

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ЮРИДИЧНИЙ ФАКУЛЬТЕТ

*Кафедра адміністративного права
та судочинства*

МІЖДИСЦИПЛІНАРНА КУРСОВА РОБОТА
з дисципліни: «Актуальні питання адміністративного права та процесу»
на тему:
«Інформаційне право України»

Виконала:

студентка групи ПРм-13

Дідушин Васирина Віталіївна

Науковий керівник:

д.ю.н., професор Кравчук М.Ю.

Національна шкала _____

Кількість балів: ____ Оцінка: ECTS: ____

Члени комісії: _____

(підпис) (прізвище та ініціали)

м. Тернопіль – 2025

ЗМІСТ

ВСТУП.....	4
Розділ 1. ТЕОРЕТИКО – ПРАВОВІ ОСНОВИ ІНФОРМАЦІЙНОГО ПРАВА	
1.1. Поняття та предмет інформаційного права.....	7
1.2. Джерела інформаційного права України.....	9
1.3. Принципи та суб'єкти інформаційних правовідносин.....	11
Розділ 2. ПРАВОВЕ РЕГУЛЮВАННЯ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ В УКРАЇНІ	
2.1. Інформаційні права та свободи громадян.....	14
2.2. Правовий режим доступу до інформації.....	15
2.3. Регулювання державної, службової, конфіденційної та таємної інформації.....	17
Розділ 3. ЗАХИСТ ІНФОРМАЦІЇ ТА ВІДПОВІДАЛЬНІСТЬ ЗА ПРАВОПОРУШЕННЯ У СФЕРІ ІНФОРМАЦІЙНОГО ПРАВА	
3.1. Система захисту інформації в Україні.....	20
3.2. Інформаційна безпека: поняття, принципи та нормативне забезпечення.....	21
3.3. Відповідальність за порушення інформаційного законодавства.....	23
Розділ 4. ПЕРСПЕКТИВИ РОЗВИТКУ ІНФОРМАЦІЙНОГО ПРАВА В УКРАЇНІ	
4.1. Інформаційне право в цифрову епоху.....	26
4.2. Гармонізація українського законодавства з міжнародними стандартами.....	27

4.3. Проблемні питання та шляхи їх вирішення.....	28
ВИСНОВКИ	30
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	32

ВСТУП

Актуальність теми дослідження. Сучасне суспільство дедалі більше трансформується в інформаційне, де доступ до інформації, її збереження, обробка та передача відіграють ключову роль в усіх сферах життєдіяльності.

У сучасному світі володіння інформацією часто дорівнює володінню владою — як у політичній, так і в економічній чи соціальній площині. Саме тому регулювання обігу, доступу, обробки та захисту інформації стало ключовим завданням держави і суспільства.

У цьому контексті виникає необхідність ефективного правового регулювання інформаційних відносин, що й зумовлює актуальність формування та розвитку інформаційного права як окремої галузі юридичної науки.

Інформаційне право охоплює широке коло питань: від забезпечення свободи слова й доступу до публічної інформації — до захисту персональних даних та інформаційної безпеки. Зважаючи на стрімкий розвиток цифрових технологій, кіберпростору та інтернет-комунікацій, законодавство у цій сфері має постійно оновлюватися і вдосконалюватися. Особливого значення набуває гармонізація національних норм з європейськими стандартами, що є важливим етапом у процесі євроінтеграції України.

Актуальність обраної теми зумовлена низкою причин. По-перше, інформаційні відносини все більше проникають у всі сфери життя: від комунікації громадян із державою — до функціонування бізнесу, освіти, охорони здоров'я. По-друге, українське суспільство дедалі частіше стикається з викликами у сфері інформаційної безпеки — як у вигляді кіберзлочинності, так і в інформаційній війні. По-третє, у процесі інтеграції до європейського правового простору Україні необхідно адаптувати своє інформаційне законодавство відповідно до міжнародних норм і стандартів.

Теоретико-методологічну основу дослідження становлять наукові праці українських і зарубіжних правознавців у галузі інформаційного права,

конституційного права, адміністративного та міжнародного права, а також міждисциплінарні дослідження, присвячені інформаційній безпеці, цифровим правам та кіберпростору. Зокрема, були використані теоретичні напрацювання таких вчених, як П. Антонюк, Л. Гайдук, І. Гуменюк, В. Данілевська тощо, а також аналітичні матеріали Ради Європи, Європейського Союзу та міжнародних організацій у сфері інформаційних прав і свобод.

Мета дослідження – всебічне дослідження сутності, принципів та основних інститутів інформаційного права України, аналіз чинного законодавства у сфері інформаційних правовідносин, виявлення актуальних проблем правового регулювання інформаційної діяльності, а також формулювання пропозицій щодо вдосконалення інформаційного законодавства з урахуванням сучасних викликів і європейських правових стандартів.

Об'єкт дослідження – суспільні відносини, що виникають у процесі створення, обробки, зберігання, поширення та захисту інформації в Україні, які потребують правового регулювання в умовах інформаційного суспільства.

Предмет дослідження – правові норми, інститути та механізми регулювання інформаційних відносин в Україні, а також практика їх застосування у сфері забезпечення доступу до інформації, захисту персональних даних і гарантування інформаційної безпеки.

Завдання дослідження:

- розкрити поняття, ознаки та основні функції інформації як об'єкта правового регулювання;
- дослідити зміст і структуру інформаційного права як галузі національного права України;
- проаналізувати основні нормативно-правові акти, що регламентують інформаційні правовідносини в Україні;
- розглянути питання правового захисту персональних даних та інформаційної безпеки;

- виявити основні проблеми, пов'язані з реалізацією інформаційних прав, та запропонувати шляхи їх вирішення.

Методологічна основа дослідження — становить сукупність загальнонаукових та спеціально-юридичних методів, які забезпечили комплексне та всебічне вивчення проблем інформаційного права України. Зокрема, застосовано методи аналізу та синтезу — для розкриття сутності та елементів інформаційного права. Порівняльно-правовий метод дозволив зіставити українське законодавство з міжнародними та європейськими стандартами, а історико-правовий метод дав змогу простежити етапи становлення цієї галузі. Також було враховано емпіричні дані, зокрема судову практику у сфері захисту інформаційних прав, що сприяло об'єктивності та практичній спрямованості дослідження.

Структура курсової роботи. Курсова робота складається зі вступу, основної частини, яка містить 4 розділи, висновків та списку використаної літератури.

РОЗДІЛ 1. ТЕОРЕТИКО – ПРАВОВІ ОСНОВИ ІНФОРМАЦІЙНОГО ПРАВА

1.1. Поняття та предмет інформаційного права

Сучасна епоха характеризується стрімким зростанням ролі інформації як одного з ключових стратегічних ресурсів, що також впливає на рівень розвитку держави, її економічну стабільність, національну безпеку та соціальну згуртованість. Із початку цифрової трансформації інформація набула особливої ваги, ставши основою для ухвалення рішень у сфері державного управління, економіки, політики й повсякденного життя громадян. У зв'язку з цим виникла об'єктивна потреба у формуванні правового механізму регулювання інформаційних процесів, що, у своєму разі, сприяло становленню інформаційного права як окремої галузі юридичної науки та практики.

Захист персональних даних, безпека цифрового середовища, свобода доступу до інформації, запобігання поширенню дезінформації та регулювання кіберпростору – це нові виклики, з якими зіткнулися держава та суспільство. відповідно, інформаційне право стало відповіддю на ці виклики. відповідно, значення цієї правової галузі зростає, оскільки її розвиток впливає на підтримку демократії, прав людини, інформаційного суверенітету держави та ефективної економіки.

Під інформаційним правом розуміють систему правових норм, які регулюють суспільні відносини, що виникають у процесі створення, обробки, зберігання, поширення, використання та захисту інформації. Ця галузь права займає особливе місце в національній правовій системі, адже оперує поняттям інформації як нематеріального об'єкта, що має важливе правове, соціальне, економічне й технологічне значення. Необхідність комплексного правового впорядкування усіх етапів обігу інформації стала передумовою виділення інформаційного права як окремої галузі [8].

Інформаційне право має складну й динамічну структуру, оскільки охоплює значну кількість суспільних процесів, що відбуваються як у традиційних, так і в цифрових формах комунікації. У зв'язку з цим, воно тісно пов'язане з іншими галузями права — насамперед конституційним (у контексті реалізації права на інформацію), цивільним (питання інтелектуальної власності, договірному регулювання інформаційних послуг), адміністративним (регулювання діяльності органів державної влади у сфері інформації), кримінальним (відповідальність за порушення інформаційних прав), а також міжнародним правом . (особливо у сфері цифрової безпеки та транскордонного обміну даними).

До характерних рис інформаційного права належить його здатність швидко адаптуватися до змін, зумовлених науково-технічним прогресом. Цифровізація, поширення Інтернету, розвиток соціальних мереж, впровадження штучного інтелекту й аналітики великих даних істотно трансформують розуміння інформації як ресурсу. Відтак інформаційне право не лише регламентує правовідносини, а й забезпечує баланс між свободою інформаційного обміну та захистом суспільних і особистих інтересів, сприяє підтриманню інформаційної безпеки та суверенітету держави [21].

Предметом інформаційного права є сукупність суспільних відносин, що виникають у зв'язку зі створенням, обробкою, зберіганням, поширенням, використанням і охороною інформації. Учасниками цих правовідносин виступають різні суб'єкти — органи влади, фізичні та юридичні особи, медіа, постачальники цифрових послуг тощо. Особливе значення має правове регулювання доступу до публічної інформації, захисту персональних даних, конфіденційної інформації, державної таємниці, а також забезпечення прав на інформацію як об'єкт інтелектуальної власності.

Таким чином, інформаційне право є основою нормативного забезпечення функціонування інформаційного простору України. Його розвиток сприяє

формуванню відкритого, безпечного та демократичного інформаційного середовища, в якому гарантовано підтримку прав громадян та інтересів держави.

1.2. Джерела інформаційного права

Ефективне функціонування будь-якої правової галузі неможливе без наявності чіткої та структурованої системи джерел, які закріплюють її правові норми. Регулювання інформаційної сфери в Україні будується на основі широкого спектра нормативно-правових актів, які разом формують систему джерел інформаційного права. Саме ці джерела сприяють реалізації важливих інформаційних прав громадян, забезпечують механізми захисту даних і встановлюють регламентовані правила обігу інформації в межах держави.

До джерел інформаційного права належать нормативно-правові акти, що містять правові норми для врегулювання суспільних відносин у сфері інформації. Вони утворюють правову основу, на якій базується функціонування всієї інформаційної сфери країни — від забезпечення права на доступ до інформації громадянам до врегулювання питань інформаційної безпеки, захисту персональних даних, охорони державної таємниці й авторських прав на інформацію [6].

Інформаційне право є міжгалузеву галуззю, тому його джерела мають багатоаспектну структуру та охоплюють нормативні акти з різних галузей права.

Особливе місце серед цих джерел займає Конституція України, яка визначає фундаментальні принципи інформаційного права. Наприклад, стаття 34 гарантує кожному свободу думки та слова, а також право на вільне отримання, зберігання й поширення інформації. Стаття 32 акцентує увагу на захисті особистого й сімейного життя, включаючи конфіденційність

персональних даних. Водночас стаття 57 зобов'язує державу забезпечувати доступ до правової інформації.

Важливою групою джерел є спеціальні закони, які безпосередньо регулюють інформаційні правовідносини. Серед них ключову роль відіграють:

- Закон України «Про інформацію», який визначає правову основу інформаційної діяльності та класифікацію інформації;
- Закон «Про доступ до публічної інформації», що забезпечує відкритість діяльності державних органів;
- Закон «Про захист персональних даних», який регулює обробку, зберігання та використання даних фізичних осіб;
- Закон «Про телекомунікації», «Про авторське право і суміжні права», а також «Про національну безпеку» (у частині інформаційної безпеки). Ці акти створюють нормативну рамку для регулювання інформаційного середовища [2].

До джерел також належать підзаконні нормативно-правові акти — укази Президента України, постанови Кабінету Міністрів, накази профільних міністерств, які деталізують реалізацію положень законів. Наприклад, правила ведення електронного документообігу, порядок доступу до відкритих державних реєстрів, порядок обміну інформацією в органах влади тощо.

Окреме значення мають міжнародно-правові акти, ратифіковані Україною. Серед них важливими є Загальна декларація прав людини, Європейська конвенція з прав людини, Конвенція Ради Європи про доступ до офіційних документів, рекомендації Ради Європи щодо захисту персональних даних. Вони сприяють гармонізації українського законодавства із загальноєвропейськими стандартами у сфері свободи вираження, приватності та цифрових прав [13].

Також джерелом тлумачення норм інформаційного права виступає судова практика, зокрема рішення Конституційного Суду України та Європейського суду з прав людини. Їхні правові позиції мають обов'язковий характер для

національних судів та сприяють однаковому застосуванню законодавства в інформаційній сфері.

Отже, джерела інформаційного права в Україні характеризуються складною та багатовимірною структурою, яка охоплює як національні правові акти, так і міжнародні зобов'язання держави. Їхнє комплексне застосування забезпечує ефективне правове управління у сфері інформації і сприяє гармонізації українського законодавства із міжнародними стандартами у галузі прав людини, цифрової безпеки та регулювання інформаційного простору.

1.3. Принципи та суб'єкти інформаційних правовідносин

Інформаційні правовідносини сфері інформаційного права є системою юридично врегульованих взаємозв'язків між суб'єктами в контексті створення, збирання та обробки інформаційних даних для їх подальшого поширення та використання. Ефективне функціонування таких правовідносин базується на певних основоположних засадах, що визначають логіку та спрямованість інформаційно-правової політики держави. Ці засади закріплюються як у національному законодавстві, так і в міжнародно-правових документах та наукових джерелах [23].

Принцип свободи інформації є одним з основних принципів інформаційного права, що означає право кожного на вільний доступ до інформації, її поширення та використання, якщо це не заборонено законом. Цей принцип впливає зі ст. 34 Конституції України та узгоджується з нормами міжнародного права, зокрема ст. 10 Європейської конвенції з прав людини.

Наступним важливим принципом є принцип законності, відповідно до якого усі дії суб'єктів інформаційних правовідносин повинні здійснюватися у встановлених законодавством межах. Цей принцип забезпечує правову визначеність, унеможливорює свавільне втручання в інформаційну сферу та створює передумови для судового захисту порушених прав.

Важливе значення має також принцип доступності інформації, який означає, що інформація, що не є державною чи іншою захищеною таємницею, повинна бути відкритою, публічною і доступною для користувачів. Закон України «Про доступ до публічної інформації» прямо зобов'язує органи державної влади та місцевого самоврядування створювати умови для ефективного доступу громадян до інформації про свою діяльність.

Не менш важливим є принцип достовірності та цілісності інформації. Він означає у тому, що будь-яка інформація, що створюється, поширюється або використовується, має відповідати дійсності, бути цілісною, точною та об'єктивною. Цей принцип особливо важливий у контексті боротьби з дезінформацією та маніпуляціями ЗМІ [19].

Принцип поваги до прав і свобод людини відіграє особливу роль у демократичному суспільстві, який передбачає необхідність збереження балансу між правом доступності до інформації та правом на приватність, недоторканність особистого життя, захист персональних даних. Інформаційна діяльність не повинна посягати на особисту гідність, дискримінувати чи обмежувати свободи.

Також важливим є принцип інформаційної безпеки, який полягає в захисті інформації та інформаційної інфраструктури від несанкціонованого доступу, кібератак, поширення шкідливого контенту тощо. Він є частиною загальної системи національної безпеки держави.

Таким чином, принципи інформаційних правовідносин є ключовими орієнтирами, які сприяють встановленню правового порядку у сфері інформації, сприяють розвитку відкритого інформаційного суспільства, забезпечують ефективне функціонування державних інституцій та захист прав і свобод громадян.

Щодо суб'єктів інформаційних правовідносин, то до них відносяться учасники правовідносин, які виникають у сфері інформації, і взаємодіють у

процесі її створення, обробки, зберігання, поширення та використання. Кожен із цих суб'єктів має права та обов'язки, що регулюються інформаційним законодавством.

Основним суб'єктом є громадяни України, які мають право на доступ до інформації, її поширення та захист персональних даних. Вони можуть звертатися до органів влади за публічною інформацією та користуватися своїми правами на конфіденційність і приватність.

Органи державної влади та місцевого самоврядування є постачальниками публічної інформації та зобов'язані забезпечити її доступність для громадян. Вони також відповідають за захист державної та комерційної таємниці, а також за виконання стандартів інформаційної безпеки.

Юридичні особи, зокрема медіа та інші організації, що займаються інформаційною діяльністю, також є важливими суб'єктами. Вони зобов'язані дотримуватися стандартів достовірності та об'єктивності інформації, а також правових вимог щодо захисту персональних даних.

Інформаційні посередники, такі як провайдери інтернет-послуг та хостинг-платформи, відіграють ключову роль у забезпеченні обміну та збереження інформації, контролюючи дотримання законодавства у сфері цифрової безпеки та недопущення незаконного контенту [17].

Завершальними суб'єктами є органи контролю та захисту прав, такі як омбудсмен, державні інспекції з питань захисту персональних даних і національної безпеки, які здійснюють нагляд за дотриманням законів у сфері інформації.

РОЗДІЛ 2. ПРАВОВЕ РЕГУЛЮВАННЯ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ В УКРАЇНІ

2.1. Інформаційні права і свободи громадян

Інформаційні права і свободи громадян є однією з основоположних складових правового статусу особи в інформаційному суспільстві. Вони визначають можливості громадян щодо доступу, використання та поширення інформації, а також упорядковують правові межі в сучасному інформаційному середовищі. В Україні інформаційні права та свободи громадян закріплені в Конституції та численних спеціальних законах, які забезпечують громадянам право на свободу думки, доступ до публічної інформації, право на захист персональних даних та право на недоторканність приватного життя [18].

Одним з основних прав є право на свободу думки та вираження, яке закріплене статтею 34 Конституції України. Це право дозволяє громадянам вільно отримувати та поширювати інформацію, що не суперечить законодавству, і є основою демократичного суспільства. Однак, законодавство передбачає певні обмеження на це право, зокрема у випадках захисту державної таємниці, боротьби з насильством або дискримінацією.

Право на доступ до публічної інформації є ще одним важливим правом, яке дозволяє громадянам звертатися до державних установ для отримання необхідної інформації. Це право закріплене в Законі України «Про доступ до публічної інформації». Проте існують обмеження на доступ до певної інформації, що стосується національної безпеки, державних таємниць або особистих даних громадян. У таких випадках доступ до інформації може бути обмежений.

Захист персональних даних є ще одним важливим правом, яке забезпечує громадянам контроль над використанням їхніх особистих відомостей. Закон України «Про захист персональних даних» зобов'язує організації отримувати

згоду громадян на обробку їхніх даних та гарантує належний рівень захисту цих даних від несанкціонованого доступу [20].

Право на інформаційну безпеку включає захист від дезінформації та фальшивих новин, які можуть впливати на громадську думку та стабільність суспільства. Важливим аспектом є також захист від кіберзлочинності та інших загроз, які можуть спричинити витік або втрату важливих особистих або державних даних.

Крім того, право на приватність є важливою частиною інформаційних прав громадян. Це право захищає особисте життя та комунікації від незаконного втручання, зокрема забезпечує конфіденційність особистих даних, кореспонденції та телефонних розмов. Законодавство встановлює чіткі вимоги до обробки персональних даних, щоб забезпечити їх безпеку та захист прав громадян.

Таким чином, інформаційні права та свободи громадян є невід'ємною частиною їхнього правового статусу та відіграють важливу роль у розвитку демократичного суспільства. Вони забезпечують громадянам можливість вільно отримувати і поширювати інформацію, захищати свої персональні дані та приватність, а також сприяють розвитку відкритого та прозорого інформаційного середовища.

2.2. Правовий режим доступу до інформації

У сучасному суспільстві, яке стрімко трансформується під впливом цифрових технологій, доступ до інформації набуває особливого значення як інструмент реалізації демократичних прав і свобод людини. Правовий режим доступу до інформації виступає гарантією прозорості діяльності органів державної влади та ефективної участі громадян у прийнятті суспільно важливих рішень.

Правовий режим доступу до інформації — це система юридичних норм, що регулює порядок одержання, використання, поширення та обмеження доступу до інформації в суспільстві. У демократичній державі забезпечення відкритості та прозорості є невід’ємною частиною взаємодії між громадянами і державними структурами, тому законодавче врегулювання доступу до інформації відіграє ключову роль у формуванні довіри до влади, реалізації прав людини і запобіганні зловживанням [22].

В Україні правовий режим доступу до інформації закріплено, передусім, у Конституції України (стаття 34), яка гарантує кожному право вільно збирати, зберігати, використовувати та поширювати інформацію. Крім того, базовим нормативним актом, що безпосередньо визначає правові засади доступу до інформації, є Закон України «Про доступ до публічної інформації». Він встановлює принципи прозорості, відкритості, оперативності, достовірності, законності та забезпечення максимально широкого доступу до інформації, яка створюється чи зберігається органами державної влади, місцевого самоврядування та іншими суб’єктами публічного права.

Інформація, відповідно до чинного законодавства, поділяється на відкриту та інформацію з обмеженим доступом. До останньої належить конфіденційна, таємна та службова інформація. Кожна з цих категорій має свій режим правового захисту. Наприклад, обмеження доступу до інформації можливе лише у випадках, коли розголошення може завдати шкоди національній безпеці, правопорядку, правам та інтересам інших осіб, а саме обмеження є законним, необхідним і пропорційним.

Закон «Про доступ до публічної інформації» визначає, що розпорядники інформації зобов’язані надавати її за запитом громадянина протягом п’яти робочих днів. Якщо ж інформація стосується життя чи здоров’я особи, стану довкілля, якості харчових продуктів або аварій, що загрожують безпеці громадян, — така інформація має надаватися невідкладно, не пізніше 48 годин з

моменту отримання запиту. Водночас закон встановлює підстави для відмови в наданні інформації, зокрема, якщо запитувана інформація є з обмеженим доступом або якщо запит складено з порушенням встановлених вимог.

Також варто зазначити, що суб'єктами, які можуть бути розпорядниками публічної інформації, є не лише державні органи, але й юридичні особи, що фінансуються з державного або місцевого бюджету, або виконують делеговані владні функції. Вони так само зобов'язані забезпечити відкритість і доступ до інформації про свою діяльність [11].

Значна увага в сучасних умовах приділяється цифровому доступу до інформації. Розвиток електронного врядування дозволяє громадянам отримувати значну частину публічної інформації через офіційні вебсайти органів влади, публічні електронні реєстри, портали відкритих даних тощо. Такі механізми сприяють реалізації принципу «максимальної відкритості» у практиці державного управління.

У цілому правовий режим доступу до інформації в Україні формується на основі демократичних принципів, міжнародних стандартів і практик, зокрема вимог Європейської конвенції з прав людини та рішень Європейського суду з прав людини. Його основне завдання — забезпечення балансу між відкритістю та захистом суспільно важливої або чутливої інформації, з урахуванням прав і свобод кожного громадянина.

2.3. Регулювання державної, службової, конфіденційної та таємної інформації

У системі інформаційного права важливе місце займає правове регулювання обігу інформації з обмеженим доступом, зокрема державної, службової, конфіденційної та таємної. Усі ці види інформації мають різні правові режими, особливості захисту та обмеження щодо доступу, що

зумовлено необхідністю забезпечення національної безпеки, охорони прав і свобод людини, а також підтримки публічного порядку.

Державна таємниця — це вид інформації, що охоплює відомості у сферах оборони, економіки, науки й техніки, зовнішніх зносин, безпеки держави, розголошення яких може зашкодити національним інтересам України. Порядок класифікації та охорони державної таємниці регулюється Законом України «Про державну таємницю». Інформація, яка становить державну таємницю, підлягає спеціальному захисту та має гриф секретності (наприклад, «таємно», «цілком таємно», «особливої важливості»). Доступ до неї мають лише особи, які пройшли спеціальну перевірку і отримали допуск до роботи з такою інформацією [12].

Службова інформація — це відомості, які створюються у процесі службової діяльності державних органів і не підлягають широкому розголошенню, але водночас не становлять державної таємниці. До цієї категорії належать, наприклад, проекти рішень, внутрішні службові документи, службові листування тощо. Такі відомості обмежуються у доступі відповідно до вимог законодавства, зокрема відповідно до Закону України «Про інформацію» та підзаконних актів, які регулюють порядок надання статусу «для службового користування».

Конфіденційна інформація — це відомості, доступ до яких обмежується фізичною або юридичною особою самотійно, з метою захисту особистих, професійних або комерційних інтересів. Найпоширенішими прикладами є персональні дані громадян, комерційна таємниця, медична, банківська або адвокатська таємниця. Законодавство України, зокрема Закон «Про захист персональних даних», встановлює механізми обробки, передачі й зберігання такої інформації, включаючи вимогу отримання згоди суб'єкта на її використання та обов'язок забезпечити її захист від несанкціонованого доступу [15].

Таємна інформація, як загальне поняття, охоплює інформацію, що за умовами доступу може бути державною, службовою або конфіденційною. Основною ознакою такої інформації є наявність спеціального режиму доступу до неї. Регулювання такої інформації спрямоване на досягнення балансу між правом суспільства на інформацію та необхідністю обмеження доступу задля охорони публічних чи приватних інтересів.

Важливо зазначити, що будь-яке обмеження доступу до інформації повинно бути законним, обґрунтованим і не перевищувати меж, необхідних у демократичному суспільстві. Це положення впливає як із Конституції України, так і з міжнародних правових стандартів, зокрема практики Європейського суду з прав людини. Забороняється класифікація інформації як таємної з метою приховування фактів порушення прав людини, зловживань владою чи уникнення відповідальності посадовців.

Отже, ефективне регулювання обігу інформації з обмеженим доступом є важливою умовою як для забезпечення публічного інтересу, так і для захисту приватного життя особи. Правові механізми, які існують в Україні, покликані створити збалансовану систему, що гарантує належну інформаційну безпеку без необґрунтованого втручання в свободу вираження поглядів і право на доступ до інформації.

РОЗДІЛ 3. ЗАХИСТ ІНФОРМАЦІЇ ТА ВІДПОВІДАЛЬНІСТЬ ЗА ПРАВОПОРУШЕННЯ У СФЕРІ ІНФОРМАЦІЙНОГО ПРАВА

3.1. Система захисту інформації в Україні

Захист інформації набуває важливого значення в умовах розвитку інформаційного суспільства. Захист інформації є важливою частиною національної безпеки та прогресу демократії в Україні, оскільки це правова держава. Інформація стала не лише ресурсом, а й об'єктом потенційних небезпек, особливо в Інтернеті. Таким чином, для стабільності, правопорядку та реалізації прав людини

Система захисту інформації в Україні — це сукупність організаційних, технічних, правових та інституційних заходів, спрямованих на забезпечення безпеки даних, збереження цілісності, конфіденційності та доступності інформації. Її структура охоплює державну політику у сфері інформаційної безпеки, дії уповноважених органів, відповідне законодавство та спеціалізовані технології захисту даних [16].

Система захисту інформації базується на кількох ключових принципах: законності, системності, безперервності, превентивності та відповідальності. Особливе значення має принцип співмірності — заходи захисту повинні бути адекватними реальним загрозам і не порушувати конституційні права громадян. Наприклад, обмеження доступу до певної інформації можливе лише за чітко визначеними законами умовами і має бути тимчасовим, обґрунтованим і пропорційним.

Центральним органом виконавчої влади, що координує політику у цій сфері, є Державна служба спеціального зв'язку та захисту інформації України (ДССЗІ). До її функцій належить контроль за захистом державних інформаційних ресурсів, сертифікація засобів криптографічного та технічного захисту, координація у сфері кібербезпеки. Також важливу роль відіграють

Служба безпеки України, яка контролює питання захисту державної таємниці, та Національний координаційний центр кібербезпеки при РНБО.

Система захисту інформації постійно розвивається через активну цифровізацію державних процесів, розвиток електронного врядування та гібридні загрози в умовах війни. У відповідь на нові виклики постає необхідність змін нормативної бази, реорганізації державних структур, залучення міжнародного співробітництва. У сфері кіберзахисту Україна активно працює з демократичними країнами, такими як ЄС, НАТО та інші [4].

Таким чином, система захисту інформації в Україні постійно змінюється, багаторівневою і взаємодіє з різними сторонами. У цифрову епоху її ефективне використання є важливим для безпеки держави та захисту громадян. Цей захист залежить від довіри суспільства до держави, а також від здатності країни протистояти сучасним інформаційним атакам.

3.2. Інформаційна безпека: поняття, принципи та нормативне забезпечення

Інформація зараз є стратегічним ресурсом, який визначає економічну та наукову силу держав, а також політичну стабільність і безпеку. Враховуючи зростання залежності суспільства від інформаційно-комунікаційних технологій, важливим є забезпечення безпеки інформаційного простору. Таким чином, поняття інформаційної безпеки є життєво-важливим для функціонування держави та її установ, а також для захисту прав і свобод людини.

Інформаційна безпека — це стан захищеності особи, суспільства і держави від зовнішніх та внутрішніх загроз у сфері інформації. Вона охоплює як технічні аспекти захисту інформаційних систем, так і соціально-правові механізми, що запобігають маніпуляціям, дезінформації, витоку конфіденційних даних та порушенням інформаційних прав. Таким чином,

інформаційна безпека є міждисциплінарним поняттям, яке включає правову, організаційну, технічну та ідеологічну складові [5].

Інформаційна безпека в Україні визначається Конституцією, міжнародними зобов'язаннями та національними інтересами. Законність, відкритість і доступність, пропорційність обмежень, недоторканність приватного життя, невтручання в свободу вираження думок, системність і комплексність є основними принципами. З іншого боку, держава має право та обов'язок вживати превентивні та реактивні заходи, щоб запобігти загрозам інформаційній сфері національній безпеці, зокрема під час війни або масових кібератак.

Правовий фундамент інформаційної безпеки України утворюють низка ключових нормативно-правових актів. Основним документом є Закон України «Про національну безпеку», в якому інформаційна безпека визначена як одна з основних складових національної безпеки поряд з воєнною, економічною, екологічною тощо. Також значну роль відіграють Закони України «Про інформацію», «Про захист персональних даних», «Про державну таємницю», «Про основні засади забезпечення кібербезпеки України». Ці акти регламентують як загальні вимоги до інформаційної політики, так і специфіку кіберзахисту, поводження з інформацією обмеженого доступу та обов'язки суб'єктів інформаційної сфери [7].

Після початку збройної агресії Росії проти України у 2014 році, яка супроводжувалася сильним інформаційним тиском, питання інформаційної безпеки стало особливо актуальним. У результаті держава була змушена ввести нові заходи для захисту інформації. Ці заходи включали обмеження на розповсюдження ворожого контенту, блокування певних інформаційних ресурсів і активне створення національного інформаційного простору.

Важливим інституційним елементом забезпечення інформаційної безпеки є Національний координаційний центр кібербезпеки при РНБО, Державна

служба спеціального зв'язку та захисту інформації України, а також Служба безпеки України. Ці органи відповідають за моніторинг кіберзагроз, реагування на інциденти, сертифікацію засобів захисту інформації та координацію міжвідомчої взаємодії у сфері інформаційної безпеки [1].

Поряд із державними діями важливою є суспільна свідомість. Інформаційні загрози можна успішно подолати лише за умови високої медіаграмотності населення, здатності критично сприймати інформацію та активної участі громадянського суспільства у формуванні інформаційного порядку.

Підводячи підсумок, варто зазначити, що інформаційна безпека — це не лише питання технічного захисту, а це також питання правових і соціальних питань, які стосуються здатності держави захистити суверенітет, демократичні принципи та створити безпечне та вільне інформаційне середовище для своїх громадян. Для її успішного забезпечення потрібні комплексний підхід, планування на перспективу та постійне оновлення правової бази відповідно до нових викликів сьогодення.

3.3. Відповідальність за порушення інформаційного законодавства

У сфері інформаційного права відповідальність за порушення встановлених норм і правил відіграє важливу роль у забезпеченні правопорядку, захисті державних і приватних інтересів, а також у гарантуванні безпеки інформаційного простору. В умовах інтенсивного розвитку інформаційних технологій та цифровізації суспільства порушення інформаційного законодавства можуть мати серйозні наслідки — від втрати конфіденційної інформації до загроз національній безпеці. Відповідальність у цій сфері виступає не лише як міра покарання, а й як інструмент попередження та правового регулювання.

Залежно від характеру порушення та ступеня його суспільної небезпеки, в українському законодавстві передбачено чотири основні види юридичної відповідальності: кримінальна, адміністративна, цивільно-правова та дисциплінарна. Кожен із цих видів має свої підстави, механізми реалізації та санкції.

Кримінальна відповідальність передбачена за найтяжчі правопорушення в інформаційній сфері. Відповідно до Кримінального кодексу України, до таких злочинів належать: несанкціоноване втручання в роботу комп'ютерів, систем і мереж (ст. 361), створення шкідливих програм (ст. 361-1), порушення роботи електронно-обчислювальних систем (ст. 362), незаконне збирання або використання персональних даних (ст. 182), поширення державної таємниці або іншої інформації з обмеженим доступом (ст. 328–330). Санкції за такі дії можуть включати позбавлення волі, штрафи, заборону обіймати певні посади тощо.

Адміністративна відповідальність застосовується у випадках, коли порушення не тягнуть за собою кримінального переслідування, але мають правопорушючий характер. Зокрема, Кодекс України про адміністративні правопорушення передбачає покарання за неправомірне використання інформації, порушення порядку доступу до публічної інформації, розголошення службової або комерційної таємниці, недотримання вимог щодо зберігання персональних даних. Санкції можуть включати штрафи, конфіскацію носіїв інформації, адміністративне стягнення тощо.

Цивільно-правова відповідальність виникає у випадках, коли порушення інформаційних прав заподіює шкоду фізичній чи юридичній особі. Наприклад, незаконне поширення конфіденційної інформації, публікація недостовірних відомостей, порушення авторських прав у цифровому середовищі можуть стати підставами для пред'явлення позову про відшкодування матеріальної та

моральної шкоди. У таких випадках сторони звертаються до суду, а відшкодування визначається залежно від обсягу завданих збитків.

Дисциплінарна відповідальність стосується працівників, які у процесі виконання службових обов'язків допустили порушення вимог щодо обігу інформації, наприклад, службової або конфіденційної. Відповідно до трудового законодавства, це може бути підстава для догани, зниження в посаді або звільнення. Особливо це стосується держслужбовців, співробітників органів влади, суддів, працівників банківських та телекомунікаційних структур.

Крім того, Україна активно адаптує своє законодавство до міжнародних стандартів у сфері інформаційної безпеки та цифрових прав, зокрема в контексті євроінтеграції. Це включає впровадження механізмів захисту персональних даних, боротьбу з кіберзлочинністю, посилення відповідальності за дії, які шкодять цифровим правам громадян і цілісності інформаційного простору держави.

У сучасних умовах надзвичайно важливо не лише виявляти і карати порушення, а й створювати ефективну систему профілактики, що включає правову освіту, підвищення рівня обізнаності користувачів про свої права і обов'язки, а також вдосконалення механізмів контролю й моніторингу у сфері інформаційної безпеки.

Таким чином, юридична відповідальність за порушення інформаційного законодавства є ключовим інструментом забезпечення інформаційної безпеки в Україні. Вона сприяє формуванню правової культури у сфері цифрової комунікації, зменшенню ризиків інформаційних загроз та забезпеченню ефективного функціонування правової держави в умовах інформаційного суспільства.

РОЗДІЛ 4. ПЕРСПЕКТИВИ РОЗВИТКУ ІНФОРМАЦІЙНОГО ПРАВА В УКРАЇНІ

4.1. Інформаційне право в цифрову епоху

Цифрові технології різко змінили кожен сферу суспільного життя, від економіки та освіти до особистого та національного управління комунікаціями, а інформація стала стратегічним ресурсом у XXI столітті. У цьому контексті інформаційне право особливо важливо, оскільки це галузь, яка регулює правові відносини в інформаційній сфері. Його розробка відповідає на проблеми, викликані глобальною цифровізацією, масовим використанням Інтернету, штучного інтелекту, великими даними та соціальними мережами.

У цифрову епоху межі управління інформаційними потоками значно ускладнилися. Інформаційні загрози, такі як дезінформація, кібератаки та витік персональних даних, поширені з безпрецедентною швидкістю, а користувачі залишаються не лише споживачами, а й творцями контенту. Крім того, сучасне інформаційне право має не лише фіксувати правила обігу інформації, а й забезпечити ефективний механізм захисту особистих, суспільних і державних інтересів у цифровому середовищі.

Серед ключових аспектів інформаційного права в цифрову епоху — регулювання доступу до публічної інформації, захист персональних даних, запобігання кіберзлочинності, встановлення правового режиму для електронних ресурсів, цифрового контенту та інтернет-платформ. Особливої ваги набуває питання цифрових прав людини, зокрема права на приватність, свободу слова в інтернеті та захист від цифрової дискримінації [9].

Національне законодавство України поступово оновлюється відповідно до цих викликів. Закони «Про інформацію», «Про захист персональних даних», «Про електронні довірчі послуги», «Про кібербезпеку» відображають прагнення держави інтегрувати європейські правові стандарти в інформаційну сферу.

Водночас глобальні технологічні зміни потребують гнучкого, динамічного й міждисциплінарного підходу до формування правової політики.

Отже, у цифрову епоху інформаційне право є більше, ніж просто сферою регулювання. Це інструмент також для збереження балансу між технологічними досягненнями та збереженням прав людини, між відкритістю інформаційного простору та безпекою суспільства. Розвиток цього сектора є досягненням якості демократичних процесів і правової безпеки держави в цифровій реальності.

4.2. Гармонізація українського законодавства з міжнародними стандартами

У контексті європейської інтеграції Україна активно працює над гармонізацією свого інформаційного законодавства з міжнародними нормами, зокрема з правом Європейського Союзу. Це передбачає адаптацію національних актів до таких документів, як Загальний регламент про захист даних (GDPR), Конвенція №108 Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних, а також до принципів свободи вираження та доступу до інформації, викладених у міжнародних правозахисних інструментах [3].

Ключовими напрямками гармонізації є захист персональних даних, кібербезпека, боротьба з кіберзлочинністю, забезпечення прозорості діяльності органів влади та захист цифрових прав людини. Таким чином, прийнявши закони «Про захист персональних даних», «Про доступ до публічної інформації» та оновлення Закону «Про інформацію» свідчать про поступове наближення України до європейських стандартів.

Але гармонізація — це не просто формальне узгодження законів, це також реальне впровадження правових механізмів, що потребують професійного підходу, навчання кадрів і зміцнення організацій. Зміцнення правового захисту

громадян в інформаційному суспільстві вимагає успішної інтеграції в міжнародний правовий простір.

4.3. Проблемні питання та шляхи їх вирішення

Інформаційне право в Україні, як і в багатьох інших країнах, розвивається в умовах стрімкої цифровізації, глобалізації та технологічних змін. Незважаючи на певні досягнення в законотворчості та впровадженні цифрових стандартів, ця галузь залишається однією з найбільш динамічних і водночас проблемних у національній правовій системі. Існує низка актуальних викликів, які потребують законодавчого, організаційного та концептуального вирішення.

Однією з головних проблем є фрагментарність та нестабільність законодавства в інформаційній сфері. Закони часто ухвалюються ситуативно, без комплексного бачення або у відриві від уже чинних нормативних актів. Як наслідок — виникають колізії, правова невизначеність та труднощі в реалізації інформаційних прав і обов'язків. Наприклад, питання щодо визначення статусу електронних доказів, хмарних сервісів, цифрової ідентифікації або обробки великих даних досі залишаються недостатньо врегульованими.

Ще одним серйозним викликом є низький рівень захисту персональних даних. Попри наявність відповідного закону, Україна лише частково відповідає вимогам Загального регламенту ЄС про захист даних (GDPR). Відсутність ефективного нагляду за обробкою персональних даних, слабка відповідальність за порушення, а також недостатня обізнаність громадян про свої цифрові права посилюють ризики зловживань у цій сфері.

Кібербезпека та протидія кіберзлочинності також залишаються критично важливими проблемами. З одного боку, держава ухвалила Закон України «Про основні засади забезпечення кібербезпеки», однак рівень захищеності державних інформаційних систем, бізнесу та громадян ще далекий від

належного. У законодавстві часто бракує чітких технічних вимог, єдиних стандартів безпеки та узгоджених процедур реагування на інциденти [14].

Проблема доступу до публічної інформації також залишається актуальною. Хоча законодавство гарантує відкритість органів влади, на практиці реалізація цього права стикається з бюрократичними перепонами, затягуванням відповідей, відмовами під формальними приводами. Особливо це стосується журналістських запитів та громадського контролю.

Для вирішення зазначених проблем доцільно вжити таких законодавчих і практичних заходів:

1. Комплексна кодифікація інформаційного законодавства, зведення його в єдину систему, що охоплює базові поняття, принципи, види інформації, правовий режим та відповідальність.
2. Гармонізація із міжнародними стандартами, насамперед із законодавством Європейського Союзу в сфері персональних даних, конфіденційності, кібербезпеки та цифрових прав.
3. Підвищення цифрової грамотності громадян, у тому числі правової, через освітні програми, онлайн-курси, соціальні ініціативи.
4. Посилення спроможності державних органів, відповідальних за контроль у сфері інформаційного права (наприклад, Уповноваженого з прав людини у сфері захисту персональних даних).
5. Розвиток електронного урядування як способу спрощення доступу громадян до інформаційних ресурсів та підвищення прозорості діяльності влади.

Отже, проблематика інформаційного права в Україні є складною, але вирішуваною. Ефективна модернізація цієї сфери потребує не лише правових реформ, а й усвідомлення ролі інформації як стратегічного ресурсу, від якого залежить демократичний розвиток, національна безпека та права людини в цифровому світі [10].

ВИСНОВКИ

Ми живемо в епоху інформації. Знання, дані, цифрові потоки — усе це стало не лише частиною повсюдного життя, але й ключовим ресурсом для влади, бізнесу, науки та культури. Україна, як і більшість демократичних країн, стикається з проблемою захисту прав громадян в умовах стрімкої цифровізації, а також контролю над інформаційними процесами. Інформаційне право має важливе значення саме в цьому контексті.

У процесі дослідження інформаційного права України було з'ясовано, що ця галузь права є порівняно новою, динамічною та критично важливою для функціонування інформаційного суспільства та правової держави. Інформаційне право регулює правовідносини, що виникають у сфері створення, збирання, обробки, зберігання, поширення та захисту інформації, а також гарантує дотримання прав людини на інформацію.

Інформаційне право — це більше, ніж просто правила, що регулюють доступ і захист персональних даних. Це система юридичних механізмів, спрямованих на підтримку балансу між розвитком технологій і прав людини, відкритістю держави та безпекою суспільства, свободою слова та відповідальністю за її зловживання.

На жаль, інформаційне право в Україні усе ще перебуває на етапі становлення. Попри наявність окремих законів — таких як «Про інформацію», «Про доступ до публічної інформації», «Про захист персональних даних», — наша країна стикається з низкою проблем. Серед них: фрагментарність законодавства, колізії між нормативними актами, слабкий контроль за дотриманням прав у цифровому середовищі. Наприклад, українське законодавство ще не повною мірою готове до викликів, пов'язаних із розвитком штучного інтелекту, Big Data чи навіть масовим поширенням фейкових новин.

Проблема захисту персональних даних також залишається складною. Користуючись соціальними мережами чи мобільними застосунками, багато

людей навіть не бачать, що розголошують конфіденційні дані. При цьому майже немає засобів контролю та правозастосування.

Тим не менше, в цій сфері відбуваються позитивні зміни. Україна активно впроваджує електронне урядування та цифрові сервіси, такі як застосунок «Дія», і працює над дотриманням європейських стандартів законодавства. такі проекти створюють основу для створення сучасного та ефективного інформаційного права. Важливо, щоб ці зміни були реальними, відповідали потребам людей і спиралися на досвід розвинених країн.

Таким чином, інформаційне право України є не лише юридичним терміном, а й показником нашої готовності до життя в цифровому світі. Якість побудови цієї галузі важлива для безпеки країни, а також для права кожного з нас на інформацію, приватність і свободу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Антонюк П. Протидія дезінформації в Україні: законодавчі ініціативи. Право і тех. регулювання. 2023. № 2. С. 35–40.
2. Буроменський М. Право на інформацію : монографія. Київ : Юрид. думка, 2019. 368 с.
3. Гайдук Л. Особливості правового регулювання обігу відкритих даних. Інформ. технології і право. 2022. № 3. С. 10–15.
4. Гуменюк І. Захист персональних даних в Україні: проблеми та перспективи. Право України. 2021. № 9. С. 35–42.
5. Данілевська В. Інформаційне право в умовах цифровізації: виклики сьогодення. Право і суспільство. 2023. № 4. С. 76–82.
6. Кириченко О. Становлення та розвиток інформаційного законодавства в Україні. Держ. управління: теорія і практика. 2023. № 1. С. 35–41.
7. Красноступ Н. Інформаційне право: міжнародні стандарти і національні реалії. Юридичний часопис. 2023. № 4. С. 22–27.
8. Кучеренко І. Інформаційне право України : навч. посіб. Харків : Право, 2020. 272 с.
9. Липинський В. Інформаційне право України: проблеми формування і розвитку. Юрид. вісн. України. 2023. № 5. С. 14–19.
10. Махиня О. Інформаційні відносини в умовах воєнного стану: правові виклики. Юрид. наука. 2023. № 3. С. 67–73.
11. Мельник Р. Проблеми правового забезпечення доступу до публічної інформації. Публічне право. 2022. № 4. С. 88–94.
12. Носенко Ю. Електронна демократія як складова інформаційного суспільства. Вісн. НАДУ. 2022. № 3. С. 56–61.
13. Олійник Ю. Інформаційна політика держави: сучасні тенденції та загрози. Наук. записки Ін-ту законодавства ВРУ. 2023. № 1. С. 17–24.

- 14.Панова І. Правове регулювання обігу інформації в мережі Інтернет. Інформ. право. 2022. № 1. С. 12–17.
15. Петренко О. Захист прав суб'єктів персональних даних в Україні. Електронне правосуддя. 2022. № 6. С. 14–19.
- 16.Петухов В. Проблеми захисту інформаційних прав у цифровій трансформації. Юрид. вісн. 2023. № 2. С. 45–52.
- 17.Савчин М. Інформаційне право : навч. посіб. Київ : Юрінком Інтер, 2021. 320 с.
18. Селезньова О.М. Інформаційні права: теоретичні та системні положення. Інформація і право. № 3(30)/2019. С. 9-15.
19. Сидоренко Н. Правове регулювання діяльності ЗМІ в умовах воєнного стану. Юридичний огляд. 2023. № 4. С. 30–36.
20. Тищенко Д. Цифрові права людини в умовах гібридної війни. Інформ. безпека. 2023. № 2. С. 51–57.
21. Хряпченко В.П. Розуміння комплексних галузей українського права. Науковий вісник Ужгородського національного університету. Серія ПРАВО. 2016. Випуск 36. Том 1. С. 27–32.
22. Швидка К. Проблеми захисту конфіденційної інформації у правовому полі України. Право і безпека. 2023. № 2. С. 38–44.
- 23.Шевчук С. Свобода вираження поглядів і право на інформацію : практ. ЄСПЛ. Київ : Фенікс, 2022. 200 с.