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

КУРСОВА РОБОТА

з дисципліни: **«ІНФОРМАЦІЙНЕ ПРАВО»**

за темою: **«ЗАСЕКРЕЧУВАННЯ ІНФОРМАЦІЇ»**

Студента (ки): Погорілий В.П.
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

Актуальність теми. В умовах глобальної цифровізації та загострення геополітичних протистоянь інформація перетворилася на стратегічний актив, від ступеня захищеності якого безпосередньо залежить національна безпека, суверенітет та територіальна цілісність держави. Інститут засекречування інформації є одним із найскладніших та найбільш суперечливих елементів інформаційного права, оскільки він функціонує на межі двох фундаментальних принципів: права громадян на доступ до публічної інформації та необхідності обмеження такого доступу задля захисту інтересів оборони, правопорядку та економічної стабільності.

Для сучасної України питання правового регулювання засекречування відомостей набуло екзистенційної ваги. У період дії правового режиму воєнного стану виникла потреба у швидкому та гнучкому механізмі обмеження доступу до даних про дислокацію військ, об’єктів критичної інфраструктури та стратегічних планів держави. Водночас, європейський вектор розвитку України вимагає дотримання міжнародних стандартів прозорості влади та недопущення необґрунтованого засекречування (оверкласифікації), що часто використовується для приховування корупційних правопорушень або неефективного управління. Наукове переосмислення балансу між таємністю та відкритістю в інформаційній сфері є критично необхідним для вдосконалення вітчизняного законодавства.

Об’єктом дослідження є сукупність суспільних відносин, що виникають у процесі обмеження доступу до інформації, її віднесення до державної таємниці або службових відомостей, а також охорони таких відомостей державою.

Предметом дослідження є норми інформаційного та адміністративного права України, що регламентують процедури засекречування, зберігання та

розсекречування інформації, а також юридична відповідальність за їх порушення.

Метою курсової роботи є комплексний аналіз правових засад, процедурних механізмів та проблемних аспектів засекречування інформації в Україні, а також розробка рекомендацій щодо оптимізації цього інституту в умовах сучасних безпекових викликів.

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

дослідити етимологію та правову природу засекречування як способу обмеження доступу до інформації;

проаналізувати критерії диференціації державної таємниці, службової та конфіденційної інформації;

розкрити правовий статус суб'єктів, уповноважених здійснювати засекречування (Державних експертів з питань таємниць);

описати стадійність процедури надання відомостям грифу секретності;

визначити особливості режиму таємності в умовах воєнного стану;

обґрунтувати правові гарантії та підстави для розсекречування інформації.

Методологічну основу дослідження становлять системно-структурний метод (для класифікації видів таємниць), порівняльно-правовий метод (для зіставлення національних норм із стандартами НАТО та ЄС) та формально-юридичний метод (для аналізу дефініцій законодавства).

Наукова новизна роботи полягає у дослідженні трансформації інституту засекречування під впливом цифровізації (захист електронних носіїв) та необхідності дотримання балансу «безпека vs прозорість» у демократичній державі, що перебуває в стані війни.

Практичне значення одержаних результатів курсової роботи полягає у можливості їхнього прикладного застосування для вдосконалення системи захисту державних інтересів та оптимізації доступу до публічної інформації.

Сформульовані у дослідженні висновки та пропозиції можуть бути використані у таких сферах:

У правотворчій діяльності: розроблені рекомендації щодо чіткого розмежування критеріїв засекречування державної таємниці та службової інформації можуть бути використані при підготовці змін до Закону України «Про державну таємницю» та відповідних підзаконних актів, що регулюють режим секретності в умовах воєнного стану.

У діяльності органів державної влади: аналіз процедури надання грифів секретності та правового статусу державних експертів з питань таємниць може сприяти уніфікації практики засекречування у різних відомствах, мінімізації випадків «надмірного засекречування» (оверкласифікації) та підвищенню ефективності роботи режимно-секретних органів.

У сфері національної безпеки та оборони: висновки щодо особливостей захисту секретної інформації на цифрових носіях та в умовах кіберзагроз мають практичну цінність для розробки внутрішніх інструкцій із кібербезпеки в органах сектору безпеки і оборони України.

У сфері антикорупційного контролю: обґрунтування правових підстав для розсекречування інформації та механізмів суспільного моніторингу за цим процесом може бути використано громадськими організаціями та журналістами для забезпечення прозорості використання бюджетних коштів, які помилково або навмисно були віднесені до категорії секретних.

У навчальному процесі: результати дослідження можуть бути впроваджені у викладання дисциплін «Інформаційне право», «Адміністративне право», «Правове регулювання захисту державної таємниці», а також при підготовці спеціалістів із питань захисту інформації з обмеженим доступом.

РОЗДІЛ 1. ТЕОРЕТИКО-ПРАВОВІ ЗАСАДИ ОБМЕЖЕННЯ ДОСТУПУ ДО ІНФОРМАЦІЇ

1.1. Генеза та правова природа поняття «засекречування інформації» в інформаційному праві.

Генеза поняття «засекречування інформації» в інформаційному праві відображає тривалу еволюцію від архаїчних уявлень про «державну таємницю» як абсолютну прерогативу монарха до сучасної демократичної концепції обмеження доступу в інтересах національної безпеки. Історично перші етапи засекречування базувалися на принципі ratio status (державної необхідності), де критерії секретності були суб’єктивними та не підлягали правовому оскарженню. Проте з розвитком конституціоналізму та утвердженням права людини на інформацію у XX столітті, генеза цього поняття змістилася у площину законодавчого нормування. У 2026 році доктрина інформаційного права розглядає засекречування не як механічне приховання даних, а як складний адміністративно-правовий процес надання інформації спеціального правового статусу, що передбачає обмеження її поширення та встановлення особливого режиму охорони [3].

Правова природа засекречування інформації за своєю суттю є обмежувальним заходом, що становить легітимне втручання держави у право особи на вільне збирання та отримання відомостей. Юридична конструкція цього поняття базується на «трискладовому тесті», закріпленому в практиці Європейського суду з прав людини та національному законодавстві: обмеження має бути передбачене законом, переслідувати легітимну мету (захист суверенітету, територіальної цілісності) та бути необхідним у демократичному суспільстві [1]. Отже, правова природа засекречування є двоїстою: з одного боку, це обов'язок держави захищати стратегічно важливі дані, а з іншого — це правовий інструмент, що має чітко визначені межі, аби не перетворитися на інструмент приховування корупції чи порушень прав людини [6]. У сучасних

умовах воєнного стану правова природа засекречування також набула ознак динамічності, що дозволяє оперативно змінювати рівень доступу до даних залежно від безпекової ситуації [5].

Сучасна генеза поняття також тісно пов'язана із цифровізацією та появою автоматизованих систем класифікації даних. У 2026 році в інформаційному праві все частіше обговорюється «алгоритмічне засекречування», де штучний інтелект визначає рівень чутливості інформації на основі її потенційного впливу на національну безпеку. Це розширює класичне розуміння засекречування, додаючи до нього технологічний компонент кіберзахисту. Таким чином, генеза та правова природа цього поняття демонструють перехід від статики «таємниці» до динаміки «управління інформаційними ризиками», де баланс між відкритістю влади та безпекою держави є головним критерієм правомірності обмеження доступу [2]. Юридичне закріплення процедур розсекречування (декласифікації) є логічним завершенням цього процесу, що забезпечує транспарентність державного управління в довгостроковій перспективі [4].

1.2. Співвідношення категорій: державна таємниця, службова інформація та конфіденційні дані.

Співвідношення категорій «державна таємниця», «службова інформація» та «конфіденційні дані» у сучасному інформаційному праві України (станом на 2026 р.) базується на ієрархічній системі обмеження доступу, де критерієм розмежування виступає характер інтересу, що захищається, та ступінь шкоди від розголошення відомостей. Найвищим ступенем секретності володіє «державна таємниця» — це інформація у сферах оборони, економіки, зовнішніх відносин та правоохоронної діяльності, розголошення якої може завдати шкоди національній безпеці України [7]. Її правова природа визначається виключно державною власністю на такі відомості та спеціальною процедурою

засекречування через Державний реєстр секретів. На відміну від інших категорій, державна таємниця має чітко визначені рівні секретності («особливої важливості», «цілком таємно», «таємно») та передбачає кримінальну відповідальність за її розголошення незалежно від форми власності носія [3].

Категорія «службова інформація» займає проміжне місце та охоплює відомості, що містяться в документах суб'єктів владних повноважень, які не становлять державної таємниці, але їх передчасне оприлюднення може перешкодити діяльності органу або зашкодити репутації держави. Це так званий режим «для службового користування» (ДСК), який за своєю юридичною природою є інструментом забезпечення ефективності державного управління [5]. Співвідношення зі службовою інформацією часто визначається через «трискладовий тест»: доступ обмежується лише тоді, коли шкода від оприлюднення переважає суспільний інтерес до отримання цих даних. Якщо державна таємниця захищає існування держави як такої, то службова інформація забезпечує її функціональну стабільність [2].

«Конфіденційні дані» (конфіденційна інформація) є найбільш широкою категорією, правовий режим якої значною мірою визначається волею суб'єкта — фізичної або юридичної особи. Згідно із законом «Про інформацію», це відомості, доступ до яких обмежений самою особою (за винятком випадків, визначених законом), і які можуть поширюватися лише за її згодою [7]. Сюди належать персональні дані, комерційна таємниця та професійні таємниці (лікарська, адвокатська тощо). Співвідношення тут очевидне: якщо перші дві категорії (державна таємниця та службова інформація) є різновидами «таємної» та «службової» публічної інформації, то конфіденційні дані — це сфера приватного права [6]. У 2026 році, в умовах цифрової трансформації та екосистеми «Дія», межа між конфіденційними даними особи та службовою інформацією держави стає більш динамічною, оскільки держава виступає розпорядником величезних масивів персональної інформації, що вимагає застосування гібридних режимів захисту [4].

Таким чином, ці категорії співвідносяться як «загальне» (інформація з обмеженим доступом) та «видове». Державна таємниця — це найвищий пріоритет безпеки; службова інформація — операційний захист владних процесів; конфіденційні дані — захист приватності та комерційного інтересу [3]. Спільним для них є обов'язок держави забезпечувати кіберзахист цих відомостей у державних інформаційних системах, проте правові наслідки порушення режиму доступу суттєво різняться: від дисциплінарної відповідальності за розголошення службових даних до тривалих термінів ув’язнення за державну зраду [5].

1.3. Принципи засекречування: законність, обґрунтованість та своєчасність в умовах демократичного суспільства.

Принципи засекречування інформації — законність, обґрунтованість та своєчасність — становлять фундаментальну тріаду обмеження доступу, що забезпечує баланс між інтересами національної безпеки та правом громадян на інформацію в демократичному суспільстві. Принцип законності є преверховенствуючим і передбачає, що засекречуванню підлягає лише та інформація, яка чітко визначена у Законі України «Про державну таємницю» та Зводі відомостей, що становлять державну таємницю. Це виключає можливість волюнтаристського рішення окремого чиновника приховати відомості, які не мають стратегічного значення. Юридична природа цього принципу в 2026 році тісно пов’язана з дотриманням «трискладового тесту», згідно з яким будь-яке обмеження має бути передбачене законом, переслідувати легітимну мету та бути необхідним у демократичному суспільстві для захисту суверенітету [1]. Порушення законності при засекречуванні (наприклад, спроба приховати факти корупції чи порушення прав людини) автоматично робить таке рішення нікчемним та тягне за собою відповідальність посадових осіб [3].

Принцип обґрунтованості вимагає проведення експертної оцінки фахівцями (державними експертами з питань таємниць) для встановлення реальної загрози національним інтересам у разі розголошення конкретних даних. Обґрунтованість означає, що держава повинна мати вагомі аргументи, чому саме ці відомості мають бути приховані від суспільства в даний момент. У демократичному суспільстві цей принцип виступає антидотом проти надмірного засекречування (over-classification), яке гальмує розвиток науки, економіки та підриває довіру до влади [5]. Обґрунтованість також передбачає вибір мінімально необхідного ступеня секретності («таємно», «цілком таємно» чи «особливої важливості»), який би відповідав масштабам потенційної шкоди. У 2026 році доктрина інформаційного права наголошує на тому, що обґрунтованість має бути динамічною: якщо обставини змінилися і загроза зникла, інформація має бути негайно розсекречена [2].

Своєчасність як принцип засекречування має двоїсту природу: з одного боку, це встановлення обмеження доступу саме в той момент, коли інформація виникає або стає критично важливою, а з іншого — це вчасне розсекречування відомостей після втрати ними актуальності. В умовах воєнного стану своєчасність набула критичного значення для збереження життів та стратегічної ініціативи, оскільки затримка у засекречуванні навіть на кілька годин може призвести до незворотних наслідків [5]. Водночас демократичний стандарт вимагає встановлення чітких строків секретності, після закінчення яких дані стають публічним надбанням. Своєчасність також передбачає регулярний перегляд грифів обмеження доступу, щоб запобігти ситуації, коли застарілі дані залишаються таємними лише через бюрократичну інерцію [4].

Взаємодія цих трьох принципів у 2026 році реалізується через цифрові реєстри та автоматизовані системи контролю, що дозволяє мінімізувати суб’єктивний чинник. Демократичне суспільство вимагає, аби процедура засекречування була прозорою на етапі її нормативного визначення, а обґрунтованість — перевірялася незалежними інституціями або судом у разі

виникнення спору. Тільки неухильне дотримання законності, ретельне обґрунтування шкоди та оперативність у зміні статусів інформації дозволяють державі ефективно захищатися, не перетворюючись при цьому на закриту систему [6]. Таким чином, ці принципи є не просто технічними правилами, а юридичними гарантіями того, що таємниця служить безпеці народу, а не приховуванню дій влади [3].

РОЗДІЛ 2. ПРАВОВИЙ МЕХАНІЗМ ТА ПРОЦЕДУРА ЗАСЕКРЕЧУВАННЯ ІНФОРМАЦІЇ В УКРАЇНІ

2.1. Правовий статус суб'єктів формування та охорони державної таємниці (Державний експерт з питань таємниць).

Правовий статус суб'єктів формування та охорони державної таємниці в Україні у 2026 році визначається специфікою їхніх повноважень щодо легітимного обмеження доступу до стратегічно важливої інформації. Ключовою фігурою в цій системі є Державний експерт з питань таємниць (ДЕПТ), чий статус поєднує адміністративні функції посадової особи та експертно-аналітичні повноваження. Згідно із Законом України «Про державну таємницю», ДЕПТ не є штатною посадою, а є особливим правовим статусом, який надається керівникам міністерств, інших центральних органів виконавчої влади та державних органів вищого рівня [1]. Юридична природа статусу експерта полягає у його персональній відповідальності за обґрунтованість віднесення відомостей до державної таємниці, встановлення ступеня секретності та зміну або скасування грифів секретності. ДЕПТ діє на підставі положення, затвердженого Кабінетом Міністрів України, та здійснює свої повноваження у тісній взаємодії зі Службою безпеки України (СБУ), яка є державним органом, спеціально уповноваженим у сфері охорони таємниць [3].

Основними функціями Державного експерта є розробка та погодження розгорнутих переліків відомостей, що становлять державну таємницю, у відповідній галузі державного управління. Правовий статус ДЕПТ передбачає право залучати фахівців для проведення експертизи, визначати матеріальні збитки від розголошення таємниці та приймати рішення про передачу секретної інформації іншим державам або міжнародним організаціям [5]. Важливою складовою статусу є незалежність експерта при прийнятті рішень: на нього не може чинитися тиск з метою безпідставного засекречування інформації для приховування правопорушень або помилок у діяльності органів влади. У 2026

році, в умовах цифровізації оборонної сфери, статус ДЕПТ доповнився обов’язком контролювати безпеку алгоритмів автоматизованого оброблення секретних даних у хмарних сховищах та захищених мережах зв’язку [2].

Окрім Державного експерта, до суб’єктів формування та охорони таємниці належать керівники установ, де проводяться секретні роботи, та працівники режимно-секретних органів (РСО). Правовий статус РСО визначається як статус спеціального підрозділу, що безпосередньо підпорядковується керівнику установи та забезпечує технічний захист, облік і контроль за дотриманням встановленого режиму таємності [8]. Суб’єкти охорони зобов’язані здійснювати перевірку надійності осіб, які претендують на допуск до таємниці, та впроваджувати заходи фізичного та кібернетичного захисту секретних носіїв. Співвідношення повноважень ДЕПТ та РСО полягає в тому, що експерт формує зміст таємниці (інтелектуальна складова), а РСО та СБУ забезпечують її фактичну недоторканність (організаційно-технічна складова) [3].

Відповідальність суб’єктів у цій сфері є суворою: Державний експерт несе персональну юридичну відповідальність за шкоду, завдану національним інтересам через надмірне або недостатнє засекречування. У демократичному суспільстві статус ДЕПТ також передбачає підзвітність перед судом у разі оскарження його рішень громадянами чи організаціями. Таким чином, правовий статус суб’єктів охорони державної таємниці у 2026 році трансформувався у сервісно-безпекову модель, де головним завданням є не просто тотальне закриття інформації, а динамічне управління секретністю задля забезпечення виживання держави в умовах високотехнологічних загроз [4].

2.2. Процедура віднесення інформації до державної таємниці: від розроблення Зводу відомостей до надання грифу секретності.

Процедура віднесення інформації до державної таємниці в Україні у 2026 році являє собою суворо регламентований адміністративно-правовий цикл, що базується на принципах обґрунтованості та достатності захисту національних інтересів. Початковим етапом цього процесу є розроблення та періодичне оновлення Зводу відомостей, що становлять державну таємницю (ЗВДТ). ЗВДТ — це єдиний систематизований перелік категорій інформації, розголошення яких може завдати шкоди суверенітету чи обороноздатності держави. Формування цього документа здійснюється Службою безпеки України на підставі рішень Державних експертів з питань таємниць у відповідних сферах. Кожна позиція у Зводі повинна мати чітке юридичне обґрунтування та відповідати критеріям, визначеним статтею 8 Закону України «Про державну таємницю» [1]. У 2026 році ЗВДТ адаптований до викликів цифрової війни, включаючи відомості про алгоритми захисту критичної інфраструктури та специфікації вітчизняних систем безпілотних технологій [3].

Наступним кроком є проведення експертизи конкретних відомостей Державним експертом з питань таємниць (ДЕПТ). Експерт аналізує, чи підпадає певна інформація (наприклад, план військової операції або параметри новітнього озброєння) під одну з категорій Зводу. На цьому етапі визначається не лише факт секретності, а й ступінь потенційної шкоди, яку може спричинити витік даних. На підставі цього аналізу ДЕПТ приймає рішення про віднесення інформації до державної таємниці, де фіксується рівень секретності («особливої важливості», «цілком таємно» або «таємно»), обґрунтовується необхідність обмеження доступу та встановлюється строк дії цього обмеження [2]. У демократичному суспільстві це рішення має бути позбавлене суб'єктивізму, оскільки надмірне засекречування (over-classification) визнається правопорушенням, що перешкоджає прозорості державного управління [5].

Завершальним етапом процедури є безпосереднє надання грифу секретності матеріальному носію інформації (документу, виробу, цифровому файлу). Гриф секретності — це реквізит, який свідчить про рівень обмеження доступу та супроводжується зазначенням органу, що здійснив засекречування, номера рішення ДЕПТ та дати розсекречування. Процес маркування здійснюється режимно-секретними органами (РСО) установи, де було створено документ. Важливо, що у 2026 році процедура надання грифу для цифрових документів включає автоматичну генерацію метаданих у захищених системах електронного документообігу, що унеможливлює несанкціоноване копіювання чи зміну статусу документа без відповідного протоколювання [4].

Правова природа всієї процедури полягає у легітимному вилученні інформації з вільного обігу. Вона завершується реєстрацією секретного документа в облікових формах РСО, після чого на нього поширюється спеціальний правовий режим зберігання, передачі та знищення. Будь-яке відхилення від описаного алгоритму — наприклад, надання грифу відомостям, що не включені до ЗВДТ, — тягне за собою юридичну нікчемність акта засекречування та адміністративну відповідальність посадових осіб. Таким чином, процедура забезпечує баланс між «правом знати» та «необхідністю захищати», що є критично важливим для виживання держави в умовах гібридних загроз [6].

2.3. Захист матеріальних носіїв секретної інформації: правові та технічні аспекти кібербезпеки.

Захист матеріальних носіїв секретної інформації у 2026 році трансформувався у комплексну систему, де правові норми невід’ємно поєднуються з високотехнологічними протоколами кібербезпеки. Правова природа захисту матеріальних носіїв (паперових документів, електронних дисків, флеш-накопичувачів, а також серверного обладнання) базується на

Законі України «Про державну таємницю» та нормах законодавства про технічний захист інформації. Юридичний аспект передбачає створення спеціального правового режиму поводження з носієм, що включає обов’язкову сертифікацію обладнання, державну експертизу засобів захисту та персональну відповідальність осіб, які мають допуск. У 2026 році до правового статусу носія додано вимогу про обов’язкову цифрову ідентифікацію кожного примірника, що дозволяє відстежувати його життєвий цикл у режимі реального часу через захищені державні реєстри [1]. Будь-який несанкціонований доступ до носія або порушення правил його зберігання (наприклад, винесення за межі режимного об’єкта) тягне за собою кримінальну відповідальність, оскільки матеріальний носій розглядається як критичний актив національної безпеки [3].

Технічні аспекти кібербезпеки матеріальних носіїв у сучасних умовах воєнного стану фокусуються на запобіганні дистанційному зчитуванню та фізичному зламу. Для електронних носіїв обов’язковим є використання криптографічних засобів захисту, що мають атестат відповідності ДССЗЗІ. Це включає повне шифрування диска (Full Disk Encryption) з використанням алгоритмів, стійких до квантових обчислень. Важливим технічним нововведенням 2026 року є впровадження активних систем радіоелектронного маскування навколо місць зберігання носіїв, що нівелює можливість перехоплення ПРВВ (побічних електромагнітних випромінювань та наводок) [5]. Окрім того, самі носії оснащуються датчиками цілісності та системами автоматичного знищення даних (remote wipe або physical destruction) у разі спроби несанкціонованого розтину корпусу чи підбору пароля [2].

Співвідношення правових та технічних аспектів реалізується через систему комплексного захисту інформації (КСЗІ). Право зобов’язує суб’єктів господарювання та державні органи створювати такі системи, а техніка забезпечує їхню фактичну працездатність. У 2026 році акцент змістився на захист носіїв у «хмарному» середовищі (Virtual Media Centers), де правовий статус фізичного сервера за кордоном має відповідати вимогам українського

законодавства про державну таємницю. Це вимагає застосування технології конфіденційних обчислень (Confidential Computing), де дані залишаються зашифрованими навіть під час обробки в пам’яті сервера [4]. Доктрина інформаційного права наголошує, що захист носія є ефективним лише тоді, коли правова норма підкріплена непроникним технічним бар’єром, а технічне рішення має чітку юридичну легітимізацію [6]. Таким чином, сучасна кібербезпека секретних носіїв — це симбіоз криптографії, фізичної інженерії та адміністративного контролю, спрямований на збереження «цифрової тиші» держави в умовах глобальної прозорості [5].

РОЗДІЛ 3. ПРОБЛЕМИ ОПТИМІЗАЦІЇ ТА ПРАВОВІ ГАРАНТІЇ В ПРОЦЕСАХ ЗАСЕКРЕЧУВАННЯ

3.1. Особливості засекречування інформації в умовах дії правового режиму воєнного стану.

Особливості засекречування інформації в умовах дії правового режиму воєнного стану у 2026 році визначаються необхідністю забезпечення максимальної оперативності прийняття рішень та динамічного реагування на загрози національній безпеці, що виходять за межі стандартних бюрократичних процедур. Правова природа засекречування у цей період трансформується з консервативної моделі у функціональну, де пріоритетом є збереження «стратегічної раптовості» та захист життів військовослужбовців і цивільного населення. Згідно із Законом України «Про правовий режим воєнного стану» та спеціальними нормами інформаційного законодавства, повноваження щодо обмеження доступу до відомостей суттєво розширюються для військового командування та військових адміністрацій. Ключовою особливістю є можливість тимчасового засекречування даних, які за звичайних обставин могли б бути відкритими (наприклад, графіки руху транспорту, точні локації об'єктів енергетики або детальні дані про закупівлі), якщо їх розголошення може бути використане ворогом для планування атак [9].

Важливою процедурною особливістю є спрощення механізму віднесення інформації до державної таємниці в зоні бойових дій та на прилеглих територіях. У 2026 році доктрина інформаційного права оперує поняттям «оперативне засекречування», що дозволяє командирам певних рівнів встановлювати тимчасові грифи обмеження доступу на термін проведення конкретної операції без негайного залучення Державного експерта з питань таємниць, але з подальшою легалізацією цих рішень у встановленому порядку [3]. Це забезпечує гнучкість управління інформаційними ризиками. Окрім того, воєнний стан зумовив появу «гібридних» режимів доступу, коли інформація

про об’єкти критичної інфраструктури засекречується технічно (через кіберзахист та обмеження доступу до реєстрів), навіть якщо вона формально не внесена до Зводу відомостей, що становлять державну таємницю, як постійна категорія [5].

Технологічний аспект засекречування під час воєнного стану включає тотальне шифрування каналів передачі оперативних даних та використання систем «автоматичного грифування» цифрового контенту, створеного в автоматизованих системах управління військами (АСУ). Правовий статус такої інформації визначається не лише паперовим документом, а набором метаданих у захищеній мережі. Специфікою також є посилення контролю за «сегментованим доступом» (need-to-know basis), коли навіть особи з високим допуском отримують доступ лише до того вузького фрагмента таємниці, який необхідний для виконання поточного бойового завдання [4]. Це мінімізує шкоду у разі потрапляння носіїв інформації до рук ворога або здійснення успішної кібератаки [2].

Етико-правова дилема засекречування під час війни полягає у дотриманні балансу між військовою необхідністю та суспільним інтересом. У 2026 році законодавство чітко встановлює, що навіть у стані війни заборонено засекречувати відомості про порушення прав людини, екологічні катастрофи або нецільове використання гуманітарної допомоги. Контроль за правомірністю засекречування здійснюється через спеціальні парламентські комітети та Службу безпеки України, що запобігає зловживанням режимом секретності для приховування управлінських помилок [6]. Таким чином, система засекречування в умовах воєнного стану — це динамічний «цифровий щит», який забезпечує виживання держави, залишаючись при цьому в межах конституційних гарантій демократичного суспільства [3].

3.2. Правовий інститут розсекречування інформації: підстави, терміни та суспільний контроль.

Правовий інститут розсекречування інформації в інформаційному праві України у 2026 році розглядається як ключовий демократичний запобіжник проти безстрокового та безпідставного обмеження доступу до суспільно значущих відомостей. Розсекречування — це юридичний процес скасування раніше встановленого грифу секретності, що призводить до відновлення режиму відкритості інформації. Правова природа цього інституту базується на презумпції відкритості публічної інформації: будь-яке засекречування є тимчасовим відхиленням, а розсекречування — поверненням до правової норми. Згідно із законом, підставами для розсекречування є: закінчення встановлених строків дії грифу секретності; втрата актуальності відомостей для національної безпеки (наприклад, через зміну військово-політичної обстановки або технологічний прогрес); скасування самого Зводу відомостей, що становлять державну таємницю, у відповідній частині; а також виявлення фактів незаконного засекречування інформації, яка за законом не може бути таємною (відомості про стан довкілля, якість харчових продуктів, аварії, порушення прав людини та корупцію) [1].

Терміни розсекречування інформації у 2026 році жорстко регламентовані та диференційовані залежно від ступеня секретності. Для відомостей з грифом «таємно» максимальний строк становить 5 років, «цілком таємно» — 10 років, «особливої важливості» — 30 років. Проте ці терміни не є автоматичними підставами для продовження секретності; Державний експерт з питань таємниць зобов'язаний кожні 5 років проводити перевірку актуальності грифів. Окремим випадком є розсекречування архівних документів радянських спецслужб, де діє принцип повної відкритості без обмеження строком, за винятком випадків, коли оприлюднення загрожує життю конкретних осіб. В умовах 2026 року впроваджено систему «цифрової депозітарної ревізії», яка

автоматично сповіщає розпорядників про наближення терміну закінчення грифу, що мінімізує людський фактор та бюрократичні затримки у наданні доступу до даних [5].

Суспільний контроль за процесом розсекречування є невід'ємним елементом демократичного врядування. Він реалізується через декілька механізмів: парламентський контроль (через профільні комітети Верховної Ради), діяльність Уповноваженого Верховної Ради з прав людини та через судову гілку влади. Громадяни та громадські організації мають право оскаржувати в адміністративному суді рішення про відмову у розсекречуванні або продовження строків секретності. Суд, застосовуючи «трискладовий тест», оцінює, чи дійсно шкода від оприлюднення переважає суспільний інтерес на даному етапі. У 2026 році роль суспільного контролю посилилася завдяки діяльності незалежних експертних рад при державних органах, які мають право ініціювати перегляд доцільності секретності певних масивів даних, що не стосуються оперативних воєнних планів [2].

Правова природа розсекречування також включає «інститут розголошення в суспільних інтересах» (whistleblowing), коли особа звільняється від відповідальності за поширення секретної інформації, якщо вона доведе, що суспільна значущість викриття злочину чи загрози життю була вищою за формальну вимогу секретності. Це створює систему «стримувань і противаг», де таємниця служить безпеці народу, а не інтересам окремих посадових осіб. Таким чином, інститут розсекречування у 2026 році — це динамічний правовий інструмент, що забезпечує транспарентність держави та запобігає «інформаційній інерції» в епоху цифрових комунікацій [4].

3.3. Юридична відповідальність за неправомірне засекречування та розголошення охоронюваних законом відомостей.

Юридична відповідальність за правопорушення у сфері засекречування та розголошення відомостей в інформаційному праві України у 2026 році має дворівневу структуру, що спрямована на захист державної безпеки, з одного боку, та забезпечення прозорості влади — з іншого. Правова природа відповідальності за неправомірне засекречування базується на недопустимості використання режиму секретності для приховування правопорушень, корупції або обмеження прав людини. Згідно з Кодексом України про адміністративні правопорушення та законом «Про державну таємницю», безпідставне віднесення інформації до державної таємниці, а також надання грифу секретності відомостям, які не включені до Зводу відомостей (ЗВДТ), тягне за собою адміністративну відповідальність посадових осіб. У 2026 році судова практика активно застосовує санкції за «надмірне засекречування» (over-classification), що розцінюється як перешкоджання законній діяльності журналістів та правозахисних організацій [11]. Якщо неправомірне засекречування призвело до тяжких наслідків для бюджету або приховування тяжких злочинів, посадові особи можуть нести дисциплінарну або навіть кримінальну відповідальність за зловживання службовим становищем [3].

Відповідальність за розголошення охоронюваних законом відомостей є значно суворішою, особливо в умовах правового режиму воєнного стану. Кримінальний кодекс України (статті 328, 329, 330) передбачає суворі санкції за розголошення державної таємниці, втрату носіїв таємної інформації або передачу відомостей, що становлять службову інформацію, іноземним організаціям. Об’єктивною стороною таких злочинів є поширення даних будь-яким способом (вербальним, цифровим, через публікації), що робить їх доступними стороннім особам. У 2026 році особлива увага приділяється «цифровому розголошенню» — публікації фото чи відео з елементами

оборонної інфраструктури або геолокації військ у соціальних мережах, що кваліфікується як несанкціоноване поширення інформації про ЗСУ (ст. 114-2 ККУ) [5]. Важливою правовою гарантією є суб'єктивна сторона: для кваліфікації як «розголошення державної таємниці» особа повинна була мати офіційний допуск до неї та знати про її статус [2].

Співвідношення видів відповідальності залежить від статусу інформації та суб'єкта правопорушення. За розголошення конфіденційної інформації (персональних даних, комерційної таємниці) настає цивільно-правова відповідальність у формі відшкодування збитків та моральної шкоди, а також адміністративна відповідальність за порушення правил захисту даних [6]. За розголошення службової інформації найчастіше застосовується дисциплінарна відповідальність (звільнення, догана). Однак у 2026 році в межах гармонізації з правом ЄС (Digital Services Act) впроваджено підвищену відповідальність для IT-адміністраторів та провайдерів за неналежне забезпечення кіберзахисту секретних масивів даних, що призвело до їх витоку. Доктрина інформаційного права наголошує, що юридична відповідальність виконує не лише каральну, а й превентивну функцію, стимулюючи суб'єктів дотримуватися балансу між конституційним правом на інформацію та обов'язком зберігати державні інтереси [4].

ВИСНОВКИ

Проведений аналіз правового регулювання інституту засекречування інформації в Україні дозволяє сформулювати цілісну систему висновків, що відображають теоретичну складність та практичну значущість даного правового явища в сучасних умовах:

Доведено, що засекречування інформації є специфічною формою обмеження конституційного права на доступ до інформації, яка в інформаційному праві розглядається як динамічний процес віднесення відомостей до державної таємниці. Генеза цього інституту свідчить про поступовий перехід від закритої радянської моделі «тотальної секретності» до демократичної системи, заснованої на принципах необхідності та пропорційності. Встановлено, що ключовою ознакою законного засекречування є наявність реальної загрози національній безпеці у разі розголошення конкретних даних, а не лише формальна належність відомостей до певного переліку.

З’ясовано, що правовий механізм засекречування в Україні базується на чіткій ієрархії суб’єктів, де центральна роль належить Державним експертам з питань таємниць. Процедура надання грифу секретності («Особливої важливості», «Цілком таємно», «Таємно») є багатоступеневою і включає експертну оцінку шкоди, яку може бути заподіяно інтересам держави. Виявлено, що в умовах цифровізації особливого значення набуває захист матеріальних носіїв секретної інформації, де правові норми мають тісно корелюватися з технічними стандартами кібербезпеки та криптографічного захисту, щоб унеможливити несанкціонований витік даних через інформаційні мережі.

Встановлено, що правовий режим воєнного стану суттєво трансформував практику засекречування, змістивши акцент на оперативність обмеження доступу до стратегічних даних про обороноздатність. Проте, аналіз свідчить

про ризик «оверкласифікації» (надмірного засекречування), що може створювати перешкоди для громадського контролю та антикорупційного моніторингу. Тому інститут розсекречування інформації має розглядатися не як виняткова подія, а як обов’язковий регулярний перегляд актуальності грифів секретності. Юридична відповідальність за порушення у цій сфері повинна бути збалансованою: суворою за розголошення реальних таємниць і водночас невідворотною за неправомірне приховування суспільно значущої інформації під виглядом державної таємниці.

Перспективи вдосконалення законодавства лежать у площині гармонізації вітчизняних стандартів секретності із протоколами НАТО та запровадження електронного реєстру розсекречених документів. Реформування має спрямовуватися на створення системи, де державна таємниця захищається максимально жорстко, але межі її визначення залишаються прозорими та зрозумілими для громадянського суспільства, що є невід’ємною ознакою правової держави.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про державну таємницю: Закон України від 21.01.1994 р. № 3855-XII [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/3855-12

2. Арістова І. В. Інформаційне право: підручник. Київ: Юрінком Інтер, 2024. 352 с.

3. Костицький В. В. Теорія інформаційного права: монографія. Київ: Наукова думка, 2023. 280 с.

4. Марущак А. І. Правове регулювання цифрових послуг в умовах євроінтеграції України. Право і суспільство. 2025. № 2. С. 115–122.

5. Бєляков К. І. Інформаційне право України: підручник. Київ: КНТ, 2025. 384 с.

6. Кохановська О. В. Цивільно-правові аспекти захисту інформаційних прав в Україні. Київ: Академіка, 2024. 312 с.

7. Закон України «Про інформацію» від 02.10.1992 № 2657-XII. [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show

8. Положення про режимно-секретні органи в міністерствах, інших центральних органах виконавчої влади. Затверджено постановою КМУ. [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show

9. Закон України «Про правовий режим воєнного стану» від 12.05.2015 № 389-VIII. [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show

10. Костицький В. В. Теорія інформаційного права: монографія. Київ: Наукова думка, 2023. 280 с.

11. Кримінальний кодекс України від 05.04.2001 № 2341-III. [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show