DOI https://doi.org/10.24144/2307-3322.2021.66.22
УДК 342.56(477)(043.5)

ПРИНЦИПИ ПРАВОВОГО РЕГУЛЮВАННЯ ІНСТИТУТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Баран М.В.,
здобувач освітнього ступеня доктора філософії
у галузі права кафедри адміністративно-правових дисциплін
Львівського державного університету внутрішніх справ
e-mail: baranmaria17@ukr.net
ORCID ID: 0000-0002-2434-855X

Баран М.В. Принципи правового регулювання інституту інформаційної безпеки

У статті у контексті методологій системного аналізу правових явищ розкривається зміст принципів правового регулювання інституту інформаційної безпеки. Зазначено, що інформаційна безпека визначається як неможливість нанесення шкоди об'єкту безпеки. Важливе місце у правовому забезпеченні інформаційної безпеки відіграють принципи. Базові принципи правового регулювання інформаційної сфери закріплені у Законах України «Про інформацію», «Про основні засади забезпечення кібербезпеки України» більшість яких має ключовий характер для розвитку правового регулювання процесів інформаційної безпеки. З метою вдосконалення системи інформаційної безпеки від різних викликів і загроз пропонується закріпити в інформаційному законодавстві принцип презумпції безпеки об'єктів критичної інформаційної інфраструктури, який встановлює, що об'єкти критичної інформаційної інфраструктури вважаються захищеними, поки організаційно-правове забезпечення безпеки зазначених об'єктів відповідає вимогам, закріпленим в нормативно-правових актах у сфері забезпечення інформаційної безпеки. Вказано, що широкий спектр проблем забезпечення інформаційної безпеки особи, суспільства та держави, розвитку культури кібербезпеки, забезпечення недоторканності приватного життя та захисту прав на доступ до інформації, захисту інформаційних систем, ресурсів і мереж, розширення застосування інформаційних технологій в публічному управлінні, інші проблеми інформаційної безпеки потребують ретельного вивчення. Принципи правового регулювання у сфері забезпечення інформаційної безпеки розкриваються через нормативну деталізацію. Наголошено, що за умов розвитку науково-технічного прогресу та новітніх форм обробки та використання інформації принципи регулювання у сфері забезпечення інформаційної безпеки потребують кореляції на рівні нормативного забезпечення.

Ключові слова: інформація, інформаційна безпека, принципи, правове регулювання, персональні дані, великі дані.

Baran M.V. Principles of legal regulation of the institute of information security.

The article in the context of methodologies of systematic analysis of legal phenomena reveals the content of the principles of legal regulation of the institute of information security. It is noted that information security is defined as the impossibility of causing harm by means of a security object, due to information and information structure. Principles play an important role in the legal provision of information security. The basic principles of legal regulation of the information sphere are enshrined in the Laws "On Information", "On the Basic Principles of Cyber Security of Ukraine", most of which are key to the development of legal regulation of information security processes. In order to improve the information security system from various challenges and threats, it is proposed to enshrine in information legislation the principle of presumption of security of critical information infrastructure, which establishes that critical information infrastructure is considered protected as long as the organizational and legal security of these facilities requirements set forth in regulations in the field of information security. It is stated that a wide range of problems of information security of the individual, society and state, development of cybersecurity culture, ensuring privacy and protection of access rights, protection of information systems, resources and networks, expanding the use of information technology in public administration, other information problems security needs careful study. The principles of legal regulation in the field of information security are revealed through

normative detail. It is emphasized that with the development of scientific and technological progress and the latest forms of processing and use of information, the principles of regulation in the field of information security need to be correlated at the level of regulatory support.

Key words: information, information security, principles, legal regulation, personal data, big data.

Постановка проблеми. Розвиток інформаційного суспільства, цифрової трансформації і технологій перед вченими-правознавцями ставить завдання, які стосуються пошуку можливостей правового регулювання таких явищ, як робототехніка, штучний інтелект, Інтернету речей, розвиток інформаційноосвітніх платформ. Існуюче нормативно-правове регулювання не стоїть на місці, у ньому знаходить відображення розвиток теоретичних уявлень про систему правового забезпечення інформаційної безпеки в Україні. Сьогодні виникають нові суспільні відносини, пов'язані із забезпеченням критичної інформаційної інфраструктури, вносяться зміни до інформаційного, в інше галузеве законодавство. Аналогічна ситуація склалася у сфері захисту персональних даних громадян, на яку вплив робить прийняття міжнародних правових актів.

Стан опрацювання проблематики. Вклад у дослідження системи принципів правового регулювання інституту інформаційної безпеки внесли вчені: І. Арістова, О. Баранов, В. Брижко, О. Довгань, О. Золотар, І. Корж,

Р. Калюжний, Б. Кормич, В. Ліпкан, А. Марущак, В. Пилипчук, В. Рубан, Г. Сащук, Я. Собків, О. Тихомиров, С. Феденько, Л. Харченко, В. Шамрай, та інші. Однак недостатньо дослідженими залишаються питання принципів забезпечення інформаційної безпеки, зумовлені розвитком інформаційних технологій.

Метою статті є дослідження розвитку системи принципів правового регулювання інституту інформаційної безпеки.

Виклад основного матеріалу. В умовах трансформації права під впливом розвитку цифрових технологій дуже важливим є розгляд принципів правового регулювання інституту інформаційної безпеки. Слід зазначити

фундаментальний характер дослідження принципів правового регулювання, що детерміновано впливом на розвиток системи права та державної правової політики. У правовій науці ці питання є ключовими для всіх галузей права та законодавства, включаючи інформаційне. Питання про принципи правового регулювання інформаційної безпеки має особливе значення з огляду на правову природу і роль в умовах розвитку інформаційного суспільства та цифровізації.

Принципи є основними та вихідними ідеями, засадами для різних теорій, на яких засновані знання у всіх наукових галузях. Наукові дослідження принципів у праві мають фундаментальне значення, особливо для таких молодих галузей, як інформаційне. В. Перепелюк зазначає, що правові принципи відносять до юридичних закономірностей, що відображає основні ідеї та засади права, правового регулювання і закріплених у системі діючих норм права. Це повною мірою відноситься не тільки до права у цілому, але й у значній мірі до інформаційного права [1, с. 154].

Принцип, від латинського principium «початок» або «основа», це поняття, яке має фундаментальне значення для всіх сфер життєдіяльності. Слід зазначити, що у даний час у праві принципи визначаються у різних галузях права досить широко та варіативно. Однак переважає розуміння як вихідних, основних ідей, засад права, що узагальнено виражають його сутність виходячи з ідей свободи та справедливості. Вони закріплюють у праві об'єктивні закономірності суспільних відносин, основоположні цінності та традиції суспільства. Принципи публічного управління – це основні, вихідні положення, на яких ґрунтується і функціонує управлінська діяльність і які можуть бути сформульовані у вигляді певних правил, закріплених правом [2, с. 21].

Правові засади пов'язані з такими категоріями, як «закономірність» і «сутність», є підставами загального зв'язку, що відображають об'єктивні закономірності та сутність єдиної та багаторівневої системи права. Принципи забезпечують передбачуваність і однаковість процесів у праві.

Більшість принципів володіє необхідними властивостями об'єктивних законів і має загальний і стійкий характер, що надає їм ключове значення для дослідження процесів формування правового інституту інформаційної безпеки в інформаційному праві. Базові принципи правового регулювання інформаційної сфери закріплені у Законах України «Про інформацію», «Про основні засади забезпечення кібербезпеки України» більшість яких має ключовий характер для розвитку правового регулювання процесів інформаційної безпеки [3; 4].

Доцільно звернути увагу на принципи захисту інформації в інформаційнотелекомунікаційних системах передбачених Законом України «Про захист інформації в інформаційно-телекомунікаційних системах», які створюють правові основи інформаційної безпеки [5].

У зв'язку з прийняттям постанови Кабінету Міністрів України щодо Порядку внесення об'єктів критичної інформаційної інфраструктури до державного реєстру об'єктів критичної інформаційної інфраструктури, його формування та забезпечення функціонування, важливо відзначити, що до принципів функціонування та ведення реєстру, поряд з принципами законності, дотримання прав і свобод людини та громадянина, повноти, актуальності та достовірності відомостей, законодавчо закріплені принципи безперервності ведення реєстру, застосування організаційних і технічних заходів забезпечення безпеки зазначених відомостей, застосування уніфікованого формату запису при формуванні, веденні та надання з реєстру відомостей [6].

При аналізі принципів правового регулювання доцільно зробити висновок про те, що за інформаційною безпекою доцільно закріпити такі правові принципи, як достовірність, усвідомлена добровільність і конфіденційність інформаційної безпеки.

У зв'язку з тим, що забезпечення інформаційної безпеки є інформаційний процес, особливого значення набуває виділення в якості самостійного принципу забезпечення сталого та безперебійного функціонування інформаційної інфраструктури, який повинен носити імперативний характер з метою забезпечення інформаційної безпеки особи, суспільства та держави.

Розробка правового змісту зазначених принципів необхідна з метою забезпечення достовірності результатів забезпечення інформаційної безпеки суб'єктів і об'єктів. Це завдання має ключове значення для розробки правової моделі регулювання та формування інституту інформаційної безпеки.

Принцип усвідомленої добровільності інформаційної безпеки повинен бути заснований на ідеї вибору суб'єкта можливості участі у процесах ототожнення, крім випадків, встановлених у законі, у тому числі у зв'язку з забезпеченням національних інтересів у сфері державної безпеки і оборони. Цей принцип пов'язаний з необхідністю повідомлення фізичних і юридичних осіб про наявність та зміст процесів забезпечення інформаційної безпеки.

Принцип конфіденційності забезпечення інформаційної безпеки є найскладнішим серед запропонованих за змістом. Конфіденційність інформаційної безпеки можна розглядати через такий вид інформації обмеженого доступу, як таємниця впровадження заходів інформаційної безпеки.

Права і інтереси суб'єкта інформаційних правових відносин не повинні бути порушені шляхом розголошення використовуваної для забезпечення інформаційної безпеки інформації.

З метою забезпечення прав і законних інтересів особи, суспільства та держави, попередження виникнення інформаційних ризиків в інформаційних процесах важливою є охорона конфіденційності відомостей про використовувані алгоритми та технологічні рішення, так як при розкритті виникають загрози недостовірності результатів і компрометації інституту інформаційної безпеки. У зв'язку з цим особа, яка організує інформаційний обіг або надає послуги у цій сфері, має керуватися законодавчо закріпленим правом зберігати конфіденційність технології інформаційної безпеки.

Елементом пропонованої таємниці заходів забезпечення інформаційної безпеки, що визначає, по суті, зміст відповідного принципу, повинно бути право збереження в таємниці самого факту організації інформаційної безпеки, якщо інше не випливає з обставин і вимог організації процесу інформаційної безпеки, договору або закону. У цьому зацікавлені всі суб'єкти правовідносин.

У даному контексті проаналізовано масив охоронюваних законом таємниць (банківська, податкова, таємниця зв'язку, лікарська, комерційна та інші види таємниць) в зв'язку з розвитком системи надання послуг у цифрову епоху.

З одного боку, інститут інформації обмеженого доступу об'єктивно перешкоджає вільному використанню відомостей, включаючи персональні дані, з іншого – інформація, що збирається банками, операторами зв'язку, Інтернетбізнесом, страховими та транспортними компаніями, медичними закладами може бути використана для поліпшення якості послуг і для розвитку цифрової економіки.

На основі порівняльно-правового методу вивчення законодавства державчленів Європейського Союзу було виявлено ряд важливих закономірностей, серед яких виділяються: відсутність вичерпного збалансованого переліку видів даних, що становлять таємниці, властива законодавством більшості держав тенденція, коли одні дані можуть становити різні види інформації обмеженого доступу. Наприклад, персональні дані можуть одночасно включатися до складу різних видів таємниць від лікарської до таємниці зв'язку.

Правове регулювання інформаційної безпеки як інформаційного процесу повинно відбуватися в нерозривному зв'язку з урахуванням поширення технології великих даних. Багато держав Європейського Союзу направили зусилля на розробку правових рішень забезпечення обороту великих даних. Ключовою ідеєю введення в обіг є використання процедур знеособлення інформації таким чином, щоб подальша ідентифікація суб'єктів була неможлива.

Стосовно до інформаційної безпеки, на наш погляд, можна виділити принципи обґрунтованості, своєчасності та прогнозу.

Принцип обґрунтованості захисту підлягає насамперед інформація обмеженого доступу, тобто інформація, незаконне отримання та поширення якої може завдати шкоди громадянину, суспільству, державі. Необґрунтований захист інформації, перш за все обмеження доступу, робить замах на конституційні права громадян на інформацію, в окремих випадках перешкоджає розвитку економіки, науково-технічного прогресу, відносин у життєво важливих сферах діяльності суспільства та держави.

Принцип обґрунтованості полягає у встановленні шляхом експертної оцінки доцільності обмеження доступу до конкретної інформації, виділення ймовірних економічних і інших наслідків цього акту виходячи з балансу життєво важливих інтересів особи, суспільства, держави, розробки адекватних заходів протидії зовнішнім і внутрішнім загрозам інформаційної безпеки.

Принцип своєчасності захисту інформаційної сфери дозволяє реалізувати процедуру попереднього обмеження доступу до інформації, що захищається, здійснювати захист і полягає у встановленні обмежень на поширення інформації з моменту отримання, розробки або завчасно. Значення цього принципу полягає у тому, що обмеження доступу до інформації, що захищається, інформаційних систем, якщо не виключає повністю, то робить малоймовірною можливість здійснення злочинних посягань у даній сфері.

На практиці своєчасність досягається шляхом розробки та чіткого виконання положень концепції та системи захисту об'єкта, на якому сконцентровані технічні засоби, засоби комунікації, інформація, що підлягає захисту. Система захисту включає сукупність правових, науково-технічних, спеціальних та організаційних заходів. Особливе значення даного принципу проявляється у тих випадках, коли тема, проєкт, дослідження знаходяться на стадії розробки, вивчення, аналізу, але розробники не приділяють належної уваги обмеження доступу до результатів роботи, використовують незахищені канали комунікації та персональні комп'ютери, залучають до роботи неперевірених фахівців тощо.

Нові розробки, напрями досліджень, технології представляють підвищений інтерес і є пріоритетним напрямом у діяльності розвідувальних органів іноземних держав, промислового шпигунства, конкурентів, злочинців.

Принцип прогнозу інформаційної безпеки полягає у виділенні зовнішніх і внутрішніх загроз у інформаційній сфері. Базується на об'єктивній, реальній оцінці об'єктів, що охороняються – інформації, інфраструктури, суб'єктів, пов'язаних зі створенням, перетворенням, споживання інформації; моделюванні можливої протиправної діяльності, що зазіхає на інформаційну безпеку.

Прогноз здійснюється на основі наявних матеріалів про роботу українських і правоохоронних органів Європейського Союзу та НАТО з виявлення, попередження, припинення протиправної діяльності в інформаційній сфері, вивчення і аналізу практики захисту інформації, інформаційної інфраструктури, шляхом активного застосування досягнень науки та техніки, особливо у галузі вдосконалення можливостей інформаційних систем.

Значення даного принципу полягає у тому, що створюється ймовірність здійснювати заходи забезпечення інформаційної безпеки у режимі упередження та знизити збитки від злочинних устремлінь супротивників, конкурентів, злочинців тобто, превентивне регулювання здійснюється з метою запобігання негативним соціально-правовим явищам, формування правомірної поведінки. За відсутності правопорушень не було необхідності в створенні та здійсненні правових заходів попередження [7, с. 42-43].

Дослідження які проводять українські вчені показують необхідність розвитку системи принципів інформаційної безпеки. Одним з важливих є принцип балансу інтересів людини, суспільства і держави. Інший принцип це принцип законності та правової забезпеченості. Зростання значущості інформаційної безпеки випереджає розвиток відповідній сфері права. Третій принцип – інтеграція з міжнародними системами безпеки інформації.

Для впровадження систем інформаційної безпеки необхідно дотримуватися трьох головних принципів: конфіденційність, цілісність. доступність.

З метою формування правової культури та захисту прав і свобод особи в умовах цифрового розвитку є необхідність законодавчого закріплення правового принципу усвідомленої добровільної участі, що полягає в розумінні суб'єктом інформаційних відносин можливих позитивних і негативних наслідків у залежності від обсягу наданих відомостей для інформаційної безпеки. Реалізація принципу сприяє пробудженню суспільної свідомості, формуванню громадської думки, підвищенню ролі інститутів громадянського суспільства [8, с. 47].

У сфері інформаційної безпеки фізичних осіб у наявності своєрідний дуалізм ситуації стосовно до обробки персональних даних. Якщо особа, яка обробляє інформацію має можливість ідентифікувати людину,

то воно є оператором персональних даних, несучи встановлені законом обов'язки щодо режиму персональних даних. Якщо така обробка відсутня, до зазначеної категорії суб'єктів особа не відноситься. Грань між двома ситуаціями в умовах використання технологій великих даних складно визначити.

Для збільшення обсягу захисту суб'єктів інформаційних відносин є необхідність включення у систему інформації обмеженого доступу такого нового виду таємниці, як «таємниця ідентифікації», що представляє сукупність інформації обмеженого доступу, отриманої та (або) створеної особою у межах діяльності, конфіденційність якої забезпечується спеціальними правовими режимами з метою охорони прав, свобод і законних інтересів особи, яку ідентифікують, створення умов ефективної діяльності в інформаційній сфері.

До складу таємниці ідентифікації необхідно включити наступні види інформації: про використовувані технології ідентифікації та інфраструктурі інформаційної безпеки; дані, що обробляються у процесі ідентифікації, в тому числі, конфіденційні ідентифікатори; інформація про результати ідентифікації. Дискусійним є питання, чи потрібно відносити до складу таємниці ідентифікації відомості про сам факт встановлення особи.

З огляду на необхідність забезпечення усвідомленої участі та згоди фізичної особи на ідентифікацію, у результаті якої будуть зібрані, оброблені та використовуватися персональні дані, у разі важливості подальших інформаційних процесів у сферах, які можуть стосуватися приватного життя (наприклад, здоров'я та медицина), можна ставити питання про диференційоване віднесення факту ідентифікації до зазначеної таємниці.

Ще одним дискусійним питанням може стати питання про віднесення до складу принципів принципу пропорційності. Принцип може бути пов'язаний з необхідністю забезпечення прозорості мети та завдань реалізації суспільних відносин, пов'язаних з ідентифікацією, на його основі повинні встановлюватися вимоги до ототожнення тільки в тих випадках, в яких потрібні використовувати результати встановлення особи. Наприклад, коли ідентифікація необхідна тільки для того, щоб встановити взаємодію програма-бот чи людина, не повинна відбуватися ідентифікація конкретного користувача. Принцип пропорційності повинен визначати якість і надійність використовуваних організаційнотехнічних і правових механізмів, що визначають умови процесів ототожнення у контексті забезпечення інформаційної безпеки.

З огляду на актуальність питань правового забезпечення безпеки критичної інформаційної інфраструктури України, необхідність розвитку теоретичних положень і системи принципів правового регулювання у даній сфері доцільно закріпити принцип презумпції безпеки об'єктів критичної інформаційної інфраструктури, що позначає захищеність критичної інформаційної інфраструктури, її стійке функціонування при відповідності критичної інформаційної інфраструктури вимогам інформаційної безпеки до таких об'єктів, дотриманні нормативно-правових актів у сфері інформаційної безпеки.

В умовах прискореного розвитку науково-технічного прогресу та новітніх форм обробки інформації, об'єкт і предмет регулювання у сфері забезпечення інформаційної безпеки потребує постійної кореляції на рівні нормативного забезпечення, за рахунок впровадження нових принципів [9, с. 182].

Висновки. У загальному вигляді інформаційна безпека визначається як неможливість нанесення шкоди об'єкту, що обумовлюється інформацією та інформаційною структурою. Важливе місце у правовому забезпеченні інформаційної безпеки відіграють принципи. Базові принципи правового регулювання інформаційної сфери закріплені у Законах України «Про інформацію», «Про основні засади забезпечення кібербезпеки України» більшість яких має ключовий характер для розвитку правового регулювання процесів інформаційної безпеки. З метою вдосконалення системи інформаційної безпеки від різних викликів і загроз пропонується закріпити в інформаційному законодавстві принцип презумпції безпеки об'єктів критичної інформаційної інфраструктури, який встановлює, що об'єкти критичної інформаційної інфраструктури вважаються захищеними, поки організаційно-правове забезпечення безпеки зазначених об'єктів відповідає вимогам, закріпленим в нормативно-правових актах у сфері забезпечення інформаційної безпеки.

Широкий спектр проблем забезпечення інформаційної безпеки особи, суспільства та держави, розвитку культури кібербезпеки, забезпечення недоторканності приватного життя та захисту прав на доступ до інформації, захисту інформаційних систем, ресурсів і мереж, розширення застосування інформаційних технологій в публічному управлінні, при наданні адміністративних послуг, інші проблеми інформаційної безпеки потребують ретельного вивчення. Відповідно, перспективним завданням юридичної науки є вироблення пропозицій задля удосконалення відповідних актів законодавства.

Список використаних джерел:

1. Перепелюк В. Вплив принципів права на формування єдиної правозастосовчої практики. *Публічне право.* 2019. № 4 (36). С. 153-160.

2. Адміністративне право України (загальна частина): навчальний посібник / О. І. Остапенко, М. В. Ковалів, С. С. Єсімов і інші. Львів: НУ «Львівська політехніка», 2019. 504 с.

3. Про інформацію : Закон України від 02.10.1992 р. № 2657-XII. URL. https://zakon.rada.gov.ua/laws/show/2657-12#Text

4. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10. 2017 р. № 2163-VIII. URL. https://zakon.rada.gov.ua/laws/show/216319#Text

5. Про захист інформації в інформаційно-телекомунікаційних системах :

6. Закон України від 05.07. 1994 р. № 80/94-ВР. URL. https://zakon.rada.gov.ua/laws/card/80/94-%D0%B2%D1%80

7. Деякі питання об'єктів критичної інформаційної інфраструктури : Постанова Кабінету Міністрів України від 09.10.2020 р. № 943. URL. https://zakon.rada.gov.ua/laws/show/943-2020-%D0%BF#Text

8. Єсімов С. С. Превентивне регулювання: теоретичні аспекти. *Соціальноправові студії.* 2020. Випуск 3 (9). С. 40-47.

9. Єсімов С. С., Бондаренко В. А. Транспарентність як принцип діяльності органів публічного управління в умовах використання інформаційних технологій. *Соціально-правові студії.* 2018. Випуск 1. С. 42-49.

10. Яковлєв П. О. Об'єкт і предмет державного регулювання у сфері забезпечення інформаційної безпеки України. *Право і суспільство*. 2020. № 3. С.178-183.