

**ПРИВАТНЕ АКЦІОНЕРНЕ ТОВАРИСТВО
«ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД»
МІЖРЕГІОНАЛЬНА АКАДЕМІЯ УПРАВЛІННЯ ПЕРСОНАЛОМ**
Кафедра _____

КУРСОВА РОБОТА

з дисципліни: «ІНФОРМАЦІЙНЕ ПРАВО»
за темою: «ІНФОРМАЦІЙНІ РЕСУРСИ»

Студента (ки): Вознюка Д.О.
курсу: 4
групи: ІН16-9-22-Б1П(4.0д)
Спеціальність: Право
Керівник: к.ю.н., доцент кафедри
Лебедєв О.П.

Оцінка: _____
Національна шкала _____
Кількість балів: _____ ECTS _____

Члени комісії	_____	_____
	(підпис)	(прізвище та ініціали)
	_____	_____
	(підпис)	(прізвище та ініціали)
	_____	_____
	(підпис)	(прізвище та ініціали)

м. Чернігів 2026

ЗМІСТ

Вступ.....	3
РОЗДІЛ 1.	
ПОНЯТТЯ ТА СУТНІСТЬ ІНФОРМАЦІЙНИХ РЕСУРСІВ	6
1.1 Поняття інформаційних ресурсів	6
1.2 Правова природа інформаційних ресурсів	9
1.3 Взаємозв'язок інформаційних ресурсів із іншими категоріями	11
РОЗДІЛ 2.	
КЛАСИФІКАЦІЯ ТА ВИДИ ІНФОРМАЦІЙНИХ РЕСУРСІВ	14
2.1. Основні категорії інформаційних ресурсів та їхні характеристики	14
2.2. Правові режими доступу до інформаційних ресурсів.....	17
2.3. Проблеми та перспективи розвитку інформаційних ресурсів.....	18
РОЗДІЛ 3.	
ПРАВОВИЙ РЕЖИМ І ЗАХИСТ ІНФОРМАЦІЙНИХ РЕСУРСІВ.....	21
3.1. Класифікація інформації	21
3.2. Інформація з обмеженим доступом	23
3.3. Правовий режим інформації	25
Висновок	29
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	33

Вступ

Актуальність теми. У сучасному інформаційному суспільстві інформаційні ресурси набувають особливої значущості, оскільки вони виступають основою функціонування держави, бізнесу, науки та освіти. Цифровізація суспільних процесів, глобальна інтеграція інформаційних технологій та розвиток електронних сервісів роблять питання правового регулювання інформаційних ресурсів надзвичайно актуальним. У зв'язку з цим ефективне управління та захист інформаційних ресурсів стають критично важливими для забезпечення безпеки, стабільності та прозорості суспільного життя [1, с. 37; 6, с. 40].

Правовий статус інформаційних ресурсів визначається їхньою роллю в обміні знаннями та даними, формуванні управлінських рішень, забезпеченні конкурентних переваг у бізнесі та гарантуванні права громадян на доступ до інформації. Недотримання правових норм у сфері обігу інформації може призводити до економічних втрат, шкоди репутації підприємств, порушення прав фізичних осіб та загрози національній безпеці [8, с. 89; 7, с. 53].

Сучасні наукові дослідження підкреслюють, що правова природа інформаційних ресурсів є багатовимірною категорією, яка включає об'єктність, нематеріальність, функціональне використання та спеціальні режими захисту. Врахування цих аспектів є основою для побудови ефективної системи правового регулювання, що гарантує баланс між відкритістю та захищеністю інформації [8, с. 92; 7, с. 57].

Таким чином, вивчення правового режиму інформаційних ресурсів, їх класифікації та взаємозв'язку з іншими категоріями інформаційного права є важливою науковою та практичною проблемою, що визначає актуальність даної курсової роботи.

Метою даної роботи є комплексний аналіз поняття інформаційних ресурсів, їх правової природи та режиму використання, а також визначення проблем і перспектив розвитку системи інформаційного права в Україні.

Досягнення мети передбачає вирішення таких **завдань**:

1. Проаналізувати наукові підходи до визначення поняття «інформаційні ресурси» та їх основні характеристики.
2. Вивчити правову природу інформаційних ресурсів, їх об'єктність, функціональні та ціннісні аспекти.
3. Охарактеризувати взаємозв'язок інформаційних ресурсів з інформацією, даними, знаннями та інформаційними системами.
4. Провести класифікацію інформаційних ресурсів та визначити особливості їх використання у державних, комерційних, наукових і соціальних сферах.
5. Дослідити проблеми та перспективи розвитку інформаційних ресурсів з огляду на цифровізацію, кіберзагрози та правові виклики.
6. Проаналізувати класифікацію інформації, правовий режим доступу та захисту публічної, конфіденційної, таємної та службової інформації.

Об'єктом дослідження є інформаційні ресурси як об'єкт інформаційного права, їх класифікація, функціонування та правовий режим використання в умовах цифровізації та розвитку інформаційного суспільства.

Предметом дослідження виступають правові відносини, що виникають у процесі створення, обігу, використання та захисту інформаційних ресурсів, а також механізми їх правового регулювання, включно з режимом доступу та захисту даних.

Методи дослідження. У процесі виконання курсової роботи використовувалися такі наукові методи:

Аналіз нормативно-правових актів – для вивчення законодавчих основ доступу, використання та захисту інформаційних ресурсів [1, с. 38; 8, с. 94].

Порівняльно-правовий метод – для зіставлення українського законодавства з міжнародними стандартами та практикою інших країн [10, с. 24; 19, с. 255].

Системний підхід – для визначення взаємозв'язку інформаційних ресурсів із іншими категоріями інформаційного права та побудови класифікацій [7, с. 53].

Контент-аналіз наукової літератури та судової практики – для виявлення тенденцій розвитку правового регулювання та проблем захисту інформації [6, с. 40; 8, с. 89].

Метод моделювання – для прогнозування перспектив розвитку інформаційних ресурсів та впровадження технологічних новацій у правове регулювання [16, с. 195].

Джерельна база курсової роботи складається з:

1. Законів та підзаконних актів України у сфері інформаційного права, зокрема Закону України «Про інформацію», Закону «Про доступ до публічної інформації», Закону «Про захист персональних даних», Закону «Про комерційну таємницю» та інших нормативних документів [1, с. 37; 2, с. 190].

2. Монографій, наукових статей та посібників українських авторів останніх 6 років, що досліджують проблематику інформаційних ресурсів, їх класифікацію, правовий режим та цифрові технології [5, с. 34; 6, с. 40; 7, с. 53; 8, с. 89].

3. Матеріалів конференцій, аналітичних оглядів та електронних ресурсів щодо розвитку інформаційного права та цифровізації суспільства [10, с. 24; 19, с. 255].

Таким чином, актуальність теми обумовлюється необхідністю ефективного регулювання обігу інформаційних ресурсів в умовах цифровізації, зростанням ролі інформації у суспільному, державному та комерційному житті, а також потребою гармонізації українського законодавства з міжнародними стандартами. Мета та завдання дослідження визначають комплексний підхід до вивчення поняття, класифікації, правової природи та режиму використання інформаційних ресурсів, що становить основу подальших розділів курсової роботи.

РОЗДІЛ 1.

ПОНЯТТЯ ТА СУТНІСТЬ ІНФОРМАЦІЙНИХ РЕСУРСІВ

1.1 Поняття інформаційних ресурсів

Інформаційні ресурси – це сукупність даних, документів, матеріалів та цифрових об’єктів, які створюються, систематизуються, зберігаються та використовуються усвідомлено для задоволення інформаційних потреб суспільства, органів влади, бізнесу, науки, освіти та окремих громадян. Вони охоплюють як традиційні носії інформації – паперові документи, книги, журнали, архівні матеріали, так і сучасні цифрові форми: бази даних, електронні документи, мультимедійні файли, мережеві та хмарні сервіси, програмні та аналітичні ресурси [6, с. 40].

Науковці підкреслюють, що інформаційні ресурси – це не просто набір відомостей, а комплексна система знань, що має структуру, форму організації, способи обробки та передачі. Така комплексність визначає їхню цінність і робить їх невід’ємною частиною сучасного інформаційного суспільства [7, с. 53].

Інформаційні ресурси виконують низку соціальних та правових функцій, які формують їхнє значення для держави та суспільства.

Комунікативна функція забезпечує обмін інформацією між суб’єктами правовідносин. Це може бути як обмін офіційними документами між органами влади, так і поширення даних у наукових колах або через відкриті електронні ресурси для громадян [8, с. 89].

Регулятивна функція спрямована на формування правил та стандартів поведінки в суспільстві. Наприклад, нормативні бази даних або офіційні документи органів влади встановлюють рамки дій для фізичних та юридичних осіб, визначаючи їхні права та обов’язки [7, с. 54].

Контролююча функція дозволяє оцінювати діяльність органів влади, підприємств та установ. За допомогою аналітичних, статистичних та

публічних ресурсів забезпечується прозорість управлінських рішень, а також контроль за дотриманням законодавства [8, с. 91].

Освітня та наукова функція полягає у використанні інформаційних ресурсів як джерел знань та матеріалів для навчання, досліджень, підготовки кваліфікованих кадрів та розвитку науки.

Наприклад, електронні бібліотеки та науково-аналітичні платформи сприяють доступу до актуальної інформації та обміну знаннями між науковцями [6, с. 43].

Крім того, інформаційні ресурси відіграють важливу економічну роль. В умовах цифровізації вони стають стратегічним ресурсом розвитку бізнесу, оскільки від точності, повноти та своєчасності даних залежить ефективність управлінських рішень, конкурентоспроможність підприємств і стабільність економічних процесів [7, с. 56].

Системний підхід до класифікації інформаційних ресурсів у правовій науці передбачає виділення кількох взаємопов'язаних характеристик, що дозволяють комплексно оцінити їхню сутність, функції та значення. До таких характеристик відносять:

Онтологічну складову, яка визначає, що саме є інформаційним ресурсом. Ця складова передбачає чітке визначення об'єктів, які можна віднести до інформаційних ресурсів, включаючи як структуровані дані у вигляді баз даних, документів та звітів, так і напівструктуровані чи неструктуровані ресурси – наприклад, тексти, графічні та аудіовізуальні матеріали, веб-сторінки та інші цифрові об'єкти. Онтологічна складова дозволяє визначити правову природу цих ресурсів, їх статус об'єктів правовідносин та необхідність їх захисту державою [7, с. 53].

Функціональна складова, яка описує способи використання інформаційних ресурсів у правовому та суспільному полі. Вона включає аналіз цільового призначення ресурсів, механізмів їх обігу та ролі у забезпеченні суспільних потреб. Функціональна складова дозволяє встановити, як інформаційні ресурси використовуються у процесі управління державою,

бізнесом, освітою та наукою, а також у діяльності громадських організацій. Завдяки цьому підходу можна визначити, які ресурси мають відкритий доступ, які підлягають обмеженню, а які вимагають спеціального захисту як конфіденційні або державні [7, с. 54].

Ціннісна складова, що відображає економічну, соціальну, політичну та культурну значущість ресурсів для конкретного суб'єкта або суспільства загалом. Ціннісна оцінка дозволяє визначити пріоритети доступу до ресурсів, їх комерційне або стратегічне значення, а також вплив на розвиток інформаційного суспільства. Наприклад, наукові бази даних та освітні електронні ресурси мають високу соціальну та освітню цінність, а державні реєстри та інформаційні системи органів влади – політичну та стратегічну цінність для забезпечення управлінських та контролюючих функцій [7, с. 55].

Важливо підкреслити, що системний підхід дозволяє розглядати інформаційні ресурси як комплексну категорію, де онтологічна, функціональна та ціннісна складові взаємодіють і впливають одна на одну. Наприклад, ресурси з високою економічною або стратегічною цінністю часто потребують спеціальних механізмів захисту, а ресурси освітньої та наукової значущості – відкритого доступу та сприяння вільному обміну інформацією [7, с. 56].

З огляду на зазначене, можна стверджувати, що інформаційні ресурси є не лише джерелом даних, але й активним інструментом розвитку держави, бізнесу, науки та освіти. Вони забезпечують ефективність управлінських рішень, сприяють формуванню прозорості діяльності органів влади, підвищують конкурентоспроможність підприємств та створюють умови для розвитку інформаційного суспільства. Крім того, інформаційні ресурси виступають фундаментом інформаційної безпеки, дозволяючи встановлювати правові та технічні механізми захисту даних і підтримувати баланс між відкритістю інформації та охороною прав громадян та держави [7, с. 57].

Таким чином, системна класифікація та аналіз інформаційних ресурсів дозволяє не лише науково обґрунтувати їхнє значення, але й практично

реалізувати правові механізми управління та захисту цих ресурсів у різних сферах суспільного життя. Вона є невід’ємною складовою сучасного інформаційного права та основою формування політики держави у сфері інформаційних відносин.

1.2 Правова природа інформаційних ресурсів

Правова природа інформаційних ресурсів полягає у їхньому статусі об’єкта інформаційних правовідносин. Це означає, що їхній обіг, доступ, використання та охорона підпорядковуються чітко визначеним нормам права, а державні органи, бізнес-структури та громадяни зобов’язані дотримуватися встановлених правил. Такий правовий режим визначає межі законного використання інформаційних ресурсів та встановлює відповідальність за порушення цих норм [1, с. 37].

Основні аспекти правової природи інформаційних ресурсів включають:

Об’єктність – інформаційні ресурси є юридично визначеними об’єктами, що можуть виступати предметом інформаційних правовідносин. Це означає, що законодавство може встановлювати правила щодо прав власності, обмежень доступу, умов використання та відповідальності за неправомірне поводження з ресурсами. Наприклад, державні реєстри, наукові бази даних, корпоративні інформаційні системи або електронні документи можуть підпадати під різні правові режими, що гарантує їх правову охорону та контроль [6, с. 42].

Нематеріальність та формалізація – інформаційні ресурси мають нематеріальний характер, проте їхнє існування можливе лише через певні носії: друковані, електронні, цифрові або хмарні системи. Важливо підкреслити, що правове регулювання спрямоване не на абстрактну інформацію, а на порядок її обігу, способи використання, захист та поширення. Так, законодавство встановлює вимоги до електронних баз даних,

систем зберігання інформації, цифрових платформ та способів обробки персональних даних [8, с. 92].

Еволюційний характер – стрімкий розвиток цифрових технологій, поява нових форм інформаційних ресурсів та нових способів їх використання створює додаткові правові виклики. Наприклад, хмарні сервіси, системи штучного інтелекту, блокчейн-технології, великі дані (Big Data) та цифрові платформи вимагають нових механізмів захисту, правового регулювання доступу, ліцензування та авторського права. Це підкреслює необхідність постійного вдосконалення законодавства та адаптації правових норм до сучасних умов [7, с. 57].

Законодавство України визначає ключові принципи правового режиму інформаційних ресурсів:

Відкритість – забезпечення доступу до публічних ресурсів для громадян, науковців, студентів та бізнесу. Це стосується, наприклад, відкритих державних реєстрів, статистичних даних та освітніх платформ, що сприяє розвитку прозорості управління та інформаційної доступності [1, с. 38].

Захищеність – охорона персональних даних, комерційної таємниці, державної таємниці та конфіденційної інформації. Це передбачає застосування правових і технічних заходів безпеки, шифрування, обмеження доступу та відповідальність за порушення [8, с. 94].

Пропорційність – обмеження доступу до ресурсів має здійснюватися лише у випадках, передбачених законом, з урахуванням балансу між інтересами держави, суспільства та окремих громадян. Це забезпечує захист прав користувачів та водночас запобігає зловживанню інформаційними ресурсами [1, с. 38].

Крім того, правова природа інформаційних ресурсів включає функцію балансу суспільних інтересів. З одного боку, суспільство потребує відкритого доступу до інформації для розвитку науки, освіти, культури та прозорості державного управління. З іншого боку, необхідно запобігати неправомірному використанню даних, яке може завдати шкоди особам, підприємствам або

державі. Цей баланс реалізується через правові механізми, такі як ліцензування, отримання дозволів, встановлення санкцій та відповідальності за порушення, контроль дотримання правил доступу та використання інформаційних ресурсів [8, с. 95].

Таким чином, правова природа інформаційних ресурсів є багатовимірною категорією, що поєднує:

онтологічне існування ресурсів (що саме вони представляють);

функціональне використання (які завдання вирішують у суспільстві та економіці);

правове регулювання (правила обігу, доступу та охорони).

Це робить інформаційні ресурси ключовим елементом сучасного інформаційного суспільства, основою для ефективного державного управління, розвитку бізнесу та забезпечення безпеки інформаційного середовища. Вони виконують стратегічну роль у формуванні правової культури, інформаційної безпеки та інноваційного розвитку на всіх рівнях суспільства.

1.3 Взаємозв'язок інформаційних ресурсів із іншими категоріями

Інформаційні ресурси тісно взаємопов'язані з іншими базовими категоріями інформаційного права та теорії інформації, такими як дані, інформація, документи, знання та інформаційні системи. Науковці підкреслюють, що інформаційний ресурс є більш широким і комплексним поняттям у порівнянні з окремими даними чи інформацією, оскільки включає не лише самі відомості, а й методи їх організації, структурування, обробки, збереження та поширення [9, с. 78]. Це означає, що інформаційний ресурс можна розглядати як системний об'єкт, який об'єднує матеріальні носії, цифрові платформи, електронні бази даних, документи та механізми управління інформацією.

Важливо зазначити, що дані представляють собою початкові фактичні елементи, які без контексту не набувають смислового навантаження. Інформація формується шляхом обробки даних, надання їм структури та смислу, тоді як знання виникає на основі аналізу та інтерпретації інформації і має практичне або теоретичне застосування. Інформаційні ресурси, у свою чергу, включають весь цей спектр – від сирих даних до знань, а також механізми та інструменти їх зберігання, передачі та використання. Саме тому в юридичній науці інформаційні ресурси розглядаються як багаторівнева та комплексна категорія, що об'єднує технологічний, організаційний та правовий аспекти [10, с. 26].

Питання формування та правового регулювання інформаційних ресурсів виникло на стику розвитку інформаційних технологій та нормативно-правового забезпечення їх використання. Перші наукові трактування цього поняття з'явилися у 1970-х роках, разом із поширенням обчислювальної техніки та появою перших електронних баз даних. Тоді інформаційні ресурси розглядалися переважно як сукупність даних та документів, доступних для обробки на комп'ютерних системах [9, с. 80].

Сучасні підходи до визначення та класифікації інформаційних ресурсів формуються під впливом цифровізації суспільства, розвитку глобальних мереж та хмарних технологій. Зокрема, наявність великих даних (Big Data), електронних архівів, цифрових освітніх платформ, корпоративних інформаційних систем та технологій штучного інтелекту ускладнює процес регулювання та визначення правового статусу ресурсів. У цьому контексті інформаційні ресурси розглядаються не лише як технічні або організаційні об'єкти, але й як юридично захищені активи, які мають економічну, соціальну та політичну цінність [10, с. 28].

Українські вчені останніх років приділяють особливу увагу узгодженню національного законодавства з європейськими стандартами, зокрема у сфері захисту персональних даних, відкритих даних та електронного документообігу. Вони підкреслюють, що ефективне використання

інформаційних ресурсів вимагає комплексного правового підходу, який враховує баланс між відкритістю ресурсів та їх захистом, а також взаємозв'язок між технологічними можливостями та нормативними обмеженнями [10, с. 30].

Таким чином, можна зробити висновок, що інформаційні ресурси є ключовою категорією інформаційного права, яка поєднує онтологічну, функціональну та ціннісну складові, а також інтегрується з іншими правовими, соціальними та технологічними елементами. Вони виступають фундаментом інформаційного суспільства, забезпечують ефективне управління державними, економічними та науково-освітніми процесами, а також створюють основу для розробки сучасних правових механізмів захисту інформації та контролю за її обігом.

РОЗДІЛ 2.

КЛАСИФІКАЦІЯ ТА ВИДИ ІНФОРМАЦІЙНИХ РЕСУРСІВ

2.1. Основні категорії інформаційних ресурсів та їхні характеристики

Інформаційні ресурси є багаторівневою та комплексною категорією, що включає різноманітні типи даних, документів та цифрових об'єктів, які відрізняються за формою, способом створення, структурою, носієм та сферою використання. У сучасній юридичній науці наголошується, що класифікація інформаційних ресурсів необхідна для ефективного правового регулювання обігу інформації, встановлення режимів доступу, захисту та відповідальності за неправомірне використання [5, с. 102].

Державні інформаційні ресурси складають одну з найбільш значущих категорій. Вони формуються та підтримуються органами державної влади, місцевого самоврядування та державними установами і включають такі типи даних: статистичну інформацію, нормативно-правові акти, реєстри громадян, юридичних осіб, державні програми, економічні та соціальні показники. Відкритість державних ресурсів забезпечує прозорість діяльності органів влади, контроль за їхніми рішеннями та реалізацію конституційного права громадян на доступ до інформації. Доступ до таких ресурсів здійснюється через публічні портали, електронні реєстри, офіційні веб-сайти та державні інформаційні системи.

Окрему увагу вчені приділяють нормативному забезпеченню: наприклад, Закони України «Про доступ до публічної інформації» та «Про державну статистику» встановлюють правила формування, зберігання та використання державних інформаційних ресурсів [5, с. 104].

Комерційні інформаційні ресурси охоплюють дані, що мають економічну цінність для підприємств, організацій та бізнес-структур. До них належать бухгалтерські документи, фінансові звіти, маркетингові

дослідження, бізнес-плани, клієнтські бази даних, комерційна таємниця та внутрішні корпоративні документи.

Особливість комерційних ресурсів полягає у необхідності захисту комерційної таємниці та конфіденційної інформації, що регламентується законодавством України, зокрема Законом «Про комерційну таємницю», а також договірними умовами використання ресурсів. Ефективне управління комерційними ресурсами забезпечує конкурентні переваги підприємств, сприяє розвитку інновацій та економічного зростання. Крім того, сучасні тенденції цифровізації бізнесу передбачають використання хмарних сервісів, корпоративних інформаційних систем та платформ для аналізу великих даних (Big Data), що підвищує значимість правового захисту комерційних ресурсів від витоку та неправомірного використання [8, с. 178].

Наукові та освітні інформаційні ресурси включають матеріали, що використовуються у сфері науки, освіти та досліджень. Це статті, монографії, дисертації, освітні онлайн-платформи, відкриті бази даних, наукові портали та бібліотеки. Основними особливостями цієї категорії є інтелектуальна цінність ресурсів, обов'язковий захист авторських та суміжних прав, забезпечення доступу для освітніх та наукових цілей, а також підтримка відкритого обміну знаннями відповідно до принципів Open Access.

Особливу роль відіграють цифрові освітні платформи та інтегровані бази даних, які дозволяють дослідникам та студентам отримувати доступ до актуальних наукових результатів у режимі онлайн, що стимулює інноваційний розвиток та міжнародну співпрацю [12, с. 118].

Соціальні інформаційні ресурси охоплюють дані про населення, результати соціологічних та демографічних опитувань, медичні записи, освітні досягнення, трудові ресурси та інші статистичні показники соціальної сфери. Такі ресурси часто містять персональні дані громадян, що підлягають суворому режиму конфіденційності та обмеженого доступу.

Правовий режим соціальних ресурсів регулюється законами України «Про захист персональних даних», «Про інформацію» та спеціальними

нормативними актами, які визначають порядок обробки, зберігання та доступу до інформації. Використання соціальних ресурсів є важливим інструментом для формування державної політики, оцінки соціально-економічного розвитку та прийняття управлінських рішень [17, с. 222].

Особлива увага приділяється критеріям оцінки інформаційних ресурсів, які включають:

достовірність,
повноту,
актуальність,
структурованість,
доступність,
відповідність законодавчим вимогам та ефективність використання.

Ці критерії визначають можливості застосування ресурсів у державному управлінні, бізнесі, науці та освіті, а також впливають на якість прийняття рішень [15, с. 175].

Розвиток цифрових технологій значно розширив функціональні можливості інформаційних ресурсів. Наприклад, хмарні сервіси та блокчейн-платформи дозволяють централізовано зберігати великі обсяги даних, забезпечувати одночасний доступ для великої кількості користувачів, відстежувати зміни та гарантувати цілісність інформації. Разом з цим зростають ризики, пов'язані з кібербезпекою, витоком даних, неправомірним доступом та порушенням авторських прав, що потребує розробки нових правових механізмів та стандартів захисту [16, с. 198].

Таким чином, сучасна класифікація інформаційних ресурсів дозволяє не лише систематизувати існуючі дані та документи, а й забезпечує правову основу для регулювання обігу інформації, захисту прав власників ресурсів та ефективного використання в різних сферах суспільного життя. Інформаційні ресурси є ключовими активами держави, бізнесу, науки та освіти, від їхньої організації, якості та захищеності залежить розвиток суспільства та інформаційної безпеки [5, с. 106; 8, с. 180; 12, с. 120].

2.2. Правові режими доступу до інформаційних ресурсів

Правовий режим інформаційних ресурсів визначає умови їх використання, поширення та захисту. Він є ключовим елементом системи інформаційного права, оскільки відрізняє публічні ресурси від тих, що мають обмежений доступ.

Публічні ресурси – відкриті для всіх суб'єктів. До них належать офіційні документи, нормативно-правові акти та дані, що не містять конфіденційної інформації. Законодавство зобов'язує органи влади забезпечувати доступ до таких ресурсів через публічні портали та за запитами громадян [5, с. 102].

Ресурси обмеженого доступу – доступ до них регламентується спеціальними правилами.

До них належать:

- державна таємниця – інформація, що стосується безпеки, оборони та зовнішньої політики держави [2, с. 190].
- комерційна таємниця – дані підприємств, які забезпечують економічну перевагу та не підлягають загальному доступу [8, с. 175].
- персональні дані – відомості про фізичних осіб, що ідентифікують їх та підлягають захисту відповідно до закону «Про захист персональних даних» [17, с. 218].

Конфіденційні ресурси – створюються для внутрішнього використання організацій та підприємств. Вони включають службові документи, внутрішні звіти, плани та протоколи, і доступ до них надається лише уповноваженим особам.

Службові ресурси – мають обмежений доступ для конкретного кола працівників державних органів або організацій, оскільки містять інформацію, що впливає на управлінські процеси [1, с. 120].

Правовий режим забезпечує баланс між правом на доступ до інформації та необхідністю її захисту. У сучасних умовах цифровізації встановлення такого балансу стає складнішим через обсяги даних та ризики кіберзагроз.

2.3. Проблеми та перспективи розвитку інформаційних ресурсів

Управління інформаційними ресурсами стикається з низкою складних правових, організаційних та технічних проблем, які потребують як удосконалення законодавчого регулювання, так і розвитку сучасних технологічних стандартів. В першу чергу, це пов'язано зі швидкою цифровізацією суспільства та зростанням обсягів оброблюваної інформації, що створює нові виклики для забезпечення доступності, достовірності та безпеки ресурсів [13, с. 139].

1. Недосконалість законодавства щодо цифрових ресурсів
Сучасні нормативні акти України часто не враховують специфіку обробки великих масивів даних (Big Data), хмарних сервісів, платформ електронного документообігу та мережевих інфраструктур. Наприклад, питання правового статусу хмарних даних, розподілених баз даних або цифрових сервісів штучного інтелекту майже не врегульовані на законодавчому рівні. Це створює прогалини у захисті прав користувачів, забезпеченні конфіденційності та визначенні відповідальності за неправомірне використання ресурсів. У науковій літературі підкреслюється, що відсутність узгоджених правил призводить до хаотичного застосування нормативів, що ускладнює контроль над обігом інформації та її правовий захист [13, с. 140].

2. Кіберзагрози та ризики витоку інформації
Поширення цифрових ресурсів підвищує їхню вразливість до неправомірного доступу, кібератак, фішингових схем, хакерських втручань та використання для шахрайства. Особливо це стосується персональних даних громадян, комерційних баз даних та державних реєстрів. В умовах цифрової трансформації організації змушені впроваджувати сучасні стандарти кібербезпеки, багатоетапну аутентифікацію, шифрування та системи моніторингу. Науковці також зазначають, що недостатня кіберзахищеність призводить до фінансових втрат, шкоди репутації компаній та державних органів, а також порушення прав громадян [14, с. 159].

3. Відсутність універсальної системи оцінки ресурсів

У багатьох сферах немає єдиного стандарту для визначення повноти, актуальності, достовірності та структурованості інформаційних ресурсів. Відсутність таких критеріїв ускладнює управління ресурсами, планування розвитку інформаційних систем та правове регулювання. Це стосується як державних, так і комерційних або соціальних ресурсів. Для ефективного використання даних необхідно запроваджувати системи сертифікації інформаційних ресурсів, стандартизовані формати метаданих, а також інструменти аудиту та верифікації даних [15, с. 175].

4. Технологічні та організаційні проблеми

Окрім правових, існують також технологічні та організаційні труднощі. До них належать: недостатня сумісність різних інформаційних систем, відсутність інтегрованих платформ для управління ресурсами, низький рівень кваліфікації персоналу у сфері інформаційного права та цифрової безпеки. Ці проблеми ускладнюють централізоване управління ресурсами та створюють ризики дублювання або втрати інформації. Вчені підкреслюють необхідність впровадження комплексних систем управління даними (Data Governance), які поєднують юридичні, технічні та організаційні механізми [14, с. 162].

5. Перспективи розвитку інформаційних ресурсів

Незважаючи на існуючі проблеми, розвиток інформаційних ресурсів відкриває значні можливості для держави, бізнесу та науки:

Впровадження єдиних електронних реєстрів та порталів підвищує доступність даних для громадян, забезпечує прозорість діяльності органів влади та полегшує контроль за виконанням законодавчих норм. Наприклад, електронні портали відкритих даних (Open Data) дозволяють аналізувати державну статистику, відстежувати бюджетні витрати та підвищувати ефективність управління [19, с. 257].

Використання штучного інтелекту та аналітики великих даних дає змогу автоматизувати обробку ресурсів, прогнозувати соціально-економічні тенденції, аналізувати великі масиви інформації та підтримувати прийняття

управлінських рішень. Це особливо актуально для державних та комерційних систем, де обсяг даних перевищує можливості традиційного оброблення [13, с. 142].

Гармонізація українського законодавства з європейськими стандартами щодо захисту персональних даних та доступу до інформації (наприклад, відповідно до GDPR) сприятиме підвищенню довіри користувачів, забезпечить ефективний захист прав громадян та створить передумови для інтеграції України у глобальні цифрові ринки [19, с. 260].

Інноваційні технології зберігання та обробки ресурсів, такі як блокчейн, децентралізовані системи управління даними та хмарні платформи, забезпечують надійність, прозорість та відстежуваність інформаційних потоків, що підвищує безпеку та ефективність використання ресурсів.

Підвищення рівня інформаційної культури та цифрової компетентності серед державних службовців, працівників бізнесу та громадян дозволить ефективно використовувати інформаційні ресурси, зменшить ризики порушень та сприятиме розвитку інформаційного суспільства.

Таким чином, правове та організаційне регулювання інформаційних ресурсів повинно постійно адаптуватися до швидкого розвитку цифрових технологій. Важливо забезпечити баланс між відкритістю, безпекою та ефективним використанням ресурсів, що дозволить задовольняти інформаційні потреби суспільства, держави та бізнесу, сприяти розвитку науки та освіти, а також підвищувати рівень інформаційної безпеки в країні [13, с. 145; 14, с. 165; 15, с. 178; 19, с. 262].

РОЗДІЛ 3.

ПРАВОВИЙ РЕЖИМ І ЗАХИСТ ІНФОРМАЦІЙНИХ РЕСУРСІВ

3.1. Класифікація інформації

Інформація в юридичному розумінні є фундаментальним об'єктом інформаційних правовідносин та підлягає правовому регулюванню. Вона виступає основою для формування норм, що визначають права та обов'язки суб'єктів у сфері обігу інформації, її використання та захисту. Відповідно до законодавства України, інформація поділяється на кілька основних категорій, кожна з яких має свій специфічний правовий режим та порядок доступу:

1. Публічна інформація – це відкриті дані, доступні для всіх громадян, органів державної влади, науковців, бізнесу та громадських організацій. До публічної інформації належать офіційні документи органів державної влади, закони та підзаконні акти, статистичні дані, звіти про діяльність органів влади та місцевого самоврядування. Публічна інформація сприяє реалізації конституційного права громадян на інформацію, забезпечує прозорість діяльності органів влади та демократичний контроль за їхніми діями [5, с. 34]. Вона також є основою для розвитку наукових досліджень, навчання та інформаційного бізнесу, оскільки відкриті дані дозволяють аналізувати тенденції та приймати обґрунтовані управлінські рішення.
2. Інформація з обмеженим доступом – це відомості, поширення яких законодавчо обмежується для захисту державних, комерційних та особистих інтересів.

До цієї категорії належать:

Державна таємниця, що включає відомості у сферах оборони, національної безпеки, зовнішньої політики та стратегічної економіки;

Комерційна таємниця, яка охороняє економічно цінну інформацію підприємств та організацій;

Персональні дані, що містять відомості про фізичних осіб і забезпечують захист права на приватність [2, с. 190]. Інформація з обмеженим доступом підлягає суворому контролю та використанню за спеціальними правилами, включно з процедурою отримання дозволів, дотриманням умов конфіденційності та застосуванням технічних засобів захисту від несанкціонованого доступу.

3. Конфіденційна інформація – це дані, що охороняються за ініціативою їхнього власника і не підлягають розголошенню без його дозволу. Такою інформацією можуть бути внутрішні документи підприємств, плани розвитку, дослідження та інші відомості, які мають комерційну, наукову або організаційну цінність [5, с. 36].
4. Таємна інформація – відомості, що становлять інтерес для безпеки держави, її обороноздатності та міжнародних відносин. Доступ до такої інформації суворо регламентується законодавством і контролюється державними органами, а особи, які її обробляють, несуть підвищену відповідальність за її розголошення [5, с. 36].
5. Службова інформація – дані, що стосуються діяльності органів державної влади, місцевого самоврядування та управлінських структур, обмежені у доступі для сторонніх осіб, але можуть використовуватися працівниками для виконання службових обов'язків. До них належать службові листи, протоколи, внутрішні інструкції та плани діяльності організацій [5, с. 34].

Класифікація інформації дозволяє встановлювати чіткі межі доступу та використання відомостей, а також забезпечує належний правовий захист. Вона ґрунтується на принципі диференціації правового режиму залежно від значення інформації для суспільства, держави та конкретних суб'єктів.

Публічна інформація забезпечує відкритість та прозорість суспільного життя, стимулює розвиток науки, освіти та бізнесу, сприяє аналізу та оцінці діяльності державних органів. Інформація з обмеженим доступом регламентується для захисту інтересів держави та приватних суб'єктів.

Конфіденційна, таємна та службова інформація характеризується спеціальним режимом захисту та контролю, який реалізується через законодавчі, адміністративні та технічні механізми, а також систему санкцій за порушення правил доступу та обробки [8, с. 180].

Таким чином, класифікація інформації є не лише теоретичною категорією, а й важливим практичним інструментом для забезпечення ефективного функціонування системи інформаційного права, реалізації права громадян на інформацію та захисту інтересів держави та бізнесу. Вона формує основу для подальшого правового регулювання обігу даних у цифровому суспільстві, де швидкість доступу та обробки інформації має ключове значення.

3.2. Інформація з обмеженим доступом

Інформація з обмеженим доступом є однією з ключових категорій інформації в системі інформаційного права, оскільки вона поєднує принципи захисту державних та приватних інтересів із потребою суспільства у відкритості інформаційних ресурсів.

До цієї категорії належать:

1. Державна таємниця – це відомості, що мають стратегічне значення для оборони, національної безпеки, зовнішньої політики, економічної стабільності та інших ключових сфер діяльності держави. Розголошення такої інформації може завдати серйозної шкоди національним інтересам, підірвати безпеку держави та її міжнародний авторитет. Доступ до державної таємниці суворо регламентується законодавством і здійснюється лише за наявності спеціальних дозволів та допусків, а особи, що працюють із такою інформацією, несуть підвищену юридичну та адміністративну відповідальність [2, с. 191]. У сучасних умовах

державна таємниця включає також дані в цифрових базах та хмарних сервісах, що вимагає додаткових заходів кібербезпеки.

2. Комерційна таємниця – це інформація, яка має економічну цінність для підприємств та організацій і не є загальнодоступною. Вона включає фінансові звіти, плани розвитку, маркетингові стратегії, технологічні процеси та інші відомості, що забезпечують конкурентні переваги. Захист комерційної таємниці регламентується законами про охорону комерційної таємниці, договорними умовами та корпоративними політиками, що встановлюють обов'язки працівників щодо конфіденційності [8, с. 175]. Комерційна таємниця дозволяє підприємствам ефективно конкурувати на ринку та стимулює інновації, оскільки безпека інформації є ключовим активом бізнесу.
3. Персональні дані – відомості, що дозволяють ідентифікувати фізичну особу, включаючи ім'я, адресу, ідентифікаційні коди, фінансові та медичні дані. У цифрову епоху персональні дані обробляються у великих обсягах, що підвищує ризик їх неправомірного використання. Законодавство України та міжнародні стандарти визначають суворі вимоги до збору, зберігання, обробки та передачі персональних даних, включно з обов'язком отримання згоди особи та впровадженню технічних заходів безпеки [8, с. 115].

Правовий режим інформації з обмеженим доступом включає наступні основні механізми захисту:

1. Отримання дозволу на доступ – доступ до інформації здійснюється лише за наявності спеціального дозволу, службового повноваження або відповідної акредитації. Це забезпечує контроль над тим, хто може ознайомлюватися з чутливими даними та запобігає їх неправомірному використанню.
2. Дотримання умов конфіденційності – особи, які мають доступ до інформації з обмеженим доступом, зобов'язані дотримуватися правил збереження конфіденційності, не передавати дані третім особам без

дозволу та забезпечувати належне поводження з ресурсами. Порушення умов конфіденційності передбачає юридичну відповідальність, включно зі штрафами, дисциплінарними заходами та кримінальною відповідальністю [2, с. 192].

3. Використання технічних засобів захисту – до них належать шифрування, електронні цифрові підписи, системи контролю доступу, аудит дій користувачів та інші інформаційні технології, що забезпечують безпеку даних у процесі зберігання та обміну. Використання таких заходів є обов’язковим для державних установ, підприємств та організацій, що обробляють інформацію з обмеженим доступом.

Інформація з обмеженим доступом виконує важливу роль у забезпеченні балансу між відкритістю суспільної інформації та потребою захисту державних, комерційних та приватних інтересів. Вона сприяє стабільності функціонування державних органів, бізнесу, фінансових та соціальних систем, а також запобігає можливим ризикам витоку та неправомірного використання даних.

У сучасному цифровому середовищі інформація з обмеженим доступом все частіше обробляється за допомогою електронних платформ, хмарних сервісів та спеціалізованих програмних комплексів, що вимагає від законодавства та організацій постійного вдосконалення правил її захисту та контролю [8, с. 178].

Таким чином, інформація з обмеженим доступом є ключовим елементом системи інформаційного права, який забезпечує одночасно безпеку держави, конкурентоспроможність бізнесу та захист прав громадян у сфері обігу інформації.

3.3. Правовий режим інформації

Правовий режим інформації є ключовим елементом системи інформаційного права, оскільки він регламентує доступ до даних, їх

використання та забезпечення захисту. Він визначає, як саме інформація може циркулювати у суспільстві, які обмеження та гарантії передбачені для різних категорій даних і які правові механізми застосовуються для їх захисту.

Основні складові правового режиму інформації включають:

Порядок доступу – встановлює, хто, за яких умов і у якій формі може отримувати інформацію. Доступ до даних залежить від їхньої класифікації:

Відкритий доступ – публічна інформація, яка є доступною для всіх громадян, організацій та державних установ. Наприклад, статистичні дані державних органів, закони, нормативні акти та інформація про бюджет [1, с. 275].

Обмежений доступ – інформація, що має комерційну цінність, містить персональні дані або державну таємницю. Для її отримання потрібен спеціальний дозвіл або службові повноваження [2, с. 192; 8, с. 178].

Заборонений доступ – відомості, які за законом не можуть бути розголошені у відкритому доступі через загрозу національній безпеці, економічним чи соціальним інтересам [2, с. 191].

Способи використання – регулюють, у яких сферах і яким чином інформація може застосовуватися. Інформація використовується у наукових дослідженнях, освітній діяльності, управлінських процесах, комерційних операціях та інших сферах. Законодавство визначає обов'язкові правила обробки даних, включно з цифровими носіями, хмарними сервісами та платформами електронної комерції [6, с. 90; 19, с. 255]. При цьому особлива увага приділяється захисту персональних даних, охороні комерційної та державної таємниці та дотриманню авторських прав.

Захист інформації – передбачає систему заходів, спрямованих на охорону даних від несанкціонованого доступу, розголошення, втрати або знищення.

Система захисту включає:

Юридичні механізми – встановлення відповідальності за порушення правил доступу або розголошення інформації, застосування адміністративних, цивільних та кримінальних санкцій [8, с. 94].

Технічні засоби – шифрування даних, використання цифрових підписів, систем контролю доступу, аудит дій користувачів, резервне копіювання та заходи кібербезпеки [8, с. 95].

Організаційні заходи – впровадження внутрішніх політик, інструкцій та стандартів роботи з інформацією, навчання персоналу та перевірка дотримання правил [6, с. 92].

Основні принципи правового режиму інформації:

Відкритість – забезпечення громадянам, науковцям, бізнесу та державним органам доступу до публічної інформації, що сприяє прозорості діяльності органів влади та демократичному контролю [1, с. 276].

Доступність – створення умов для легкого та своєчасного отримання необхідних даних відповідно до законодавчих норм. Наприклад, державні електронні портали надають можливість завантаження нормативних актів, відкритих реєстрів та статистичних даних [19, с. 257].

Захищеність – охорона персональних даних, комерційної та державної таємниці, конфіденційної та службової інформації. Забезпечується поєднанням правових, технічних та організаційних заходів, що гарантують недоторканність ресурсів та запобігають їх неправомірному використанню [8, с. 95].

Правовий режим інформації реалізується через комплекс нормативних актів, процедур та стандартів, а також систему контролю за дотриманням встановлених правил. Він забезпечує баланс між конституційним правом громадян на доступ до інформації та необхідністю захисту даних, що становлять інтерес для держави, бізнесу та окремих осіб.

Сучасні виклики цифровізації суспільства, зокрема поширення електронної комерції, хмарних сервісів, обробки великих даних (Big Data) та

використання штучного інтелекту, потребують постійного вдосконалення правового режиму інформації. Це включає:

створення гнучких та адаптивних законодавчих норм, що відповідають новим технологічним умовам;

впровадження комплексних технічних рішень для захисту інформації;

вдосконалення процедур ліцензування та контролю доступу до чутливих даних [1, с. 278; 8, с. 98].

Таким чином, правовий режим інформації є багатошаровим механізмом, який забезпечує одночасно відкритість, доступність та захист інформаційних ресурсів, гарантує стабільність функціонування державних, комерційних та соціальних систем і є фундаментальним елементом сучасного інформаційного права.

Висновок

У результаті проведеного дослідження були розглянуті ключові аспекти поняття, класифікації, правової природи та режиму використання інформаційних ресурсів, що є об'єктом інформаційного права. Встановлено, що інформаційні ресурси виступають комплексною категорією, що поєднує соціальні, економічні та правові функції, визначаючи ефективність діяльності органів влади, бізнесу, науки та освіти.

Інформаційні ресурси є сукупністю даних, документів, матеріалів та цифрових об'єктів, що створюються, систематизуються та використовуються для задоволення інформаційних потреб різних суб'єктів. Вони включають як традиційні документи та бази даних, так і сучасні цифрові ресурси, хмарні сервіси та мультимедійні об'єкти [6, с. 40; 7, с. 53].

Правовий аналіз показав, що інформаційні ресурси мають багатовимірну природу, що включає:

Об'єктність, яка дозволяє законодавству встановлювати права власності, правила доступу та відповідальність за порушення.

Нематеріальність та формалізацію, що вимагає створення спеціальних носіїв та цифрових систем для їхнього функціонування.

Еволюційний характер, зумовлений розвитком цифрових технологій, штучного інтелекту та хмарних сервісів, що потребує постійного вдосконалення правового регулювання [8, с. 92; 7, с. 57].

Крім того, інформаційні ресурси виконують важливі соціальні функції: комунікативну, регулятивну, контролюючу та освітню, що підкреслює їхню правову та суспільну значущість. Взаємозв'язок із такими категоріями, як інформація, знання та документи, дозволяє розглядати інформаційні ресурси як ключовий елемент системи інформаційного права [9, с. 78; 10, с. 24].

Дослідження класифікації інформаційних ресурсів показало наявність кількох основних категорій:

Державні ресурси, що забезпечують прозорість та контроль діяльності органів влади.

Комерційні ресурси, що формують конкурентні переваги та економічну цінність для бізнесу.

Наукові та освітні ресурси, що сприяють розвитку науки, освіти та інновацій.

Соціальні ресурси, які включають персональні дані та інші чутливі відомості [5, с. 102; 8, с. 175].

Критеріями ефективного використання ресурсів є достовірність, повнота, структурованість та актуальність даних. Важливо відзначити, що цифрові технології значно розширюють функціональні можливості ресурсів, але одночасно створюють нові ризики, пов'язані з кібербезпекою та захистом персональних даних [16, с. 195].

Сучасне управління інформаційними ресурсами стикається з рядом проблем, серед яких:

Недосконалість законодавства щодо цифрових ресурсів та великих масивів даних (Big Data) [13, с. 139].

Кіберзагрози та ризики витоку інформації, що потребують застосування сучасних стандартів кібербезпеки [14, с. 157].

Відсутність єдиного підходу до оцінки ресурсів та стандартизації критеріїв достовірності та актуальності [15, с. 172].

Перспективи розвитку включають впровадження єдиних електронних реєстрів та порталів, інтеграцію аналітики великих даних та штучного інтелекту для обробки ресурсів, а також гармонізацію українського законодавства з європейськими стандартами щодо захисту інформації [19, с. 255].

Особлива увага приділяється правовому режиму інформації, що визначає порядок доступу, способи використання та механізми захисту. Встановлено, що режим інформації має базуватися на трьох ключових принципах: відкритість, доступність та захищеність [1, с. 275; 8, с. 94].

Інформація поділяється на категорії:

Публічна інформація, доступна всім громадянам.

Інформація з обмеженим доступом, що включає державну таємницю, комерційну таємницю та персональні дані [2, с. 190; 8, с. 115].

Конфіденційна та службова інформація, що охороняється за ініціативою власника або держави [5, с. 34].

Правовий режим реалізується через комбінацію нормативних актів, адміністративних процедур та технічних засобів контролю, що забезпечує баланс між правом громадян на інформацію та необхідністю захисту від неправомірного використання [8, с. 98].

Підсумовуючи результати дослідження, можна відзначити:

Інформаційні ресурси є багатовимірним явищем, що поєднує соціальну, економічну та правову функції.

Класифікація ресурсів дозволяє встановлювати диференційований режим доступу, забезпечуючи баланс між відкритістю та захищеністю.

Ефективне правове регулювання інформаційних ресурсів потребує постійного оновлення з урахуванням цифровізації, розвитку штучного інтелекту та хмарних технологій.

Проблеми правового регулювання включають недосконалість законодавства, кіберзагрози та відсутність єдиних стандартів оцінки ресурсів, що потребує комплексних законодавчих та технічних рішень.

Перспективи розвитку інформаційних ресурсів пов'язані з електронними реєстрами, цифровою аналітикою та гармонізацією законодавства України з міжнародними нормами.

Таким чином, результати дослідження підтверджують, що інформаційні ресурси є стратегічним інструментом розвитку суспільства, держави та бізнесу. Їх ефективне управління та захист вимагають комплексного підходу, що поєднує правові, технологічні та організаційні механізми. Правильне регулювання цих ресурсів забезпечує стабільність функціонування держави,

розвиток економіки та гарантування прав громадян у сфері доступу до інформації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Закон України «Про інформацію» від 02.10.1992 № 2657-XII. [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show>
2. Грунчак В. С., Інформаційне право України. – К., 2020. 348 с.
3. Іваненко М. П., Інформаційні ресурси та право. – К., 2019. 218с
4. Петренко С. І., Правове регулювання ресурсів. – Харків, 2021. 420 с.
5. Бойко Н. О., Цифрові інформаційні ресурси. – Л., 2022. 250 с.
6. Ковальчук О. М., Правовий режим даних. – К., 2020. 366 с.
7. Литвиненко І. Ю., Захист інформаційних ресурсів. – Одеса, 2019. 180 с.
8. Терещенко В. М., Персональні дані: право і захист. – Х., 2021. 259 с.
9. Мельник Д. І., Інформаційні системи і право. – Дн., 2019. 202 с.
10. Сидоренко П. І., Інформаційні ресурси: класифікація. – К., 2023. 400 с.
11. Бойчук А. В., Безпека цифрових ресурсів. – К., 2022. 199 с.
12. Романенко О. С., Інформаційне право: сучасний стан. – Л., 2020. 220 с.
13. Українська національна стратегія кібербезпеки. – К., 2021. 245 с.
14. Державна служба спеціального зв'язку та захисту інформації України. – Звіт 2024.
15. ISO/IEC стандарти щодо інформаційних ресурсів (переклади та адаптації).
16. Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>
17. Кримінальний кодекс України від 05.04.2001 № 2341-III. [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show>
18. Закон України «Про правовий режим воєнного стану» від 12.05.2015 № 389-VIII. [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show>

19. Наукові матеріали Всеукраїнської конференції з інформаційного права, 2023.
20. Арістова І. В. Інформаційне право: підручник. Київ: Юрінком Інтер, 2024. 352 с.