сфер (фінансові послуги, транспорт, енергетика, охорона здоров'я), а також компанії, які діють в інформаційному просторі, спільно з державними адміністраціями затверджувати правила поведінки в разі виникнення ризиків для забезпечення безперебійного функціонування комп'ютерних систем і повідомляти про всі інциденти у сфері безпеки щодо послуг, які ними надаються. Для того, щоб зазначені пропозиції вступили в силу, їх має розглянути і прийняти Європейський Парламент. У разі їх затвердження у країн-учасниць ЄС буде 18 місяців на впровадження у життя плану мережевої та інформаційної безпеки.

Завершуючи короткий огляд визначеної проблеми, необхідно зазначити, що неможливо розглянути все різноманіття підходів та досвіду, що накопичений у сфері кібезбезпеки різними країнами світу. В той же час навіть проведений огляд проблеми правового та організаційного забезпечення кібербезпеки свідчить про значні зміни, що відбулись за останні роки у цій сфері.

Зрозуміло, що опрацювання зарубіжного досвіду не означає його прямого перенесення у вітчизняну практику. В той же час це дає можливість сформувати таку модель забезпечення кібербезпеки, яка, з одного боку, більшою мірою відповідатиме потребам України, а з іншого – сприятиме розвитку міжнародного співробітництва, об'єднанню можливостей та зусиль перед спільними загрозами. З цією метою вважаємо необхідним:

- на національному рівні з огляду на прийняття Стратегії національної безпеки розпочати підготовку Стратегії кібернетичної безпеки України;

- сформувати чинне нормативно-правове законодавство в сфері кіберзлочинності, визначити основні поняття у сфері кібербезпеки: «кібербезпека», «критична кіберінфраструктура» та інші, що мають сталий обіг у цій галузі і сутнісне значення для неї;

- на законодавчому рівні чітко визначити розподіл повноважень правоохоронних органів у сфері кібербезпеки. Пропонуємо покласти повноваження щодо кіберзахисту об'єктів критичної кіберінфраструктури на Департамент контррозвідувального захисту інтересів держави у сфері інформаційної безпеки Служби безпеки України, внести відповідні зміни до Закону України «Про Службу безпеки України»;

- закріпити в Законі України «Про кібернетичну безпеку України» визначення критичної інформаційної інфраструктури (або критичної кіберінфраструктури).

Одним із важливих напрямків вдосконалення вітчизняного законодавства у сфері забезпечення національної кібербезпеки слід вважати створення законодавчих засад для розвитку державно-приватного партнерства у сфері кібербезпеки, стимулювання участі приватного сектору у програмах такого партнерства, а також для розвитку та реалізації програм міжнародного співробітництва.

Настюк Василь Якович
завідувач кафедри адміністративного права
та адміністративної діяльності Національного університету
«Юридична академія України імені Ярослава Мудрого»
член-кореспондент НАПрН України
доктор юридичних наук, професор,

Функціонування офіційних відкритих джерел інформації як інструмент протидії корупції в Україні

Кінець XX - початок XXI століття ознаменувався інтенсивним розвитком глобального інформаційного суспільства, що фактично прийшло на зміну постіндустріальному, і становленням нового соціального порядку, в якому основним ресурсом є інформація. Відповідно до сучасних реалій відбувається трансформація і модернізація багатьох суспільних і державних інститутів у бік формування їх інформаційної відкритості та прозорості (транспарентності). Міжнародним, національним і регіональним соціально-політичним трендом, що особливо актуалізувався в останнім часом, стає боротьба за вільний доступ до офіційної інформації та урядових документів. Дане право є необхідною умовою формування інформованості, а також демократичного контролю громадян над владними інститутами з метою формування їх істинної, а не декларативної підзвітності перед населенням. Зміцнюється справедлива віра людей у те, що сутність формальних інститутів, до яких відносяться, в першу чергу, органи державної влади, полягає в публічності і відвертості. Негативна «культура секретності» і відповідний їй «архаїчний» (застарілий) тип мислення, супроводжуючий діяльність багатьох чиновників, повинен повністю викоренитися

з усвідомленням того, що інформація, якою вони користуються, належить громадськості, і громадяни мають повне право на її отримання. З кожним роком більшість держав розробляють і приймають закони, що створюють і гарантують інститут доступу до офіційної інформації, що вносить вирішальний внесок у формування так званої позитивної «культури відвертості». Не дивлячись на те, що законодавство у сфері обігу інформації існує вже досить давно, воно продовжує еволюціонувати, відповідаючи на нові вимоги часу.

Вказане й обумовлює актуальність розгляду цієї проблеми як окремого комплексного напряму боротьби із корупційними проявами у сфері функціонування відкритих джерел інформації, що мають стати інструментом такої протидії. При цьому необхідно відмітити, що протидія корупції є необхідною умовою життєдіяльності суспільства, а її забезпечення має розглядатися як важлива функція держави, що ґрунтується на загальних принципах, методах і формах безпекової діяльності. Проте, вона має й свої особливості, які залежать від характеру завдань та функцій щодо боротьби з корупцією системи органів, що її забезпечують, їх компетенції, форм і методів діяльності, а також місця і ролі в цьому процесі громадянського суспільства.

Наполегливе небажання влади використовувати громадський потенціал для протидії корупції може говорити або про відсутність розуміння того, як функціонує інформаційне суспільство, або про елементарний «страх» перед змінами. Ще одна проблема – це необхідне ухвалення змін та доповнень до законодавства України щодо охорони приватного життя громадян, згідно з яким незаконний збір, використання, розповсюдження та зберігання інформації тягне за собою юридичну відповідальність.

Не дивлячись на вказані стримуючі чинники, на даному етапі вважається важливим, щоб все більше і більше громадян включалося до цього процесу. Вже на цей час відкриті інформаційні бази, такі як, наприклад, сайт щодо держзакупівель, дозволяють знаходити і надати гласності різноманітні зловживання. Має сенс вивчати декларації про доходи (а незабаром і про витрати) чиновників, які в обов'язковому порядку публікуються на сайтах відомств. Проте, сьогодні даний процес не функціонує належним чином. Для такої роботи був би дуже корисний єдиний портал з деклараціями.

Також слід відмітити, що Єдина база дисертацій допоможе не тільки у справі викриття чиновників, які отримали вчені ступені шляхом корупційних дій, але і допоможе повернути в наукову сферу реальну і чесну конкуренцію, зробить українську науку ефективнішою.

Відкриття для загального доступу до Єдиного державного реєстру юридичних осіб та індивідуальних підприємців дозволить громадським активістам шукати аффілірованих у бізнесі чиновників.

З метою надати зацікавленим платникам податків більше можливостей перевірити, наскільки адекватно витрачаються державні кошти, у сфері контролю за державним замовленням можна зробити наступне: створити спеціалізовані реєстри високотехнологічної продукції - від телекомунікаційного устаткування до медичних приладів, наприклад, томографів. Головне - чітко прописати специфікації такої техніки та максимально їх стандартизувати, прив'язати до ринкових цін, щоб у процесі конкурсу чиновники відштовхувалися від реальної вартості предмету замовлення. В першу чергу, така інформаційна система дозволить будь-якій зацікавленій особі без особливих зусиль перевірити обґрунтованість первинної ціни замовлення, а значить, обмежить чиновницьке свавілля і можливість змови з постачальником. Крім того, буде легше дізнатися, наскільки адекватна реальним потребам та або інша комплектація техніки, що купується, щоб уникнути надмірного витрачання бюджету на сумнівні потреби.

Таким чином, вільний обіг інформації може стати фундаментом протидії корупції. Однак на цьому фундаменті не можливо щось побудувати, якщо в суспільстві не буде розвинена культура роботи з такою інформацією, зокрема й громадської участі в житті держави у цілому. Але наведене потребує окремих досліджень.

Слід відзначити, що без належного забезпечення вільного та максимально розширеного доступу населення до інформації про діяльність органів влади неможливо реалізувати фундаментальну основу постіндустріальної демократії - розвиненого громадянського суспільства. Даний інститут сприяє контролю за діяльністю державних органів, конструктивному впливу на ухвалення і реалізацію їх рішень з боку громадськості.

Тим часом, особливі надії покладаються на інститут доступу до офіційної інформації в контексті протидії боротьби з системною корупцією, що є основною дисфункцією сучасної Української держави. Свобода інформації є головним засобом захисту від корупції і зловживання владою, оскільки відвертість і прозорість в процесі ухвалення державних рішень зобов'язують органи влади виконувати закони і діяти на користь населення. Так, Конвенція ООН проти корупції (ратифікована Законом України від 18.10.2006 р. № 251-V) приділяє особливу увагу даній проблемі. Так, ст. 10 «Державна звітність» за-

значає, що з урахуванням необхідності боротьби з корупцією кожна Держава-учасниця вживає, згідно з основоположними принципами свого внутрішнього права, таких заходів, які можуть бути необхідними для посилення прозорості в її державному управлінні, у тому числі стосовно її організації, функціонування та, у належних випадках, процесів прийняття рішень. Такі заходи можуть включати, inter alia, таке: a) прийняття процедур або правил, які дозволяють членам суспільства отримувати, у належних випадках, інформацію про організацію, функціонування та процеси прийняття рішень у державному управлінні та, з належною увагою до захисту приватного життя й даних особистого характеру, про рішення та нормативно-правові акти, що стосуються членів суспільства; b) спрощення адміністративних процедур, у належних випадках, для полегшення доступу громадськості до компетентних органів, які приймають рішення; та c) опублікування інформації, яка може включати періодичні звіти про ризики корупції в державному управлінні. У свою чергу, ст. 13 «Участь суспільства» вказаного документа свідчить, що «кожна Держава-учасник вживає належні заходи в межах своїх можливостей і відповідно до основоположних принципів свого внутрішнього законодавства для сприяння активній участі окремих осіб і груп за межами публічного сектора, таких як цивільне суспільство, неурядові організації і організації, що функціонують на базі общин в попередженні корупції і боротьбі з нею і для поглиблення розуміння загального факту існування, причин і небезпечного характеру корупції, а також створюваних нею загроз. Цю участь слід укріплювати за допомогою таких заходів, як: A. Посилення прозорості і сприяння залученню населення в процеси ухвалення рішень; B. Забезпечення для населення доступу до інформації; C. Проведення заходів щодо інформування населення; D. Повага, заохочення і захист свободи пошуку, отримання, опублікування та поширення інформації про корупцію».

Проблема корупції в Україні знаходиться на одному з основних місць у порядку денному, представляючи реальну загрозу функціонуванню Українській держави, а також його прогресивному розвитку. Крім того, вона протидіє соціально-політичній модернізації нашої держави, сприяє виникненню відчуження між політичною владою і суспільством, кризі інституційної довіри, істотному зниженню ефективності соціально-політичних інститутів і легітимності влади.

Панченко Валентина Миколаївна
старший науковий співробітник
Національної академії СБ України,
кандидат технічних наук, майор

Визначення основних понять у сфері захисту національної інфраструктури від кібератак

Національна інфраструктура традиційно відноситься до потенційних ресурсів, що визначають можливості економічного зростання та безпеки певної території. Водночас, розвиток інформаційних технологій, їх впровадження в усі сфери життєдіяльності суспільства обумовлює складність та взаємопов'язаність окремих складових національної інфраструктури, внаслідок чого руйнування однієї з інформаційних систем об'єктів життєзабезпечення може призвести до руйнування інших. З огляду на це, питання захисту національної інфраструктури від кібератак є на сьогодні вкрай актуальним.

Формування системи захисту національної інфраструктури від кібератак в Україні, зокрема її нормативно-правового забезпечення, розпочалося не так давно. Так, на виконання п. 4.7 Указу Президента України від 3 лютого 2010 року №92/2010 започатковано розбудову системи реагування на кібернетичні атаки на національну інформаційну інфраструктуру, здатну взаємодіяти з відповідними системами іноземних держав та міжнародних організацій в режимі реального часу. У рішенні РНБО України від 25 травня 2012 року, введеному в дію Указом Президента № 388/2012 від 8.06.2012 р., Кабінету Міністрів України доручено розробку проекту закону про кібернетичну безпеку України. У березні 2013 року на розгляд Верховної Ради України подано схвалений Кабінетом Міністрів проект Закону України «Про внесення змін до деяких законів України щодо забезпечення кібернетичної безпеки України» (№ 2483 від 07.03.2013 р.).

Загалом позитивно оцінюючи цілеспрямовані поступальні кроки держави у напрямку формування нормативно-правового підґрунтя для організації захисту національної інфраструктури від кібератак, автор вважає за доцільне звернути увагу на неоднозначність окремих термінів, які містяться в останньому законопроекті. Зокрема, більш детального вивчення потребує питання доцільності нормативного закріплення поняття «об'єкти критичної інформаційної інфраструктури».