

В. М. Роллер

ад'юнкт
Військового інституту
Київського національного університету імені Тараса Шевченка

ВПЛИВ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА НА ЕФЕКТИВНІСТЬ АДМІНІСТРАТИВНО-ПРАВОВОГО РЕГУЛЮВАННЯ КІБЕРБЕЗПЕКИ ДЕРЖАВИ

Суспільні відносини у сфері інформаційних технологій та в кіберсфері органічно розвиваються відповідно до вимог часу. Але водночас правового регулювання як на міжнародному, так і на державному рівнях не вистачає для вирішення всіх правових питань у сфері використання інформаційних технологій. Поруч із виробленням правил приватного використання інформаційно-комунікаційних технологій постають питання використання останніх органами державної влади, питання здійснення захисту від кібератак і співпраці між державним та приватним секторами в цій сфері. Необхідне вироблення механізмів адміністративно-правового регулювання кібербезпеки.

Ключові слова: громадянське суспільство, кіберзахист, адміністративно-правове регулювання кібербезпеки.

Постановка проблеми. Питання кібератак на ресурси державних та приватних організацій є одним з актуальних. Приватні організації і державні органи однаково страждають від впливу хакерів, кібершпигунів та кібердиверсій. Різняться ж значущість наслідків: для приватних компаній в основному це матеріальні збитки, тоді як для органів державної влади – ризик завдання шкоди державі та громадянам.

Об'єктивною реальністю є те, що приватні компанії й організації випередили органи державної влади у сфері захисту від кібератак та їх відбиття. Причиною такої ситуації є низка об'єктивних чинників: краща матеріально-технічна база, краще фінансування, зацікавленість компаній у власній репутації та збереженні комерційної таємниці.

Але водночас кіберпростір є неподільним, а кібератаки можуть здійснюватися одночасно і на приватні організації і на органи державної влади. На даний момент в Україні адміністративно-правові механізми взаємодії органів державної влади та приватного сектора лише починають формуватися. Через неподільність і пов'язаність кіберпростору дуже важливою є участь суспільства в процесі формуван-

ня адміністративно-правових механізмів кіберзахисту.

Аналіз останніх досліджень і публікацій. Проблему взаємозв'язку між розвитком громадянського суспільства та адміністративно-правовими механізмами досягнення кібербезпеки розглянуто не ґрунтовно, проте окремі питання, які стосуються громадянського суспільства чи адміністративно-правового регулювання гарантування кібербезпеки, розглядаються багатьма авторами. Так, питання правового регулювання кібербезпеки та протидії кіберзлочинності вивчають О. Баранов, Ю. Батурина, П. Біленчук, Д. Дубов, О. Орлова й інші. Питання функціонування громадянського суспільства розглядають О. Ременець, М. Бойчук, О. Чувардинський. Взаємозв'язок громадянського суспільства та Збройних сил України у своїй монографії розглядає І. Коропатнік.

Метою статті є проведення аналізу питань функціонування громадянського суспільства в державі та встановлення взаємозалежності між рівнем розвитку громадянського суспільства та виробленням ефективних механізмів адміністративно-правового регулювання.

Виклад основного матеріалу. До питань кібербезпеки. Президент Європейської комісії Жан-Клод Юнкер назвав

кібербезпеку ключовим пріоритетним напрямом у 2018 р. Він визначив кіберзагрози таким же важливим питанням, як і зміни в кліматі, міграційні питання та питання захисту кордонів. Європейською комісією запропоновано введення єдиних технічних стандартів визначення кіберзагроз, які учасники мають ухвалити добровільно [1].

Така зацікавленість проблемою в міжнародній спільноті вказує на її значущість і необхідність пошуку шляхів вирішення.

Для України як держави, що перебуває в стані збройного конфлікту з Російською Федерацією; держави, частину територій якої анексовано та проти якої ведеться інформаційна війна, питання формування адміністративно-правових механізмів гарантування кібербезпеки є надзвичайно актуальним.

Основу формування адміністративно-правового механізму закладають нормативно-правові акти, що на рівні держави регулюють правовідносини у сфері кібербезпеки.

Основними нормативно-правовими актами у сфері кібербезпеки України є Стратегія кібербезпеки України, ухвалена 2016 р., та Закон України «Про основні засади забезпечення кібербезпеки України» від 2017 р., який набув чинності в травні 2018 р. Отже, законодавство у сфері кібербезпеки України є досить «молодим». Крім того, Україна є учасницею Конвенції про кіберзлочинність, яку ратифікувала 2005 р. Але всі ці нормативно-правові акти визначають основні *принципові положення* гарантування кібербезпеки, повноваження органів державної влади, але не визначають чітких адміністративно-правових схем взаємодії між органами влади, а також між останніми із громадянським суспільством.

Якщо звернутися до Стратегії кібербезпеки України [2], то вже в перших рядках тексту можна побачити, що законодавець розуміє, що «відкритий та вільний кіберпростір розширює свободу і можливості людей, збагачує суспільство, <...> стимулює відповідальну та ефективну роботу влади і *активно залучення громадян до управління державою* та вирішення питань місцевого значення, забезпечує пу-

блічність та прозорість влади». Водночас у Стратегії кібербезпеки України зазначено загрози, які виникають із доступом до кіберпростору: хакевізм, кібершпигунство, кібердиверсії й інше.

Отже, нормотворець чітко розуміє не тільки всі привілеї, які надає кіберпростір, але і загрози, які в ньому існують. Метою стратегії визначено створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави.

Крім того, одними з основних принципів, на яких має базуватися механізм кібербезпеки в державі, відповідно до Стратегії кібербезпеки України, визначені державно-приватне партнерство, широка співпраця із громадянським суспільством у зазначеній сфері. *Отже, громадянське суспільство визначено одним з основних учасників відносин щодо гарантування кібербезпеки. І таке визначення, на нашу думку, є дуже влучним, оскільки головною відмінністю сфери правового регулювання кібербезпеки від інших є те, що розвиток приватного сектора використання інформаційно-комунікаційних технологій (далі – ІКТ) відбувається набагато швидше та динамічніше, ніж публічного.*

Визначення терміна «кібератака» в українському законодавстві надано в Законі «Про основні засади забезпечення кібербезпеки України».

Але необхідно зазначити, що досліджуване питання є нагальним не тільки для України, але і для більш розвинених держав Європи та світу загалом. Пов'язано це з необмеженістю кіберпростору та відсутністю державних кордонів у всесвітній мережі. Така ж ситуація склалася щодо державних та приватних користувачів у кіберпросторі. Адже приватний користувач з однієї держави може здійснити кібератаку чи вдатися до кібершпигунства стосовно державних органів іншої країни.

У тексті Стратегії кібербезпеки України немає визначення термінів «кібербезпека», «кіберзагроза». Лише опосередковано зазначено: «Забезпечення кібербезпеки України як стану захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі,

що досягається комплексним застосуванням сукупності правових, організаційних, інформаційних заходів». Згадані терміни визначено в Законі України «Про основні засади забезпечення кібербезпеки України» від 2017 р. (далі – Закон про кібербезпеку) [3].

Кібербезпека визначається як захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України в кіберпросторі. Отже, заходи з кібербезпеки покликані захищати в кіберпросторі передусім людину і громадянина, а вже потім суспільство і державу.

Крім того, у Законі про кібербезпеку зазначено необхідність забезпечення сталого розвитку інформаційного суспільства, тобто суспільства нового типу, що формується у результаті глобальної соціальної революції та породжується вибуховим розвитком і конвергенцією інформаційних та комунікаційних технологій [4, с. 3].

Щодо міжнародної спільноти. Ще 1997 р. проблеми кіберзлочинності обговорювалися у форматі міністрів юстиції та внутрішніх справ від представників G8, а у квітні 2013 р. – у Лондоні вже відбулася зустріч міністрів закордонних справ, на якій чимало часу було відведено дискусіям із проблем кібербезпеки. Було констатовано, що в боротьбі з кіберзлочинністю більшими мають бути спільні зусилля держав, бізнесу та громадянського суспільства [5, с. 172].

Отже, у міжнародних документах та у внутрішньому законодавстві України питання кіберзахисту тісно пов'язують із наявністю інформаційного та громадянського суспільства, взаємодією із цим суспільством та його захистом під час протидії кібератакам.

Тому ми вважаємо за необхідне більш детально розглянути зв'язок громадянського суспільства та стану кіберзахисності держави.

Щодо питань громадянського суспільства. У теорії права громадянське

суспільство визначається як певна сукупність людей, яка утворюється на засадах визначених спільних інтересів та взаємного співробітництва. Але варто пам'ятати, що робочий колектив чи група студентів не можуть вважатися суспільством, оскільки за своїми чисельними й якісними показниками не підпадають під таку категорію. Окреме суспільство формується на території певної держави на основі політичних, економічних та соціальних чинників, які напряму впливають на рівень його розвитку.

Як стверджував Ч. Тейлор, «кожне політичне суспільство потребує певних жертв і певної дисципліни з боку його членів – вони повинні платити податки або служити в армії й узагалі зазнавати певних обмежень. Щоб зробити суспільство вільним, цей примус необхідно змінити на інше. Це може бути тільки «добровільне ототожнення громадян із полісом, відчуття того, що політичні інститути в їхньому товаристві є вираженням їх самих» [6, с. 16]

Ця думка охоплює два протилежні погляди на громадянське суспільство: як суспільство, яке потребує покірності та жертв, або як суспільство, яке потребує свідомого вибору й активних дій.

На нашу думку, громадянське суспільство має характеризуватися як суспільство вільних, свідомих та активних жителів (громадян), які небайдуже ставляться до подій, які відбуваються навколо них, у державі як політичному обрамленні цього суспільства.

Відомо, що суспільство відділене від держави та функціонує дотично до неї. Залежно від того, наскільки суспільство є розвиненим, громадянським, воно зможе побудувати відповідну державу.

І. Коропатнік у своїй монографії зазначає: «Незважаючи на існуюче, на перший погляд, різноманіття визначень громадянського суспільства, у цілому як його змістову ознаку виокремлюють діяльність незалежних від держави добровільних об'єднань громадян, спрямованих на реалізацію спільних інтересів у різних сферах суспільного життя. Але водночас неможливо не звернути увагу на те, що більшістю з них, як правило, не береться до уваги такий складник, як економічна

незалежність громадян від держави, тобто наявність вільного підприємництва та ринкової економіки» [6, с. 20].

Отже, громадянське суспільство функціонує всередині держави, співпрацює з державою, впливає на рішення органів державної влади, базується на принципах вільної ринкової економіки, а зовнішніми формами прояву громадянського суспільства є: функціонування громадських та благодійних організацій, активний прояв громадянської позиції членами суспільства у вирішенні питань державного значення, волонтерські рухи та громадські ради при органах державної влади й інші форми, перелік яких не може бути вичерпним.

У підсумку не можна не погодитися з думкою Л. Новосколькової, яка підкреслює: «Громадянське суспільство створює демократичну державу, а не навпаки» [7, с. 62].

До питань адміністративно-правового регулювання гарантування кібербезпеки. На даний час в українському законодавстві відсутні норми, які б формували механізм адміністративно-правової взаємодії між органами державної влади та суспільством у сфері кібербезпеки.

Правовий інститут взаємодії органів державної влади та громадянського суспільства є досить новим для України, оскільки наше суспільство переживає перехідний період, а громадянське суспільство неформоване. Але водночас українське суспільство можна назвати інформаційним, оскільки, відповідно до даних соціологічних досліджень, 67% жителів України мають підключення до мережі Інтернет у власних помешканнях [8]. Крім того, в Україні достатньо розвинена мережа точок підключення безпроводного інтернету (Wi-Fi) у місцях загального користування, громадському транспорті, на зупинках, у закладах харчування та навіть на деяких станціях метрополітену. І здебільшого підключення до цих мереж не потребує реєстрації або сплати коштів за користування.

Отже, з одного боку, інформатизація державних органів, створення системи електронного урядування, введення медичної системи e-health, з іншого – активне використання громадянами інтернету

та різноманітних інформаційних ресурсів, велика кількість фахівців IT-сфери, вказують на необхідність врегулювання державно-приватних відносин у цій галузі, вироблення адміністративно-правових механізмів досягнення кібербезпеки.

Адміністративно-правове регулювання необхідно розуміти як процес застосування державними органами влади спеціальних методів впливу на суспільні відносини з метою досягнення певного результату в конкретній сфері їхнього розвитку.

З огляду на доцільність використання принципів позитивного права під час визначення поняття адміністративно-правового регулювання, І. Шопіна розглядає його як адміністративно-правовий вплив на суспільні відносини, який здійснюється за допомогою комплексу адміністративно-правових засобів та інших правових явищ, які в сукупності становлять механізм адміністративно-правового регулювання [9, с.142].

Відповідно до аналітичної доповіді до щорічного послання Президента України до Верховної Ради України «Про внутрішнє та зовнішнє становище України у 2017 р.», у сфері застосування ІКТ актуальним залишається виконання принаймні трьох «стартових» фундаментальних завдань, а саме: 1) оптимізації державного управління та регулювання галузю; 2) максимально можливого вивільнення приватної ініціативи і використання потенціалу інноваційного розвитку та міжнародного співробітництва; 3) модернізації системи профільної освіти й кадрового менеджменту [10, с. 651].

Як найгостріше питання виділено розроблення адміністративно-правових механізмів у сфері регулювання об'єктів критичної інфраструктури.

Оскільки тільки держава має повноваження на вироблення саме адміністративно-правових механізмів взаємодії із приватним сектором, то ці механізми мають бути розроблені так, щоб зберегти баланс між захистом інтересів держави та непорушенням законних прав осіб та організацій, які діють у сфері використання та застосування ІКТ.

У результаті аналізу законодавства, що регулює питання кібербезпеки, можна

виділити декілька напрямів, в яких необхідно виробити адміністративно-правові механізми взаємодії між державним і приватним секторами.

Одним із таких напрямів є обмін інформацією про кібератаки та кіберінциденти.

На даний момент в українському законодавстві закріплено принципи добровільної співпраці в цьому напрямі, але водночас необхідно пам'ятати досвід Сполучених Штатів Америки (далі – США), де 2015 р. Затверджено Cybersecurity Information Sharing Act (CISA) – документ, який визначає порядок надання органам державної влади інформації про кібератаки, зокрема інтернет-трафік та відомості про користувачів, що спричинило бурю невдоволення в суспільстві [11]. Через побоювання компаній через те, що до органів державної влади може потрапити інформація про приватне життя користувачів.

Отже, виробляти механізм обміну інформацією про кіберінциденти доцільно добровільним порядком, тобто здійснювати регулювання не на рівні окремих відомств, а на рівні держави.

Ще одним механізмом адміністративно-правової взаємодії є запровадження порядку впровадження аудиту інформаційної безпеки на об'єктах національної критичної інформаційної інфраструктури, встановлення вимог до аудиторів інформаційної безпеки і визначення порядку їх атестації. Але такий механізм, на нашу думку, не буде прийнятий суспільством, оскільки в такому разі надаються широкі повноваження органам державної влади. Про це йдеться в аналітичній доповіді Інституту стратегічних досліджень «Актуальні питання розвитку державно-приватної взаємодії у сфері забезпечення кібербезпеки в Україні» [12, с. 4], де підкреслено: «Державна служба спеціального зв'язку та захисту інформації України визначальною мірою контролює створення та діяльність інституту аудиторів (включаючи незалежних), формування вимог до проведення аудиторських перевірок і сертифікації об'єктів критичної інфраструктури, а Служба безпеки України має право негласно перевіряти готовність таких об'єктів до можливих кібератак та кіберінцидентів».

Крім того, необхідно пам'ятати про необхідність налагодження з боку держави діалогу із приватним сектором та розроблення відповідних адміністративно-правових механізмів у цій сфері. Такі механізми доцільно впроваджувати в межах окремих відомств шляхом організації комунікації із суспільством, організації круглих столів, громадських рад при відомствах.

Щодо впливу громадянського суспільства на розвиток адміністративно-правового механізму. Суспільство України, на нашу думку, ще не можна віднести до громадянського. Це пов'язано як з історичними подіями, тим, що держава є відносно молодою та перебуває в стадії становлення, так і з ідеологією минулого, яка не заохочувала залучення громадян до управління державними процесами. Але водночас українці є активними користувачами ІКТ, зокрема інтернет-ресурсами та мобільним зв'язком. Але говорити про наявність інформаційного суспільства в державі занадто рано.

Вважаємо, що побудові здорового інформаційного суспільства має передувати функціонування сталого громадянського суспільства.

Із 2014 р. дотепер наявне поживлення в суспільному житті українців, що здебільшого пов'язане із проведенням антитерористичної операції на сході України та операції об'єднаних сил (із 2018 р.). Проявами громадянського суспільства стали численні волонтерські рухи на підтримку Збройних сил України й організації добровольчих батальйонів, готових виступити на захист держави.

Під час розгляду питання впливу громадянського суспільства на формування адміністративно-правових механізмів регулювання кібербезпеки можна визначити декілька закономірностей. Чим краще розвинене громадянське суспільство, тим легше воно сприймає певні розумні обмеження, які держава має запровадити для захисту національних інтересів та прав громадян, тим легше воно йде на діалог з органами державної влади, а не лише критикує їх. Чим краще розвинене громадянське суспільство, тим більше пропозицій воно може надати органам державної

влади щодо поліпшення їхньої роботи, тим активнішим та раціональнішим є його контроль за діяльністю та рішеннями органів державної влади.

Отже, саме від рівня усвідомлення громадянами власної сили та можливості впливати на рішення органів державної влади, від небайдужості до подій, що відбуваються навколо, залежить рівень добробуту в суспільстві.

Необхідно ще раз наголосити на важливості активної участі представників громадськості у вирішенні питань формування адміністративно-правового механізму регулювання кібербезпеки, оскільки ця сфера суспільних відносин має деякі особливості, пов'язані з використанням особистої інформації громадян, доступу до даних. Отже, з боку держави можуть вживатися заходи щодо обмеження прав та інтересів окремих громадян для безпеки всієї держави.

Висновки і пропозиції. У результаті аналізу зазначеної в статті інформації можна дійти таких висновків: громадянське суспільство в Україні перебуває на стадії формування; для формування інформаційного суспільства необхідна наявність громадянського суспільства, проте українці є активними користувачами ІКТ та інтернету; на даний час українське законодавство у сфері гарантування кібербезпеки є «молодим», закладає основоположні принципи здійснення кіберзахисту, визначає основні функції органів державної влади в цій галузі; взаємодія держави та громадянського суспільства визначена українським законодавством як один із принципів гарантування кібербезпеки держави; актуальним питанням залишається питання державно-приватного партнерства у досліджуваній області; сьогодні не вироблено адміністративно-правових механізмів взаємодії органів державної влади та громадянського суспільства щодо кібербезпеки; взаємодія та співпраця держави та громадян у сфері гарантування кібербезпеки держави дуже важлива, оскільки кіберпростір є неподільним, а багато об'єктів критичної інформаційної інфраструктури перебувають у приватній власності; оскільки механізми адміністративно-правового регулювання

впроваджує саме держава, в інтересах громадянського суспільства брати участь у формуванні цих механізмів; якість вироблених адміністративно-правових механізмів регулювання кібербезпеки держави напряму залежить від активності громадянського суспільства та його впливу на рішення в цій сфері.

З таких висновків можна виробити пропозицію про активне залучення органами державної влади громадськості до участі у формуванні механізмів адміністративно-правового регулювання кібербезпеки держави. На нашу думку, найлегше зробити це на рівні окремих відомств залежно від їхніх функцій і повноважень у цій сфері. Залучення може відбуватися шляхом проведення консультацій та круглих столів, обговорення проектів нормативно-правових актів.

Список використаної літератури:

1. Єврокомісія визначила п'ять пріоритетів ЄС на наступний рік. Українська правда. URL: <https://www.eurointegration.com.ua/news/2017/09/13/7070901/> (дата звернення: 18.06.2018).
2. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 р. «Про Стратегію кібербезпеки України»: Указ Президента України від 15 березня 2016 р. № 96/2016. URL: <http://zakon5.rada.gov.ua/laws/show/96/2016> (дата звернення: 18.06.2018).
3. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 р. № 2163-VIII. URL: <http://zakon2.rada.gov.ua/laws/show/2163-19> (дата звернення: 18.06.2018).
4. Івлєв О. Засади правового регулювання розвитку інформаційного суспільства в Європі: досвід для України. Державне управління та місцеве самоврядування: історія та сучасність: збірник тез науково-практичної конференції за підсумками стажування слухачів 26 вересня 2012 р. URL: <http://kbuapa.kharkov.ua/e-book/conf/2012-2/doc/5/04.pdf> (дата звернення: 20.06.2018).
5. Дубов Д. Кіберпростір як новий вимір геополітичного суперництва: монографія. Київ, 2014. URL: http://www.niss.gov.ua/content/articles/files/Dubov_mon-89e8e.pdf (дата звернення: 21.06.2018).
6. Коропатнік І. Взаємодія громадянського суспільства і Збройних сил України:

- адміністративно-правові засади: монографія. К., 2016. 412 с.
7. Новоскольцева Л. Специфіка моделювання правового поля діяльності громадських рухів. Актуальні проблеми взаємодії громадянського суспільства і Збройних сил України: збірник матеріалів Міжнар. наук.-практ. конф. / за заг ред. О. Караман та ін. Старобільськ, 2015. С. 62–64.
 8. Матеріали соціологічних досліджень, травень 2018 р. / Factum Group Ukraine. URL: <http://inau.ua/proekty/doslidzhennya-internet-audytoriyi> (дата звернення: 19.06.2018).
 9. Шопіна І. Адміністративно-правове регулювання управління органами внутрішніх справ України: дис. ... докт. юрид. наук: 12.00.07. К., 2012. 514 с.
 10. Про внутрішнє та зовнішнє становище України у 2017 р.: аналітична доповідь до щорічного послання Президента України до Верховної Ради України. К.: НІСД, 2017. 928 с. URL: http://www.niss.gov.ua/public/File/book_2017/Poslanya_druk_fin.pdf (дата звернення: 21.06.2018).
 11. Cybersecurity Information Sharing Act (CISA) // Wikipedia: the free encyclopedia. URL: https://en.wikipedia.org/wiki/Cybersecurity_Information_Sharing_Act (дата звернення: 04.07.2018).
 12. Гнатюк С. Актуальні питання розвитку державно-приватної взаємодії у сфері забезпечення кібербезпеки в Україні: аналітична записка. URL: <http://www.niss.gov.ua/content/articles/files/kiberbezpek-d3e61.pdf> (дата звернення: 18.06.2018).

Роллер В. Н. Влияние гражданского общества на эффективность административно-правового регулирования кибербезопасности государства

Общественные отношения в сфере информационных технологий и в киберсфере органично развиваются в соответствии с требованиями времени. Но правового регулирования как на международном, так и на государственном уровнях недостаточно для решения всех правовых вопросов, возникающих в сфере использования информационных технологий. Наряду с выработкой правил частного использования информационно-коммуникационных технологий возникают вопросы использования последних органами государственной власти, осуществления защиты от кибератак, налаживания сотрудничества между государственным и частным сектором в этой сфере. Необходимо выработать механизмы административно-правового регулирования кибербезопасности.

Ключевые слова: гражданское общество, киберзащита, административно-правовое регулирование кибербезопасности.

Roller V. The Civil Society influence on the efficiency of the administrative and legal regulation of the State cyber security

Public relations in the field of information technologies and in the cyber sphere are organically developed in accordance with the requirements of time. But at the same time the legal regulations that exist, both at the international and national level, are not enough to resolve all legal issues arising in the area of information technology use. Along with the development of rules for the private use of information and communication technologies (ICTs), there are questions about the use of ICT by public authorities, the issue of protection against cyberattacks and cooperation between the public and private sectors in this area. One of the important issues is the need to develop mechanisms for the administrative and legal regulation of cyber security.

Key words: civil society, cyber defense, administrative-legal regulation of cybersecurity.