УДК 342.9

Діордіца І. В.,
кандидат юридичних наук, доцент,
доцент кафедри кримінального права і процесу
Національного авіаційного університету

РЕПРЕЗЕНТАЦІЯ ТЕРМІНОЛОГІЇ КІБЕРБЕЗПЕКОВОЇ ПОЛІТИКИ В ТЕКСТАХ НОРМАТИВНО-ПРАВОВИХ АКТІВ УКРАЇНИ

Анотація. Нормативно-правова регламентація такого новітнього явища, як кібернетична безпека, має носити системний характер і реалізовуватися як на науково-концептуальному рівні, так і на рівні формування політики в цій сфері, а також на рівні механізму правового регулювання через норми, затверджені в законах і підзаконних актах. Автор статті детально аналізує процеси, що відбуваються на цьому шляху. Використовуючи методи системного, порівняльного і контент-аналізу, він встановлює тенденції термінотворення й застосування термінів, пропонує фасетну класифікацію юридичної термінології в галузі кібербезпекової політики.

Ключові слова: кібербезпекова політика, термін, термінологія, термінознавство, юридична техніка нормотворчості, фасетна класифікація, кіберзахист, кіберзахищеність.

Постановка проблеми. Кібербезпекова політика є одним з найсучасніших напрямів діяльності держави. Поява такого напряму зумовлена стрімким технічним прогресом і проникненням інформаційних технологій у всі сфери життєдіяльності. Правове регулювання зазначеного сегменту стає дедалі більш нагальним з огляду на збільшення 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.

Аналіз публікацій. Процеси юридичного термінотворення й законодавчої стилістики, насамперед, є сферою правничої лінгвістики, а тому активно розробляються фахівцями у названій галузі. Серед публікацій останнього часу особливо слід зазначити наукові розвідки Л.Л. Бєсєдної щодо мовно-термінологічних проблем законодавства України [1], О.С. Колюшевої з питань англійської адміністративно-правової термінології в адміністративному праві України [2], М.В. Коцюби щодо української термінології державного управління [3], М.І. Любченко щодо поняття, особливостей та видів юридичної термінології [4], А.С. Токарської з проблеми комунікативної стратегії законотворчої і законодавчої діяльності [5]. Зі свого боку, ключові засади кібернетичної безпеки, зокрема з позицій термінознавства, досліджуються юристами, управлінцями, політологами. У цьому напрями плідно працюють такі фахівці, як О.А. Баранов, В.А. Ліпкан, Р.В. Лук'янчук, В.П. Шеломенцев та ін.

Незважаючи на великий інтерес науковців до питань кібернетичної безпеки, тезаурус кібербезпекової політики поки що залишається несформованим і несистематизованим, що мало сприяє створенню ефективної законодавчої регламентації процесів державного управління у вказаній сфері.

Мета статті – дослідження механізму відтворення в текстах нормативно-правових документів термінології, яка являє собою денотат ключових понять кібербезпекової політики, а також класифікацію масиву термінів у відповідних фасетних групах, що у подальшому сприятиме логіко-семантичній систематизації цієї термінології.

Виклад основного матеріалу дослідження. Синкретизм наукової проблеми, що досліджується, виявляється не тільки через її міждисциплінарний характер, а й через співвідношення статичних і динамічних чинників, що впливають на перебіг процесів творення й вживання вузькоспеціальної термінології у нормативно-правових актах.

До усталених (статичних) чинників ми відносимо ті теоретичні засади, що доволі детально розроблені в науці, зокрема в термінознавстві. Так, майже аксіоматичним сприймається визначення поняття терміна, за яким під ним розуміється «слово або словосполучення на позначення поняття спеціальної галузі знання або діяльності» [12, с. 508] До характерних рис терміна зазвичай відносять системність, наявність дефініції, тенденцію до моносемантичності в межах свого термінологічного поля, відсутність експресії, стилістичну нейтральність, активне застосування в науці [13; 16] Дослід динаміки основних тенденцій у сфері творення й застосування термінів дозволяє констатувати, що останнім часом активізувалися процеси номінації (пошуку відповідної назви на позначення нових понять, явищ, реалій, предметів), інтернаціоналізації (створення спільного наукового тезаурусу, що можна розглядати як прояв глобалізації в науці), ретермінологізації (перенесення термінів однієї галузі на іншу із повним або частковим переосмисленням), часткової детермінологізації (виходом терміна за власне наукове застосування і вживання його в інших стилях – офіційно-діловому, публіцистичному, а іноді – й розмовному). Вважаємо, що найбільш рельєфно ці процеси відбуваються у сфері кібернетичної безпеки.

Стрімкий темп науково-технічної революції призводить до необхідності мовного позначення нових об'єктів і предметів, які щойно відкриваються внаслідок наукової діяльності. Гносеологія як теорія пізнання невід'ємно пов'язана із номінацією понять, що з'являються в уяві або чуттєво сприймаються й аналізуються людиною. Ментально-логічні одиниці (концепти) з'являються внаслідок практичної, теоретико-пізнавальної, експериментально-пізнавальної діяльності людини, матеріалізуються або ж так і залишаються абстрактами. На рівні когнітивістики виникає потреба у знаходженні найбільш точної назви для досліджуваних об'єктів, конкретизується семантичне поле певної мовної одиниці. Об'єктивація ускладнюється з огляду на специфічні особливості світосприйняття й картини світу кожного індивіда, формування системи його знань у парадигмі певних наукових концепцій і методологічних засад.

Саме цим можна пояснити той факт, що не вщухають наукові дискусії щодо сутності понять «інформаційний простір», «кібернетичний простір», «кібернетична безпека», «кібербезпекова політика» тощо. Навіть за первинної усталеності ключових номінацій їхнє тлумачення, зокрема й на законодавчому рівні, не перестає бути спірним предметом. Позаяк до текстів нормативно-правових актів терміни мають потрапляти у своєму найбільш точному значенні.

Інтернаціоналізація термінології кібернетичної безпеки детермінована, насамперед, транснаціональним характером явища, домінантою англомовної термінології в силу екстралінгвістичних чинників (пріоритетність окремих країн в галузі наукових досліджень, більший досвід у сфері державного управління певними явищами, глобалізаційні процеси, широка розповсюдженість як світової мови тощо). Зазначене пояснює причину широкого вжитку запозичень у сфері кібербезпеки, починаючи із самого елементу «кібер», який став дуже продуктивним у словотворенні.

Природа ретермінізації мовних одиниць сфери, що досліджуються, також є на поверхні. Техногенний характер феномена породжує соціальні явища, а це, у свою чергу, викликає необхідність вироблення відповідної політики та її закріплення у нормативно-правових актах. Тож у цій ситуації технічні терміни переймаються такими гуманітарними науками, як філософія, соціологія, політологія, право, і в кожній з наук набувають свого предметного забарвлення в залежності від її специфіки.

Як уже зазначалося, згідно зі стилістичними нормами застосування термінологія обмежується науковим стилем та його підстилями. Проте застосування правничої термінології поза текстами наукових досліджень, а саме – у мові закону – певною мірою розмиває власне наукові властивості терміна, додає йому нових якостей і функцій, що, по суті, стає детермінологізацією.

У такий спосіб, виникають підстави стверджувати, що відбувається процес репрезентації термінології в текстах нормативно-правових актів. Іншими словами, терміни проходять шлях від складової концептосфери як методологічного підґрунтя об'єкта, явища, дії до наукового втілення ідеї, а згодом – і виходу за межі науки з перетинанням у сферу правотворчості. Легалізація, тобто законодавче закріплення терміна, надає йому принципово іншого статусу, фактично робить його складовою норм права, а відтак –і частиною механізму правового регулювання.

Тож перед суб'єктами законодавчої ініціативи постає низка завдань з категорії юридичної техніки нормотворчості, а саме: ретельний відбір термінів, що найбільш автентично передають сутність регламентованих понять; вибір україномовного чи запозиченого варіанту найменування за наявності повних синонімів; створення легалізованих дефініцій ключових термінів юридичного акта; формулювання й мовне оформлення норм, правил, приписів щодо правового регулювання в певній сфері.

З метою систематизації об'єктів концептосфери кібербезпекової політики, які віднайшли своє відображення в нормативно-правових актах, був проведений контент-аналіз текстів низки документів, зокрема: Закону України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 [17]; Стратегії кібербезпеки України, затвердженої Указом Президента України від 15 березня 2016 р. [18]; Положення про Національний координаційний центр кібербезпеки від 07 червня 2016 р. [19].

Унаслідок 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 певні 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 [17] термінів за принципами фасетної класифікації дозволяє виокремити наступні 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 в 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).

Безумовно, наведений перелік не можна вважати вичерпним, у подальшому він може набути більш деталізованого

й розгалуженого вигляду. Тим не менш, він достатньо наочно демонструє репрезентацію термінів сфери, що досліджується, 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 розвиток інформаційного суспільства та цифрового комунікативного середовища; державу, її конституційний лад, суверенітет, територіальну цілісність і недоторканість; 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 в законі [17] віднесені до категорії кібербезпеки, а об'єкти критичної інформаційної інфраструктури – до кіберзахисту. З огляду на це, виникає потреба в 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…». То ж чітко відстежується одночасне вживання в межах одного нормативно-правового акта паронімів «захист» і «захищеність». Принагідно зазначимо, що в законодавчій практиці це не єдиний випадок. Так, у Законі України «Про основи соціальної захищеності інвалідів в Україні» паралельно застосовуються ті ж самі парні назви. [20] Водночас, Закон України «Про соціальний і правовий захист військовослужбовців та членів їх сімей» [21] 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» [22, с. 339] Лексема «захищеність» в тлумачних словниках сучасної української мови загалом 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 англомовною 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 знаходиться 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, недоторканість, доступність, придатність для користування. Враховуючи компаративний аналіз, було б незайвим у подальшому під час розробки питань кібернетичної безпеки спиратися на таке розуміння.

Існує точка зору, що кібербезпека, як і кіберпростір, може описуватися тріадою її складових: інформаційні ресурси, комп'ютерна і мережева архітектура, способи взаємодії користувачів. [23, с. 26] Такий погляд здається нам занадто звуженим і неґрунтовним, доволі технократичним, адже він не відображає ані правових, ані управлінських аспектів забезпечення цієї важливої сфери життєдіяльності. Відображення в нормативно-правових актах України принципово інших концептуальних підходів підкреслює роль політичної, управлінської складової, її значення для забезпечення національної безпеки в цілому.

Висновки. Отже, подальший розвиток діяльності держави у сфері кібернетичної безпеки, концептуальне вироблення засад політики в цій галузі можливі лише за умови комплексного поєднання науково виважених засад різних інтегративних наук і відтворення провідних концепцій у текстах відповідних нормативно-правових актів.

Література:

1. Бєсєдна Л.Л. Мовно-термінологічні проблеми законодавства України / Л.Л. Бєсєдна, О.В. Гладківська [за заг. ред. Гладківської О.В.] ; НАПрН України, НДІ інформатики і права. – К. : Пан Тот, 2015. – 126 с.
2. Колюшева О.С. Англійська адміністративно-правова термінологія в адміністративному праві України: автореф. дис. … канд. юрид. наук: 12.00.07 / О.С. Колюшева, НДІ публ. права. – К., 2017. – 18 с.
3. Коцюба М.Й. Українська термінологія державного управління (становлення та розвиток): автореф. дис. … канд. філол. наук: 10.02.01 / Коцюба М.Й, Львів. нац. ун-т. ім. І. Франка. – Львів, 2004. – 16 с.
4. Любченко М.І. Юридична термінологія: поняття, особливості, види / М.І. Любченко ; М-во освіти і науки України; Нац. юрид. ун-т ім. Я. Мудрого. – Харків: Права людини, 2015. –270 с.
5. Токарська А.С. Комунікативна стратегія законотворчої і законодавчої діяльності : навч. посіб. / А.С. Токарська. – Львів: Львівський держ. ун-т внутр. справ, 2016. –243 с.
6. Баранов О.А. Про тлумачення та визначення поняття «кібербезпека» / О.А. Баранов [Електронний ресурс]. – Режим доступу : ippi.org.ua.
7. Діордиця І.В. Система забезпечення кібербезпеки: сутність та призначення / І.В. Діордиця [Електронний ресурс]. – Режим доступу : http://goal-int.org/sistema-zabezpechennya-kiberbezpeki-sutnist-ta-priznachennya
8. Ліпкан В.А. Теоретико-методологічні засади управління у сфері національної безпеки України : [монографія] / В.А. Ліпкан. – К. : Текст, 2005. – 350 с.
9. Ліпкан В.А. Адміністративно-правове регулювання національної безпеки України : [монографія] / В.А. Ліпкан. – К. : Текст, 2008. – 440 с.
10. Лук'янчук Р.В. Державне управління у сфері забезпечення кібербезпеки України : автореф. дис. … канд. наук з держ. упр. : 25.00.01 / Р.В. Лук'янчук ; Ін-т законодавства Верховної Ради України. – К., 2017. – 19 с.
11. Шеломенцев В.П. Сутність організаційного забезпечення системи кібернетичної безпеки України та напрями його удосконалення / Шеломенцев В.П. // Боротьба з організованою злочинністю і корупцією (теорія і практика). – К. : Міжвідом. наук.-дослід. центр з проблеми боротьби з організ. злочинністю, 2012. – № 2(28). – С. 299–309.
12. Лингвистический энциклопедический словарь / гл. ред. В.Н. Ярцева. – М. : Сов. Энциклопедия, 1990. – 685 с.
13. Артикуца Н.В. Мова права і юридична термінологія : навч. посіб. для студентів юрид. спец. вищих навч. закл. / Н.В. Артикуца, Нац. ун-т «Києво-Могилянська академія», центр інновац. методик правн. освіти. – 2-е вид., змін. і доповн. – К. : Стилос, 2004. – 275 с.
14. Вербенєц М.Б. Юридична термінологія української мови: історія становлення і функціонування : автореф. дис. … канд. філол. наук: 10.02.01 / М.Б. Вербенєц, Київ. нац. ун-т ім. Т. Шевченка, Ін-т філол. – К., 2004. – 20 с.

15. Дерба С.М. Українська термінологія в галузі прикладної (комп'ютерної) лінгвістики (логіко-лінгвістичний аналіз) : автореф. дис. … канд. філол. наук: 10.02.01/ С.М. Дерба. – К., 2007.–20 с.
16. Ткач Н.С. Українська правнича термінологія у XX ст. : автореф. дис. … канд. філол. наук: 10.02.01 / Н.С. Ткач, Чернів. нац. ун-т ім. Ю. Федьковича. – Чернівці, 2009.–20 с.
17. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017, набуває чинності з 09.05.2018 [Електронний ресурс]. – Режим доступу : // http://zakon2.rada.gov.ua/laws/show/2163-19
18. Стратегія кібербезпеки України. Введена в дію Указом Президента України від 15 березня 2016 р. № 96/2016. [Електронний ресурс]. – Режим доступу : // http://zakon2.rada.gov.ua/laws/show/n0003525-16.
19. Положення про Національний координаційний центр кібербезпеки від 07.06.2016 р. [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/242/2016
20. Про основи соціальної захищеності інвалідів в Україні : Закон України від 21 березня 1991 р. (в редакції від 26.10.2017) [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/875-12
21. Про соціальний і правовий захист військовослужбовців та членів їх сімей Закон України від 20 грудня 1991 р. (в редакції від 07.05.2017) [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/2011-12/page?text=%E7%E0%F5%E8%F9%E5%ED%B3%F1%F2%FC.
22. Великий тлумачний словник сучасної української мови / уклад. і гол. ред. В.Т. Бусел. – К. : Ірпінь: ВТФ «Перун», 2003. – 1440 с.
23. Безкоровайный М.М., Татузов А.Л. Кибербезопасность – подходы к определению понятия / М.М. Безкоровайный, А.Л. Татузов // Вопросы кибербезопасности. – 2014. – № 1(2). – С. 22–27.

Диордица И. В. Репрезентация терминологии политики кибербезопасности в текстах нормативно-правовых актов Украины

Аннотация. Нормативно-правовая регламентация такого новейшего явления, как кибернетическая безопасность, должна носить системный характер и реализовываться как на научно-концептуальном уровне, так и на уровне формирования политики в данной сфере, а также на уровне механизма правового регулирования через нормы, закрепленные в законах и подзаконных актах. Автор статьи детально анализирует процессы, происходящие на этом пути. Используя методы системного, сравнительного и контент-анализа, он устанавливает тенденции терминообразования и использования терминов, предлагает фасетную классификацию юридической терминологии в области политики кибербезопасности.

Ключевые слова: политика кибербезопасности, термин, терминология, терминоведение, юридическая техника нормотворчества, фасетная классификация, киберзащита, киберзащищенность.

Diorditsa I. Representation of terminology of cyber-security policy in texts of normative and legal acts of Ukraine

Summary. The regulatory and legal regulation of such a new phenomenon as cybernetic security should be systemic in nature and implemented both at the scientific and conceptual level and at the level of policy-making in this area, as well as at the level of the legal regulation mechanism through the norms enshrined in laws and by-laws acts. The author of the article analyzes in detail the processes taking place on this path. Using methods of system, comparative and content analysis, he establishes the trends of terminology and use of terms, offers a facet classification of legal terminology in the field of cybersecurity policy.

Key words: cybersecurity policy, term, terminology, legal rulemaking technique, facet classification, cyber safety object, cyber security object.