УДК 347.1

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

ПРЕВЕНТИВНИЙ ПРАВОВИЙ ЗАХИСТ ІНФОРМАЦІЙНИХ РЕСУРСІВ: ОСОБЛИВОСТІ РЕГУЛЮВАННЯ

Постановка проблеми. Сьогодні значна увага приділяється удосконаленню організаційних заходів захисту інформації щодо дотримання правил роботи з інформаційними ресурсами. Власне, будь-який компонент інформаційного середовища – апаратні засоби (комп'ютери та їх складові, програмне забезпечення) і персонал – може бути підданий зовнішньому впливу, вийти з ладу, отримати пошкодження чи інші загрози. Мова йде про визначення певного переліку дозволених (безпечних) і заборонених (небезпечних) станів. У даному контексті має набути визначеності поняття інциденту інформаційної безпеки як будь-якої небажаної, непередбачуваної події, що може порушити діяльність системи чи інформаційну безпеку. Такими загрозами вважаються системні збої, зокрема у програмному забезпеченні, перевантаження, неконтрольовані зміни систем, відмови технічних засобів, порушення правил доступу. До інформаційно-безпекових інцидентів, внаслідок існування яких порушуються певні властивості інформації, інфраструктури чи завдається шкода об'єктам інформаційних систем, також варто віднести такі ризики суб'єктивного характеру, як помилки користувачів і персоналу, недотримання політики або рекомендацій з інформаційної безпеки, втрата послуг, обладнання та приладів, порушення фізичних засобів захисту. З огляду на різний характер, походження та спрямованість загроз повинен бути напрацьований системний захист від інформаційних правопорушень.

Найбільш адекватний рівень інформаційної безпеки досягається у випадку задіяння комплексного підходу, що охоплює не лише організаційні методи захисту, а й програмно-технічні, адміністративні та правові. Зокрема, серйозна роль у забезпеченні безпеки належить системам захисту інформації, різним програмам, які здійснюють захист серверів та окремих користувачів мережі Інтернет від зловмисних дій хакерів, здійснюваних ними ззовні, захист секретної, конфіденційної та особистої інформації від доступу до неї сторонніх осіб і цільового її спотворення, захист від витоку інформації по побічним каналах (по мережах живлення, каналу електромагнітного випромінювання від комп'ютера чи монітора тощо), захист від шпигунських приладів, облаштованих безпосередньо в комплектуючих комп'ютера, забезпечення безпечної передачі інформації та контролю за цілісністю інформаційно-передавального процесу, організації антивірусного захисту і тому подібне [1, с. 65]. У цій сфері неабияке значення має економічна доцільність використання технічних засобів захисту. Вона значною мірою полягає у співставленні затрат на охорону та передбачуваних збитків, яких вдасться запобігти. Інакше кажучи, сума шкоди, наприклад, при зламі системи захисту інформації має перевищувати вартість розроблення і запровадження засобів комплексного захисту інформації.

Вказані засоби правового захисту електронної та комп'ютерної інформації наразі є вкрай важливим елементом діяльності кожної установи, компанії, як державної, так і недержавної форми власності, як великої, так і малої. Окремі об'єкти, такі, як банки, органи державного управління, оборонні підприємства, транспортна інфраструктура, промислові інформаційні мережі тощо, потребують запровадження особливих заходів правового захисту й охорони даних. Це, наприклад, пов'язано з посиленням вимог до якості та комплектації комп'ютерних інформаційних систем відповідно до змісту, характеру і значення завдань, які вони вирішують.

Аналіз останніх досліджень та публікацій. Питання інформаційної безпеки та захисту інформації було досліджено в працях таких науковців, як: І. Арістова, В. Голубєв, В. Гриценко, О. Дзьобань, Р. Калюжний, М. Кареліна, Б. Кормич, В. Ліпкан, С. Ляшко, Ю. Максименко, В. Печенкін, В. Цимбалюк, О. Юдін та інші. Водночас вказані роботи переважно були зосереджені на питаннях організаційного та правового реагування на реальні правопорушення та загрози, які відбуваються в інформаційному середовищі. Одночасно недостатньо вивченим залишається питання юридичного забезпечення превентивних заходів, спрямованих на попередження майбутніх ризиків щодо витоку інформації, несанкціонованого доступу до неї, охорони матеріальних інформаційних носіїв та електронного і комп'ютерного обладнання. Тож метою статті є на основі вивчення різних доктринальних підходів з'ясувати правовий зміст, реальну сутність і порядок застосування таких охоронних засобів, як превентивні дії правоволодільця з метою захисту інформації як об'єкта посягання.

Система інформаційного захисту мусить невпинно розвиватися, працюючи на випередження

у розвиткові інформаційних загроз, що розглядаються в цій праці. Концепція інформаційної безпеки, зокрема при використанні методів охорони в мережах і комп'ютерних системах, може стати ефективною та дієвою, якщо буде постійно оновлюватися, ґрунтуватися на останніх наукових розробках у сфері права, техніки, управління тощо. Це дасть змогу уникнути нових, щораз більш досконалих і витончених атак і запобігти шкідливим наслідкам. Інакше кажучи, забезпечення інформаційної безпеки не є разовим актом, цей процес буде розвиватися і вдосконалюватися, допоки будуть існувати загрози, а останні здійснюватимуться, поки існуватиме предмет посягання – інформація.

Отже, в інформаційній сфері одним із визначальних напрямків правової охорони є захист інформації. Цьому питанню з огляду на появу нових технологій, розвиток комп'ютерних систем збереження та оброблення інформації наразі приділяється підвищена увага. Бо для того, щоб відповідати сучасним вимогам, ефективність інформаційного захисту мусить зростати разом з удосконаленням технічних аспектів архітектури збереження даних. Сучасна система оброблення даних та інформації є досить складною, вона містить значну кількість компонентів, які, у свою чергу, складаються із блоків та елементів різного ступеня автономності. Усі ці складові системи між собою взаємопов'язані та здійснюють постійний обмін даними. У свою чергу загроза інформаційним ресурсам стала підставою того, що забезпечення інформаційної безпеки набуло значення однієї з обов'язкових характеристик інформаційної системи. Особи – власники інформації (економічної, політичної, правової, індивідуальної та іншої) повинні розробляти необхідну документацію із захисту інформації, нормативні та рекомендаційні положення, здійснювати відповідне технічне оснащення. Усе це спрямоване на запобігання проникненню зловмисників до інформаційних носіїв, технічним негараздам і виходам із ладу апаратних і програмних засобів, помилкам персоналу.

Правовий захист в інформаційній сфері спрямований на гарантування недоторканості суб'єктивних прав носія та забезпечення їхньої вільної реалізації, охорону від вчиненого чи можливого правопорушення. До того ж як інформаційне порушення слід розглядати таке, що завдає шкоди (небезпеки) інформаційним правам або свободам людини й громадянина, інформаційній інфраструктурі держави або скоюється за допомогою інформаційно-телекомунікаційних технологій чи засобів зв'язку [2]. Порушення інформаційних прав особи як необхідного кваліфікаційного предмета повинні мати об'єкт, стосовно якого вони вчиняються. Таким об'єктом є інформація у вигляді документованих або публічно оголошених відомостей про події та явища, що відбуваються в суспільстві, державі й навколишньому середовищі. Ці явища можуть відбуватися в галузі політики, економіки, культури, охорони здоров'я, а також у соціальній, екологічній, міжнародній та інших сферах. Одночасно в різних випадках інформація може відігравати як головну, так і другорядну роль. Суб'єктами інформаційних відносин, а відтак і можливими правопорушниками є громадяни України, юридичні особи й держава, інші держави, їх громадяни та юридичні особи, міжнародні організації й особи без громадянства.

Серед основних загроз інформаційній безпеці вважаються такі, як несанкціонований доступ до інформації, витоки її, розголошення, пошкодження, зокрема спотворення, знищення як самої інформації, так і її носіїв. Практика показує, що закладена в основу нормативного регулювання презумпція попереджувального значення закону, на жаль, не працює задовільно. Нормативні приписи мають ефект лише тоді, коли потенційний порушник усвідомлює, що він може понести кару за несанкціонований доступ до інформації, незаконне втручання в діяльність інформаційних систем тощо. Тож з огляду на проблемність із пошуками та притягненням до відповідальності зловмисників в інформаційному середовищі наразі створюється та задіюється велика кількість шкідливого та шпигунського продукту, використання якого спрямовується на пошкодження контенту в базах даних і документів, що зберігаються в комп'ютерних мережах. Постійні оновлювання, поповнювання й удосконалення таких програм змушують володільців інформаційних ресурсів постійно модернізувати системи безпеки. Адже загальні цивільно-правові способи захисту від подібних правопорушень у вигляді відшкодування нанесеної шкоди часто виявляються просто фізично неможливими.

Звісно, цивільно-правове законодавство передбачає можливість особи, чиє суб'єктивне право порушене, захистити його в різний спосіб. Як головний і найбільш поширений із них розглядається звернення управненої особи до компетентних органів держави з вимогою про захист порушеного чи оспорюваного права. Це один із найбільш дієвих засобів захисту для носіїв суб'єктивних цивільних прав. Зокрема, подібний захист може мати судову форму реалізації, і подібна можливість входить до змісту суб'єктивного матеріального права на позов [3, с. 38–39]. Водночас судовий спосіб захисту порушеного цивільного права не є єдиним варіантом реалізації права на захист. Тим більше, що держава не завжди може оперативно та в прийнятній для суспільства формі забезпечити примусовий захист права. Ст. 20 Цивільного кодексу України (далі – ЦКУ) чітко вказує про те,

що право на захист здійснюється особою на свій розсуд [4, с. 13]. Цю норму слід розуміти так, що особа має право вирішувати не лише питання про захист чи відмову від нього, а й обирати відповідні його форму та спосіб.

У випадку, коли охоронне правовідношення виконується без звернення до державного юрисдикційного органу, право на захист може здійснюватися шляхом активної поведінки самого уповноваженого. Логічно, що при цьому акценти робляться на застосуванні механізму, пов'язаного з перешкоджанням вчиненню протиправних дій щодо інформації або інформаційних ресурсів. Такі діяння мають превентивний характер. З правової точки зору вони спрямовані на закріплення повноважень суб'єктів правоохоронного процесу на попереджувальні акти стосовно охорони інформаційних прав та інтересів громадян й організацій. Подібним заходам превентивного характеру через специфіку охоронюваного об'єкта надається перевага навіть у межах комплексного системного регулювання з урахуванням задіяння організаційних, технічних та адміністративних заходів. Це дає змогу визнати такий спосіб захисту як основний, коли йдеться про перешкоджання правопорушенням у сфері інформаційної безпеки, зокрема за наявності посягань на право власності на інформацію.

Як правило, факт наявності посягання визначається внаслідок фіксації реалізації загрози – впливу небезпечного явища на певний інформаційний об'єкт, що має конкретні просторові та часові координати. Водночас чинне законодавство передбачає можливість протидії таким протиправним діянням не лише після їхнього настання, а й за наявності реальних і визначених підстав вважати конкретні загрози реальними та шкідливими. Відтак можливість запобігання подібному впливу, його профілактика, усунення та мінімізація негативних наслідків цілком охоплюються ідеологією охоронного правовідношення, і подібні вчинки є складовою частиною правового статусу уповноваженої особи. Це досить показово саме в царині інформаційних взаємин, позаяк тут загрози охоронюваному благу пов'язані з діяльністю людини, що носить протиправний характер чи набуде його надалі.

Інформаційна безпека в коментованій царині здійснюється в межах заходів охоронного типу та має значні відмінності від класичних правозахисних функцій. До того ж варто відділяти превентивні функції, що реалізуються в даній сфері, від функцій, спрямованих на реагування на правопорушення, яке відбулося. Для інформаційних відносин і, зокрема, для інформаційної безпеки прикметним є надання значного пріоритету саме першій із наведених категорій. Адже, як відомо, краще попередити можливе правопорушення, ніж усувати його наслідки. На відміну від цивільно-правового поняття «захист права», під яким розуміється здійснення захисних повноважень у межах охоронного правовідношення, яке почалося після порушення, а відповідні заходи спрямовані на відновлення нормального стану права та покарання зловмисника, превентивні заходи спрямовуються на запобігання факту правопорушення, і подібні дії охоплюються більш широким визначенням «охорона права».

Самозахист вважається законним і допускається за наявності очевидної небезпеки порушення цивільного права, існування фактичної спроможності щодо припинення (попередження) порушення власними силами, адекватності заходів ступеню небезпеки, яка загрожує носієві охоронюваного суб'єктивного права. Відповідно до припису ст. 1169 ЦКУ при застосуванні таких заходів у випадку протиправних посягань порушнику може бути заподіяна шкода. Скажімо, вийде з ладу його обладнання, за допомогою якого він посягав на несанкціоноване отримання конфіденційної інформації. Щоб вказані дії, пов'язані з нанесенням шкоди в результаті охоронних діянь не кваліфікувалися як неправомірні, закон встановлює відповідні нормативні ознаки: у результаті самозахисту від протиправних посягань не були перевищені межі необхідної оборони. До того ж слід враховувати особливості цивільного захисту порушеного права, зокрема, важливість блага, якому загрожувало посягання, характеристику способу здійснення загрози та захисту, відсутність елементів злочину в самому неправомірному діянні та заході протидії йому. Запровадження вказаного механізму покладає на правозастосовні органи серйозне завдання: встановлення в разі виникнення спірних ситуацій у кожному окремому випадку меж здійснення охоронного права, виходячи з аналізу співвідношення усунутої та вірогідної шкоди і своєчасності реагування.

Недотримання вказаного принципу, що часто виявляється у неправильному встановленні фактичного стану, на практиці проявляється у рішеннях, коли судові органи розглядають правомірні дії розпорядника інформації як правопорушення, і навпаки. З урахуванням недосягнення поки що однозначності в правозастосовній практиці щодо питань обґрунтованості реальності загрози й адекватності охоронних превентивних заходів, не може набути подальшого розвитку і концепція, що має поширення в літературі, стосовно встановлення правової відповідальності не тільки за завдану шкоду, але і за «делікт створення небезпеки» [5, с. 798–802]. Вважаємо, що навряд чи можна в такий спосіб тлумачити приписи Цивільного кодексу про захист права власності, адже ст. 386 ЦКУ не передбачає відшкодування шкоди в разі наявності у власника підстав передбачати

можливість порушення свого права власності іншою особою. А норми гл. 82 даного акту прямо не визнають загрозу заподіяння шкоди підставою настання цивільної відповідальності. Тож можливість утілення юридичної концепції про необхідність перенесення деліктної відповідальності «на більш ранній ступінь, коли протиправне діяння створює можливість заподіяння шкоди або коли сама діяльність має небезпечні властивості» залежить від доктринальної та правозастосовної визначеності поняття «очевидна загроза», яке не має опрацьованості й однозначного усвідомлення.

Отже, як бачимо, заходи самозахисту як оборонного, так і превентивного характеру, мають бути адекватними обсягам можливого посягання на суб'єктивне право, повинні мати чіткі межі свого здійснення, одночасно будучи втіленням правопорядку в суспільстві [6, с. 38]. Здійснення правової охорони шляхом вчинення заходів самозахисту можливе до початку фізичних дій посягаючого від моменту, коли виникла реальна загроза посягання [7, с. 14–16]. До того ж ознака реальності посягання є визначальною для кваліфікації вказаних превентивних дій як правомірних засобів самозахисту. Саме в цьому полягає юридична відмінність між поняттями «охорона» та «захист» суб'єктивного матеріального права.

Скажімо, встановлення на вхідних дверях у приміщеннях серверних спеціальних пристроїв, які здатні перешкодити проникненню та запобігти порушенню речового права на інформацію, або приладів, пов'язаних з її обробкою, треба кваліфікувати як загально-охоронні заходи, а не як спосіб захисту, попри зворотне твердження окремих цивілістів [8, с. 116–117]. Якщо у випадку їхнього задіяння при правопорушенні з боку певного суб'єкта останньому було завдано серйозної шкоди, за загальним правилом, це не буде вважатися діянням, вчиненим у стані самозахисту. І навпаки, якщо особа чітко знає, що на її суб'єктивне право чи законний інтерес відбудеться конкретне посягання, або сукупність наявних факторів свідчить про реальність такої можливості, вчинення тих самих дій, що й у попередній ситуації, мусимо кваліфікувати як заходи самозахисту. Беручи до уваги викладене, заходи самостійної реалізації зазначених охоронних повноважень щодо захисту цивільних прав у разі їхнього оскарження до суду можуть бути визнані неадекватними не тільки з огляду на невідповідність їхнього змісту нормам законодавства, моральним засадам суспільства та конкретній обстановці, а й зважаючи на їхню віддаленість від моменту порушення. Скажімо, якби дії фактичного плану були вчинені під час нападу або коли мала місце реальна його загроза, їх можна було б кваліфікувати як правомірні односторонні дії управленої особи. Коли реагування почалося після закінчення нападу, воно не може бути віднесене до заходів самозахисту [9, с. 22].

Як підкреслювалося у цивілістичній літературі, охоронні дії із самозахисту в цивільно-правовому значенні цього терміна притаманні, як правило, захисту абсолютних суб'єктивних прав, зокрема речових [10, с. 17–18]. З огляду на те, що Цивільний кодекс України кваліфікує інформацію як різновид особистих нематеріальних благ особи, такий захист, як превентивні заходи охоронного типу, є не тільки можливим, а й прямо санкціонованим у нормативному порядку. Те ж саме можемо сказати про захист носіїв інформації, елементів електронних систем, мереж, комп'ютерного та іншого обладнання. Адже в цьому випадку попереджувальні охоронні дії вчиняються власником із метою запобігання протиправним посяганням. Наприклад, встановлення антивірусної програми має превентивне значення для захисту програмного забезпечення та обладнання від майбутнього знищення чи пошкодження, тож вони цілком охоплюються поняттям правомірних дій охоронного типу. У такий спосіб захищається абсолютне право власності шляхом здійснення заходів самооборони.

Зважаючи на викладене, треба зробити певні висновки. Сьогодні інформаційний обіг і відповідні технології є невід'ємним елементом нашого життя, за допомогою мережевих технологій наразі регулюються практично всі сторони суспільних відносин. Дані процеси потребують підвищеної уваги як науковців, так і законодавця, бо вони мають досить специфічний предмет дослідження та регулювання, особливістю цих відносин є наявність технічного компонента, інформаційне наповнення, особливий суб'єктний склад. Тож нормативно-правовий інструментарій у цій сфері повинен розбудовуватися з урахуванням не тільки особливостей правової, інформаційної та технічної природи, але також зважаючи на складні соціально-політичні, гуманітарні, морально-етичні зв'язки, які створюються в соціумі навколо та всередині інформаційного середовища.

До того ж з огляду на те, що інформаційний оборот шляхом використання технічних засобів оброблення і передачі даних постійно зростає та поглиблюється, охоплюючи практично всі галузі діяльності суспільства, величезне значення надається питанням організації та забезпечення інформаційної безпеки. У разі порушення чи за наявності вагомих підстав вважати, що існує реальна загроза порушення інформаційних прав особи, носій абсолютних прав може захищати їх як шляхом відповідного реагування на вчинене посягання (відновлення становища, що було до порушення, відшкодування збитків і моральної шкоди, заборона подальших дій, що порушують право тощо), так і шляхом задіяння превентив-

них механізмів. Останні полягають у вчиненні дій охоронного типу, які є адекватними характеру та рівню передбачуваних загроз і спрямовані на запобігання ризикам, фізичному недопущенню посягань і припиненню правопорушення в момент його початку. Відтак не можна розглядати судову чи несудову санкцію, що реалізується в межах охоронного правовідношення, лише як механізм спонукання правопорушника до виконання встановленого правила поведінки, тобто розуміти санкцію тільки в контексті її відновлювального значення. Цивільно-правова санкція має й інші функції: компенсаторну, штрафну, попереджувальну тощо. У статті з'ясовано, що превентивний захист інформаційних прав як прояв самозахисту є основним способом у даній сфері охоронно-правових відносин. Адже для правоволодільця часто неможлива, а іноді й недоцільна подальша реалізація повноваження, закладеного в порушеному праві. Натомість наявність самої можливості протидії та застосування заходів самозахисту суттєво впливає на належність виконання зобов'язаною особою в абсолютних відносинах свого регулятивного обов'язку – не перешкоджати уповноваженому реалізувати своє право.

Література

1. Токарев А. Системы защиты информации как основа информационной безопасности, и методы повышения эффективности функционирования данных систем. Территория науки. 2013. № 3. С. 63–67.

2. Максименко Ю. Інформаційні правопорушення: поняття та ознаки. Глобальна організація союзницького лідерства. URL: http://www.goal-int.org/informacijni-pravoporushennya-ponyattya-ta-oznaki.

3. Мотовиловкер Е. Право на иск в механизме защиты субъективных гражданских прав. Механизмы защиты субъективных гражданських прав: сб. науч. тр. / Под ред. В.В. Бутнева, Ярославль: ЯрГУ, 1990. С. 36–46.

4. Антонюк О. Право учасників цивільних правовідносин на самозахист: дис. ... канд. юрид. наук. Харків, 2004. 212 с.

5. Боброва Д. Зобов'язання, що виникають зі створення небезпеки при порушенні довкілля. Зобов'язальне право: теорія і практика. К.: Юрінком Інтер, 1998. 912 с.

6. Сидельников Р. Легітимація і легалізація самозахисту цивільних прав. Проблеми законності. 2003. Вип. № 59. С. 34–39.

7. Витрянский В. Судебная защита гражданских прав: автореф. дис. ... докт. юрид. наук. М., 1996. С. 44 с.

8. Страунинг Э. Самозащита гражданских прав: дис. ... канд. юрид. наук. М., 1999. 167 с.

9. Луць В. Строки захисту цивільних прав. Конспекти лекцій зі спецкурсу. Львів: ЛДУ, 1993. 60 с.

10. Завидов Б. Гражданские права предпринимателей нуждаются в защите / Б. Завидов, О. Гусев. Законодательство и экономика. 2000. № 8. С. 6–20.

Анотація

Гуйван О. П. **Превентивний правовий захист інформаційних ресурсів: особливості регулювання.** – Стаття.

У статті проаналізовано теоретичні та практичні засади організації захисних правових дій, спрямованих на перешкоджання протиправним посяганням в інформаційному середовищі. Встановлено, що дії управленої на захист особи можуть вчинятися як у судовому, так і позасудовому порядку. До останнього засобу відносяться превентивні дії охоронного змісту. Вони забезпечують запобігання незаконному доступу до інформації, припинення протиправних загроз, уникнення шкоди. Такі діяння охоплюються цивільно-правовим змістом охорони суб'єктивного права.

Ключові слова: охорона права, превентивний захист, безпека інформації.

Аннотация

Гуйван О. П. **Превентивная правовая защита информационных ресурсов: особенности регулирования.** – Статья.

В статье проанализированы теоретические и практические основы организации защитных правовых действий, направленных на препятствование противоправным посягательствам в информационной среде. Установлено, что действия управомоченного на защиту лица могут совершаться как в судебном, так и внесудебном порядке. К последнему средству относятся превентивные действия охранительного содержания. Они обеспечивают предотвращение незаконного доступа к информации, прекращение противоправных угроз, избежание вреда. Такие действия охватываются гражданско-правовым содержанием охраны субъективного права.

Ключевые слова: охрана права, превентивная защита, безопасность информации.

Summary

Guyvan O. P. **Preventive legal protection of information resources: the features of regulation.** – Article.

The article analyzes the theoretical and practical foundations of the organization of protective legal actions aimed at preventing illegal encroachments in the information environment. It is established that the actions of the person authorized for protection can be carried out both in judicial and extrajudicial order. The latter means preventive actions of protective content. They ensure the prevention of illegal access to information, the cessation of illegal threats, avoidance of harm. Such actions are covered by the civil law content of the protection of subjective law.

Key words: protection of rights, preventive protection, information security.