ПРИНЦИПИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

Олійник О.В.,
кандидат юридичних наук,
старший науковий співробітник,
головний консультант Інституту законодавства
Верховної Ради України

У статті проаналізовано принципи забезпечення інформаційної безпеки як складової національної безпеки України.
Ключові слова: інформаційна безпека, принципи інформаційної безпеки, інформаційна інфраструктура, національна безпека.

В статье проанализированы принципы обеспечения информационной безопасности как составляющей национальной безопасности Украины.
Ключевые слова: информационная безопасность, принципы информационной безопасности, информационная инфраструктура, национальная безопасность.

The article analyzes the metodological aspects of information security as a component of the national security of Ukraine.
Keywords: information security, principles of the informational security, information infrastructure, national security.

Принципи забезпечення інформаційної безпеки - є вихідними положеннями, нормами і правилами поведінки, які диктують усім суб'єктам правила поведінки. Комплекс принципів, що нижче розглядаються, - це вихідні положення, норми і правила поведінки, спрямовані на формування і забезпечення функціонування системи забезпечення інформаційної безпеки. Зважаючи на те, що процес удосконалення системи забезпечення інформаційної безпеки триває, найбільш прийнятним підходом буде систематизація принципів окремо правових і окремо організаційних. Це сприятиме вдосконаленню як правової бази забезпечення інформаційної безпеки, так і системи його організаційного забезпечення. Визначення, обґрунтування і практичне застосування правових і організаційних принципів слугуватиме базою для вирішення широкого кола завдань забезпечення інформаційної безпеки. До правових принципів забезпечення інформаційної безпеки доцільно включення наступних: законності; пріоритету норм міжнародного права над національним законодавством; права власності; економічної доцільності.

Принцип законності полягає у застосуванні механізмів забезпечення інформаційної безпеки та механізмів і технологій управління системою забезпечення інформаційної безпеки тільки на основі чинного законодавства та нормативно-правової бази регулювання як суспільних інформаційних відносин, так і міжнародного інформаційного співробітництва.

При цьому слід нагадати про те, що в умовах демократизації суспільних відносин принцип законності всіх дій стосовно забезпечення інформаційної безпеки набуває надзвичайно важливого значення.

Чинним законодавством встановлено широкі права суб'єктів України на співробітництво з іншими державами та зарубіжними міжнародними організаціями в сфері інформації, у тому числі на створення і діяльність спільних організацій у галузі інформації за участю вітчизняних та іноземних юридичних осіб і громадян. Незважаючи на те, що вказані права і свободи стосовно інформаційної діяльності захищаються Законом, у тому числі правовими санкціями Кримінального кодексу України (ст. 177, 229, 231, 232, 330 тощо), у зв'язку з відсутністю необхідного комплексу механізмів захисту цих прав і свобод вони можуть бути і порушені. Причиною цього може бути те, що права і свободи інформаційної діяльності не корелюються з системою експортного контролю за зовнішньоекономічними операціями щодо товарів, технологій і послуг, що підлягають експортному контролю. Відповідно до переліку товарів, технологій і послуг, затверджених Урядом України та системою експортного контролю [1,2], можуть бути застосовані певні обмеження на передання іноземній державі чи міжнародній організації інформації, яка підпадає під ознаки цього переліку.

Обмеження експорту наукомістких технологій - це світова практика і вона активно застосовується розвиненими країнами, в тому числі нашими стратегічними партнерами, якими є США та Російська Федерація. При цьому такі обмеження і механізми їх застосування вводяться тільки на рівні законів. Так, у Російській Федерації спеціальним законом регулюються відносини щодо експортного контролю. Окремим законом регулюються відносини в процесі міжнародного інформаційного співробітництва. Цей закон також чітко визначає обмеження та механізми їх застосування під час здійснення міжнародного інформаційного обміну.

Інформаційна сфера є надзвичайно чутливою до відхилень від законодавчих вимог щодо регулювання суспільних інформаційних відносин та управління з боку держави процесами забезпечення інформаційної безпеки. Будь-які обмеження прав і свобод інформаційної діяльності, не передбачених чинним законодавством, у суспільстві сприймаються вкрай негативно. Особливо у випадках, пов'язаних з діями державних органів. А це гостро ставить питання про необхідність на законодавчому рівні чіткого визначення компетенції органів державної влади, органів регіонального і місцевого самоврядування їх посадових осіб та спеціальних підрозділів і служб у сфері управління системою забезпечення інформаційної безпеки.

Принцип пріоритету норм міжнародного права над національним законодавством, за винятком Конституції України, в системі забезпечення інформаційної безпеки полягатиме в прямій дії загальновизнаних принципів і норм міжнародного права, міжнародних договорів на всій території країни на рівні Конституції України.

Відповідно до правової норми Основного закону в даному разі йдеться про міжнародні договори, укладені з іноземними державами або до яких приєдналася Україна, згода на обов'язковість яких надано Верховною Радою України. Поряд з цим, правовою нормою Основного закону заборонено укладання міжнародних договорів, що суперечать Конституції України. Такі договори можуть укладатися лише після внесення змін

до Основного закону України [3, ст.9]. При цьому слід нагадати, що у відповідності з нормами міжнародного права кожна суверенна держава має право самостійно вирішувати питання про зміст забезпечення інформаційної безпеки. Легітимність обмежень на поширення інформації світовим співтовариством визначається тільки у випадках, коли такі обмеження і механізми забезпечення встановлені національними законами.

Так, не підлягають засекречуванню відомості про розміри асигнувань на здійснення державної програми розвитку озброєння та військової техніки, які надаються Україною у відповідності з міжнародними зобов'язаннями по лінії Організації з безпеки та співробітництва в Європі та Організації Об'єднаних Націй [4, п. 2.39]. Не можуть бути засекречені також відомості про військове, військово-технічне та науково-технічне співробітництво, які мають передаватися відповідно до міжнародних зобов'язань України [4, п. 3.3]. Генеральна Асамблея Організації Об'єднаних Націй у резолюції № 46/36 запропонувала країнам-членам ООН подавати щорічні звіти про експорт-імпорт певних видів важких озброєнь і військової техніки для реєстрації [5]. Відомо також, що однією з умов членства України в Європейському Союзі є подання цій організації відомостей про дійсний стан справ у нашій економіці.

Наведене вище є підставою для наступних висновків про те, що практична реалізація принципу пріоритету норм міжнародного права над національним законодавством має два важливих взаємопов'язаних напрями діяльності.

Перший. Забезпечення єдиної державної політики, спрямованої на вдосконалення національного законодавства з питань забезпечення інформаційної політики на основі загальновизнаних світових стандартів. Зумовлено це тим, що в процесі міжнародного обміну інформацією кожна країна забезпечує її захист відповідно до вимог національних законів. Недосконалість законодавства з питань забезпечення інформаційної безпеки в процесі міжнародних стосунків створюватиме передумови для ураження інтересів суб'єктів України.

Другий. Проведення активної політики щодо участі України в розробці міжнародних правових документів, які торкаються національних інтересів нашої країни в інформаційній сфері, а також приєднання України до діючих міжнародних конвенцій, договорів та угод з питань захисту прав суб'єктів інформаційної діяльності.

Принцип права власності в процесі забезпечення інформаційної безпеки передбачає гарантування прав суб'єктів України на інформацію за винятком обмежень, встановлених чинним законодавством.

У відповідності з вимогами Конституції України " право приватної власності є непорушним " [3, ст. 41]. У нових умовах господарювання, зростання обсягів приватної власності в процесі роздержавлення власності – це дуже важливий аспект, що регулюватиме суспільні економічні відносини на новому етапі розвитку соціально-економічної системи. Водночас згідно з чинним законодавством встановлено певні обмеження щодо здійснення права власності на інформацію, які випливають із дії об'єктивного закону інформаційної сфери щодо примусового відчуження й усуспільнення інформації.

Захист прав створювачів і власників об'єктів промислової власності здійснюється відповідними правовими нормами цивільно-правового, адміністративного і кримінального законодавства.

У відповідності з висновками, які сформулював А.Долгополий у своїй праці, проблеми захисту прав на об'єкти промислової власності мають декілька аспектів.

Перший. Зіткнення інтересів безпосереднього створювача об'єкта інтелектуальної власності, який прагне одержати максимальне матеріальне винагородження і стимулювання своєї праці та претензій суспільства на певну частину вартості цього об'єкта, обґрунтованих створенням умов для появи даного результату творчої діяльності. Це частково вирішується законодавчим встановленням права власності на створений об'єкт і обмеженням строку дії його захисту.

Другий. Патент являє собою обмежену строком монополію на певне технічне рішення, визначену на встановлених патентним законодавством підставах, а будь-яка монополія веде до обмежень конкуренції, на варті якої стоїть антимонопольне законодавство. Виходом із цього становища є розумний компроміс між положенням патентного й антимонопольного законодавств, що забезпечує стимулювання патентною монополією технічного прогресу за умов збереження конкуренції.

Третій. В міжнародному аспекті існує прагнення, з одного боку, держав, що провадять переважно інноваційну політику, до посилення захисту прав на об'єкти інтелектуальної власності, а, з другого боку, – держав, що провадять переважно адаптаційну політику щодо чужих інновацій, до послаблення цього захисту. На думку автора публікації, в цьому аспекті рішення може полягати в компромісі конфліктуючих інтересів різних країн і прийнятті в майбутньому міжнародних угод щодо стандартів захисту прав інтелектуальної власності [6, с. 64].

Таким чином, принцип права власності потребує вдосконалення правових механізмів захисту цих прав у процесі суспільних інформаційних відносин та правового регулювання діяльності суб'єктів України стосовно обміну з іноземними партнерами інформацією.

Принцип економічної доцільності системи забезпечення інформаційної безпеки полягає в оцінюванні секретності та конфіденційності як споживацьких властивостей і включення їх вартості, на підставі вимог законодавства, до загальної ціни виробленої продукції.

Відповідно до чинного законодавства " фінансування витрат на здійснення діяльності, пов'язаної з державною таємницею, в бюджетних установах і організаціях здійснюється за рахунок державного бюджету України, бюджету Автономної Республіки Крим та місцевих бюджетів. Кошти на зазначені витрати передбачаються у відповідних бюджетах окремим рядком.

Розглянемо механізм забезпечення реалізації принципу економічної доцільності.

Розмір економічної шкоди та тяжкість інших негативних наслідків для життєво важливих інтересів країни доцільно вважати головним критерієм застосування принципу економічної доцільності забезпечення інформаційної безпеки. Підкреслимо ще раз, що це дуже важливий визначальний аспект, однак він не дає повного обґрунтування змістовної сутності принципу економічної доцільності. А це потребує введення додаткових критеріїв для обґрунтування економічної доцільності системи забезпечення інформаційної безпеки. Однак, зважаючи на світовий досвід та накопичений в суспільстві досвід найбільш важливі ознаки цих критеріїв можна окреслити вже тепер.

Серед таких критеріїв, які доцільно враховувати в процесі обґрунтування економічної доцільності забезпечення інформаційної безпеки, можуть бути наступні:

визначення переваг відкритого використання відомостей, що можуть бути віднесені до інформації з обмеженим доступом і підлягають захисту;

- підрахунок витрат на захист таких відомостей.

Переваги відкритого використання відомостей, що підлягають віднесенню до категорії з обмеженим доступом, можуть бути обґрунтовані наступними факторами:

політичною доцільністю відкритого опублікування таких відомостей;

- отриманням значного економічного ефекту від широкого відкритого використання цих відомостей в економіці країни;

- прискорення вітчизняного науково-технічного прогресу;

- зміцнення зовнішньоторговельних позицій України на світовому ринку.

Безумовно, з наведених факторів можуть бути винятки, за яких необхідність забезпечення інформаційної безпеки пояснюється інтересами забезпечення національної безпеки, життя і гідності людини. Такі категорії як національна безпека, життя і гідність людини в цивілізаційному вимірі завжди були пріоритетними в діяльності суверенних держав, у тому числі й у сфері захисту відповідної інформації.

Таким чином, принцип економічної доцільності забезпечення інформаційної безпеки передбачає необхідність всебічного врахування як розміру можливої економічної шкоди та тяжкості інших негативних наслідків. А це створюватиме передумови для захисту лише тієї інформації, захист яких дійсно життєво необхідний особі, суспільству, державі.

До організаційних принципів забезпечення інформаційної безпеки можна віднести наступні: об'єктивності; наукового підходу до організації захисту інформації; комплексного підходу; безперервності забезпечення інформаційної безпеки; єдиноначальності; персональної відповідальності; централізовано-децентралізованого державного управління.

Практичне застосування організаційних принципів є основою, яка зв'язує в єдину систему всі інші елементи забезпечення інформаційної безпеки. Як відзначено у праці [7], організаційні принципи зазнали значно менших змін ніж правові, що вони відображають за своєю цінністю загальні правила і підходи до забезпечення інформаційної безпеки і можуть застосовуватися будь-якою соціально-політичною та економічною системою. Як обґрунтовано у теорії адміністративного права: " Організаційні принципи функціонування (діяльності апарату державного управління застосовуються для визначення змісту діяльності конкретних управлінських структур. …За допомогою цих принципів забезпечується прийняття правильних управлінських рішень, організація і застосування раціональних управлінських процедур, дійовий контроль і виконавська дисципліна. Вони фіксуються у відповідних нормативних актах " [8, с. 24 – 25].

Принцип об'єктивності в системі забезпечення інформаційної безпеки має надзвичайно важливе, визначальне значення. Тільки на основі об'єктивної оцінки реальних і потенційних загроз інформації і сфері її обігу, стану правового й організаційного забезпечення, а також реальних можливостей застосування матеріально-технічних, кадрових і фінансових ресурсів хоча б у мінімально необхідних і достатніх обсягах можна забезпечити захист інформації та інформаційну безпеку або послабити дію загроз безпеці сфери її обігу. Окрім того, як підкреслено у праці [9, с. 355], принцип об'єктивності зумовлює необхідність дотримання в усіх управлінських процесах вимог об'єктивних закономірностей, потребує вивчення цих закономірностей та ретельного аналізу наявних можливостей, ведення постійного моніторингу усіх суттєвих процесів.

Система забезпечення інформаційної безпеки та управління цією системою передбачає активність, перманентність і превентивність дій з боку держави та інших суб'єктів інформаційної діяльності. Тільки за таких умов можна розраховувати на позитивні результати; тобто, лише на основі оцінки реального стану інформаційної безпеки з урахуванням об'єктивних законів і закономірностей інформаційної сфери можлива розробка і впровадження ефективних заходів забезпечення безпеки інформації та сфери її обігу.

Принцип об'єктивності несумісний із суб'єктивізмом, стихійністю та ігноруванням законів і закономірностей розвитку інформаційної сфери. Тільки на основі всебічного врахування усіх аспектів принципу об'єктивності можна сформувати і забезпечити подальше вдосконалення ефективно діючої системи забезпечення інформаційної безпеки та управління цією системою з боку держави, інших суб'єктів управлінської діяльності.

Принцип наукового підходу до організації забезпечення інформаційної безпеки передбачає: з одного боку, – всебічне пізнання об'єктивних законів і закономірностей розвитку інформаційної сфери та механізмів їх практичної реалізації; з другого боку – наукове осмислення і юридичне закріплення на рівні законодавчих, нормативно-правових актів та інших державних рішень усього комплексу проблем, пов'язаних із формуванням, удосконаленням системи забезпечення інформаційної безпеки та управління цією системою.

Україна як суверенна і незалежна держава створила певну систему забезпечення інформаційної безпеки, і вживаються заходи для її вдосконалення. Водночас слід зауважити, що, як свідчить аналіз процесів наукового осмислення проблем забезпечення інформаційної безпеки і створення необхідної правової бази, в перші 5-6 років незалежності вказана діяльність здійснювалася значно більш активними темпами. Україна створювала систему забезпечення інформаційної безпеки паралельно з іншими державами на пострадянському просторі, а за деякими напрямами випереджала навіть Російську Федерацію. В останні роки вказані процеси значно уповільнювалися. Незважаючи на певні обсяги досліджень проблем забезпечення інформаційної безпеки, на юридичному рівні досі залишаються незакріпленими: понятійно-категорійний апарат щодо забезпечення інформаційної безпеки.

Наукове осмислення існуючих проблем є основою для розробки і впровадження доцільних й ефективних механізмів регулювання суспільних відносин, пов'язаних із забезпеченням інформаційної безпеки та прав суб'єктів інформаційної діяльності як у середині країни.

Принцип комплексного підходу до організації забезпечення інформаційної безпеки передбачає створення органічно взаємозв'язаної сукупності сил, засобів і спеціальних методів, спрямованих на забезпечення безпеки інформації, що підлягає захисту та сфери її обігу.

Для забезпечення реалізації цього принципу необхідне повне знання всіх компонентів об'єкта захисту, тобто його складових, до яких слід віднести наступні:

інформаційні ресурси, що підлягають захисту, серед яких: відомості, віднесені до державної таємниці, до іншої інформації з обмеженим доступом та відкрита інформація, важлива для особи, суспільства, держави;

сферу обігу інформаційних ресурсів, що підлягають захисту, а саме: державні органи та підприємства, установи й організації незалежно від форм власності; інформаційно-телекомунікаційні системи, різних класів і призначення, включаючи системи збирання, обробки, зберігання і поширення закритої інформації та засоби її захисту;

громадян, у тому числі певне коло посадових осіб та суспільні організації як носії інформації, що підлягає захисту, а також їх право на одержання, використання і поширення інформації, захист конфіденційної інформації та інтелектуальної власності.

Важливе значення для реалізації комплексного підходу до забезпечення інформаційної безпеки має забезпечення логічного поєднання державно-управлінських

рішень у всіх сферах діяльності. Деякі дослідники [7], враховуючи цей аспект як один із проявів комплексного підходу, визначають єдність у рішенні виробничих, комерційних, фінансових та режимних заходів як окремий принцип забезпечення інформаційної безпеки, що має самостійне значення.

Принцип безперервності забезпечення інформаційної безпеки полягає у повсякденному (безперервному) застосуванні як загальних, так і спеціальних засобів і методів забезпечення інформаційної безпеки на всіх її етапах життєвого циклу.

Базовий акт законодавства щодо інформаційної сфери, яким є Закон України "Про інформацію", гарантує право на інформацію, орієнтує на добування, придбання, накопичення, користування і поширення інформації.

Принцип безперервності забезпечення інформаційної безпеки передбачає необхідність впровадження активних, превентивних, ефективних і різноманітних заходів і спеціальних методів; забезпечує безпеку інформації і сфери її обігу у просторі і часі від реальних і потенційних загроз як у звичайних, так і в екстремальних умовах. У процесі співробітництва з іноземними державами та міжнародними організаціями – полягає у розробці і закріпленні у відповідних договорах, угодах взаємо узгоджених процедур, норм, механізмів забезпечення інформаційної безпеки, які передують спільним роботам та обміну вказаною інформацією.

Принцип єдиноначальності передбачає обов'язки покладання правовими нормами на керівників державних органів, органів місцевого самоврядування, підприємств, установ і організацій, діяльність яких пов'язана з забезпеченням інформаційної безпеки, обовў

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Положення про державний експортний контроль: затверджено Указом Президента України від 13.02.1998 року №117 // Офіційний вісник України. – 1998. – № 7. – Ст. 40.
2. Про дальше вдосконалення державного експортного контролю: Указ Президента України від 28.12.1996 року № 1249.
3. Конституція України // Закони України / Верховна Рада України; Ін-т законодавства. – К.: Книга, 1997. – Т. 10. – С. 5-40.
4. Стандартизована звітна форма. Додаток А до Резолюції Генеральної Асамблеї ООН "Про категорії бойової техніки, поставки якої підлягають реєстрації", №46/32. – К.: МЗС України, 1992. – 7 с.
5. Степанов Е. А. Информационная безопасность и защита информации: Уч. пособ. / Е. А. Степанов, И. К. Корнеев. – М.: Инфра, 2000. – 302 с.
6. Долгополый А. Промышленная информация и ноу-хау: особенности создания, защиты и использования / А. Долгополый // Арсенал XXI столетия. – 2000. – № 2. – С. 62-66.
7. Шиверский А. А. Защита информации: проблемы теории и практики / А. А. Шиверский. – М.: Юрист. – 1996. – 112 с.
8. Колпаков В. К. Адміністративне право України: Підручник / В. К. Колпаков, О. В. Кузьменко. – К.: Юрінком Інтер. – 2003. – 544 с.
9. Князєв В. Філософсько-методологічні засади державно-управлінських рішень / В. Князєв, В. Бакуменко // Вісник.УАДУ. – 2000. – № 2. – С. 341-357.
10. Національна безпека України 1994-1996рр.: Наукові доповіді НІСД/Редкол.: О.Ф.Бєлов (голова) та ін. (Сер. "Загальноінститутські доповіді"). – К.: НІСД, 1997. – 200 с.
11. Про державну таємницю: Закон України в редакції від 21.09.1999 року // Відом. Верховної Ради України. – 1999. – № 49. – Ст. 428.