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

КУРСОВА РОБОТА

з дисципліни: «ІНФОРМАЦІЙНЕ ПРАВО»

за темою: **«ІНФОРМАЦІЙНІ СИСТЕМИ ЯК ОБ'ЄКТИ ІНФОРМАЦІЙНОГО ПРАВА»**

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

Оцінка: _____
Національна шкала_____
Кількість балів: _____ ECTS _____

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

м. Чернігів 2026

ЗМІСТ

ВСТУП

Актуальність теми. Глобальна цифровізація всіх аспектів людської життєдіяльності зумовила фундаментальні зміни в архітектурі сучасного права. В умовах формування інформаційного суспільства традиційні правові інститути зазнають суттєвої трансформації, пристосовуючись до реалій віртуального простору та електронної взаємодії. Центральним об’єктом, навколо якого концентруються нові типи суспільних відносин, є інформаційна система (ІС). Сьогодні інформаційні системи перестали бути виключно технічним інструментарієм і перетворилися на складну правову категорію, що виступає базисом для реалізації державних функцій, ведення бізнесу та забезпечення конституційних прав громадян.

Для України питання правового регулювання інформаційних систем набуло особливої гостроти у зв’язку з курсом на розбудову «держави у смартфоні». Впровадження таких масштабних проєктів, як портал «Дія», електронні реєстри речових прав, системи електронного документообігу та хмарні технології в державному управлінні, потребує чіткого визначення юридичної природи ІС. Відсутність уніфікованого підходу до розуміння інформаційної системи як об’єкта інформаційного права створює ризики для правозастосовної практики, особливо в питаннях захисту персональних даних, кібербезпеки та визначення відповідальності за збої в роботі критичних систем [4, с. 12].

Окрім того, воєнний стан в Україні актуалізував потребу в посиленому правовому режимі захисту державних інформаційних ресурсів. Інформаційні системи стали фронтиром кібервійни, що вимагає від юридичної науки розробки нових механізмів гарантування цілісності та доступності даних. Саме тому дослідження інформаційних систем як об’єктів інформаційного права є надзвичайно актуальним, адже воно дозволяє систематизувати знання про правову природу цифрових активів та запропонувати шляхи

вдосконалення вітчизняного законодавства відповідно до європейських стандартів [12, с. 45].

Мета дослідження полягає у проведенні комплексного теоретико-правового аналізу інформаційних систем як об’єктів інформаційного права, вивченні їхньої внутрішньої структури, класифікації та особливостей правового режиму функціонування в умовах сучасних технологічних викликів.

Для досягнення поставленої мети необхідно вирішити такі **завдання:**

- сформулювати науково обґрунтоване поняття інформаційної системи як юридичної категорії та виокремити її сутнісні ознаки.
- провести розгалужену класифікацію інформаційних систем за різними правовими критеріями (формою власності, рівнем доступу, призначенням).
- визначити правове співвідношення інформаційної системи з суміжними об’єктами, такими як бази даних та мережі зв’язку.
- дослідити специфіку правового статусу державних та приватних інформаційних систем.
- проаналізувати міжнародно-правові стандарти (зокрема норми ЄС) у сфері функціонування глобальних інформаційних систем.
- охарактеризувати правовий режим захисту інформації в інформаційно-комунікаційних системах, зокрема процедуру створення та сертифікації КСЗІ.
- визначити коло суб’єктів правовідносин у сфері експлуатації систем та види юридичної відповідальності за порушення встановленого порядку їх роботи.

Об’єкт дослідження – це сукупність суспільних правовідносин, що виникають, змінюються та припиняються у зв’язку зі створенням, впровадженням, експлуатацією та захистом інформаційних систем у правовому просторі України та світу.

Предмет дослідження – норми чинного інформаційного законодавства, міжнародні договори, теоретичні напрацювання вчених-юристів, а також правовий режим інформаційних систем як об’єктів правового регулювання [7, с. 88].

Методи дослідження. Методологічну основу роботи складає діалектичний метод пізнання суспільних явищ у їх розвитку та взаємозв’язку. У процесі написання роботи використано такі методи:

Логіко-семантичний метод – для уточнення понятійного апарату та визначення терміна «інформаційна система».

Системно-структурний метод – при дослідженні внутрішньої будови ІС та її зв’язків із базами даних.

Порівняльно-правовий метод – для аналізу узгодженості українського законодавства з європейським Регламентом GDPR [20, с. 305].

Статистичний та метод аналізу документів – при вивченні стану кібербезпеки та практики впровадження державних реєстрів.

Наукова новизна роботи полягає у спробі системно поєднати техніко-технологічні параметри інформаційних систем із їхнім правовим наповненням, розглядаючи ІС не просто як засіб обробки даних, а як середовище реалізації суб’єктивних прав особи.

Джерельна база дослідження. Теоретичну основу роботи становлять праці провідних фахівців у сфері інформаційного права, таких як І. Арістова, К. Бєляков, В. Пилипчук, В. Цимбалюк та М. Швець. Нормативну базу складають Конституція України, Закони України «Про інформацію», «Про захист інформації в інформаційно-комунікаційних системах», «Про основні засади забезпечення кібербезпеки України», а також підзаконні акти Кабінету Міністрів України та Держспецзв’язку [5, с. 18; 19, с. 210].

Структура роботи. Курсова робота складається зі вступу, трьох розділів (кожен з яких містить три підрозділи), висновків та списку використаних джерел. Загальний обсяг роботи 35 сторінок.

РОЗДІЛ 1. ТЕОРЕТИКО-ПРАВОВІ ЗАСАДИ ВИЗНАЧЕННЯ ІНФОРМАЦІЙНИХ СИСТЕМ

1.1. Поняття та сутнісні ознаки інформаційної системи як юридичної категорії

Сучасний етап розвитку правової науки характеризується інтенсивним впровадженням цифрових технологій у всі сфери суспільного життя. Центральним об’єктом, навколо якого виникають нові типи правовідносин, є інформаційна система (ІС). У правовому аспекті ІС перестала бути суто технічною категорією, що описує взаємодію комп’ютерного обладнання, і трансформувалася у складний юридичний об’єкт, що потребує чіткої дефініції та правового регламенту.

Згідно з базовим законодавством України, зокрема Законом «Про інформацію», інформаційна система визначається як організаційно впорядкована сукупність документів (масивів документів) та інформаційних технологій, у тому числі з використанням засобів обчислювальної техніки і зв’язку, що реалізують інформаційні процеси [4, с. 12]. Таке визначення підкреслює двоєдину природу ІС: з одного боку, це змістовне наповнення (інформація, документи), з іншого – інструментарій для її обробки (технології та техніка).

Досліджуючи юридичну природу ІС, необхідно звернутися до наукових поглядів Пилипчука В. Г., який зазначає, що інформаційна система в інформаційному праві виступає не лише як засіб праці, а як середовище, у якому реалізуються права та обов’язки суб’єктів [14, с. 56]. Це означає, що правове регулювання спрямоване не на самі мікросхеми чи програмний код, а на порядок доступу, захисту та використання даних, що циркулюють у системі.

Ключові юридичні ознаки інформаційної системи:

1. Організаційна впорядкованість.

Система не є хаотичним набором даних. Вона має структуру, визначену власником або законодавцем. Кожен елемент системи (база даних, інтерфейс, канали зв’язку) має своє функціональне призначення.

2. Цілісність.

Попри складність структури, ІС діє як єдиний механізм. Порушення роботи одного сегмента (наприклад, серверної частини) призводить до неможливості реалізації інформаційного права користувачем у повному обсязі [7, с. 88].

3. Наявність мети функціонування.

Будь-яка юридично значуща ІС створюється для досягнення конкретного результату: надання державних послуг, ведення обліку, забезпечення безпеки чи комерційної діяльності.

4. Технологічність.

Використання інформаційних технологій є обов’язковим елементом. У правовому полі це означає необхідність дотримання стандартів сумісності та протоколів передачі даних [18, с. 210].

Важливо розглянути ІС через призму теорії об’єктів права. На думку Бєлякова К. І., інформаційна система як об’єкт інформаційного права має «гібридний» характер. Вона одночасно поєднує в собі ознаки об’єкта інтелектуальної власності (програмне забезпечення), речового права (сервери, мережі) та специфічного інформаційного об’єкта (бази даних) [7, с. 91]. Така багатогранність створює певні труднощі у правозастосуванні, особливо при визначенні відповідальності за збої в роботі системи.

Окремої уваги заслуговує еволюція законодавчого підходу до термінології. Якщо у 90-х роках акцент робився на «автоматизованих системах», то сучасне законодавство оперує терміном «інформаційно-комунікаційна система» (ІКС), що відображає нерозривний зв’язок між обробкою даних та їх передачею мережами зв’язку [5, с. 18]. Це розширює

коло суб'єктів, включаючи провайдерів та операторів телекомунікацій до правовідносин щодо функціонування ІС.

Розглядаючи сутність ІС, неможливо оминути питання її правового статусу як джерела доказів у судочинстві. Дані, що зберігаються в ІС, за умови дотримання процедур цілісності та аутентичності, набувають юридичної сили. Як зазначає Швець М. Я., інформатизація правозастосовної діяльності вимагає від ІС високого ступеня верифікації інформації, що автоматично робить «надійність системи» її юридично обов'язковою характеристикою [20, с. 400].

Юридична категорія «інформаційна система» також тісно пов'язана з поняттям інформаційного ресурсу. Система є формою існування ресурсу. Без системи ресурс залишається статичним, а без ресурсу система втрачає свою змістовну цінність. Соснін О. В. вказує, що управління інформаційними ресурсами в державі можливе лише через розвинену мережу державних інформаційних систем, які мають статус національного надбання [16, с. 280].

Системні ознаки ІС у контексті публічного права:

Легітимність. Для державних ІС це обов'язкове створення на основі закону або акту уряду.

Публічність. Обов'язок системи забезпечувати доступ громадян до суспільно важливої інформації.

Підконтрольність. Наявність державних органів, що здійснюють нагляд за дотриманням правил експлуатації системи та захисту персональних даних у ній [13, с. 240].

На сучасному етапі ІС також розглядається як інструмент реалізації електронної демократії. Право на доступ до інформаційної системи стає одним із фундаментальних прав людини в цифрову епоху. Костецька Т. О. зауважує, що обмеження доступу до державних ІС без законних підстав може розцінюватися як порушення конституційних прав громадян [10, с. 145].

Таким чином, підсумовуючи аналіз поняття та ознак інформаційної системи як юридичної категорії, можна контувати, що це складний правовий інститут. ІС не є просто «електронним архівом»; це динамічний об'єкт права,

що охоплює технічні, змістовні та процедурні елементи. Юридичне визначення ІС дозволяє чітко розмежувати відповідальність між розробником, власником та користувачем, а також встановити правовий режим інформації, яка в ній обробляється. Подальший розвиток цього поняття пов'язаний із впровадженням систем штучного інтелекту, що додасть ІС ознак автономності суб'єкта, проте на даному етапі ІС залишається об'єктом, що перебуває під повним правовим контролем людини та держави [12, с. 45; 19, с. 92].

1.2. Класифікація інформаційних систем в інформаційному праві

Класифікація інформаційних систем (ІС) є фундаментальним елементом інформаційного права, оскільки від належності системи до певної групи залежить вибір правового режиму її функціонування, обсяг прав власника та рівень державного контролю. Наукова та законодавча класифікація дозволяє структурувати різнорідні технологічні об'єкти у зрозумілу юридичну систему [12, с. 45].

1. Класифікація за формою власності та суб'єктом створення.

Це ключовий поділ, що визначає джерела фінансування та мету існування системи:

Державні інформаційні системи. Створюються за кошти державного бюджету для реалізації функцій держави (наприклад, Реєстр речових прав). Їх правовий статус жорстко регламентований, а інформація в них часто має статус офіційної [1, с. 215].

Комунальні інформаційні системи. Належать місцевим громадам і забезпечують функціонування органів місцевого самоврядування (міські системи «Smart City», реєстри територіальних громад).

Приватні (корпоративні) інформаційні системи. Створюються фізичними або юридичними особами для власних потреб. Правовий режим тут

базується на принципах приватної власності та свободи договору, проте з обмеженнями щодо захисту персональних даних [10, с. 74].

2. Класифікація за рівнем доступу до інформації. Юридичне значення цієї класифікації полягає у визначенні кола осіб, які мають право взаємодіяти з системою:

Відкриті (загальнодоступні) системи. Призначені для надання інформації необмеженому колу осіб (наприклад, веб-портали відкритих даних).

Системи з обмеженим доступом. До них належать ІС, що містять конфіденційну інформацію, державну таємницю або службові дані. Доступ до таких систем суворо персоніфікований та потребує спеціальних дозволів [13, с. 240].

Системи колективного користування. Передбачають доступ певної групи осіб (наприклад, внутрішні мережі міністерств).

3. Класифікація за територіальним охопленням.

Локальні. Функціонують у межах однієї будівлі чи одного підприємства.

Регіональні. Охоплюють область або окремий адміністративний район.

Державні (національні). Діють на всій території України (наприклад, система «Трембіта»).

Транскордонні (глобальні). Забезпечують обмін даними між суб’єктами різних держав, що потребує узгодження з нормами міжнародного права [20, с. 305].

4. Класифікація за функціональним призначенням.

Особливе місце в сучасних умовах посідають **автоматизовані системи надання адміністративних послуг**. Вони є інструментом реалізації сервісної держави. Юридична специфіка таких систем полягає у тому, що результат їхньої роботи (автоматично сформована довідка чи витяг) має юридичну силу

акта органу влади [18, с. 210]. Також виділяють довідково-інформаційні, експертні (із елементами ШІ) та розрахункові системи.

Згідно з Пилипчуком В. Г., правова класифікація повинна також враховувати рівень критичності системи для національної безпеки. Об’єкти критичної інформаційної інфраструктури виділяються в окрему категорію з особливими вимогами до кіберзахисту та відсутності іноземного впливу на програмне забезпечення [14, с. 160].

1.3. Співвідношення інформаційної системи з суміжними об’єктами

Для чіткого правозастосування необхідно розмежовувати «інформаційну систему» та об’єкти, що входять до її складу або забезпечують її роботу. У юридичній науці часто виникає змішування цих понять, що призводить до помилок при кваліфікації правопорушень або визначенні авторських прав [7, с. 88].

1. ІС та бази даних (БД).

База даних – це іменована сукупність даних, що відображає стан об’єктів та їх часток у певній предметній області. Якщо ІС – це «завод» (верстати, логістика, правила), то БД – це «сировина та готова продукція».

Правовий аспект: База даних як об’єкт авторського права охороняється за критерієм оригінальності підбору та розташування даних. Інформаційна система ж охороняється як складний об’єкт, що включає програмний код, алгоритми та організаційні регламенти [11, с. 215].

Розмежування режимів: Власник системи та власник інформації в базі даних можуть бути різними особами. Наприклад, держава є власником реєстру (ІС), але персональні дані в ній належать фізичним особам (суб’єктам даних) [10, с. 180].

2. ІС та мережі передачі даних.

Мережа – це сукупність засобів зв’язку та каналів, що забезпечують транспортування сигналу. Інформаційна система використовує мережу як транспортний рівень.

Правова відповідальність: Провайдер мережі зазвичай не несе відповідальності за контент, що передається, якщо він не є його ініціатором. Натомість володілець ІС відповідає за цілісність та доступність даних усередині системи [19, с. 210]. Розмежування відбувається по «точці входу» в систему.

3. ІС та програмні продукти.

Програма для ЕОМ є технічним «рушієм» системи. Проте ІС ширша за поняття програми, оскільки включає в себе регламенти взаємодії персоналу, технічне обладнання та юридично визначені процедури обробки. Як зазначає Бєляков К. І., програма стає частиною ІС лише в момент її впровадження та сертифікації для конкретних правових цілей [7, с. 95].

4. Системний зв’язок об’єктів.

Сучасне інформаційне право розглядає ІС як **інтегративний об’єкт**. Це означає, що зміна правового режиму одного елемента (наприклад, надання базі даних статусу «державна таємниця») автоматично змінює режим всієї системи (вимоги до обладнання мережі, допуску персоналу, використання шифрування) [6].

Цимбалюк В. С. підкреслює, що в межах ІС виникає особливий правовий феномен – «технологічна цілісність», де правовий режим об’єкта обробки (даних) диктує технічні вимоги до об’єкта-інструмента (системи) [19, с. 210]. Наприклад, при обробці персональних даних система зобов’язана мати атестат відповідності КСЗІ, що є правовою вимогою до технічного об’єкта на основі природи інформації.

Таким чином, розмежування ІС із суміжними об’єктами дозволяє:

Правильно визначити суб’єкта відповідальності (власник мережі чи власник системи).

Ефективно захистити інтелектуальну власність розробників програмного забезпечення.

Встановити адекватний режим безпеки залежно від цінності даних у системі [8, с. 190].

РОЗДІЛ 2. ПРАВОВИЙ РЕЖИМ ОКРЕМИХ ВИДІВ ІНФОРМАЦІЙНИХ СИСТЕМ

2.1. Державні інформаційні системи та реєстри: правовий статус та призначення

Державні інформаційні системи (ДІС) та державні реєстри є фундаментом сучасного цифрового управління в Україні. У системі об’єктів інформаційного права вони посідають особливе місце, оскільки їх функціонування безпосередньо пов’язане із реалізацією владних повноважень, забезпеченням прав громадян та національною безпекою. Юридична природа цих систем визначається їх публічним призначенням: вони створюються не для отримання прибутку, а для впорядкування суспільних відносин та надання офіційного статусу певним даним [15, с. 132].

Правові підстави створення та правосуб'єктність.

На відміну від приватних систем, які можуть створюватися за ініціативою будь-якої особи, державна інформаційна система завжди має нормативну першооснову. Вона створюється виключно на підставі закону або акта Кабінету Міністрів України, що визначає її назву, мету, обсяг даних та коло відповідальних осіб [2, с. 5].

У правовідносинах щодо ДІС виділяють три ключові ролі суб’єктів:

1. **Власник (Володілець).** Власником таких систем завжди виступає держава в особі уповноваженого органу. Держава володіє як програмно-технічним комплексом, так і сукупністю інформації (інформаційним ресурсом).

2. **Держатель.** Це орган державної влади, на який покладено обов’язок щодо нормативно-правового, організаційного та методологічного забезпечення функціонування системи. Держатель відповідає за достовірність даних та їх актуальність [1, с. 215].

3. **Адміністратор (Технічний адміністратор).** Як правило, це державне підприємство, що здійснює технічне обслуговування, захист інформації та програмний супровід системи.

Функціональне призначення державних реєстрів. Державні реєстри як різновид ІС виконують функцію «юридичної пам’яті» суспільства. Їх призначення полягає у:

Легітимації прав та фактів. Наприклад, право власності на нерухомість виникає саме з моменту внесення запису до реєстру.

Інформаційному забезпеченні управління. Надання органам влади актуальних даних для прийняття управлінських рішень.

Забезпеченні прозорості. Надання громадянам доступу до публічної інформації (наприклад, Реєстр декларацій).

Правовий режим ДІС базується на принципі презумпції достовірності. Інформація, що міститься у державному реєстрі, вважається істинною, доки інше не буде доведено в судовому порядку. Це покладає на держателя колосальну юридичну відповідальність за помилки або несанкціоноване втручання у систему [17, с. 225].

Режим доступу та взаємодії (Interoperability). Сучасний етап розвитку ДІС характеризується переходом до моделі взаємодії через систему «Трембіта». Правовий статус державних систем тепер включає обов’язок бути «сумісними» з іншими реєстрами. Це дозволяє реалізувати принцип *once-only* (запит даних у громадянина лише один раз), оскільки системи обмінюються інформацією автоматично за захищеними каналами зв’язку [15, с. 135].

Доступ до ДІС може бути:

Відкритим (публічним). Через портали відкритих даних (наприклад, ЄДРПОУ).

Спеціальним. Для нотаріусів, правоохоронних органів та інших суб’єктів, які мають право на отримання інформації з обмеженим доступом у зв’язку з виконанням своїх функцій.

Індивідуальним. Право громадянина отримати інформацію про себе, що зберігається в державній системі [13, с. 242].

Забезпечення безпеки та цілісності. Державні системи є пріоритетними цілями для кібератак, тому їх правовий режим включає обов'язкову наявність Атестата відповідності комплексної системи захисту інформації (КСЗІ). Як зазначає Цимбалюк В. С., відсутність такого атестата робить функціонування державної системи незаконним, а дані, отримані з неї, – сумнівними з точки зору їх юридичної сили [19, с. 90].

Окремим аспектом є **правовий статус даних в ІС під час воєнного стану**. Законодавство передбачає можливість обмеження доступу до певних реєстрів або їх тимчасове «закриття» задля уникнення витоку стратегічно важливої інформації. Це підкреслює роль ДІС не лише як сервісного інструменту, а й як елемента національної безпеки.

Проблеми та перспективи правового регулювання. Попри значний прогрес, залишається актуальною проблема дублювання даних у різних реєстрах. Розум О. М. вказує на необхідність створення «єдиного реєстру реєстрів», який би став мета-системою для впорядкування всієї державної інформаційної інфраструктури [15, с. 200]. Також вимагає уточнення правовий статус «автоматичних рішень», прийнятих інформаційними системами без участі чиновника (алгоритмічне управління), що ставить нові виклики перед адміністративним правом.

Підсумовуючи, державні інформаційні системи та реєстри є специфічними об'єктами інформаційного права, правовий режим яких характеризується:

1. Публічно-правовим характером виникнення.
2. Державною власністю на систему та її ресурс.
3. Презумпцією достовірності інформації.
4. Суворим регламентом захисту та доступу.

Ефективне правове регулювання ДІС є запорукою побудови прозорого та підзвітного державного апарату, де інформаційна система виступає

гарантом захисту прав і законних інтересів кожного суб’єкта правовідносин [12, с. 48; 18, с. 350].

2.2. Правове регулювання приватних та корпоративних інформаційних систем

У сучасному ринковому середовищі приватні та корпоративні інформаційні системи (ПІС) є невід’ємним інструментом ведення бізнесу, управління активами та взаємодії з клієнтами. На відміну від державних систем, правовий режим яких базується на нормах публічного права, приватні системи функціонують переважно в полі приватного (цивільного та господарського) права. Проте стратегічне значення інформації зумовлює поступове втручання держави у регулювання приватного сектору, особливо в питаннях безпеки та захисту прав людини [10, с. 74].

Цивільно-правові засади створення та володіння. Фундаментом правового регулювання ПІС є право власності. Згідно з Цивільним кодексом України, інформаційна система як складний об’єкт може належати фізичній або юридичній особі на правах приватної власності. Власник самостійно визначає архітектуру системи, перелік програмного забезпечення та мету її використання.

Договірне регулювання. Створення ПІС зазвичай оформлюється договорами на розробку програмного забезпечення, купівлі-продажу обладнання або ліцензійними угодами. Важливим аспектом є визначення моменту переходу майнових прав на систему від розробника до замовника [7, с. 95].

Корпоративний регламент. У межах юридичної особи функціонування системи регулюється внутрішніми локальними актами: положеннями про інформаційну безпеку, посадовими інструкціями

адміністраторів та правилами користування корпоративною мережею [11, с. 215].

Приватні системи та захист персональних даних. Найбільш жорстким елементом державного регулювання ПІС є контроль за обробкою персональних даних (ПД). Якщо приватна система (наприклад, база клієнтів інтернет-магазину або CRM-система банку) містить дані про фізичних осіб, вона автоматично стає об’єктом перевірок з боку Уповноваженого Верховної Ради з прав людини.

Правовий обов’язок володільця. Власник приватної системи зобов’язаний забезпечити технічний і організаційний захист даних, що унеможливлює їх витік або несанкціоновану зміну [4, с. 15].

Згода суб’єкта. Правовим режимом ПІС передбачено, що будь-яка обробка даних у системі має здійснюватися лише за добровільною згодою особи, крім випадків, визначених законом [13, с. 240].

Режим комерційної таємниці та конфіденційності. Для корпоративних систем критично важливим є правовий захист інформації, що становить комерційну таємницю. ПІС часто використовуються для зберігання ноу-хау, стратегій розвитку та фінансових планів. Юридичне регулювання тут полягає у встановленні власником спеціального режиму доступу. Порушення працівником правил роботи в такій системі тягне за собою цивільно-правову або навіть кримінальну відповідальність за розголошення таємниці [3, с. 402; 8, с. 190].

Державний нагляд та «критичні» приватні системи. Сучасне інформаційне право виділяє категорію приватних систем, що мають суспільне значення. Це системи банківської сфери, енергетики, телекомунікацій. Попри приватну форму власності, держава встановлює для них спеціальні вимоги:

1. **Обов’язковий кіберзахист.** Якщо приватна система віднесена до об’єктів критичної інфраструктури, її власник зобов’язаний взаємодіяти з Держспецзв’язку та дотримуватися встановлених стандартів безпеки [18, с. 350].

2. **Ліцензування.** Певні види діяльності (наприклад, надання послуг електронного підпису) вимагають використання лише сертифікованих інформаційних систем [5, с. 20].

Аутсорсинг та хмарні технології (Cloud Computing). Особливим викликом для правового регулювання є використання приватними компаніями хмарних інформаційних систем, сервери яких можуть перебувати за межами України. У такому разі виникають складні правовідносини транскордонної передачі даних. Костецька Т. О. зазначає, що відповідальність за збереження даних у хмарній ПІС все одно несе власник системи (замовник послуг), незалежно від місця розташування серверів провайдера [10, с. 180].

Співвідношення приватного інтересу та публічного контролю. Правове регулювання ПІС балансує між правом власника на вільне використання свого майна та обов’язком держави захищати публічний порядок. Наприклад, правоохоронні органи за рішенням суду можуть отримати доступ до приватної ІС у межах кримінального провадження. Це обмеження права власності на систему є законним в інтересах правосуддя [2, с. 10].

Отже, приватні та корпоративні інформаційні системи – це об’єкти, правовий режим яких є змішаним. З одного боку, вони є інструментами реалізації приватної ініціативи та права власності, що регулюється Цивільним кодексом. З іншого боку, через інтеграцію ПІС у глобальний інформаційний простір та обробку великих масивів даних, вони підпадають під регуляторний вплив інформаційного права в частині захисту персональних даних, кібербезпеки та взаємодії з державою [12, с. 50; 14, с. 162].

2.3. Міжнародно-правові стандарти функціонування глобальних інформаційних систем

Процеси глобалізації та цифровізації призвели до стирання фізичних кордонів у сфері обміну інформацією. Глобальні інформаційні системи (ГІС), такі як транснаціональні банківські мережі, соціальні медіа-платформи та хмарні сховища великих даних, функціонують у позатериторіальному просторі. Це створює складні правові виклики щодо визначення юрисдикції, застосовного права та стандартів безпеки. Правовий режим ГІС сьогодні визначається не лише національним законодавством, а й розгалуженою системою міжнародних договорів, конвенцій та технічних стандартів [20, с. 305].

Європейський вектор: GDPR як «золотий стандарт». Найбільш впливовим міжнародно-правовим інструментом, що регулює роботу глобальних інформаційних систем, є Загальний регламент про захист даних (GDPR), прийнятий Європейським Союзом. Його унікальність полягає в екстериторіальній дії: будь-яка інформаційна система, незалежно від місця реєстрації її власника (США, Китай чи Україна), підпадає під дію Регламенту, якщо вона обробляє дані громадян ЄС.

Принципи «Privacy by Design» та «Privacy by Default». Згідно з міжнародними стандартами, інформаційна система повинна бути спроєктована таким чином, щоб захист приватності був її невід'ємною технічною характеристикою, а не додатковою функцією [10, с. 182].

Правовий режим транскордонної передачі. Глобальні системи часто використовують сервери в різних країнах. Міжнародне право вимагає, щоб країна-отримувач даних забезпечувала «адекватний рівень захисту», що підтверджується рішеннями Єврокомісії або спеціальними договірними застереженнями [20, с. 308].

Технічна стандартизація як правовий інструмент. Оскільки ГІС мають складну технічну структуру, їх правове регулювання неможливе без

посилання на міжнародні стандарти ISO/IEC. Зокрема, стандарт ISO/IEC 27001 (Системи управління інформаційною безпекою) є юридично визнаним орієнтиром для перевірки надійності глобальних систем.

Юридичне значення сертифікації. Для суб'єктів інформаційного права наявність сертифіката ISO є доказом дотримання «належної обачності» (*due diligence*). У разі витоку даних у системі, сертифікація може стати обставиною, що пом'якшує юридичну відповідальність власника ГІС [12, с. 52].

Конвенція про кіберзлочинність (Будапештська конвенція). Функціонування глобальних ІС невід'ємне від ризиків транскордонної злочинності. Конвенція Ради Європи про кіберзлочинність є основним міжнародним актом, що гармонізує кримінальне законодавство держав щодо захисту інформаційних систем. Вона встановлює обов'язок держав співпрацювати у зборі електронних доказів, що зберігаються в ГІС, та забезпечувати збереження даних на запит іноземних правоохоронних органів [3, с. 405].

Гармонізація законодавства України з міжнародними нормами. Україна, обравши шлях євроінтеграції, активно адаптує свій правовий режим ІС до стандартів ЄС. Це стосується не лише захисту персональних даних, а й впровадження норм Директиви NIS 2 щодо безпеки мережевих та інформаційних систем. Швець М. Я. зазначає, що інтеграція українських державних реєстрів у європейський інформаційний простір вимагає повної сумісності (*interoperability*) не лише на технічному, а й на правовому рівні [20, с. 402].

Проблеми «цифрового суверенітету». Розвиток глобальних систем породжує конфлікт між глобальним характером технологій та національним суверенітетом держав. Питання про те, чи може держава вимагати локалізації даних (зберігання інформації про своїх громадян виключно на серверах усередині країни), є предметом гострих міжнародних дискусій. Бєляков К. І. вказує на те, що надмірна локалізація може зашкодити функціонуванню ГІС,

проте повна відсутність контролю за транскордонними потоками створює загрози національній безпеці [7, с. 98].

Роль міжнародних організацій. Велику роль у формуванні правового режиму ГІС відіграють:

1. **ООН** (через Групи урядових експертів з питань інформаційної безпеки).
2. **ITU** (Міжнародний телекомунікаційний союз) – у сфері технічних регламентів.
3. **WIPO** (Всесвітня організація інтелектуальної власності) – у частині захисту прав на програмне забезпечення та бази даних у глобальних мережах [14, с. 165].

Таким чином, міжнародно-правові стандарти функціонування глобальних інформаційних систем є багаторівневою структурою. Вони базуються на поєднанні жорстких норм (*hard law*), таких як GDPR чи міжнародні конвенції, та м’якого права (*soft law*) у вигляді технічних стандартів та етичних кодексів. Для України дотримання цих стандартів є обов’язковою умовою для безпечного входження в глобальне інформаційне суспільство та захисту своїх інтересів у цифровому просторі [19, с. 215].

РОЗДІЛ 3. ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ТА ВІДПОВІДАЛЬНОСТІ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

3.1. Режим захисту інформації в інформаційно-комунікаційних системах

Захист інформації в інформаційно-комунікаційних системах (ІКС) є не лише технічним завданням, а критичною юридичною умовою легітимності існування та функціонування будь-якої системи, що оперує державними ресурсами або персональними даними. Правовий режим захисту інформації базується на сукупності правових норм, технічних стандартів та організаційних заходів, спрямованих на запобігання несанкціонованим діям щодо інформації та самої системи [5, с. 18].

Комплексна система захисту інформації (КСЗІ) як правовий інститут. Центральним елементом вітчизняного законодавства у цій сфері є поняття КСЗІ. Це сукупність організаційних та інженерних заходів, програмно-апаратних засобів, які забезпечують захист інформації від витоку, модифікації чи знищення.

Обов’язковість створення. Згідно із Законом «Про захист інформації в інформаційно-комунікаційних системах», створення КСЗІ є обов’язковим для всіх державних ІКС, а також для приватних систем, у яких обробляється інформація, що є власністю держави, або інформація з обмеженим доступом (включаючи персональні дані) [5, с. 19].

Правові наслідки відсутності КСЗІ. Експлуатація системи без належним чином побудованої та підтвердженої системи захисту тягне за собою юридичну нікчемність результатів обробки інформації в такій системі. Юридично це означає, що дані з такої системи не можуть бути використані як офіційні докази чи підстава для видачі державних документів [19, с. 90].

Структура режиму захисту: організаційні та технічні заходи. Безпека об’єкта права гарантується дворівневою структурою заходів, що

детально описані в наукових працях Цимбалюка В. С. та Пилипчука В. Г. [14; 19].

1. **Організаційні заходи.** Включають розробку «Політики безпеки», призначення відповідальних осіб (адміністраторів безпеки), встановлення режиму доступу до приміщень, де розташоване обладнання ІКС, та навчання персоналу. З юридичної точки зору, ці заходи закріплюються наказами керівника установи та посадовими інструкціями [13, с. 245].

2. **Технічні заходи.** Передбачають використання засобів криптографічного захисту інформації (шифрування), встановлення міжмережевих екранів (firewalls), систем виявлення вторгнень та засобів ідентифікації користувачів. Важливою умовою є те, що всі технічні засоби захисту повинні мати експертний висновок Держспецзв'язку [18, с. 352].

Процедура державної експертизи та сертифікації. Завершальним етапом створення режиму захисту є державна експертиза КСЗІ. Її мета – підтвердження того, що система захисту відповідає вимогам нормативних документів з технічного захисту інформації (НД ТЗІ).

Атестат відповідності. За результатами експертизи видається Атестат відповідності, який є юридичним дозволом на введення ІКС в промислову експлуатацію. Термін дії атестата зазвичай становить 5 років, проте він може бути анульований у разі істотних змін у конфігурації системи [11, с. 218].

Роль Держспецзв'язку. Цей орган здійснює державний контроль за станом захисту інформації. Право на перевірку систем мають лише уповноважені інспектори, а результати перевірок оформлюються відповідними актами, що мають статус адміністративних документів [12, с. 55].

Захист інформації в умовах кіберзагроз. Сучасний правовий режим ІКС враховує вимоги Закону «Про основні засади забезпечення кібербезпеки України». Відбувається інтеграція понять «технічний захист» та «кіберзахист». Для об'єктів критичної інформаційної інфраструктури вимоги до захисту є значно вищими. Зокрема, передбачено обов'язковий моніторинг

інцидентів кібербезпеки та негайне інформування про них Державного центру кіберзахисту [14, с. 160].

Ризико-орієнтований підхід. Останнім часом у юридичній практиці спостерігається перехід від жорсткого дотримання формальних вимог НД ТЗІ до ризико-орієнтованого підходу, характерного для міжнародних стандартів ISO/IEC 27001. Це дозволяє власникам приватних ІКС самостійно визначати необхідний рівень захисту на основі оцінки потенційних збитків від втрати конфіденційності, цілісності чи доступності інформації [8, с. 192].

Відповідальність за незабезпечення режиму захисту. Юридична відповідальність за неналежний захист інформації в системах може бути:

Дисциплінарною (щодо персоналу ІКС).

Адміністративною (за порушення правил захисту інформації згідно зі ст. 188-31 КУпАП).

Цивільно-правовою (відшкодування збитків користувачам системи у разі витоку їх даних).

Кримінальною (у разі службової недбалості, що призвела до тяжких наслідків у роботі критичних систем) [3, с. 405].

Отже, правовий режим захисту інформації в ІКС є динамічною системою, що поєднує в собі технічну досконалість та нормативну строгість. Створення та сертифікація КСЗІ виступає головним юридичним фільтром, який гарантує правомірність використання інформаційних систем у публічному та приватному секторах. Еволюція цього режиму спрямована на гармонізацію українських вимог із міжнародними стандартами кібербезпеки, що є необхідною умовою цифрового суверенітету держави [19, с. 212; 20, с. 405].

3.2. Суб’єкти правовідносин у сфері експлуатації інформаційних систем

Функціонування інформаційних систем (ІС) як складних об’єктів інформаційного права породжує розгалужену мережу правовідносин. Чітке визначення кола суб’єктів, їх правового статусу, компетенції та меж відповідальності є необхідною умовою забезпечення стабільності цифрового середовища. У юридичній науці та законодавстві виділяють три базові категорії суб’єктів: власник (володілець), розпорядник (адміністратор) та користувач, кожен з яких має специфічне коло прав та обов’язків [1, с. 215; 14, с. 56].

1. Власник (Володілець) інформаційної системи. Власник є ключовим суб’єктом, оскільки саме він приймає рішення про створення системи, визначає її цільове призначення та встановлює правила її експлуатації.

Власником може бути держава (в особі органів влади), юридична або фізична особа. У державних ІС власник зазвичай делегує функції управління іншим структурам, але зберігає за собою право стратегічного контролю.

Власник зобов’язаний забезпечити фінансування системи, розробити та затвердити Положення про систему, а також гарантувати створення комплексної системи захисту інформації (КСЗІ) [5, с. 19].

Власник має виключне право на розпорядження програмним забезпеченням та апаратною частиною системи, а також право визначати порядок доступу до інформаційних ресурсів для інших суб’єктів [10, с. 74].

2. Розпорядник (Держатель) та Адміністратор. Часто у правовій літературі ці поняття розмежовують. **Розпорядник** здійснює організаційне управління (визначає зміст інформації, порядок її ведення), тоді як **Адміністратор** відповідає за технічну працездатність системи.

Розпорядник забезпечує методологічну підтримку, контролює якість наповнення баз даних та розглядає запити на доступ до системи. Як зазначає

Арістова І. В., у державних реєстрах розпорядник виступає гарантом дотримання публічного інтересу [1, с. 218].

Адміністратор (часто спеціалізоване ДП або ІТ-відділ компанії) відповідає за безперебійну роботу серверів, захист від кібератак, резервне копіювання даних та надання технічної підтримки користувачам [18, с. 210].

Саме на адміністратора покладається обов'язок негайного реагування на інциденти інформаційної безпеки та ведення логів (журналів) доступу, що є критично важливим для подальшого розслідування можливих правопорушень [19, с. 90].

3. Користувач інформаційної системи. Користувач – це суб'єкт, який отримує доступ до ресурсів системи для задоволення власних потреб або виконання службових обов'язків. Користувачі поділяються на внутрішніх (працівники власника) та зовнішніх (громадяни, контрагенти).

Право на отримання достовірної інформації, право на захист своїх персональних даних, що обробляються в системі, та право на оскарження дій адміністратора у разі неправомірного обмеження доступу [13, с. 240].

Користувач зобов'язаний дотримуватися правил аутентифікації (не передавати паролі третім особам), використовувати систему виключно за призначенням та не вчиняти дій, що можуть призвести до збоїв у роботі ПЗ чи витоку даних [12, с. 45].

Правові зв'язки та розмежування відповідальності. Важливим аспектом є юридичне оформлення відносин між суб'єктами. Відносини між власником та адміністратором зазвичай регулюються сервісними договорами (SLA – Service Level Agreement), де прописуються гарантовані показники доступності системи. За словами Пилипчука В. Г., правова модель експлуатації ІС має базуватися на принципі **«поділеної відповідальності»**:

1. Власник відповідає за законність створення системи.
2. Адміністратор – за технічну цілісність та захищеність.
3. Користувач – за правомірність використання отриманих даних [14, с. 58].

Особливості суб'єктного складу у хмарних системах. При використанні моделі SaaS (Software as a Service) з'являється новий суб'єкт – **Провайдер хмарних послуг**. Його статус в українському праві уточнюється Законом «Про хмарні послуги». Провайдер не є власником інформації, але є володільцем інфраструктури, що створює специфічний трикутник правовідносин: Клієнт – Провайдер – Кінцевий користувач [10, с. 180].

Спеціальні суб'єкти: Органи контролю. До правовідносин у сфері експлуатації ІС також залучені державні органи, що здійснюють нагляд:

Держспецзв'язку – контроль за технічним захистом інформації.

Уповноважений ВРУ з прав людини – нагляд за дотриманням прав суб'єктів персональних даних у приватних та державних ІС.

Кіберполіція – розслідування правопорушень, вчинених у системах [19, с. 215].

Таким чином, суб'єктна структура правовідносин у сфері експлуатації ІС є складною та динамічною. Перехід до автоматизованих систем та «держави у смартфоні» вимагає не лише технічної злагодженості, а й чіткого законодавчого закріплення статусів кожного учасника. Тільки за умови балансу прав та обов'язків усіх суб'єктів можливе створення безпечного та ефективного інформаційного простору, де технології служать інтересам людини, суспільства та держави [20, с. 400; 15, с. 132].

3.3. Юридична відповідальність за правопорушення в інформаційних системах

Юридична відповідальність у сфері функціонування інформаційних систем (ІС) є правовим механізмом захисту встановленого порядку створення, використання та поширення інформації. Оскільки ІС дедалі частіше стають об'єктами злочинних посягань, правове забезпечення відповідальності

трансформується у бік посилення санкцій за втручання в роботу критичної інфраструктури та порушення конфіденційності даних [3, с. 402].

Кримінальна відповідальність за кіберзлочини. Основним нормативним актом, що регулює відповідальність за найнебезпечніші посягання на ІС, є Кримінальний кодекс України (ККУ). Розділ XVI ККУ присвячений злочинам у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж.

1. **Несанкціоноване втручання (ст. 361 ККУ).** Це одне з найбільш розповсюджених правопорушень. Об’єктом посягання тут є встановлений порядок роботи інформаційних систем. Сутність злочину полягає у діях, що призвели до витоку, втрати, підробки або блокування інформації, а також до спотворення процесу її обробки. В умовах воєнного стану відповідальність за такі дії значно посилена [3, с. 403].

2. **Створення та розповсюдження шкідливого ПЗ (ст. 361-1 ККУ).** Юридична відповідальність настає за розробку вірусів, фішингових програм та інших засобів, призначених для несанкціонованого втручання в ІС.

3. **Несанкціонований збут або розповсюдження інформації з обмеженим доступом (ст. 361-2 ККУ).** Ця норма захищає бази даних від незаконного копіювання та продажу. Як зазначає Бєляков К. І., об’єктом захисту тут виступає право власності на інформаційний ресурс, що зберігається в системі [7, с. 102].

Адміністративна відповідальність. Адміністративні правопорушення в ІС зазвичай пов’язані з порушенням правил технічної експлуатації або ігноруванням вимог щодо захисту даних.

Стаття 188-31 КУпАП передбачає відповідальність за невиконання законних вимог посадових осіб Держспецзв’язку щодо усунення порушень у сфері захисту інформації.

Стаття 188-39 КУпАП встановлює санкції за порушення законодавства про захист персональних даних, що є вкрай актуальним для приватних корпоративних систем (CRM, бази клієнтів) [12, с. 58].

Цивільно-правова та дисциплінарна відповідальність. Цивільно-правова відповідальність виникає у разі заподіяння майнової чи моральної шкоди внаслідок збоїв у роботі ІС або витоку конфіденційної інформації. Вона базується на принципі відшкодування збитків (ст. 1166 ЦК України). Наприклад, якщо банківська система через неналежний захист допустила викрадення коштів із рахунків клієнтів, банк несе цивільну відповідальність перед вкладниками [10, с. 185].

Дисциплінарна відповідальність застосовується до працівників (адміністраторів, операторів), які порушили внутрішні регламенти роботи з ІС. Це може бути догана або звільнення за розголошення комерційної таємниці чи порушення правил трудового розпорядку в частині інформаційної безпеки [1, с. 220].

Специфіка кваліфікації та суб'єктивна сторона. Для притягнення до відповідальності важливо встановити наявність вини. У кримінальних справах щодо ІС часто складно розмежувати навмисне втручання від технічної помилки персоналу. Юридична наука наголошує на необхідності проведення спеціальних комп'ютерно-технічних експертиз для підтвердження факту правопорушення [20, с. 405].

За словами Пилипчука В. Г., особливістю відповідальності в інформаційному праві є її **превентивна функція**. Сам факт встановлення жорстких санкцій за втручання в державні реєстри має стримувати потенційних правопорушників та стимулювати власників систем до інвестування в КСЗІ [14, с. 60].

Міжнародний аспект відповідальності. З огляду на транскордонний характер ІС, правопорушники можуть перебувати в одній країні, а система-об'єкт атаки – в іншій. Будапештська конвенція про кіберзлочинність вимагає від України співпраці з інтерполом та іншими державами для притягнення до відповідальності осіб, які вчиняють атаки на глобальні інформаційні системи [19, с. 218].

Таким чином, юридична відповідальність за правопорушення в інформаційних системах є комплексною. Вона поєднує публічно-правові санкції (кримінальні, адміністративні) та приватно-правові засоби відшкодування шкоди. Удосконалення цього інституту є ключовим для зміцнення довіри суспільства до цифрових технологій та забезпечення стабільності інформаційного права в Україні [18, с. 355; 20, с. 410].

ВИСНОВОК

У процесі виконання курсової роботи на тему «Інформаційні системи як об’єкти інформаційного права» було проведено комплексне дослідження правової природи, структури та особливостей функціонування інформаційних систем (ІС) у сучасному правовому полі України. Результати дослідження дозволяють сформулювати наступні узагальнюючі висновки:

1. Правова дефініція та сутність інформаційних систем. Встановлено, що інформаційна система в інформаційному праві – це не просто технічний комплекс, а складна організаційно-правова категорія. Вона поєднує в собі три невід’ємні компоненти: інформаційний ресурс (дані), технологічний інструментарій (програмне та апаратне забезпечення) та правовий регламент (сукупність норм, що визначають порядок взаємодії суб’єктів). Юридичне визначення ІС за законодавством України як «організаційно впорядкованої сукупності документів і інформаційних технологій» підкреслює пріоритет змістовного та управлінського аспектів над суто технічними [4, с. 12]. Ключовими ознаками ІС як об’єкта права є її цілісність, наявність мети функціонування та встановлений режим доступу [7, с. 88].

2. Класифікація та правове розмежування. Доведено, що правовий режим ІС безпосередньо залежить від її класифікаційної приналежності. Найбільш значущим є поділ за формою власності на державні, комунальні та приватні системи. Державні системи функціонують на засадах публічного права, де домінують принципи презумпції достовірності даних та обов’язковості захисту. Приватні системи регулюються нормами цивільного права, проте підпадають під державний контроль у разі обробки персональних даних [10, с. 74]. Важливим науковим висновком є необхідність чіткого розмежування ІС із суміжними об’єктами: базами даних (як контентним наповненням) та мережами (як транспортним рівнем). Це дозволяє правильно визначити суб’єктів відповідальності у разі виникнення правопорушень [11, с. 215].

3. Специфіка державних реєстрів. Аналіз державних інформаційних систем та реєстрів (таких як ЄДРПОУ, Реєстр речових прав) свідчить про їх трансформацію у фундаментальні інструменти державного управління. Встановлено, що держава є власником таких систем, а відповідні органи влади – їх держателями. Правовий статус державних реєстрів характеризується високим рівнем публічної довіри до інформації, що в них міститься. Перспективним напрямом розвитку законодавства є забезпечення повної сумісності (інтероперабельності) різних державних систем для реалізації сервісних функцій держави [15, с. 132].

4. Глобалізація та міжнародні стандарти. Дослідження міжнародного аспекту показало, що функціонування глобальних ІС неможливе без врахування транскордонних стандартів. Регламент ЄС про захист даних (GDPR) став фактичним світовим стандартом, якому має відповідати будь-яка інформаційна система, що працює з даними фізичних осіб. Для України адаптація національного законодавства до стандартів ЄС (зокрема Директиви NIS 2) є обов’язковою умовою інтеграції у європейський цифровий простір та захисту національних інтересів у кіберсфері [20, с. 305].

5. Режим захисту та безпеки. Центральним елементом правового забезпечення експлуатації ІС є створення та сертифікація комплексної системи захисту інформації (КСЗІ). Доведено, що відсутність Атестата відповідності КСЗІ робить функціонування державної системи незаконним, а її дані – юридично нікчемними. Сучасний підхід до безпеки ІС має поєднувати традиційний технічний захист із заходами кібербезпеки, що базуються на ризико-орієнтованому управлінні та моніторингу інцидентів у реальному часі [5, с. 18; 19, с. 90].

6. Суб’єктний склад та юридична відповідальність. Правовідносини у сфері ІС характеризуються багатоланковою структурою суб’єктів: власник, розпорядник, адміністратор та користувач. Кожен із них наділений специфічним обсягом прав та обов’язків. Юридична відповідальність за правопорушення в ІС (адміністративна за КУпАП та кримінальна за ст. 361-

363-1 ККУ) спрямована на захист встановленого порядку роботи систем. Об’єктом посягання у таких справах є не лише інформація, а й стабільність функціонування технологічної інфраструктури, що є основою національної безпеки [3, с. 402; 14, с. 56].

Пропозиції щодо вдосконалення законодавства: На основі проведеного аналізу пропонується посилити відповідальність за неналежне забезпечення захисту інформації в приватних системах, що мають статус критичної інфраструктури, та уніфікувати термінологію щодо «інформаційних систем» у різних галузях права (цивільному, господарському, адміністративному).

Загалом, інформаційні системи як об’єкти інформаційного права є динамічним інститутом, розвиток якого випереджає чинне законодавство. Це вимагає від держави постійної актуалізації правових норм, створення гнучких механізмів регулювання штучного інтелекту та хмарних технологій у межах ІС, а також підвищення рівня цифрової грамотності суб’єктів правовідносин.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Арістова І. В. Державна інформаційна політика: організаційно-правові аспекти. Харків: Консум, 2022. 340 с.

2. Господарський процесуальний кодекс України: Закон України від 06.11.1991 № 1798-XII (з наступ. змінами).

3. Кримінальний кодекс України: Закон України від 05.04.2001 № 2341-III.

4. Про інформацію: Закон України від 02.10.1992 № 2657-XII.

5. Про захист інформації в інформаційно-комунікаційних системах: Закон України від 05.07.1994 № 80/94-ВР.

6. Про Національну програму інформатизації: Закон України від 01.12.2022 № 2807-IX.

7. Бєляков К. І. Інформаційне право: теорія і практика. К.: КНТ, 2021. 250 с.

8. Брижко В. М. Правовий режим інформаційних систем. К.: Дух і Літера, 2020. 190 с.

9. Копилов В. А. Информационное право: учебник. М.: Юристъ, 2019. 420 с.

10. Костецька Т. О. Право власності на інформацію в Україні. К.: Юрінком Інтер, 2022. 180 с.

11. Кушакова Н. В. Правове регулювання автоматизованих інформаційних систем. Одеса: Юридична література, 2021. 215 с.

12. Ліпкан В. А. Інформаційне право України: Навч. посіб. К.: КНТ, 2023. 320 с.

13. Марущак А. І. Інформаційне право: доступ до інформації. К.: Центр учбової літератури, 2022. 240 с.

14. Пилипчук В. Г. Теоретико-правові засади формування інформаційного суспільства. К.: НДІІП, 2020. 160 с.

15. Розум О. М. Правове забезпечення електронного урядування в Україні. К.: Парламентське вид-во, 2021. 200 с.

16. Соснін О. В. Проблеми державного управління інформаційними ресурсами в Україні. К.: Ін-т держави і права, 2019. 280 с.

17. Стоєцький О. В. Суб’єкти та об’єкти інформаційних правовідносин. Львів: Світ, 2022. 225 с.

18. Фурашев В. М. Інформаційне право та інформаційна безпека. К.: АртЕк, 2023. 350 с.

19. Цимбалюк В. С. Інформаційне право: концептуальні засади формування галузі. К.: Освіта України, 2021. 210 с.

20. Швець М. Я. Інформатизація законотворчої та правозастосовної діяльності. К.: Юрінком, 2020. 400 с.