УДК 342.9

ЮРИДИКО-ЛІНГВІСТИЧНІ ЗАСАДИ ФОРМУВАННЯ КОНЦЕПТОСФЕРИ КІБЕРБЕЗПЕКОВОЇ ПОЛІТИКИ

LEGAL AND LINGUISTIC FOUNDATIONS FOR CONCEPTOSPHERE FORMATION OF CYBER SECURITY POLICY

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

Розробка наукових засад кібербезпекової політики є водночас і теоретичним, і прикладним питанням. Будь-який концепт реалізується через його матеріалізацію у понятт'єво-категоріальному апараті. Це створює підґрунтя для використання методів юридичної лінгвістики. У статті представлені дві моделі формування концептосфери: гібридного ментального простору і семіотичного простору. Автор демонструє можливості їхнього застосування і доводить ефективність використання подібних моделей, підкреслюючи, що це не єдині можливі способи. Надалі планується дослідження й інших аспектів даної проблеми.
Ключові слова: кібербезпекова політика, формування концептосфери, юридична лінгвістика, модель гібридного ментального простору, модель семіотичного простору.

Разработка научных основ политики кибербезопасности является одновременно и теоретическим, и прикладным вопросом. Любой концепт реализуется путем материализации в понятийно-категориальном аппарате. Это дает основания для использования методов юридической лингвистики. В статье представлены две модели формирования концептосферы: гибридного ментального пространства и семиотического пространства. Автор демонстрирует возможности их применения и доказывает эффективность использования подобных моделей, подчеркивая, что это не единственно возможные способы. В дальнейшем планируется исследование и других аспектов данной проблемы.
Ключевые слова: политика кибербезопасности, формирование концептосферы, юридическая лингвистика, модель гибридного ментального пространства, модель семиотического пространства.

The development of the scientific foundations of cybersecurity policy is both a theoretical and applied issue. Any concept is realized by materialization in the conceptual-categorical apparatus. This gives grounds for using the methods of legal linguistics. The article presents two models for the formation of the conceptosphere: a hybrid mental space and a semiotic space. The author demonstrates the possibilities of using them and proves the effectiveness of using such models, emphasizing that these are not the only possible ways. In the future, it is planned to study other aspects of this problem.
Key words: cybersecurity policy, formation of conceptosphere, legal linguistics, model of hybrid mental space, model of semiotic space.

Постановка проблеми. Кібернетична безпека є невіддільною частиною національної безпеки, а відтак – запорукою суверенності та життєздатності держави. Тож, доки питання кібербезпеки вирішуватимуться сегментарно в окремих галузях і проекціях, стверджувати її дієвість доволі проблематично. Насамперед, потребується розробка для умов України концептуальних підходів кібербезпекової політики, що стратегічно й тактично об'єднує усі аспекти даного напряму діяльності.

Стан опрацювання. Складність і багатогранність проблеми зумовили її дослідження різнопрофільними фахівцями: юристами (О.О. Климчук, В.А. Ліпкан, Р.В. Лук'янчук, Д.С. Мельник, І.М. Рязанцева), філософами і політологами (М.А. Дмитренко, О.П. Дзьобань, Д.В. Дубов, В.В. Петров, М.А. Ожеван), спеціалістами з інформаційних технологій (В.М. Бондаренко, С.С. Забара, В.Г. Зайцев, О.В. Соснін, В.Г. Хахановський, В.Л. Шевченко).

Останнім часом значно активізувалася й наукова діяльність у галузі юридичної лінгвістики, що знаходиться на перетині права і прикладної лінгвістики. Суттєвий внесок у розробку засад даного напряму належить Н.В. Артикуці, Ю.Ф. Прадіду, А.С. Токарській, Л.І. Чулінді та ін. У полі зору вчених знаходяться різноманітні аспекти формування й функціонування юридичної терміносистеми, нормативності тлумачення мовних одиниць в юридичній лексикографії, мові права й мові законів на рівні лексико-стилістичного й граматичного застосування мовних засобів у текстах нормативно-правових актів.

Попри суттєві доробки у суміжних галузях науки, питання щодо юридико-лінгвістичних засад формування концептосфери кібербезпекової політики практично залишилося поза увагою науковців, тож потребує свого висвітлення.

Мета статті є встановлення за допомогою методів юридичної лінгвістики механізму формування концептуальної сфери кібербезпекової політики та її репрезентації у текстах нормативно-правових актів.

Виклад основного матеріалу. Використовуючи наукові метафори, норму права можна порівняти з верхівкою айсбергу, основна частина якого знаходиться під водою. У цій невидимій частині «ховається» концептосфера як цілісно сформоване уявлення про те чи інше поняття в його автономному бутті і у парадигмі взаємодії з іншими елементами системи. Отже, є підстави розглядати концептосферу

не тільки як умовний абстракт, а й через матеріалізацію ідей завдяки метамові. Розуміння даного механізму є принципово важливим у зв'язку з тим, що здебільшого вчені намагаються аналізувати тексти актів, які вже є чинними або пропонуються в якості проектів. По суті це являє собою роботу з результатами, а не з моделлю самої цілісної ідеї. У зв'язку із зазначеним актуалізується проблема методики роботи з метамовою різних галузей. Вона має ґрунтуватися на специфіці кожної окремої сфери.

Щодо сфери кібербезпеки констатуємо принципово важливий вплив бінарного характеру ключових понять. З одного боку, дедалі все більше відбувається глобалізація світу, чому чимало сприяла поява кіберпростору, що ламає традиційні кордони, локалізацію джерел інформації, привносить транснаціональний компонент протиправним діям у сфері інформаційних технологій. Це створює підстави для розуміння масштабності єдиного кібернетичного простору й відповідальності кожної держави перед світовою спільнотою. З іншого боку, забезпечення національної безпеки було й залишається невіддільною функцією будь-якої держави. Оскільки кібербезпека виступає як складова національної безпеки, потрібна розробка, реалізація, постійне удосконалення системних управлінських, економічних, технологічних заходів. Сама єдина концепція здійснення кібербезпекової політики дозволяє це здійснювати ефективно.

Знову ж таки, слід мати на увазі, що при формуванні концептосфери кібербезпекової політики відбувається різноспрямований багатофункціональний рух. Україна не може не враховувати досвід, набутий іншими державами. Це стає важливим і для адаптації національного законодавства, і для реалізації міжнародного співробітництва у вказаній сфері. Проте уповноваженим органам, науковим організаціям слід походити з категорії національних інтересів, захисту інформаційного суверенітету держави. Подібна ситуація суттєво ускладнює завдання, оскільки потребує чітко визначеного концептуального підходу до пошуку гармонії між національним та інтернаціональним.

Даний екстралінгвістичний чинник дає підстави для використання при дослідженні метамови концептосфери кібербезпекової політики модель гібридного ментального простору, розроблену фахівцями з когнітивної лінгвістики Жилєм Фоконьє і Марком Тернером [1]. За баченням авторів, теорія концептуальної інтеграції, як ключове поняття, застосовує «бленд», що по суті являє собою проекцію різних просторів, які не перетинаються між собою, проте ці простори можуть зливатися в єдине ціле у спільній родовій єдності, яка іменується «generic». Тож відносно державних аспектів кібербезпекової політики доцільно говорити про певний бленд, ментально обмежений специфікою національної правової системи. Хоча з урахуванням інтеграції у поняттях кібербезпеки юридичних, політичних, информаційно-технологічних категорій варто навіть у масштабах окремо взятої країни застосовувати поняття гіперблend як ієрархічний багатофункціональний міжнауковий концепт, що співвідноситься з реаліями конкретної держави. Розробка спільних концепцій міжнародного масштабу виходить на рівень генерації, позбавляючись національної специфіки і конгломеруючи спільні для усіх блендів і гіперблендів компоненти. Таким чином, когнітивна модель фундаторів кібербезпекової політики ґрунтується на чітко визначеній уявній взаємодії блендів і гіперблендів.

Екстраполяція когнітивної діяльності у сфері вироблення концептів кібербезпекової політики цілком укладається у теорію семіотичного простору, запропоновану Ю.С. Степановим [2, 3]. Відповідно до цієї теорії метамова функціонує у тримірному просторі, що представлений через категорії семантики, синтактики і прагматики.

Семантика «(від гр. sêmantikos – означальний) – лінгв. Значення, смисл слова або мовного звороту» [4, с. 551] виступає як невіддільний первинний компонент метамови. Перед укладачем закону, політологом, юристом насамперед постає питання зі сфери номінації: як саме назвати те чи інше поняття, явище, юридичний факт; використати при цьому вже існуючі мовні одиниці чи запроваджувати неологізми, у тому числі шляхом запозичення й лексикалізації іншомовних слів; яким принципам номінації слід віддати перевагу тощо. Лінгвістична компетентність фахівця з кібербезпеки повинна охоплювати поняття полісемії термінів, їхньої етимології, вимог до норм слововживання і т.ін. Міжмовні аспекти семантики у разі застосування інтернаціоналізмів (а їх у сфері правової інформатики й кібернетичної безпеки чимало і це може стати темою окремого дослідження) мають враховувати диференційні ознаки мовних одиниць у кожній окремій мові.

Продемонструємо це на прикладі ключового терміну «кібербезпека». За своєю словотворчою структурою він є складноскороченим словом, перша частина якого – інтернаціоналізм, друга – загальновживане українське слово. Його можна розглядати як кальку з інтернаціонального терміну «Cybersecurity». Разом з тим, семантика даної лексичної одиниці, згідно із дефініціями, що містяться у нормативних документах різних країн суттєво відрізняється.

Для порівняльного аналізу скористаємося матеріалами інформаційної довідки «Законодавство та стратегії у сфері кібербезпеки країн Європейського Союзу, США, Канади та інших», підготовленої Європейським інформаційно-дослідницьким центром [5]. Згідно з даними довідки сутність поняття «кібербезпека» у одних держав передається через ключове слово «заходи»: «сукупність організаційних, правових, технічних та освітніх заходів, спрямованих на забезпечення безперервного функціонування кіберпростору» (Політика захисту кіберпростору Республіки Польща); «заходи з попередження шкоди від збоїв у роботі ІКТ та в її усуненні» (Національна стратегія кібербезпеки Королівства Нідерланди). Інші держави у своїх нормативних актах будують дефініцію, спираючись на лексему «стан»: «бажаний

стан безпеки інформаційних технологій, за якого ризики для кіберпростору скорочені до прийнятного мінімуму» (Стратегія кібербезпеки Німеччини); «бажаний стан інформаційної системи, за якого вона може протидіяти викликам кіберпростору, які можуть негативно вплинути на достовірність, цілісність та конфіденційність даних, що зберігаються або обробляються даною системою» (Стратегія безпеки та оборони інформаційних систем Франції).

Для не чутливої до мови особи взагалі незрозуміла різниця між станом і заходами, проте при формуванні концептів кібербезпекової політики принципово важливим є розрізнення цих понять, вибір пріоритетів, а можливо – й пошуку своїх підходів. Зокрема, як нам вбачається, виходячи з конотації об'єктів, концепт кібербезпеки може бути зорієнтований, насамперед, не тільки на технічну й технологічну складові (як це представлено у наведених вище дефініціях), а й містити значний гуманітарний компонент, що методологічно підпорядкований принципам антропоцентризму, адже зрештою важливе не просто безперебійне функціонування механізмів і систем, а безпечне існування людей, які живуть у цьому просторі. Враховуючи той факт, що в українському законодавстві на сьогодні відсутня юридично закріплена дефініція поняття «кібербезпека» (її ще належить сформувати й ухвалити), подібне положення є принциповим. Воно повністю кореспондується зі ст. 3 Конституції України, відповідно до якої «людина, її життя і здоров'я, честь і гідність, недоторканість і безпека визнаються в Україні найвищою соціальною цінністю» [6].

Ми навели лише один приклад, але подібні ситуації характерні майже для усього понятєвого апарату сфери, що досліджується.

Другий аспект тримірного простору метамови – синтактика «(від гр. syntaktikos – синтаксичний) – розділ семіотики, що вивчає синтаксис різних знакових систем» [4, с. 561]. Її можна умовно порівняти з «алхімією» слів, адже поєднання мовних одиниць на рівні словосполучень, мікротекстів і текстів створює нові інтенціональні простори. Відповідно до законів функціонування метамови, мікротексти і тексти можуть утворюватися лише на підставі взаємодії окремих складових цього інформаційно-комунікативного обширу.

Для ілюстрації можна порівняти семантику ключових для сфери кібербезпеки споріднених термінологічних сполучень «кібербезпекова політика» і «політика кібербезпеки». Справа не лише у формально-граматичних ознаках, за якими одне з них являє собою поєднання атрибутива з номінативом, а інше виступає іменною конструкцією. Головне – це нові лексико-семантичні смисли, що передаються поєднанням співзвучних слів. Так, синтаксичні конструкції, створені за моделлю «номінатив плюс номінатив у родовому відмінку» (N + N2), вирізняються своєю конкретизованістю об'єктних відносин. На відміну від них конструкції типу «атрибутив + номінатив» (Ad + N) передають більш узагальнені характеристики, що взагалі спроможні абстрагувати й масштабувати сутність поняття. Достатньо порівняти з аналогом подібних конструкцій синтаксичні пари «громадянське суспільство» – «суспільство громад» або ж «інформаційне право» і «право на інформацію». Повертаючись до термінології сфери кібербезпеки, зазначимо, що саме методи юридичної лінгвістики дозволяють диференціювати семантику досліджуваних терміносполучень. Тож, поняття «політика кібербезпеки» є більш конкретизованим і вузьким. Воно може вживатися (і до речі, вживається) у діяльності окремих установ, організацій, закладів, комерційних структур на позначення управлінських вимог щодо безпечного користування комп'ютерною технікою з дотриманням норм конфіденційності інформації, правил службової поведінки у мережі Інтернет тощо. Якщо ж йдеться про «кібербезпекову політику», то розуміється системна діяльність держави з протистояння інформаційним загрозам, розповсюджуваних через кібернетичний простір, координація діяльності усіх державних і недержавних структур, задіяних у забезпеченні кібернетичної безпеки, убезпеченні від можливих протиправних дій у даній сфері.

Принагідно зазначимо, що чималу роль у синтактиці відіграють потенції мовних засобів. Так, наприклад, за правилами російської мови можлива лише номінативна конструкція («политика кибербезопасности»). Англомовний аналог «cybersecurity policy» у залежності від контексту може перекладатися українською двома варіантами.

Отже, синтактика як складова юридико-лінгвістичних засад формування концептосфери кібербезпекової політики є не менш важливим компонентом фундації понятійно-категоріального апарату вказаної сфери.

Прагматика «(гр. pragmatikos – діловий) – 1) розділ семіотики, що вивчає відношення між знаковими системами та їх користувачами, а також самі ці відносини; 2) вчення про діяльність, практика» [4, с. 491] у контексті формування концептосфери переслідує вирішення за допомогою мовних засобів прикладних аспектів проблеми. Насамперед, йдеться, про визначення цілей і пріоритетів кібербезпекової політики, кола суб'єктів, що виступають носіями такої політики. З іншого боку, прагмалінгвістика дозволяє ефективно вирішувати юридико-стилістичні та комунікативні завдання, які виникають на етапі створення нормативно-правових актів. Завдяки прагматиці вдається інтегрувати на рівні концептів когнітивні, логічні, методологічні складові ментального смислу, а це, у свою чергу, дозволяє систематизувати картину світу.

Прагматика певною мірою віддзеркалює правничий дискурс, оскільки вбирає у себе не тільки константні характеристики, більшою мірою властиві семантиці й синтактиці, а й спроможна чітко реагувати на динаміку швидко плинних змін у суспільстві, появу нових реалій і сучасних викликів. Знову ж таки, якщо семантика й синтактика здебільшого зосереджені на точності формулювання інформації, то прагматика привносить компоненти перцепції (взаєморозуміння, врахування особливостей сприй-

няття інших осіб) та інтеракції (способів організації комунікативної взаємодії).

Специфіка взаємодії розглянутої умовної системи координат, які покладені в основу моделі дослідження, полягає у тому, що кожна з них, попри свою певну автономність, проявляється у взаємозв'язку і при формуванні концептосфери реалізується у невіддільній єдності. Досить рельєфно це можна простежити на рівні віддзеркалення термінологією кібербезпеки пріоритетів політичної стратегії і тактики різних держав. Скористаємося прикладом з наукової статті за авторством О.В. Булавіна, який, проводячи порівняльний аналіз кібербезпекової політики США і Китаю, звернув увагу на те, що у Сполучених Штатах здебільшого віддається перевага терміну «кібербезпека», тобто основний акцент робиться на безпеці архітектури Інтернету. У той же час Китай та Росія значно частіше використовують поняття «інформаційна безпека» з опорою на обмеження у розповсюдженні інформації, цензурування текстів [7, с. 28].

Безумовно, у межах однієї статті продемонструвати аналіз термінології, що формує концептосферу кібербезпекової політики, за моделлю семіотичного простору неможливо, проте ми й не ставили перед собою такого завдання. Це лише одна з моделей, яка є функціонально ефективною при роботі з ідеологемами. Тож, надалі необхідно розглянути й інші підходи, що може стати темою нових досліджень.

Висновки. Феномен кібербезпекової політики полягає у тому, що на початковому етапі вона з'являється як деякий абстрагований концепт, що потребує визначення основних теоретико-методологічних засад подальшої діяльності, зокрема її правового регулювання. Без цього неможливо подальше проектування правових норм, що матеріалізуються у текстах законодавчих актів. Зазначене створює підґрунтя для наукових досліджень, які б дозволяли знаходити оптимальні підходи й запроваджувати ефективну юридичну техніку.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Fauconnier G. The Way We Think: Conceptual Blending and the Mind's Hidden Complexities / Gilles Fauconnier, Mark Turner. – New York : Basic Books, 2003. – 464 p.

2. Степанов Ю.С. Язык и метод. К современной философии языка / Ю.С. Степанов. – М. : Наука, 1998. – 779 с.

3. Степанов Ю.С. Функции и глубинное / Ю.С. Степанов // Вопросы языкознания. – 2002. – № 5. – С. 3–18.

4. Новий словник іншомовних слів : більше 40 000 сл. і словосполучень / Л.І. Шевченко, О.І. Ніка, О.І. Хом'як. – К. : АРІЙ, 2008. – 672 с.

5. Законодавство та стратегії у сфері кібербезпеки країн Європейського Союзу, США, Канади та інших країн. [Електронний ресурс]. – Режим доступу: http://euinfocenter.rada.gov.ua/uploads/documents/28982.pdf

6. Конституція України (редакція від 30.09.2016) [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/254к/96-вр

7. Булавин А.В. О подходах США и Китая к обеспечению кибербезопасности / А.В. Булавин // Общество: политика, экономика, право. – 2014. – № 3. – С. 27–31.