*Кормич Б. А., ОНЮА*

# ОСНОВНІ ПРИНЦИПИ ПРАВОВОГО РЕГУЛЮВАННЯ ДІЯЛЬНОСТІ ІЗ ЗАХИСТУ ІНФОРМАЦІЇ

*В статье анализируются ключевые принципы, установленные в рамках правового института защиты информации. Характеризуется сущность и основные направления государственного регулирования в данной сфере.*

*The article provides the analyses of the key points set within the frameworks of the legal institute of the protection of information. The essence and main directions of the state's regulation in this field are also characterized.*

Діяльність із захисту інформації є важливим аспектом забезпечення дотримання відповідних режимів інформаційних ресурсів та доступу до інформації, що набуває виключної актуальності на сьогоднішньому рівні розвитку інформаційних відносин та формування інформаційного суспільства.

Питання захисту інформації ставали предметом досліджень цілого ряду фахівців в галузі інформаційного права, серед яких І. Арістова, І. Бачило, Р. Калюжний, В. Копилов, В. Лопатін, В. Ярочкин тощо. Разом з тим, досить часто захист інформації більшою мірою розглядається з точки зору аналізу окремих прийомів за засобів його здійснення. При чому значною мірою акцент робиться на відповідних технічних нормах. Одночасно для формування в інформаційному праві інституту захисту інформації важливим є аналіз загальних принципів правового регулювання діяльності суб'єктів інформаційних відносин в даній сфері, що ми і спробуємо зробити в рамках даної статті.

Відразу слід зазначити, що захист може здійснюватися щодо інформації з будь-яким видом режиму доступу, але одночасно мета та завдання такого захисту будуть розрізнятися у відповідності до вимог відповідного режиму. Зокрема, на таку особливість вказується у Правилах забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджених Кабінетом Міністрів України [1], якими розрізняються вимоги щодо захисту відкритої інформації та інформації з обмеженим доступом.

Основною вимогою щодо захисту відкритої інформації є *збереження її цілісності*, що забезпечується шляхом захисту від

несанкціонованих дій, які можуть призвести до її випадкової або умисної модифікації чи знищення.

Відповідно дотримання режиму доступу до такої інформації передбачає, що:

– усім користувачам повинен бути забезпечений доступ до ознайомлення з відкритою інформацією;

– модифікація або знищення відкритої інформації може здійснюватися лише користувачами, яким надано відповідні повноваження.

– спроби модифікації чи знищення відкритої інформації користувачами, які не мають на це повноважень, повинні блокуватися.

Захист конфіденційної та таємної інформації, натомість передбачає здійснення комплексу організаційних та правових заходів, які забезпечують вирішення цілої низки завдань до яких входять захист відповідної інформації від: *1) несанкціонованого та неконтрольованого ознайомлення, 2) модифікації, 3) знищення, 4) копіювання, 5) поширення*.

Відповідно забезпечення дотримання режиму доступу до таємної або конфіденційної інформації передбачає, що:

– доступ до конфіденційної інформації надається тільки користувачам, які мають на це повноваження;

– спроби доступу до такої інформації осіб чи користувачів, які не мають відповідних повноважень повинні блокуватися;

– користувачеві може надаватися право на виконання однієї або кількох конкретних операцій з обробки конфіденційної інформації або позбавлення його такого права.

Як правило захист інформації здійснюється в рамках певних інформаційних систем, які з правової точки зору представляють собою «організаційно впорядковану сукупність документів (масивів документів) і інформаційних технологій, в тому числі з використанням засобів обчислювальної техніки і зв'язку, які реалізують інформаційні процеси» [2]. Цілком логічним виглядає застереження «в тому числі» по відношенню до комп'ютерних технологій. Адже автоматизовані засоби обробки інформації з'явилися за історичними мірками зовсім недавно. І навпаки, на протязі декількох тисячоліть існують традиційні способи обробки та передачі інформації. Вже з початком XX століття до них поступово додалися телеграфні, телефонні, радіо, телевізійні і, нарешті комп'ютерні мережі передачі інформації. Слід зазначити, що

відповідні цілі діяльності із захисту інформації є універсальними та не залежать від виду інформаційної системи, інформаційного ресурсу або фізичного носія інформації. Адже загальні вимоги будуть однаковими як для електронних інформаційних ресурсів так і для інформаційних ресурсів на паперових або інших фізичних носіях.

Захист інформації є комплексною категорією, що обумовлюється багатьма факторами. Будь-яка інформаційна система, особливо автоматизована «поділяється на функціональну частину та частину забезпечення, кожна з яких поділяється на складові елементи мінімально можливої розмірності» [3]. Функціональна частина інформаційної системи спрямована на виконання функцій і завдань, що підлягають реалізації за допомогою цієї системи. Частина забезпечення представляє собою «наповнення» функціональної частини, за допомогою якого фактично реалізуються функції і завдання системи. Узагальнюючи такий підхід, ми можемо говорити, що інформаційна система функціонує за тими ж самими правилами і законами, що і будь-який інший вид систематизованої діяльності з розподілом ролей і функцій. Створення будь-якої системи обробки чи передачі інформації, починаючи від поштової служби і закінчуючи комп'ютерними мережами, включає величезну кількість етапів та елементів. До цього переліку входить: створення фізичних об'єктів на яких ця система розміщується, створення технічного і програмного забезпечення, підготовка кадрів, забезпечення фінансовими та енергетичними ресурсами тощо. І загрози, які повинні бути відвернуті або попереджені системою заходів із захисту інформації можуть виникати на будь-якому етапі створення та експлуатації інформаційної системи.

Ще однією виключно важливою проблемою є визначення конкретних факторів, які необхідно враховувати, щоб охарактеризувати безпечність як конкретної інформаційної системи. Для цього необхідно виходити з функціонального призначення систем та об'єктів інформаційної системи. Головне їх завдання полягає у реалізації інформаційних процесів. А звідси головною цінністю є та інформація, яка обробляється в цих системах. Таким чином інформаційна інфраструктура повинна забезпечувати інформацію або інформаційні ресурси, які обробляються від «потенційно, або реально можливих дій, що приводять до неправомірного заволодіння відомостями що охороняються».

Видами таких неправомірних дій можуть бути:

– ознайомлення з конфіденційною інформацією різними шляхами і способами без порушення її цілісності;

– модифікація інформації в протиправних цілях як часткова або значна зміна складу і змісту відомостей;

– руйнування (знищення) інформації як акт вандалізму або з метою заподіяння прямої матеріальної шкоди.

Результатом неправомірних дій з інформацією є «порушення її конфіденційності, повноти, достовірності та доступності, що у свою чергу призводить до порушення як режиму управління, так і його якості в умовах спотвореної або неповної інформації» [4].

Таким чином ми можемо говорити про те, що головним об'єктом загрози для інформаційної системи є суспільні відносини які складаються з приводу управління і користування об'єктами. А безпосереднім предметом загрози – інформаційні ресурси та інформація, що обробляється. Таким чином в аспекті безпеки інформаційна інфраструктура представляє собою певну оболонку, яка захищає інформацію, що знаходиться всередині її, від негативного впливу зовнішніх факторів.

Ці негативні фактори впливу можна класифікувати, в залежності від його джерела на три групи [5]:

*Антропогенні фактори* (безпосередньо створені людьми), які складають:

– ненавмисні або навмисні діяння обслуговуючого і управлінського персоналу, програмістів, користувачів, служби безпеки інформаційної системи;

– дії несанкціонованих користувачів (діяльність іноземних розвідувальних і спеціальних служб, кримінальних структур, недобросовісних партнерів та конкурентів, а також протиправна діяльність інших окремих осіб).

*Техногенні фактори* (викликані випадковим впливом технічних об'єктів):

– внутрішні (неякісні технічні і програмні засоби обробки інформації; засоби зв'язку, охорони, сигналізації; інші технічні засоби, що застосовуються в установі);

– глобальні техногенні загрози (небезпечні виробництва, мережі енерго-, водопостачання, каналізації, транспорт тощо), які призводять до зникнення або коливання електропостачання і інших засобів забезпечення і функціонування, відмов та збоїв апаратно-програмних засобів;

– електромагнітні випромінювання і наводки, витік через канали зв'язку (оптичні, електричні, звукові) тощо.

*Природні фактори* (вплив негативних природних чинників) – стихійні лиха, магнітні бурі, радіоактивний вплив.

Звідси для інформаційної структури взагалі і для кожного об'єкта її, зокрема, важливим є забезпечити незмінність внутрішніх умов обробки інформації, при зміні (в тому числі і негативному) зовнішніх умов. Таким чином **безпеку інформаційних систем можна охарактеризувати як стан забезпеченості необхідних умов і параметрів інформаційних процесів, що реалізуються за їх допомогою, від негативного впливу ззовні.**

Можна виділити два способи регулювання питань захисту інформації. Перший забезпечується державною власністю на найбільш важливі (стратегічні) інформаційні системи та інформаційні ресурси, і полягає в безпосередньому державному управлінні відповідними об'єктами. Другий забезпечується юрисдикцією держави на власній території і полягає в запровадженні єдиних, обов'язкових, стандартів інформаційних процесів, які повинні дотримуватися власниками або операторами об'єктів інформаційної інфраструктури.

Взагалі, коли мова йде про захист інформації, то більшість дослідників погоджується з тим, що цей захист може мати лише комплексний характер. Але в цій комплексній системі можна виділити цілий спектр напрямків діяльності суб'єктів захисту інформації, які характеризуються властивими специфічними методами і способами захисту інформації. Зазвичай виділяють:

правовий захист – спеціальні закони, інші нормативні акти, правила, процедури і заходи, що забезпечують захист інформації на правовій основі;

організаційний захист – це регламентація виробничої діяльності і взаємовідносин виконавців на нормативно-правовій основі, що виключає або послаблює завдання якої-небудь шкоди виконавцям;

інженерно-технічний захист – використання різних технічних засобів, що попереджають завдання шкоди інформації.

Але слід зазначити, що в будь-якому випадку в основі всіх перерахованих заходів лежать правові норми, якими регламентується діяльність в сфері захисту інформації. Крім того, правовий захист інформації, який було розглянуто в попередніх розділах, стосується так би мовити інформації в «чистому» вигляді, незалежно

від її носія. А от наступні – організаційний і інженерно-технічний аспекти захисту інформації, спрямовані не безпосередньо на інформацію, а на системи, об'єкти та носії, на яких ця інформація збирається, зберігається, обробляється та розповсюджується.

На сьогоднішній день найбільш актуальним аспектом захисту інформації, безумовно є захист інформації представленої в електронному виді, адже саме такий вид інформації, з огляду на її нематеріальний характер, високу здатність до трансформації та передачі є найбільш вразливим щодо протиправних дій. Інформація в електронній формі обробляється, передається та розповсюджується за допомогою інформаційно-телекомунікаційних систем, виступаючи їх основним наповненням. В Україні останніми роками створено достатньо широку нормативно-правову базу щодо провадження діяльності по захисту даного виду інформації. При чому можна виділити два аспекти захисту інформації в інформаційно-телекомунікаційних системах. Так, по-перше, це стосується встановлення певних стандартів та вимог щодо характеристик самих інформаційних систем, які повинні забезпечувати дієвість даної системи. Інший аспект стосується безпосередньо правового регулювання діяльності із захисту інформації.

Так, наприклад, Закон України «Про телекомунікації» [6] (ст. 1) виділяє дві характеристики пов'язані з безпекою інформаційних систем та мереж.

По-перше, це ***інформаційна безпека телекомунікаційних мереж***, яка визначається як здатність телекомунікаційних мереж забезпечувати захист від знищення, перекручення, блокування інформації, її несанкціонованого витоку або від порушення встановленого порядку її маршрутизації.

По-друге, це ***сталість телекомунікаційної мережі***, яка представляє собою властивості телекомунікаційної мережі зберігати повністю або частково свої функції за умови впливу на неї дестабілізуючих чинників.

Стаття 9 Закону України «Про телекомунікації» встановлює обов'язки операторів та провайдерів телекомунікацій щодо забезпечення відповідних характеристик та властивостей засобів телекомунікацій.

Правовою основою провадження діяльності із захисту інформації є Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» [7].

Відповідно до норм ст. 1 цього Закону ***захист інформації в системі це – діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі***.

Сама ж автоматизована система представляє собою систему, що здійснює автоматизовану обробку даних і до складу якої входять технічні засоби їх обробки (засоби обчислювальної техніки і зв'язку), а також методи і процедури, програмне забезпечення.

Закон виділяє п'ять основних видів несанкціонованих дій з інформацією, до яких відносяться:

1) блокування інформації в системі – дії, внаслідок яких унеможливлюється доступ до інформації в системі;

2) виток інформації – результат дій, внаслідок яких інформація в системі стає відомою чи доступною фізичним та/або юридичним особам, що не мають права доступу до неї;

3) знищення інформації в системі – дії, внаслідок яких інформація в системі зникає;

4) порушення цілісності інформації в системі – несанкціоновані дії щодо інформації в системі, внаслідок яких змінюється її вміст;

Іншим аспектом інформаційної безпеки є захист інформації яка передається, зберігається та обробляється за допомогою комунікаційних систем різних типів. В цьому напрямку в Україні вже створено цілу низку нормативно-правових актів.

Об'єктами захисту від неправомірних зазіхань є:

– інформація, що обробляється в автоматизованій системі;

– права власників цієї інформації та власників автоматизованої системи;

– права користувача.

Захист інформації здійснюється шляхом застосування сукупності організаційно-технічних заходів і правових норм для запобігання заподіянню шкоди інтересам власника інформації чи автоматизованої системи та осіб, які користуються інформацією.

Також Законом України «Про захист інформації в автоматизованих системах» визначаються: відносини між суб'єктами в процесі обробки інформації в автоматизованих системах, загальні вимоги щодо захисту інформації в АС і порядок організації цього захисту, відповідальність за порушення норм цього закону та засади міжнародного співробітництва України в сфері автоматизованих систем.

Слід зазначити, що конкретний зміст вимог щодо захисту інформації, насамперед залежить від права власності на конкретну інформації, що обробляється за допомогою автоматизованої системи.

Так, згідно норм ст. 11 Закону України «Про захист інформації в автоматизованих системах» вимоги і правила щодо захисту інформації, яка є власністю держави, або інформації, захист якої гарантується державою, визначаються відповідними нормативно-правовими актами. Ці вимоги є обов'язковими для власників автоматизованих систем, де така інформація обробляється, а от для інших суб'єктів права власності на інформацію такі вимоги мають лише рекомендаційний характер.

Політика в галузі захисту інформації в автоматизованих системах визначається Верховною Радою України, а державне управління в цій сфері здійснюється Кабінетом Міністрів.

Державне управління в сфері захисту інформації в автоматизованих системах здійснюється шляхом:

– проведення єдиної технічної політики щодо захисту інформації;

– розроблення концепції, вимог, нормативно-технічних документів і науково-методичних рекомендацій щодо захисту інформації в автоматизованих системах;

– затвердження порядку організації, функціонування та контролю за виконанням заходів, спрямованих на захист оброблюваної в автоматизованій системі інформації, яка є власністю держави, а також рекомендацій щодо захисту інформації – власності юридичних та фізичних осіб;

– організації випробувань і сертифікації засобів захисту інформації в автоматизованих системах, в якій здійснюється обробка інформації, яка є власністю держави;

– створення відповідних структур для захисту інформації в автоматизованих системах;

– проведення атестації сертифікаційних (випробувальних) органів, центрів і лабораторій, видачі ліцензії на право проведення сервісних робіт в галузі захисту інформації в автоматизованих системах;

– здійснення контролю захищеності оброблюваної в автоматизованих системах інформації, яка є власністю держави;

– визначення порядку доступу осіб і організацій зарубіжних держав до інформації в автоматизованих системах, яка є власністю держави, або до інформації – власності фізичних

та юридичних осіб, щодо поширення і використання якої державою встановлено обмеження.

Нормами законодавства встановлюється комплексний характер захисту інформації. Так, зокрема відзначається, що захист державних інформаційних ресурсів в автоматизованих системах, що входять до складу інформаційно-телекомунікаційних систем, здійснюється шляхом запровадження комплексної системи захисту інформації (КСЗІ). КСЗІ складається з комплексу технічних, криптографічних, організаційних та інших заходів і засобів, спрямованих на недопущення блокування інформації, несанкціонованого ознайомлення з нею та/або її модифікації. [8]

Основними елементами комплексної системи захисту інформації можна вважати заходи технічного та криптографічного захисту інформації, а також комплекс заходів організаційного характеру який включає встановлення відповідних режимів діяльності об'єктів інформаційних систем, контроль за дотриманням правил і норм здійснення захисту інформації, контроль за діяльністю суб'єктів захисту інформації тощо.

Таким чином можна стверджувати про наявність визначених законодавством загальних правил та принципів, що визначають діяльність із захисту інформації, незалежно від виду суб'єктів цієї діяльності. Відповідна сукупність правових норм, свідчить про наявність в інформаційному праві окремого інституту захисту інформації, що має універсальний характер.

***Література:***


1. Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах: Постанова Кабінету Міністрів України від 29 березня 2006 р. № 373.
2. Копылов В. А. Информационное право. – 2-е изд., перераб. и доп. – М.: Юристъ, 2002. – С. 63.
3. Копылов В. А. Информационное право. – М.: Юристъ, 1997. – С. 152.
4. Ярочкин В. И. Информационная безопасность. – М.: Международные отношения, 2000. – С. 17-18.
5. Бачило И. Л., Лопатин В. Н., Федотов М. А. Информационное право / Под. ред. акад. РАН Б. Н. Топорнина. – СПб.: Юридический центр Пресс», 2001. – С. 643.
6. Про телекомунікації: Закон України від 18 листопада 2003 р. № 1280-IV // Відомості Верховної Ради України. – 2004. – № 12. – Ст. 155.

7. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 31 травня 2005 р. № 2594-IV // Відомості Верховної Ради України. – 2005. – № 26. – Ст. 347.
8. Про затвердження Порядку захисту державних інформаційних ресурсів у інформаційно-телекомунікаційних системах: Наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації СБ України від 24 грудня 2001 р. № 76.

***Єзеров А. А., ОНЮА***

# УЗГОДЖЕННЯ НОРМАТИВНО-ПРАВОВИХ АКТІВ ТА ДІЙ СУБ'ЄКТІВ КОНСТИТУЦІЙНИХ ПРАВОВІДНОСИН ЯК ЗАСІБ ЗДІЙСНЕННЯ ВПЛИВУ НА КОНСТИТУЦІЙНИЙ КОНФЛІКТНИЙ ПРОЦЕС

*В статье рассмотрены проблемы влияния субъектов конституционно-правовых отношений на конституционные конфликты с целью их предупреждения или прекращения путем гармонизации соответствующих правовых актов и действий. Определены юридические средства влияния на конституционные конфликты и перспективные цели такого воздействия.*

*The problems of subjects of constitutionally-legal relations influence on constitutional conflicts with the purpose of their prevention or stopping by harmonization of the proper legal acts and actions are considered in the article. Legal facilities of influence on constitutional conflicts and perspective aims of such influence are defined.*

Здійснення впливу на конституційні конфлікти вимагає врахування їх суперечливої природи: з одного боку, конструктивна риса робить їх стимулом суспільного розвитку, а з іншого – руйнівний аспект конфліктів дезінтегрує систему конституційних правовідносин. Засоби впливу на конституційний конфліктний процес передбачають: переведення його у річище раціональної діяльності та взаємодії суб'єктів конституційно-правових відносин; продуманий вплив на конфліктну поведінку суб'єктів з метою досягнення бажаних результатів; обмеження протистояння рамками конституційного законодавства. Кінцевою метою застосування засобів впливу на конституційний конфліктний процес є попередження або припинення конституційних конфліктів. Для зручності