УДК 351.746
DOI https://doi.org/10.32782/2408-9257-2025-5-12

Бабіч Р. В.,
аспірант відділу аспірантури та докторантури
Національної академії Служби безпеки України
https://orcid.org/0009-0006-8990-3717

РОЗМЕЖУВАННЯ АДМІНІСТРАТИВНИХ ПРАВОПОРУШЕНЬ У СФЕРІ ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНИХ (АВТОМАТИЗОВАНИХ) СИСТЕМАХ

DEFINITION OF ADMINISTRATIVE OFFENCES IN THE FIELD OF INFORMATION PROTECTION IN INFORMATION (AUTOMATIZED) SYSTEMS

У статті здійснено комплексний науково-правовий аналіз проблеми розмежування адміністративних правопорушень у сфері захисту інформації в інформаційних (автоматизованих) системах, що має ключове значення в умовах стрімкої цифровізації державного управління, розвитку електронних сервісів та підвищення рівня кіберзагроз. Розглянуто сучасний стан нормативно-правового регулювання інформаційних правовідносин в Україні, зокрема у контексті застосування статей 212–6, 212-2, 188–31, 188–39 Кодексу України про адміністративні правопорушення (КУпАП), які визначають відповідальність за порушення законодавства про захист інформації, технічний і криптографічний захист, а також невиконання законних вимог посадових осіб уповноважених органів у цій сфері.

Проаналізовано основні елементи складів зазначених правопорушень, їхній об'єкт, суб'єктний склад, об'єктивну та суб'єктивну сторони, що дозволило виявити як спільні, так і відмінні ознаки між ними. Особливу увагу приділено питанню розмежування адміністративних деліктів від суміжних правопорушень у сфері службової діяльності, господарського управління та забезпечення державної таємниці. Розкрито підходи українських учених-адміністративістів до проблеми кваліфікації порушень у сфері інформаційної безпеки, а також наведено приклади з практики судових органів, що демонструють відмінності у правозастосуванні.

Автором запропоновано систематизовані критерії розмежування адміністративних правопорушень у сфері захисту інформації за п'ятьма ознаками: об'єкт посягання, суб'єкт відповідальності, форма вини, наслідки правопорушення та ступінь суспільної небезпечності. Підкреслено необхідність оновлення адміністративно-деліктного законодавства з урахуванням розвитку європейських стандартів у галузі кібербезпеки, норм GDPR та вимог Закону України «Про основні засади забезпечення кібербезпеки України». Зроблено висновок про доцільність гармонізації положень КУпАП із актами інформаційного законодавства, що дозволить підвищити ефективність правового захисту інформації та забезпечити баланс між свободою інформації та вимогами її безпеки.

Ключові слова: *адміністративна відповідальність, інформаційна безпека, захист інформації, інформаційні системи, правопорушення, КУпАП, кібербезпека, кваліфікація, правове регулювання, судова практика.*

The article provides an in-depth legal analysis of the differentiation of administrative offenses in the field of information protection within information (automated) systems, which has become increasingly relevant in the context of rapid digitalization, the expansion of e-governance, and the escalation of cybersecurity threats. The research examines the current state of the legal framework governing information relations in Ukraine, focusing on the interpretation and application of Articles 212–6, 212–2, 188–31, and 188–39 of the Code of Ukraine on Administrative Offenses (CUAO), which regulate liability for violations of information protection legislation, technical and cryptographic information security, and non-compliance with lawful demands of authorized officials.

The study analyzes the essential elements of these offenses – their object, subject composition, objective and subjective aspects – and identifies both overlapping and distinctive features among them. Special attention is paid to distinguishing information-related administrative delicts from adjacent categories of offenses, such as those involving public service misconduct, state secrets protection, and breaches of management regulations. The author summarizes the prevailing doctrinal approaches of Ukrainian administrative law scholars and integrates relevant examples from judicial practice that illustrate inconsistencies in qualification and application.

The article proposes a structured system of differentiation criteria based on five dimensions: the object of encroachment, the subject of liability, the form of guilt, the consequences of the offense, and the degree of public danger.

© Бабіч Р. В., 2025

The research emphasizes the need to update Ukraine's administrative-delict legislation in line with European cybersecurity standards, the provisions of the GDPR, and the Law of Ukraine "On the Basic Principles of Cybersecurity in Ukraine." The conclusions stress the importance of harmonizing the CUAO with national information laws to enhance the effectiveness of information protection mechanisms and to balance informational freedom with security imperatives in the digital environment.

Key words: *administrative liability, information security, information protection, information systems, offenses, CUAO, cybersecurity, qualification, legal regulation, judicial practice.*

Вступ. В умовах стрімкого розвитку цифрових технологій питання забезпечення захисту інформації набуває виняткового значення. Інформація є стратегічним ресурсом держави, а її витік, несанкціонований доступ чи знищення становлять реальну загрозу національній безпеці [1, с. 12]. Сучасне правове регулювання в Україні передбачає низку видів юридичної відповідальності за порушення у сфері захисту інформації, серед яких особливе місце займає адміністративна відповідальність.

В умовах розбудови інформаційного суспільства в Україні особливого значення набуває інститут адміністративної відповідальності, який є обґрунтованим засобом охорони інформаційних правовідносин, що спрямовується на запобігання порушень прав людини та інтересів держави у зазначеній сфері відносин [5, с. 31].

Водночас аналіз норм КУпАП показує наявність суттєвих прогалин і колізій у визначенні складів адміністративних правопорушень у сфері інформаційної безпеки. Це обумовлює необхідність наукового переосмислення критеріїв розмежування таких правопорушень між собою, а також відмежування їх від кримінально караних діянь.

1. Нормативно-правове підґрунтя адміністративної відповідальності у сфері захисту інформації

Базовими нормативними актами у сфері захисту інформації є Закон України «Про захист інформації в інформаційно-комунікаційних системах» [2], Закон України «Про основні засади забезпечення кібербезпеки України» [3] та Кодекс України про адміністративні правопорушення [4].

Відправною у даному дослідженні слід вважати норму статі 212–6 «Здійснення незаконного доступу до інформації в інформаційних (автоматизованих) системах, незаконне виготовлення чи розповсюдження копій баз даних інформаційних (автоматизованих) систем» КУпАП, яка встановлює адміністративну відповідальність за [4]:

– здійснення незаконного доступу до інформації, яка зберігається, обробляється чи передається в інформаційних (автоматизованих) системах, в т. ч. вчинена стосовно інформаційних (автоматизованих) систем, 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.

Таким чином, об'єктом вказаного адміністративного правопорушення є суспільні відносини з дотримання вимог із захисту інформації в автоматизованих системах, включаючи несанкціонований доступ, копіювання, поширення або знищення даних. У зв'язку з чим вказане адміністративне правопорушення можна умовно віднести до сфери захисту інформації, інформаційних ресурсів, носіїв інформації або режимів доступу.

З метою здійснення порівняльного аналізу, до вказаної сфери також можна віднести такі склади адміністративних правопорушень як:

– порушення законодавства про державну таємницю в частині невиконання норм і вимог криптографічного та технічного захисту секретної інформації, внаслідок чого виникає реальна загроза порушення її конфіденційності, цілісності і доступності (п. 9 ч. 1 ст. 212-2 КУпАП) [4];

– недодержання встановленого законодавством про захист персональних даних порядку захисту персональних даних, що призвело до незаконного доступу до них або порушен-

ня прав суб'єкта персональних даних (ч.4 ст. 188-39 КУпАП) [4];

– невиконання законних вимог посадових осіб органів Державної служби спеціального зв'язку та захисту інформації України щодо усунення порушень законодавства про криптографічний та технічний захист державних інформаційних ресурсів, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, і законодавства у сферах електронних довірчих послуг та електронної ідентифікації, а також створення інших перешкод для виконання покладених на них обов'язків (ч.1 ст. 188-31 КУпАП) [4];

Ці норми покликані забезпечити дотримання державних стандартів у сфері кібербезпеки, а також встановлюють правовий механізм реагування на адміністративні делікти, пов'язані з обробкою інформації з обмеженим доступом [6, с. 46].

Всі вищезазначені адміністративні правопорушення мають спільний родовий об'єкт – встановлений порядок управління, однак мають певні відмінності, які є підставою їх розмежування та полягають у наступному.

2. Аналіз складів адміністративних правопорушень у сфері захисту інформації

2.1. Склад правопорушення, передбаченого статтею 212–6 КУпАП.

Ця норма була запроваджена з метою забезпечення державної політики у сфері технічного та криптографічного захисту інформації, а також інформаційної безпеки в державних і недержавних інформаційних системах [3].

Розглянемо його за класичною структурою складу адміністративного правопорушення:

1) об'єкт правопорушення.

Безпосередній об'єкт – це суспільні відносини у сфері забезпечення захисту інформації в інформаційно-телекомунікаційних системах (ІТС), які забезпечують: конфіденційність, цілісність, доступність інформації, законність обробки й зберігання даних у межах функціонування ІТС.

2) об'єктивна сторона

Об'єктивна сторона виражається у діях або бездіяльності, що полягають у:

1) порушенні встановлених вимог захисту інформації, а саме:

– невиконанні положень політик безпеки або правил доступу;

– невикористанні сертифікованих засобів технічного чи криптографічного захисту;

– порушенні режимів обробки або зберігання інформації в ІТС;

– невиконанні вимог до адміністрування, резервного копіювання, контролю доступу.

2) недодержанні вимог нормативних документів ТЗІ або КЗІ, затверджених Адміністрацією Держспецзв'язку.

3) невиконанні заходів з локалізації або усунення наслідків несанкціонованого доступу, якщо такий факт мав місце.

Діяння може проявлятися у формі:

– бездіяльності (не вжито заходів захисту, не встановлено сертифіковане ПЗ, не забезпечено журналювання доступу);

– дії (навмисне відключення систем контролю, передача паролів, несанкціонована зміна конфігурацій).

Форма складу – формальна або матеріальна:

– у більшості випадків достатньо самого факту порушення правил без потреби доведення шкоди;

– проте, якщо наслідком стало порушення конфіденційності, цілісності або доступності інформації, склад набуває матеріального характеру.

3) Суб'єкт правопорушення

Суб'єкт – спеціальний. Ним може бути:

– посадова особа органу державної влади, місцевого самоврядування, підприємства, установи, організації;

– громадянин-суб'єкт підприємницької діяльності;

– адміністратор або користувач ІТС, який має доступ до технічних засобів захисту інформації.

У деяких випадках до відповідальності можуть бути притягнуті керівники організацій, які не забезпечили створення належних умов захисту інформації або не організували контроль за цим процесом.

2.4. Суб'єктивна сторона.

Вина може виражатися в умислі або необережності.

Прямий умисел: особа свідомо порушує встановлені норми, розуміючи, що це може призвести до загрози безпеці (наприклад, ігнорує встановлення сертифікованих засобів КЗІ).

Необережність: неналежне виконання обов'язків, недбалість, неуважність до вимог технічного регламенту або стандартів безпеки.

2.2. Склад правопорушення, передбаченого п.9 ч.1 ст. 212-2 КУпАП.

На відміну від попередньої норми, стаття 212–2 охоплює правопорушення, пов'язані з порушенням порядку захисту державної таємниці з урахуванням вимог технічного та криптографічного захисту інформації.

Розглянемо його за класичною структурою складу адміністративного правопорушення:

1) об'єкт правопорушення.

Безпосереднім об'єктом є суспільні відносини у сфері охорони державної таємниці та забезпечення інформаційної безпеки держави.

Додатковими об'єктами виступають:

– порядок дотримання режиму секретності;

– захист секретної інформації технічними та криптографічними засобами;

– інтереси держави у збереженні конфіденційності, цілісності та доступності відомостей, що становлять державну таємницю.

2) об'єктивна сторона.

Об'єктивна сторона полягає у дії або бездіяльності, що виражається в:

– невиконанні норм і вимог криптографічного та технічного захисту секретної інформації,

– що призвело або могло призвести до виникнення реальної загрози порушення конфіденційності, цілісності чи доступності такої інформації.

Обов'язкові ознаки об'єктивної сторони:

Діяння: невиконання встановлених нормативними актами вимог (інструкцій, положень, стандартів, зокрема ДСТУ та НД ТЗІ);

Наслідки: не обов'язково настання витоку чи розголошення, достатньо реальної загрози порушення захищеності;

Причинний зв'язок: між порушенням вимог захисту та загрозою безпеці секретної інформації.

Форма прояву – бездіяльність (невжиття заходів) або дії (використання несертифікованих засобів захисту, відключення криптосистеми, порушення режиму збереження носіїв тощо).

3) суб'єкт правопорушення.

Суб'єкт – спеціальний. Це посадова особа або працівник, на якого покладено обов'язки щодо:

– забезпечення режиму секретності;

– організації криптографічного чи технічного захисту секретної інформації;

– експлуатації технічних або програмних засобів захисту.

До таких суб'єктів належать, наприклад:

– працівники режимно-секретних органів;

– фахівці з технічного (криптографічного) захисту інформації;

– керівники установ, які мають доступ до державної таємниці.

4) суб'єктивна сторона.

Форма вини – умисел або необережність.

У більшості випадків це необережна форма вини – коли порушення вимог стало наслідком недбалості, несумлінного виконання обов'язків, халатності.

Проте можливий і прямий умисел, якщо особа свідомо ігнорувала вимоги режиму (наприклад, навмисно використовувала незахищені канали зв'язку).

Мотиви – службова недбалість, халатність, спрощення процедур, байдужість до вимог безпеки.

Відмінність від статті 212–6 полягає у предметі посягання: якщо в першому випадку мова йде про будь-яку інформацію, у другому – виключно про інформацію, яка містить державну таємницю.

Отже, критерієм розмежування є:

1) об'єкт адміністративного правопорушення – інформація з обмеженим доступом, який є спеціальним по відношенню до об'єкту, передбаченого ст. 212-6 КУпАП;

2) об'єктивна сторона правопорушення, передбаченого п.9 ч.1 ст. 212-2 КУпАП є спеціальною по відношенню до об'єктивної сторони правопорушення, передбаченого ст. 212-6 КУпАП та є одною із форм його вчинення.

2.3. Склад правопорушення, передбаченого ч.4 ст. 188–39 КУпАП

Адміністративне правопорушення, передбачене ч.4 ст. 188-39 КУпАП стосується однієї з найактуальніших проблем сучасного адміністративного права: захисту персональних даних у цифровому суспільстві.

Розглянемо склад адміністративного правопорушення, передбаченого ч. 4 ст. 188-39 КУпАП, системно, за класичною структурою чотирьох елементів:

1) об'єкт правопорушення.

Безпосередній об'єкт – це суспільні відносини у сфері захисту персональних даних, асаме–забезпеченнязаконногорежимуїхзбирання, зберігання, обробки, поширення та захисту.

Додатковий об'єкт – права і свободи фізичних осіб, зокрема:

– право на недоторканність приватного життя;

– право на повагу до честі, гідності, ділової репутації;

– право на інформаційне самовизначення (контроль над власними персональними даними).

Отже, об'єктом є суспільні відносини, спрямовані на реалізацію конституційних гарантій захисту приватного життя (ст. 32 Конституції України).

2) об'єктивна сторона.

Об'єктивна сторона цього правопорушення полягає в недодержанні встановленого законодавством порядку захисту персональних даних, якщо це призвело до незаконного доступу до них або порушення прав суб'єкта персональних даних.

Обов'язкові елементи об'єктивної сторони:

Діяння (дія або бездіяльність):

– відсутність або неналежна реалізація організаційних і технічних заходів захисту;

– невиконання вимог Закону України «Про захист персональних даних» (статті 24–27), а також нормативів КМУ, НД ТЗІ, наказів Уповноваженого ВРУ з прав людини;

– зберігання баз персональних даних без реєстрації або без визначеного режиму доступу;

– несанкціоноване надання доступу, копіювання чи передача даних.

Наслідки:

– незаконний доступ до персональних даних (витік, розголошення, злам, передача без згоди суб'єкта);

– або порушення прав суб'єкта персональних даних (наприклад, безпідставна відмова у доступі до власних даних, неправильна обробка, дискримінаційне використання інформації).

Причинний зв'язок між порушенням порядку захисту та зазначеними наслідками.

Отже, склад має матеріальний характер, оскільки для притягнення до відповідальності потрібно встановити факт настання шкідливих наслідків.

3. Суб'єкт правопорушення

Суб'єкт – спеціальний. Це посадова особа або уповноважений працівник володільця чи розпорядника персональних даних, який:

– відповідає за організацію або реалізацію системи захисту персональних даних;

– має доступ до баз даних чи здійснює їх обробку;

– порушив службові обов'язки щодо забезпечення конфіденційності, цілісності та доступності інформації.

4) суб'єктивна сторона.

Форма вини:

– умисел – коли особа свідомо порушує встановлені вимоги або навмисно допускає доступ сторонніх осіб;

– необережність – коли порушення стало наслідком недбалості, халатності, некомпетентності.

Мотиви: службова недбалість, економія часу або коштів, нехтування процедурами захисту, байдужість до прав суб'єктів.

Мета: не є обов'язковою ознакою складу, проте може бути врахована при кваліфікації та визначенні ступеня вини.

Отже, ч. 4 ст. 188-39 КУпАП і ст. 212-6 КУпАП дійсно мають схожий об'єкт правової охорони – інформаційні відносини, але різняться предметом посягання, характером порушення та наслідками.

Розмежування правопорушень за ч. 4 ст. 188-39 і ст. 212-6 КУпАП базується на різному предметі посягання та наслідках: перше спрямоване на захист особистих прав громадян, друге – на забезпечення технічної цілісності інформаційних систем.

Тому під час кваліфікації важливо встановити, чи стосувалася інформація конкретної фізичної особи, та чи були порушені її права – саме це є визначальною ознакою для застосування ч. 4 ст. 188-39 КУпАП.

2.4. Склад правопорушення, передбаченого ч. 1 ст. 188-31 КУпАП.

Частина 1 ст. 188-31 КУпАП встановлює відповідальність за невиконання законних вимог посадових осіб органів Держспецзв'язку у сферах технічного та криптографічного захисту інформації, електронних довірчих послуг і електронної ідентифікації.

Розглянемо вказаний склад адміністративного правопорушення, системно, за класичною структурою чотирьох елементів:

1) об'єкт правопорушення.

Безпосереднім об'єктом є суспільні відносини у сфері державного контролю за забезпеченням криптографічного й технічного захисту інформації, а також у сфері функціонування електронних довірчих послуг та систем електронної ідентифікації.

2) об'єктивна сторона

Об'єктивна сторона полягає у бездіяльності або діях, що виражаються в одному з таких проявів:

– невиконання законних вимог посадових осіб Держспецзв'язку (наприклад, вимоги усунути порушення у сфері ТЗІ чи КЗІ, внести зміни до політик безпеки, посилити контроль доступу тощо).

– створення перешкод посадовим особам у здійсненні перевірок або виконанні службових повноважень (відмова надавати документи, недопуск до перевірки, приховування інформації).

До об'єктивної сторони також належить:

– відмова виконати припис про усунення виявлених порушень;

– ігнорування акта перевірки або розпорядження Держспецзв'язку;

– невжиття заходів для виправлення недоліків системи захисту.

Форма складу – формальна, тобто відповідальність настає незалежно від фактичних наслідків (не потрібно доводити настання витоку чи знищення інформації).

3) Суб'єкт правопорушення.

Суб'єкт – спеціальний. Ним є посадові особи органів державної влади, місцевого самоврядування, підприємств, установ чи організацій, на яких покладено обов'язок дотримуватися вимог у сфері захисту інформації [13].

До них можуть належати:

– керівники державних органів або підприємств;

– відповідальні за інформаційну безпеку (CISO, адміністратори безпеки, фахівці ТЗІ/КЗІ);

– посадові особи, відповідальні за експлуатацію інформаційних систем.

2.4. Суб'єктивна сторона

Вина – умисна або необережна.

Умисна форма вини має місце, коли посадова особа свідомо не виконує законні вимоги або створює перешкоди перевірці.

Необережність полягає у недбалості, байдужості або неналежному контролі за виконанням обов'язків щодо інформаційної безпеки.

Мотиви можуть бути різні – від небажання витрачати ресурси на усунення порушень до спроби приховати інші порушення або технічні вади системи.

Розмежування правопорушень за ч. 1 ст. 188-31 і ст. 212-6 КУпАП базується на відмінностях об'єкту: ст. 188-31 КУпАП об'єктом виступає дотримання приписів і законних вимог посадових осіб Держспецзв'язку, тоді як об'єктом правопорушення, передбаченого ст. 212-6 КУпАП є безпосереднє порушення технічних або криптографічних норм захисту інформації. Разом з тим, слід звернути на різні завдання, визначені законодавцем, при формулюванні вказаних норм – ст. 188-31 КУпАп, по суті, є засобом забезпечення дієвості діяльності контролюючих органів (Держспецзв'язку), тоді як метою ст. 212-6 КУпАП можна вважати протидію загрозі порушенням правил, норм чи стандартів технічного захисту інформації.

Висновки. Розмежування адміністративних правопорушень у сфері захисту інформації є важливим елементом забезпечення ефективного функціонування правової системи кібербезпеки України. Чітке визначення складів правопорушень сприятиме єдності судової практики та підвищенню ефективності правозастосування. Системне оновлення адміністративного законодавства у цій сфері повинно враховувати міжнародні стандарти та динаміку розвитку інформаційних технологій.

ЛІТЕРАТУРА:

1. Кучер О. В. Інформаційна безпека держави: правові аспекти / О. В. Кучер. – Київ: Юрінком Інтер, 2021. – 210 с.

2. Про захист інформації в інформаційно-комунікаційних системах: Закон України від 05.07.1994 № 80/94-ВР // Відомості Верховної Ради України. – 1994. – № 31. – Ст. 286.

3. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII // Відомості Верховної Ради України. – 2017. – № 45. – Ст. 403.

4. Кодекс України про адміністративні правопорушення: Закон УРСР від 7 грудня 1984 року № 8073-X.

5. Топчій В. В., Бодунова О. М. Адміністративна відповідальність у сфері забезпечення кібербезпеки України // Адміністративне право і процес; фінансове право; інформаційне право. – 2021. – №5, т.3. – С.31-35

6. Тихомиров О. М. Адміністративна відповідальність у сфері кібербезпеки: сучасні тенденції та виклики // Вісник Національного університету «Одеська юридична академія». – 2022. – № 3. – С. 45–53.

7. Скакун О. Ф. Теорія держави і права. – Харків: Право, 2020. – 520 с.

8. Петренко В. І. Правопорушення у сфері захисту інформації: проблеми кваліфікації // Юридичний вісник України. – 2021. – № 9. – С. 50–54.

9. Кримінальний кодекс України: Закон України від 05.04.2001 № 2341-III // Відомості Верховної Ради України. – 2001. – № 25–26. – Ст. 131.

10. Коваль Л. В. Юридична відповідальність у сфері інформаційної безпеки. – Львів: ЛНУ ім. І. Франка, 2022. – 198 с.

11. Мельник М. І. Адміністративна юрисдикція у сфері кібербезпеки: теорія та практика. – Київ: НАВС, 2023. – 184 с.

12. Кохановська О. В., Швець М. Я. Правове регулювання захисту персональних даних // Науковий вісник Київського університету права. – 2023. – № 3. – С. 112–119.

13. Постанова КМУ від 29.03.2006 р. № 373 «Про затвердження Положення про Держспецзв'язок».

Дата першого надходження рукопису до видання: 22.10.2025
Дата прийнятого до друку рукопису після рецензування: 25.11.2025
Дата публікації: 19.12.2025