakon5.rada.gov.ua/laws/show/994_575 (дата звернення 10.09.2018).

32. Про національну безпеку України: Закон України від 21 червня 2018 р. № 2469-VIII. *Офіційний вісник України*. 2018. № 55. Ст. 51.

33. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 р. № 2163-VIII. *Відомості Верховної Ради України*. 2017. № 45. Ст. 42.

34. Про призначення відповідального із забезпечення кібербезпеки, кіберзахисту та безпеки інформаційних технологій у Верхньодніпровській районній державній адміністрації: Розпорядження Голови Верхньодніпровської районної державної адміністрації від 05 січня 2018 р. № Р-05. URL: http://www.verhn-rn.dp.gov.ua/OBLADM/vdnepr_rda.nsf/docs/061C3145AC68E2ACC225822B005340B9?OpenDocument&PrintForm (дата звернення 10.09.2018).

35. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» : указ Президента України від 25 лютого 2017 р. № №47/2017. *Офіційний вісник України*. 2017. № 20. Ст. 8.

36. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України»: указ Президента від 26 травня 2015 р. № 287/2015. *Офіційний вісник України*. 2015. № 43. Ст. 14.

37. Про службу безпеки України: Закон України від 25 березня 1992 р. №2229-XII. *Відомості Верховної Ради України*. 1992. № 27. Ст. 382.

38. Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки та затвердження плану заходів щодо її реалізації: рішення Кабінету Міністрів України від 17 січня 2018 р. № 67-р. *Офіційний вісник України*. 2018. № 16. Ст. 70.

39. Стиран В. Як не стати кібержертвою: поради з персональної кібер-безпеки. URL: https://github.com/sapran/dontclickshit (дата звернення 10.09.2018).

40. Сулацький Д. В. Генеза поняття «телекомунікаційна послуга» в українському та європейському законодавстві. *Інформація і право.* 2012. № 2(5) С. 18-22.

41. Супрунов Ю. М. Напрями та окремі проблеми використання соціальних сервісів Інтернету в контексті інформаційної безпеки держави. *Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем*. 2013. Вип. 7. С. 145-159. URL: http://nbuv.gov.ua/UJRN/Psvz_2013_7_18 (дата звернення 10.09.2018).

42. Типова інструкція з документування управлінської інформації в електронній формі та організації роботи з електронними документами в діловодстві, електронного міжвідомчого обміну: Деякі питання документування управлінської діяльності : постанова Кабінету Міністрів України від 17 січня 2018 р. № 55. URL: http://zakon1.rada.gov.ua/laws/show/55-2018-%D0%BF?test=dCCMfOm7xBWMKeFEZiWk7Ch6HI4WUs80msh8Ie6 (дата звернення 10.09.2018).

43. Фурашев В. М. Законодавче забезпечення інформаційної безпеки України. *Інформація і право.* 2014. №1(10) С. 59-67.

44. Шеломенцев В.П. Сутність організаційного забезпечення системи кібернетичної безпеки України та напрями його удосконалення. *Боротьба з організованою злочинністю і корупцією (теорія і практика).* 2012. № 2. С. 299-309. URL: http://nbuv.gov.ua/UJRN/boz_2012_2_36 (дата звернення 10.09.2018).

45. Щербакова А. В., Федорова Г. С. Многоуровневый подход к построению гибридной интеллектуальной системы. *Системи обробки інформації*. 2011. Випуск 3 (93). С. 96 – 99.

References

1. Cornish, P. (2009). *Cyber Security and Politically, Socially and Religiously Motivated Cyber Attacks* [*Cyber Security and Politically, Socially and Religiously Motivated Cyber Attacks*]. Brussels : European Parliament, [in English]

2. *On the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)* (2016). Brussels: Regulation of the European Parliament and of the Council of 27 april 2016 №2016/679. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679 [in English]

3. Bezkorovainii, M.M., & Tatuzov, A.L. (2014). Kiberbezopasnost – podhody k oopredeleniyu poniatiia [Cybersecurity – the approaches to the notion definition]. *Voprosy kiberbezopasnosti – Cybersecurity Issues, 1(2),* 22-27 [in Russian]

4. Bilenchuk, P.D., Borysova, L.V., Kobylianskiy, O.L. & Sobyna, V.O. (2018). *Stratehiya informatsiinoi bezpeky Ukraiyny: pravovi zasady zahystu informatsiyi [Information Security Strategy of Ukraine: legal bases of information protection]*. Kyiv: UkrDHRI [in Ukrainian]

5. Buryachok, V.L., Tolubko, V.B., Horoshko, V.O., Toliuoa, S.V. (2015). *Informatsiina ta kiberbezpeka: sotsiotehnichnii aspect [Information and Cybersecurity: sociotechnical aspect].* Kyiv: DUT [in Ukrainian]

6. Havlovskyi, V.D., Butuzov, V.M., & Titunina, K.V. (2009). Kompiuterna zlochynnist: mizhnarodnyi dosvid borotby s perspectyvy dlia Ukrainy [Cyberdelinquency: international experience of struggling against criminal activity and prospects for Ukraine]. *Pravova informatyka – Legal Informatics, 1(21).* Retrieved from http://ippi.org.ua/sites/default/files/09gvdbpu_0.pdf [in Ukrainian]

7. Halushko, S.O. (2011). Protyborstvo v informatsiinomu prostori [Confrontation in cyberspace]. *Oboronnyi Visnyk – Herald of Defence, 11,* 16-19 [in Ukrainian]

8. Holubev, V.A. (2013). Analiz kiberzlochynnosti u sferi ekonomichnoi bezpeky [Analysis of the cyber delinquency in the sphere of economic security]. *Information Technology and Security, 1,* 26-32. Retrieved from http://ippi.org.ua/sites/default/files/09gvdbpu_0.pdf [in Ukrainian]

9. Elementy dlia stvorennya globalnoi kultury kiberbezpeky [Elements of creation of global culture of cybersecurity] (2002). *Resolution of General Assembly of UNO of December 20, 2002 № 57/239.* Retrieved from http://zakon2.rada.gov.ua/laws/show/995_b42 [in Ukrainian]

10. Illiash, A.I. (2012). *Transformatsii sistemy socialnoy bezopasnosti Ukrainy: regionalnoye izmereniie [Transformation of Social Security System of Ukraine: regional dimension]*. Lviv: PAIS [in Ukrainian]

11. Informatsiini tehnolohii. Kryptohrafichnii zahyst informatsii. Tsyfrovyi pidpys, shcho gruntuyetsya na eliptychnyh kryvyh. Formuvannya ta pereviryannya (2002): Derzhavnyi standart Ukrainy (DSTU 4145-2002) [Information technologies. Cryptographic protection of information. Elliptic Curve Digital Signature. Generation and Check: *State Standard of Ukraine]. State Committee on technical regulation and consumers policy, Order 31.* Retrieved from http://gostshifr.url.ph/dstu_4145_2002.pdf [in Ukrainian]

12. Kodeks Ukrainy pro administratyvni pravoporushennya [Code on Administrative Delinquencies of Ukraine]. (n.d.). *zakon.rada.gov.ua.* Retrieved from http://zakon0.rada.gov.ua /laws/show/80731-10 [in Ukrainian]

13. Kolesnikov, A.V., & Yashin A.M. (2001). *Gibridnyie intellektualnyie sistemy. Teoriia i Tehnologiia razrabotki [Hybrid Intellectual Systems. Theory and Technology of the Development].* SPb.: SPbGTU [in Ukrainian]

14. Konstytutsiia Ukrainy vid 28.06.1996 № 254к/96 [Constitution of Ukraine]. (1996). Kiev, Vidomosti Verkhovnoi Rady Ukrainy, 30, 141. [in Ukrainian].

15. Kryminalnyi Kodeks Ukrainy [Penal Code of Ukraine]. (n.d.). *zakon.rada.gov.ua.* Retrieved from http://zakon5.rada.gov.ua/laws/show/2341-14 [in Ukrainian]

16. Lipkan, V.A., Lipkan, O.S., & Yakovenko, O.O. (2006). *Natsionalna i mizhnarodna bezpeka v vyznachennyah i ponyattyah [National and International Security in Definitions and Terms]*. Kyiv: Tekst [in Ukrainian]

17. Metodychni rekomendatsii shchodo dii orhanizatsiino-tehnichnoho haracteru derzhavnyh ta privatnyh notariusiv u sferi bezpeky vykorystannia Yedynyh ta Derzhavnyh reiesriv Ukrainy (2016) [Methodic Recommendations on the Organization and Technical Actions of State and Private Notaries in the Field of Usage of Common and State Registrars of Ukraine]. Retrieved from https://www.notar.ks.ua/wp-content/uploads/2016/07/metod-npu-kiber.pdf [in Ukrainian]

18. Mizhnarodna Konventsiia pro borotbu z finansovym teroryzmom [International Convention for the Suppression of the Financing of Terrorism]. (1999) (n.d.). *zakon.rada.gov.ua.* Retrieved from http://zakon2.rada.gov.ua/laws/show/995_518 [in Ukrainian]

19. Konventsiia Rady Yevropy “Pro vidmyvannia, poshuk, aresht ta konfiskatsiiu dohodiv, oderzhanyh zlochynnym shliahom” [Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime: Council of Europe]. (1990) (n.d.). *zakon.rada.gov.ua.* Retrieved from http://zakon2.rada.gov.ua/laws/show/995_029 [in Ukrainian].

20. Zakon Ukrainy “Pro Derzhavnu sluzhbu spetsialnoho zv’iazku ta zakhystu informatsii Ukrainy” vid 23.02. 06, No 3475-IV [The Law of Ukraine “On the State Service for Special Communications and Information Protection of Ukraine”]. (2006). Kyiv, *Vidomosti Verkhovnoi Rady Ukrainy, 30*, 258. [in Ukrainian].

21. Zakon Ukrainy “Pro Derzhavnu Taiemnytsiu” vid 21.01.1994 No 3855-XII [The Law of Ukraine “On State Secrets”]. (1994). Kiev, *Vidomosti Verkhovnoi Rady Ukrainy, 16,* 422. [in Ukrainian].

22. Zakon Ukrainy “Pro Dostup Do Publichnoi Informatsii” vid 13.01.2011 No 2939-VI [The Law of Ukraine “On Access to Public Information”]. (2011). Kiev, *Vidomosti Verkhovnoi Rady Ukrainy, 32,* 314. [in Ukrainian].

23. Nakaz Administratsii Derzhavnoi Sluzhby specialnoho zviazku ta zahystu informatsii “Pro zatverdzhennia vymoh do formative, struktury ta protokoliv, shcho realizuiutsia u nadiinyh zasobah elektronnohi tsifrovoho pidpysu” [Order of the State Service of Special Communications and Information Protection of Ukraine “On Ratification of Requirements to formats, structure and protocols of secure means of digital signature”]. (2012) (n.d.). *zakon.rada.gov.ua.* Retrieved from http://zakon5.rada.gov.ua/laws/show/z1398-12 [in Ukrainian].

24. Postanova Natsionalnoho Banku Ukrainy “Pro zatverdzhennia Polozhennia pro zabezpechennia bezperervnoho funktsionuvannia informatsiinyh system Natsionalnoho Banku

Ukrainy ta bankiv Ukrainy" [Regulation of the National Bank of Ukraine "On Ratification of Regulations on the Provision of Continuous Functioning of Information Systems of the National Bank of Ukraine and banks of Ukraine"]. (2004). Kiev, *Ofitsiinyi Visnyk Ukrainy, 28,* 1910. [in Ukrainian].

25. Nakaz Administratsii Derzhavnoi Sluzhby specialnoho zviazku ta zahystu informatsii "Pro zatverdzhennia Polozhennia pro poriadok rozroblennia, vyrobnytstva ta ekspluatatsii zasobiv kryptohrafichnogo zahystu informatsii" [Order of the State Service of Special Communications and Information Protection of Ukraine "On Ratification of Regulations on the Development, Production and Usage of Cryptographic Information Protection Means"]. (2007). (n.d.). *zakon.rada.gov.ua.* Retrieved from http://zakon1.rada.gov.ua/laws/show/z0862-07 [in Ukrainian].

26. Proekt Postanovy Kabinetu Ministriv Ukrainy "Pro zatverdzhennia poriadkiv formuvannia obiektiv krytychnoi informatsiinoi infrastructury, poriadku vnesennia obektiv krytychnoi informatsiinoi infrastructury do derzhavnoho reiestru obektiv krytychnoi informatsiinoi infrastructury, yioho formuvannia ta zabezpechennia funtsionuvannia" [Draft Regulation of the Cabinet of Ministers of Ukraine "On Ratification of Regulations on the Methods of Forming of the Units of Critical Information Infrastructure, Algorithm of Including of the Units of Critical Information Infrastructure to the State Registrar of the Units of Critical Information Infrastructure, its creation and functioning"]. (2018). Retrieved from http://www.drs.gov.ua/wp-content/uploads/2018/08/10345-23.07.2018_2018.pdf [in Ukrainian]

27. Postanova Kabinetu Ministriv Ukrainy "Pro zatverdzhennia Pravyl zabezpechennia zahystu informatsii v informatsiinyh, telekomunikatsiinyh ta informatsiino-telekomunikatsiinyh systemah" [Regulation of the Cabinet of Ministers of Ukraine "On Ratification of the Rules of Information Protection Provision in Informational, Telecommunication and Informational-Telecommunication Systems"]. (2006). (n.d.). *zakon.rada.gov.ua.* Retrieved from http://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF [in Ukrainian]

28. Zakon Ukrainy "Pro zahyst informatsii u telekomunikatsiinyh systemah" vid 05.07.1994 No №80/94-BP [The Law of Ukraine "On Information Protection in Telecommunication Systems"]. (1994). Kiev, *Vidomosti Verkhovnoi Rady Ukrainy, 31,* 286. [in Ukrainian].

29. Zakon Ukrainy "Pro zahyst personalnyh danyh" vid 01.06.2010 No 2297-VI [The Law of Ukraine "On Personal Data Protection"]. (2010). Kiev, *Vidomosti Verkhovnoi Rady Ukrainy, 34,* 481. [in Ukrainian].

30. Zakon Ukrainy "Pro informatsiiu" vid 02.10.1992 No 2657-XII [The Law of Ukraine "On Information"]. (1992). Kiev, *Vidomosti Verkhovnoi Rady Ukrainy, 48,* 650. [in Ukrainian].

31. Konventsiia Rady Yevropy "Pro kiberzlochynnist" [The Convention of the Council of Europe on Cybercrime]. (2001). (n.d.). *zakon.rada.gov.ua.* Retrieved from http://zakon1.rada.gov.ua/laws/show/z0862-07 [in Ukrainian].

32. Zakon Ukrainy "Pro natsionalnu bezpeku" vid 21.06.2018 No 2469-VIII [The Law of Ukraine "On National Security"]. (2018). Kiev, *Oficiinyi Visnyk Ukrainy, 55,* 51. [in Ukrainian].

33. Zakon Ukrainy "Pro osnovni zasady zabezpechennya kiberbezpeky Ukrainy" vid 05.10.2017 No 2163-VIII [The Law of Ukraine "On Bases of Cybersecurity Provision of Ukraine"]. (2007). Kiev, *Vidomosti Verkhovnoi Rady Ukrainy, 45,* 42. [in Ukrainian].

34. Rozporiadzhennia Holovy Verhniodniprovskoi raionnoi derzhavnoi administratsii "Pro pryznachennia vidpovidalnoho iz zabezpechennia kiberbezpeky, kiberzahystu ta bezpeky

informatsiinyh tehnolohii u Verhniodniprovskii raionnii derzhavnii administratsii" [Order of the Head of Verhniodniprovskii District State Administration "On Appointment of the Responsible Officer on Cybersecurity, Cyberprotection and Information Technologies Security in the Verhniodniprovskii District State Administration"]. (2018). Retrieved from http://www.verhn-rn.dp.gov.ua/OBLADM/vdnepr_rda.nsf/docs/061C3145AC68E2ACC225822B005340B9?OpenDocument&PrintForm [in Ukrainian]

35. Ukaz Prezydenta Ukrayiny vid 25 Liutoho 2017 roku №47/2017 "Pro Doktrynu Natsionalnoyi Bezpeky Ukrainy" [Doctrine of National Security of Ukraine]. (2017). Kiev, *Oficiinyi Visnyk Ukrainy, 20,* 8. [in Ukrainian].

36. Ukaz Prezydenta Ukrayiny vid 26 Travnya 2015 roku № 287/2015 "Pro zatverdzhennya "Stratehiyi natsionalnoyi bezpekyUkrayiny" [Strategy of National Security of Ukraine]. (2015). Kiev, *Oficiinyi Visnyk Ukrainy, 43,* 14. [in Ukrainian].

37. Zakon Ukrainy "Pro sluzhbu bezpeky Ukrainy" vid 25.03.1992 №2229-XII [The Law of Ukraine "On Security Service of Ukraine"]. (1992). Kiev, *Vidomosti Verkhovnoi Rady Ukrainy, 27*, 382. [in Ukrainian].

38. Rishennia Kabinetu Ministriv Ukrainy "Pro shvalennia Kontseptsii rozvytku tsyfrovoi ekonomiky ta syspilstva Ukrainy na 2018-2020 roky ta zatverdzhennia planu zahodiv shchodo ii realizatsii" [Decision of the Cabinet of Ministers of Ukraine "On the Approvement of the Concept of the Digital Economy and Society Development of Ukraine and Approvement of the List of Activities aimed at its Fulfilment"]. (2018). Kiev, *Oficiinyi Visnyk Ukrainy, 16,* 70. [in Ukrainian].

39. Styran, V. (2018). How to stay safe online. Retrieved from https://github.com/sapran/dontclickshit [in Ukrainian].

40. Sulatskii, D.V. (2012). Heneza poniattia "telekomunikatsiina posluha" v ukrainskomu ta yevropeiskomu zakonodavstvi [Genesis of the notion of "telecommunication service" in the Ukrainian and European legislation]. *Informatsiia i Pravo – Information and Law, 2(5),* 18-22 [in Ukrainian].

41. Suprunov, Yu.M. (2013). Napriamky ta okremi problem vykorystannia socialnyh servisiv Internetu v konteksti informatsiinoi bezpeky derzhavy [Directions and Some Issues of Internet Social Services Usage in the context of Information Security of the State]. *Problemy stvorennia, vyprobuvannia, zastosuvannia ta ekspluatatsii skladnyh informatsiinyh system – Problems of Creation, Testing, Usage and Exploitation of Complex Information Systems, 7,* 145-159 [in Ukrainian].

42. Postanova Kabinetu Ministriv Ukrainy "Pro deiaki pytannia dokumentuvannia upravlinskoi diialnosti : Typova instructsiia z dokumentuvannia upravlinskoi informatsii v elektronnii formi ta orhanizatsii roboty z elektronnymy dokumentamy v dilovodstvi, elektronnoho mizhvidomchoho obminu" [Regulation of the Cabinet of Ministers of Ukraine "On Certain Issues of Documentation of Management Activity : Standard Manual on Documentation of Management Information in Electronic Form and Organization of Work with Digital Documents, Electronic Interdepartamental Exchange"]. (2018). (n.d.). *zakon.rada.gov.ua.* Retrieved from http://zakon1.rada.gov.ua/laws/show/55-2018-%D0%BF?test=dCCMfOm7xBWMKeFEZiWk7Ch6HI4WUs80msh8Ie6 [in Ukrainian].

43. Furashev, V.M. (2014). Zakonodavche zabezpechennia informatsiinoi bezpeky Ukrainy [Legal Provision of Information Security of Ukraine]. *Informatsiia i Pravo – Information and Law, 1(10),* 59-67 [in Ukrainian].

44. Shelomentsev, V.P. Sutnist orhanizatsiinoho zabezpechennia systemy kibernetychnoi bezpeky Ukrainy ta napriamy yoho udoskonalennia [Main Points of the Organizational Provision of Cybernetic System Security of Ukraine and Directions for Its Improvement]. Borotba z orhanizovanoiu zlochynnistiu i koruptsiieiu (teoriia I praktyka) – *Struggle Against Organized Crime Activity and Corruption (Theory and Practice), 2,* 299 – 309 [in Ukrainian].

45. Shcherbakova A.V., & Fedorova H.S. (2011). Mnogourovnevyi podhod k postroieniiu gybridnoi intellektualnoi sistemy [Multilevel Approach to the Creation of a Hybrid Intellectual System]. *Systemy obrobky informatsii – Information Processing Systems, 3(93)*, 96-99 [in Ukrainian].