

Правове регулювання захисту інформації в інформаційних системах

Шапіро В. С.

Сумський державний університет, юридичний факультет
аспірант каф. адміністративного, господарського права та фінансово-економічної безпеки
e-mail: shapiro_viktoriya@mail.ru

The report reveals the content of legal regulation of information security in information systems, particularly in telecommunications and information and telecommunication systems. Basic principles of informative safety of Ukraine are considered, established the legal basis of information in information systems and urgent problems are selected in the field of information security in information systems.

ВСТУП

Сьогодні однією із сучасних тенденцій розвитку українського суспільства є поступова інтеграція до світового інформаційного простору. Існування та функціонування світового інформаційного суспільства більшою мірою базується на здійсненні діяльності на основі надання певних послуг, використовуючи засоби електронного зв'язку та новітніх комп'ютерних технологій. Таким чином, слід зазначити, що інформаційне суспільство характеризується зростанням ролі інформації, як його базового елементу, а також швидкістю процесів її розповсюдження завдяки комп'ютерно-обчислювальній техніці, що дає змогу створення нових інформаційних технологій. Зважаючи на високий рівень інформатизації суспільства і розповсюдження інформації через інформаційні та телекомунікаційні системи сьогодні досить актуальним постає питання її захисту.

Одним з основних прав громадян України в сфері інформаційних правовідносин є право на інформацію, що закріплено як в законах, так і підзаконних нормативно-правових актах. Це право знаходить свою регламентацію в Конституції України від 28 червня 1996 року, що є основним джерелом. Відповідно до ст. 34 Конституції кожен має право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб – на свій вибір. Положення ст. 32 Основного Закону також є важливим, відповідно до якого не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини [1].

Слід відмітити, що Основний Закон дає загальне визначення права на інформацію. Розкриття питань щодо правового регулювання інформаційних відносин можна знайти в Законах України, зокрема Законі «Про внесення змін до Закону України «Про інформацію» від 13 січня 2011 року, «Про доступ до публічної інформації» від 13 січня 2011 року тощо [2; 4].

Зміст права громадян на одержання інформації складається з цілого ряду правомочностей, серед яких право на доступ до документів, інформаційних ресурсів та систем, право здійснювати запити, адресовані органам влади, а також знайомитися і отримувати від органів державної влади та органів місцевого самоврядування інформацію про їх діяльність, зокрема доступ до офіційних документів, можливість отримувати інформацію через засоби масової діяльності, наукових праць, через всесвітньо відому глобальну мережу Інтернет.

Задля ефективності реалізації права громадянами на одержання інформації в чинному законодавстві безпосередньо закріплено ряд принципів інформаційних правовідносин. Відповідно до ст. 2 Закону України «Про внесення змін до Закону України «Про інформацію» такими принципами є:

- гарантованість права на інформацію;
- відкритість, доступність інформації, свобода обміну інформацією;
- достовірність і повнота інформації;
- свобода вираження поглядів і переконань;
- правомірність одержання, використання, поширення, зберігання та захисту інформації; захищеність особи від втручання в її особисте та сімейне життя.

Відповідно до Указу Президента України «Про доктрину інформаційної безпеки України» від 08 липня 2009 року: за умов глобальної інтеграції та жорсткої міжнародної конкуренції головною ареною зіткнень і боротьби різновекторних національних інтересів держав стає інформаційний простір. Сучасні інформаційні технології дають змогу державам реалізувати власні інтереси без застосування воєнної сили, послабити або завдати значної шкоди безпеці конкурентної держави, яка не має дієвої системи захисту від негативних інформаційних впливів. Таким чином, інформаційна безпека є невід'ємною складовою кожної зі сфер національної безпеки. Водночас інформаційна безпека є важливою самостійною сферою забезпечення національної безпеки. Саме тому розвиток України як суверенної, демократичної, правової та економічно стабільної держави можливий тільки за умови забезпечення належного рівня її інформаційної безпеки [3]. Відповідно до основних засад інформаційної безпеки України її забезпечення має базуватися на певних принципах, серед яких:

- свобода збирання, зберігання, використання та поширення інформації;
- достовірність, повнота та неупередженість інформації;
- обмеження доступу до інформації виключно на підставі закону;
- гармонізація особистих, суспільних і державних інтересів;
- запобігання правопорушенням в інформаційній сфері;
- економічна доцільність;
- гармонізація українського законодавства в інформаційній сфері з міжнародним;
- пріоритетність національної інформаційної продукції.

Забезпечення захисту інформації в інформаційних системах України здійснюється відповідно до Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджених Постановою Кабінету Міністрів України від 29 березня 2006 року. Відповідно до неї захисту в системі підлягає:

1) відкрита інформація, яка належить до державних інформаційних ресурсів, а також відкрита інформація про діяльність суб'єктів владних повноважень, військових формувань, яка оприлюднюється в Інтернеті, інших глобальних інформаційних мережах і системах або передається телекомунікаційними мережами;

2) конфіденційна інформація, яка перебуває у володінні розпорядників інформації, визначених ч. 1 ст. 13 Закону України «Про доступ до публічної інформації»;

3) службова інформація; інформація, яка становить державну або іншу передбачену законом таємницю;

4) інформація, вимога щодо захисту якої встановлена законом [5].

У системі здійснюється контроль за цілісністю програмного забезпечення, яке використовується для обробки інформації, запобігання несанкціонованій його модифікації та ліквідація наслідків такої модифікації. Контролюється також цілісність програмних та технічних засобів захисту інформації. У разі порушення їх цілісності обробка в системі інформації припиняється.

З метою забезпечення захисту інформації в системі створюється комплексна система захисту інформації. При цьому відповідальність за забезпечення захисту інформації в системі, своєчасне розроблення необхідних для цього заходів та створення системи захисту

покладається на керівника (заступника керівника) організації, яка є власником (розпорядником) системи, та керівників її структурних підрозділів, що забезпечують створення та експлуатацію системи. Організація та проведення робіт із захисту інформації в системі здійснюється службою захисту інформації, яка забезпечує визначення вимог до захисту інформації в системі, проектування, розроблення і модернізацію системи захисту, а також виконання робіт з її експлуатації та контролю за станом захищеності інформації. Захист інформації на всіх етапах створення та експлуатації системи здійснюється відповідно до розробленого службою захисту інформації плану захисту інформації в системі, який повинен містити:

- завдання захисту, класифікацію інформації, яка обробляється в системі, опис технології обробки інформації;
- визначення моделі загроз для інформації в системі;
- основні вимоги щодо захисту інформації та правила доступу до неї в системі;
- перелік документів, згідно якими здійснюється захист інформації в системі;
- перелік і строки виконання робіт службою захисту інформації.

Вимоги та порядок створення системи захисту встановлюються Адміністрацією Держспецзв'язку [5]. Здійснення захисту прав суб'єктів у сфері користування інформаційними ресурсами, застосування інформаційних систем, а також розробки новітніх технологій і засобів щодо їх забезпечення має на меті попередження правопорушень та відновлення порушених прав, що включає відшкодування заподіяної шкоди. Такий захист здійснюється судом з урахуванням специфіки здійсненого правопорушення та розміру завданих збитків.

ВИСНОВКИ

На сьогодні в результаті порушення роботи автоматизованих систем можуть виникнути проблеми щодо вагомих порушень функціонування інформаційного суспільства. Це пояснюється виникненням і функціонуванням в наш час злочинних формувань, які для здійснення неправомірних дій можуть використовувати досягнення науково-технічного розвитку. Таким чином, нагальною є потреба захисту інформації в інформаційних та комунікаційних системах від несанкціонованого доступу та її використання, розроблення відповідних заходів боротьби з таким явищем задля нормального функціонування зазначених систем та забезпечення належного рівня інформаційної безпеки в державі.

ЛІТЕРАТУРА

- [1] Конституція України від 28 червня 1996 року // ВВР. – 1996. – № 30. – ст. 141.
- [2] Про внесення змін до Закону України «Про інформацію»: Закон України від 13 січня 2011 року [Електронний ресурс]. – Режим доступу: <http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2938-17>
- [3] Про доктрину інформаційної безпеки України: Указ Президента України від 08 липня 2009 року [Електронний ресурс]. – Режим доступу: <http://zakon2.rada.gov.ua/laws/show/514/2009>
- [4] Про доступ до публічної інформації: Закон України від 13 січня 2011 року [Електронний ресурс]. – Режим доступу: <http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2939-17>
- [5] Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах: Постанова Кабінету Міністрів України від 29 березня 2006 року [Електронний ресурс]. – Режим доступу: <http://zakon2.rada.gov.ua/laws/show/373-2006-%D0%BF>.

