УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ЯК СУТНІСНА СКЛАДОВА ПОБУДОВИ ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА В УКРАЇНІ

В.Ю. Артемов,
канд. юрид. наук, доцент Інститут захисту інформації з обмеженим доступом

Захист інформації з обмеженим доступом є, безумовно, найважливішим завданням України. У зв'язку із виникненням нових викликів у інформаційній сфері, а також активною участю нашої держави в процесі реалізації системи колективної безпеки перед структурами, які забезпечують організацію захисту інформації з обмеженим доступом, постають нові завдання.

До проблеми управління інформаційною безпекою зверталися такі відомі зарубіжні та вітчизняні науковці як А. Роберте, В. Хорошко, В. Ящуринсь-кий, В. Маричєв, В. Василюк, С. Климчук та ін. Зазначені науковці натомість мало уваги приділяли постановки проблеми менеджменту захисту інформації з обмеженим доступом, та функціонуванню субсистеми інформаційного права.

Поява та усвідомлення проблем інформаційної безпеки призводять до необхідності подальшого розвитку та розширення інформаційного права як галузі юридичної науки. В цілому це відповідає сучасним тенденціям, оскільки в наш час система права переживає період поділу, у зв'язку зі значним розширенням кордонів та особливостей правового регулювання.

Мета даної статті - дослідити та проаналізувати сутність міжнародних норм та стандартів в галузі захисту інформації з урахуванням жорстких вимог щодо свободи інформації та лібералізації права.

Захист інформації з обмеженим доступом є, безумовно, найважливішим завданням України. У зв'язку із виникненням нових викликів у інформаційній сфері, а також активною участю нашої держави в процесі реалізації системи колективної безпеки перед структурами, які забезпечують організацію захисту інформації з обмеженим доступом, постають нові завдання.

Здавалося б, вирішення цих завдань слід шукати в контексті запозичення міжнародних норм та стандартів. В той же час, міжнародна практика показала, що сліпе копіювання чужих юридичних норм та правил не забезпечує ефективне вирішення поставлених завдань. їх вирішення насправді вимагає глибокої та своєчасної теоретико-правової підтримки з боку вітчизняної юридичної науки.

Підвищення ролі інформації у життєдіяльності сучасного суспільства і пов'язана з цим необхідність захисту інформації від впливів зовнішніх та внутрішніх дестабілізуючих і руйнуючих факторів породили новий напрям наукових досліджень у правовій сфері, яке отримало назву «інформаційне право».

Особливий інтерес до цієї галузі права викликаний тим, що заходи по забезпеченню інформаційної безпеки є високозатратними, причому вони постійно зростають (у геометричній відповідності до розвитку інформаційних технологій).

Однак, світове суспільство змушене йти на ці витрати тому, що в інформаційному суспільстві, в якому ми живемо сьогодні, прогалини в системі захисту інформації створюють ризики не лише стосовно економічного розвитку, але й для політичної стабільності. Ось чому правове забезпечення суспільних відносин, яке стосується згаданої сфери, в наш час має надзвичайно важливе значення.

Ряд авторів, у тому числі П.У. Кузнецов, виходячи із системного підходу до вирішення проблем права, вбачають місце інформаційного права та його подальших підрозділів у складі певної трирівневої структури, яка показана на рис. 1.

При цьому вся система права розглядається як метасистема, власне інформаційне право - як система, а інформаційно-захисне право пропонується згаданим вище науковцем як субсистема або одна з підсистем інформаційно-захисного права. Подальше розчленування, на думку автора, дозволяє розглядати інформаційне право як метасистему, інформаційно-захисне право - як систему, що дозволяє вводити субсистемами такі, наприклад, складові як охорона державної таємниці та інтелектуальної власності (рис. 2).

Безумовно, кожен правовий інститут інформаційного права вирізняється своєрідністю та особливостями правового режиму. Він може бути більш жорстким або, навпаки, м'якішим. Все це визначається ризиками, пов'язаними з порушеннями правових режимів.

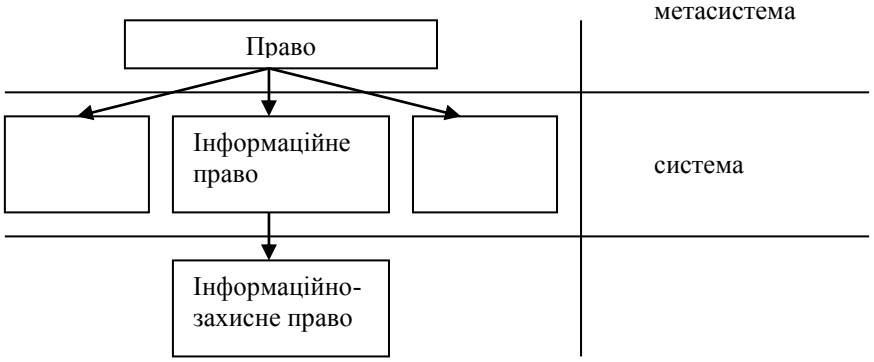

Рис. 1. Місце інформаційно-захисного права в загальній структурі права

Ми допускаємо, що саме на принципі «розподілу ризиків» повинна проводитися диференціація правової системи та виділення сукупності окрек інформаційних правових норм.

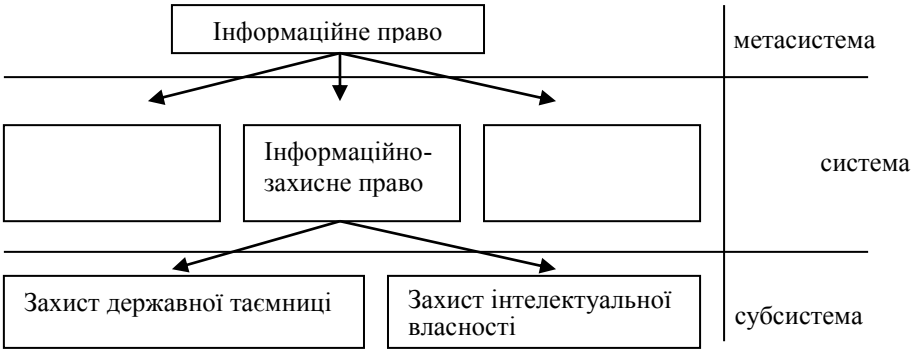

Рис. 2. Можлива диференціація інформаційно-захисного права в загальній структурі інформаційного права

Ось чому, в цілому погоджуючись із пропозиціями, наведеними на рис. та рис. 2, слід запропонувати дещо іншу структуру поділу інформаційно-захисного права (рис. 3). В основу такого поділу слід покласти принцип класифікації інформації. Причому класифікацію інформації слід виробляти на підставі ризиків можливих втрат її правоволоділців, незалежно від того, ким вони чи то державою, чи міждержавними спілками, або ж це фізичні та юридичні особи. Причому ризики, по можливості, слід оцінювати з економічного боку. Саме **за** таким принципом здійснюється класифікація інформації в ЄС та НАТО.

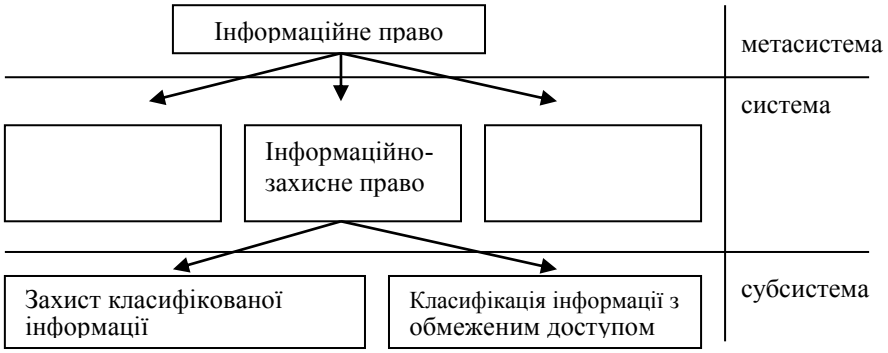

Рис. 3. Запропонована структура інформаційно-захисного права в загальній структурі інформаційного права

Відповідно до цього принципу, вся інформація поділяється на ту, що потребує класифікації, і ту, що повинна класифікуватися за ступенем захисту. В ЄС та НАТО встановлено такі рівні класифікованої інформації: TOP SECRET, SECRET та CONFEDENTIAL. НАТО, крім того, захищає так звану некласифіковану, але чутливу інформацію (Unclassified But Sencetive). В НАТО також можна зустріти документи під грифом ABOVE TOP SECRET.

Термін «інформація з обмеженим доступом» може застосовуватися у вузькому та широкому сенсі. У вузькому сенсі - це інформація, ступінь захисту котрої нижчий, ніж у таємної або цілком таємної. В цьому сенсі вона відповідає рівню CONFIDENTIAL або «Для службового користування». В широкому сенсі інформація з обмеженим доступом - це вся інформація, яка потребує захисту, тоді вона співпадає тільки з CONFIDENTIAL.

Класифікація за ступенем захисту інформації не лише впливає на диференціацію правової системи в цілому, але й формує систему інформаційного права у всіх його структурних елементах, виділяючи сукупність галузевих інформаційних правових норм.

Запропонований спосіб класифікації забезпечує обмеження зони відповідальності, в якій суб'єкт управління може приймати рішення. В правознавстві такі зони визначаються як предмети ведення. В системі управління процесом правового забезпечення інформаційної безпеки питання підзвітності (предмети ведення) посідають особливе місце. Вирішення проблеми підзвітності пов'язано із необхідністю координації правозастосовчої діяльності з боку авторитетного державного органу, яким може бути і спецслужба, і який був би спроможний проводити моніторинг правового забезпечення захисту інформації з

обмеженим доступом, а в необхідних випадках - виходити на найвищій рівень державного управління як суб'єкт законодавчої ініціативи.

Це дозволяє виокремити як субсистему інформаційного права захист класифікованої інформації або захист інформації з обмеженим доступом. Самостійність такої субсистеми проявляється в такому індикаторі, як правовий інститут. До специфічного правового інституту субсистеми слід віднести такі групи норм та механізмів їх реалізації, котрі регулюють найбільш стійкі та однорідні відносини в сфері захисту інформації. До них можна віднести і «політику безпеки», і «доступ» та «допуск», і «секрет» та «таємність», і «право на інформацію» та «захист інформації» тощо. При цьому предметною сферою правового регулювання захисту інформації з обмеженим доступом є самостійне об'єктивне явище суспільних відносин. А правовий інструмент регулювання при цьому являє собою систему галузевих методів права, що об'єднуються загальним терміном - «менеджмент захисту інформації з обмеженим доступом».

Паралельно інформацію, що потребує захисту, можна класифікувати ще й у залежності від її природи, виокремлюючи державну, міждержавну, медичну, комерційну, банківську та іншу таємницю. Правові норми рознесення такої інформації за класами захисту в залежності від її природи є предметом іншої субсистеми (див. рис. 3), правовим інструментом якої повинен стати менеджмент диференціації інформації з обмеженим доступом.

При цьому аналіз ризиків слід розглядати не лише як метод ідентифікації та оцінок, але й у більш широкому сенсі, як методологію побудови замкнутої системи на основі аналізу ризиків. Актуальна на даний час теорія ризику та безпеки [3] має фундаментальний характер. її практичне застосування базується на використанні стандартів організаційного та технічного рівня. Такий підхід дозволяє не лише отримати оцінку стану інформаційної безпеки, але й обґрунтувати план та доцільність тих чи інших заходів щодо захисту інформації. На жаль, ці напрацювання не отримали поки застосування в сфері захисту інформації з обмеженим доступом.

Менеджмент захисту інформації з обмеженим доступом є тією галуззю, необхідність теоретичного осмислення якої стала очевидна зовсім нещодавно. Перші дослідження в галузі інформаційної безпеки почалися наприкінці 80-х років минулого століття, а наприкінці 90-х з'явилися перші національні та міжнародні стандарти (ISCMEC 17799,15408 та 27001). Однак факт появи таких стандартів не вирішує проблем захисту інформації з обмеженим доступом. Навпаки, завдання управління захистом інформації ускладнюються з кожним роком. Проблема полягає в тому, що впровадження міжнародних стандартів вимагає потужної нормативно-правової підтримки. Тут вельми доцільними є напрацювання в галузі порівняльного правознавства [4]. На жаль, і ці скромні напрацювання досі ще не отримали застосування в сфері захисту інформації з обмеженим доступом.

Тож, наслідком сучасного стану науки в галузі права та нагальних вимог практики безумовно є необхідність фундаментальних наукових досліджень в галузі захисту інформації з обмеженим доступом, виокремлення її в окрему субсистему загальної системи інформаційного права.

Безумовно, в загальній структурі забезпечення захисту інформації з обмеженим доступом важливу роль грають не лише такі сутності як юридична наука, нормативне узагальнення, правові механізми, але й практика правоза-стосування правосвідомості та правова культура.

Разом з тим, проведення наукового дослідження з розробки теоретичних основ менеджменту захисту інформації з обмеженим доступом як нової суб-системи права відповідає не лише запитам сьогодення, але й перспективам розвитку інформаційного суспільства України.