УДК 347.1

Гуйван О. П.,
здобувач кафедри цивільного права і процесу
Харківського національного університету внутрішніх справ

ЗАСАДИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЯК СПОСОБУ ЗАХИСТУ ІНФОРМАЦІЇ

BASES OF INFORMATION SECURITY AS A METHOD OF PROTECTION OF INFORMATION

У роботі проведене дослідження сутності механізмів інформаційного захисту. Вивчено характер та спрямованість різних загроз правовідносинам у сфері інформаційного обороту.

Ключові слова: *інформаційна безпека, охорона інформації, активні та пасивні ризики.*

В данной работе проведено исследование сущности механизмов информационной защиты. Изучен характер и направленность различных угроз правоотношениям в сфере информационного оборота.

Ключевые слова: *информационная безопасность, охрана информации, активные и пассивные риски.*

In this paper, the essence of information protection mechanisms was investigated. The nature and direction of various threats to legal relations in the sphere of information turnover has been studied.

Key words: *information security, information protection, active and passive risks.*

Значення інформації як блага та як об'єкта суспільних відносин важко переоцінити. У Резолюції 59 Генеральної Асамблеї ООН вказано, що свобода інформації є основним правом людини та критерієм усіх інших свобод. У такий спосіб інформація визначається основоположним багатоаспектним явищем, яке використовується та формує принципи здійснення та гарантування багатьох фундаментальних прав особи. Усе це знайшло відображення в Основному Законі України. Так, у ній декларується заборона цензури в інформаційній сфері (ст. 15), таємниця переписки, телефонних розмов, телеграфної та іншої кореспонденції (ст. 31), заборона втручання в особисте та сімейне життя, кожний громадянин має право знайомитися в органах державної влади, органах місцевого самоврядування, установах і організаціях із відомостями про себе, які не є державною або іншою захищеною законом таємницею (ст. 32), право на свободу думки і слова, на вільне вираження своїх поглядів і переконань, кожен має право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб – на свій вибір (ст. 34), право на свободу світогляду і віросповідання (ст. 35), право володіти, користуватися і розпоряджатися своєю власністю, результатами своєї інтелектуальної, творчої діяльності. (ст. 41) та інші.

Різноманітність наукових підходів до постулювання поняття інформації та визначення його сутності з огляду на багатогалузевість застосування цього об'єкту в кожному разі обумовлюється специфікою сфери його використання. Відмінності в способах створення, передачі та поширення інформації, формах закріплення та надання інформаційних продуктів, видах інформаційних загроз обумовлює різні погляди на наукове вивчення ключових аспектів регулювання інформаційних відносин, у тому числі інформаційної безпеки [1, с. 32]. Відтак наразі специфіка кожної галузі визначає особливості її інформаційного правового забезпечення. Це, можливо, сприяє більшій визначеності конкретного правозастосування, але аж ніяк не зумовлює єдність юридичних механізмів та законодавчих і наукових концепцій.

Науковому дослідженню питань різних аспектів інформатизації та розвитку інформаційних процесів, у тому числі і щодо гарантування їхнього правового захисту, присвячено численні праці таких вчених, як С.В. Балабай, М.Я. Швець, Р.А. Калюжний, І.В. Куприянов, В.В. Печенкін, В.А. Саницький, А.М. Карацюба, В.А. Ліпкан та інших. Втім, слід відмітити, що дані дослідження здійснювалися в межах комплексного доктринального аналізу загальних характеристик інформаційних відносин у суспільстві. Тож конкретиці правового регулювання саме охоронних відносин, що часто виникають у цій сфері, приділялося недостатньо уваги. Так, не набули якісних наукових характеристик такі явища, як захист інформації та захист права на інформацію, та не охарактеризовані відмінності між ними, не відмежовані нормативні засади захисту інформації від стороннього втручання та захист від її незаконного поширення тощо. З урахуванням викладеного в рамках даної статті буде розглянуто роль та значення правових норм для формування інформаційного права в цілому та відповідних способів правового впливу на інформаційні відносини з метою їх охорони та захисту для забезпечення стабільності та визначеності учасників таких відносин.

У доктрині та практиці завжди з виникненням певних нових суспільних взаємин та з набуттям ними достатньої розвиненості важливе значення, як для їхніх учасників, так і для соціуму в цілому, набуває відповідне правове забезпечення. У сфері інформаційного обороту, передовсім, мова йде про необхідність правової організації суспільних відносин із метою становлення, існування та прогресивного розвитку інформаційних взаємодій за допомогою

адекватного юридичного інструментарію. Правове регулювання обігу та захисту інформації має ґрунтуватися на основоположних засадах, дотримання яких забезпечить непорушність та дієвість відповідних прав. Це такі основоположні принципи, як свобода шукати, отримувати, передавати, виготовляти та розповсюджувати інформацію в будь-який законний спосіб; відкритість та доступність інформації про діяльність органів держави та місцевого самоврядування, крім випадків, встановлених законом; виключно законодавче (на рівні закону) встановлення обмежень у доступі до інформації; достовірність інформації та своєчасність її надання; недоторканність приватного життя, неприпустимість обробки, в тому числі зберігання, збирання, використання та поширення персональних даних про особу, включаючи конфіденційну інформацію про приватне життя особи, без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини.

Досліджуючи питання інформаційного середовища, окремі науковці вважають, що з огляду на особливості інформації як об'єкту правовідносин вона не має нічого спільного з традиційними об'єктами, такими як матеріальні речі або нематеріальні блага, відтак не вписується до існуючої системи правових відносин. Втім, якщо виходити з позиції цивільного законодавства, то воно достатньо чітко вказує на місце інформації серед особистих немайнових прав особи. Звісно, маємо враховувати істотні сутнісні відмінності інформаційного статусу особи від основних природно-правових її повноважень, але задля забезпечення визначеності конкретних взаємин, саме виходячи з ознак нематеріальності та абсолютності прав на інформацію, здійснюється правова та організаційна побудова доктрини у сфері інформаційних правовідносин, включаючи інформаційну безпеку.

Отже, інформація має притаманні їй специфічні ознаки, які відображають її внутрішню природу та сутність, впливаючи на вибір способів захисту інформаційних прав, саме цим керується законодавець, запроваджуючи механізми юридичного захисту даного об'єкту Зокрема, ці питання знайшли відображення в конкретних законах: щодо охорони такого виду інформації, як державна таємниця (Закон від 21 січня 1994 р. № 3855-XII «Про державну таємницю»), конфіденційна інформація (Закон 2 жовтня 1992 р. № 2657-XII, та закон від 13 січня 2011 р. N 2939-VI)), інформація в автоматизованих системах (Закон від 5 липня 1994 р. № 80/94-ВР) тощо. Детальне дослідження змісту правових актів у частині, присвяченій охороні інформаційних відносин, показує, що законодавець розрізняє поняття «захист інформації» і «захист прав на інформацію». Власне, проблематика захисту цивільних прав на інформацію, будучи вельми актуальною та складною, має враховувати специфічність такого блага як об'єкта права. По-перше, не всі способи захисту, які мають загальний характер (ст. 16 ЦКУ), можуть застосовуватися під час здійснення охоронно-правових повноважень. По-друге, застосування різних санкцій також залежить від суб'єктного складу правовідносин та, особливо, від різновиду об'єкту, на який спрямоване посягання.

У переважній більшості випадків санкції, встановлені в ст. 16 ЦКУ, застосовуються під час порушення права особи на інформацію в такі способи, як ненадання інформації чи доступу до неї, неправомірне поширення, недостовірність тощо. На порушників такого права накладаються санкції у вигляді зобов'язання виконати обов'язок в натурі (скажімо, порушник мусить надати конкретні дані, що відповідають умовам договору), розірвання договору (як приклад подібної оперативної санкції можна згадати передбачені нормативно заходи щодо припинення або зміни правовідношення як наслідок договірного порушення, в тому числі – ненадання інформації), відшкодування нанесеної шкоди, обов'язку спростування інформації, сплатити штраф тощо.

З іншого боку, захист інформації передбачає вчинення комплексу організаційних та юридичних заходів [2, с. 18], які покликані уберегти певну інформацію, що не має бути поширена поза межами, встановленими законом чи договором. У таких ситуаціях законодавство робить акцент на інших способах відповідальності правопорушника. Приміром, законодавство стосовно санкцій за порушення встановленого режиму таємниці, що охороняється законом, порядку поводження із цією інформацією передбачає застосування значного спектру заходів відповідальності, як цивільної, так і кримінальної, адміністративної та дисциплінарної. При цьому кожна відповідальність відрізняється підставою, порядком застосування та наслідками, що обумовлено тяжкістю протиправної поведінки та значимістю відомостей.

У свою чергу, визначення «захист інформації» також може бути розділений на два елементи. Першим із них є організація правового регулювання належної діяльності персоналу, відповідального за збереження та недоступність визначених законом відомостей, і результат у цій сфері, як вже вказувалося, досягається, в першу чергу, за рахунок запровадження ризиків застосування різних жорстких видів відповідальності. Інший напрямок – створення передумов для запобігання несанкціонованому доступу сторонніх осіб до закритої інформації шляхом вчинення заходів превентивного характеру. За великим рахунком, така діяльність охоплюється поняттям «охорона об'єкта», який має ширший зміст, ніж суто правовий захист. Адже захист, за ідеєю, відбувається в межах існуючого правопорушення – після того, як воно почалося, принаймні коли майбутнє посягання стало очевидним. Тоді як охорона містить у собі, крім заходів припинення порушення, ще і попереджувальні дії. Такі правовідносини притаманні, зокрема, для ситуацій, пов'язаних із захистом інформації, яка зібрана, зберігається та обробляється із застосуванням інформаційно-телекомунікаційної інфраструктури. На відміну від загального правового механізму, нормативно-правове регулювання в цій площині переважно відбувається підзаконними нормативно-

правовими актами і потребує узгодження з європейськими стандартами.

На даному етапі суспільного розвитку відбуваються серйозні зміни в інформаційному середовищі, які забезпечують якісний поступ, пов'язаний із масовим використанням комп'ютерних та інформаційних технологій. В Україні, як і в інших частинах світу, набула значного поширення концепція, за якою відомості, що становлять інформацію, мають бути не лише створені та оброблені, а й повинна бути організована можливість об'єктивного сприйняття її людиною та збереження. Бо, в іншому разі, інформація може бути непотрібною, втратить для особи всіляку цінність та значення як благо, здатне задовольнити її потреби. Отже, технічне оснащення інформаційного процесу, хочемо ми того чи ні, вносить до сучасного дефініційного правового визначення певні корективи. Слід погодитися, що сьогодні інформація є сукупністю відомостей про осіб, предмети, факти, події, явища та процеси незалежно від форми їх виявлення, які сприймаються людиною безпосередньо або за допомогою спеціальних пристроїв [3, с. 122].

При цьому, враховуючи величезне значення для обігу інформації новітніх технічних засобів, законодавство має регулювати не лише характер поведінки учасників, а й забезпечувати належні їх взаємодії з техніко-інформаційними засобами, враховуючи особливості нормативного регулювання в цій царині. Наразі існує значне коло нормативних актів, що впорядковують використання систем зберігання і обробки інформації, де в процесі їхнього застосування особлива увага приділяється питанням охорони конфіденційної інформації як фактору, спрямованому на досягнення інформаційної безпеки держави. Це, наприклад, банківські юридичні системи безпечного документообігу, для яких забезпечення захисту інформації є життєво важливим завданням [4, с. 45]. Тож із метою досягнення збалансованості та надійності відповідного захисту інформації та ресурсів правове забезпечення такої діяльності має бути спрямоване на урахування безпекових факторів під час створення інформаційних систем, їхній експлуатації та захисті інформації, яка там знаходиться. При цьому неприпустимо встановлювати в нормативних актах якихось переваг одних інформаційних систем над іншими (за виключенням випадків, коли закон встановлює обов'язковість застосування певних інформаційних технологій для створення й експлуатації державних інформаційних систем).

Таким чином, охорона інформаційних даних у системах, комп'ютерних мережах видається однією з актуальних проблем сучасного права. Адже в силу постійного розвитку та вдосконалення технологій істотний збій в інформаційних системах може зупинити діяльність великих компаній і банків, стати причиною значних збитків. За таких обставин питання боротьби з порушеннями в інформаційній сфері набувають все більшої актуальності. Зростання інтеграції інформаційних технологій у різні сфери, послуг та сервісів, що здійснюються на їхній основі, супроводжується посиленням незаконної активності. Причому особи, які посягають на вказаний об'єкт, можуть бути як добросовісними (користувачі інформації, що не усвідомлюють її обмежений характер), так і недобросовісними (конкуренти чи кримінальні елементи). Тож охорона має поширюватися на будь-яку інформацію, несанкціонований (незаконний) доступ до якої наносить шкоду її власникові чи іншій особі, що правомірно володіє інформацією чи використовує її. Зокрема, підлягає посиленому захисту конфіденційна інформація, бо негативний вплив на неї із боку зловмисників може призвести до дезорганізації діяльності як окремої структури, так і держави в цілому. Особа, яка вчиняє протиправне діяння по відношенню до елемента інформаційної системи, наприклад незаконно отримуючи конфіденційну інформацію, реалізує загрозу та порушує встановлені правила. Це дозволяє говорити про правопорушення, спрямовані на недоторканність інформаційних систем, як окрему групу форм реалізації інформаційних загроз.

З метою боротьби з наведеними правопорушеннями необхідна розробка комплексної та цілеспрямованої системи захисту інформаційних ресурсів. Це дозволить ефективно попередити настання суспільно шкідливих наслідків у результаті таких неправомірних дій учасників інформаційної діяльності, як використання незаконних методів та способів доступу до обмежених ресурсів, порушення порядку розміщення та розповсюдження інформації, порушення прав і свобод людини в процесі інформаційної діяльності. Утім, варто зауважити, що абсолютно надійного та нездоланного захисту створити неможливо, будь-яка система захисту інформації може бути лише адекватна потенційним загрозам, що наразі існують.

У науці під інформаційною безпекою розуміється захищеність інформації від незаконного ознайомлення, поширення, перетворення та знищення та захищеність відповідних систем та ресурсів від неправомірних впливів на них, направлених на порушення їхньої роботоздатності, спроможність нейтралізувати чи послабити дію внутрішніх і зовнішніх потенційних і реальних інформаційних загроз [5, с. 59]. Сутність таких загроз і впливів та їх спрямованість бувають різними. Джерелами загроз можуть виступати: людина, технічні пристрої, моделі, алгоритми, програми; технологічні схеми обробки; зовнішнє середовище [6, с. 67]. Тому інформаційна безпека набуває ключового значення в організації безпеки держави в цілому. Це зумовлено, в першу чергу, швидким розвитком технологічних можливостей сучасних інформаційних систем. Вони наразі стають найбільш значимими та всеохоплюючими за своїм впливом на політику, соціально-економічне життя, суспільну поведінку людей, духовну сферу, ідеологію.

Разом із тим слід відмітити, що на сучасному етапі питання інформаційної безпеки, котрі викликають великий інтерес, на науковому рівні вивчаються

переважно в техніко-прикладній площині та зорієнтовані на захищеність ресурсів технічними засобами. Відверто недостатньо уваги присвячується соціально-правовим аспектами даного питання. Між тим потребує юридичного вирішення проблематика забезпечення достовірності, повноти, доступності інформації, що поряд із забезпеченням її надійної охорони повинно створити комплексну систему. Інформаційна безпека в контексті її правового оформлення ще далека від завершеності концептуального осмислення.

Інформаційні загрози можуть створювати проблеми інформаційній безпеці гуманітарного характеру. Вони, приміром, виникають у зв'язку з безконтрольним використанням персональних даних громадян, втручанням у приватне життя особи, тобто в разі крадіжки інформації, яка може використовуватися в корисливих або інших низинних цілях [7, с. 101]. Недотримання правил інформаційної безпеки може призводити до проблем загальнополітичного характеру. Це пов'язується з атаками на інформаційні системи важливих оборонних об'єктів, транспортних та промислових структур, кібервійнами та електронною розвідкою в інтересах окремих політичних груп, компрометацією державної таємниці та політиків, дезінформацією керівників значних установ та політичних організацій тощо. Нарешті, проблеми з інформаційною безпекою безпосередньо відображаються в економіці. Вони полягають у наслідках витоку, перекручування і втрати комерційної та фінансової інформації, крадіжок брендів і інтелектуальної власності, розкриття інформації про матеріальне становище громадян, промисловому шпигунстві і поширенні матеріалів, що завдають шкоди репутації компаній. Необхідність захисту інформації полягає в тому, що, наприклад, у випадку блокування комп'ютерної інформації власник інформації тимчасово або постійно позбавляється можливості застосовувати зазначену інформацію і здійснювати з нею різні операції у своїх інтересах. Зокрема, власник комп'ютерної інформації не може вчасно оплатити рахунок у банку, здійснити вчасно замовлення на потрібну підприємству техніку і здійснити інші господарські операції [8, с. 90].

У залежності від виду і характеру можливих загроз інформації вони поділяються на активні та пасивні. Згідно з даною класифікацією відбувається і поділ заходів інформаційної безпеки як елементу правової охорони. За даною класифікацією пасивна загроза (ризик) спрямована на позаправове використання інформаційних ресурсів, але при цьому не мається на меті порушення функціонування інформаційної системи. Такі прояви порушень інформаційної безпеки характерні, скажімо, у випадку несанкціонованого доступу до баз даних чи прослуховуванні каналів передачі даних. Чинне національне законодавство за подібні порушення передбачає різні заходи відповідальності зловмисника, як цивільного, так і адміністративного чи кримінального характеру, в залежності від характеру наслідків та тяжкості караного діяння.

До категорії пасивних ризиків порушення слід віднести і такі, що спрямовані, приміром, на недотримання права інтелектуальної власності з метою одержання інформації в обхід встановленого порядку та правил такого доступу. Скажімо, особа всупереч закону за відсутності ліцензійного договору про користування правами інтелектуальної власності використовує неліцензовану копію програмного забезпечення, аби отримати певну інформацію від її власника. У такий спосіб даний суб'єкт порушує не лише нормативні приписи, а й умови договору між власником інформаційного ресурсу та власником програми, яка забезпечує технічну можливість його отримання. На сьогодні вирішення даної проблеми на правозастосовному рівні переведено в площину спірних відносин між порушником та інтелектуальним власником.

При цьому, як правило, інтереси власника інформації залишаються поза увагою правозастосовного органу. Вважаємо, що з розвитком суспільних відносин, наданням їм європейських якісних ознак даному питанню має бути приділена додаткова увага. Пропонується в спеціальних законах про інформацію та право інтелектуальної власності передбачити можливість розподілу сум компенсаційних стягнень за подібні порушення між власниками інтелектуального права та інформаційного ресурсу. Питання механізму та порядку такого розподілу перебуває поза межами предмету даного дослідження і потребує додаткового з'ясування.

Більш значну загрозу інформаційній безпеці становлять активні ризики, направлені на порушення функціонування інформаційної системи шляхом вчинення атаки на її компоненти. То може в найпростішому варіанті проявлятися в пошкодженні працездатності певного гаджета шляхом пошкодження його програмного забезпечення або фізичному руйнуванні комп'ютера. Більш значний та показовий негативний вплив на носії інформації задля її знищення чи спотворення відбувається внаслідок вірусних атак, що часом має значні несприятливі результати. З урахуванням цього дуже важливим засобом превентивного захисту є антивірусні програми. У даному відношенні найбільш ефективними прийнято вважати багатовендерні варіанти, що передбачає застосування антивірусних механізмів від різних виробників і дозволяє збільшити вірогідність виявлення вірусу за рахунок того, що кожен файл чи повідомлення перевірятимуться різними ядрами.

Підсумовуючи проведене дослідження матеріально-правової природи поняття інформаційної безпеки та змісту існуючих потенційних загроз, маємо зазначити, що організація інформаційної безпеки вимагає системного підходу, який передбачає досягнення оптимального співвідношення між організаційними, технічними, правовими, програмними та фізичними заходами реагування. Інформаційні загрози поширені повсюди, вони будуть існувати, допоки існує об'єкт посягання. Відтак головною метою правової науки та законодавця є напрацювання та втілення цілісної системи захисту інформації

та інформаційних ресурсів з урахуванням форм реалізації конкретних посягань. Для цього додатково необхідно провести аналіз таких посягань, зокрема їх чітких обрисів і просторово-часову прив'язку, що дозволяє встановити і зафіксувати відповідний факт впливу небезпечного явища на об'єкт. Також має бути напрацьована практика створення засобів захисту інформації на будь-якому етапі циклу її обробки системою. У такий спосіб буде реалізоване завдання попередження та припинення небезпечного посягання, профілактика загроз та усунення або мінімізація шкідливих наслідків.

ЛІТЕРАТУРА:

1. Кормич Б.А. Організаційно-правові основи політики інформаційної безпеки України : дис.. … доктора юрид. наук. спец. 12.00.07. Одеса, 2004. 427 с.

2. Войціховський А.В. Питання інформаційної безпеки в Україні на сучасному етапі. Право і безпека. 2015. № 3(58). С. 15.

3. Малинин В.Б. Правовое регулирование информации. Ленинградский юридический журнал. 2015. № 3(41). С. 120–129.

4. Чернадчук Т. Забезпечення інформаційної безпеки як один з напрямів банківської діяльності. Юридична України. 2013. № 3. С. 45.

5. Олійник О.В. Стан забезпечення інформаційної безпеки в Україні. Юридичний вісник. 2014. № 2(31). С. 59–65.

6. Хмелевський Р.М. Дослідження оцінки загроз інформаційній безпеці об'єктів інформаційної діяльності. Сучасний захист інформації. 2016. № 4. С. 65.

7. Уголовное право России в вопросах и ответах [Текст]: учебное пособие / Г.Н. Борзенков [и др.]; ред. В.С. Комиссаров. 2-е изд., перераб. и доп. М.: Проспект, 2008. 384 с.

8. Копылов В.А. Информационное право: учеб. пособие. М.: Юристъ, 2009. 532 с.