ІМПЛЕМЕНТАЦІЯ МІЖНАРОДНИХ ПРИНЦИПІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ЗАКОНОДАВСТВО УКРАЇНІ ЯК ГАРАНТІЯ ПРАВ ЛЮДИНИ

Андрій Андрійович СТАРОДУБЦЕВ,

доктор юридичних наук, доцент,
професор кафедри права Національного
аерокосмічного університету
ім. М. Є. Жуковського
«Харківський авіаційний інститут»

Василь Романович ОСТРОПІЛЕЦЬ,

кандидат юридичних наук,
доцент кафедри права Національного
аерокосмічного університету
ім. М. Є. Жуковського
«Харківський авіаційний інститут»

Ірина Миколаївна ПОПОВИЧ,

кандидат юридичних наук, головний науковий
співробітник лабораторії теоретичних
досліджень, редакційно-видавничої та науково-
методичної діяльності Національного наукового
центру «Інститут судових експертиз
ім. Засл. проф. М. С. Бокаріуса»

Реформування державних інституцій після Революції гідності торкнулося усіх сфер суспільного життя, і в першу чергу, захисту основних прав і свобод людини і громадянина. Зокрема, Стратегією національної безпеки України, введеною в дію Наказом Президента України від 14 вересня 2020 року № 392/2020 [1] підкреслено, що посилення спроможностей національної системи кібербезпеки для ефективної протидії кіберзагрозам у сучасному безпековому середовищі є найголовнішим завданням усіх державних органів та інституцій. Адже національними інтересами України в інформаційній сфері визнаються життєво важливі інтереси особи: забезпечення конституційних прав і свобод людини на збирання, зберігання, використання та поширення інформації; забезпечення конституційних прав людини на захист приватного життя; захищеність від руйнівних інформаційно-психологічних впливів [2] тощо.

Удосконалення інформаційно-комунікаційні технологій супроводжується розширенням можливостей їх недобросовісного використання, яке створює загрози інформаційній безпеці та може призводити до порушення прав людини.

У науковій літературі проблемам імплементації міжнародних принципів інформаційної безпеки в законодавство Україні було приділено увагу

таких вчених, як: І. Арістова, О. Баранов, О. Довгань, І. Корж, Р. Калюжний, О. Логінов, В. Ліпкан, А. Марущак, Є. Мануйлов, І. Панова, М. Присяжнюк, В. Рубан, Я. Собків, О. Тихомиров, Л. Харченко, В. Шамрай та інших. Але, аналіз питань імплементації міжнародних принципів інформаційної безпеки в законодавство Україні як гарантії забезпечення прав людини виявило багато теоретичних та практичних проблем недостатності системності й ефективності відповідних правових практик.

Імплементація міжнародних принципів інформаційної безпеки в законодавство Україні забезпечить посилення державного впливу на використання інформації в різноманітних Інтернет ресурсах та значно підвищить стан убезпечення прав людини в нашій державі.

У вітчизняній правовій літературі під інформаційною безпекою розуміється стан захищеності інформаційного простору, який забезпечує його формування та розвиток в інтересах особистості, суспільства та держави. При цьому поняття «інформаційна безпека» розглядається як більш загальна категорія по відношенню до поняття «захист інформації», в якому акцент робиться на комплексі заходів і дій, спрямованих на забезпечення безпеки информации [4]. В даному випадку мова йде про стан захищеності інформації, а не інтересів особистості, суспільства і держави.

У правовій доктрині Європейського Союзу та США визначення «інформаційної безпеки» здійснюється через перерахування конкретних елементів інформаційної сфери, на захист яких вона спрямована[1] [3, с. 17], і пов’язується з правовими принципами конфіденціальності, цілісності та доступності інформації й інформаційних систем [4, с. 4].

Реалізація даних принципів дозволяє забезпечити баланс інтересів між різними сторонами правовідносин, виступаючи, таким чином, гарантією прав людини у сфері забезпечення інформаційної безпеки.

Роль *принципу конфіденційності* полягає в запобіганні шкоди, яку може бути заподіяно суспільним відносинам в результаті неправомірного надання і поширення інформації, що зберігається в таємниці в силу її значення для безпеки особистості, суспільства або держави. Даному принципу відповідає свого роду право «приховувати» інформацію, тобто зберігати її в таємниці, обмежувати доступ третіх осіб до неї, контролювати її цільове використання.

На відміну від принципу конфіденційності, принцип *забезпечення цілісності інформації* став актуальним в процесі розвитку комп'ютерних технологій і появи можливостей несанкціонованого доступу до інформації з метою внесення до неї змін або знищення. Особа, яка володіє інформацією або правом доступу до інформації, має право вимагати забезпечення її цілісності, а також в ряді випадків цілісності носія інформації, тобто збереження їх в оригінальному, незмінному вигляді, забезпечувати невтручання в структуру (форму) і зміст інформації.

---

[1] У даному випадку інформаційна безпека може передбачати захист інформаційних об'єктів, які охоплюють не тільки власне інформацію, але також комп'ютерне програмне забезпечення, технічні засоби, мережі та інфраструктуру, яка забезпечує інформаційні системи.

Принцип доступності відіграє важливу роль у формуванні гарантій права особи на доступ до інформації. Даний принцип спрямований на запобігання обмеження і створення умов доступу до соціально-значимої інформації, перш за все, при взаємодії людини з органами влади, а також до іншої інформації, представлення якої він має право вимагати. Цей принцип лежить в основі реалізації заходів по забезпечення доступу до інформації про діяльність державних органів і органів місцевого самоврядування, екологічної інформації, в тому числі шляхом розміщення інформації на офіційних сайтах державних органів і організацій.

Дотримання названих принципів суттєво впливає на захист прав та свобод людини, особливо конституційного права на таємницю особистого життя. У стаття 32 Конституції України зазначається, що ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України. 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 [5].

Без інформаційної безпеки не може бути недоторканності особистого життя. Тому забезпечення інформаційної безпеки особистості становить основу правового захисту недоторканності особистого життя. З розвитком технологій суттєво збільшуються обсяги та швидкість обміну інформацією, розширюється спектр можливих способів її збору, обробки, надання та поширення. У результаті шкоду, яку може бути заподіяно індивіду шляхом розкриття певної інформації або в зв'язку зі збереженням її в таємниці, також зростає.

З одного боку, в якості гарантій права на недоторканність особистого життя виступають заходи щодо забезпечення інформаційної безпеки, безпосередньо спрямовані на захист даного права. При цьому вироблення відповідних заходів здійснюється шляхом конкретизації правових принципів конфіденційності, цілісності та доступності з урахуванням істоти права на недоторканність особистого життя і його можливих порушень. З іншого боку, при встановленні обмежень права на недоторканність особистого життя відповідні гарантії повинні попереджати можливі зловживання такими обмеженнями, що призводять до погроз інформаційної безпеки людини. Тому Україна повинна дотримуватися міжнародних вимог захисту особистого життя, шляхом імплементації міжнародних принципів інформаційної безпеки.

Окремі загальнолюдські принципи вже передбачені національним законодавством, створюючи так звані правові принципи захисту права на недоторканність особистого життя, в яких визначаються межі і умови здійснення даного права [6]. У зв’язку з принципом конфіденційності такі спеціальні правові принципи визначають можливість збору персональних даних лише законними засобами для конкретно визначених цілей за умови попереднього повідомлення або попередньої згоди суб'єкта персональних даних, забезпечення їх захисту від таких ризиків як втрата або несанкціонований доступ, знищення, використання, зміна або розкриття даних.

У той же час з розвитком мережі Інтернет та інтернет-сервісів, створенням потужних колекцій інформації (відомих як «Великі

дані») [7, с. 601-609] і розвитком хмарних технологій дані механізми виявляються недостатніми для дотримання права людина на недоторканність особистого життя. Фактично користувач поступово втрачає контроль над використанням своїх персональних даних. Так, при використанні хмарних технологій процес передачі та обробки відомостей стає для користувача невизначеним і на практиці може полягати в дробленні інформації та її розміщенні на серверах, розташованих в різних національних юрисдикціях. Крім того, більшість користувачів дає згоду на обробку їх персональних даних, належним чином не ознайомившись з його умовами, не розуміючи правових наслідків такої згоди і не передбачаючи подальшого використання своєї особистої інформації. В результаті механізм отримання згоди користувача на обробку його особистої інформації стає слабкою, по суті, формальною гарантією, що не забезпечує конфіденційності особистої інформації і реального захисту права на недоторканність особистого життя.

Враховуючи думки науковців та досвід міжнародних правових організацій, зокрема Європейського суду з прав людини, хочемо підкреслити, що нагляд за заходами спостереження може здійснюватися на трьох етапах: коли спостереження санкціоновано, під час його проведення і після того, як воно закінчилося. У процесі нагляду цінності демократичного суспільства повинні дотримуватися якомога сумлінніше.

Таким чином, в умовах розвитку технологій забезпечення інформаційної безпеки виступає однією з найважливіших гарантією прав людини, а імплементація міжнародних принципів інформаційної безпеки в законодавство Україні підвищить міжнародний рейтинг нашої держави.

Список використаних джерел:

1. Про рішення ради національної безпеки і оборони України від 14 вересня 2020 року «Про стратегію національної безпеки України» Указ президента України від 14.09.2020 № 392/2020. URL: https://www.president.gov.ua/documents/3922020-35037.

2. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України». Указ президента України від 29 грудня 2016 року №47/2017. URL: https://www.president.gov.ua/documents/472017-21374

3. Information Security and Privacy: a Practical Guide for Global Executives, Lawyers, and Technologists. Shaw T. (ed.). Chicago: American Bar Association, 2011.

4. Grama J. Legal Issues in Information Security. Sudbury: Jones and Bartlett Publishers, 2010.

5. Конституція України. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text.

6. Information Security and Privacy: A Practical Guide for Global Executives, Lawyers and Technologists.

7. Про захист персональних даних. Закон України. Відомості Верховної Ради України (ВВР), 2010, № 34, ст. 481. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text.

8. Church P. Is «Big Data» Creepy? // Computer Law and Security Review. 2013.№ 29. P. 601–609.