

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

КУРСОВА РОБОТА

з дисципліни: **«ІНФОРМАЦІЙНЕ ПРАВО»**

за темою: **«ОХОРОНА ДЕРЖАВНОЇ ТАЄМНИЦІ»**

Студента (ки): Льовіна Д.С.

курсу: 4

групи: ІН16-9-22-Б1П (4.0д)

Спеціальність: 081 Право

Керівник: доцент, к.ю.н. Лебедєв О.П.

Оцінка: _____

Національна шкала _____

Кількість балів: _____ ECTS _____

Члени комісії

(підпис)

(прізвище та ініціали)

(підпис)

(прізвище та ініціали)

(підпис)

(прізвище та ініціали)

м. Чернігів 2026

Зміст

ВСТУП.....	3
РОЗДІЛ 1. ТЕОРЕТИКО-ПРАВОВІ ОСНОВИ ДЕРЖАВНОЇ ТАЄМНИЦІ	5
1.1. Поняття державної таємниці.....	5
1.2. Правова природа державної таємниці.....	7
1.3. Джерела правового регулювання охорони державної таємниці	9
РОЗДІЛ 2. ПРАВОВИЙ РЕЖИМ ДЕРЖАВНОЇ ТАЄМНИЦІ	13
2.2. Порядок доступу до державної таємниці	15
2.3. Організація охорони державної таємниці.....	17
РОЗДІЛ 3. ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ В УКРАЇНІ.....	20
3.1. Юридична відповідальність за порушення законодавства про державну таємницю	20
3.2. Проблеми правового регулювання охорони державної таємниці.....	22
ВИСНОВКИ	26
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	29

ВСТУП

У сучасних умовах розвитку інформаційного суспільства інформація набуває стратегічного значення, виступаючи одним із ключових ресурсів функціонування держави, суспільства та економіки. Особливе місце серед різних видів інформації займає інформація, що становить державну таємницю, оскільки її розголошення може спричинити істотну шкоду національній безпеці, обороноздатності та іншим життєво важливим інтересам держави. У зв'язку з цим питання охорони державної таємниці набуває особливої актуальності та потребує належного правового регулювання.

Актуальність теми курсової роботи зумовлена необхідністю забезпечення ефективного функціонування механізмів охорони державної таємниці в умовах сучасних викликів, зокрема військової агресії, кіберзагроз, розвитку цифрових технологій та глобалізації інформаційного простору. Зростання обсягів інформації, що підлягає захисту, а також ускладнення способів її обробки і передачі вимагають постійного вдосконалення законодавства та практики його застосування.

Стан наукової розробки теми свідчить про значну увагу вітчизняних науковців до проблем інформаційної безпеки та правового регулювання державної таємниці. У наукових працях досліджуються питання визначення поняття державної таємниці, особливості її правового режиму, механізми захисту та відповідальність за порушення законодавства у цій сфері. Водночас динамічний розвиток суспільних відносин та зміни у законодавстві зумовлюють необхідність подальшого комплексного дослідження зазначеної проблематики.

Метою курсової роботи є комплексне дослідження правових засад охорони державної таємниці, визначення її сутності, особливостей правового режиму, а також аналіз проблем і перспектив розвитку законодавства у цій сфері.

Для досягнення поставленої мети необхідно вирішити такі завдання: розкрити поняття державної таємниці; визначити її правову природу; проаналізувати джерела правового регулювання охорони державної таємниці; охарактеризувати класифікацію та ступені секретності інформації; дослідити порядок доступу до державної таємниці; проаналізувати організацію охорони державної таємниці; визначити механізми забезпечення її захисту;

дослідити юридичну відповідальність за порушення законодавства; окреслити основні проблеми та напрями вдосконалення правового регулювання.

Об'єктом дослідження є суспільні відносини, що виникають у сфері охорони державної таємниці.

Предметом дослідження є правове регулювання охорони державної таємниці, її правовий режим, а також механізми забезпечення її захисту.

Методи дослідження. У процесі виконання курсової роботи використано комплекс загальнонаукових і спеціально-юридичних методів, зокрема: діалектичний метод — для аналізу розвитку правового регулювання у сфері інформаційної безпеки; формально-юридичний — для дослідження норм законодавства; системний — для визначення місця інституту державної таємниці у системі інформаційного права; порівняльно-правовий — для аналізу підходів до регулювання зазначених відносин.

Джерельну базу дослідження становлять нормативно-правові акти України, що регулюють питання державної таємниці та інформаційної безпеки, наукові праці вітчизняних учених, а також сучасні наукові публікації з відповідної тематики.

Структура курсової роботи визначається метою та завданнями дослідження і складається зі вступу, трьох розділів, що поділяються на підрозділи, висновків та списку використаних джерел.

РОЗДІЛ 1. ТЕОРЕТИКО-ПРАВОВІ ОСНОВИ ДЕРЖАВНОЇ ТАЄМНИЦІ

1.1. Поняття державної таємниці

У сучасному інформаційному суспільстві інформація виступає одним із ключових ресурсів, що забезпечує функціонування держави, розвиток суспільства та реалізацію прав людини. Водночас не вся інформація може бути відкритою, оскільки її розголошення здатне завдати шкоди національним інтересам. У цьому контексті особливого значення набуває інститут державної таємниці, який є важливим елементом системи інформаційного права та національної безпеки.

Поняття державної таємниці закріплено на законодавчому рівні. Відповідно до Закону України «Про державну таємницю», державна таємниця — це вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України [2]. Таке визначення підкреслює, що ключовим критерієм віднесення інформації до державної таємниці є потенційна шкода державним інтересам.

Важливою ознакою державної таємниці є її нормативна визначеність. Це означає, що віднесення певної інформації до категорії державної таємниці здійснюється виключно відповідно до закону та на підставі чітко визначених критеріїв. Такий підхід спрямований на запобігання зловживанням з боку органів влади та забезпечення прозорості у сфері обмеження доступу до інформації.

Сутність державної таємниці полягає у забезпеченні захисту життєво важливих інтересів держави. До таких інтересів належать, зокрема, обороноздатність країни, її економічна стабільність, безпека державного управління, ефективність діяльності правоохоронних органів. У цьому контексті державна таємниця виступає як інструмент забезпечення національної безпеки [15, с. 42].

У науковій літературі підкреслюється, що державна таємниця є складною правовою категорією, яка поєднує в собі інформаційний і правовий аспекти. З одного боку, вона є інформацією, що має певний зміст, а з іншого — об'єктом

правового регулювання, який підпадає під спеціальний правовий режим [14, с. 120]. Такий режим передбачає встановлення обмежень щодо доступу, використання, поширення та зберігання інформації.

Однією з ключових характеристик державної таємниці є її виключно публічно-правова природа. На відміну від конфіденційної інформації, яка може належати фізичним або юридичним особам, державна таємниця є власністю держави і охороняється нею. Це обумовлює особливий порядок встановлення режиму секретності та контролю за дотриманням відповідних вимог.

Важливим аспектом є також співвідношення державної таємниці з правом на інформацію. Конституція України гарантує кожному право на інформацію, проте це право може бути обмежене в інтересах національної безпеки [1]. Таким чином, державна таємниця виступає як один із легітимних інструментів обмеження доступу до інформації, що забезпечує баланс між відкритістю та безпекою.

Слід зазначити, що державна таємниця має чітко визначену сферу застосування. Вона охоплює лише ті відомості, які прямо передбачені законодавством. Це означає, що не будь-яка інформація може бути засекречена, а лише та, яка відповідає встановленим критеріям. Зокрема, не підлягає засекречуванню інформація про стан довкілля, якість харчових продуктів, аварії та катастрофи, що становлять загрозу для населення.

У сучасних умовах значення державної таємниці значно зростає у зв'язку з розвитком інформаційних технологій та збільшенням кількості кіберзагроз. Це вимагає не лише вдосконалення законодавства, але й впровадження сучасних засобів захисту інформації. У наукових дослідженнях зазначається, що ефективність охорони державної таємниці залежить від поєднання правових і технічних механізмів захисту [13, с. 182].

Окремої уваги заслуговує питання динамічності державної таємниці. З розвитком суспільства змінюються як види інформації, що підлягає засекречуванню, так і підходи до її регулювання. Це обумовлює необхідність постійного перегляду переліку відомостей, що становлять державну таємницю, та адаптації законодавства до сучасних умов.

У науковій доктрині також підкреслюється, що державна таємниця виконує не лише захисну, але й регулятивну функцію. Вона визначає порядок обігу інформації у певних сферах діяльності та встановлює правила поведінки для суб'єктів інформаційних відносин [16, с. 47]. Це сприяє упорядкуванню інформаційних процесів і забезпеченню їх безпеки.

Таким чином, державна таємниця є особливим видом інформації з обмеженим доступом, що характеризується наявністю спеціального правового режиму, спрямованого на захист національних інтересів. Вона виступає важливим інструментом забезпечення національної безпеки та функціонування держави, а її правове регулювання має ключове значення для розвитку сучасного інформаційного суспільства.

1.2. Правова природа державної таємниці

Правова природа державної таємниці є складною та багатовимірною категорією, що відображає її місце у системі права та особливості правового регулювання. Вона визначається поєднанням інформаційної сутності відповідних відомостей і спеціального правового режиму, спрямованого на забезпечення національної безпеки та захист життєво важливих інтересів держави.

Передусім, державна таємниця є різновидом інформації, що має особливу цінність для держави. Вона належить до категорії інформації з обмеженим доступом і характеризується тим, що її розголошення може спричинити негативні наслідки для обороноздатності, економічної стабільності, міжнародних відносин або інших сфер функціонування держави. Таким чином, державна таємниця є не просто інформацією, а інформацією, що має підвищений рівень значущості.

Особливістю правової природи державної таємниці є її публічно-правовий характер. На відміну від конфіденційної інформації, яка може належати приватним особам, державна таємниця є об'єктом виключної охорони з боку держави. Саме держава визначає перелік відомостей, що становлять державну таємницю, порядок їх засекречування, доступу до них та заходи щодо

їх захисту [2]. Це зумовлює централізований характер правового регулювання у цій сфері.

Державна таємниця є об'єктом правового регулювання одразу кількох галузей права. Зокрема, її регулювання здійснюється нормами конституційного права, які встановлюють загальні засади обмеження права на інформацію; адміністративного права, що визначає порядок діяльності органів державної влади; кримінального права, яке передбачає відповідальність за порушення режиму секретності; а також інформаційного права, що формує загальні підходи до регулювання інформаційних відносин. Такий міжгалузевий характер свідчить про комплексність даного інституту.

У системі інформаційного права державна таємниця розглядається як самостійний інститут, що об'єднує правові норми, спрямовані на регулювання відносин у сфері засекречування інформації, забезпечення режиму секретності та контролю за її використанням. Цей інститут має власний предмет правового регулювання, який полягає у визначенні умов і порядку обмеження доступу до інформації, що має особливу значущість для держави.

Суттєвою характеристикою правової природи державної таємниці є наявність спеціального правового режиму. Такий режим передбачає встановлення чітких правил щодо обігу інформації, включаючи порядок її створення, обліку, зберігання, передачі та знищення. Крім того, він визначає коло осіб, які мають право доступу до такої інформації, а також встановлює відповідальність за порушення встановлених вимог [17, с. 52].

Важливим елементом правової природи державної таємниці є її зв'язок із категорією національної безпеки. Державна таємниця виступає одним із ключових інструментів забезпечення безпеки держави, оскільки дозволяє обмежити доступ до інформації, яка може бути використана на шкоду державним інтересам. У цьому контексті вона виконує захисну функцію, спрямовану на запобігання загрозам як внутрішнього, так і зовнішнього характеру [15, с. 43].

Не менш важливим є питання співвідношення державної таємниці з правами і свободами людини. З одного боку, право на інформацію є одним із фундаментальних прав, гарантованих Конституцією України. З іншого боку, це

право може бути обмежене у випадках, коли це необхідно для захисту національної безпеки. Таким чином, державна таємниця виступає як правовий механізм, що забезпечує баланс між відкритістю інформації та необхідністю її обмеження [1].

Особливу увагу слід приділити принципу законності у сфері державної таємниці. Віднесення інформації до категорії державної таємниці можливе лише на підставі закону та відповідно до встановлених процедур. Це означає, що будь-яке обмеження доступу до інформації повинно бути обґрунтованим і відповідати вимогам законодавства. Такий підхід сприяє забезпеченню правової визначеності та запобіганню зловживанням.

Державна таємниця також характеризується динамічністю. З розвитком суспільства та зміною умов функціонування держави змінюється і зміст інформації, що підлягає засекречуванню. Це обумовлює необхідність постійного оновлення законодавства та адаптації правового регулювання до нових викликів, зокрема у сфері інформаційних технологій та кібербезпеки.

У науковій літературі підкреслюється, що державна таємниця виконує не лише захисну, але й організаційну функцію. Вона визначає порядок обігу інформації у державних органах, встановлює правила доступу до неї та забезпечує контроль за дотриманням режиму секретності [18, с. 46]. Це сприяє ефективному функціонуванню державного апарату та підвищенню рівня інформаційної безпеки.

Таким чином, правова природа державної таємниці характеризується комплексністю, публічно-правовим характером та наявністю спеціального правового режиму. Вона відображає особливу роль цієї категорії у забезпеченні національної безпеки та функціонуванні держави, а також визначає необхідність її належного правового регулювання в умовах сучасного інформаційного суспільства.

1.3. Джерела правового регулювання охорони державної таємниці

Правове регулювання охорони державної таємниці в Україні здійснюється на основі розгалуженої системи нормативно-правових актів, що мають різну юридичну силу та сферу застосування. Ця система формує

комплексний механізм забезпечення режиму секретності та спрямована на ефективний захист інформації, що становить державну таємницю.

Основу правового регулювання становлять норми Конституції України, які закріплюють фундаментальні права і свободи людини, зокрема право на інформацію, а також визначають можливість обмеження цього права в інтересах національної безпеки. Конституційні положення створюють загальну правову рамку, в межах якої здійснюється регулювання відносин у сфері охорони державної таємниці [1].

Центральним нормативно-правовим актом у цій сфері є Закон України «Про державну таємницю», який визначає правові основи віднесення інформації до державної таємниці, порядок її засекречування, розсекречування, доступу до неї та заходи щодо її охорони. Саме цей закон встановлює основні поняття, принципи та механізми функціонування інституту державної таємниці, а також визначає компетенцію органів державної влади у цій сфері [2].

Важливу роль у системі джерел правового регулювання відіграє Закон України «Про інформацію», який визначає загальні засади інформаційних відносин, включаючи класифікацію інформації за порядком доступу. У ньому закріплено положення про те, що інформація може бути відкритою або з обмеженим доступом, що створює основу для виділення державної таємниці як особливого виду інформації [3].

Значення має також Закон України «Про доступ до публічної інформації», який встановлює порядок доступу до інформації, що перебуває у володінні суб'єктів владних повноважень. Цей закон визначає критерії обмеження доступу до інформації та запроваджує механізм «трискладового тесту», що дозволяє оцінити правомірність віднесення інформації до категорії з обмеженим доступом [4]. Він відіграє важливу роль у забезпеченні балансу між відкритістю інформації та необхідністю її захисту.

Окреме місце у системі джерел займає законодавство у сфері національної безпеки. Закон України «Про національну безпеку України» визначає основні принципи забезпечення безпеки держави, у тому числі інформаційної безпеки. У цьому контексті охорона державної таємниці розглядається як один із важливих елементів системи національної безпеки [7].

Суттєву роль відіграють також закони, що регулюють діяльність спеціальних державних органів. Зокрема, Закон України «Про Службу безпеки України» визначає повноваження цього органу у сфері охорони державної таємниці, включаючи контроль за дотриманням режиму секретності. Закон України «Про розвідку» встановлює особливості роботи з інформацією, що має обмежений доступ, у сфері розвідувальної діяльності [5; 6].

Важливим елементом системи джерел є норми кримінального та адміністративного законодавства, які встановлюють відповідальність за порушення режиму державної таємниці. Кримінальний кодекс України передбачає відповідальність за розголошення державної таємниці, втрату документів, що містять таку інформацію, а також інші правопорушення, пов'язані з порушенням режиму секретності [8]. Кодекс України про адміністративні правопорушення визначає відповідальність за менш тяжкі порушення у цій сфері [9].

Окрему групу джерел становлять підзаконні нормативно-правові акти, які деталізують положення законів та забезпечують їх практичну реалізацію. До таких актів належить, зокрема, Порядок організації та забезпечення режиму секретності в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях. Цей документ встановлює конкретні правила роботи з інформацією, що становить державну таємницю, включаючи порядок її обліку, зберігання, використання та знищення [11].

Слід також відзначити значення законодавства у сфері захисту інформації в інформаційно-телекомунікаційних системах, яке регулює питання технічного захисту інформації. У сучасних умовах, коли значна частина інформації обробляється в електронній формі, забезпечення її захисту від несанкціонованого доступу набуває особливого значення [10].

У науковій літературі підкреслюється, що система джерел правового регулювання охорони державної таємниці має комплексний і багаторівневий характер. Це зумовлено необхідністю врахування різних аспектів інформаційних відносин, а також забезпечення ефективного функціонування механізмів захисту інформації [19, с. 92].

Крім того, важливу роль відіграють міжнародні стандарти у сфері інформаційної безпеки, які впливають на формування національного законодавства. Вони визначають загальні принципи захисту інформації та сприяють гармонізації правового регулювання з міжнародними вимогами.

Таким чином, джерела правового регулювання охорони державної таємниці утворюють цілісну систему, що включає конституційні норми, спеціальне та галузеве законодавство, підзаконні акти, а також норми, що встановлюють юридичну відповідальність. Їх взаємодія забезпечує ефективний захист державної таємниці та створює необхідні правові умови для функціонування держави в умовах сучасного інформаційного суспільства.

РОЗДІЛ 2. ПРАВОВИЙ РЕЖИМ ДЕРЖАВНОЇ ТАЄМНИЦІ

2.1. Класифікація та ступені секретності інформації

Класифікація інформації, що становить державну таємницю, та встановлення ступенів її секретності є важливими елементами правового режиму державної таємниці. Вони забезпечують диференційований підхід до захисту інформації залежно від ступеня її значущості та можливих наслідків розголошення. Такий підхід дозволяє ефективно організувати систему охорони державної таємниці та забезпечити належний рівень інформаційної безпеки.

Відповідно до законодавства України, інформація, що становить державну таємницю, підлягає класифікації за сферами, у яких вона використовується. Зокрема, Закон України «Про державну таємницю» визначає, що до державної таємниці можуть бути віднесені відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку [2]. Така класифікація дозволяє систематизувати інформацію та визначити особливості її правового режиму залежно від сфери застосування.

Сфера оборони охоплює інформацію, пов'язану з військовою діяльністю держави, зокрема відомості про чисельність, озброєння, дислокацію військ, плани оборони та мобілізації. Розголошення такої інформації може безпосередньо вплинути на обороноздатність країни, що обумовлює необхідність її суворого захисту.

У сфері економіки до державної таємниці можуть належати відомості про стратегічні ресурси, фінансову політику, державні резерви та інші аспекти, що мають важливе значення для економічної безпеки. У сучасних умовах економічна інформація також набуває особливого значення у контексті міжнародної конкуренції та санкційної політики.

Сфера науки і техніки включає інформацію про новітні розробки, технології, наукові дослідження, які можуть мати оборонне або стратегічне значення. Захист такої інформації сприяє збереженню науково-технічного потенціалу держави та запобігає її використанню іншими державами.

У сфері зовнішніх відносин державна таємниця охоплює інформацію про дипломатичну діяльність, міжнародні переговори, укладення договорів та інші

аспекти міжнародної співпраці. Розголошення такої інформації може негативно вплинути на міжнародний імідж держави та її позиції на міжнародній арені.

Сфера державної безпеки та охорони правопорядку включає відомості про діяльність правоохоронних органів, спеціальних служб, методи боротьби зі злочинністю, а також інформацію про оперативно-розшукову діяльність. Захист цієї інформації є необхідною умовою ефективного функціонування відповідних органів [5].

Окрім класифікації за сферами, важливе значення має встановлення ступенів секретності інформації. Законодавство України передбачає три основні ступені секретності: «особливої важливості», «цілком таємно» та «таємно» [2]. Кожен із цих ступенів відповідає певному рівню потенційної шкоди, яка може бути завдана у разі розголошення інформації.

Ступінь «особливої важливості» застосовується до інформації, розголошення якої може спричинити найтяжчі наслідки для національної безпеки держави. Це можуть бути відомості, що безпосередньо впливають на обороноздатність, стратегічне управління або міжнародні відносини держави.

Ступінь «цілком таємно» передбачає високий рівень секретності і застосовується до інформації, розголошення якої може завдати значної шкоди державним інтересам. Така інформація також потребує суворого контролю за доступом і використанням.

Ступінь «таємно» є найнижчим рівнем секретності серед інформації, що становить державну таємницю. Водночас її розголошення також може мати негативні наслідки, тому вона підлягає відповідному захисту.

Встановлення ступеня секретності здійснюється уповноваженими державними органами відповідно до законодавства. При цьому враховується характер інформації, її значущість та можливі наслідки розголошення. Такий підхід дозволяє забезпечити адекватний рівень захисту інформації.

Важливим аспектом є також строк дії секретності. Інформація не може бути засекречена безстроково, і законодавство передбачає необхідність її періодичного перегляду. Це пов'язано з тим, що з часом інформація може втрачати свою актуальність і переставати становити загрозу для національної безпеки.

У науковій літературі зазначається, що ефективність класифікації інформації та встановлення ступенів секретності залежить від чіткості законодавчих критеріїв і належного рівня правозастосування [16, с. 95]. Недостатня визначеність може призводити до зловживань або, навпаки, до недостатнього захисту інформації.

Таким чином, класифікація інформації та встановлення ступенів секретності є важливими складовими правового режиму державної таємниці. Вони забезпечують системність і ефективність заходів щодо охорони інформації та сприяють захисту національних інтересів держави.

2.2. Порядок доступу до державної таємниці

Порядок доступу до державної таємниці є одним із ключових елементів правового режиму секретної інформації, оскільки саме він визначає умови, за яких конкретні особи можуть отримувати, використовувати та зберігати відомості, що становлять державну таємницю. Встановлення чіткої процедури доступу забезпечує належний рівень захисту інформації та мінімізує ризики її неправомірного розголошення.

Законодавство України передбачає, що доступ до державної таємниці може надаватися лише особам, які мають відповідний допуск і необхідність працювати з такою інформацією у зв'язку з виконанням службових обов'язків [2]. Таким чином, доступ до державної таємниці є обмеженим і надається за сукупності двох умов: наявності допуску та потреби у використанні відповідної інформації.

Допуск до державної таємниці — це спеціальний правовий інститут, який передбачає надання особі права працювати з інформацією певного ступеня секретності. Видача допуску здійснюється уповноваженими державними органами, зокрема Службою безпеки України, після проведення відповідної перевірки особи. Така перевірка включає з'ясування обставин, що можуть вплинути на здатність особи забезпечувати збереження державної таємниці [5].

Залежно від ступеня секретності інформації встановлюються різні форми допуску. Зокрема, особи можуть отримати допуск до інформації зі ступенем «таємно», «цілком таємно» або «особливої важливості». Кожен рівень допуску

відповідає певному обсягу прав щодо роботи з інформацією і передбачає різні вимоги до перевірки особи.

Важливим елементом процедури доступу є оформлення зобов'язання про нерозголошення державної таємниці. Особа, яка отримує допуск, зобов'язується дотримуватися встановлених правил поведінки з інформацією та не розголошувати її без відповідного дозволу. Порухення цього зобов'язання може спричинити юридичну відповідальність.

Окрім допуску, важливе значення має також поняття «допуску за посадою». Це означає, що доступ до державної таємниці надається лише у межах службових повноважень особи. Навіть за наявності допуску особа не має права ознайомлюватися з інформацією, яка не стосується її службової діяльності. Такий підхід забезпечує принцип «необхідності знання», який є основоположним у сфері захисту державної таємниці.

Процедура надання доступу також передбачає ведення обліку осіб, які мають допуск до державної таємниці. Це дозволяє здійснювати контроль за обігом інформації та запобігати її витоку. Відповідні облікові дані зберігаються у спеціальних реєстрах і підлягають захисту.

Суттєвим аспектом є також можливість обмеження або припинення доступу до державної таємниці. Законодавство передбачає, що допуск може бути скасований у разі порушення особою встановлених правил, зміни її службового становища або виникнення обставин, що ставлять під загрозу збереження державної таємниці [2]. Це дозволяє оперативно реагувати на потенційні загрози.

Особливу увагу слід приділити доступу до державної таємниці в умовах воєнного стану. У таких умовах можуть застосовуватися додаткові заходи безпеки, спрямовані на посилення контролю за обігом інформації. Це обумовлено зростанням ризиків, пов'язаних із розвідувальною діяльністю та кіберзагрозами.

Важливим є також питання доступу до державної таємниці для іноземців та осіб без громадянства. Законодавство передбачає обмеження щодо надання такого доступу, оскільки це може створювати додаткові ризики для національної безпеки. У разі необхідності доступ може надаватися лише за спеціальною процедурою та за умови дотримання додаткових вимог.

У науковій літературі підкреслюється, що ефективність системи доступу до державної таємниці залежить від чіткості процедур, рівня контролю та правосвідомості осіб, які працюють із секретною інформацією [20, с. 123]. Недотримання встановлених правил може призвести до витоку інформації та завдати шкоди державним інтересам.

Важливим елементом є також технічний контроль доступу до інформації. У сучасних умовах значна частина державної таємниці зберігається в електронному вигляді, що вимагає застосування сучасних засобів захисту, таких як системи авторизації, криптографічний захист, контроль доступу до інформаційних систем. Це дозволяє забезпечити додатковий рівень безпеки.

Слід також зазначити, що порядок доступу до державної таємниці має бути чітко регламентований і зрозумілий для всіх суб'єктів. Це сприяє підвищенню ефективності правового регулювання та запобігає виникненню правових колізій.

То ж, порядок доступу до державної таємниці є складною системою правових, організаційних та технічних заходів, спрямованих на забезпечення належного рівня захисту секретної інформації. Його ефективність залежить від дотримання встановлених процедур, рівня контролю та відповідальності осіб, які мають доступ до такої інформації.

2.3. Організація охорони державної таємниці

Організація охорони державної таємниці є ключовим елементом забезпечення інформаційної безпеки держави та передбачає комплекс правових, організаційних і технічних заходів, спрямованих на недопущення несанкціонованого доступу до секретної інформації, її розголошення або втрати. Ефективна організація охорони державної таємниці забезпечує стабільне функціонування державних інститутів та захист національних інтересів.

Основу організації охорони державної таємниці становить законодавство України, яке визначає загальні принципи, суб'єктів та механізми забезпечення режиму секретності. Центральну роль у цьому процесі відіграє Закон України «Про державну таємницю», який встановлює правові засади охорони інформації та визначає повноваження державних органів у цій сфері [2].

Організація охорони державної таємниці здійснюється на різних рівнях: державному, відомчому та рівні окремих підприємств, установ і організацій. На державному рівні визначаються основні напрями політики у сфері захисту інформації, здійснюється координація діяльності відповідних органів та контроль за дотриманням законодавства.

Важливу роль у забезпеченні охорони державної таємниці відіграє Служба безпеки України, яка здійснює спеціальні функції у цій сфері. Зокрема, вона контролює дотримання режиму секретності, проводить перевірки, надає допуски до державної таємниці, а також здійснює інші заходи, спрямовані на запобігання витоку інформації [5]. Таким чином, Служба безпеки України є ключовим суб'єктом у системі охорони державної таємниці.

На рівні органів державної влади, підприємств і організацій створюються спеціальні підрозділи або призначаються відповідальні особи, які здійснюють організацію роботи з державною таємницею. До їхніх функцій належить ведення обліку секретних документів, контроль за їх зберіганням і використанням, організація доступу до інформації, а також проведення інструктажів для працівників.

Одним із ключових елементів організації охорони державної таємниці є встановлення режиму секретності. Цей режим включає систему правил і заходів, спрямованих на забезпечення збереження секретної інформації. Він охоплює порядок обігу документів, що містять державну таємницю, правила їх зберігання, передачі, копіювання та знищення [11].

Важливим аспектом є також фізичний захист інформації. Це передбачає забезпечення належних умов зберігання документів, обладнання приміщень спеціальними засобами захисту, обмеження доступу сторонніх осіб, використання сейфів, сигналізації та інших технічних засобів. Фізичний захист є основою забезпечення безпеки матеріальних носіїв інформації.

У сучасних умовах значну роль відіграє технічний захист інформації. Оскільки значна частина державної таємниці обробляється в електронному вигляді, виникає необхідність застосування сучасних інформаційних технологій для її захисту. До таких заходів належать криптографічний захист, системи

контролю доступу, захист інформаційних систем від несанкціонованого втручання, резервне копіювання даних [10].

Особливе значення має організація кадрового забезпечення у сфері охорони державної таємниці. Особи, які працюють із секретною інформацією, повинні проходити відповідну підготовку, інструктажі та перевірки. Важливим є також формування у них відповідального ставлення до виконання своїх обов'язків та дотримання режиму секретності.

Не менш важливим є контроль за дотриманням вимог законодавства у сфері охорони державної таємниці. Такий контроль здійснюється як внутрішніми службами організацій, так і державними органами. Він включає перевірки стану збереження інформації, аналіз дотримання встановлених процедур та виявлення порушень.

Слід зазначити, що ефективність організації охорони державної таємниці значною мірою залежить від узгодженості дій усіх суб'єктів, які беруть участь у цьому процесі. Взаємодія між державними органами, підприємствами та іншими організаціями є необхідною умовою забезпечення належного рівня інформаційної безпеки.

У науковій літературі підкреслюється, що сучасні виклики, пов'язані з розвитком інформаційних технологій та кіберзагрозами, вимагають постійного вдосконалення системи охорони державної таємниці [17, с. 53]. Це передбачає впровадження нових технологій, удосконалення законодавства та підвищення рівня підготовки фахівців.

Окремої уваги заслуговує проблема людського фактору, який є однією з основних причин витоку інформації. Недбалість, недостатня підготовка або навмисні дії працівників можуть призвести до порушення режиму секретності. Тому важливим є посилення контролю за діяльністю осіб, які мають доступ до державної таємниці.

Таким чином, організація охорони державної таємниці є складною системою взаємопов'язаних заходів, спрямованих на забезпечення захисту секретної інформації. Вона включає правові, організаційні, технічні та кадрові елементи, які у своїй сукупності забезпечують ефективне функціонування системи інформаційної безпеки держави.

РОЗДІЛ 3. ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ В УКРАЇНІ

3.1. Юридична відповідальність за порушення законодавства про державну таємницю

Юридична відповідальність за порушення законодавства про державну таємницю є важливим елементом механізму її охорони та забезпечення інформаційної безпеки держави. Вона виконує як каральну, так і превентивну функції, сприяючи дотриманню встановленого режиму секретності та запобіганню правопорушенням у цій сфері.

Законодавство України передбачає різні види юридичної відповідальності за порушення вимог щодо охорони державної таємниці, зокрема кримінальну, адміністративну, дисциплінарну та цивільно-правову. Такий підхід обумовлений різноманітністю правопорушень та ступенем їх суспільної небезпечності.

Найбільш суворим видом відповідальності є кримінальна відповідальність, яка настає за вчинення суспільно небезпечних діянь, пов'язаних із розголошенням державної таємниці або іншими порушеннями режиму секретності. Кримінальний кодекс України передбачає відповідальність за такі злочини, як розголошення державної таємниці, втрата документів або матеріальних носіїв інформації, що містять державну таємницю, а також шпигунство [8]. Ці правопорушення можуть завдати значної шкоди національній безпеці, що обумовлює суворість покарань.

Розголошення державної таємниці полягає у доведенні секретної інформації до відома сторонніх осіб без належного дозволу. Важливою ознакою цього злочину є наявність у винної особи допуску до державної таємниці або доступу до відповідної інформації у зв'язку з виконанням службових обов'язків. При цьому відповідальність настає незалежно від того, чи було розголошення умисним або необережним.

Шпигунство є одним із найнебезпечніших злочинів у цій сфері, оскільки передбачає передачу або збирання інформації, що становить державну таємницю, на користь іноземної держави або організації. Такий злочин має

безпосередній вплив на національну безпеку та може спричинити серйозні наслідки для держави.

Окрім кримінальної відповідальності, законодавство передбачає адміністративну відповідальність за порушення правил охорони державної таємниці. Кодекс України про адміністративні правопорушення встановлює відповідальність за недотримання встановлених вимог щодо обліку, зберігання та використання секретної інформації [9]. Такі правопорушення є менш небезпечними, однак також можуть створювати передумови для витоку інформації.

Дисциплінарна відповідальність застосовується до працівників, які порушили правила роботи з державною таємницею у межах службових відносин. Вона може проявлятися у вигляді догани, звільнення або інших заходів впливу. Дисциплінарна відповідальність спрямована на забезпечення належного виконання службових обов'язків та дотримання внутрішніх правил організацій.

Цивільно-правова відповідальність може наставати у випадках, коли порушення режиму державної таємниці спричинило матеріальну шкоду. У таких випадках винна особа зобов'язана відшкодувати завдані збитки. Хоча цей вид відповідальності застосовується рідше, він також є важливим елементом системи захисту державної таємниці.

Слід зазначити, що юридична відповідальність у сфері державної таємниці має комплексний характер і застосовується залежно від обставин конкретного правопорушення. У деяких випадках можливе одночасне застосування кількох видів відповідальності, наприклад, кримінальної та дисциплінарної.

Важливим аспектом є також превентивна функція юридичної відповідальності. Усвідомлення невідворотності покарання за порушення законодавства сприяє підвищенню дисципліни серед осіб, які мають доступ до державної таємниці, та запобігає вчиненню правопорушень.

У науковій літературі підкреслюється, що ефективність юридичної відповідальності залежить не лише від суворості санкцій, але й від рівня їх застосування на практиці [12, с. 340]. Важливим є забезпечення невідворотності покарання та об'єктивності розгляду відповідних справ.

Сучасні виклики, пов'язані з розвитком інформаційних технологій, зумовлюють необхідність удосконалення механізмів юридичної відповідальності. Зокрема, зростає кількість правопорушень, пов'язаних із незаконним доступом до інформаційних систем, що містять державну таємницю. Це потребує адаптації законодавства до нових умов та посилення відповідальності за кіберзлочини.

Окремої уваги заслуговує питання співвідношення юридичної відповідальності та прав людини. При застосуванні санкцій необхідно забезпечувати дотримання принципів законності, справедливості та пропорційності. Це сприяє формуванню довіри до правової системи та забезпечує ефективність правозастосування.

Таким чином, юридична відповідальність за порушення законодавства про державну таємницю є важливим інструментом забезпечення інформаційної безпеки. Вона охоплює різні види відповідальності та спрямована на захист національних інтересів держави, попередження правопорушень і забезпечення належного функціонування системи охорони державної таємниці.

3.2. Проблеми правового регулювання охорони державної таємниці

У сучасних умовах розвитку інформаційного суспільства та зростання ролі інформації у забезпеченні національної безпеки особливого значення набуває ефективність правового регулювання охорони державної таємниці. Попри наявність розвиненої нормативної бази, практика її застосування свідчить про існування низки проблем, які ускладнюють забезпечення належного рівня захисту секретної інформації.

Однією з ключових проблем є недосконалість законодавчого визначення критеріїв віднесення інформації до державної таємниці. Хоча Закон України «Про державну таємницю» встановлює загальні підходи до визначення такої інформації, на практиці ці критерії часто залишаються недостатньо конкретизованими [2]. Це створює ризики як необґрунтованого засекречування інформації, так і, навпаки, недостатнього рівня її захисту.

Проблема надмірної секретності є однією з найбільш дискусійних у науковій літературі. У ряді випадків органи державної влади можуть відносити

до державної таємниці інформацію, яка фактично не становить загрози національній безпеці. Це обмежує доступ громадян до інформації та суперечить принципам відкритості і прозорості діяльності держави [22, с. 70]. Така практика може негативно впливати на розвиток демократичного суспільства.

З іншого боку, існує проблема недостатнього рівня захисту інформації. У сучасних умовах зростає кількість випадків витоку інформації, що пов'язано як із технічними недоліками систем захисту, так і з людським фактором. Особливо актуальною ця проблема є у сфері кібербезпеки, де традиційні методи захисту інформації часто виявляються недостатніми.

Ще однією важливою проблемою є фрагментарність правового регулювання. Норми, що стосуються охорони державної таємниці, містяться у різних нормативно-правових актах, що іноді призводить до колізій і неузгодженості у їх застосуванні. Це ускладнює практичну діяльність органів державної влади та знижує ефективність правового регулювання [18, с. 215].

Значні труднощі виникають також у сфері доступу до державної таємниці. Процедури отримання допуску часто є складними та тривалими, що може негативно впливати на ефективність роботи державних органів. Водночас недостатній контроль за особами, які вже мають доступ до секретної інформації, створює додаткові ризики її витоку.

Окремої уваги заслуговує проблема недостатньої адаптації законодавства до сучасних інформаційних технологій. Значна частина нормативних актів була прийнята в умовах, коли інформаційні технології не мали такого розвитку, як сьогодні. У зв'язку з цим законодавство не завжди враховує особливості обробки, зберігання та передачі інформації в електронній формі [19, с. 287].

У сучасних умовах особливої актуальності набуває проблема кіберзагроз. Зростання кількості кібератак, спрямованих на отримання доступу до секретної інформації, вимагає вдосконалення правового регулювання у сфері кібербезпеки. Водночас чинне законодавство не завжди забезпечує належний рівень захисту інформації від таких загроз.

Ще однією проблемою є недостатній рівень підготовки кадрів, які працюють із державною таємницею. Недостатня обізнаність працівників щодо правил поводження з секретною інформацією може призводити до порушень

режиму секретності. У наукових дослідженнях підкреслюється, що людський фактор є однією з основних причин витоку інформації [13, с. 184].

Проблемним є також питання контролю за дотриманням законодавства. Хоча відповідні органи мають широкі повноваження у цій сфері, на практиці контроль не завжди є достатньо ефективним. Це може бути пов'язано як із обмеженими ресурсами, так і з недосконалістю механізмів контролю.

Важливим аспектом є також співвідношення державної таємниці та права на інформацію. У ряді випадків виникають конфлікти між необхідністю захисту секретної інформації та правом громадян на доступ до інформації. Вирішення таких конфліктів потребує чіткого визначення меж обмеження права на інформацію та застосування принципу пропорційності.

Суттєвою проблемою є також тривалі строки засекречування інформації. У деяких випадках інформація залишається засекреченою навіть тоді, коли вона вже втратила свою актуальність. Це свідчить про недостатню ефективність механізмів перегляду ступеня секретності та розсекречування інформації.

У контексті євроінтеграційних процесів важливим є питання гармонізації національного законодавства з міжнародними стандартами. Україна поступово адаптує своє законодавство до європейських вимог, однак цей процес потребує подальшого вдосконалення. Зокрема, необхідно враховувати стандарти прозорості та захисту прав людини, які є характерними для європейського правового простору.

Ще однією проблемою є недостатній рівень координації між різними органами державної влади у сфері охорони державної таємниці. Відсутність належної взаємодії може призводити до дублювання функцій або, навпаки, до прогалин у системі захисту інформації.

У науковій літературі також звертається увага на необхідність удосконалення відповідальності за порушення законодавства у цій сфері. Зокрема, пропонується посилення відповідальності за правопорушення, пов'язані з використанням інформаційних технологій, а також удосконалення механізмів притягнення до відповідальності [20, с. 124].

Таким чином, сучасний стан правового регулювання охорони державної таємниці характеризується наявністю низки проблем, що потребують

комплексного вирішення. До них належать недосконалість законодавства, фрагментарність правового регулювання, недостатній рівень захисту інформації, проблеми кадрового забезпечення та контролю, а також виклики, пов'язані з розвитком інформаційних технологій. Вирішення цих проблем є необхідною умовою підвищення ефективності системи охорони державної таємниці та забезпечення національної безпеки України.

ВИСНОВКИ

У результаті проведеного дослідження було комплексно проаналізовано правові засади охорони державної таємниці як важливого інституту інформаційного права України. Отримані результати дозволяють сформулювати низку теоретичних узагальнень і практичних висновків.

По-перше, встановлено, що державна таємниця є особливим видом інформації з обмеженим доступом, яка має стратегічне значення для забезпечення національної безпеки держави. Її сутність полягає у захисті відомостей, розголошення яких може завдати шкоди обороноздатності, економічній стабільності, міжнародним відносинам та іншим життєво важливим інтересам держави. Таким чином, державна таємниця виступає важливим інструментом забезпечення функціонування держави в умовах сучасних викликів.

По-друге, визначено, що правова природа державної таємниці характеризується комплексністю та публічно-правовим характером. Вона поєднує в собі інформаційний і правовий аспекти, виступаючи як об'єкт правового регулювання та як елемент системи національної безпеки. Державна таємниця регулюється нормами різних галузей права, що свідчить про її міжгалузевий характер і значущість у правовій системі.

По-третє, досліджено систему джерел правового регулювання охорони державної таємниці, яка має багаторівневий характер і включає Конституцію України, спеціальне законодавство, галузеві нормативно-правові акти, а також підзаконні акти. Встановлено, що така система забезпечує правову основу для функціонування механізму захисту державної таємниці, однак потребує подальшого вдосконалення з метою усунення прогалин і неузгодженостей.

По-четверте, з'ясовано, що важливим елементом правового режиму державної таємниці є класифікація інформації та встановлення ступенів її секретності. Відповідний поділ дозволяє диференціювати заходи захисту залежно від рівня значущості інформації та можливих наслідків її розголошення. Такий підхід сприяє більш ефективній організації системи охорони державної таємниці.

По-п'яте, встановлено, що порядок доступу до державної таємниці є складною процедурою, яка передбачає надання допуску, проведення перевірок та дотримання принципу «необхідності знання». Цей механізм спрямований на забезпечення контролю за обігом секретної інформації та мінімізацію ризиків її витоку.

По-шосте, досліджено організаційні засади охорони державної таємниці, які включають систему правових, організаційних і технічних заходів. Встановлено, що ефективність цієї системи залежить від узгодженості дій державних органів, рівня технічного забезпечення та підготовки кадрів. Особливу роль у цьому процесі відіграють спеціально уповноважені органи, зокрема Служба безпеки України.

По-сьоме, проаналізовано юридичну відповідальність за порушення законодавства про державну таємницю, яка має комплексний характер і включає кримінальну, адміністративну, дисциплінарну та цивільно-правову відповідальність. Встановлено, що така система відповідальності спрямована на забезпечення дотримання режиму секретності та запобігання правопорушенням.

По-восьме, виявлено основні проблеми правового регулювання охорони державної таємниці, серед яких: недосконалість законодавчих критеріїв, фрагментарність нормативної бази, недостатній рівень захисту інформації, проблеми кадрового забезпечення, а також виклики, пов'язані з розвитком інформаційних технологій та кіберзагрозами. Ці проблеми негативно впливають на ефективність системи захисту державної таємниці та потребують комплексного вирішення.

Узагальнюючи результати дослідження, можна зробити висновок, що інститут державної таємниці відіграє ключову роль у системі інформаційного права та забезпеченні національної безпеки України. Водночас ефективність його функціонування значною мірою залежить від якості правового регулювання, рівня організації охорони інформації та здатності держави адаптуватися до сучасних викликів.

Таким чином, подальший розвиток правового регулювання у сфері охорони державної таємниці має бути спрямований на підвищення його

ефективності, забезпечення балансу між безпекою та правами людини, а також адаптацію до умов цифровізації та глобалізації інформаційного простору.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Нормативно-правові акти

1. Конституція України : Закон України від 28 черв. 1996 р. № 254к/96-ВР.
2. Про державну таємницю : Закон України від 21 січ. 1994 р. № 3855-XII.
3. Про інформацію : Закон України від 02 жовт. 1992 р. № 2657-XII.
4. Про доступ до публічної інформації : Закон України від 13 січ. 2011 р. № 2939-VI.
5. Про Службу безпеки України : Закон України від 25 бер. 1992 р. № 2229-XII.
6. Про розвідку : Закон України від 17 верес. 2020 р. № 912-IX.
7. Про національну безпеку України : Закон України від 21 черв. 2018 р. № 2469-VIII.
8. Кримінальний кодекс України : Закон України від 05 квіт. 2001 р. № 2341-III.
9. Кодекс України про адміністративні правопорушення : Закон України від 07 груд. 1984 р. № 8073-X.
10. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05 лип. 1994 р. № 80/94-ВР.
11. Порядок організації та забезпечення режиму секретності в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях : постанова Кабінету Міністрів України.

2. Спеціальна література

12. Антонов К. В. Проблеми правового захисту інституту державної таємниці у кримінальному провадженні. Юридичний науковий електронний журнал. 2020. № 2. С. 335–358.
13. Басараб О., Блистів Т. Організаційно-правові засади забезпечення інформаційної безпеки. Sworld-Us Conference Proceedings. 2023. С. 181–185.

14. Брижко В. М. Інформаційне право України : навч. посіб. Київ : Інститут інформації, безпеки і права, 2020. 360 с.
15. Козюбра М. І. Проблеми забезпечення інформаційної безпеки. Право України. 2021. № 6. С. 40–48.
16. Костецький А. Інформаційне право України : підручник. Київ : Юрінком Інтер, 2022. 420 с.
17. Мельник М. І. Інформаційна безпека та державна таємниця. Київ : Алерта, 2023. 350 с.
18. Смаглюк С. В. Європейський досвід правового регулювання державної таємниці. Науковий вісник. 2022. С. 45–52.
19. Харитонova О. О. Державна таємниця як об'єкт правового захисту. Юридична наука. 2023. № 3. С. 90–96.
20. Хашев В. Г. Поняття та сутність державної таємниці в системі національної безпеки. Юридичний електронний журнал. 2025. № 3. С. 120–126.
21. Шаптала Н. К. Інформаційне право : навч. посіб. Київ : Центр учбової літератури, 2021. 312 с.
22. Шевчук О. Право на доступ до інформації та національна безпека: проблеми співвідношення. Юридичний журнал. 2023. № 2. С. 66–74.