АДМІНІСТРАТИВНЕ ТА ФІНАНСОВЕ ПРАВО

УДК 351.746
DOI https://doi.org/10.32782/2408-9257-2024-3-11

Бабіч Р. В.,
аспірант відділу аспірантури та докторантури
Національної академії Служби безпеки України

СПІВВІДНОШЕННЯ АДМІНІСТРАТИВНОЇ ТА ІНШИХ ВИДІВ ВІДПОВІДАЛЬНОСТІ ЗА ПОРУШЕННЯ ЗАКОНОДАВСТВА ПРО ЗАХИСТ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНИХ (АВТОМАТИЗОВАНИХ) СИСТЕМАХ

THE RELATIONSHIP BETWEEN ADMINISTRATIVE AND OTHER TYPES OF LIABILITY FOR VIOLATIONS OF INFORMATION PROTECTION LEGISLATION IN INFORMATION (AUTOMATED) SYSTEMS

У сучасному суспільстві інформація є одним з найважливіших ресурсів, що робить її захист надзвичайно актуальним завданням. Стаття аналізує правове регулювання захисту інформації в інформаційних системах в Україні, особливу увагу приділяючи нормативним актам та відповідальності за порушення законодавства. Основним документом, що регулює цю сферу, є Закон України «Про захист інформації в інформаційно-комунікаційних системах», який встановлює принципи захисту інформації, порядок її обробки та зберігання, а також передбачає відповідальність за порушення цих правил.

У статті детально розглядаються різні види юридичної відповідальності за порушення законодавства про захист інформації: адміністративна, кримінальна, дисциплінарна, матеріальна та цивільна. Адміністративна відповідальність охоплює штрафи, заборону діяльності, вилучення обладнання, обов'язкові заходи для відновлення безпеки, анулювання ліцензій або сертифікатів та інші санкції. Кримінальна відповідальність передбачає більш суворі заходи, такі як позбавлення волі, обмеження волі, великі штрафи та конфіскація майна за серйозні порушення, що мають високий рівень суспільної небезпеки. Цивільна відповідальність спрямована на відшкодування збитків, завданих порушенням прав на інформацію, та включає компенсацію матеріальної та моральної шкоди.

Стаття також акцентує на співвідношенні між адміністративною та іншими видами відповідальності, підкреслюючи важливість комплексного підходу до захисту інформації. Такий підхід передбачає координацію між різними видами відповідальності для забезпечення повноцінного захисту інформації. Адміністративна відповідальність слугує першою лінією оборони, тоді як кримінальна та цивільна відповідальність застосовуються для вирішення складніших випадків.

Автор зазначає, що для ефективного захисту інформації необхідно вдосконалювати законодавство, уточнювати межі відповідальності, посилювати санкції та розвивати практичні аспекти його застосування. Важливим є підвищення кваліфікації працівників правоохоронних органів та суддів, а також активна співпраця України з міжнародними організаціями для запозичення найкращих практик у сфері кібербезпеки.

Таким чином, стаття робить висновок про необхідність комплексного підходу до захисту інформації, що включає різні види відповідальності, з метою забезпечення ефективного правового регулювання та реагування на сучасні виклики в інформаційній сфері.

Ключові слова: *адміністративна відповідальність, інформаційні системи, захист інформації, правове регулювання, автоматизовані системи.*

The article addresses the critical importance of information protection in modern society, highlighting the growing relevance of safeguarding information due to its role as a key resource. With the increasing complexity of societal life, integration processes in Europe and globally, and the influence of European and international human rights standards on national legal systems, the threats to human existence and societal functioning – stemming from economic, environmental, and political crises, terrorism, crime, and more – have intensified. This has led to a significant increase in the mutual responsibility of the state, individuals, and other entities regarding information security.

In Ukraine, the legal regulation of information protection in information (automated) systems is ensured by several legislative acts, notably the Law of Ukraine "On Information Protection in Information and Communication Systems." Violations of this legislation entail various forms of responsibility, including administrative, criminal, and civil.

The article thoroughly examines the legal framework governing information protection in Ukraine, starting with an analysis of the primary legislation and regulations, such as the Law "On Information Protection in Information and Communication Systems" and the "Rules for Ensuring Information Protection in Information, Electronic Communication, and Information and Communication Systems." It outlines the types of information subject to protection, including state information resources, confidential information, official information, and information classified as a state or other legally protected secret.

The discussion extends to the different types of liability for violating information protection laws: administrative, criminal, disciplinary, material, and civil. Administrative responsibility, regulated by the Code of Ukraine on Administrative Offenses, includes penalties such as fines, activity bans, equipment confiscation, and mandatory security measures. Criminal liability, governed by the Criminal Code of Ukraine, addresses more severe offenses, such as illegal access to information systems and the distribution of harmful software, with penalties ranging from fines to imprisonment.

The article also explores the relationship between administrative and other forms of liability, emphasizing the need for coordination to ensure comprehensive information protection. Administrative liability serves as the first line of defense, while criminal and civil liabilities address more serious or complex cases. The analysis underscores the necessity of a complex approach that combines these different forms of liability to effectively protect information in today's rapidly evolving technological landscape.

In conclusion, the article stresses the importance of a well-coordinated and comprehensive legal approach to information security, considering the growing risks and the need for effective legal tools to prevent and address violations. The development of legislation, practical application, and international cooperation are highlighted as critical factors in enhancing the effectiveness of information protection in Ukraine.

Key words: *administrative liability, information systems, information protection, legal regulation, automated systems.*

Вступ. Інформація в сучасному суспільстві є одним з найважливіших ресурсів, тому питання її захисту набуває особливої актуальності.

В умовах значного ускладнення сучасного суспільного життя, інтенсивного розвитку інтеграційних процесів у Європі та світі, підвищення впливу європейських і міжнародних стандартів прав людини на національні правові системи, посилення загроз нормальному існуванню і розвитку людини та функціонуванню суспільства, які викликані економічними, екологічними, політичними кризами, тероризмом, злочинністю тощо, взаємна відповідальність держави, особи та інших суб'єктів істотно зростає [9, с. 5].

В Україні нормативно-правове регулювання захисту інформації в інформаційних (автоматизованих) системах забезпечується низкою законодавчих актів, зокрема Законом України «Про захист інформації в інформаційно-комунікаційних системах» [1]. Порушення цього законодавства тягне за собою різні види відповідальності, зокрема адміністративну, кримінальну та цивільну.

1. Нормативно-правове регулювання захисту інформації в інформаційних системах

Основним нормативним актом, що регулює захист інформації в інформаційних (автоматизованих) системах, є Закон України «Про захист інформації в інформаційно-комунікаційних системах» [1]. Він встановлює загальні принципи та вимоги щодо захисту інформації, визначає порядок обробки та зберігання інформації, а також передбачає відповідальність за порушення цього законодавства.

Так, відповідно до абз. 7 ч. 1 ст. 1 закону України «Про захист інформації в інформаційно-комунікаційних системах», захист інформації в системі – діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі [1].

Відповідно до п. 4 Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, затверджених постановою КМУ від 29 березня 2006 р. № 373 [6], захисту підлягає:

– 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 електронними комунікаційними мережами;

– конфіденційна інформація, яка перебуває у володінні розпорядників інформації, визначених частиною 1 статті 13 Закону України «Про доступ до публічної інформації»;

– інформація, вимога щодо захисту якої встановлена законом;

– інформація, яка становить державну або іншу передбачену законом таємницю;

– службова інформація [11, с. 51-52].

Важливим аспектом є також Закон України «Про основні засади забезпечення кібербезпеки України» [2], який регулює питання захисту критичної інформаційної інфраструктури та встановлює вимоги до суб'єктів забезпечення кібербезпеки.

2. Адміністративна відповідальність за порушення законодавства про захист інформації

Адміністративна відповідальність за порушення законодавства про захист інформації передбачена Кодексом України про адміністративні правопорушення (КУпАП) [3]. Так, статтею 212-6 КУпАП передбачено перелік діянь, наявність яких у діях суб'єкта правопорушення міститиме склад адміністративного проступку:

– здійснення незаконного доступу до інформації, яка зберігається, обробляється чи передається в інформаційних (автоматизованих) системах;

– здійснення незаконного доступу до інформації, яка зберігається, обробляється чи передається в інформаційних (автоматизованих) системах, призначених для зберігання та обробки інформації з обмеженим доступом;

– незаконне копіювання інформації, яка зберігається в інформаційних (автоматизованих) системах, у паперовій чи електронній формі;

– безоплатне незаконне розповсюдження інформації, яка зберігається в інформаційних (автоматизованих) системах, у паперовій чи електронній формі;

– незаконний збут інформації, яка зберігається в інформаційних (автоматизованих) системах, у паперовій чи електронній формі [3].

Відповідальність за порушення законодавства про захист інформації в інформаційних (автоматизованих) системах може мати різні прояви. Проаналізувавши норми чинного законодавства можна виділити такі основні види санкцій за порушення законодавства про інформацію, яка зберігається, обробляється чи передається в інформаційних (автоматизованих) системах:

1. Штрафи. Найбільш поширений вид адміністративної відповідальності. На фізичних та юридичних осіб, які порушують закони про захист інформації в інформаційних системах, можуть накладатись штрафи.

2. Заборона діяльності. У випадках серйозних порушень може бути застосована заборона використання або експлуатації інформаційно-телекомунікаційних систем.

3. Вилучення обладнання. В разі виявлення обладнання, що використовується для порушення захисту інформації, може бути прийнято рішення про його вилучення.

4. Обов'язкові заходи для відновлення безпеки. Вирішення проблем, які виникають внаслідок порушень захисту інформації, може включати обов'язкові заходи для відновлення безпеки систем та даних.

5. Анулювання ліцензій чи сертифікатів. Порушення захисту інформації може призвести до втрати ліцензій чи сертифікатів, які дозволяють здійснювати певні види діяльності.

6. Інші адміністративні санкції. Законодавство може передбачати інші адміністративні санкції в залежності від конкретних обставин порушення [11, с. 52–53].

3. Співвідношення адміністративної та інших видів відповідальності

Співвідношення адміністративної та інших видів відповідальності за порушення законодавства про захист інформації є складним питанням, яке потребує всебічного аналізу. У цьому контексті важливо враховувати правову природу різних видів відповідальності, їхні цілі, функції та межі застосування.

Одночасно з цим, важливою є координація між різними видами відповідальності для забезпечення повноцінного захисту інформації. Адміністративна відповідальність повинна слугувати першою лінією оборони, тоді як кримінальна та цивільна відповідальність – засобами для вирішення більш складних або тяжких випадків.

3.1. Адміністративна відповідальність

Адміністративна відповідальність має на меті забезпечення публічного порядку та дисципліни у сфері захисту інформації. Вона встановлюється за правопорушення, які не досягають рівня суспільної небезпеки, що характерний для кримінальних правопорушень. Адміністративні санкції, як правило, включають штрафи, попередження, конфіска-

цію предметів, що використовувалися у правопорушенні, а також позбавлення спеціальних прав, таких як право займати певні посади або займатися певною діяльністю.

Хоча адміністративна відповідальність є швидким і відносно простим механізмом реагування на правопорушення, вона не завжди є достатньо ефективною. Випадки серйозних порушень потребують більш суворих санкцій, що виходять за рамки адміністративного права, що підкреслює необхідність розвитку кримінальних та цивільних інструментів впливу.

3.2. Кримінальна відповідальність

Кримінальна відповідальність є найсуворішою формою юридичної відповідальності і застосовується за вчинення злочинів, що мають високий рівень суспільної небезпеки. Законодавець закріпив шість складів злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж, об'єктивна сторона яких виражається у таких формах:

1) несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж (ч. 1 ст. 361 КК України);

2) створення з метою протиправного використання, розповсюдження або збуту, а також розповсюдження або збут шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж (ч. 1 ст. 361^1 КК України);

3) несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації, створеної та захищеної відповідно до чинного законодавства (ч. 1 ст. 361^2 КК України);

4) несанкціоновані зміна, знищення або блокування інформації (ч. 1 ст. 362 КК України) та несанкціоновані перехоплення або копіювання інформації (ч. 2 ст. 362 КК України), яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах чи комп'ютерних мережах або зберігається на носіях такої інформації;

5) порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється (ст. 363 КК України);

6) умисне масове розповсюдження повідомлень електрозв'язку, здійснене без попередньої згоди адресатів (ч. 1 ст. 363^1 КК України) [9, с. 148–151].

3.3. Дисциплінарна відповідальність за порушення законодавства про захист інформації

Дисциплінарна відповідальність має юридичною підставою Кодекс законів про працю [7] та накладається адміністрацією підприємств, установ, організацій (особою, що має розпорядчо-дисциплінарну владу над конкретним працівником) внаслідок вчинення дисциплінарних проступків: 1)відповідно до правил внутрішнього трудового розпорядку; 2) в порядку підпорядкованості; 3) відповідно до дисциплінарних статутів і положень.

Реалізується виключно в рамках службової підпорядкованості. Правозастосовний акт – наказ. Застосовується до фізичної особи [10, с. 46].

3.4. Матеріальна відповідальність за порушення законодавства про захист інформації

Матеріальна (юридична підстава – Кодекс законів про працю [7] настає за вчинене майнове правопорушення, шкоду, заподіяну підприємству, установі, організації робітниками та службовцями (фізична особа) при виконанні ними своїх трудових обов'язків. Притягає до відповідальності адміністрація підприємства. Правозастосовний акт – наказ [10, с. 46].

3.5. Цивільна відповідальність

Цивільно-правова відповідальність – це виконання обов'язку з відновлення порушеного становища (права) особи або компенсації їй завданих правопорушенням шкоди, збитків, упущеної вигоди, що забезпечується відповідними заходами державного примусу, передбаченими нормами цивільного права.

Саме у сфері інформаційної діяльності чинним цивільним законодавством України передбачений механізм немайнового відновлення порушених цивільних прав. Він полягає

в обов'язку спростувати недостовірну інформацію, поширення якої порушило особисті немайнові права фізичної особи (ст. 277 ЦК України), а також у забороні поширення інформації, якою порушуються такі права (ст. 278 ЦК України). Водночас застосування цього механізму не виключає інших видів відшкодування. [9, с. 45–46].

4. Порівняльний аналіз та ефективність застосування різних видів відповідальності

Адміністративна відповідальність є важливою складовою системи захисту інформації, оскільки дозволяє оперативно реагувати на правопорушення та застосовувати заходи впливу, не пов'язані з позбавленням волі. Вона є ефективною у випадках, коли правопорушення мають незначну суспільну небезпечність та потребують співрозмірного покарання.

Кримінальна відповідальність, у свою чергу, є більш суворою та застосовується у випадках серйозних порушень, що мають високий рівень суспільної небезпеки. Вона дозволяє не тільки карати правопорушників, але й запобігати вчиненню подібних злочинів носячи превентивний характер.

Цивільна відповідальність забезпечує відновлення порушених прав потерпілих та компенсацію завданих збитків. Вона є важливим елементом системи захисту інформації, оскільки дозволяє потерпілим сторонам отримати компенсацію за завдану шкоду.

5. Взаємодія та комплексний підхід до застосування відповідальності

Ефективна система захисту інформації в інформаційних (автоматизованих) системах передбачає комплексний підхід, що включає застосування адміністративної, кримінальної та цивільної відповідальності залежно від характеру та тяжкості правопорушення. Такий підхід дозволяє забезпечити як своєчасне реагування на правопорушення, так співрозмірне покарання.

Комплексний підхід до регулювання відповідальності за порушення інформаційної безпеки є критичним для ефективного захисту інформації в сучасних умовах. У світлі стрімкого розвитку технологій та зростання ризиків кіберзагроз, законодавча система повинна відповідати вимогам часу, забезпечуючи як попередження, так і адекватне покарання за правопорушення.

Важливою є координація між різними видами відповідальності для забезпечення повноцінного захисту інформації. Адміністративна відповідальність повинна слугувати першою лінією оборони, тоді як кримінальна та цивільна відповідальність – засобами для вирішення більш складних або тяжких випадків.

Взаємодія між різними видами відповідальності є важливим аспектом, що забезпечує цілісність системи правового регулювання захисту інформації. Адміністративна відповідальність може слугувати попереджувальним заходом, кримінальна відповідальність – засобом покарання за тяжкі злочини, а цивільна та дисциплінарна відповідальність – механізмом відшкодування збитків.

Хоча адміністративна відповідальність є швидким і відносно простим механізмом реагування на правопорушення, вона не завжди є достатньо ефективною. Випадки серйозних порушень потребують більш суворих санкцій, що виходять за рамки адміністративного права, що підкреслює необхідність розвитку кримінальних та цивільних інструментів впливу.

6. Практичні аспекти застосування відповідальності

На практиці застосування адміністративної, кримінальної та цивільної відповідальності за порушення законодавства про захист інформації має свої особливості. Спеціально уповноважені суб'єкти, що здійснюють контроль за дотриманням законодавства, повинні мати достатні повноваження та ресурси для ефективного виявлення, розслідування та притягнення до відповідальності правопорушників

Таким чином, залежно від ступеня тяжкості скоєного правопорушення проти встановленого порядку захисту інформації та негативних наслідків, які наступили внаслідок цього правопорушення, можуть наступати різні види юридичної відповідальності, або навіть їх комбінації, виходячи з вимог ст. 61 Конституції України [8]: «Ніхто не може бути двічі притягнений до юридичної відповідальності одного виду за одне й те саме правопорушення» [10, с. 46].

Існує потреба у вдосконаленні законодавства в напрямку уточнення меж відповідальності, посилення санкцій та визначення чітких критеріїв застосування різних видів відповідальності. Це дозволить забезпечити більшу

юридичну визначеність і підвищити ефективність правового регулювання.

Крім удосконалення законодавства, важливим є розвиток практичних аспектів його застосування, зокрема покращення кваліфікації працівників правоохоронних органів та суддів, що займаються справами у сфері захисту інформації. Це сприятиме підвищенню ефективності розслідування та розгляду справ, пов'язаних з порушенням інформаційної безпеки.

З огляду на глобальний характер інформаційних загроз, Україна повинна активно співпрацювати з міжнародними організаціями та іншими державами у питаннях кібербезпеки та правового регулювання захисту інформації. Це допоможе запозичити найкращі практики та ефективніше реагувати на глобальні виклики.

Висновки. Співвідношення адміністративної та інших видів відповідальності за порушення законодавства про захист інформації в інформаційних (автоматизованих) системах є важливим аспектом правового регулювання цієї сфери.

Адміністративна відповідальність є важливим інструментом попередження правопорушень, однак у деяких випадках вона може бути недостатньо ефективною, оскільки слугує першою лінією оборони, тоді як кримінальна та цивільна відповідальність застосовуються для вирішення складніших випадків.

Для забезпечення надійного та ефективного захисту інформації в інформаційних (автоматизованих) системах необхідно застосовувати комплексний підхід, який включає вдосконалення законодавства, розвиток правозастосування, уточнення меж відповідальності, посилення санкцій та розвиток практичних аспектів його застосування, та посилення міжнародного співробітництва. Важливим є підвищення кваліфікації працівників правоохоронних органів та суддів, а також активна співпраця України з міжнародними організаціями для запозичення найкращих практик у сфері кібербезпеки.

Адміністративна, кримінальна та цивільна відповідальність повинні працювати в тісній взаємодії, що забезпечить ефективний захист інформації та попередження правопорушень у цій сфері.

ЛІТЕРАТУРА:

1. Про захист інформації в інформаційно-комунікаційних системах. Закон України від 05.07.1994 № 80/94-ВР.
2. Про основні засади забезпечення кібербезпеки України. Закон України від 05.10.2017 № 2163-VIII.
3. Кодекс України про адміністративні правопорушення: Закон УРСР від 7 грудня 1984 року № 8073-X.
4. Кримінальний кодекс України. Закон України від 05.04.2001 № 2341-III.
5. Цивільний кодекс України. Кодекс від 16.01.2003 № 435-IV.
6. Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах. Постанова КМУ від 29.03.2006 № 373.
7. Кодекс законів про працю України. Кодекс від 10.12.1971 № 322-VIII.
8. Конституція України. Закон України від 28.06.1996 № 254к/96-ВР.
9. Тихомиров О. О. Юридична відповідальність за правопорушення в інформаційній сфері : навч. посіб. / О. О. Тихомиров, О. К. Тугарова. К. : Нац. акад. СБУ, 2015. 172 с.
10. Бакалинський О., Богданов О., Мохор В. Відповідальність за порушення законодавства про захист інформації в інформаційних, телекомунікаційних та інформаційно телекомунікаційних системах. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*. 2009. №1(18). С.43–49.
11. Бабіч Р. В. Адміністративна відповідальність за порушення законодавства про захист інформації в інформаційних (автоматизованих) системах. *Актуальні проблеми управління інформаційною безпекою держави* : збірник матеріалів XV Всеукраїнської науково-практичної конференції. 2024. С. 50–54.