України; 2) що мають вирішуватися в порядку кримінального судочинства; 3) про накладення адміністративних стягнень, крім випадків, визначених цим Кодексом; 4) щодо відносин, які відповідно до закону, статуту (положення) громадського об'єднання, саморегулівної організації, віднесені до його (її) внутрішньої діяльності або виключної компетенції, крім справ у спорах, визначених пунктами 9, 10 частини першої цієї статті.

Отже, як бачимо, зважаючи на судову практику, до переліку публічно-правових спорів пропонується віднести спори щодо оскарження рішень атестаційних, конкурсних, медико-соціальних експертних комісій та інших подібних органів, рішення яких є обов'язковими для органів державної влади, органів місцевого самоврядування, інших осіб; спори щодо формування складу державних органів, органів місцевого самоврядування, обрання, призначення, звільнення їх посадових осіб (стаття 19 нової редакції КАСУ).

Відповідно до нових правил юрисдикції та підсудності, запропонованих законопроектом № 6232 від 23.03.2017, юрисдикція між загальними, господарськими та адміністративними судами розмежовується залежно, в першу чергу, від предмета спору (в залежності від змісту спірних відносин), а не суб'єктного складу сторін.

Отже, з метою попередження юрисдикційних спорів та «дублювання» цивільних, господарських, адміністративних справ вводиться поняття «похідних вимог», які в окремих випадках можуть бути об'єднані з основними, навіть, якщо окремо вони мали б розглядатися за різними правилами судочинства. Також до кодексів включено низку механізмів, які мають запобігати маніпуляціям з визначенням підсудності.

УДК 34:004(043.2)

Сопілко І. М., д.ю.н., доцент,
Національний авіаційний університет, м. Київ, Україна

ПИТАННЯ КІБЕРБЕЗПЕКИ І ДЕРЖАВНА ІНФОРМАЦІЙНА ПОЛІТИКА

Сучасні процеси інформаційної глобалізації, транспарентності та подальшого розвитку громадянського й інформаційного суспільства несуть різнорівневе навантаження на систему державного управління. У вирії як наукових досліджень, так численних законодавчих актів чимало зусиль слід докласти для оформлення цілісного уявлення про державну інформаційну політику сучасної української держави, становлення механізмів її кореляції із засадами зовнішньої та внутрішньої політики та у зв'язку із виникненням нових викликів, пов'язаних із Інтернетом. Тому,

певним явищам негативного характеру, які мають бути враховані при виробленні засад державної інформаційної політики, слід приділити особливу увагу. Без цього правильне сприйняття інформаційної політики не є повним, не може бути адекватно презентовано в рамках концептуального законодавчого акта, в якому і має бути вона оформлена.

Серед останніх таких явищ є питання забезпечення кібербезпеки в інформаційному просторі. Кібербезпеку можна визначити як стан захищеності кіберпростору держави в цілому або окремих об'єктів її інфраструктури від ризику стороннього кібервпливу, за якого забезпечується їх сталий розвиток, а також своєчасне виявлення, запобігання й нейтралізація реальних і потенційних викликів, кібернетичних втручань і загроз особистим, корпоративним і/або національним інтересам [1, с. 15].

Дедалі частіше об'єктами кібератак та кіберзлочинів стають інформаційні ресурси фінансових установ, підприємств транспорту та енергозабезпечення, державних органів, які гарантують безпеку, оборону, захист від надзвичайних ситуацій. Новітні технології застосовуються не лише для скоєння традиційних видів злочинів, але і для скоєння принципово нових видів злочинів, притаманних суспільству з високим рівнем інформатизації.

Складності розслідування і протидії кіберзлочинності пов'язані із основними властивостями, що притаманні кіберзлочинам, а саме: як правило вони носять інтелектуальний творчий характер, що базується на певній інформаційній базі, можливість їх вчиняти без обмежень віку, статті, національності, фізичних можливостей, проте інтелектуальний характер має бути присутній. Також немає обмежень по віддаленості, в тому числі і щодо держав; транснаціональність та розповсюдженість. Окремо дослідники зазначають, що велика частина подібних злочинів має певну політизованість, адже неврегульованість кіберпростору "розвязує руки" державам-агресорам і таким чином дозволяє їм проводити агресивні дії без оголошення війни і відповідальності за ці дії, а також окремих радикальним ісламських групам.

Починаючи з 80 років минулого століття Рада Європи активно протидії подібним злочинам і сьогодні є певний масив законодавства в зазначеній сфері. Найбільш значним кроком є прийняття Конвенції «Про кіберзлочинність», яка містить норми матеріального права, щодо поняття та видів злочинів в інформаційній сфері та особливості співробітництва держав які до неї приєдналися. До Конвенції було прийнято Додатковий протокол щодо заборони проявів у висловлюваннях щодо расизму та ксенофобії та відповідальності за такі висловлювання, до якого приєдналась і Україна.

Про стан правового забезпечення питання кібербезпеки в Україні свідчить той факт, що 05.10.2017 року був прийнятий ЗУ «Про основні

засади забезпечення кібербезпеки України», що набере чинності 09.05.2018 [2].

Цей Закон визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки та має практичне значення сучасних умовах державотворення.

Метою закону є врегулювання відносин, пов'язаних із забезпеченням кібербезпеки, як складової національної безпеки України, провадженням діяльності із захисту національних інтересів та національних інформресурсів у кіберпросторі, кіберзахистом систем електронних комунікацій органів державної влади та місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до законів України, комунікаційних та технологічних систем, які використовуються критичними інфраструктурними об'єктами, що дасть можливість належно реагувати на сучасні інформаційні виклики.

Також, цей закон чітко визначає об'єкти кібербезпеки і кіберзахисту. Відповідно до закону об'єктами кібербезпеки є: конституційні права і свободи людини і громадянина; суспільство, сталий розвиток інформаційного суспільства та цифрового комунікативного середовища; держава, її конституційний лад, суверенітет, територіальна цілісність і недоторканність; національні інтереси в усіх сферах життєдіяльності особи, суспільства та держави; об'єкти критичної інфраструктури. Відповідно до закону обєктами кіберзахисту є: комунікаційні системи всіх форм власності, в яких обробляються національні інформаційні ресурси та/або які використовуються в інтересах органів державної влади, органів місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до закону; об'єкти критичної інформаційної інфраструктури; комунікаційні системи, які використовуються для задоволення суспільних потреб та/або реалізації правовідносин у сферах електронного урядування, електронних державних послуг, електронної комерції, електронного документообігу [2].

В сучасних умовах розвиток українського законодавства повинен усвідомлювати необхідність розвитку кібернетичних стратегій, що повинні відігравати ключову роль у захисті комп'ютерних систем. Треба розуміти той факт, що тепер ураження комп'ютерних систем вірусними технологіями можна очікувати не тільки від країн з сильним військовим потенціалом, а також від менших країн, що поставлять собі за мету активно розвивати кібернетичні системи. Усі ці загрози сьогодні стали не

лише предметом наукових дискусій, але і елементом нашого інформаційного простору.

Сьогодні однозначно можна сказати, що ні держави, ні інші світові професійні інституції не можуть самостійно боротися в повній мірі із тими викликами, які постали у зв'язку із розширенням Інтернету. До них слід віднести наступні: виклики щодо кіберзлочинності, захист авторського права в мережі, хакерство в економічній та політичних сферах, тощо. Відповіді на них повинні бути дані із врахуванням основних стандартів Ради Європи і практики Європейського Суду з прав людини, які мають стати в законотворчій роботі напрямком щодо реформування законодавства щодо забезпечення інформаційної безпеки України. Особливої актуальності заслуговує питання вдосконалення програмного забезпечення діяльності основних державних інституцій, організацій та підприємств. Паралельно, усе вищевикладене свідчить про потребу прийняття нормативно-правових актів в яких був би передбачений механізм захисту інформаційних прав громадян від протиправних дій третіх осіб щодо інформації та обмеження її впливу на особу, в тому числі і в мережі Інтернет та посили роботу відповідних органів, що відповідають за інформаційну безпеку держави, особливо в такий небезпечний історичних період розвитку держави.

Література

1. Бурячок В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / за заг. ред. д.т.н., проф. В. Б. Толубка. – К.: ДУТ, 2015. – 288 с.

2. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/2163-19.

УДК 34:004(043.2)

Татарінцева А. В., студентка,
Національний авіаційний університет, м. Київ, Україна
Науковий керівник: Гусар О. А., к.ю.н.

КІБЕРБЕЗПЕКА ЯК СКЛАДОВА ЧАСТИНА НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

У процесі розвитку високих технологій виникло принципово нове середовище – кіберпростір, що формується із соціальної, технічної, телекомунікаційної, інформаційної, мережевокомп'ютерної складової частини.

Кіберпростір одночасно виступає як суб'єкт та об'єкт впливу. Сучасна успішна геополітика неможлива без стійкого домінування у кіберпросторі. Кіберборотьба набула стратегічного управлінського спрямування. Вона