ВІДОБРАЖЕННЯ ПОНЯТІЙНО-КАТЕГОРІАЛЬНОГО АПАРАТУ КІБЕРБЕЗПЕКОВОЇ ПОЛІТИКИ В ТЕКСТАХ НОРМАТИВНО-ПРАВОВИХ АКТІВ УКРАЇНИ

Діордіца І.В., доктор юридичних наук, доцент,
професор кафедри приватного та публічного права
Київського національного університету технологій та дизайну
(Україна)

Кібербезпекова політика є одним з найсучасніших напрямів діяльності держави. Поява даного напряму зумовлена стрімким технічним прогресом і проникненням інформаційних технологій у всі сфери життєдіяльності. Правове регулювання зазначеного сегмента стає все більш нагальним у зв'язку із збільшенням реальних загроз як окремим громадянам, так і організаціям, установам, закладам, державі в цілому. У свою чергу, процес нормотворчості передбачає опертя на термінологічний апарат, який в галузі кібернетичної безпеки поки що знаходиться на етапі своєї розробки і потребує створення наукових засад номінації та застосування понять.

З метою систематизації об'єктів концептосфери кібербезпекової політики, які віднайшли своє відображення у нормативно-правових актах, був проведений контент-аналіз текстів ряду документів, зокрема: Закону України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 р.; Стратегії кібербезпеки України, затвердженої Указом Президента України від 15 березня 2016 року; Положення про Національний координаційний центр кібербезпеки від 07 червня 2016 року.

У результаті проведеного аналізу встановлено, що правового статусу набули терміни, які раніш вживалися лише у сфері науки, зокрема: *індикатори кіберзагроз, інцидент кібербезпеки, кібератака, кібербезпека, кібероборона, кіберрозвідка, кібертероризм, кібершпигунство, критична інформаційна інфраструктура, система управління технологічними процесами* тощо**.**

Наведені приклади віддзеркалюють ряд тенденцій, а саме: 1. Номінація понять і явищ у сфері кібернетичної безпеки майже не передається одним простим словом. Це або складне (складноскорочене) слово, або ж термінологічне сполучення. 2. Найбільш продуктивною словотвірною моделлю стали так звані «композити», що з'являються шляхом додавання до ключового елементу «кібер-» слів широкого вжитку (наприклад, *загроза, безпека, захист*), а також правничих термінів, які активно застосовуються і самі по собі (наприклад, *злочин, тероризм, шпигунство* та ін.), проте у варіанті складноскороченого слова набувають принципово нової семантики. 3. Порівняно із текстами нормативно-правових актів, що регламентують діяльність у сфері адміністрування, цивільно-правових чи кримінально-правових відносин, значно вищим є коефіцієнт вживання запозичених слів або так званих «кальок», що по суті є перекладом усталеного англомовного виразу (наприклад, *кіберінцидент, відеохостинг, веб-сайт*).

Розподіл представлених у Законі термінів за принципами фасетної класифікації дозволяє виділити певні лексико-семантичні групи термінології кібербезпекової політики за номінаціями:

1. Суб'єктів (*суб'єкти забезпечення кібербезпеки, власники і розпорядники об'єктів критичної інфраструктури та ін.*);
2. Об'єктів (*кіберпростір, критична інформаційна інфраструктура, об'єкти критичної інфраструктури, об'єкти кіберзахисту, національна система кібербезпеки, сфера електронних комунікацій, зовнішнє та внутрішнє безпекове середовище України, інформаційні та веб- ресурси, веб-сайт, блог-платформа, відеохостинги та ін.*);
3. Відомостей, предметів і явищ (*інформація про інцидент кібербезпеки, індикатори кіберзагроз, кіберзлочинність*);
4. Дій і заходів, діяльності управлінсько-правового характеру (*державна політика у сфері кібербезпеки, забезпечення кібербезпеки; координація діяльності у сфері кібербезпеки; забезпечення захисту прав користувачів комунікаційних систем, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі, кібероборона, запобігання кіберінцидентів, захист національних інформаційних ресурсів; державно-приватна взаємодія у сфері кібербезпеки; контроль за законністю заходів із забезпечення кібербезпеки*);
5. Технологічних процесів, процедур, засобів (*виявлення та реагування на кіберзагрози, засоби кіберзахисту, система управління технологічними процесами, захист інформації; впровадження організаційно-технічної моделі кіберзахисту*)
6. Юридично значущих подій (*інцидент кібербезпеки, кібератака, кіберзагроза, загроза безпеці систем електронних комунікацій*)
7. Правопорушень/злочинів (*кіберзлочин (комп'ютерний злочин), кібертероризм; кібершпигунство; зрив та/або блокування роботи системи, та/або несанкціоноване управління її ресурсами; порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів*) [1, с. 65].

Безумовно, наведений перелік не можна вважати вичерпним, у подальшому він може набути більш деталізованого й розгалуженого вигляду. Тим не менш, він достатньо чітко унаочнює відображення термінів сфери кібербезпекової політики у нормативно-правових актах.

Характерно, що законодавець чітко розмежовує об'єкти кібербезпеки і об'єкти кіберзахисту. До першої групи він відносить такі глобальні категорії, як конституційні права і свободи людини і громадянина; суспільство, сталий РІС та цифрового комунікативного середовища; державу, її конституційний лад, суверенітет, територіальну цілісність і недоторканність; національні інтереси в усіх сферах життєдіяльності особи, суспільства та держави; об'єкти критичної інфраструктури. Як бачимо, на цьому рівні відбувається поєднання абстрактних категорій із цілком матеріальними об'єктами. До другої групи (об'єкти кіберзахисту) віднесені номінації, що позначають реальні об'єкти: комунікаційні системи, об'єкти критичної інформаційної інфраструктури.

Варто звернути увагу на те, що об’єкти критичної інфраструктури у Законі віднесені до категорії кібербезпеки, а об’єкти критичної інформаційної інфраструктури – до кіберзахисту. У зв’язку з цим виникає потреба у порівняльному аналізі нормативного тлумачення понять «кібербезпека» і «кіберзахист».

Законодавець, надаючи дефініцію першого поняття, спирається на денотат «захищеність»: «Кібербезпека – захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору…». Що ж до спорідненого поняття, то воно тлумачиться так: «Кіберзахист – сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації…». Тож чітко відстежується одночасне вживання в межах одного нормативно-правового акта паронімів «захист» і «захищеність». Принагідно зазначимо, що у законодавчій практиці це не єдиний випадок. Так, у Законі України «Про основи соціальної захищеності інвалідів в Україні» паралельно застосовуються ті ж самі парні назви. У той же час Закон України «Про соціальний і правовий захист військовослужбовців та членів їх сімей» подібної пари не містить.

Звернення до лінгвістичних лексикографічних джерел з метою актуалізації семантики зазначених термінів дозволило виявити, що в них представлений лише термін «захист» зі значеннями: «1. Дія за знач. захищати, захистити і захищатися, захиститися. 2. Заступництво, охорона, підтримка. 3. Місце, притулок, де можна захиститись, заховатись від кого-, чого-небудь; укриття. 4. Сторона, яка захищає обвинуваченого під час суду; оборона.» [2, с. 339] Лексема «захищеність» в тлумачних словниках сучасної української мови взагалі відсутня. Зауважимо, що подібне відставання лексикографічної практики від законотворчої йде не на користь тим, хто намагається системно порозумітися на букві закону.

У цій ситуації доцільно провести паралель з англійськомовною термінологією, де чітко розрізняється «Cyber safety object» (базується на понятті «захищеність») і «Cyber security object» (базується на понятті «захист). У першому випадку йдеться про такі умови існування об’єкта, за яких він перебуває у стані захисту або малої вірогідності небезпеки та ризиків. У другому ж випадку, маються на увазі зовнішні дії, процедури, заходи, що убезпечують об’єкт, зберігаючи конфіденційність, цілісність, недоторканність, доступність, придатність для користування.

Існує точка зору, що кібербезпека, також як і кіберпростір, може описуватися тріадою її складових: інформаційні ресурси, комп’ютерна і мережева архітектура, способи взаємодії користувачів [3, с. 26]. Подібна точка зору здається нам занадто звуженою і неґрунтовною, доволі технократичною, адже вона не відображає ані правових, ані управлінських аспектів забезпечення цієї важливої сфери життєдіяльності. Відображення у нормативно-правових актах України принципово інших концептуальних підходів підкреслює роль політичної, управлінської складової, її значення для забезпечення національної безпеки в цілому.

Література:

1. Діордіца І. В. Репрезентація термінології кібербезпекової політики в текстах нормативно-правових актів України. *Науковий вісник Міжнародного гуманітарного університету. Серія : Юриспруденція.* - 2017. - Вип. 29 (1). - С. 64-67. - Режим доступу: http://www.vestnik-pravo.mgu.od.ua/archive/juspradenc29/part_1/18.pdf.

2. Великий тлумачний словник сучасної української мови / [уклад. і голов. ред. В. Т. Бусел]. Київ ; Ірпінь : Перун, 2003. 1440 с.

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

КОРУПЦІЯ ЯК ОДИН ІЗ ЗЛОЧИНІВ В ДІЯЛЬНОСТІ ПУБЛІЧНОЇ ВЛАДИ

Жданюк К.Г. студентка юридичного факультету
Дніпропетровського державного університету внутрішніх справ

Іваниця А.В., кандидат юридичних наук,
доцент кафедри загальноправових дисциплін
Дніпропетровського державного університету внутрішніх справ
(Україна)

Корупція є базовою проблемою в діяльності публічної влади. До сих пір при наявності великої кількості наукових праць вітчизняних та зарубіжних вчених, при намаганні застосування європейського досвіду у боротьбі з цим явищем на практиці, на жаль, викорінити її цілком так і не вдалося. Тому дана проблематика є вельми актуальною і потребує детального розгляду. Проблема наявності корупції в органах публічної влади України впливає на формування волевиявлення української держави.

У галузі державного управління проблема корупції здебільшого досліджується в контексті аналізу нормативно-правового регулювання механізмів функціонування органів влади (В. Авер'янов, В. Бакуменко, С. Дубенко, М. Мельник, В. Мартиненко, Т. Мотренко, Н. Нижник, В. Олуйко, О. Прохоренко, М. Стрельбицький та ін.), ефективності професійної діяльності посадовців (Н. Липовська, С. Серьогін), невідворотності покарань (О. Кальман, М. Погорецький, М. Потебенько, Б. Романюк, Є. Скулиш, В. Захарченко та ін.), впливу корупції на соціально-політичні процеси (М. Камлик, О. Маркеєва, Є. Невмержицький, С. Рогульський, С. Серьогін, Р. Тучак). Зокрема, С. Серьогін приділяє значну увагу механізмам попередження та протидії корупції в органах публічної влади України. Є. Невмержицький досліджує корупцію як соціально-політичний феномен та причини і наслідки її виникнення. С. Рогульський вивчає адміністративно-правові заходи боротьби з корупцією в Україні. Р. Тучак розглядає питання правового статусу суб'єктів боротьби з корупцією. Велика кількість висловлених та обгрунтованих ними зауважень та пропозицій були враховані законодавцями, унаслідок чого внесені зміни до законодавства, що регулює питання боротьби з корупцією. Проте зменшення рівня корумпованості державних службовців та