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

УДК 342.9

НАУКОВА РЕФЛЕКСІЯ СТАНОВЛЕННЯ КІБЕРВЛАДИ В УКРАЇНІ

Формування й ефективна реалізація державної політики у сфері кібербезпеки (далі – кібербезпекової політики), у межах якої розробляється комплекс заходів щодо правових та організаційних засад забезпечення захисту життєво важливих інтересів людини й громадянина, суспільства та держави, національних інтересів України в кіберпросторі, формуються та визначаються основні цілі, напрями й принципи цієї політики, повноваження державних органів, підприємств, установ, організацій, осіб і громадян у цій сфері, засади державно-приватної взаємодії, а також принципи координації їх діяльності із забезпечення кібербезпеки, – необхідна умова результативного розвитку кіберсуспільства в Україні.

В умовах глобалізації інформаційних процесів, їх інтеграції в різні сфери суспільного життя керівництво провідних держав світу приділяє посилену увагу створенню й удосконаленню ефективних систем як кіберзахисту та кібероборони, так і кібербезпеки об'єктів критичної інфраструктури від зовнішніх і внутрішніх загроз кібернетичного характеру.

Зауважу, що в багатьох провідних країнах світу вже сформовані загальнодержавні (національні) *системи кібернетичної безпеки* як найбільш оптимальні організаційно-функціональні структури, здатні за короткий проміжок часу акумулювати сили й засоби компетентних органів державної влади із залученням громадських організацій для протидії кіберзагрозам різного характеру (кіберінцидентам, кібератакам, кіберзлочинам).

В Україні також відбувається процес формування національної системи кібербезпеки. На це чітко вказано як у Стратегії кібербезпеки України, так і в Законі України «Про основні засади забезпечення кібербезпеки України», який вступить у дію 9 травня 2018 р.

Питання кібернетичної безпеки поступово стає предметом дослідження українських учених. Проте звертають на нього увагу насамперед фахівці з питань національної безпеки та представники юридичної науки, зокрема В.А. Ліпкан [1–4], Л.І. Рудник [5–6], В.А. Лахно [7], В.М. Панченко [8] та інші.

Окремо зазначу свої публікації, у яких закладено фундамент для наукових висновків статті [9–14].

Незважаючи на наведене, увага до проблем кібернетичної безпеки звертається здебільшого побіжно – лише в контексті або реалізації державної інформаційної політики, або забезпечення інформаційної безпеки. Відтак ні кібернетична безпека, ні формування кібервлади не є наразі парадигмально пріоритетним напрямом наукового розвитку інформаційного права, незважаючи на об'єктивно існуючі тенденції як інформатизації, так і загалом кіборгізації суспільства.

Також зазначу ще один прикрий факт: станом на грудень 2017 р. в Україні з юридичних наук не захищено жодної дисертації з проблем правового регулювання державної кібербезпекової політики або забезпечення кібербезпеки, незважаючи на нагальність наукового вивчення цієї проблеми.

Підґрунтям для розроблення нової теми – формування кібернетичної влади – може бути робота М.Г. Каращука *«Інформаційна влада як чинник демократизації сучасного суспільства»* (2006 р.). У ній автор аналізує феномен інформаційної влади, визначаючи її поняття, структуру, особливості політичного впливу, роль у демократизації сучасного суспільства [15].

Екстраполюючи висновки із цієї роботи, можу зазначити, що сутність *кібернетичної влади* полягає в структурно-функціональній взаємодії суб'єктів кіберпростору, формуванні та утворенні особливого виду мережевого зв'язку, який забезпечує здатність суб'єктів за допомогою цілеспрямованого створення, збирання, одержання, зберігання, використання, поширення, охорони й захисту інформації реалізовувати свої цілі, причому як у кіберпросторі, так і в реальному житті.

У найближчому майбутньому вплив кібернетичної влади на поведінку людей суттєво відрізнятиметься від звичайного інформування асиметричністю впливу комунікатора на реципієнта, високим ступенем не завжди усвідомленого з боку об'єкта управління контролю за його поведінкою. Суб'єктами та основними носіями кібернетичної влади в кіберсуспільстві виступатимуть новоутворені кібернетичні інститути – засоби масової інформації в кіберпросторі, кібермережі, соціальні мережі, утворені з наперед визначеною метою для певної цільової аудиторії, наукові та науково-просвітницькі установи в кіберпросторі тощо. Таким чином, концепція етатизму має бути переформатована згідно з новими тенденціями трансформації влади та зміщення її в кіберпростір. Якщо цього не відбудеться, то реальність влади в реальному світі стане віртуальною, оскільки стейкхолдери соціальних мереж, глобальних інформаційних систем (наприклад, таких як Google, Amazon, Facebook) зможуть вирішувати свої завдання поза впливом реальних інституціональних структур. Інакше кажучи, формуються умови позаправового контексту діяльності суб'єктів у кіберпросторі за умови збереження ортодоксаль-

ного підходу до правового регулювання соціальних відносин у кіберпросторі.

Визначальним моментом формування кібернетичної влади є формування надійного механізму реалізації законних прав та інтересів громадян у кіберпросторі, тому подальших досліджень потребує встановлення та ідентифікація зв'язку кібернетичної влади з кіберполітикою як один з основних чинників кіберполітики. Це дасть змогу моделювати плюралістичні стратегії трансформації державної влади в умовах збільшення ваги самоорганізації соціо-гуманітарних систем, у тому числі в кібернетичну владу.

Вагомим і конститутивним чинником ефективності функціонування кібернетичної влади є необхідність формування системи правового регулювання кібернетичної політики. Відтак сміливо можна стверджувати, що реалізація кібернетичної функції та формування засад кібербезпекової політики можуть розглядатись у контексті формування й розвитку кібернетичної влади. Тому робота М.Г. Каращука розцінюється мною як вагомий здобуток інформаційно-правової науки саме з позицій її методологічних потенцій.

Дуже цікавий підхід було запропоновано в монографії *«Правові засади розвитку інформаційного суспільства в Україні»* за редакцією В.А. Ліпкана, де було виділено такий прошарок суб'єктів інформаційного суспільства, як *інформаційні маргінали* [16, с. 26].

Цей термін було введено в науковий обіг представниками наукової школи В.А. Ліпкана. За допомогою цього поняття науково обґрунтовано можливості інформаційного поневолення та наслідки інформаційного імперіалізму, одним із результатів яких є формування нової верстви інформаційного суспільства – ***інформаційних маргіналів*** – осіб, які перебувають за межами інформаційного суспільства та втратили свій інформаційний статус унаслідок унікальності власної соціокультурної ситуації під час переходу до глобальної взаємодії в межах інформаційного капіталізму та нездатності протистояти нав'язуванню й пристосуватись до якісно нової мережної архітектури інституційних структур інформаційного суспільства [16, с. 26].

Украй необхідне вивірення кожного параметру розвитку кіберпростору, оскільки соціокультурна та інформаційна грамотність, а також інформаційна ідентичність кожної соціальної системи по-різному визначаються як можливості входження та напрями розвитку соціальної системи в межах кіберпростору.

Важливим аспектом у цьому ракурсі, на який слушно вказують також інші дослідники [17, с. 19–20], з урахуванням методу екстраполяції є ***необхідність правового регулювання*** (відповідно до предмета мого дослідження) таких явищ:

– державної кібернетичної політики;

– розвитку кіберсуспільства та його інститутів;

– державного контролю за кібернетичною владою;

– механізмів громадського й інформаційного контролю за трансформацією кібернетичного суспільства;

– цифрової взаємодії учасників кібернетичних правовідносин тощо.

Окремо феномен маргінальності як предмет дослідження був розглянутий у дисертації А.Л. Свящука *«Феномен маргінальності в генезисі сітьового суспільства»*, де проаналізовано структурний і культурний маргінальні стани соціальних суб'єктів, що виникають під час трансформації соціальної структури та соціокультурної сфери суспільства в обставинах переходу до нового способу структурної стійкості – інформаціонального капіталізму, який діє в умовах глобальної економіки й політики. Висвітлено питання зміни принципів соціальної стратифікації й наступності соціальних структур під час становлення сітьового суспільства з урахуванням регіональної специфіки. Запропоновано авторський підхід до дослідження маргінальності в сітьовому суспільстві. Дисертантом сформульовано нові визначення концептів маргінальності, а також маргінальні наслідки «сітьовізації», що відбувається на стику глобалізаційних і локалізаційних процесів. Це важливо для нас, адже маргінальні елементи є членами та становлять інформаційне суспільство [18].

Викладене матиме важливе значення, насамперед прикладне, для подальшого вивчення кіберсуспільства та розроблення конкретних методик щодо впровадження дієвих механізмів унеможливлення кібермаргіналізації українських соціальних мережевих систем.

Для мого дослідження також корисні погляди О.Л. Свящука на «прояви маргінального в генезі мережевого суспільства в Україні», а саме:

– різка поляризація соціальних верств за рівнем життя;

– перевага спадної соціальної мобільності;

– занепад колишнього середнього класу;

– збільшення периферійних верств – тих, хто, не ідентифікуючи себе з основними соціальними групами, не бере участь у відносинах та діяльності центральних інститутів;

– втрата суспільством колишньої єдності;

– зростання соціального відчуження;

– розрив соціальних і культурних зв'язків;

– наростання в периферійних верствах почуттів розгубленості, непевності, тривоги, нестабільності, дезорієнтації, аномії, втрати звичних і перевірених орієнтирів, що призводить до відчуття себе чужим у рідному суспільстві;

– добровільний відхід цілих соціальних груп за межі панівних відносин;

– замкнутість у субкультурах;

– культурна й духовна фрагментарність;

– збільшення кількості сект;

– зростання рівня злочинності й наркоманії серед молоді за умов неконтрольованого суспільством завершення формування ідентичності;

– вороже ставлення до центральних інститутів влади та протестна поведінка;

– сепаратистські настрої й політичний екстремізм;

– зайва заполітизованість більшості суспільних процесів;

– конфлікт етнічних, релігійних і цивільних ідентичностей у ситуації ідеологічної невизначеності;

– відсутність політичної суб'єктності;

– тінізація економіки [18, с. 15].

Таким чином, у роботі, підготовленій ще в 2006 р., майже повністю було передбачено те, що відбувається в Україні зараз. Нездатність влади вчасно ідентифікувати ці чинники, неспроможність центральних органів виконавчої влади до реалізації державної кібербезпекової політики призводять до того, що наведені чинники трансформуються в стійкі та сталі тенденції розвитку, що згодом створює небезпечні умови для кібернетичної маргіналізації всього українського суспільства.

Корисним і правильним у цьому контексті є виділення А.Л. Свящуком видів небезпек від маргіналізації *на рівні суспільних одиниць* (розкол єдиного соціокультурного простору на слабко інтегровані різнорідні сегменти, а також політична нестабільність і дисфункціональні збої в суспільній системі) та *на рівні індивідів* (випадання індивіда із соціальної взаємодії, а також руйнівна здатність деформувати особистість у результаті тривалого перебування в маргінальному стані) [18, с. 15].

Я вже неодноразово в роботах із використанням різноманітних як за змістом та характером, так і за рівнем аргументів обґрунтовував той факт, що в Україні, незважаючи на проголошений курс щодо підвищення кібербезпеки, на формування національної кібербезпеки, говорити про справжні засади кібербезпекової політики поки що не варто [9–14]. Навіть сама назва Закону України «Про основні засади забезпечення кібернетичної безпеки України» свідчить про втрату українським законодавцем, насамперед авторами текстів законів, розуміння значення ключових термінів. Адже засади не можуть бути основними чи неосновними, як і не можуть існувати закономірності принципів. Маргінальність сьогодні стає визначальним чинником насамперед інтелектуального складника формування нормативно-правових актів у сфері кібербезпеки, тому наша роль як наукової спільноти має трансформуватись не лише у формування наукових концепцій, а й у створення реальних механізмів реалізації цих гіпотез, унеможливлення викривлення історичних традицій і наукового підходу в державному управлінні.

Більшість учених тиражують методологічну помилку дослідників інформаційної безпеки та аналізують кібернетичну безпеку поза контекстом державної кібернетичної політики, тобто аналізують кібербезпекову політику як окремий складник державної політики.

Більше того, за сучасних умов замало робіт, у яких проблематика кібернетичної маргіналізації розглядалася б у контексті загрози кібернетичній безпеці. Адже в більшості досліджень ці загрози під різним кутом подаються, виходячи з уже наявних і легітимованих загроз, чітко визначених у Стратегії кібербезпеки України, Доктрині інформаційної безпеки України, Стратегії національної безпеки України, Стратегії розвитку інформаційного суспільства тощо.

Однак через такий підхід залишаються осторонь важливі проблеми зв'язку кібернетичної політики та кібернетичної безпеки, зумовленість напрямів кібербезпеки інтересами кібернетичної політики, а не інтересами самої кібербезпеки. Тому можемо спостерігати досить чітко виражені фрустрації дослідників у контексті аналітичного осмислення методологічних і концептуальних засад формування державної кібернетичної політики, що загалом позначається також на рівні підготовлених текстів відповідальними особами як щодо щорічного послання Президента України, так і в наукових та аналітичних доповідях Національного інституту стратегічних досліджень, які лягають в основу формування текстів законодавчих актів у цій сфері.

Аналіз наведених та інших робіт уможливлює постановку висновку про те, що інформаційна маргіналізація створює рушійні передумови до кібернетичної десуверенізації всієї соціальної системи. У цьому розрізі проблема правового регулювання державної кібербезпекової політики висуває на перше місце питання сталого поступу держави в річище кібербезпекової реальності на умовах збереження кібернетичного суверенітету, кібернетичної демаргіналізації та закладення основ для реалізації національних інтересів у кіберпросторі.

Розуміння коріння формування коректного алгоритму управління приведе не до побудови теоретичної моделі державної кібербезпекової політики, а до формування практичних напрямів створення кібербезпекового балансу між тенденціями розвитку та збереженням суттєво важливих параметрів системи за умови впливу чинників різної природи.

Неперсічну роль у формуванні й збереженні такого балансу, особливо в контексті визначення аксіологічних, онтологічних, феноменологічних, гносеологічних, методологічних, епістемологічних та ідеологічних засад, відіграє робота В.М. Семиколенова *«Мораль в інформаційному суспільстві»*, у якій здійснено філософське дослідження проблеми впливу інформаційного суспільства на мораль як на основний механізм регуляції індивідуальної й соціальної дії, з'ясовано специфіку буття моралі в інформаційному суспільстві, визначається роль моральної рефлексії в протистоянні інформаційному маніпулюванню свідомістю, роль інформаційної еліти у формуванні моралі, вплив процесів глобалізації на мораль [19].

Названа праця може бути джерельною базою для подальшого розроблення теми та формування моральної парадигми кібернетичного суспільства [19, с. 12]. У контексті мого дослідження зазначені напрацювання можуть бути використані під час вивчення кібернетичної культури та кіберсвідомості як чинників, що впливають на засади кібернетичної політики, оскільки аморальна кібернетична політика

завжди стає підґрунтям інформаційного протиборства та гібридної війни.

З урахуванням найважливіших компетентностей майбутнього (таких як комунікація, креативність, кооперація, критичне мислення) маємо прийняти думку про те, що штучний інтелект виступатиме суб'єктом правових відносин у кібернетичній сфері, а кібернетична влада прийде на зміну владі в традиційному розумінні.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Стратегічні комунікації : [словник] / [Т.В. Попова, В.А. Ліпкан] ; за заг. ред. В.А. Ліпкана. – К. : ФОП Ліпкан О.С., 2016. – 416 с.
2. Ліпкан В.А. Національна і міжнародна безпека у визначеннях та поняттях / В.А. Ліпкан, О.С. Ліпкан. – 2-е вид., доп. і перероб. – К. : Текст, 2008. – 400 с.
3. Ліпкан В.А. Національна безпека України : [навч. посібник] / В.А. Ліпкан. – 2-ге вид. – К. : КНТ, 2009. – 576 с.
4. Ліпкан В.А. Інформаційна безпека України в умовах євроінтеграції : [навч. посібник] / В.А. Ліпкан, Ю.Є. Максименко, В.М. Желіховський. – К. : КНТ, 2006. – 280 с.
5. Рудник Л.І. Право на доступ до інформації : дис. … канд. юрид. наук : спец. 12.00.07 / Л.І. Рудник ; Нац. ун-т біоресурсів і природокористування України. – К., 2015. – 247 с.
6. Рудник Л.І. Роль та місце стратегічних комунікацій в сучасному суспільстві знань / Л.І. Рудник [Електронний ресурс]. – Режим доступу : http://goal-int.org/rol-ta-mistse-strategichnih-komunikatsij-v-suchasnomu-suspilstvi-znan/.
7. Лахно В.А. Побудова адаптивної системи розпізнавання кіберзагроз на основі нечіткої кластерізації ознак / В.А. Лахно // Восточно-Европейский журнал передовых технологий. – 2016. – № 2(9). – С. 18–25.
8. Панченко В.М. Зарубіжний досвід формування систем захисту критичної інфраструктури від кіберзагроз / В.М. Панченко // Інформаційна безпека людини, суспільства, держави: науково-практичний журнал. – К., 2012. – № 3(10). – С. 100–109.
9. Діордіца І.В. Поняття та зміст кіберзлочинності / І.В. Діордіца [Електронний ресурс]. – Режим доступу : http://goal-int.org/ponyattya-ta-zmist-kiberzlochinnosti/.
10. Діордіца І.В. Сучасний кібертероризм: аспекти правового регулювання / І.В. Діордіца [Електронний ресурс]. – Режим доступу : http://goal-int.org/suchasnij-kiberterorizm-aspekti-pravovogo-regulyuvannya/.
11. Діордіца І.В. Система забезпечення кібербезпеки: сутність та призначення / І.В. Діордіца [Електронний ресурс]. – Режим доступу : http://goal-int.org/sistema-zabezpechennya-kiberbezpeki-sutnist-ta-priznachennya/.
12. Діордіца І.В. Поняття та зміст кіберзагроз на сучасному етапі / І.В. Діордіца [Електронний ресурс]. – Режим доступу : http://goal-int.org/ponyattya-ta-zmist-kiberzagroz-na-suchasnomu-etapi/.
13. Діордіца І.В. Кібертероризм як елемент дестабілізації системи стратегічних комунікацій / І.В. Діордіца [Електронний ресурс]. – Режим доступу : http://goal-int.org/kiberterorizm-yak-elementi-destabilizacii-sistemi-strategichnix-komunikacij/.
14. Діордіца І.В. Поняття та зміст кібершпигунства / І.В. Діордіца [Електронний ресурс]. – Режим доступу : http://goal-int.org/ponyattya-ta-zmist-kibershpigunstva/.
15. Каращук М.Г. Інформаційна влада як чинник демократизації сучасного суспільства : дис. … канд. політ. наук : спец. 23.00.02 «Політичні інститути та процеси» / М.Г. Каращук ; Київський нац. ун-т ім. Т. Шевченка. – К., 2006. – 171 с.
16. Правові засади розвитку інформаційного суспільства в Україні : [монографія] / [В.А. Ліпкан, І.М. Сопілко, В.О. Кір'ян] / за заг. ред. В.А. Ліпкана. – К. : ФОП Ліпкан О.С., 2015. – 664 с.
17. Кір'ян В.О. Правові засади розвитку інформаційного суспільства в Україні : дис. … канд. юрид. наук : спец. 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право» / В.О. Кір'ян ; Нац. авіаційний ун-т. – К., 2014. – 252 с.
18. Свящук А.Л. Феномен маргінальності в генезисі сітьового суспільства : дис. … канд. філос. наук : спец. 09.00.03 «Соціальна філософія та філософія історії» / А.Л. Свящук ; Харківський ун-т Повітряних Сил ім. І. Кожедуба. – Х., 2006. – 200 с.
19. Семиколенов В.М. Мораль в інформаційному суспільстві : дис. … канд. філос. наук : спец. 09.00.04 «Філософська антропологія, філософія культури» / В.М. Семиколенов ; Таврійський нац. ун-т ім. В.І. Вернадського. – Сімферополь, 2006. – 212 с.
20. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовтня 2017 р. № 2163-VIII // Відомості Верховної Ради України. – 2017. – № 45. – Ст. 403.

Діордіца І.В. НАУКОВА РЕФЛЕКСІЯ СТАНОВЛЕННЯ КІБЕРВЛАДИ В УКРАЇНІ

Автором статті проаналізовано особливості формування й реалізації державної політики у сфері кібербезпеки. Особливу увагу приділено працям українських дослідників (таких як В.А. Ліпкан, Л.І. Рудник, В.А. Лахно, В.М. Панченко). Виявлено сутність кібернетичної влади, визначено основні цілі, напрями й принципи державної політики, а також умови результативного розвитку кіберсуспільства в Україні.

Ключові слова: державна політика, кібервлада, кібербезпека, кібербезпекова політика, кіберпростір, глобалізація, інтеграція, інформаційне суспільство.

Диордица И.В. НАУЧНАЯ РЕФЛЕКСИЯ СТАНОВЛЕНИЯ КИБЕРВЛАСТИ В УКРАИНЕ

Автором статьи проанализированы особенности формирования и реализации государственной политики в сфере кибербезопасности. Особое внимание уделено работам украинских исследователей (таких как В.А. Липкан, Л.И. Рудник, В.А. Лахно, В.М. Панченко). Выявлена сущность кибернетической власти, определены основные цели, направления и принципы государственной политики, а также условия результативного развития киберобщества в Украине.

Ключевые слова: государственная политика, кибервласть, кибербезопасность, кибербезопастностная политика, киберпространство, глобализация, интеграция, информационное общество.

Diorditsa I.V. SCIENTIFIC REFLECTION OF FORMATION OF CYBER POWER IN UKRAINE

The author of the article analyzes the features of the formation and implementation of state policy in the field of cybersecurity. Particular attention is paid to the work of Ukrainian researchers (in particular V.A. Lipkan, L.I. Rudnik, V.A. Lakhno, V.M. Panchenko). The essence of cybernetic power is revealed; the main goals, directions and principles of state policy are defined; conditions for the effective development of cyber-society in Ukraine.

Key words: state policy, cyber-law, cybersecurity, cyber-spam policy, cyberspace, globalization, integration, information society.