Ключові аспекти проекту закону України «Про безпеку інформації»

Володимир ФУРАШЕВ,
кандидат технічних наук,
заступник директора з наукової роботи
Науково-дослідного центру
правової інформатики НАПрНУ

Здійснивши аналіз національного законодавства у сфері інформаційних відносин і особливо актів, котрі безпосередньо стосуються безпеки інформації та кібербезпеки, можна дійти таких висновків.

Нормативно-правові визначення поняття «інформація» [2] потребують переосмислення, тому що не відображають сутності цього явища. Ці визначення мають суто технологічний характер і застосовуються задля зручності подальшої побудови, розвитку та регламентації інформаційних відносин і в загальному, і в специфічному їх сенсі.

Визначення поняття «інформація» мають домінуючий вплив на «дух» і «букву» законів України та інших нормативно-правових актів, котрі стосуються інформаційних відносин.

У документах (чинних або їхніх проектах), що стосуються започаткування, розвитку та регулювання інформаційних відносин, слід уникати надання загального визначення поняття «інформація», оперуючи дефініціями терміна «інформація» згідно із сутністю того чи іншого аспекту інформаційних відносин.

Сукупність процедур та механізмів породження, передачі, використання, доступу, оцінки та аналізу, збереження й знищення інформації становить систему інформаційних відносин, у центрі якої знаходяться людина, суспільство й держава [6, с. 25].

Офіційний статус поняття «інформація» не передбачено жодним нормативно-правовим актом, зокрема й тими, що оприлюднені на офіційних веб-сайтах органів виконавчої влади. У Законі України «Про доступ до публічної інформації» [4] визначено: «доступ до інформації забезпечується шляхом систематичного та оперативного оприлюднення інформації, в т.ч. на офіційних веб-сайтах у мережі Інтернет» (ст. 5). Але в цьому законі застосовано саме поняття «публічної інформації» як такої, що «відображена та задокументована будь-якими засобами та на будь-яких носіях, отримана або створена в процесі виконання суб'єктами владних повноважень, своїх обов'язків, передбачених чинним законодавством, або яка знаходиться у володінні суб'єктів владних повноважень, інших розпорядників публічної інформації, визначених цим Законом» (ст. 1). Тобто цю інформацію можна розглядати лише як інформативну.

У переважній більшості чинних законодавчих та інших нормативно-правових актів, спрямованих на встановлення, розвиток та регулювання інформаційних відносин, **не застосовується** поняття «інформаційна безпека».

У законах України та інших документах, де з певною метою згадується поняття «інформаційна безпека», **не дається** його визначення. Винятком є Закон України «Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» [5], в якому **окреслюється визначення** цього поняття. Але наведену дефініцію з урахуванням спрямованості закону не можна вважати законодавчим визначенням.

Переважна більшість положень законів України та інших нормативно-правових актів, які безпосередньо стосуються інформаційних відносин, **спрямована саме на захист інформації. Статті зі спрямованістю на захист людини, суспільства** й відповідно **держави** від інформації – «у меншості».

Доктрина інформаційної безпеки України [3] розглядає інформаційну безпеку як складову сукупності політичних, соціальних, економічних та інформаційних відносин разом із організаційно-адміністративними та техніко-технологічними заходами.

З огляду на природу поняття «інформація» та сутність інформаційних відносин можна встановити, що:

– **об'єктами** інформаційних відносин є людина, суспільство, держава та інформація, а суб'єктами – норми і правила, які визначають ці відносини;

– об'єктами інформаційної безпеки є людина, суспільство та держава, а **суб'єктами** – інформація в усіх її проявах, джерела інформації, механізми та засоби її створення, доступу, розповсюдження та наслідки її використання, а також установчі й регуляторні нормативно-правові та адміністративно-організаційні норми і правила, які визначають їх формування, використання та припинення дії. Закон України «Про внесення змін до Закону України «Про інформацію» [2] визначає, що «захист інформації – це сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї». Відповідно, **об'єктом** захисту інформації є інформація, а **суб'єктами** – дії з інформацією на всіх стадіях її «життєвого

циклу» (створення, розповсюдження, збереження, знищення, спотворення, фальсифікація тощо);

— інформація не існує заради інформації. Вона існує та існуватиме доти, доки людина, суспільство чи держава матиме в ній потребу;

— у зв'язку з тим, що інформація має визначальний вплив на людину, цілком логічним є захист людини, суспільства від негативних проявів такого впливу, тобто у цьому разі **об'єктом захисту** залишається інформація, але **суб'єктами захисту** вже стають наслідки дій із нею для людини, суспільства й держави на всіх стадіях її «життєвого циклу» (створення, розповсюдження, збереження, знищення, спотворення, фальсифікація та інше). Тобто йдеться про **безпеку інформації** для людини, суспільства, держави. Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007—2015 роки» [5] визначає сутність поняття «безпека інформації» як «стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації» (розділ 13).

Варто звернутися до **Конвенції про кіберзлочинність** [1], схвалену в Будапешті 23 листопада 2001 року, котра акцентує увагу світової спільноти на тому, що *«комп'ютерні мережі та електронна інформація можуть також використовуватися для вчинення кримінальних правопорушень, а докази, пов'язані з такими правопорушеннями, можуть зберігатися і передаватися цими мережами», та на необхідності «зупинення дій, спрямованих проти конфіденційності, цілісності й доступності комп'ютерних систем, мереж та даних, а також зловживання такими системами, мережами й даними».*

Водночас у Конвенції наголошено на *«необхідності забезпечення належного балансу між правоохоронними потребами і повагою до основних прав людини, як це передбачено Конвенцією Ради Європи про захист прав людини і основних свобод 1950 року, Міжнародною Хартією ООН про громадянські і політичні права 1966 року й іншими міжнародними угодами з прав людини, які підтверджують право кожного безперешкодно дотримуватися власних поглядів; право на свободу слова, включаючи право на пошук, отримання і передачу будь-якої інформації та ідей, незважаючи на кордони; право на повагу до приватного життя», а також міститься заклик пам'ятати «про право на захист особистої інформації, як це передбачено Конвенцією Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних 1981 року».*

Отже, Конвенція про кіберзлочинність **об'єктами** кіберзлочинності визначає комп'ютерні системи, мережі та електронну інформацію, а **суб'єктами** — дії, спрямовані проти конфіденційності, цілісності й доступності комп'ютерних систем, мереж і даних, а також зловживання такими системами, мережами й даними.

Згідно з логікою «дія-протидія» можна стверджувати, що зазначені об'єкти та суб'єкти кіберзлочинності також є **об'єктами** та **суб'єктами** кіберзахисту.

Однак захист не потрібний заради захисту, адже він спрямований на щось інше, чим, зрештою, є людина, суспільство, держава.

На основі того, що *«кібернетика — наука про управління, зв'язок і переробку інформації»*, а також зважаючи на те, що людський мозок, людське суспільство — приклад кібернетичних систем, котрі, у свою чергу, є безліччю взаємопов'язаних об'єктів, здатних сприймати, запам'ятовувати й переробляти інформацію, можна порушувати питання про поняття **«кібербезпека»**, **об'єктами** якої є механізми впливу (управління) інформації на людину, суспільство й державу, а **суб'єктами** — процеси та механізми, пов'язані з регулюванням ступеня впливу на всіх стадіях «життєвого циклу» інформації.

Відповідно **інформаційна безпека** — стан захищеності життєво важливих інтересів людини, суспільства й держави, за якого завданню шкоди можна запобігти через:

— негативний інформаційний вплив за допомогою, найперше, несанкціонованого створення, розповсюдження, використання свідомо спрямованої із визначеною метою неповної, невчасної, невірогідної та упередженої інформації;

— негативні наслідки застосування інформаційних технологій;

— несанкціоноване порушення режиму доступу до інформації з подальшим її розповсюдженням та використанням.

Безпека інформації — склад та стан інформації, а також дії з нею, якими забезпечується певний рівень інформаційної безпеки.

Кібербезпека — стан спроможності людини, суспільства й держави запобігати та уникати спрямованого, насамперед несвідомого, негативного впливу (управління) інформації.

Питання безпеки інформації є серйозним такою мірою, що заслуговує чіткого визначення в окремому системоутворювальному (базовому) Законі України «Про безпеку інформації» (або «Про основи безпеки інформації», але така назва, на думку автора, не зовсім відповідатиме суті цього нормативно-правового акта). За змістом згаданий закон повинен бути спрямований на надання чітких та зрозумілих базових визначень таких понять, як «інформаційна безпека», «безпека інформації», «кібербезпека», «захист інформації», «кіберзлочинність» тощо (як загальних, так і в межах «галузевого» розподілу), а також ключових принципів їх забезпечення чи усунення при збереженні гарантованих Конституцією України прав і свобод людини. Крім того, визначаючи наведені поняття, необхідно враховувати положення Указу Президента України «Про Доктрину інформаційної безпеки України» [3].

Зрозуміло, що надалі положення цього закону мають увійти до Інформаційного кодексу України, як це передбачено абзацами другим та третім частини 2 розділу III Закону України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007—2015 роки» [5], але в ширшому сенсі. Обираючи пріоритети розробки та впровадження зазначених законопроектів, треба брати до уваги часові показники.

Та, безперечно, на розробку й впровадження спеціалізованого законопроекту «Про безпеку інформації» знадобиться значно менше часу, ніж на розробку, погодження та впровадження такого системоутворювального законопроекту, як Інформаційний кодекс України.

Джерела

1. Конвенція про кіберзлочинність: міжнародний документ. — [Електронний ресурс]. — http://zakon2.rada.gov.ua

2. Про внесення змін до Закону України «Про інформацію»: Закон України від 13.01.2011 р. № 2938-VI // Офіційний вісник України. — 2011. — № 10.

3. Про Доктрину інформаційної безпеки України: Указ Президента України від 08.07.2009 р. № 514/2009 // Офіційний вісник Президента України. — 2009. — № 20. — С. 18.

4. Про доступ до публічної інформації: Закон України від 13.01.2011 р. № 2939-VI // Відомості Верховної Ради України. — 2011. — № 32. — Ст. 314.

5. Про основні засади розвитку інформаційного суспільства в Україні на 2007—2015 роки: Закон України від 09.01.2007 р. № 537-V // Відомості Верховної Ради України. — 2007. — № 12. — Ст. 102.

6. *Соснін О.* Проблеми правового регулювання інформаційної політики в Україні // Вісник. — 2008. — № 20. — С. 22—26.