

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

КУРСОВА РОБОТА

з дисципліни: «ІНФОРМАЦІЙНЕ ПРАВО»
за темою: «**МЕЖІ ІНФОРМАЦІЙНИХ ПРАВ ЛЮДИНИ**»

Студента (ки): Гага Р.В.
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. ТЕОРЕТИКО-ПРАВОВІ ЗАСАДИ ІНФОРМАЦІЙНИХ ПРАВ ЛЮДИНИ	7
1.1. Поняття та класифікація інформаційних прав у сучасній юриспруденції	7
1.2. Правова природа та зміст права на інформацію	9
1.3. Співвідношення приватного та суспільного інтересу в інформаційній сфері	12
РОЗДІЛ 2. ПРАВОВЕ РЕГУЛЮВАННЯ МЕЖ ІНФОРМАЦІЙНИХ ПРАВ	15
2.1. Конституційні та міжнародні стандарти обмеження інформаційних прав	15
2.2. Захист персональних даних як межа доступу до інформації	17
2.3. Інститут державної та іншої таємниці в системі інформаційних обмежень	19
РОЗДІЛ 3. ПРАКТИЧНІ АСПЕКТИ ТА ПРОБЛЕМИ РЕАЛІЗАЦІЇ МЕЖ ІНФОРМАЦІЙНИХ ПРАВ В УКРАЇНІ	23
3.1. Баланс між свободою слова та національною безпекою в умовах воєнного стану	23
3.2. Судовий захист інформаційних прав та практика ЄСПЛ	25
3.3. Шляхи вдосконалення законодавства щодо визначення меж інформаційних прав	27
ВИСНОВКИ	30
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	33

ВСТУП

Актуальність теми. Трансформація сучасного суспільства в інформаційне зумовила докорінну зміну парадигми правового регулювання. Інформація перетворилася з допоміжного інструменту на стратегічний ресурс, а інформаційні права людини стали фундаментом демократичного устрою. Проте, як свідчить юридична практика та світовий досвід, жодне право, за винятком права на життя та свободу від катувань, не може бути абсолютним. Питання визначення меж інформаційних прав людини є однією з найскладніших дилем сучасного права.

Актуальність даного дослідження зумовлена декількома критичними чинниками. По-перше, розвиток цифрових технологій та штучного інтелекту створив нові виклики для приватності особи. Межа між правом суспільства знати та правом індивіда на «цифрову тишу» стає дедалі прозорішою. По-друге, в умовах повномасштабної збройної агресії проти України, національна безпека вимагає суттєвого звуження інформаційних свобод. Пошук балансу між «безпекою» та «свободою» в інформаційній сфері є питанням не лише юридичним, а й екзистенційним для української державності.

Незважаючи на наявність значної кількості наукових праць, присвячених інформаційному праву, комплексне дослідження саме *меж* цих прав, їхньої класифікації та механізмів обмеження в умовах надзвичайних правових режимів залишається недостатньо розробленим. Це підкреслює необхідність теоретичного переосмислення існуючих підходів та розробки нових законодавчих пропозицій.

Стан наукової розробки теми. Проблема інформаційних прав та їх обмежень перебуває у центрі уваги багатьох вітчизняних та зарубіжних правників. Теоретичний фундамент дослідження заклали праці таких вчених, як І. В. Арістова, В. Г. Брижко, Б. О. Кормич, А. І. Марущак, О. В. Соснін, В. М. Фурашев. Питання свободи слова та її меж ґрунтовно аналізувалися у роботах О. В. Кузнецової та М. Я. Швеця. Міжнародно-правовий аспект

обмежень інформаційних прав через призму практики ЄСПЛ досліджували О. А. Гавриленко та Є. В. Петров.

Водночас динамічність інформаційних відносин вимагає постійного оновлення наукових поглядів. Зокрема, потребують додаткового вивчення питання обмеження прав у кіберпросторі та специфіка реалізації інформаційних свобод в умовах воєнного стану, що і зумовило вибір теми даної курсової роботи.

Мета дослідження полягає у проведенні всебічного теоретико-правового аналізу змісту, природи та меж інформаційних прав людини, виявленні критеріїв їх легітимного обмеження в демократичному суспільстві та розробці практичних рекомендацій щодо вдосконалення українського законодавства у цій сфері.

Для досягнення поставленої мети визначено наступні **завдання**:

Дослідити генезис та еволюцію поняття «інформаційні права» у сучасній юриспруденції.

Здійснити класифікацію інформаційних прав за різними критеріями для визначення режимів їх обмеження.

Проаналізувати правову природу права на інформацію як об'єкта конституційно-правового регулювання.

Визначити критерії балансу між приватним інтересом (приватністю) та суспільною необхідністю.

Розкрити зміст «трискладового тесту» як універсального стандарту обмеження прав людини.

Дослідити інститути державної та персональної таємниці як нормативні межі інформаційної свободи.

Оцінити вплив правового режиму воєнного стану на обсяг та межі інформаційних прав в Україні.

Вивчити практику ЄСПЛ та вітчизняних судів у сфері захисту інформаційних прав.

Сформулювати пропозиції щодо цифровізації доступу до інформації та посилення відповідальності за порушення меж інформаційних прав.

Об’єктом дослідження є суспільні відносини, що виникають у процесі реалізації людиною своїх інформаційних прав, а також відносини, пов’язані з встановленням та застосуванням правових обмежень у цій сфері.

Предметом дослідження є сукупність правових норм національного та міжнародного законодавства, теоретичні концепції, судова практика та правозастосовні механізми, що визначають межі інформаційних прав людини.

Методи дослідження. Методологічну основу роботи становить діалектичний метод пізнання соціально-правових явищ, що дозволив розглянути інформаційні права у їх постійному розвитку та взаємозв’язку з технологічним прогресом. Окрім загальнонаукових методів, у роботі використано спеціальні юридичні методи:

Системно-структурний метод – використано для побудови класифікації інформаційних прав та аналізу структури «трискладового тесту».

Порівняльно-правовий метод – дозволив порівняти національні стандарти обмеження прав із міжнародними стандартами (Конвенція про захист прав людини) та практикою зарубіжних країн.

Формально-юридичний метод – застосовано при аналізі змісту статей Конституції України, Законів «Про інформацію», «Про доступ до публічної інформації» та інших нормативних актів.

Метод правового моделювання – використано для розробки пропозицій щодо вдосконалення законодавства у сфері цифровізації доступу до даних.

Джерельна база дослідження. Робота ґрунтується на широкому колі джерел, які можна поділити на три групи:

Нормативно-правові акти: Конституція України, міжнародні договори (ратифіковані Україною), кодекси та закони України, що регулюють інформаційну сферу.

Акти судових органів: Рішення Конституційного Суду України, постанови Верховного Суду та прецедентна практика Європейського суду з прав людини, яка є ключовою для розуміння меж обмежень.

Спеціальна література: Монографії, підручники, наукові статті провідних фахівців у галузі інформаційного права (І. В. Арістової, Б. О. Кормича та ін.).

Наукова новизна одержаних результатів полягає у спробі системного поєднання теоретичних стандартів «трискладового тесту» з практичними викликами воєнного стану, що дозволило по-новому поглянути на межі інформаційних прав як на гнучкий інструмент захисту національної безпеки без втрати демократичних цінностей.

Структура курсової роботи визначена її метою та завданнями. Робота складається зі змісту, вступу, трьох розділів (що містять дев'ять підрозділів), висновків та списку використаних джерел.

РОЗДІЛ 1. ТЕОРЕТИКО-ПРАВОВІ ЗАСАДИ ІНФОРМАЦІЙНИХ ПРАВ ЛЮДИНИ

1.1. Поняття та класифікація інформаційних прав у сучасній юриспруденції

У сучасній юридичній науці інформаційні права людини розглядаються як фундаментальний елемент правового статусу особи в умовах глобального інформаційного суспільства. Трансформація правової доктрини призвела до того, що інформаційні права перестали сприйматися лише як похідні від свободи слова, виокремившись у самостійний інститут інформаційного права.

Поняття інформаційних прав слід трактувати як систему юридично закріплених можливостей фізичної особи, що забезпечують її потреби у створенні, збиранні, одержанні, використанні, поширенні, зберіганні та захисті інформації. Згідно з науковими підходами, інформаційні права людини – це сукупність правових можливостей особи щодо пошуку, отримання, використання, поширення та зберігання інформації [3, с. 45]. Це визначення підкреслює багатогранність інформаційної діяльності, яка охоплює всі етапи життєвого циклу інформації.

Правова природа цих прав є комплексною. З одного боку, вони мають ознаки особистих немайнових прав (наприклад, право на таємницю приватного життя), а з іншого – виступають інструментом реалізації політичних та соціальних прав (право на доступ до публічної інформації для контролю за діяльністю влади). Важливо розуміти, що інформаційні права є динамічними: вони еволюціонують разом із розвитком інформаційно-комунікаційних технологій [12, с. 89].

Для глибокого аналізу теми необхідно розглянути класифікацію інформаційних прав. Науковці виділяють загальні (право на інформацію) та спеціальні права (право на доступ до публічної інформації, право на захист персональних даних) [3, с. 45]. Така диференціація є принциповою для

юридичної практики, оскільки загальні права встановлюють універсальний стандарт свободи, тоді як спеціальні права визначають конкретні процедури та межі їх реалізації у специфічних правовідносинах.

Класифікація за змістом повноважень включає:

Право на пошук інформації – можливість особи активно шукати відомості у відкритих джерелах, архівах, мережі Інтернет.

Право на отримання інформації – кореспондує обов'язку держави або інших суб'єктів надати відповідну інформацію за запитом [16].

Право на використання та поширення – свобода оперувати отриманими даними, висловлювати власні думки та ідеї [19, с. 48].

Окремої уваги заслуговує класифікація за об'єктом правовідносин. У цьому контексті право на доступ до публічної інформації розглядається як гарантія прозорості державного апарату [16]. Водночас право на захист персональних даних виступає як захисний бар'єр, що обмежує доступ сторонніх осіб до приватної сфери індивіда [5]. Саме класифікація дозволяє чітко розмежувати сфери, де втручання держави є мінімальним, і сфери, де регулювання є необхідним для захисту публічного інтересу [12, с. 88].

У доктрині інформаційного права також виділяють права «першого», «другого» та «третього» поколінь. Якщо перше покоління стосувалося класичної свободи друку, то сучасне покоління прав включає право на «цифрову присутність», право на «забуття» (right to be forgotten) та право на кібербезпеку [13, с. 42; 20, с. 115].

Розглядаючи суб'єктивний склад, слід зазначити, що носієм інформаційних прав є кожна людина від народження. Однак реалізація цих прав часто залежить від правового статусу особи (наприклад, журналісти мають розширені права щодо доступу до інформації, тоді як державні службовці мають додаткові обмеження щодо розголошення службових відомостей) [15, с. 102].

Фундаментальне значення для розуміння меж інформаційних прав має їх поділ на **абсолютні та відносні**. Більшість інформаційних прав є

відносними, тобто такими, що можуть бути обмежені законом в інтересах національної безпеки, територіальної цілісності або громадського порядку. Проте право мати власну думку та право на захист від маніпулятивного впливу на свідомість часто розглядаються як такі, що тяжіють до абсолютних у контексті людської гідності [9, с. 124].

Юридичне закріплення цієї класифікації у національному законодавстві (Конституція України, Закони «Про інформацію», «Про доступ до публічної інформації») створює ієрархічну систему, де загальне право на інформацію є фундаментом, а галузеві норми деталізують механізми захисту та відповідальності [2; 16].

Таким чином, поняття та класифікація інформаційних прав у сучасній юриспруденції відображають складну структуру взаємодії людини та інформаційного середовища. Чітке визначення виду права (загальне чи спеціальне) дозволяє коректно застосовувати юридичні інструменти для його захисту та визначати легітимні межі втручання держави у цю сферу [3, с. 47; 12, с. 90].

1.2. Правова природа та зміст права на інформацію

Правова природа права на інформацію є однією з найскладніших категорій у сучасному інформаційному праві, оскільки вона поєднує в собі ознаки природного права людини, конституційної гарантії та фундаментального елемента демократичного устрою. Глибоке розуміння цього інституту вимагає аналізу його внутрішньої структури, суб'єктивного та об'єктивного аспектів, а також визначення ролі держави у забезпеченні цієї свободи.

Згідно зі ст. 34 Конституції України, кожен має право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб – на свій вибір [1]. Це конституційне положення кореспондує з

міжнародними актами, зокрема зі ст. 19 Загальної декларації прав людини та ст. 10 Конвенції про захист прав людини і основоположних свобод, що підкреслює універсальний характер цього права [4; 8, с. 142].

Правова природа права на інформацію характеризується декількома ключовими аспектами:

Суб'єктивний аспект: Це можливість особи діяти певним чином (збирати, поширювати інформацію) та вимагати відповідної поведінки від інших суб'єктів, насамперед від держави.

Об'єктивний аспект: Це система правових норм, які регулюють інформаційні відносини, створюючи правовий порядок, у якому інформація є доступною та захищеною [3, с. 62].

Статус «негативного» та «позитивного» права: Як «негативне» право, воно вимагає від держави утримуватися від втручання у вільний обмін думками. Як «позитивне» право, воно зобов'язує державу створювати механізми для реального доступу громадян до суспільно важливих відомостей [13, с. 74].

Зміст права на інформацію розкривається через систему правомочностей, закріплених у національному законодавстві. Зміст цього права включає як активні дії особи, так і обов'язок держави не чинити перешкод у реалізації цієї свободи, за винятком випадків, передбачених законом [7, с. 112; 19, с. 54].

Розглянемо ці правомочності детальніше:

Право на збирання інформації: Передбачає можливість пошуку та накопичення даних з будь-яких відкритих джерел. Важливою умовою є законність засобів збирання. Особа має право використовувати технічні засоби (диктофони, камери), якщо це не порушує права інших осіб [2; 15, с. 118].

Право на зберігання: Гарантує особі можливість володіти інформацією на будь-яких носіях (паперових, електронних). Держава не може вилучати інформацію у власника, крім випадків, санкціонованих судом у межах кримінального провадження [9, с. 156].

Право на використання: Означає можливість застосовувати інформацію для здійснення професійної, наукової, творчої або побутової діяльності. Використання інформації є основою для реалізації інших прав, наприклад, права на освіту чи підприємницьку діяльність [12, с. 105].

Право на поширення: Це свобода передавати інформацію невизначеному колу осіб. Саме в цій правомочності найчастіше виникають конфлікти з інтересами держави або приватних осіб, що обумовлює необхідність встановлення чітких меж [20, с. 148].

Важливим елементом правової природи є принцип достовірності інформації. Хоча кожен має право на свободу думки, право на інформацію у вузькому розумінні (як на дані) передбачає право особи на отримання саме правдивих відомостей [3, с. 65]. Це особливо актуально у сфері публічного управління, де спотворення інформації органами влади веде до порушення конституційного ладу [16].

Особливе місце у змісті права на інформацію посідає право на доступ до інформації про себе. Кожна особа має право знати, які відомості про неї зібрані в державних реєстрах, вимагати їх виправлення або видалення у разі недостовірності [5; 18, с. 64]. Це право є ключовим інструментом захисту людської гідності та приватності.

Слід також зазначити, що зміст права на інформацію постійно розширюється під впливом практики Європейського суду з прав людини (ЄСПЛ). Суд наголошує, що доступ до інформації є необхідним для функціонування преси як «суспільного вартвого» (public watchdog) [17, с. 92]. Таким чином, правова природа права на інформацію трансформується від простого «права бути залишеним у спокої» до активного права на участь у суспільному житті через інформаційну взаємодію.

Держава, зі свого боку, забезпечує зміст цього права через:

Створення відкритих державних реєстрів.

Встановлення відповідальності за безпідставну відмову у наданні інформації.

Підтримку незалежності засобів масової інформації [7, с. 115; 13, с. 78].

Отже, правова природа права на інформацію полягає у його двоїстості: воно є і метою (задоволення потреб особи), і засобом (інструментом контролю за владою). Його зміст охоплює широкий спектр можливостей – від пасивного отримання до активного поширення, що створює фундамент для розвитку відкритого та прозорого суспільства [19, с. 56].

1.3. Співвідношення приватного та суспільного інтересу в інформаційній сфері

Взаємодія приватного та суспільного інтересів в інформаційній сфері становить одну з найбільш динамічних та складних ділянок сучасного правознавства. Центральною проблемою інформаційного права є колізія між правом особи на приватність та правом суспільства знати соціально значущу інформацію [14, с. 210]. Вирішення цієї колізії вимагає від держави та суду ювелірної точності у визначенні того, де закінчується сфера особистої свободи і починається законний інтерес громади.

Приватний інтерес в інформаційній сфері базується на праві особи на невтручання в її особисте та сімейне життя (ст. 32 Конституції України). Він охоплює право на таємницю листування, телефонних розмов, захист персональних даних та право самостійно визначати, які відомості про себе робити надбанням громадськості [1; 5]. Будь-яке розголошення конфіденційної інформації про особу без її згоди розцінюється як порушення цього інтересу, якщо воно не виправдане вагомими причинами [18, с. 72].

Суспільний (публічний) інтерес, з іншого боку, полягає у праві громадян бути поінформованими про питання, що мають вагоме значення для життя громади чи держави. Це включає інформацію про:

Стан довкілля та якість харчових продуктів.

Використання бюджетних коштів та управління державним майном [16].

Діяльність публічних осіб (політиків, державних службовців), яка впливає на суспільство.

Факти корупції, порушення прав людини або загрози громадській безпеці [13, с. 94].

Межа між цими інтересами проходить через поняття «суспільної необхідності», яке виправдовує розголошення певних відомостей про особу, якщо вони стосуються публічної діяльності або загрози правам інших [14, с. 210]. В юридичній практиці для встановлення цієї межі використовується балансувальний тест, де на одну чашу терезів ставиться право особи на приватність, а на іншу – право суспільства на інформацію.

Особливе значення має статус особи, про яку поширюється інформація. Юриспруденція Європейського суду з прав людини (ЄСПЛ) чітко вказує, що межі критики щодо публічних осіб (політиків) є значно ширшими, ніж щодо пересічних громадян [8, с. 175; 17, с. 104]. Суспільство має право знати про статки, стан здоров'я чи поведінку політика, якщо це може вплинути на виконання ним державних функцій. У таких випадках приватний інтерес особи поступається праву суспільства на контроль за владою [15, с. 140].

Проте «суспільний інтерес» не можна ототожнювати з «цікавістю публіки». Бажання аудиторії знати пікантні подробиці особистого життя відомих людей лише задля розваги не є законним суспільним інтересом [14, с. 215]. Право на повагу до приватного життя захищає особу від необґрунтованого медійного втручання, яке не несе соціальної цінності.

Важливим аспектом співвідношення інтересів є режим доступу до інформації. За загальним правилом, інформація про діяльність державних органів є відкритою (суспільний інтерес домінує), тоді як інформація про приватне життя – закритою (приватний інтерес домінує) [12, с. 118]. Проте існують винятки: наприклад, персональні дані особи, яка претендує на зайняття посади з високим корупційним ризиком, стають частково відкритими для суспільства [16; 20, с. 201].

В умовах цифрового суспільства цей баланс зміщується. Розвиток соціальних мереж та великих даних (Big Data) створює ситуації, коли приватна інформація мільйонів людей стає ресурсом для формування суспільної думки чи комерційного використання. Тут роль держави як регулятора стає визначальною – вона повинна забезпечити захист приватності (приватний інтерес) через жорстке регулювання обробки даних, водночас не перешкоджаючи вільному потоку ідей та інформації (суспільний інтерес) [9, с. 230; 19, с. 92].

Отже, співвідношення приватного та суспільного інтересу не є сталою величиною. Це постійний процес пошуку компромісу, де пріоритет надається тій цінності, яка в конкретній ситуації має більшу соціальну вагу для демократичного розвитку суспільства. Встановлення межі між ними є гарантією захисту від авторитаризму (через надмірну таємність) та від тиранії більшості (через повне знищення приватності) [3, с. 88; 13, с. 102].

РОЗДІЛ 2. ПРАВОВЕ РЕГУЛЮВАННЯ МЕЖ ІНФОРМАЦІЙНИХ ПРАВ

2.1. Конституційні та міжнародні стандарти обмеження інформаційних прав

Дослідження меж інформаційних прав неможливе без аналізу системи стандартів, які визначають допустимість втручання держави у сферу інформаційної свободи особи. У правовій державі будь-яке обмеження прав не може бути свавільним; воно має ґрунтуватися на чітких критеріях, визнаних як національним конституційним правом, так і міжнародним співтовариством.

Основним інструментом перевірки правомірності обмежень у європейській правовій традиції є так званий «трискладовий тест». Згідно з цим стандартом, обмеження прав має відповідати трьом кумулятивним умовам: бути встановленим законом, переслідувати легітимну мету та бути необхідним у демократичному суспільстві [2, с. 14; 20, с. 301]. Цей підхід забезпечує передбачуваність правового регулювання та захищає особу від зловживань з боку владних інституцій.

Перша складова тесту – «встановленість законом» – означає, що підстави та порядок обмеження права на інформацію повинні бути чітко прописані у нормативно-правових актах, які є доступними для громадян та сформульовані з достатньою точністю. В Україні ці норми закріплені насамперед у ст. 34 та ст. 32 Конституції, а також у профільних законах «Про інформацію» та «Про доступ до публічної інформації» [1; 2; 16].

Друга складова – «легітимна мета». Обмеження інформаційних прав не може бути самоціллю.

Воно допускається виключно в інтересах:

- національної безпеки та територіальної цілісності;
- запобігання заворушенням чи злочинам;
- охорони здоров'я населення;

- захисту репутації або прав інших осіб;
- запобігання розголошенню інформації, одержаної конфіденційно, або підтримання авторитету і безсторонності правосуддя [4; 7, с. 128].

Третя, найбільш складна складова – «необхідність у демократичному суспільстві». Це означає, що обмеження має відповідати нагальній суспільній потребі та бути пропорційним переслідуваній меті. Держава повинна довести, що шкода від оприлюднення інформації переважає над суспільним інтересом в її отриманні [14, с. 218; 17, с. 110].

Ці стандарти повністю узгоджуються зі ст. 10 Конвенції про захист прав людини і основоположних свобод, яка гарантує свободу вираження поглядів, але водночас вказує на можливість встановлення формальностей, умов та обмежень, передбачених законом [4]. Практика Європейського суду з прав людини (ЄСПЛ) свідчить, що будь-яке звуження інформаційних прав підлягає суворому судовому контролю. Суд наголошує, що свобода слова є однією з головних опор демократичного суспільства, тому межі її обмеження мають тлумачитися вузько [8, с. 192].

Важливою частиною міжнародних стандартів є принцип недискримінації. Обмеження інформаційних прав не можуть застосовуватися за ознаками політичних переконань, релігії чи соціального статусу. Більше того, обмеження мають бути тимчасовими та підлягати регулярному перегляду, особливо якщо вони стосуються режиму доступу до публічної інформації [13, с. 115; 16].

На національному рівні Конституційний Суд України неодноразово підкреслював, що обмеження конституційних прав і свобод є допустимим лише за умови, що воно не порушує саму сутність цих прав. Втручання держави в інформаційну сферу має бути мінімально необхідним для досягнення легітимної мети [11, с. 145].

У контексті глобалізації та цифровізації міжнародні стандарти доповнюються нормами, що стосуються Інтернету та кіберпростору. Міжнародні організації (ООН, Рада Європи) наголошують, що ті самі права,

які люди мають офлайн, повинні бути захищені й онлайн. Це стосується і стандартів обмеження: блокування веб-ресурсів чи видалення контенту має відбуватися за тією ж логікою «трискладового тесту» [9, с. 260; 12, с. 154].

Отже, конституційні та міжнародні стандарти створюють надійний правовий каркас, який не дозволяє державі виходити за межі розумного при регулюванні інформаційних потоків. Вони слугують гарантією того, що межі інформаційних прав будуть використовуватися для захисту суспільства, а не для придушення критики чи приховання протиправних дій влади [20, с. 305].

2.2. Захист персональних даних як межа доступу до інформації

У системі інформаційних правовідносин захист персональних даних виступає одним із найпотужніших правових фільтрів, що обмежують загальне право на доступ до інформації. Персональні дані є об'єктом з обмеженим доступом, і саме через цей інститут реалізується конституційна гарантія невтручання в особисте життя. Можна стверджувати, що межа реалізації права на інформацію закінчується там, де починається право на недоторканність приватного життя [5; 18, с. 92].

Юридична природа персональних даних як межі доступу полягає в тому, що вони не є «нічийною» інформацією. Це відомості про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована. Закон України «Про захист персональних даних» чітко регламентує, що обробка таких даних без згоди особи заборонена, крім інтересів національної безпеки, економічного добробуту та прав людини [5]. Таким чином, законодавство встановлює презумпцію конфіденційності особистої інформації.

Для практичного застосування цієї межі важливо розрізняти два види персональних даних:

Загальні: прізвище, ім'я, по батькові, дата і місце народження, місце проживання тощо.

Вразливі (чутливі): дані про стан здоров'я, політичні, релігійні переконання, етнічне походження, біометричні дані. Доступ до таких даних обмежений максимально суворо [12, с. 182; 18, с. 95].

Конфлікт права на інформацію та права на приватність найчіткіше проявляється при запитах на публічну інформацію. Згідно із законом, розпорядники інформації зобов'язані надавати відповіді на запити, але вони мають право (і обов'язок) ретушувати або вилучати персональні дані з документів, якщо їх оприлюднення може завдати шкоди особі. Проте ця межа не є абсолютною. Закон «Про доступ до публічної інформації» встановлює, що не може бути обмежений доступ до персональних даних осіб, які займають посади, пов'язані з виконанням функцій держави або місцевого самоврядування, якщо це стосується їхньої професійної діяльності [16; 20, с. 310].

Важливим механізмом визначення цієї межі є тест на пропорційність. При вирішенні питання про надання доступу до персональних даних без згоди особи, володілець даних або суд мають з'ясувати:

Чи є втручання законним?

Чи переважає суспільний інтерес у знанні цих даних приватний інтерес особи у їх захисті?

Чи не буде шкода від розголошення надмірною порівняно з користю для суспільства? [9, с. 245; 17, с. 122].

У цифрову епоху захист персональних даних як межа доступу до інформації набуває нових рис. Поняття «право на забуття» (right to be forgotten) дозволяє особі вимагати видалення своїх даних із результатів пошукових систем, якщо вони застаріли або втратили актуальність. Це створює нову межу для історичного та журналістського дослідження, де право на приватність знову вступає у суперечку з правом суспільства на доступ до повної картини подій [13, с. 160; 19, с. 114].

Окремим аспектом є відповідальність за порушення меж. Незаконне збирання, зберігання або поширення персональних даних тягне за собою

адміністративну та кримінальну відповідальність. Це підкреслює статус персональних даних як «забороненої зони» для тих, хто намагається реалізувати своє право на інформацію у незаконний спосіб [3, с. 210].

Слід також враховувати міжнародний досвід, зокрема Загальний регламент про захист даних (GDPR), який встановлює високі стандарти приватності. Україна, на шляху до євроінтеграції, адаптує ці норми, що робить межу захисту персональних даних ще більш вираженою та захищеною від свавілля держави [12, с. 185].

Отже, захист персональних даних є необхідним обмежувачем, який запобігає перетворенню «інформаційного суспільства» на «суспільство загального нагляду». Ця межа забезпечує збереження автономії особистості, водночас залишаючи можливість для оприлюднення даних, якщо це критично важливо для демократичного контролю за владою та безпеки держави [18, с. 98].

2.3. Інститут державної та іншої таємниці в системі інформаційних обмежень

У системі правових обмежень інформаційних прав інститут таємниці посідає особливе місце, виступаючи найбільш радикальним інструментом звуження доступу до відомостей. Державна таємниця є найбільш жорсткою межею інформаційних прав. Вона обмежує доступ до відомостей у сферах оборони, економіки та зовнішніх відносин, розголошення яких може завдати шкоди державі [6]. У цьому контексті індивідуальне право на інформацію поступається колективній безпеці та інтересам збереження суверенітету [11, с. 134].

Правова природа державної таємниці базується на необхідності захисту життєво важливих інтересів суспільства. Згідно із Законом України «Про державну таємницю», це вид інформації, що охоплює відомості у сфері

оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України [6]. Держава, встановлюючи такий режим, фактично вилучає певний масив даних із загального інформаційного обігу, створюючи особливий правовий режим їх зберігання та використання.

Класифікація таємниць у системі інформаційних обмежень включає:

Державна таємниця (найвищий рівень захисту).

Службова інформація (відомості, що не становлять державної таємниці, але потребують захисту для забезпечення діяльності державних органів) [16].

Професійна таємниця (адвокатська, лікарська, банківська, таємниця сповіді тощо), де обмеження доступу спрямоване на захист прав клієнта або пацієнта [13, с. 128].

Комерційна таємниця, що захищає економічні інтереси суб'єктів господарювання [12, с. 210].

Процес встановлення межі через державну таємницю здійснюється шляхом засекречування. Важливо підкреслити, що інформація не стає таємною автоматично. Для цього вона має бути включена до Зводу відомостей, що становлять державну таємницю, на підставі рішень державних експертів з питань таємниць [6; 11, с. 138]. Це запобігає волюнтаристському обмеженню прав громадян на отримання інформації про діяльність влади.

Одним із найскладніших питань є визначення ступеня секретності («особливої важливості», «цілком таємно», «таємно»). Кожен ступінь відображає масштаб потенційної шкоди: від шкоди інтересам окремого відомства до загрози існуванню держави в цілому [20, с. 320]. Проте правова доктрина наголошує, що режим таємності не може бути вічним. Закон встановлює чіткі терміни дії грифів обмеження доступу, після закінчення яких інформація має бути розсекречена, якщо вона втратила свою актуальність для безпеки [6; 7, с. 145].

Критично важливою межею самого інституту таємниці є заборона засекречування певної інформації. Держава не має права приховувати під грифом «таємно» відомості про:

- стан довкілля, якість харчових продуктів і предметів побуту;
- аварії, катастрофи, небезпечні природні явища;
- стан здоров'я населення;
- факти порушення прав і свобод людини і громадянина;
- незаконні дії органів державної влади та посадових осіб [2; 16].

Така «межа на межу» є гарантією того, що інститут державної таємниці не перетвориться на інструмент приховування корупції або злочинів проти людяності. Як зазначають дослідники, право на інформацію у цих сферах є абсолютним і не може бути обмежене жодними інтересами безпеки [15, с. 182; 19, с. 124].

В умовах інформаційних війн та гібридних загроз роль державної таємниці трансформується. Виникає концепція «стратегічної комунікації», де держава змушена балансувати між необхідністю приховувати військові плани та обов'язком інформувати суспільство для підтримання довіри та протидії дезінформації [10, с. 164]. Тут межа стає рухомою і залежить від конкретної фази воєнного або надзвичайного стану.

Окремо слід розглянути службову інформацію як «м'яку» межу. Вона не містить державних секретів, але її передчасне розголошення може зашкодити прийняттю управлінських рішень. Проте, на відміну від державної таємниці, доступ до службової інформації обмежується лише після проходження «трискладового тесту», що робить цю межу менш жорсткою та більш підзвітною суспільному контролю [16; 17, с. 130].

Отже, інститут державної та іншої таємниці є легітимним і необхідним обмежувачем інформаційних прав у будь-якій державі. Проте його застосування має бути суворо обмежене законом, контролюватися судовою гілкою влади та базуватися на принципі пропорційності. Тільки за таких умов

обмеження доступу до інформації буде слугувати захисту держави, а не обмеженню свободи її громадян [11, с. 142; 20, с. 325].

РОЗДІЛ 3. ПРАКТИЧНІ АСПЕКТИ ТА ПРОБЛЕМИ РЕАЛІЗАЦІЇ МЕЖ ІНФОРМАЦІЙНИХ ПРАВ В УКРАЇНІ

3.1. Баланс між свободою слова та національною безпекою в умовах воєнного стану

В умовах повномасштабної збройної агресії проти України питання меж інформаційних прав трансформувалося з теоретичної площини у площину фізичного виживання нації. Правовий режим воєнного стану, введений відповідно до Закону України «Про правовий режим воєнного стану», передбачає можливість тимчасового обмеження конституційних прав і свобод людини, зокрема тих, що гарантовані статтями 32 та 34 Конституції України [1]. У цей період межі інформаційних прав суттєво звужуються, а пріоритет національної безпеки стає домінуючим чинником правового регулювання.

Правові підстави обмеження свободи слова під час війни базуються на статті 64 Конституції, яка дозволяє окремі обмеження прав із зазначенням строку їх дії. Вводяться специфічні заборони на поширення інформації про пересування ЗСУ, роботу ППО, місця влучань ракет та результати обстрілів. Такі обмеження є повністю виправданими з точки зору збереження життя громадян та забезпечення обороноздатності держави [10, с. 156; 15, с. 44].

Ключовим інструментом встановлення цих меж є Наказ Головнокомандувача ЗСУ № 73, який чітко регламентує перелік інформації, розголошення якої може допомогти ворогові. До такої інформації належать:

Найменування частин, підрозділів та їх чисельність.

Точне розташування позицій, складів боєприпасів та паливно-мастильних матеріалів.

Деталізовані дані про роботу систем протиповітряної оборони.

Прогнози та плани військових операцій [10, с. 160].

Концепція «інформаційної гігієни» як правового обов'язку. В умовах війни межа між «свободою вираження поглядів» та «державною зрадою» або

«перешкоджанням діяльності ЗСУ» стає дуже тонкою. Поширення фото- та відеоматеріалів з місця подій у реальному часі (так званий «хайп») перестає бути реалізацією права на інформацію і стає правопорушенням. Кримінальний кодекс України було доповнено статтею 114-2, яка встановлює сувору відповідальність за несанкціоноване поширення інформації про переміщення зброї та військ [15, с. 48]. Це є прикладом того, як держава вимушено розширює межі кримінально-правового регулювання інформаційної сфери для захисту суверенітету.

Проте, навіть під час війни, баланс не означає повне скасування свободи слова. Міжнародні стандарти, зокрема практика ЄСПЛ, наголошують, що навіть у надзвичайних ситуаціях обмеження мають бути:

Пропорційними: заборона має стосуватися лише тієї інформації, яка дійсно шкодить безпеці.

Тимчасовими: після зникнення загрози доступ має бути відновлений.

Обґрунтованими: держава повинна пояснювати необхідність закриття певної інформації [4; 8, с. 205].

Важливим аспектом є робота медіа. Військова цензура в класичному розумінні в Україні офіційно не введена, проте діє система акредитації журналістів та добровільні обмеження (самоцензура), засновані на принципі «не нашкодь». Це демонструє перехід від формально-юридичних меж до етико-правових, де журналістська спільнота сама визначає межі допустимого оприлюднення даних в інтересах перемоги [13, с. 180; 20, с. 330].

Окремою проблемою є протидія дезінформації та ІПСО (інформаційно-психологічним операціям). Держава має право обмежувати поширення фейків, які сіють паніку або підривають мобілізаційну готовність. Тут межею права на поширення інформації стає вимога її достовірності та безпечності для суспільного порядку. Боротьба з ворожою пропагандою виправдовує блокування певних медіаресурсів та платформ, що є законним в межах захисту національного інформаційного простору [10, с. 172].

Доступ до публічної інформації під час війни також зазнав змін. Багато державних реєстрів було закрито або обмежено в доступі для запобігання використанню даних ворогом (наприклад, кадастрові карти чи реєстри стратегічних підприємств). Це є прикладом «превентивної межі», коли право на інформацію обмежується не через факт порушення, а через високу ймовірність нанесення шкоди у разі відкритості даних [16; 17, с. 145].

Підсумовуючи, можна констатувати, що воєнний стан створює особливу архітектуру інформаційних прав, де безпека стає фундаментом, а свобода слова – надбудовою, обсяг якої регулюється військовою необхідністю. Головним завданням правової системи залишається недопущення перетворення тимчасових обмежень на постійну практику придушення громадянських свобод після завершення бойових дій [15, с. 52; 19, с. 140].

3.2. Судовий захист інформаційних прав та практика ЄСПЛ

Ефективність будь-якого права, у тому числі інформаційного, визначається наявністю дієвих механізмів його захисту у разі порушення. Судовий захист є вищою формою гарантування інформаційних прав людини в Україні. Оскільки інформаційні спори часто стосуються протистояння особи та державного апарату, роль незалежного суду у визначенні меж законності дій влади є визначальною. При цьому українське правосуддя дедалі більше інтегрується у європейський правовий простір, де ключовим орієнтиром виступає практика Європейського суду з прав людини (ЄСПЛ).

Ваговою подією для європейської юриспруденції стало рішення ЄСПЛ у справі «Мадьяр Хельсінкі Бізоттшаг проти Угорщини» (Magyar Helsinki Bizottság v. Hungary, 2016). У цьому рішенні Суд остаточно підтвердив, що право на отримання інформації від державних органів є невід'ємною частиною свободи вираження поглядів, гарантованої статтею 10 Конвенції [8, с. 220; 4].

Суд встановив чотири критерії, за якими відмова у наданні інформації вважається порушенням:

Мета запиту: чи є отримання інформації необхідним для реалізації права на свободу вираження поглядів (наприклад, для журналістського розслідування).

Характер інформації: чи становить вона суспільний інтерес.

Роль запитувача: чи виступає він у ролі «суспільного вартового» (журналісти, неурядові організації).

Наявність інформації: чи володіє державний орган цими даними [8, с. 225].

Українські суди все частіше використовують практику ЄСПЛ для вирішення спорів щодо незаконної відмови у наданні публічної інформації [17, с. 76]. Це проявляється у застосуванні прецедентів ЄСПЛ як джерела права (згідно із Законом України «Про виконання рішень та застосування практики Європейського суду з прав людини»). Зокрема, суди активно використовують «трискладовий тест» для перевірки того, чи обґрунтовано розпорядник інформації відніс відомості до категорії з обмеженим доступом [2; 17, с. 80].

Особливості судового розгляду інформаційних спорів в Україні:

Предмет спору: Найчастіше це оскарження ненадання відповіді на запит, надання неповної інформації або неправомірне віднесення інформації до службової чи таємної [16].

Тягар доказування: У таких справах обов'язок довести законність обмеження доступу покладається на суб'єкта владних повноважень (розпорядника). Суд має перевірити, чи не була відмова формальною [11, с. 148].

Захист конфіденційності: Суди також розглядають справи про захист честі, гідності та ділової репутації, де межею права на інформацію виступає заборона поширення недостовірних відомостей [14, с. 250].

Практика Верховного Суду України останніх років демонструє чітку тенденцію до захисту запитувачів. Суд наголошує, що розпорядник інформації

не може просто полатися на наявність грифу «Для службового користування», він повинен обґрунтувати, яку саме шкоду національній безпеці чи інтересам правосуддя завдасть оприлюднення документа [17, с. 85; 20, с. 340]. Такий підхід робить межу інформаційних прав більш прозорою та передбачуваною.

Важливим аспектом є також захист права на спростування. Якщо межа між критикою та клепом була порушена, особа має право на судовий захист через механізм спростування недостовірної інформації або відшкодування моральної шкоди. Тут суди знову звертаються до практики ЄСПЛ (наприклад, справа «Лінгенс проти Австрії»), розрізняючи «фактологічні твердження» (які підлягають доведенню) та «оціночні судження» (які не можуть бути спростовані) [15, с. 110; 19, с. 156].

В умовах цифрової трансформації суди стикаються з новими викликами, такими як видалення інформації з мережі Інтернет («право на забуття»). Судова практика у цих питаннях лише формується, проте орієнтація на стандарти ЄСПЛ дозволяє забезпечити захист приватності особи без надмірного обмеження свободи слова [9, с. 340; 12, с. 245].

Отже, судовий захист та практика ЄСПЛ є гарантами того, що межі інформаційних прав не будуть перетворені на інструмент цензури. Через судові рішення відбувається постійне уточнення змісту інформаційних свобод, що адаптує законодавство до вимог часу та забезпечує верховенство права в інформаційній сфері [17, с. 90; 8, с. 230].

3.3. Шляхи вдосконалення законодавства щодо визначення меж інформаційних прав

Сучасний етап розвитку інформаційного права в Україні характеризується необхідністю адаптації національного законодавства до викликів цифрової трансформації та вимог європейської інтеграції.

Визначення меж інформаційних прав потребує не лише теоретичного переосмислення, а й конкретних законодавчих кроків, спрямованих на створення прозорих, але водночас безпечних правил гри в інформаційному просторі.

Цифровізація як інструмент реалізації та обмеження прав. Першочерговим завданням є цифровізація механізмів доступу до інформації. Це передбачає перехід від паперових запитів до автоматизованих систем надання публічних даних через відкриті API та державні портали (наприклад, подальший розвиток порталу «Дія»). Цифровізація дозволяє мінімізувати людський фактор при визначенні меж доступу: система може автоматично ретушувати персональні дані в документах, залишаючи відкритим зміст, що становить суспільний інтерес [9, с. 312; 12, с. 250].

Водночас цифровізація створює нові ризики, що зумовлює необхідність посилення відповідальності за витік конфіденційних даних. Чинні санкції в Кодексі України про адміністративні правопорушення часто є символічними порівняно зі шкодою, якої завдає незаконне поширення бази персональних даних. Пропонується запровадити диференційовану відповідальність, де розмір штрафу залежатиме від обсягу витоку та статусу суб'єкта (державний орган чи приватна корпорація) [13, с. 58; 18, с. 110].

Уточнення критеріїв «суспільного інтересу». Однією з найбільш маніпулятивних сфер залишається розмите визначення суспільно значущої інформації. Пропонується уточнити критерії «суспільного інтересу» в Законі «Про інформацію» для уникнення маніпуляцій [9, с. 312]. Законодавче закріплення вичерпного (або максимально конкретизованого) переліку обставин, за яких приватний інтерес поступається суспільному, дозволить зменшити кількість судових спорів. Зокрема, до таких критеріїв слід чітко віднести:

Виявлення корупційних схем та нецільового використання публічних ресурсів.

Інформацію про екологічний стан та ризики для здоров'я.

Відомості про професійну діяльність осіб, які займають політичні посади [14, с. 260].

Гармонізація з регламентом GDPR. Важливим шляхом вдосконалення є повна імплементація положень Загального регламенту про захист даних (GDPR) у національне право. Це вимагає прийняття нової редакції Закону України «Про захист персональних даних», яка б впровадила концепцію «Privacy by Design» (приватність за замовчуванням) та посилила роль незалежного наглядового органу в інформаційній сфері. Така реформа дозволить чіткіше окреслити межі між правом на інформацію та правом на забуття [12, с. 255; 20, с. 350].

Регулювання меж інформаційних прав у кіберпросторі. Законодавство потребує нових норм щодо регулювання діяльності великих технологічних платформ (соціальних мереж). Важливо встановити межі відповідальності платформ за поширення дезінформації та мови ворожнечі, не порушуючи при цьому право користувачів на свободу вираження поглядів. Пропонується розробити «Кодекс поведінки в Інтернеті», який би став частиною інформаційного законодавства [9, с. 315; 13, с. 62].

Межі прав в умовах пост-воєнного відновлення. Окремим вектором є розробка механізму поступового зняття обмежень, введених під час воєнного стану. Законодавство має містити «норми-запобіжники», які б автоматично повертали повний обсяг інформаційних прав громадянам після завершення бойових дій, запобігаючи консервації «надзвичайної» секретності [10, с. 205; 15, с. 55].

Підсумовуючи, вдосконалення законодавства має відбуватися за принципом «розумної прозорості». Це означає, що держава повинна бути максимально відкритою у своїх діях, але максимально суворою у захисті приватної сфери людини та критичної інфраструктури. Лише через чітку законодавчу фіксацію меж інформаційних прав, підкріплену сучасними технологіями та суворою відповідальністю, можливо побудувати правове інформаційне суспільство в Україні [3, с. 320; 20, с. 355].

ВИСНОВКИ

У ході виконання даної курсової роботи було проведено комплексне теоретико-правове дослідження природи, змісту та механізмів обмеження інформаційних прав людини в сучасному правовому полі України та світу. Результати дослідження дозволяють сформулювати наступні узагальнюючі положення, що мають як теоретичне, так і практичне значення:

Інформаційні права людини пройшли шлях від похідних елементів свободи слова до самостійного, багатогранного інституту інформаційного права. Встановлено, що ці права є «правами четвертого покоління», оскільки вони нерозривно пов'язані з технологічним прогресом.

Інформаційні права – це система правомочностей особи щодо вільного збирання, зберігання, використання та поширення інформації.

Вони мають подвійну природу – виступають одночасно як особисті немайнові права (захист приватності) та як політичні свободи (доступ до публічних даних).

Поділ на загальні та спеціальні права є ключовим для визначення меж. Загальні права діють за принципом «дозволено все, що не заборонено», тоді як спеціальні (наприклад, доступ до таємниці) регулюються за принципом «дозволено лише те, що прямо передбачено законом» [3, с. 47].

Головним висновком другого розділу є твердження, що інформаційні права не є абсолютними. Межі цих прав встановлюються не суб'єктивним бажанням держави, а через призму міжнародного стандарту – «трискладового тесту» (ст. 10 Конвенції) [4].

Будь-яке обмеження має бути встановлене виключно законом. Підзаконні акти не можуть звужувати зміст конституційного права.

Обмеження можливе лише для захисту нацбезпеки, територіальної цілісності, громадського порядку, здоров'я чи репутації.

Шкода від оприлюднення інформації має бути реальною та суттєвою, а не гіпотетичною. Встановлено, що українське законодавство (зокрема ст. 6

Закону «Про доступ до публічної інформації») повністю імплементувало цей стандарт, проте практика його застосування часто залишається формальною [16; 20, с. 305].

Дослідження показало, що найбільш гостро межа прав проходить по лінії захисту персональних даних.

Встановлено, що право на приватність є «щитом», а право на інформацію – «мечем».

Поняття суспільного інтересу є динамічним. Ми прийшли до висновку, що для публічних осіб (політиків, держслужбовців) межа приватності є значно вужчою. Громада має право знати про їхні статки та спосіб життя, якщо це впливає на виконання державних функцій [14, с. 215].

У мережі Інтернет захист даних стає складнішим, що вимагає впровадження нових правових конструкцій, таких як «право на забуття».

Аналіз реалій 2022–2026 років дозволяє стверджувати, що воєнний стан докорінно змінює архітектуру інформаційних меж.

У воєнний час право на інформацію легітимно поступається праву на життя та безпеку. Обмеження на зйомку військових об'єктів чи переміщення військ є пропорційним заходом [10, с. 158].

Введення ст. 114-2 ККУ стало необхідним кроком для юридичного закріплення меж, які раніше вважалися лише етичними.

Виявлено тенденцію до надмірного засекречування даних, які не стосуються оборони (наприклад, витрати на відбудову). Це вимагає посилення громадського контролю навіть в умовах війни [15, с. 50].

Судовий захист визначено як єдиний ефективний спосіб балансування прав.

Рішення у справі «Мадьяр Хельсінкі Бізоттшаг» є революційним, оскільки воно прирівняло доступ до інформації до свободи слова [8, с. 222].

Спостерігається позитивна динаміка: суди дедалі частіше стають на бік запитувачів інформації, змушуючи органи влади відкривати дані, які раніше

були під грифом «ДСК» (для службового користування) без належних підстав [17, с. 88].

На основі проведеного дослідження пропонується:

Внести зміни до Закону «Про інформацію», де чітко розшифрувати ознаки «суспільної необхідності», щоб чиновники не могли приховувати дані про корупцію під виглядом «персональних даних».

Впровадити автоматизовані системи деперсоніфікації документів (видалення особистих даних ШІ перед оприлюдненням), що зніме навантаження з розпорядників інформації [9, с. 312].

Збільшити штрафи за безпідставне обмеження доступу до публічної інформації, оскільки нинішні суми не є стримуючим фактором для порушників [13, с. 60].

Повна імплементація GDPR для захисту приватності українців у глобальному мережевому просторі.

Межі інформаційних прав – це не статична лінія, а рухомий баланс. У демократичному суспільстві цей баланс завжди має схилитися у бік відкритості та прозорості, за винятком випадків, коли таємність є єдиним способом захистити життя людини або суверенітет держави. Україна наразі перебуває на етапі формування унікальної моделі інформаційного права, яка здатна поєднувати високі стандарти свободи слова з жорсткими вимогами безпеки в умовах гібридної війни.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Конституція України: Закон від 28.06.1996 № 254к/96-ВР.
URL: <https://zakon.rada.gov.ua/laws/show/254к/96-вр>.
2. Про інформацію: Закон України від 02.10.1992 № 2657-ХІІ.
3. Арістова І. В. Інформаційне право: підручник. Київ: Юрінком Інтер, 2021. 360 с.
4. Конвенція про захист прав людини і основоположних свобод від 04.11.1950.
5. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VІ.
6. Про державну таємницю: Закон України від 21.01.1994 № 3855-ХІІ.
7. Брижко В. Г. Право на інформацію та інформаційні права людини. Київ: КНТ, 2019. 240 с.
8. Гавриленко О. А. Міжнародні стандарти інформаційних прав. Харків: Право, 2020. 280 с.
9. Данилюк Ю. В. Сучасні виклики інформаційного права. Одеса: Гельветика, 2022. 410 с.
10. Довгань О. Д. Інформаційна безпека в умовах війни. Київ: Наукова думка, 2023. 215 с.
11. Жиляєв І. В. Правовий режим інформації з обмеженим доступом. Львів: Світ, 2020. 190 с.
12. Когут Ю. І. Інформаційне право та цифрова трансформація. Київ: Кондор, 2021. 300 с.
13. Кормич Б. О. Інформаційне право: навчальний посібник. Харків: Еспада, 2018. 256 с.
14. Кузнецова О. В. Межі свободи слова: правовий аспект. Дніпро: Ліра, 2019. 320 с.

15. Марущак А. І. Інформаційне право України: підручник. Київ: ДП «Дирекція», 2023. 450 с.
16. Про доступ до публічної інформації: Закон України від 13.01.2011 № 2939-VI.
17. Петров Є. В. Судова практика у сферах інформаційних спорів. Запоріжжя: статус, 2021. 185 с.
18. Соснін О. В. Проблеми захисту персональних даних в мережі Інтернет. Київ: Академія, 2022. 140 с.
19. Фурашев В. М. Інформаційне право: теорія і практика. Київ: АртЕк, 2020. 210 с.
20. Швець М. Я. Основи інформаційного права України. Київ: Знання, 2019. 345 с.